ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Developing Resilience and Cyber-Physical Protection Capabilities in Critical Aviation Infrastructures

Georgia Lykou

A dissertation submitted for the partial
fulfillment of a Ph.D. degree

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
SCHOOL OF INFORMATION SCIENCES & TECHNOLOGY

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
DEPARTMENT OF INFORMATICS

May 2021

Department of Informatics
Athens University of Economics & Business, Greece

(this page is intentionally left blank)

Supervising Committee:

1. **Gritzalis Dimitris**, Professor, Department of Informatics, Athens University of Economics & Business, Director of the Master's Program in Information Systems, Director of the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infosec.aueb.gr). (Chair)
2. **Magkos Emmanouil**, Associate Professor, Head of the Department of Informatics, Ionian University
3. **Kotzanikolaou Panayiotis**, Associate Professor, Department of Informatics, University of Piraeus

Examination Committee:

1. **Gritzalis Dimitris**, Professor, Department of Informatics, Athens University of Economics & Business
2. **Apostolopoulos Theodoros**, Professor, Department of Informatics, Athens University of Economics & Business
3. **Mavridis Ioannis,** Professor, Department of Applied Informatics, University of Macedonia
4. **Stamatiou Ioannis,** Professor, Department of Business Administration, University of Patras
5. **Magkos Emmanouil**, Associate Professor, Head of the Department of Informatics, Ionian University
6. **Kotzanikolaou Panayiotis**, Associate Professor, Department of Informatics, University of Piraeus
7. **Stergiopoulos George,** Assistant Professor, Department of Information and Communication Systems Engineering, University of the Aegean

Developing Resilience and Cyber-Physical Protection Capabilities in Critical Aviation Infrastructures

by

Georgia Lykou

Department of Informatics
Athens University of Economics and Business

76 Patission Ave., Athens GR-10434, Greece

"Η έγκριση διδακτορικής διατριβής υπό του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών δεν υποδηλοί αποδοχή των γνωμών του συγγραφέως."

(Ν. 5343/ 1932, άρθρο. 202)

Acknowledgements

First and foremost, I would like to thank my Ph.D. supervisor Prof. Dimitris Gritzalis. He was the one, the charismatic professor who inspired me, during my undergraduate studies in Information Systems, about Cybersecurity. For more than 8 years, he has guided me through my postgraduate and doctoral studies to work on research areas about Information Security and Critical Infrastructure Protection.

Secondly, I would like to thank ass. Prof. George Stergiopoulos for his guidance during my academic path. His passion for hard working and research contribution was very influencing on my work, trying always to improve my deliverables, so as to achieve excellence.

I am also grateful that I shared my research journey with honorable professors like Prof. Panayiotis Kotzanikolaou, Prof. Emmanouil Magkos, Prof. Theodoros Apostolopoulos, Prof. Alexios Mylonas, and Dr. Marianthi Theocharidou. They were the ones that helped me the most on my first research steps, either by co-authoring, reviewing my work, tutoring, and guiding me how to build knowledge and survey new scientific areas. I have really appreciated their support and professionalism.

During my academic studies, I was so fortunate to have colleagues like Argiro Anagnostopoulou, Despoina Mentzelioti, George Iakovakis, Stratos Vasilelis and Panayiotis Dedousis. We worked together as a win-win team, so I am thankful for their support, their excellent cooperation, and their valuable friendship during all these years.

Finally, I would like to thank all the people who stood right beside me in my entire life; my parents Ioannis & Aggeliki and my sister Lilian for their unselfish love and unconditional support, which was always inspiring for me, so as to become a better human being. Foremost, I would like to thank my beloved husband George Starakis, for coping with me all these years, for his endless support, love, and patience. Last but not least, I am grateful for sharing this journey with my precious children Nikolas & Angela, since we studied together all these years, growing up together. Hopefully, ‘mum’ is going to graduate her academic studies first, so as to proudly support her successors afterwards, and in the near future to congratulate them, while they will be progressing in their own academic paths.

Dedication

This dissertation is dedicated to my beloved family!

To the people, who stood beside me all these years,

succoring me to achieve my goals during my PhD Studies.

Abstract

Critical Infrastructures (CIs) are the backbone of society's prosperity and remain highly interconnected, whether they manifest as processes, systems, facilities, assets, or services. The modeling and analysis of these interdependencies is a research field of increasing interest for protecting CIs from threatening human actions and natural phenomena. Transport sector is a critical infrastructure that greatly supports the smooth functioning of society's welfare and viability of economies worldwide. Disruptions to transportation systems can cause large economic impacts or even human losses, so they should be adequately protected from physical and cyber-physical threats.

Regarding physical threats, climate change is an upcoming and unavoidable challenge that all critical infrastructures including transport sector will have to face in the future. Although transport sector substructures are exposed to environmental threats and they are designed to withstand weather-related stressors, shifts in climate patterns are projected to greatly increase potential risks. The area of climate adaptation planning is still relatively new, however new methodologies for assessing risks and reducing vulnerabilities to climate change are currently being developed. In our research, we have focused on climate-related risks and adaptation planning, while we provided a detailed classification and analysis of available climate change adaptation tools, which can support risk management policies in the transport sector. We demonstrated that the integration of climate change adaptation approaches, strategies, and action plans can enhance the design of new and reformed infrastructures. Furthermore, such initiatives can increase CIs robustness and life span, while minimizing unplanned outages, failures, and corrective maintenance costs.

Regarding cyber-physical threats, we focused our research on aviation sector, which is the safest transport mode, however the most interdepended one in terms of information and communication technologies applied. Cyber-attacks are increasing in quantity and persistence, so the consequences of a successful malicious cyber-attack to civil aviation operations could be severe nowadays. Initially, we performed an online survey to explore the cybersecurity resilience of commercial airports, which provide advanced services to travelers, by enhancing their operations with automation controls and smart applications. We have explored how technological advances and IoT technologies may change the security threat models and influence the operational efficiency of smart airports. This dissertation has scrutinized: (a) the implementation rate of cybersecurity measures in commercial airports; (b) malicious threats and risks occurred from vulnerabilities in Information and Communication Systems (ICS), Internet of Things (IoT) applications, and a variety of smart devices that interact in airport facilities; (c) risk scenario analysis for nefarious attacks against ICS/IoT systems with mitigation measures. Aiming to enhance operational practices and develop robust cybersecurity governance in smart airports, we have presented a systematic and comprehensive analysis of unlawful attacks towards smart airports, to facilitate airport community comprehend risks and proactively act, by implementing cybersecurity best practices and resilience measures.

Thereafter, we have focused on the area of Air Traffic Management, where the increase of capacity and efficiency has led to an enormous effort of transition towards digitalization and automation. As a result, formerly separated IT systems get connected via newly established networks for information and data exchange. Due to the growth of

complexity the attack surface has increased, while previously unknown interdependencies have been created. Limiting security risk management to "traditional" physical aspects, like air terrorism, is no longer sufficient to ensure robust operations in air transportation. Cyber-security should be enhanced by more resilient focused approaches. As both safety and security are drivers for the determination of resilience requirements, an integrated view is needed on both subjects to foster the consistency of resilience concepts in aviation. Our research examined cyber security challenges and interoperability in ATM systems and proposed an extended threat model for analyzing possible targets and risks involved. We also analyzed cyber resilience aspects in the aviation context and the need for holistic strategy of defense, prevention, and response. Under the resilience umbrella, all aviation actors should work on a collaborative and risk-based framework, in order to address security threats and increase the aviation systems resilience against future attacks.

Furthermore, as the fastest growing segment of aviation, unmanned aerial systems (UAS) continue to increase in number, technical complexity, and capabilities. Numerous civilian and commercial uses are drastically transforming civil protection, asset delivery, commercial and entertaining activities. However, UAS pose significant challenges in terms of safety, security, and privacy within society. An increasing phenomenon, nowadays, is drone-related incidents near airport facilities, which are expected to proliferate in frequency and severity, as drones become larger and more powerful. Critical infrastructures need to be protected from such aerial attacks, through effective counteracting technologies, risk management, and resilience plans. In this dissertation, we have presented a survey on drone incidents near airports and explored how counter drone technologies can prevent, detect, identify, and mitigate rogue drones. We have analyzed realistic attack scenarios of malicious drones' attacks and proposed an effective C-UAS protection plan for each case. We have also discussed the applicability limitations of C-UAS in the aviation context and proposed a resilience action plan for airports stakeholders for defending airborne threats from misused drones.

The integration of our research in the aviation sector, focused on air transport networks and introduced a risk-based method to analyze interdependencies and congestions in the aviation network. Since traffic delays incidents in air transport networks appear to have variable performance and stochastic nature, dependency graphs have been proposed to understand the delay propagation phenomenon and analyze such cascading events. The proposed methodology and developed software tool can assess delay incidents in airports and produce weighted risk dependency graphs, presenting how a delay that occurred in one airport may affect the operational efficiency of other interconnected airports. The tool can also detect the most critical airports and congested connections, based on their delay contribution in dependency chains, while it can indicate the n-order dependency chains, which should be avoided by airline flight planners, to reduce delay impacts in the aviation network.

Finally, aggregating the environmental and technological aspects that make CIs more resilient, we have developed a holistic methodology for assessing sustainability which can be applied to CIs Data Centers (DC). A scoring model evaluates how green, efficient, resilient, and sustainable can be the examined DC. This model can assist DC owners and operators to evaluate the sustainability of their facilities and take appropriate measures to increase their operating efficiency, security, and resilience, while reducing environmental footprint and step towards carbon neutral design of CIs.

Extended abstract (in Greek)

Οι Κρίσιμες Υποδομές (ΚΥ) αποτελούν αλληλένδετα συστήματα και εγκαταστάσεις, που υποστηρίζουν τις ζωτικές λειτουργίες μιας κοινωνίας με επίκεντρο την υγεία, την ασφάλεια, την οικονομική και κοινωνική ευημερία των πολιτών της. Η μοντελοποίηση και η ανάλυση των αλληλεξαρτήσεων των ΚΥ είναι ένας νέος ερευνητικός τομέας ζωτικής σημασίας για την αποτελεσματική προστασία τους από κακόβουλες ανθρώπινες παρεμβάσεις και φυσικά φαινόμενα. Ο τομέας των μεταφορών είναι μια ΚΥ, που λειτουργεί ως πυλώνας της ομαλής λειτουργίας της οικονομίας, της ευημερίας και της βιωσιμότητας των κοινωνιών, συνδέοντας ανθρώπους, κράτη και πολιτισμούς σε τοπικό και παγκόσμιο επίπεδο. Η δυσλειτουργία ή διακοπή της λειτουργίας των συστημάτων μεταφοράς μπορεί να προκαλέσει μεγάλες οικονομικές επιπτώσεις, ακόμη και ανθρώπινες απώλειες, επομένως θα πρέπει να προστατεύονται επαρκώς, τόσο από φυσικές απειλές, όσο και από απειλές του κυβερνοχώρου.

Όσον αφορά τις φυσικές απειλές, η κλιματική αλλαγή είναι μια επερχόμενη και αναπόφευκτη πρόκληση της εξέλιξης της αειφορίας του πλανήτη μας. Είναι ανάγκη να υπάρξει μια επαρκής προσαρμογή των ΚΥ στις ραγδαίες επιπτώσεις της κλιματικής αλλαγής, συμπεριλαμβανομένου και του τομέα των μεταφορών. Παρόλο που οι μεταφορές και οι ΚΥ που τις εξυπηρετούν έχουν σχεδιαστεί για να αντέχουν σε ακραία καιρικά φαινόμενα, οι μελλοντικές προβλέψεις για την αλλαγή του κλίματος προμηνύουν για σημαντική αύξηση των κινδύνων. Ο σχεδιασμός της προσαρμογής στις επιπτώσεις της κλιματικής αλλαγής είναι ένας νέος ερευνητικός τομέας, όπου αναπτύσσονται νέες μεθοδολογίες για την αξιολόγηση και τη μείωση των ευπαθειών στις επιπτώσεις της κλιματικής αλλαγής. Στην έρευνά μας, παρέχουμε μια λεπτομερή ταξινόμηση και ανάλυση των διαθέσιμων εργαλείων προσαρμογής στην κλιματική αλλαγή, που υποστηρίζουν τον τομέα των μεταφορών και τις πολιτικές διαχείρισης του κινδύνου. Η ενσωμάτωση της προσαρμογής στο σχεδιασμό νέων και αναβαθμισμένων ΚΥ, ειδικά στον τομέα των μεταφορών, που είναι ιδιαίτερα εκτεθειμένος στις επιπτώσεις ακραίων καιρικών φαινομένων, μπορεί να βελτιώσει τη σταθερότητα και τη διάρκεια ζωής των ΚΥ, στηρίζοντας την απρόσκοπτη λειτουργία τους και ελαχιστοποιώντας τις βλάβες και τυχόν κόστη διορθωτικής συντήρησης.

Όσον αφορά τις απειλές στον κυβερνοχώρο, η έρευνά μας επικεντρώθηκε στον τομέα των αερομεταφορών, ο οποίος αποτελεί μεν το ασφαλέστερο μέσο μεταφοράς, ωστόσο είναι και το πιο διασυνδεδεμένο σύστημα ανταλλαγής πληροφοριών με την αξιοποίηση νέων τεχνολογιών επικοινωνίας και επεξεργασίας δεδομένων. Καθώς οι κυβερνο-επιθέσεις αυξάνονται δραματικά τα τελευταία χρόνια, οι συνέπειες μιας επιτυχημένης κακόβουλης επίθεσης στις ψηφιακές υποδομές της πολιτικής αεροπορίας θα μπορούσαν να έχουν πολύ σοβαρό αντίκτυπο στην ασφάλεια των πτήσεων. Αρχικά, πραγματοποιήσαμε μια διαδικτυακή έρευνα για να διερευνήσουμε την ανθεκτικότητα των σύγχρονων αερολιμένων στον τομέα της κυβερνοασφάλειας, καθώς τα τελευταία χρόνια τα αεροδρόμια αναβαθμίζουν τις υποδομές τους προσθέτοντας συστήματα αυτοματισμού και έξυπνες εφαρμογές για τη καλύτερη εξυπηρέτηση των επιβατών. Στην διατριβή αυτή ερευνήσαμε: (α) το ποσοστό εφαρμογής των μέτρων ασφάλειας στον κυβερνοχώρο σε εμπορικούς αερολιμένες, (β) τις κακόβουλες απειλές που εξελίσσονται λόγω της ένταξης των συστημάτων αυτόματου ελέγχου και έξυπνων συσκευών (IoT) στις υποδομές των αεροδρομίων, (γ) την ανάλυση ρεαλιστικών σεναρίων κινδύνου με

κακόβουλες επιθέσεις μέσω αυτοματοποιημένων μηχανισμών και συστημάτων IoT, καθώς και τα μέτρα μετριασμού των απειλών αυτών. Με σκοπό την ενίσχυση των επιχειρησιακών πρακτικών και την ανάπτυξη ισχυρής διακυβέρνησης στον τομέα της κυβερνοασφάλειας, παρουσιάζουμε μια συστηματική και ολοκληρωμένη ανάλυση των κακόβουλων επιθέσεων σε σύγχρονα αεροδρόμια, για την κατανόηση των κινδύνων και την εφαρμογή βέλτιστων πρακτικών κυβερνοασφάλειας και ενίσχυσης της ανθεκτικότητας των υποδομών τους.

Στη συνέχεια, εστιάζουμε στον τομέα της διαχείρισης της εναέριας κυκλοφορίας (ATM), όπου και εδώ η ραγδαία αύξηση της αεροπορικής κίνησης τα τελευταία χρόνια, οδήγησε στην ψηφιοποίηση και τον αυτοματισμό των υποδομών ελέγχου της εναέριας κυκλοφορίας. Ως αποτέλεσμα, τα αρχικώς διαχωρισμένα συστήματα πληροφορικής & επικοινωνιών συνδέονται πλέον με δικτυακές υποδομές για την ανταλλαγή πληροφοριών και δεδομένων. Λόγω της αύξησης της πολυπλοκότητας των δικτύων αυτών, οι ευπάθειες σε απειλές του κυβερνοχώρου έχουν αυξηθεί εκθετικά. Πλέον η διαχείριση του κινδύνου για την ασφάλεια της αεροπορίας δεν μπορεί να εξασφαλιστεί μόνο με τα παραδοσιακά αντίμετρα ασφάλειας, που διαχρονικά λαμβάνονται για την προστασία των ΚΥ στις αερομεταφορές. Η ασφάλεια & προστασία ΚΥ στον κυβερνοχώρο οφείλει να επεκταθεί σε πιο εστιασμένες προσεγγίσεις μετριασμού των κινδύνων του κυβερνοχώρου για την ενίσχυση της ανθεκτικότητας στην αεροπορία. Η διατριβή αυτή εξετάζει τις προκλήσεις ασφάλειας στον κυβερνοχώρο και τη διαλειτουργικότητα των συστημάτων διαχείρισης της εναέριας κυκλοφορίας. Προτείνουμε ένα εκτεταμένο μοντέλο αντιμετώπισης των νέων απειλών που έχουν προκύψει με την ανάλυση πιθανών στόχων και μελλοντικών κινδύνων. Εισάγουμε και αναλύουμε μέτρα ενίσχυσης της ανθεκτικότητας της αεροπορίας από απειλές του κυβερνοχώρου και προτείνουμε μια ολιστική στρατηγική άμυνας, πρόληψης και μετριασμού των απειλών αυτών.

Στην ανάλυση των απειλών της αεροναυτιλίας δεν θα μπορούσε να παραληφθεί η έρευνα στον ταχύτερα αναπτυσσόμενο τομέα της αεροπορίας, που είναι τα λεγόμενα «drones», ή ελληνιστί ΣΜΕΑ ήτοι Μη Επανδρωμένα Εναέρια Αεροσκάφη ή αγγλιστί 'UAS' (Unmanned Aircraft Systems). Τα ΣΜΕΑ συνεχίζουν να αυξάνονται σε τεχνική πολυπλοκότητα και πτητική αξιοπιστία, καθώς η πληθώρα των εμπορικών χρήσεων τους έχουν μεταμορφώσει τις επιχειρησιακές δυνατότητες της πολιτικής προστασίας, τον τρόπο μεταφοράς και παράδοσης αγαθών, καθώς και τις εμπορικές και ψυχαγωγικές δραστηριότητες. Ωστόσο, τα drones θέτουν σημαντικές προκλήσεις στην ασφάλεια, στην προστασία και στην ιδιωτικότητα της κοινωνίας μας. Ένα αυξανόμενο φαινόμενο, στις μέρες μας, είναι τα περιστατικά που σχετίζονται με την ανεπιθύμητη εμφάνιση drones πλησίον αεροπορικών εγκαταστάσεων. Τέτοια φαινόμενα αναμένεται να πολλαπλασιαστούν σε συχνότητα, πολυπλοκότητα και σοβαρότητα στο μέλλον, καθώς τα drones γίνονται όλο και μεγαλύτερα και πιο ισχυρά. Οι κρίσιμες υποδομές πρέπει να προστατευθούν επαρκώς από τέτοιους εναέριους κινδύνους, μέσω αποτελεσματικών τεχνολογιών αντιμετώπισης, σχεδίων διαχείρισης του κινδύνου και ενίσχυσης της ανθεκτικότητας. Στην έρευνα αυτή, παρουσιάζουμε μια έρευνα για συμβάντα με drones κοντά σε αεροδρόμια και αναλύουμε τις τεχνολογίες ανίχνευσης, εντοπισμού και εξουδετέρωσης των drones. Παρουσιάζουμε τα οφέλη, αλλά και τους περιορισμούς των διαθέσιμων τεχνολογιών αντιμετώπισης των drones (C-UAS). Επιπρόσθετα, αναλύουμε ρεαλιστικά σενάρια επίθεσης από κακόβουλα drone και προτείνουμε ένα αποτελεσματικό σχέδιο προστασίας C-UAS για κάθε περίπτωση. Παραθέτουμε τους

περιορισμούς εφαρμογής των συστημάτων C-UAS και προτείνουμε ένα σχέδιο δράσης για την ενίσχυση της ανθεκτικότητας στους αερολιμένες και την υπεράσπιση αυτών από απειλές που χρησιμοποιούν ως μέσο επίθεσης κακόβουλα drones.

Η ολοκλήρωση της έρευνάς μας στον τομέα των αερομεταφορών επήλθε με την αξιολόγηση κινδύνου σε παγκόσμια αεροπορικά δίκτυα, με την ανάλυση αλληλεξαρτήσεων και του κινδύνου διάδοσης καθυστερήσεων στις αερομεταφορές. Δεδομένου ότι τα φαινόμενα των καθυστερήσεων στην εναέρια κυκλοφορία και στις αεροπορικές μεταφορές έχουν ευμετάβλητη φύση και στοχαστικό χαρακτήρα, προτάθηκαν γράφοι απεικόνισης των αλληλεξαρτήσεων αυτών για την κατανόηση της διάδοσης των καθυστερήσεων και την ανάλυση των επερχόμενων συμβάντων. Η μεθοδολογία και το προτεινόμενο εργαλείο λογισμικού που αναπτύξαμε μπορούν να αξιολογήσουν τα περιστατικά καθυστέρησης στα αεροδρόμια και να παράγουν σταθμισμένα γραφήματα αλληλεξαρτήσεων, παρουσιάζοντας πώς μια καθυστέρηση που συνέβη σε ένα αεροδρόμιο μπορεί να επηρεάσει άλλα διασυνδεδεμένα αεροδρόμια. Το λογισμικό μπορεί να ανιχνεύσει τα πιο κομβικά και κρίσιμα αεροδρόμια από πλευράς συνδέσεων με βάση την συμβολή τους σε αλυσίδες πρόκλησης καθυστερήσεων. Διακρίνει επίσης τις δυσμενέστερες αλυσίδες αλληλεξαρτώμενων δρομολογίων, που θα πρέπει να αποφεύγονται από τους επιμελητές πτήσεων και τους σχεδιαστές των αεροπορικών δρομολογίων των αεροπορικών εταιρειών, για τη μείωση των επιπτώσεων καθυστέρησης στο αεροπορικό δίκτυο.

Τέλος, συγκεντρώνοντας την γνώση που δομήθηκε πάνω στην μελέτη και την έρευνα των περιβαλλοντικών και τεχνολογικών παραμέτρων που συμβάλλουν στην ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών, αναπτύξαμε μια ολιστική μεθοδολογία για την αξιολόγηση της βιωσιμότητας των ΚΥ, που μπορεί να εφαρμοστεί σε υπολογιστικά κέντρα δεδομένων (Data Centers / DC), καθώς αυτά πλέον υποστηρίζουν σημαντικά τον αυτοματισμό, την ροή της πληροφορίας και την καταγραφή δεδομένων των κρίσιμων υποδομών κάθε σύγχρονης κοινωνίας. Έτσι προτείνουμε ένα μοντέλο αξιολόγησης που σταθμίζει την αποτελεσματικότητα, την ανθεκτικότητα και την βιωσιμότητα ενός υπολογιστικού κέντρου. Το προτεινόμενο μοντέλο μπορεί να βοηθήσει τους διαχειριστές ΚΥ να αξιολογήσουν τη βιωσιμότητα των εγκαταστάσεων τους και να λάβουν τα κατάλληλα μέτρα διαχείρισης αυτών, αυξάνοντας την αποτελεσματικότητα λειτουργίας, την ασφάλεια και την ανθεκτικότητά τους, μειώνοντας παράλληλα το περιβαλλοντικό αποτύπωμα και προχωρώντας προς τον σχεδιασμό υποδομών με ουδέτερο ανθρακικό αποτύπωμα, συμβάλλοντας ουσιαστικά στην αειφορία του πλανήτη μας.

Η συνεισφορά της διατριβής αυτής στην επιστημονική περιοχή της ασφάλειας, της ανθεκτικότητας και της προστασίας των Κρίσιμων Υποδομών (ΚΥ) συνοψίζεται ως εξής:

• Ανάλυση και ταξινόμηση των εργαλείων και των υφιστάμενων μεθοδολογιών Προστασίας Κρίσιμων Υποδομών (CIP), που υποστηρίζουν τον εντοπισμό των απειλών, την αξιολόγηση ευπαθειών και τη διαχείριση κινδύνου σε ΚΥ. Αναλύονται επίσης οι μορφές αλληλεξαρτήσεων των ΚΥ, καθώς και τα εργαλεία μοντελοποίησης και προσομοίωσης των αλληλεξαρτήσεων των υποδομών αυτών.

• Γίνεται ανασκόπηση και τεχνική ανάλυση των διαθέσιμων εργαλείων αυτό-αξιολόγησης της κυβερνοασφάλειας των συστημάτων ελέγχου και των έξυπνων συσκευών που χρησιμοποιούνται σε ΚΥ για τον έλεγχο και τη συλλογή δεδομένων.

• Γίνεται μια σε βάθος τεχνική ανάλυση των μέτρων προστασίας και προσαρμογής των ΚΥ στις επιπτώσεις της κλιματικής αλλαγής. Η έρευνά μας επικεντρώνεται στην

ταξινόμηση των επιλογών προσαρμογής στον τομέα των μεταφορών, στις προκλήσεις προσαρμογής, αλλά και τις ευκαιρίες βιώσιμης ανάπτυξης που προκύπτουν.

• Ακολουθεί μια πολύπλευρη ταξινόμηση και ανάλυση των διαθέσιμων εργαλείων προσαρμογής στην κλιματική αλλαγή και τις πολιτικές διαχείρισης κινδύνων στον τομέα των μεταφορών.

• Μέσω μιας διαδικτυακής έρευνας, που διεξήχθη ηλεκτρονικά σε χρονικό διάστημα έξι μηνών και της επεξεργασίας των απαντήσεων που λάβαμε, γίνεται η ανάλυση των μέτρων και των βέλτιστων πρακτικών, που εφαρμόζονται για την ενίσχυση της κυβερνοασφάλειας στα σύγχρονα αεροδρόμια σε παγκόσμιο επίπεδο. Μέσα από την έρευνα αυτή εντοπίζονται οι κακόβουλες απειλές, που μπορεί να προσβάλλουν έξυπνες διαδικτυακές συσκευές (εφαρμογές IoT), που όλο συχνότερα εφαρμόζονται στα σύγχρονα αεροδρόμια. Στην συνέχεια αναπτύσσονται σενάρια κακόβουλων επιθέσεων σε έξυπνα αεροδρόμια, με λεπτομερή ανάλυση των επιπτώσεων, των αλληλεπιδράσεων και του κινδύνου, ενώ προτείνονται μέτρα μετριασμού και ενίσχυσης της ανθεκτικότητας από απειλές του κυβερνοχώρου.

• Κατόπιν γίνεται ανάλυση των θεμάτων ασφάλειας στον κυβερνοχώρο για τα συστήματα διαχείρισης εναέριας κυκλοφορίας, όπου προτείνεται ένα μοντέλο ανάλυσης των απειλών, εντοπισμού των ευπαθειών και των πιθανών στόχων, καθώς και ανάλυσης του κινδύνου στον τομέα των αερομεταφορών. Αναπτύσσεται μια ολιστική στρατηγική άμυνας, πρόληψης και προστασίας των σύγχρονων συστημάτων ελέγχου της εναέριας κυκλοφορίας στις απειλές του κυβερνοχώρου για την ενίσχυση της ανθεκτικότητας και της επανατακτικότητας των ΚΥ στον τομέα της διαχείρισης της εναέριας κυκλοφορίας.

• Ακολουθεί μια έρευνα για περιστατικά επιθέσεων από μη επανδρωμένα αεροσκάφη (ΣΜΕΑ ή UAS ή drones) κοντά σε αεροδρόμια, καθώς και μια βιβλιογραφική ανασκόπηση για τις τεχνολογίες ανίχνευσης, εντοπισμού και αντιμετώπισης των απειλών από μη επανδρωμένα ιπτάμενα συστήματα. Εξετάζονται επίσης τα οφέλη και οι περιορισμοί των διαθέσιμων τεχνολογιών αντιμετώπισης των drones (C-UAS) για την υπεράσπιση των αεροδρομίων από την κακόβουλη χρήση μη επανδρωμένων αεροσκαφών.

• Στην συνέχεια αναπτύσσονται ολοκληρωμένα σενάρια επίθεσης και προτείνεται ένα αποτελεσματικό σχέδιο προστασίας έναντι της κακόβουλης χρήσης των drones (C-UAS) για: i) την ενημέρωση των διαχειριστών αερολιμένων και των εμπλεκομένων φορέων στον αεροπορικό τομέα σχετικά με τους κινδύνους ασφάλειας από την αλόγιστη χρήση μη επανδρωμένων αεροσκαφών, ii) την ανάλυση των πλεονεκτημάτων και των περιορισμών που υπάρχουν για τις διαθέσιμες τεχνολογίες C-UAS, και iii) προτείνεται ένα σχέδιο δράσης για την ενίσχυση της ανθεκτικότητας των αερομεταφορών, που οδηγεί στην αύξηση της ευρωστίας των ΚΥ έναντι εναέριων κακόβουλων απειλών στον τομέα της πολιτικής αεροπορίας.

• Η έρευνα στον τομέα των Αερομεταφορών ολοκληρώνεται με την ανάπτυξη μιας μεθοδολογίας, που αναλύει την κυκλοφοριακή συμφόρηση και την αλληλεπίδραση συμβάντων στα αεροπορικά δίκτυα, ως εξής: i) δημιουργεί γραφήματα εξάρτησης των αεροπορικών δικτύων ii) αξιολογεί τον κίνδυνο και τις αλληλεξαρτήσεις από συμβάντα που δημιουργούν κυκλοφοριακή συμφόρηση μεταξύ διασυνδεδεμένων αερολιμένων, iii) παράγει σταθμισμένες αλυσίδες κίνδυνου και αλληλεξαρτήσεων μεταξύ των αερολιμένων και iv) υπολογίζει τον αντίκτυπο και την πιθανότητα καθυστερήσεων στα

αεροδρόμια χρησιμοποιώντας διάφορες μεθόδους αξιολόγησης της συμφόρησης που προκαλείται από τις καθυστερήσεις των αεροσκαφών.

• Με την εφαρμογή ενός λογισμικού που αναπτύχθηκε εφαρμόζοντας την παραπάνω μεθοδολογία ανάλυσης των αλληλεξαρτήσεων γίνεται συγκριτική ανάλυση των δεδομένων των εσωτερικών πτήσεων των Η.Π.Α για τους θερινούς μήνες αιχμής σε δύο διαδοχικά έτη, όπου το εργαλείο παρέχει: α) τις συνδέσεις των πτήσεων με τον υψηλότερο κίνδυνο καθυστέρησης για καθορισμένη χρονική περίοδο, β) τις χειρότερες αλυσίδες καθυστερήσεων στο αεροπορικό δίκτυο, υπολογίζοντας τον συνολικό κίνδυνο συμφόρησης, γ) τα αεροδρόμια που πιο συχνά αποτελούν μέρος των χειρότερων κόμβων και εισάγουν καθυστερήσεις σε μεταγενέστερες πτήσεις και τέλος δ) τις αλυσίδες πτήσεων, που πρέπει να αποφεύγονται από τους προγραμματιστές δρομολογίων και τους επιμελητές πτήσεων, για τη μείωση των επιπτώσεων καθυστέρησης στο αεροπορικό δίκτυο.

• Τέλος προτείνεται ένα ολιστικό μοντέλο αξιολόγησης της βιωσιμότητας, που μπορεί να εφαρμοστεί σε κέντρα δεδομένων, που πλέον αποτελούν τον πυλώνα υποστήριξης του ψηφιακού μετασχηματισμού των ΚΥ. Το προτεινόμενο μοντέλο χρησιμοποιεί μια μεθοδολογία βαθμολόγησης και λαμβάνει υπόψη του όλα τα απαραίτητα στοιχεία για την εκτίμηση της αποδοτικότητας, της ορθολογικής διαχείρισης πόρων, της ανθεκτικότητας και της αειφορίας του εξεταζόμενου κέντρου δεδομένων (Κ.Δ). Αυτό το μοντέλο υποστηρίζει τους διαχειριστές των Κ.Δ στην αξιολόγηση της βιωσιμότητας των εγκαταστάσεων τους και στη λήψη αποφάσεων σχετικά με τις επιλογές ορθολογικής διαχείρισης των ΚΔ, αυξάνοντας την αποτελεσματικότητα της λειτουργίας τους και μειώνοντας παράλληλα το περιβαλλοντικό τους αποτύπωμα.

Η δομή της παρούσας διατριβής οργανώνεται ως εξής:

Στο Κεφάλαιο 1 παρέχονται οι βασικές έννοιες για την εισαγωγή στην ερευνητική περιοχή των ΚΥ που επικεντρώνεται η διατριβή, το ερευνητικό ενδιαφέρον και τα κίνητρα που οδήγησαν τα βήματα της έρευνας αυτής, η ερευνητική δήλωση και η συνεισφορά της διατριβής αυτής στον τομέα της προστασίας των ΚΥ.

Στο Κεφάλαιο 2 παρουσιάζεται το ερευνητικό έργο στην Περιοχή Προστασίας Κρίσιμων Υποδομών, όπου παρέχεται μια ταξινόμηση και σύγκριση των κρίσιμων εργαλείων προστασίας ΚΥ, μαζί με μια ανασκόπηση και ανάλυση των διαθέσιμων εργαλείων αυτοαξιολόγησης της κυβερνοασφάλειας.

Στο Κεφάλαιο 3, συζητούνται οι επιπτώσεις της κλιματικής αλλαγής στον τομέα των μεταφορών. Τεκμηριώνεται η ανάγκη προσαρμογής των υποδομών στις επιπτώσεις της κλιματικής αλλαγής για τη δημιουργία ανθεκτικών και βιώσιμων ΚΥ. Παρέχεται μια ανάλυση των δράσεων, πρωτοβουλιών και των επιλογών σχεδιασμού της προσαρμογής στις επιπτώσεις της κλιματικής αλλαγής, μαζί με μια λεπτομερή ταξινόμηση των εργαλείων εκτίμησης του βαθμού προσαρμογής και σχεδιασμού αντιμετώπισης των περιβαλλοντικών κινδύνων.

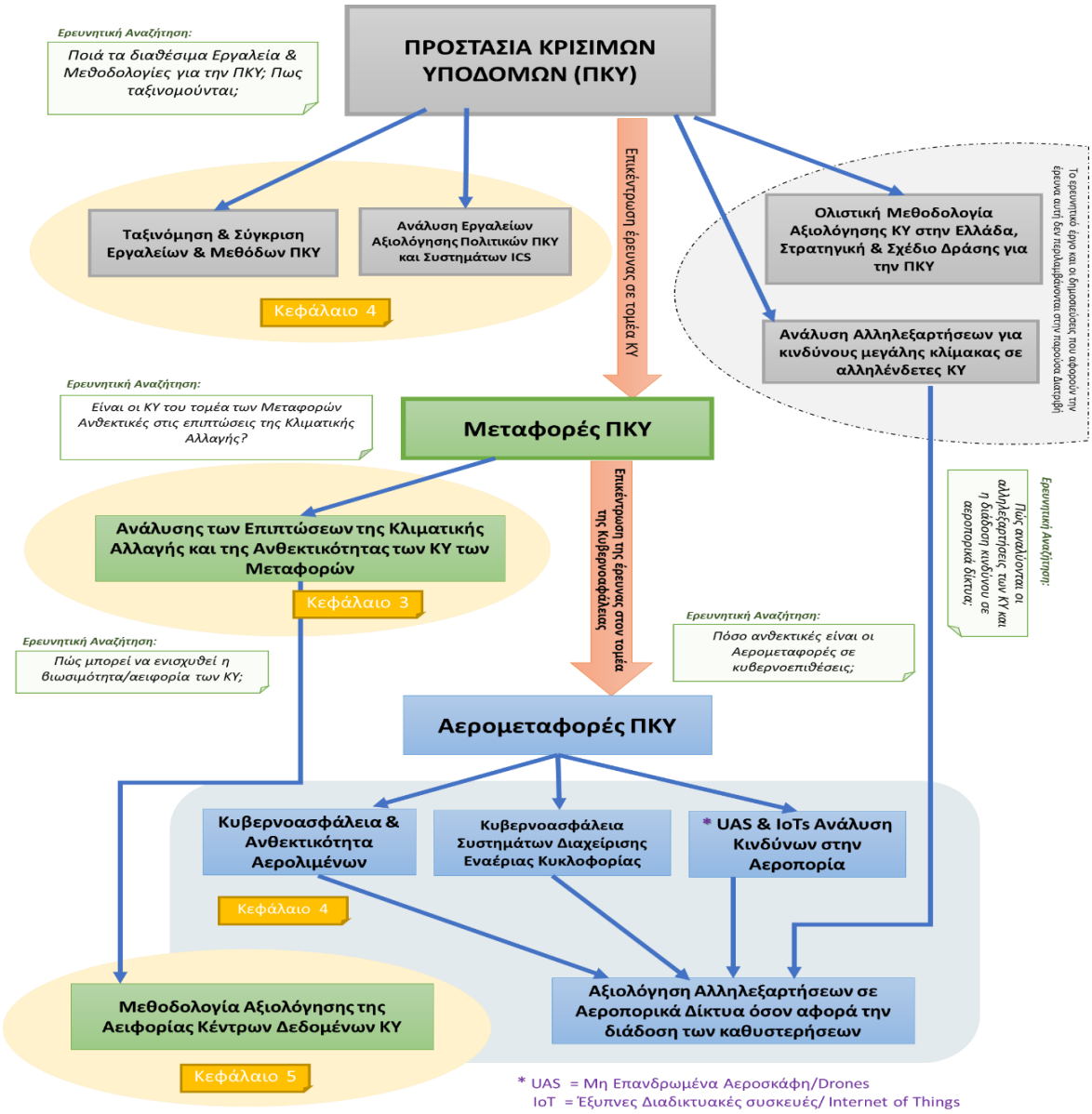
Το Κεφάλαιο 4 επικεντρώνεται στην ανάλυση των κινδύνων στις ΚΥ του αεροπορικού τομέα και πιο συγκεκριμένα η έρευνά μας επικεντρώνεται σε τέσσερις βασικούς τομείς της αεροπορίας, που είναι: i) Οι ΚΥ των αερολιμένων και οι προηγμένες πληροφοριακές υποδομές τους ii) Η διαχείριση και τα συστήματα ελέγχου της εναέριας κυκλοφορίας, καθώς και η διαλειτουργικότητα των συστημάτων αυτών, iii) Τα μη επανδρωμένα αεροσκάφη (UAS) και οι πιθανοί κίνδυνοι που εισάγουν στον τομέα της αεροπορίας, και

iv) Οι αλληλεξαρτήσεις του δικτύου αερομεταφορών, επικεντρώνοντας στις καθυστερήσεις που προκύπτουν από συμβάντα στην εναέρια κυκλοφορία.

Στο Κεφάλαιο 5, η παρούσα διατριβή διερευνά και αξιολογεί τη βιωσιμότητα των κέντρων δεδομένων, που αποτελούν τον πυρήνα υποστήριξης των τεχνολογικών εξελίξεων των τομέων πληροφορικής και επικοινωνιών στις σύγχρονες ΚΥ. Τα κέντρα δεδομένων υποστηρίζουν ευρέως τις αερομεταφορές, αλλά και συνολικά τον τομέα των μεταφορών, ενισχύοντας την διαλειτουργικότητα και την αποτελεσματική λειτουργία των ΚΥ. Μια νέα μεθοδολογία προτείνεται για την αξιολόγηση της αειφορίας με μια ολιστική προσέγγιση που αξιολογεί με σφαιρικό τρόπο τις περιβαλλοντικές επιπτώσεις και τη λειτουργική απόδοση των κέντρων δεδομένων και την ευρωστία των ΚΥ.

Το Κεφάλαιο 6 ολοκληρώνει τη διατριβή με μια περίληψη των συμπερασμάτων, ενώ παρουσιάζονται οι δημοσιεύσεις που έγιναν στα πλαίσια της πολυετούς έρευνας στον τομέα της Προστασίας των ΚΥ.

Η ροή της ερευνητικής αυτής πορείας συνοψίζεται στο παρακάτω διάγραμμα:



Πίνακας περιεχομένων

List of Figures

List of Tables

Chapter 2

Chapter 3

Chapter 4

Chapter 5

List of Acronyms

ADS–B	Automatic Dependent Surveillance –Broadcast
AIP	Aeronautical Information Packages
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATM	Air Traffic Management
BMS	Building Management Systems
BTS	US Bureau of Transportation Statistics
CC	Climate Change
CCTV	Close Circuit Television System
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CNS	Communication, Navigation & Surveillance Systems
C-UAS	Counter Unmanned Aircraft Systems
DC	Data Centers
DDoS	Distributed Denial of Service
DoS	Denial of Service
EC	European Community
EEA	European Environment Agency
ENISA	European Union Agency for Network and Information Security
EPCIP	European Program for Critical Infrastructure Protection
EU	European Union
GDPR	European General Data Protection Regulation
GIS	Geographic information systems
HVAC	Heating, Ventilation, Air Conditioning
ICAO	International Civil Aviation
ICS	Industrial Control Systems
ICT	Information & Communication Technology
IDS/IPS	Intrusion Detection & Protection Systems
IOT	Internet of Things
IPCC	United Nations Intergovernmental Panel on Climate Change
ISP	Internet Service Provider
IT	Information Technology
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
SCADA	Supervisory Control and Data Acquisition Systems
UAS	Unmanned Aircraft System
UAV	Unmanned Aviation Vehicle / Drone

Chapter 1: Introduction

This chapter provides background information, while it presents the main concepts for introducing this dissertation, along with research scope and motivational drivers, research statement and contributions. Furthermore, a synoptic diagram and the structure of this thesis are also presented.

Critical infrastructures (CIs) are the assets, systems, and networks, whether physical or virtual, so vital for our society that their incapacitation or destruction would have a debilitating effect on safety, security, national economy and public health or any combination thereof" (McLean et al., 2011a). Recent research has proven that CIs are highly interconnected nowadays, whether they manifest as processes, systems, facilities, assets, or services. The modeling and analysis of these interdependencies are relatively new research fields with increasing interest.

Critical Infrastructure Protection methodologies, models and simulations have been introduced in the past, which can facilitate the understanding of CI system's structure, CIs interdependencies, their vulnerabilities, and the impact of potential failures. The propagation rate of impacts across interdependent infrastructure systems, based upon risk assessment reports for all CIs have also been surveyed, aiming to build new concepts based on current scientific knowledge.

Transportation brings together resources of quite different nature and facilitates accessibility of services which are vital for business and for the society's quality of life. Disruptions to transportation systems can cause large economic or even human losses. For this reason, the transport sector is characterized as a CI (Transportation Research Board, 2009), since it is an important pillar of our economy and society. Physical and cyber-physical risks may threaten the smooth operations of transport sectors including aviation. Given the broad challenges of climate variations and the strong interconnectivity of transport sector's CIs, it is evident that environmental hazards along with cyber risks need to be confronted using a holistic approach, in order to mitigate inefficiencies in the transport sector, while enhance sector's sustainability and resilience to climate and cyber impacts.

1.1 Research motivation

1.1.1. Motivation for survey on CIP on ICS & IoTs used on CIs

The technological advance of CIs has introduced a plethora of automation solutions with the extensive use of supervisory control and data acquisition systems (SCADA). They are also called Industrial Control Systems (ICS) and when combined with the increased use of other interconnected smart devices, so called IoTs (Internet of

Things). These devices enhance CIs operational capabilities for advanced intelligence and systems interoperability. Adequate cyber-physical security for such systems is fundamental, due to their vital role in system's well-functioning, therefore ICS and ICT operation's team must be constantly aware of the status of information security controls, to make informed judgments and take appropriate measures to mitigate cyber-physical risks to an acceptable level. Cybersecurity risk-assessment tools support risk management procedures and provide mitigation and resilience solutions for CI operators and owners to determine the status of their information security programs and, where necessary, pinpoint specific targets for improvement.

The motivation of our survey was to capture the current knowledge and information in CIP sectors and compare existing Critical Infrastructure Protection Tools and Methodologies that can serve as a common baseline for CI risk analysis and assessment. Moreover, a review and analysis of available cybersecurity Self-Assessment tools was examined since such tools can also be supportive for ICS owners and CI operators. They enhance organizational risk management and enforce cybersecurity by identifying operating weaknesses, employee's security awareness and by evaluating implementation of effective control practices to protect cyber-physical systems against realistic threats and associated risks.

1.1.2. Motivation for focusing our research on Aviation & Transport Resilience

Research on CIP tools and methodologies has revealed that transport sector remains vulnerable and not adequately protected from physical and cyber-physical threats, so an in-depth analysis in transport sector resilience need to be further researched. While surveying the impact of physical risks, we discovered that despite the important role of transport in our society's welfare and the huge challenges posed by climate change, attention to transport adaptation and risk reduction was relatively low. Gradual climate change and the projected increase in frequency and intensity of extreme weather events will seriously challenge the transport sector. While mitigation efforts remain of great importance to reduce anthropogenic contribution to climate change, a simultaneous focus on CIs adaptation is essential (European Commission, 2011). Adaptation actions require climate vulnerability analysis and impact knowledge, so it is important that adaptation options are properly identified, evaluated, and monitored. The area of climate adaptation planning is still relatively new, so we explored the available processes and methodologies for assessing and reducing the vulnerability of transport sector to climate change.

Besides the climate change challenges in transport sector, cyber-physical risks in this area is an increasing research field. Although land and marine transportation are less vulnerable to cyber related threats due to their operational design and the nature of their infrastructures, in the aviation sector security and emerging cybersecurity threats

have become more sophisticated and challenging. Civil aviation community and aviation stakeholders rely heavily on computer-based, information and communication technology systems for their operations. This reliance is expected to grow as new and modern airports are developed, new air-traffic management systems are introduced and innovative technologies for aircraft systems have entered into service. Aviation stakeholders seek to meet the growing demand of IT-savvy passengers by using more smart applications, digital, and IT-based systems.

Aviation sector remains the safest transport mode in the world and probably also the most interconnected transport system in terms of information and communication technology. Cyber-threats are increasing in quantity and persistence, so the consequences of a successful malicious cyber-attack on civil aviation operations could be severe nowadays. New technologies introduced and the extension of connectivity in the aviation industry increase the cyber risks in the aviation sector & its critical assets, especially in the field of Air Traffic Management (ATM).

Airports enhance their infrastructure intelligence and evolve as smart facilities to support growth, by offering an enjoyable travel experience. New challenges are coming up, which aviation must deal with and adapt to, such as the integration of Industrial Control Systems (ICS) and IoT (Internet of Things) in airport facilities and the increased use of smart devices from travelers and employees. Cybersecurity is becoming a key enabler for safety, which is paramount in the aviation context.

Moreover, the applicability of unmanned aerial systems (UAS) continues to increase in number, technical complexity, and capabilities. However, drones pose significant challenges in terms of safety, security, and privacy within society. An increasing phenomenon, nowadays, is drone-related incidents near airport facilities, which are expected to proliferate in frequency, complexity, and severity, while drones become larger and more powerful. Aviation sector and its critical infrastructures need to be protected from such aerial attacks, through effective counteracting technologies, risk management and resilience plans.

Finally, while focusing our research in aviation sector and interdependencies, we have explored how a security incident is able to create disruptions or delays in the aviation network, while propagating this impact to other interconnected airports. Although network interdependencies have been investigated by academic community in the past, we discovered that concerning disruption incidents and air traffic delays, air transport networks appear to have variable performance and stochastic nature. An incident in one airport may affect the operational efficiency of others and generate various side effects to the whole aviation network. Flight delays are a widespread phenomenon nowadays, costing billions to the air transportation economy and degrading passenger's quality of service. Dependency graphs have been proposed in this research to understand the delay propagation and analyze such cascading events. A risk-based method to analyze interdependencies and congestions in the aviation network has been proposed by our research team.

1.1.3. Motivation for introducing a methodology for assessing CIs Sustainability and Resilience

Finally, while examining operational efficiency and capacity of CIs, we realised that the increased intelligence and interconnection of CIs needs especially designed Data Centers (DCs) to support efficient operations. These DCs serve as the heart of ICT technology, supporting augmented intelligence, interoperability, and innovation in CIs including transport sector. There is an increasing demand for data processing and storage, supported by the continued growth of internet services worldwide. This has led to significant energy consumption, serious environmental impacts, greenhouse gas emissions, electronic equipment waste, and severe environmental pollution. Various metrics have been proposed to evaluate operational efficiency in data centers, aiming to develop energy conscious behavior and resources savings, however they are falling short, when assessing sustainability of a data center in a holistic view. Sustainability aims at preserving the environment, along with economic, operational, and social longevity. Therefore, a new methodology has been proposed, for assessing sustainability composed by different influencing factors, with the aim to obtain a holistic approach. We introduced a new sustainability scoring model, to evaluate in a spherical way the environmental impact and operational efficiency of data centers, supporting ICT services in CIs.

1.2 Research statement and approach

Throughout this research journey our focus was to investigate Critical Infrastructure Protection (CIP) field in the appropriate depth analysis and produce knowledge for the academic community. In figure 1.1, we demonstrate in a graphical layout our research approach and methodology used, the fruits that our research has derived, and how this work has increased our contribution to the Scientific Body of Knowledge.

First, we have investigated the CIP research field, with the aim to answer the question: '***What are the available Tools and Methodologies already developed for CIP*?**' This has led to an extensive survey work and a multifaceted classification of CIP tools. Our work was presented in two international conferences with related publications in peer-reviewed conference proceedings, as presented in Chapter 2.

After introducing an in-depth analysis and classification of CIP tools and methodologies, we have focused our research on Transportation Sector. Our goal was to survey the environmental threats and Climate Change (CC) impacts in this critical and so exposed to environmental risks sector. The question posed was the following: '***Is Transport Sector Resilient to Climate Change Impacts*?**' The answer was given with scientific research, which was published in two peer-reviewed conference papers for CC Adaptation, as presented in Chapter 3.

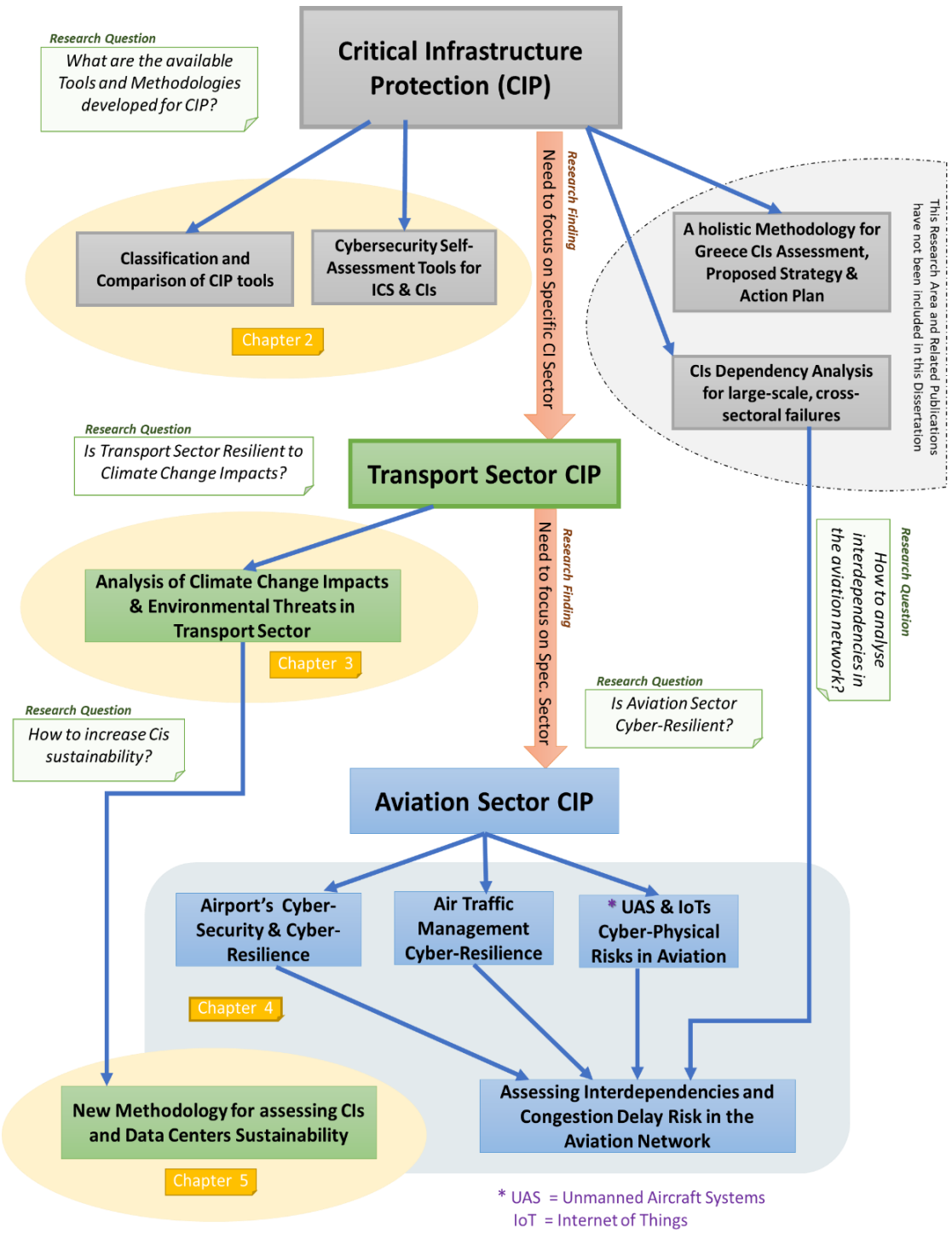


Figure 1.1: Research Methodology and Approach

With the aim to investigate the cyber resilience of transport sector, we realized that the most interconnected and ICT related sector is the Aviation sector, so we focused our research in this specific area and posed the question: '***Is Aviation Sector Cyber-Resilient?'*** To answer this question, we divided our work in three distinct scientific fields within aviation sector: a) Airports; b) Air Traffic Management; and c) Air navigation systems, where we examined cyber-physical risks, developed realistic threat scenarios, and proposed mitigation actions and resilience plans for each one. In addition, we analyzed aviation network interdependencies and proposed a new methodology combined with a new software tool to assess congestion delay risks in the entire aviation network.

The research work on aviation sector has led to the publication of one conference paper, one chapter in a book publication, along with three publications in scientific Journals for Aviation sector resilience, as presented in Chapter 4.

The last part of our research aimed to synthesize knowledge from previous research areas and contribute towards an efficient, resilient, and sustainable design of CIs and ICT Data Centers (DCs) by answering the question: '***How we can increase CIs and supporting DCs sustainability?'*** This has led to the proposal of a new methodology for assessing sustainability and the publication of a related article in peer reviewed scientific journal, as presented in Chapter 5.

To resume this research trajectory, this thesis has taken steps to improve resilience in CIP research area, focusing on transport sector and especially in the Aviation field, where interoperability and interdependencies are supported by emerging technologies and ICT innovations. In this context, this dissertation makes the following research statement:

> *The current state of aviation sector needs to increase the resilience of its critical infrastructures and promote sustainable and cyber resilient solutions to progress, innovate, and provide safe and secure services to our society.*

This thesis contains evidence that supports this statement. Our findings suggest that it is indeed possible to mitigate risk from cyber-physical threats in CIs, efficiently protect transport sector and aviation CIs, increase their resilience, while enhancing the sustainability design of CIs.

1.3 Contribution to Knowledge

This dissertation makes the following contributions to the scientific community:

- ***A classification of CIP protection tools, frameworks and methodologies*** that support threat identification, risk assessment and risk management for Critical Infrastructures. A conceptual and qualitative study about infrastructure interdependencies as well as their modeling and simulation approaches are also presented.
- ***A review and technical analysis of available cybersecurity Self-Assessment tools*** used for tailored risk assessment by ICS owners and CI operators. In addition, content analysis was performed for questionnaires, being used in these self-assessment tools, and classified according to core functions of NIST Cybersecurity Framework.

- ***An in-depth technical analysis of global adaptation initiatives for CIP and classification of adaptation options***. Our survey has focused on emerging adaptation challenges and opportunities in the transport sector.

- ***A multi-faceted taxonomy and analysis of available Climate Change Adaptation tools,*** which support transport sector for risk management policies. A detailed classification of adaptation tools that facilitate adaptation assessment and risk planning is also presented.

- ***An online survey and research analysis of measures and best practices implemented in commercial airports*** based on an online performed survey. This research has identified malicious threats for ICS and IoT applications in smart airports, and as a result a ***detailed scenario analysis of malicious attacks*** *in smart airports* assets has been developed, including cascading effects, mitigation actions and cyber-resilience measures.

- ***Analysis of cyber security challenges in civil aviation and Air Traffic Management systems***, complied with an ***extended threat model for analyzing possible targets and risks*** in the aviation sector. Cyber resilience aspects in the aviation context and the need for holistic strategy of defense, prevention, and response have also been introduced and analyzed.

- ***A survey on drone incidents near airports and a literature review on counter sensor technologies***, able to prevent, detect, identify, and mitigate rogue drones. Benefits and limitations of available counter-drone technologies (C-UAS) for defending airports against misused drone activity are also examined.

- ***Realistic attack scenarios using malicious drones complimented with an effective C-UAS protection plan*** aiming to: i) alert airport community and aviation researchers about safety and security risks revealed from nefarious drones, ii) analyze benefits and limitations of available C-UAS technologies and iii) propose a resilience action plan that supports airport operators and aviation stakeholders to increase robustness of critical assets and infrastructures against airborne malicious threats.

- ***A methodology able to analyze congestion risk interdependencies in aviation networks***, as following: i) models aviation networks as dependency graphs; ii) assesses the dependency risk of delay incidents between interconnected airports; iii) produces weighted risk dependency chains, to present how a delay occurred in one airport may affect other inter-connected airports; and iv) calculates impact and likelihood of delays in congested airports using various methods such as min-max algorithm, standard deviation timeframes, and statistical dynamic averages.

- ***A comparison analysis of airplane on-time arrival performance data of US domestic flights*** as provided by BTS (US Bureau of Transportation Statistics) for summer high season period of two consecutive years. Moreover, we detected the most congested paths, schedules, and airports to be evaded by flight planners, airline marketing managers, and other air transportation stakeholders.

- ***A software implementation of the proposed risk based methodology on interdependencies***, which can: a) indicate the flight connections with the highest delay risk for the period defined; b) identify the worst n-order airport dependencies by calculating the overall risk of cascading congestions; c) indicate airports that are frequently part of the worst n-order airport dependencies and introduce delays to the downstream flights; d) analyze what-if scenarios for the congested airport's connections; e) propose the n-order dependency chains, which should be avoided by flight planners, to reduce delay impacts in the aviation network.

- ***A holistic sustainability evaluation model is introduced that can be implemented to CIs data centers***, using a scoring system, and considering all necessary components to assess how green, how efficient, and how resilient is the examined data center. This model supports DCs owners and operators to evaluate the sustainability of their facilities and make prompt decisions on their management choices, increasing their operating efficiency and resilience, while reducing their environmental footprint.

1.4 Dissertation Structure

The rest of this dissertation is organized as follows:

Chapter 2 presents our survey work in Critical Infrastructure Protection Area, where we provide a classification and comparison of critical infrastructure protection tools, along with a review and analysis of available cybersecurity Self-Assessment tools.

In ***Chapter 3***, environmental and climate change impacts in transportation sector are discussed, introducing the need of climate change adaptation for resilient and sustainable CIs. An analysis of global adaptation initiatives and adaptation options are provided, along with a detailed classification of adaptation assessment and risk planning tools. This provides a multi-faceted taxonomy and analysis of available Climate Change Adaptation tools for risk management policies in the transport sector.

Chapter 4 focuses on Aviation Sector CIs Cyber-Resilience and more specifically our research integrates four main sections of Aviation, which are: i) Smart Airports and their advanced intelligence infrastructures; ii) Air traffic management interoperability and Air Traffic Control systems; iii) Unmanned Aircraft Systems (UAS) and their potential threats to aviation sector; and iv) Aviation network interdependencies concerning traffic delays.

The implementation rate of cybersecurity measures in aviation sector is researched through an online survey and risk scenarios are developed for cyber-physical malicious attacks, along with effective counter measures and mitigation options. Moreover, we propose a resilience action plan for aviation and airports stakeholders for defending CIs from airborne threats and misused IoTs.

Finally, after assessing aviation network interdependencies, we propose a method able to detect the most critical airports and congested connections, based on their delay contribution in dependency chains. The proposed software tool can predict the n-order dependency chains, which should be avoided by airline flight planners, aiming to reduce delay impacts in the aviation network.

In ***Chapter 5***, this thesis explores the sustainability of data centers which is the heart of IT technology and intelligent operations of CIs. Data centers support transportation and its critical infrastructures, including aviation management systems. Supporting sustainable design of DCs, a new methodology is proposed for assessing sustainability using a holistic approach and evaluating in a spherical way the environmental impact and operational efficiency of data centers.

Chapter 6 concludes the dissertation with a summary and presents peer-reviewed publications of our research.

Chapter 2: Critical Infrastructure Protection: Tools & Interdependency Analysis of cross-sectoral Risks

2.1. Classification and comparison of critical infrastructure protection tools

2.1.1 Introduction [1]

Recent research has proven that Critical Infrastructures are highly interconnected, whether they manifest as processes, systems, facilities, assets, or services. The modeling and analysis of these interdependencies are relatively new research fields with increasing interest. Dependency and risk analysis of these interconnections can be a computationally intensive problem, but also can yield useful results that aid Risk Assessments and offer Risk mitigation alternatives. This survey tries to detect and classify most existing tools, frameworks and methodologies that can serve as a common baseline for threat identification and risk assessment and, afterwards, compare their attributes and technologies. Conceptual and qualitative studies about infrastructure interdependencies as well as their modeling and simulation approaches are examined. The comparison of the tools is mainly based on two different aspects; the purpose that each tool serves and its technical modeling approach. For tools that are not publicly available, the classification used information from international bibliography, published articles and reports.

Critical infrastructures (CIs), as referred from the department of homeland security, are "the assets, systems, and networks, whether physical or virtual, so vital that their incapacitation or destruction would have a debilitating effect on security, national economy security, national public health or safety, or any combination thereof" (McLean et al., 2011a). Critical Infrastructure Protection methodologies, models and simulations may be used to understand infrastructure systems, their interdependencies, their vulnerabilities, and the impact of potential failures and their propagation across interdependent infrastructure systems, based upon risk assessment reports for all CIs involved. These methodologies may also be used to support training exercises, performance measurement, conceptual design, impact evaluation, response planning, vulnerability analysis and economic impact.

[1] *Related Publication:* Stergiopoulos G., Vasilellis E., Lykou G., Kotzanikolaou P., Gritzalis D., "*Critical Infrastructure Protection tools: Classification and comparison*", in Proc. of the 10th International Conference on Critical Infrastructure Protection (CIP-2016), USA, March 2016

The goal of this survey is to capture the current knowledge and information and try to compare existing Critical Infrastructure Protection (CIP) tools and methodologies that can serve as a common baseline for CI risk analysis and assessment. We have based the comparison of CIP related tools on two different aspects: (i) the *Purpose* (i.e. Functionality) that they serve by each tool and (ii) the Modeling Approach and technical development. In this work, we detected and examined sixty-eight (68) CIP tools and methodologies, a great number of which were developed in the U.S. (see Appendix A for a full description of the examined tools presented in this work).

2.1.2 Classification of CIP Tools Based on their Purpose

According to the National Infrastructure Protection Plan (NIPP, 2013), tools, frameworks and methodologies are classified according to the Purpose that they serve, i.e. the stage of the risk management framework that they aid with their output. These stages are: (i) *risk identification*, (ii) *risk assessment*, (iii) *risk prioritization*, (iv) *risk mitigation planning* and (v) *effectiveness evaluation*. Using systems engineering as an example, a model of the serial process is shown in Figure 2.1, as modeled by the NIPP Risk Management Framework.

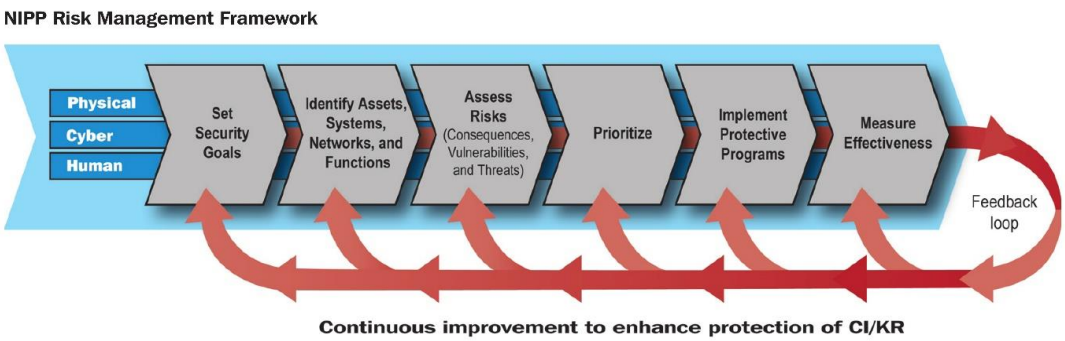


Figure 2.1. NIPP framework for Protection and Risk Management of CIs

After setting the security goals, the following goals must be achieved in serial order:

1. *Risk Identification* (RI): Identification of assets, potential vulnerabilities, and events along with relationships.
2. *Risk Assessment* (RIA): Assessment of probabilities and consequences of risk events. May include cost, schedule, performance impacts and functionality impacts.
3. *Risk Prioritization Analysis (RP)*: Aggregate and analyze risk assessment results, establish priorities that provide the greatest mitigation of risk. Criticality of risk

is assessed with the use of decision-analytic rules, applied to rank risk events from most critical to the least.

4. *Risk Mitigation Planning and Implementation (RMP)*: Selection of sector-appropriate protective actions or programs to reduce or manage the risk identified.
5. *Effectiveness Evaluation (EE):* The effectiveness of selected measures and strategies is evaluated. Existing and newly identified risk events are reassessed.

Figure 2.2 provides a visual depiction of the classification of the sixty-eight (68) tools gathered in this survey, according to the risk management purpose that they serve. Tools that are deeper than others in the same branch, provide additional risk analysis purposes, *i.e.* they support additional stages of the risk management framework.

As shown in the classification tree, the majority of the tools start with the risk identification stage and then proceed to further analysis steps. Very few tools skip the first two stages, while even fewer tools (only 3) support all the stages of the Risk Management Framework.

2.1.3 Classification of CIP Tools based on Modelling Approach

CI modeling approaches refer to the techniques used during the development of CIP tools. They are often chosen based on the intended purpose of every tool. All approaches serve risk assessment purposes but there are some unique characteristics to every approach. Ouyang (2014) first categorized CIP tools and methodologies using five main types of modeling and simulation approaches:

- *Empirical approaches***:** The empirical approaches analyze CIs interdependencies according to historical events, disaster data and expert knowledge. They can identify failure patterns, quantify interdependency strength metrics to aid decision making, perform empirically based risk analysis and provide alternatives to minimize risk in interdependent infrastructures.
- *System dynamics-based approaches:* System dynamics-based approaches utilize a top-down method to manage and analyze complex adaptive systems involving interdependencies. Feedback, stock, and flow are the basic concepts in this type of approaches. Feedback loops indicate connection and direction of effects between CI components.
- *Agent based approaches:* Agent based approaches are the most common tool-building techniques. Due to the inherent complexity of CIs and the related decision-making processes, CIs are usually regarded as *Complex Adaptive Systems* (CASs). To analyze CASs, agent-based approaches adopt a bottom-up method and assume that complex behavior or phenomena emerge from many

individual and relatively simple interactions of autonomous agents. Most CI components can be viewed as agents. A model's agent interacts with others and its environment, based on a set of rules, which mimic the way a real counterpart would react. Hence, agent-based approaches are widely used to model the CI interdependencies and they are mainly used by several national laboratories.

- *Network based approaches:* In network-based approaches CIs are described as networks where nodes represent different CIs components and links mimic the physical and relational connections among them. Thus, they can provide an intuitive CI representation along with descriptions of topologies and flow patterns. Performance response of CIs to hazards can also be analyzed by modeling the component failures from hazards at component level and then simulating cascading failures within and across CIs at system level.

- *Other approaches:* Other approaches exist that can model and analyze interdependent CIs, such as models of economic interdependencies, cellular automata, mathematical equation and others. Namely, we identified four major miscellaneous approaches: (i) Economic Theory-based, (ii) Cellular Automata-based, (iii) Mathematical Equation-based and (iv) Real-Time Simulation-based.

CI modeling seems to be associated with simulation techniques and mathematical models that are combined with the aforementioned computational techniques like continuous time-step simulation, discrete time-step simulation, Monte Carlo simulation, decision trees, geographic information techniques (GIS), risk management techniques as well as event or real time record.

In the following classification tree, the Ouyang's approach classification model (2014b) is used in order to categorize the examined CIP software tools. Each tool has been assigned to one category, in an effort to map all detected CI analysis software. Many CIP methodologies are hybrid (i.e. belong to more than one approach). The same is true for some tools – they may belong to more than one category. Hybrid methodologies/tools have been categorized based on their dominating (i.e. most appropriate) category and afterwards further classified based on additional approaches used; the deeper a methodology/tool is positioned in the approach classification tree in Figure 2.3, the more complicated simulation technique is used. The majority of tools are using Agent based or Network based approaches to perform the modeling and risk analysis report. Then, they are further categorized according to supplementary modeling techniques (Continuous/Discrete time-step simulation, Monte Carlo, Decision trees, GIS etc.).

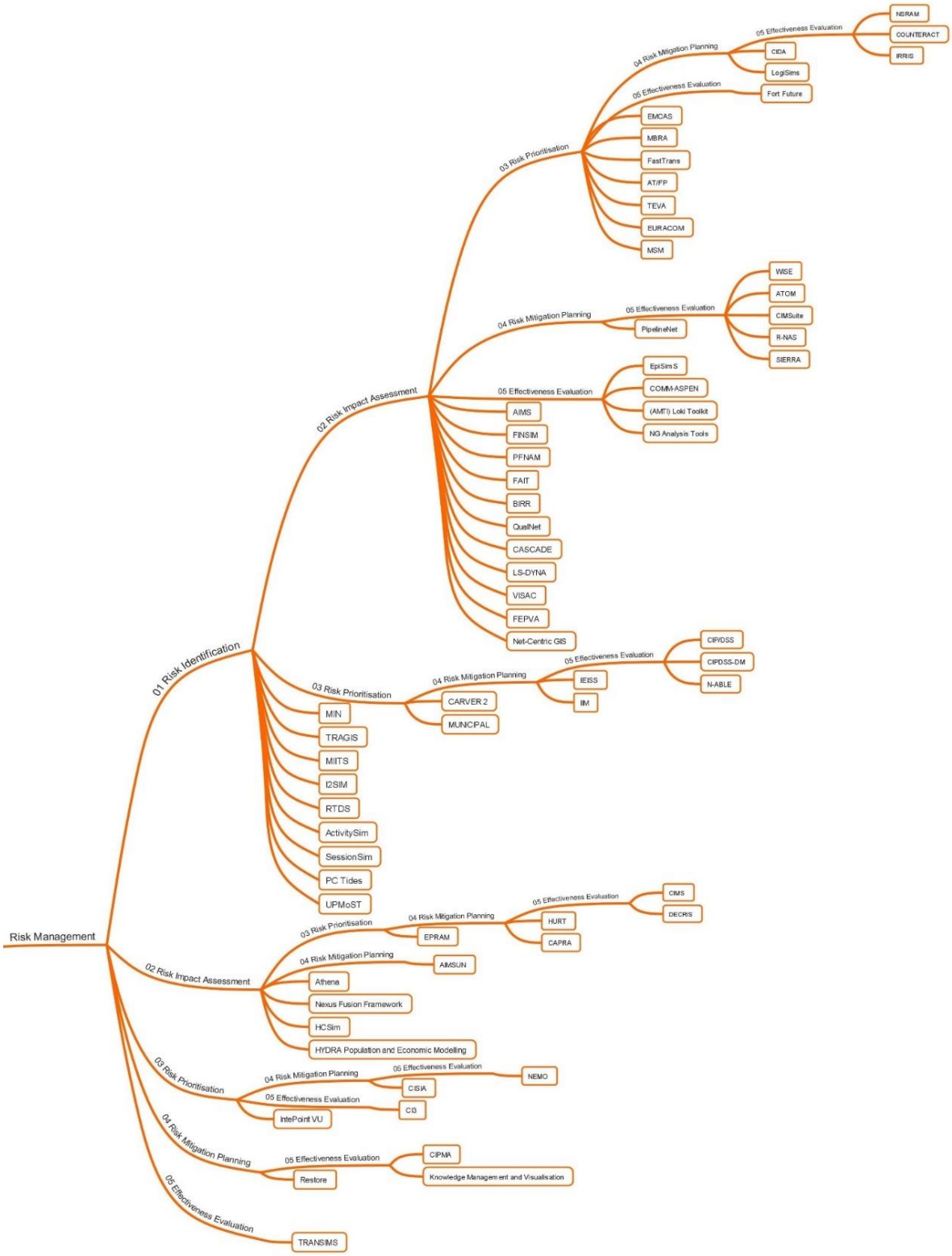


Figure 2.2. CIP tools Classification according to Risk Management Purpose

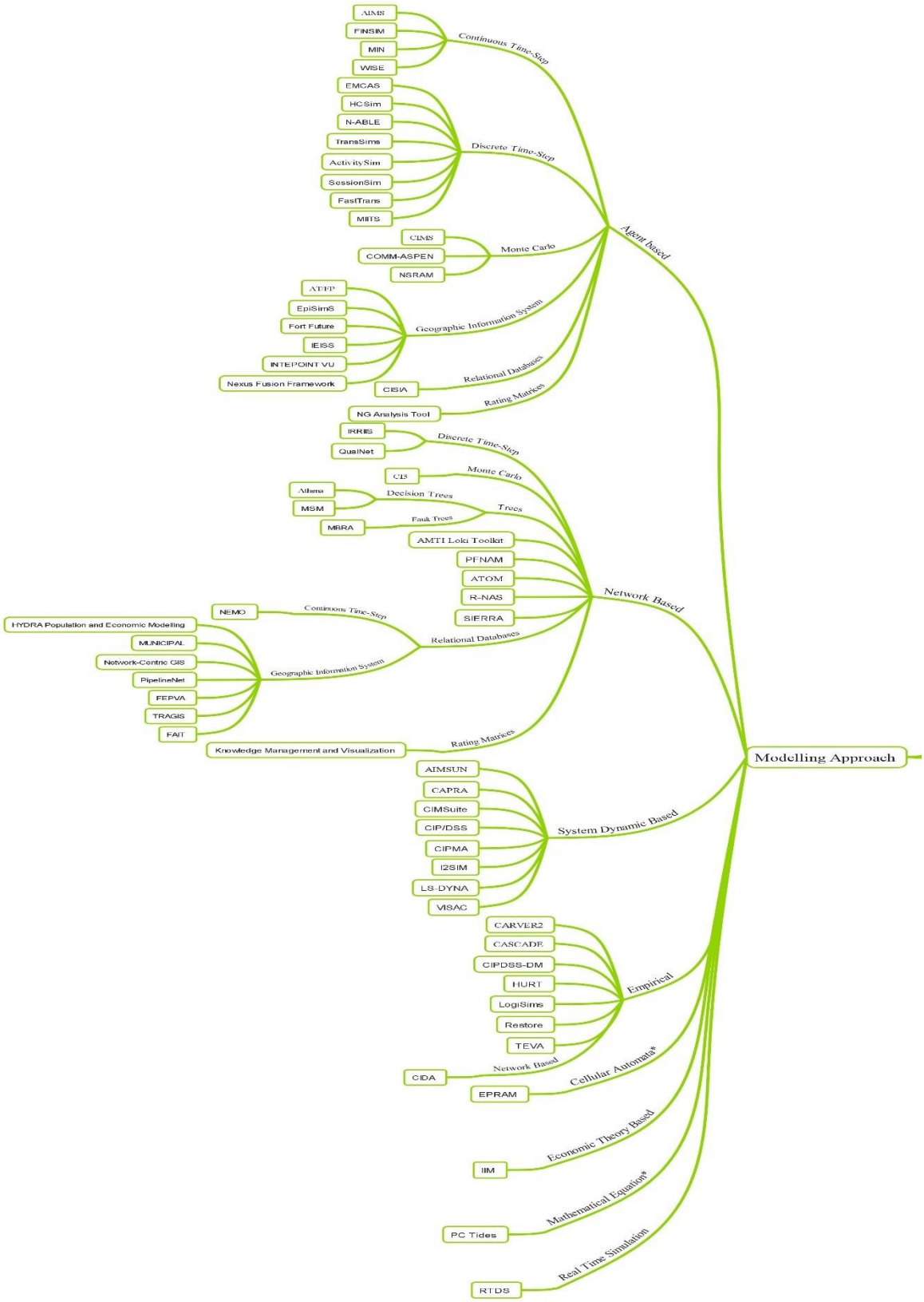


Figure 2.3. CIP tools Classification according to Modeling Approach

2.1.4 Classification Summary

The department of Homeland Security (*Critical Infrastructure Sectors | CISA*, 2013) identifies sixteen CI sectors as shown in Table 2.1.

Table 2.1. Sector Prefixes

Critical Infrastructure Sectors	***Prefixes***	***Critical Infrastructure Sectors***	***Prefixes***
Chemical	CH	Financial Services	FS
Commercial Facilities	CF	Food and Agriculture	FA
Critical Manufacturing	CM	Government Facilities	GF
Dams	D	Healthcare and Public Health	HPH
Defense Industrial Base	DIB	Information Technology	IT
Emergency Services	ES	Nuclear Reactors, Materials, and Waste	NRMW
Energy	E	Transportation Systems	TS

We use these CI sectors and reported prefixes in the following Table 2.2 to depict which sectors are covered by each tool. For the same use, abbreviation prefixes for Risk Purpose and Modeling Techniques are presented in figure 2.5, while figure 2.4 presents the comparison aspects used for the classification of CIP tools

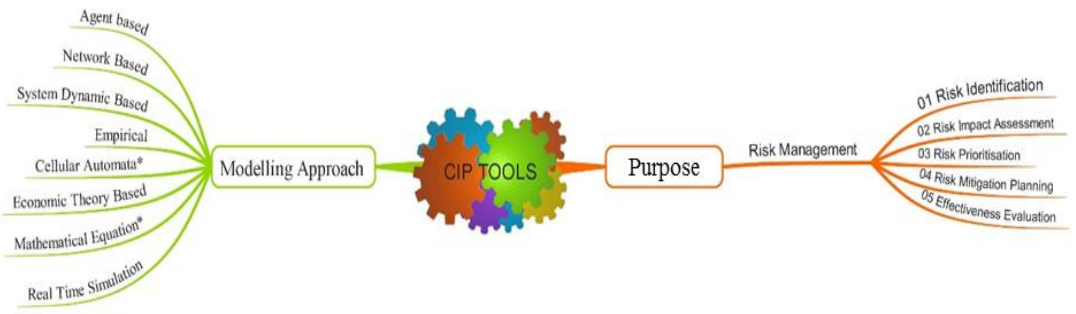


Figure 2.4. Comparison aspects for Classification of CIP tools

Purpose Functionality	Prefix
Risk Identification	RI
Risk Impact Assessment	RIA
Risk Prioritization	RP
Risk Mitigation Planning	RMP
Effectiveness Evaluation	EE

Modelling Technique	Prefix
Continuous Time-Step	CS
Decision Trees	DT
Discrete Time-Step	DS
Geographic Information System	GIS
Monte Carlo	MC

Figure 2.5. Classification abbreviation prefixes

In Table 2.2 we have summarized all the examined CIP tools and methodologies, based on their modeling approaches, risk purpose functionalities and the CI sectors that each tool can support.

Table 2.2. CIP Tools Classification

TOOL / METHODOLOGY	MODELLING APPROACH	PURPOSE FUNCTIONALITY	CI SECTOR
ActivitySim	Agent Based, DS	RI	CF
AIMS	Agent Based, CS	RI, RIA	CF, C, E, IT, WWS
AIMSUN	System Dynamic Based	RIA, RMP	TS
AMTI Loki Toolkit	Network Based	RIA, EE	E, FS, TS
AT/FP	Agent Based, GIS	RI, RIA, RP	DIB, ES, HPH, TS
Athena	Network based, DT	RIA	CF, C, CM, DIB, E, FS, IT, NRMW, TS, WWS
ATOM	Network based	RI, RIA, RMP, EE	TS
BIRR	Methodology (No modeling)	RI, RIA	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CAPRA	System Dynamic Based	RIA, RP, RMP	FS, HPH, TS, WWS
CARVER2	Empirical	RI, RP	HPH
CASCADE	Empirical	RI, RIA	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CI3	Network Based, MC	RP, EE	C, CM, E, NRMW, WWS
CIMS	Agent Based, MC	RIA, RP, RMP,EE	CF, C, E, HPH, TS
CIDA	Empirical Based, Network Based	RP, RMP, EE	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CIMSuite	System Dynamic Based	RI, RIA, RMP, EE	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CIP/DSS	System Dynamic Based	RI, RP, RMP, EE	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CIPDSS-DM	Empirical	RI, RP, RMP, EE	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
CIPMA	System Dynamic Based	RMP, EE	C, E, FS, IT, TS

CISIA	Agent Based, Relational Databases	RP, RMP	C, CM, E, NRMW, WWS
COMM-ASPEN	Agent Based, MC	RI, RIA, EE	C, E, FS
COUNTERACT	Methodology (No modeling)	RI, RIA, RP, RMP, EE	E, HPH, TS
DECRIS	Methodology	RIA, RP, RMP,EE	C, E, IT, TS, WWS
EMCAS	Agent Based, DS	RI, RIA, RP	C, E, FS, WWS
EpiSimS	Agent Based, GIS	RI, RIA, EE	HPH
EPRAM	Cellular Automata	RIA, RP	E
EURACOM	Methodology (No modeling)	RI, RIA, RP	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
FAIT	Network Based, Relational Databases, GIS	RI, RIA	ES, E, FS, NRMW, TS
FastTrans	Agent Based, DS	RI, RIA, RP	TS
FEPVA	Network Based, Relational Databases, GIS	RI, RIA	E
FINSIM	Agent Based, CS	RI, RIA	C, E, FS
Fort Future	Agent Based, GIS	RI, RIA, RP, EE	CF, C, CM, DIB, E, FS, HPH, IT, NRMW, TS, WWS
HCSim	Agent Based, DS	RIA	D, HPH, NRMW
HURT	Empirical	RIA, RP, RMP	HPH
HYDRA Population and Economic Modeling	Network Based, Relational Databases, GIS	RIA	FS, HPH
I2SIM	System Dynamic Based	RI	CF, CM, HPH, T
IEISS	Agent Based, GIS	RI, RP, RMP	E, NRMW, WWS
IIM	Economic Theory Based	RI, RP, RMP	C, E, FS, IT, TS, WWS
INTEPOINT VU	Agent Based, GIS	RP	CF, C, E, TS
IRRIIS	Network Based, DS	RI, RIA, RP, RMP, EE	C, CF, CM, D, DIB, ES, E, FS, FA, GF, HPH, IT, NRMW, TS, WWS
Knowledge Management and Visualization	Network Based, Rating Matrices	RMP, EE	E, TS, WWS
LogiSims	Empirical	RI, RIA, RP, RMP	E, HPH
LS-DYNA	System Dynamic Based	RI, RIA	CM, D, TS
MBRA	Network based, FT	RI, RIA, RP	E, FS, TS
MIITS	Agent Based, DS	RI	C, IT
MIN	Agent Based, CS	RI	CF, TS
MSM	Network based, DT	RI, RIA, RP	E, HPH, WWS

MUNICIPAL	Network Based, Relational Databases, GIS	RI, RP	C, E, IT, TS
N-ABLE	Agent Based, DS	RI, RP, RMP, EE	E, FS, TS
NEMO	Network Based, Relational Databases, CS	RP, RMP, EE	C, DIB, E, TS, WWS
Net-Centric GIS	Network Based, Relational Databases, GIS	RI, RIA	TS, WWS
NEXUS Fusion Framework	Agent Based, GIS	RIA	CF, C, DIB, E, TS
NG Analysis Tools	Agent Based, Relational Databases	RI, RIA, EE	E
NSRAM	Agent Based, MC	RI, RIA, RP, RMP, EE	C, E, IT
PC Tides	Mathematical Equation	RI	D, ES, HPH, WWS
PFNAM	Network Based	RI, RIA	E
PipelineNet	Network Based, Relational Databases, GIS	RI, RIA, RMP	HPH, WWS
QualNet	Network Based, DS	RI, RIA	C
Restore	Empirical	RMP	CM ,E
R-NAS	Network Based	RI, RIA, RMP, EE	FA, TS
RTDS	Real Time Simulation	RI	E
SessionSim	Agent Based, DS	RI	C
SIERRA	Network Based	RI, RIA, RMP, EE	TS
TEVA	Empirical	RI, RIA, RP	HPH, WWS
TRAGIS	Network Based, Relational Databases, GIS	RI	TS, WWS
TranSims	Agent Based, DS	EE	CF, TS
UPMoST	Methodology (No modeling)	RI	CF
VISAC	System Dynamic Based	RI, RIA	CH, NRM
WISE	Agent Based, CS	RI, RIA, RMP, EE	CF, HPH, NRMW, WWS

Available links for most tools, gathered at the time of publication of this survey, can be found at the Appendix A section at the end of this thesis.

2.1.5 CI Modelling Tool Comparison

Critical Infrastructure Protection plans are mainly based on risk management frameworks, with NIPP being the most advanced program, not only in objectives, but also in strategies and references to other plans worldwide. Various countries adopt similar CIP plans for the prevention and protection of Critical Infrastructures.

All tools are used by either internal or external analysts. An *external analyst* makes use of the analytical tools outside the developing organization, whereas an *internal*

analyst uses them only internally. The classification criteria are related to the amount of expertise required in order to use the product, as well as the application requirements and the analytical output of each product. As far as requirements are concerned, criteria are driven by complexity, size and/or the nature of the underlying data used by each tool.

2.1.5.1 Comparison Based on PURPOSE

By comparing the CIP tools based on which risk management stages are covering, useful insight can be provided: 76% of the tools are dealing with Risk Identification (RI) and 67% are covering Risk Impact Assessment (RIA). 42% provide some sort of Risk Prioritization (RP) and 41% of them provide Risk Mitigation Planning (RMP), while only 35% evaluates the Effectiveness (EE). Results showed that covering all risk management stages is quite hard to achieve with a single tool, since it requires complicated data analysis. Only 4% (3 tools) cover all five risk purpose stages, while 17% (11 tools) cover four risk purpose stages. The other 80% of tools cover one, two or three stages as depicted in Figure 2.6:

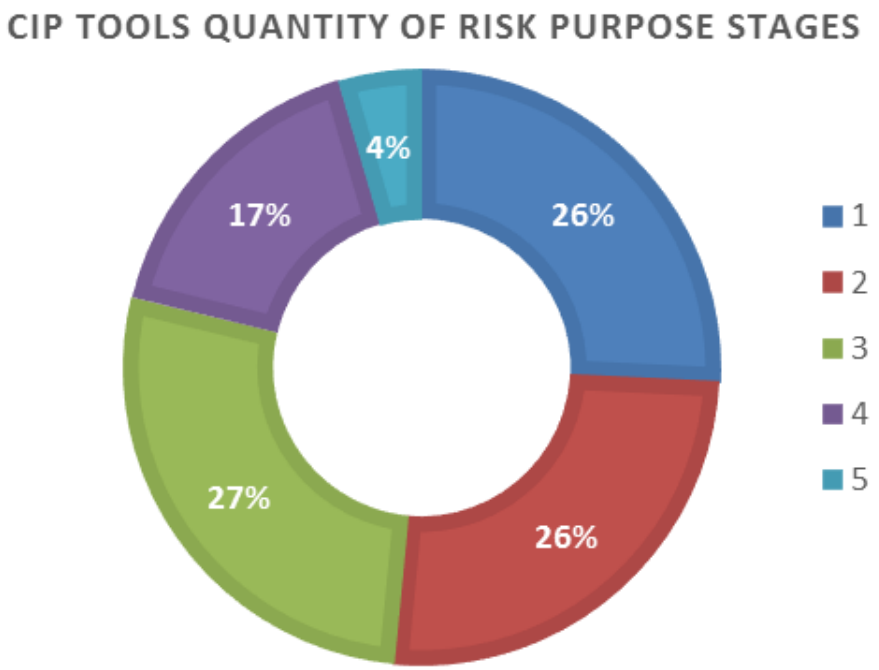


Figure 2.6. CIP Tool: No of Risk Stages Classification

Tools that cover all five stages of risk purpose are less than 5%, Most of them are either broad methodologies (like COUNTERACT, IRRIIS, EURACOM, BIRR) or

very sophisticated tools like NSRAM. NSRAM tool is a complex network system simulation modeling tool, but is covering only three sectors (E, IT, C).

Tools that can cover more than four risk purpose stages and more than 10 different sectors are very limited (5%). Again, most of them are either broad methodologies as mentioned before or advanced tools developed in the US (like CIMSuite, CIP/DSS, CIPDSS-DM, Fort Future), These tools will be discussed in more detail in the rest of this section.

CIP/DSS is a tool worth mentioning. It is a complete risk assessment methodology that can be applied to all sectors. It is developed by the National Infrastructure Protection Plan (NIPP). It is mostly used by military and government segments as a probabilistic optimization integrated system model that uses system dynamics as a modeling technique with continuous time-step simulation. Similar to CIP/DSS, the CIPDSS-DM tool has the same abilities, but it is designed to facilitate analysts and policy makers in the evaluation and selection of the optimal risk mitigation strategies. All things considered, CIP/DSS combined with CIPDSS-DM is a powerful and robust critical infrastructure protection tool because it can be applied to all sectors as they are derived from NIPP. Moreover, the ability of CIPDSS-DM to facilitate in the selection of the most effective mitigation strategy is very helpful not only in terms of restricting the impact of potential incidents, but also economic losses. Finally, its modelling (system dynamic based) seems more attractive for interdependency analysis, predicting responses and policy implementations.

Fort Future was developed by the US. Army Corps of Engineers. It is an agent-based tool that runs multiple dynamic simulations to evaluate a set of alternative scenarios. It supports geographic information systems. It is unavailable for civilian applications and is only being used for military purposes.

CIMSuite is a powerful software which enables users to run different scenarios. It can depict cascading effects on all sectors. It can also depict infrastructure relationships. It is a system-dynamic tool implementing a variety of algorithmic probabilistic simulations and incorporating the human response element into its physical infrastructure model. CIMSuite covers four (RI, RIA, RMP, EE) risk purpose stages and it is commercially available by the Idaho National Laboratories.

Athena is another interesting tool. Even though it only supports the Risk Impact Assessment stage, still it supports a number of different sectors and it can also be used for studying the interdependencies between different CIs along with their potential cascading effects. We have distinguished it because it is the only tool that can create ontological models with certain abstraction characteristics. One of Athena's shortcomings is its need for extensive data concerning the network of CIs and their

corresponding interdependencies. Athena is currently restricted and only provided to government and military users.

Concerning the stages of Risk identification (RI) and Risk Prioritization (RP), Still, two tools stand out due to their interesting output, CARVER 2 which stands for Criticality Accessibility Recoverability Vulnerability Espyability Redundancy, and MUNICIPAL which stands for Multi-Network Interdependent Critical Infrastructure Program for Analysis of Lifelines. Both seem able to analyze multiple sectors of a critical infrastructure in order to identify the most critical components as well as prioritize them according to severity; i.e. impact if a failure occurs in them. The approach, however, that each one of them uses is slightly different. CARVER2 uses rating matrices which is the basis for the generation of hazard maps, whereas MUNICIPAL uses relation databases on asset inventories for networks in order to deal with as much information as possible for each asset that constitutes the critical infrastructure. MUNICIPAL seems slightly better because it uses risk management techniques in order to identify risks, as well as because its output is based on GIS, which is very useful to determine the area of impact.

Other tools can also provide Risk Mitigation planning (RM) on top of RI and RP. Some interesting tools are IEISS (Interdependent Environment for Infrastructure System Simulations) and IIM (Inoperability Input – Output Model). IEISS mostly addresses military and government segments. It is best suited for sectors like energy, water and wastewater systems, nuclear reactors material and waste, as it simulates their dynamic behavior, including interdependencies between systems. IIM is a continuous input-output model developed by Sandia National Laboratories and Los Alamos National Laboratories and sponsored by Department of Homeland Security. It uses analytical models to determine the impact of an attack on infrastructure and its cascading effects in all other interconnected infrastructures.

Both tools analyze energy, water and wastewater sectors. Also, both of them use continuous simulation and are mostly used for internal, in-house analysis. Furthermore, both are built for risk identification risk prioritization and risk mitigation planning purposes. On the other hand, their diversities are not few. IIM has a wider variety of sectorial coverage contrary to those supported by IEIIS. Moreover, IEISS uses multi-agent systems with Monte Carlo simulation as a supplementary technique for modeling, where IIM uses rating matrices and network theory with continuous time-step simulation in order understand the dynamic behavior of the infrastructure systems. As a result, IEISS can be applied to numerous sectors, and its ability to perform a thorough experiments using Monte Carlo simulation seems promising and valuable.

CIDA (Critical Infrastructure Dependency Analysis tool) is a hybrid (empirical and network) based tool that extends a previous graph-based, risk analysis methodology to dynamically assess the evolution of cascading failures over time. It employs different growth models to capture slow, linear, and fast evolving effects, but instead of using static projections, the evolution of each interdependency between CIs is "objectified" by a fuzzy control system that considers the effect of near dependencies. To achieve this, the impact (and, eventually, risk) of each dependency is quantified on a time axis, in a form of many-valued logic. CIDA can analyze the last three stages of NIPP's Risk Assessment framework (RP, RMP, EE).

2.1.5.2 Comparison Based on TECHNICAL APPROACH

By comparing the modeling approach used by each tool along with the number of risk assessment stages covered, we have noticed that empirical based tools are mostly used to cover the first two risk management stages (RI, RP). Agent based tools are mostly popular for RI purposes, while network-based approaches can cover three risk stages (RI, RIA, RMP). System dynamic and network-based approaches are used mainly with tools which cover four risk management stages, but these tools are quite few and even fewer (only 3) are the tools that cover all 5 risk purpose stages with no specific approach trend. This info is depicted in figure 2.7, where the examined tools have been categorized according to their modeling approach in relation with number of purpose stages covered.

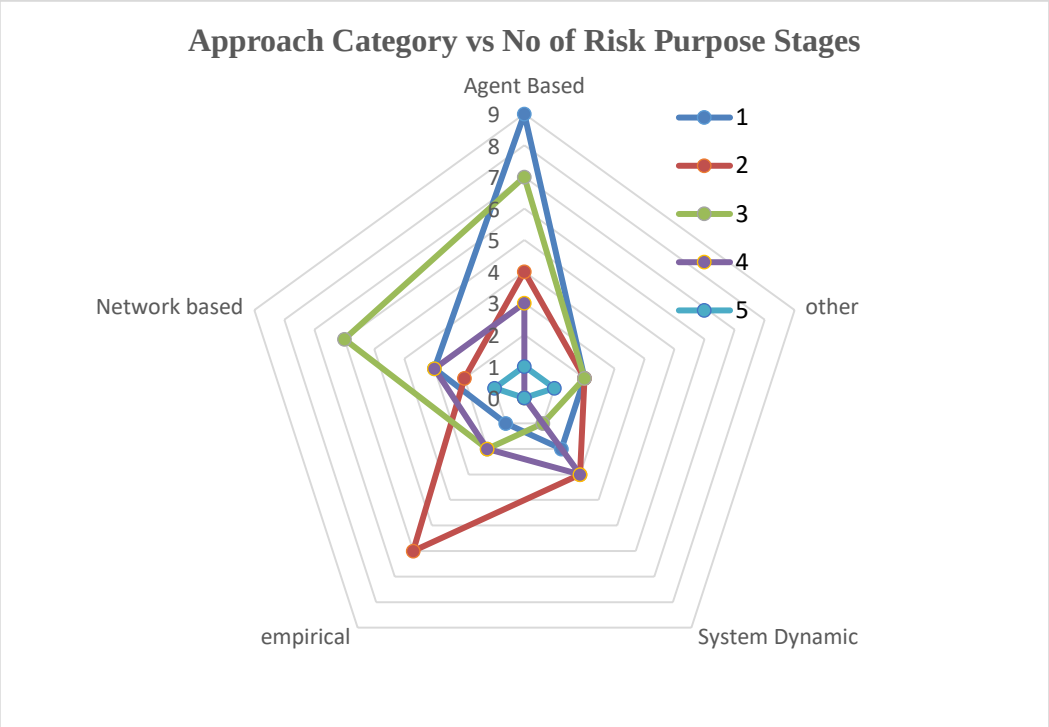


Figure 2.7. Modeling approach compared to Number of Risk Purpose Stages

Critical infrastructure modelling is mainly associated with simulation techniques and mathematical models, which are combined with the aforementioned supplementary computational techniques. Categorization according to the modeling approach used per number of sectors is presented in Figure 2.8. Agent based and network-based tools are covering mainly up to three CI sectors. Only a handful of tools and methodologies cover more than seven types of CI sectors.

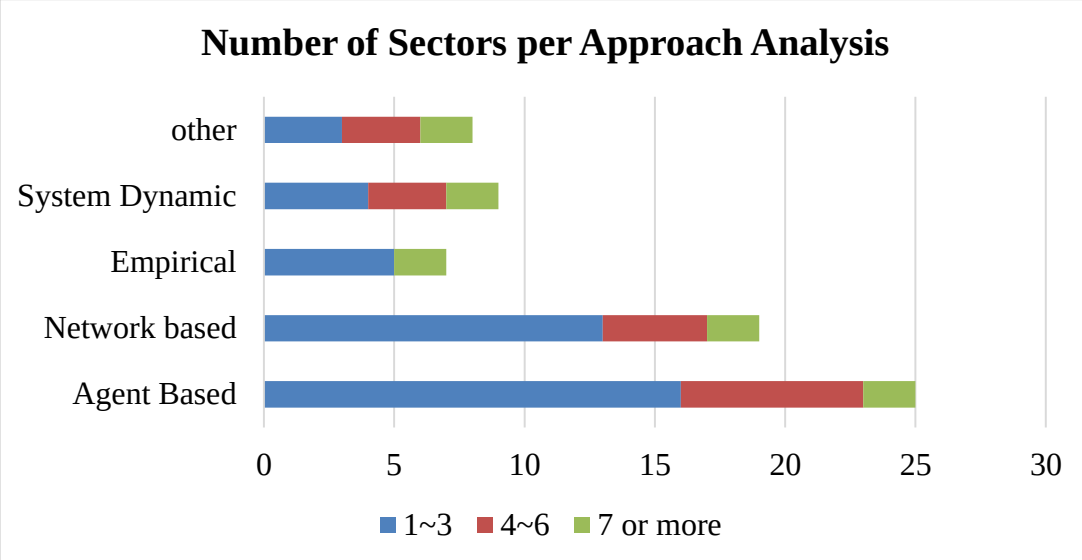


Figure 2.8. CIP Tools Classification per Modeling approach and No of Purpose Stages

For tools covering one or two sector, energy, transportation systems and/or public health sectors seem to be the most popular.

A wide acceptance of simulation paradigms exists, especially through modelling with the use of multi-agent systems as well as of system dynamics, that are most commonly combined with the computational methods of Monte Carlo simulation, discrete time-step simulation and continuous time-step simulation, because they are most suitable for optimal solutions. There are also other applications of agent-based simulation, which are combined with geographic information systems (GIS) in order to predict not only human behavior, but also the performance of the infrastructure in case of an emergency within specific geographic areas.

Relational databases, on the other hand, are currently the predominant choice to store data, information and records which represent the properties of a system in a precise manner. Thus, relational databases are widely used in asset inventorying which can be combined with monitoring of events, real time recording, geo-referencing (GIS), error logs, access control, risk components etc. By doing this, it is easier to establish relationships among elements that compose the critical infrastructure, just by matching data using common characteristics found within the data sets.

What is more, rating matrices are useful in assessing the severity of a risk, when an event occurs, through and decision-making procedure. These kind of modelling techniques not only include data processing in risk analysis and risk mapping to support decision making, but also make use of traditional techniques. They are quite popular due to the fact that they allow combination with every computational technique and also have the ability to facilitate on sensitivity analysis. Last but not least, rating matrices, are appropriate for data classification of geographic information systems (GIS) as well as of monitoring events, because they may, but not necessarily, contain weighted data.

As far as network theory is concerned, it makes possible to identify the most critical nodes of an infrastructure, by using graphical models which refer at the properties of the system in a precise manner. The complexity of network theory models, however, can increase exponentially for very large infrastructures. Thus, these models are practically applicable only to cases of smaller systems.

The majority of tools are dedicated to a specific sector (one or two similar sectors) (39 out of 68 tools) with energy and transportation sectors being the most popular sectors. NG Analysis Tools, EPRAM, FEPVA and RTDS are dedicated to the Energy Sector. NG Analysis Tools is an agent-based suite covering three purpose stages (RI, RIA, EE). FEPVA is a network-based tool that covers two purpose stages (RI, RIA) and EPRAM differentiates by being the only cellular automata modeling tool. EPRAM (Electric Power Restoration Analysis Model) calculates potential restoration times for electric power systems and determines the time point when restoration needs to start. Restoration results used in EPRAM are based on cellular automata models and industry data. This is a specific type of analysis that models each sector individually, since cellular automata have two possible values for each cell (0 or 1), and rules that depend on nearest neighbor values. The Real Time Digital Simulator (RTDS) tool provides simulation of power systems technology. It is used to study power systems with complex High Voltage networks. Since the simulator functions in real-time, the power system algorithms are calculated quickly enough to continuously produce output conditions which realistically represent conditions in a real network.

Some tools are only dedicated to the Transport Sector, namely ATOM, SIERRA, FastTrans & AIMSUN. Among them, ATOM and SIERRA cover more than four risk purpose stages and they are both implement network-based method approaches. FastTrans is an agent-based tool that covers three purpose stages (RI, RIA, RPR). AIMSUN is the only EU originated tool and can cover two purposes (RIA, RM). Each analysis approach is based on system dynamics.

Europe has developed mainly methodologies (COUNTERACT, EURACOM, IRRIIS) and not full simulation tools. AIMSUN is the only Transport Simulation tool developed in Spain. Its analysis approach is based on system dynamics. The tool is able to cover two purpose stages (RI, RPR) but only one sector (Transportation).

It is worth to mention that a meta-tool has been developed in the U.S., namely SimCore. SimCore combines multi-agents as its modelling technique with discrete time-step simulation. It utilizes a collection (family) of simulation applications (ActivitySim, DemandSim, SessionSim, FastTrans and MIITS-NetSim) All of them follow the SimCore modelling paradigm as a library for building large-scale distributed-memory discrete event simulations and can work together by exchanging events.

2.1.6. Summary of Research Work

In this work we have identified, classified, and compared various tools that have been developed to analyze CIs and support CI risk management. Emphasis has been given on the comparison of similar tools from the perspective of their purpose and modeling approach. Most Critical Infrastructure Protection plans have been based on risk management frameworks. USA/NIPP keeps the most advanced program in developing strategies, techniques, and applications. In general, the study of threats and vulnerabilities in Critical Infrastructure systems is categorized in two distinct aspects in the development of methodologies and applications.

The first one describes the current state of an infrastructure, by using purpose stages to obtain a clearer view of infrastructure performance and its response to vulnerabilities. Literature review identified the models used for each stage of risk assessment and mitigation and showed that significant research focuses on risk identification and risk assessment stages.

Critical Infrastructure modeling tools and applications use modeling approaches that utilize and possibly merge multi-agent systems, system dynamics, the network theory, or empirical systems. Multi-agent and network-based systems are the most widespread modeling techniques.

The effective implementation of the CIP plans depends on the degree to which government and private sector partners engage in systematic, effective, multi-directional information sharing. Therefore, it is strongly recommended any cooperation between governmental or supranational organizations or agencies with appropriate levels of authority and responsibility.

2.2. Cybersecurity Self-assessment Tools: Evaluating Importance for Securing Industrial Control Systems in Critical Infrastructures

2.2.1. Introduction [2]

Periodically assessing the security status of Industrial Control Systems (ICS) is essential to enable cybersecurity compliance and performance evaluation against an organization's risk appetite. Ensuring appropriate security level is especially important in Critical Infrastructures (CI). Existing cybersecurity risk management methodologies provide frameworks through which CI stakeholders can enhance security and better protect their assets, against cybersecurity risks. Following traditional risk assessment procedures, a self-assessment tool can support an organization to build up on knowledge and security awareness, check implemented cybersecurity practices and responsibilities. Such methods and tools, when systematically implemented, can identify security weaknesses, establish cybersecurity targets, and improve resilience. This subsection aims to provide a review and analysis of available cybersecurity Self-Assessment tools, which can be used by ICS owners and CI operators. We also focus on questionnaire content analysis, used in self-assessment tools, with the purpose to create a classification of questions content, according to core functions of NIST Cybersecurity Framework.

Adequate security of information in Industrial Control Systems (ICS) and supporting Critical Infrastructures (CI) is a fundamental management responsibility. ICS employees and supervisors must be constantly aware of the status of their information security controls, to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Cybersecurity self-assessment tools realize risk assessment and risk management procedures and provide automated solutions for CI operators and owners to determine the status of their information security programs and, where necessary, pinpoint specific targets for improvement. Self-assessment tools usually utilize extensive and structured questionnaires containing specific control objectives and security measures against which any ICS or group of interconnected ICS systems can be tested and evaluated (Stouffer, Lightman, et al., 2015).

[2] *Related Publication:* Lykou G., Anagnostopoulou A., Stergiopoulos G., Gritzalis D., "CYBERSECURITY SELF-ASSESSMENT TOOLS: Evaluating Importance for Securing Industrial Control Systems in Critical Infrastructures", in Proc. of the 13th Intern. Confer on Critical Information Infrastructures Security, CRITIS-2018, Kaunas, September 2018.

This work aims to provide a review and analysis of available cybersecurity Self-Assessment tools, which can be used by ICS owners and CI operators. These tools support organizational risk management and enforce cybersecurity by identifying operating weaknesses, employee's security awareness and by evaluating implementation of effective control practices to protect ICS against realistic threats and associated risks. In addition, we deepen our research into questionnaire content analysis, which is used by the examined self-assessment tools, with the purpose to create a classification on questions content, according to the Core Functions presented by the newly published "Cybersecurity Framework v.1.1" of National Institute of Standards and Technology (NIST), which promotes the protection and resilience of critical infrastructures (NIST, CYBERSECURITY FRAMEWORK, 2018)

The structure of this work after the Introductory part is as follows: Subsection 2.2.2 presents Security Challenges for ICS and 2.2.3 related work on ICS Cybersecurity Risk Assessment and Management. Subsection 2.2.4 presents four developed self-assessment tools and provides a comprehensive comparison. In subsection 2.2.6, the analysis is extended to questionnaire content analysis and classification. Finally, subsection 2.2.6 extracts main conclusions and importance evaluation of using Cybersecurity Self -Assessment Tools for risk management purposes.

2.2.2 Cybersecurity Challenges for Industrial Control Systems

ICS is a general term describing cyberphysical and automation systems responsible for data acquisition, visualization and control of processes found in industrial sectors and supporting CIs. They play a critical role, not only in maintaining the business continuity, but also in ensuring functional and technical safety, preventing large industrial accidents and environmental disasters. ICS encompasses several types of control systems, including Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) and others.

In the past, ICS had little resemblance to the traditional information technology (IT) systems, since they were isolated systems, running proprietary control protocols and using specialized hardware & software (Stouffer, Lightman, et al., 2015). Widely available, low-cost Internet Protocol devices are now replacing proprietary solutions, which increases their functionality and interoperability, along with the possibility of cyber security vulnerabilities and incidents. Moreover, the goals of safety and efficiency sometimes conflict with security in the design and operation, since ICS have unique execution criticality and reliability requirements (24hr x 365 days/year), thus change management can jeopardize their integrity and performance.

The trend toward integrating ICS systems with IT networks provides significantly less isolation from the outside world, creating a greater need to secure these systems from remote, external risks. Threats to both ICS and IT systems can come from numerous sources, including malicious intruders, terrorist groups, disgruntled employees, accidents and others (ENISA, 2015a). Therefore, ICS have greater security challenges to confront, since they have not achieved yet the same level of cybersecurity maturity as other cyber or IT resources.

2.2.3 Related work on ICS Security Management

Over the last decade, a number of standards and directives dealing with cybersecurity of ICS systems have emerged. In 2004, NIST published the System Protection Profile for Industrial Control Systems, which covered the risks of ICS systems. In 2007, the US President's Critical Infrastructure Protection Board and the Department of Energy outlined the steps an organization must undertake to improve the security of ICS networks by introducing 21 Steps to Improve Cyber Security of SCADA Networks (US Department of Energy, 2007). In 2008, the Centre for Protection of National Infrastructure (CPNI) produced a Good Practice Guide for Process Control and SCADA Security encapsulating best security practices (Guide & Governance, 2006). In 2013, the European Union Agency for Network and Information Security (ENISA) released the recommendations for Europe on ICS security and three years later published security good practices for ICS/SCADA Systems. In 2014, the North American Electric Reliability Corporation (NERC) introduced the development of a wide range of standards covering many aspects of ICS cyber security. Finally, NIST has released a comprehensive guidance on wide range of security issues, and technical, operational and management security controls, last updated in 2015 (Stouffer, Lightman, et al., 2015). Over and above to these guidance work, scientific research has developed various CIP tools, able to model CI characteristics, their interdependencies and the impact of potential failures in their systems. In previous work (Stergiopoulos, Vasilellis, et al., 2016), a review of sixty-eight available in literature tools, frameworks and methodologies for CI protection were analyzed and classified. However, these tools do not concentrate on ICS systems, instead they examine CIs entities as a whole.

Risk assessment is generally understood as the process of identifying, estimating and prioritizing risks to the organizational assets and operations. This is an essential activity within security management, as it provides the foundation for risk identification and treatment with the adoption of effective cybersecurity measures. Several methods and tools are available in literature for conducting risk assessments. These vary according to contexts, as well as the type of organizations and the CI for which the assessment is designed. A few examples of the most popular and well-

regarded approaches include ISACA, ISO/IEC 27001, OCTAVE, COBIT, CRAMM, MAGERIT and EBIOS. Their origins range from standard-setting bodies (e.g., ISACA and ISO/IEC) to governments (e.g., UK for CRAMM, France for EBIOS, Spain for Magerit etc).

Despite the large number of risk assessment methodologies, the particularities of SCADA often prevent the straightforward application and adjustment is required to fit the context of SCADA systems. Therefore, focused on ICS systems, a detailed overview of twenty-four risk assessment methods developed for SCADA systems was presented by (Cherdantseva et al., 2016). This work pinpointed that, for the vast majority of the methods examined for ICS, there was no software prototype or automated tool in order to support them. Instead, in several methods the development of software prototype was outlined as a subject for future work. Our literature research revealed that despite exhaustive work on ICS cybersecurity protection guidance, risk assessment and management tools, no research has been presented related to self-assessment tools analysis and their complementary effect on ICS cybersecurity and efficient risk management.

Self-assessments usually provide an additional tool for organizations to determine current status of their information security programs, improve staff security awareness, prepare organization before security audits and establish new targets for improvement (Swanson & Lennon, 2001). Most self-assessment methods utilize an extensive questionnaire survey, containing specific audit objectives, for testing and evaluating control systems or group of interconnected systems. These questionnaires do not establish new security requirements. Instead, their control objectives and techniques are abstracted directly from long-standing requirements & established standards, as found in statute, policy, and guidance on security. For a self-assessment to be effective, a complementary risk assessment should be conducted by security experts in parallel or in advance. Therefore, a self-assessment does not eliminate the need for a risk assessment within the organization Risk Management Program.

NIST has introduced in 2003 the first Automated Security Self-Evaluation Tool (ASSET) to automate the process of completing a system self-assessment, contained in NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems (Swanson & Lennon, 2001). Since then, several security self-assessment tools have been developed, evolved, and enhanced with functionalities which are presented, analyzed, and compared in subsection 2.2.4. As part of its efforts to increase awareness, understanding and reducing cyber risks to critical infrastructures, NIST has also developed a voluntary framework, based on existing standards, guidelines, and practices (NIST, CYBERSECURITY FRAMEWORK, 2018). This cybersecurity framework creates a solid basis for managing cybersecurity risks related to critical infrastructure. It provides a risk-based approach for cyber-

security through five core functions: i) identify; ii) protect; iii) detect; iv) respond; and v) recover. These core functions represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions. A short description of each function is listed below:

1) *The Identify Function* assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data and capabilities.

2) *The Protect Function* outlines appropriate safeguards to ensure delivery of critical infrastructure services.

3) *The Detect Function* defines the appropriate activities to identify the occurrence of a cybersecurity event. It enables timely discovery of cybersecurity events.

4) *The Respond Function* includes appropriate activities towards a detected security incident, by enhancing the ability to contain impact of any cybersecurity incident.

5) *The Recover Function* identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, by supporting timely recovery to normal operations.

2.2.4. ICS Cyber Security Self-Assessment Tools

In this section we briefly present four self-assessment tools that have been developed with the scope to support cybersecurity management in critical CIs and provide specific analysis, or a dedicated section for ICS & SCADA evaluation.

i) Control System Cyber Security Self-Assessment Tool (CS^2SAT): is a desktop software tool that gathers information about the facility of ICS, guides users through a step-by-step process to collect specific control system information and makes appropriate recommendations for improving system's cyber-security. The purpose of CS^2SAT is to provide organizations that use ICS to control any physical process with a self-assessment tool for evaluating the programmatic and certain aspects of security (Lee, 2008). It is designed as a self-contained tool to assist individuals in identifying cyber security vulnerabilities and then it provides a comprehensive evaluation of implemented security programs and comparison to existing industry standards and regulations.

For organizing the self-assessment, the following steps are followed: 1) *Preparation for Self-Assessment* which includes the formation of team and collection of ICS architecture and related information; 2) *Documentation of Assessment Information* which maintains organization reference information and a baseline for future assessments; 3) *Determination of Security Assurance Level (SAL*) which gives an overall rating of criticality according to the users' reviews of security scenarios and estimated consequences; 4) *Network Topology Drawing* to create the representative network architecture; 5) *Question Answering* based on the network diagram, addressed to both component, system and administrative-level; 6) *Generation of Reports* depending on the SAL level selected by user, including information related to standards compliance. The CS^2SAT also provides recommendations from a database of industry available cyber-security practices. Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities (Lee, 2008).

ii) Cyber Security Evaluation Tool (CSET): is a desktop software tool, which helps through a step-by-step process, owners to assess information and operational systems cybersecurity practices, by asking a series of detailed questions about system components and architectures, as well as operational policies and procedures (CISA, 2018b). These questions are derived from accepted industry cybersecurity standards. Self-assessment tool is organized based on the following steps: 1) *Selection of Standards* where user chooses according to its needs to comply with; 2) *Determination of Security Assurance Level (SAL)* which depends on the responses related to the potential consequences of a successful cyber-attack on an ICS or related facility; 3) *Diagram Creation* through a graphical interface for the creation of network topology; 4) *Question Answering* based on the selection of the triad: network topology, selected security standards and SAL; 5) *Analysis of Results* provided both in summary and detailed form, pinpointing top areas of security concern. CSET includes a dedicated section to support ICS and SCADA security analysis for a tailored assessment of cyber vulnerabilities. Once ICS standards have been selected and the resulting questionnaire is answered, CSET creates a compliance summary, compiles variance statistics, ranks top areas of concern, and generates security recommendations.

iii) SCADA Security Assessment Tool (SSAT): is a tool developed by UK Centre for the Protection of National Infrastructure (CPNI) for SCADA utilities and CIs. According to CPNI, it provides a high-level snapshot of the information assurance of an organization's ICS that are deemed to constitute the UK critical national infrastructure. Moreover, it contains 99 questions divided into various categories for physical, personnel and electronic evaluation performance, based upon CPNI Good Practice Guidance and international good practices. SSAT output result is a

performance scoring, aggregating users answering on specific targeted questions and providing high level understanding of SCADA/ICS security status. Finally, SSAT is not a standalone self-assessment tool, so it is less robust tool than the previous examined ones.

iv) Cyber Resilience Review Self-Assessment Package (CRR): is an interview-based assessment able to evaluate an CIs organization's cybersecurity practices and operational resilience. It has a dedicated section for control management and can be either conducted as a self-assessment or as on-site assessment facilitated by cybersecurity professionals (CISA, 2018a). CRR focuses on key areas that typically contribute to the overall cyber resilience and measures essential cybersecurity capabilities to provide indicators of an organization's operational resilience during normal operations and during times of operational stress. CRR assesses enterprise programs and practices across several domains including risk management, incident management, service continuity etc. CRR can evaluate cyber resilience capabilities of a wide range of organizations both in terms of different critical services or CI sectors and in terms of organizational size and maturity.

Cybersecurity Self-Assessment Tools Comparison

The comparison of the above presented tools is exhibited in Table 2.3, based on standards compliance, usability and functionalities offering to their users. Analysis has revealed many commonalities in their design and principal characteristics, as summarized below:

Table 2.3: Cybersecurity Self-Assessment Tools Comparison

TOOL DESCRIPTION	CS²SAT	CSET	SSAT	CRR
Type	Desktop software application tool	Desktop software application tool	Questionnaire XLS assisted Tool	Questionnaire PDF assisted Tool
Developer	Department of Energy National Laboratories	ICS-CERT / DHS	CPNI	US-CERT / DHS Carnegie Mellon University
Origin	USA	USA	UK	USA
Description	Self-contained tool step-by-step process	Self-contained tool step-by-step process	SSAT Questionnaire which links directly to the CPNI SCADA security good practice.	Self-contained tool

TOOL DESCRIPTION	CS²SAT	CSET	SSAT	CRR
Step Process	6	5	1	1
Survey Method	Structured Questionnaire	Structured Questionnaire	Structured Questionnaire	Structured Questionnaire
Security Expertise Needed	YES	NO	YES	NO
Standards Compliance	NERC CIP, NIST SSP-CIPCS, NIST SSP-ICS, NIST SP 800-53, DoD 8500.2 ISO/IEC 15408	DHS Cat. of CS NERC CIP 002-009 NIST SP 800-82 NIST SP 800-53 NRC Reg. Guide 5.7 CNSSI 1253 INGAA Control Security Guidelines NISTIR 7628 Guide	CPNI Good Practices NIST SPP-CIPCS NIST SPP-ICS ISO/IEC 15408 NERC CIP 002-009 NIST SP 800-53 DoD IA	NIST SP 800-18 NIST SP 800-30 NERC CIP FISCAM Clinger-Cohen law GISRA law FIPS 102 OMB Circul. A-130
Checks ICS Compliance with Security Standard	YES	YES	NO	NO
Database of industry available cyber-security practices	YES	YES	NO	NO
Sector average score	NO	YES	YES	NO
Recommendation List	YES	YES	YES	YES
Type of Result	Full Performance Evaluation	Full Performance Evaluation & Compliance of Selected Std	Scoring Result	Full Performance Evaluation

Three out of four examined tools have been developed in the US and comply with the majority of cybersecurity guidance, standards, and regulatory requirements for Critical Infrastructures such as NIST, NERC, DHS, CIP etc. Also, since it is quite important for organizations to certify compliance with specific standards both CSET and CS²SAT provide compliance check functionality, while SSAT and CRR do not. CRR is focused on resilience capabilities and contingency plans and reflects best

practices from industry for managing operational resilience across the disciplines of security management. All tools provide a list of recommendations, while only CSET and CS^{2}SAT can relate each recommendation with included database of industry cybersecurity practices. In addition, CSET and SSAT can provide a sector average scoring result, which can assist operators evaluate their performance related to industry average.

From graphical facilities, CSET and SSAT contain a graphical user interface that allows users to diagram network topology and identify the "criticality" of the network components. Moreover, in CSET user can import a pre-built template diagram or import an existing MS Visio diagram.

One main difference occurs in the presentation of the results, where CSET gives a full report of evaluation performance with compliance analysis according to selected standards. Less detailed report is produced by CS^{2}SAT, while CCR report focus more on resilience and contingency reporting analysis and recommendations. Finally, the SSAT provides a simple scoring result with limited technical analysis and recommendations.

One common functionality of all presented tools is that they base they evaluation on a well-structured and specific targeted questionnaire to assess the security programs and organization risk management effectives. Therefore, in the following section we will further investigate questionnaire functionalities, design and characteristics.

2.2.5. Questionnaire Content Analysis

As we have seen in Table 2.3, for every Self-Assessment tool a structured questionnaire is used as a survey method for collecting valuable information for self-evaluation purposes. This is a common technique for collecting information and completing an internal assessment of the security controls designed, applied, and performed.

These questionnaires can serve for many purposes. First, they can be used by management team and experts who know their agency's systems and security controls to gain a general understanding of security assurance and make informed decisions about the agency improvement needs. Second, they can be used as a guide for thoroughly evaluating the status of security for a system. Third, they can enhance and support employees' security awareness. Finally, the results of such thorough reviews provide a much more reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resource needs. Therefore, the completed self-assessment questionnaires are a useful resource for

compiling agency reports, such as: security program management and security planned activities.

In this subsection we analyze and compare the questionnaires used for assessing ICS security, which are namely: i) NIST SP 800-26 Security Self-Assessment Questionnaire which is used in the first three examined tools; ii) CSET Scada Self-Assessment Questionnaire when not using NIST Cybersecurity Framework; and iii) CRR Self-Assessment Questionnaire used by the CRR tool.

Overview of Scada Self-Assessment Questionnaires

NIST SP 800-26 Security Self-Assessment Questionnaire: As already stated before, NIST developed this questionnaire to assess the status of security controls of an IT system, an interconnected group of systems. There are 260 questions, which are separated into three major control areas: operational, management and technical controls. Figure 2.9 depicts the topics of each of the above areas that are included in the questionnaire.

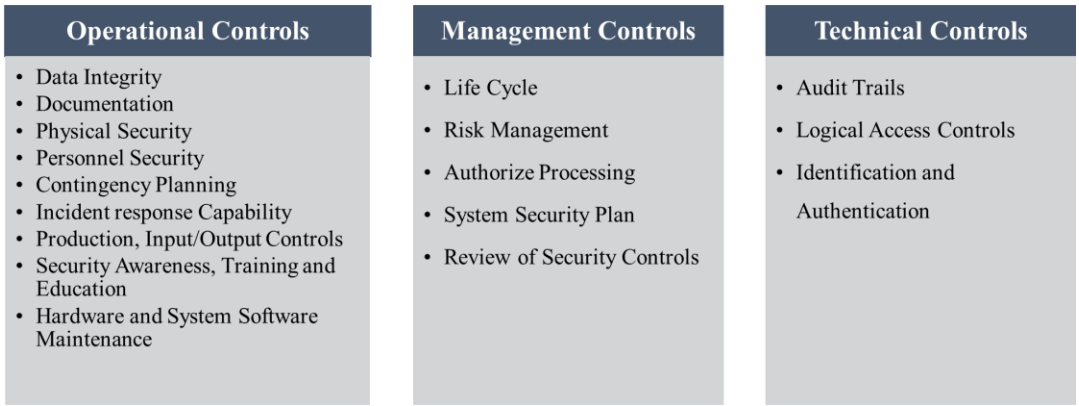


Figure 2.9: NIST Topic Areas of Questions

Moreover, instead of positive or negative answering for each question posed, a progressive scale of effective implementation has been developed to measure and evaluate five compliance levels, which are:

i) LEVEL_1: Documented policies
ii) L_2: Procedures for implementing the control
iii) L_3: Control implemented
iv) L_4: Control Tested
v) L_5: Controls are integrated in agency's organizational culture, so procedures and controls are fully integrated into a robust security program.

In Figure 2.10, the screenshot of NIST questionnaire completing form is presented.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								

Figure 2.10: NIST Questionnaire Screenshot

CSET Scada Self-Assessment Questionnaire: assess security of information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architectures, as well as operational policies and procedures. CSET provides a variety of questionnaires structures derived from selected by user industry cybersecurity standards. Specifically, CSET questionnaire starts survey by requesting information about the critical sector, the industry, the gross value of the assets that the organization wants to protect and time expected to be spent for the assessment effort. Moreover, users are able to choose whether privacy is a significant concern for their assets, their procurement supply chain assessment needs and the use of ICS systems. So, after completing this interactive section, next step is to specify Security Assurance Level and the appropriate Standards. Depending on the above selections up to 1030 questions reposed to responders, which can be separated into three major areas: management, operational and technical controls. Figure 2.11 depicts the topics of each of the above areas that are included in the questionnaire.

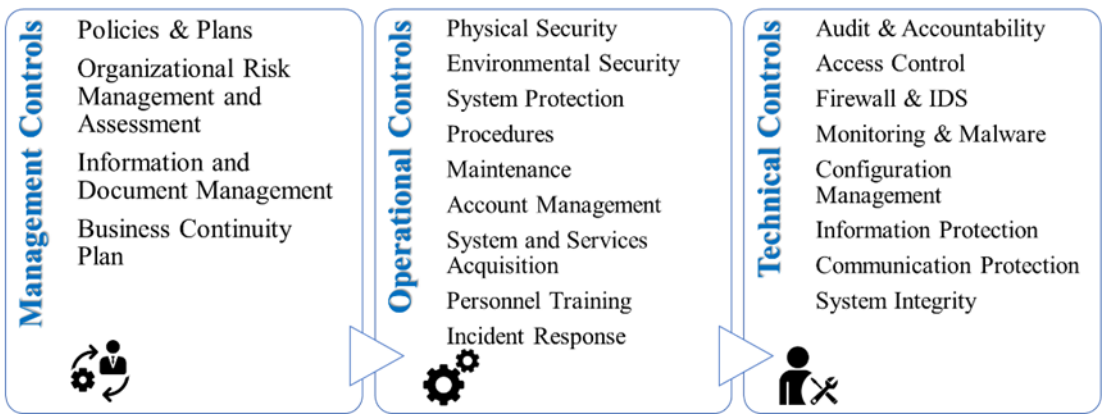


Figure 2.11: CSET Topic Areas of Questions

CRR Self-Assessment Questionnaire: is a resilience focused questionnaire created by DHS for the purpose of evaluating the cybersecurity and service continuity practices of critical infrastructure owners and operators. The CRR consists of 365 questions, to elicit answers from the critical infrastructure organization's personnel in cybersecurity and operations. The CRR is derived from the CERT Resilience Management Model (CERT-RMM), which was developed by Carnegie Mellon University and reflects best practices from industry and government for managing operational resilience, business continuity management, and information technology operations management. As shown in Table 2.4, the number of goals and practice questions varies by domain and there are ten questionnaire domains examined.

Table 2.4: CRR Questionnaire Domain Composition

CRR QUESTIONAIRE DOMAIN	GOALS	GOAL PRACTICES	QUESTIONS
Asset Management (AM)	7	29	78
Controls Management (CM)	4	16	38
Configuration and Change Management (CCM)	3	23	37
Vulnerability Management (VM)	4	15	47
Incident Management (IM)	5	23	36
Service Continuity Management (SCM)	4	15	31
Risk Management (RM)	5	13	26
External Dependencies Management (EDM)	5	14	27
Training and Awareness (TA)	2	11	24
Situational Awareness (SA)	3	8	21
TOTAL	42	167	365

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of maturity indicator level questions. The MIL scale uses six maturity levels, which are: i) Incomplete, ii) Performed, iii) Planned, iv) Managed, v) Measured, vi) Defined. The CRR divides assets into four categories: People, Information, Technology, and

Facilities. Some questions require a separate answer for each of the four assets, while other questions refer to all assets.

Questionnaires Comparison

In this section, we compare the above questionnaires and their qualitative and quantitative characteristics. As we can see in Table 2.5 the examined questionnaires have a very diversified number of questions (q), to perform self-assessment evaluations, that is NIST has 258q; CSET has 1030q to ask the user when high level of SAL is selected, and CRR has 365q. As obvious from questionnaire's size, CSET offers more detailed investigation for each area of controls examined and provides real defense-in-depth analysis.

Table 2.5: Questionnaire Analysis

QUESTIONNAIRE ANALYSIS	NIST	CSET	CRR
Number of Available Questions	258	1030	365
Question Type	Close Ended, Scaled Answering (L1-L5)	Open & Close Ended, YES/NO Answering	Open & Close Ended, YES/NO Answering
Link to supplementary information or explicatory info provided	No	Yes	Yes
Additional Comments Allowed	Yes	Yes	Yes
Complementary data requested based on user's answering allowed	No	Yes	No
Static/ Dynamic security flow analysis	Static Flow	Dynamic Flow	Static Flow

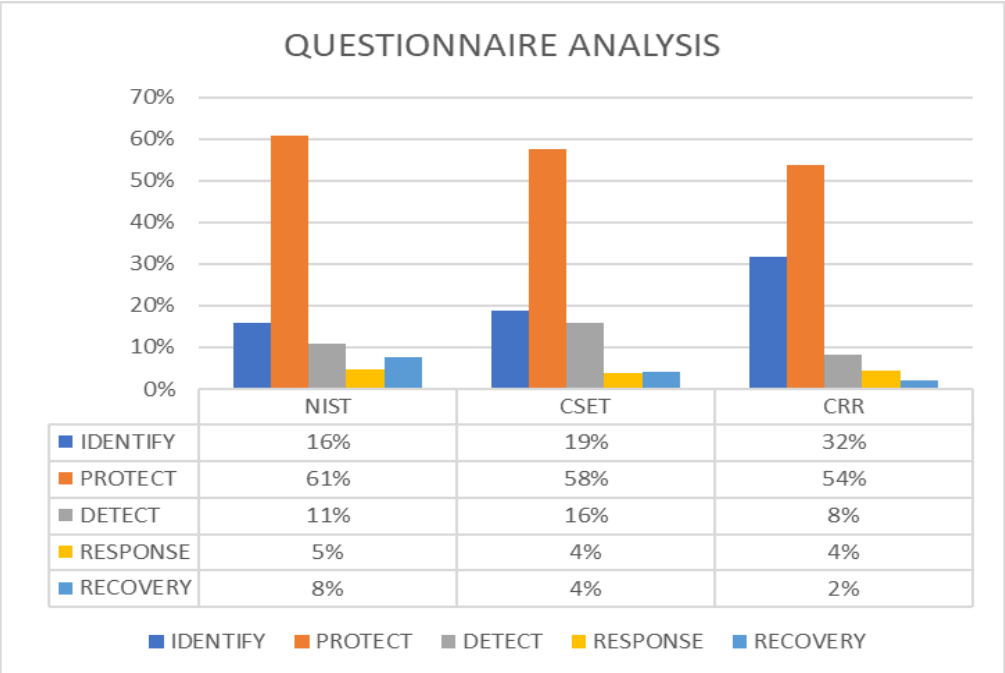
NIST has a static flow of questioning structure for analysing the 17 topic areas presented in figure 2.9, while question type permits a scaled answering with 5 implementation levels. CSET is the most detailed and advanced questionnaire with a dynamic flow of questions, and interaction based on user's selection. It can accept additional information either in the form of comments, data, files, graphs, diagrams and other material, while the user can override any question he considers as irrelevant. CRR uses both close and open-ended questions from ten thematic domains and can provide additional information to respondents to assist and facilitate their assessment.

Furthermore, by using the 5 Core Functions of NIST Cybersecurity Framework, we have analyzed all questionnaires and classified according to their content. Each

question was classified to a specify core function. Analysis results are depicted in Figure 2.12.

Although the examined questionnaires have a very diversified number of questions, to perform self-assessment evaluations, when percentage analysis is performed, the majority of questions with percentage range from 54% to 61% belong to Protect Core Function. This reveals the importance given to technical measures and safeguards to ensure cybersecurity performance.

Questions related to the Identify Function vary from 16% or 41q in NIST Questionnaire, 19% or 194q in CSET and 32% or 116q in CRR, which indicates that organizational understanding to cybersecurity management is more trivial to assess. On the other hand, the questions dealing with Response and Recovery Function keep a very low as a percentage, despite resilience and contingency necessity in ICS and CI facilities.



	NIST	CSET	CRR
IDENTIFY	16%	19%	32%
PROTECT	61%	58%	54%
DETECT	11%	16%	8%
RESPONSE	5%	4%	4%
RECOVERY	8%	4%	2%

Figure 2.12: Questionnaire Analysis based on NIST Cybersecurity Framework

It is obvious from above graph that the greatest gravity of self-assessment questionnaires is given to protective measures and controls, related to less importance given on managerial and operational practices as included in the identify function. We can also realize that response and recovery investigation functions are significantly less examined, despite being an essential function for organization's resilience. This area should be further enriched in the future with additional content to assess specific areas to self-assessment questionnaires and related tools.

2.2.6. Summary of research work

Adequate security of information in Industrial Control Systems (ICS) and supporting Critical Infrastructures (CI) is a fundamental management responsibility. ICS employees must be constantly aware of the status of their information security controls, in order to make informed judgments and appropriately mitigate risks to an acceptable level. There are many methods and tools for agency officials to help determine the current status of their security programs relative to existing security policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify weaknesses and where necessary, establish targets for continuing improvement.

Self-assessment tools provide a tailored assessment for CI operators and owners for assessing cyber vulnerabilities of ICS. Based on a selectable array of cybersecurity standards, these tools provide structured questionnaires to build organizational knowledge and create a cybersecurity compliance report with compiled statistics and security recommendations. Since self-assessment tools do not generate a complex risk assessment, they won't provide a detailed architectural analysis of the network or detailed hardware/software configuration review. Therefore, periodic onsite reviews and inspections must still be conducted, using a holistic approach including facility inspection, interviews, examination of facility practices, and penetration testing.

It is important to note that self-assessment tool is not intended to provide an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in cybersecurity standards and government/legal mandates. In addition, specific technical controls, such as those related to individual technologies or vendors, are not specifically provided due to their volume and dynamic nature.

Cybersecurity self-assessment questionnaires are only one component of the overall cyber security assessment and should be complemented with a robust cyber security evaluation program within the organization. A self-assessment cannot reveal all types of security weaknesses and should not be the sole means of determining an organization's security posture. It should also be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately.

Chapter 3: Analysis of Climate Change Impacts and Environmental Threats in Transport Sector

3.1. Protecting the transportation sector from the negative impacts of climate change

3.1.1 Introduction [3]

Observed and projected climate change, such as increases in temperature, sea level rise and the increase in frequency and intensity of extreme weather events, have come to challenge the operation of critical infrastructures (CIs). The transport sector belongs to CIs, as it is an important pillar of our economy and society. Transport, as many other CI sectors, is comprised of complex systems with responsibilities distributed across many different stakeholders. This situation makes integrated adaptation approaches challenging to achieve, requiring appropriate governance, and coordinated action. In recent years, climate change adaptation started to emerge as a need for resilient and sustainable infrastructures. Despite the key role of transport and the huge challenges posed by climate change, attention to the need of adaptation and risk reduction at the given sector is relatively low. Good adaptation action requires climate vulnerability analysis and impact knowledge, so it is important that adaptation options are properly identified, evaluated, and monitored.

This subsection aims to detect and analyze global adaptation initiatives, in order to classify adaptation options, while focusing on emerging adaptation challenges and opportunities in the transport sector. This will enable stakeholders to improve transport effectiveness and future sustainability, while stimulating what additional actions are needed for climate change adaptation.

Recent modeling studies indicate that global average temperatures will increase in excess of two degrees Celsius over the next century (IPCC, 2014). Evidence from the United Nations Intergovernmental Panel on Climate Change (IPCC) indicate that these changes will have significant implications for extreme weather events, development, economic stability, population and ecological health. Climate change issues and concerns for Critical Infrastructures focus on climate variations and

[3] *Related Publication:* Lykou G., Stergiopoulos G., Papachrysanthou A., Gritzalis D., "Climate adaption: Addressing risks and impacts of climate change on Transport Sector", 11th International Conference on Critical Infrastructure Protection (CIP-2017), USA, March 2017.

extreme weather events that are projected to change in magnitude, frequency or duration (US EPA, 2015). CIs are typically designed to withstand weather-related stressors common in a particular locality but shifts in climate patterns increase the range and type of potential risks. Most infrastructures being built today are expected to last for decades or even centuries (McLean et al., 2011b). Investing in infrastructures that were not designed to consider potential changes to future climate, can result in significant cost increases later and can rise the potential for unplanned outages and failures.

The rest of this study is structured as follows: A short presentation of transport sector is given in subsection 3.1.2, while its impacts from climate change are exhibited in 3.1.3. Adaptation approaches are presented in subsection 3.1.4 and adaptation assessment in 3.1.5. Options identification and classification are introduced in subsection 3.1.6. In subsection 3.1.7 how adaptation options, that can be applied to transport sector, are analyzed, while implemented measures are collected and classified according to classification methods already discussed. Finally, subsection 3.1.8 concludes our research and proposes further work.

3.1.2 Introduction to Transport Sector as CI

Transport is a critical infrastructure that greatly supports the smooth functioning of society's prosperity and viability of economies worldwide (Committee on Climate Change and U.S. Transportation, 2008). It facilitates accessibility of services that are vital for business and for the quality of life of citizens. Gradual climate change such as increases in temperature, sea level and rainfall regimes along with the projected increase in frequency and intensity of some extreme weather events will seriously challenge the transport sector. While mitigation efforts remain of great importance, in order to reduce anthropogenic contribution to climate change, a simultaneous focus on CIs adaptation is essential (European Commission, 2011).

In this research, we have studied Climate Change Adaptation approaches, strategies, and action plans, with a goal to present a survey of adaptation measures applied to the Transport section, along with a detailed classification and analysis of each measure according to established classification methodologies. We have specifically focused on transport sector impacts, searching into national and sectoral adaptation plans for best practices and efficient adaptation options.

Transport is the movement of people and goods from one location to another. It consists of: (i) **transport infrastructure** (fixed installations including roads, railways, bridges, canals and pipelines and terminals such as airports, railway stations, bus stations, seaports etc.), (ii) **vehicles** (such as cars, buses, trucks, railcars and locomotives, ships and barges, aircraft and drones, etc.), and (iii) **operations**

(people, institutions, laws, policies, and information systems) that convert infrastructure and vehicles into working transportation networks. Modes of transport include air, rail, road, water, pipeline and space. In this subsection, the transport sector and detected climate impacts on different transportation modes are presented and analyzed.

Transport activity is the result of bringing together resources of quite different nature. Service providers put together these resources to make transport services available for different needs, thereby using different transport modes. Regulators at the various administrative levels provide the basic rules to facilitate operations to run smoothly, efficiently and with minimum impacts (European Commission, 2011). Finally, the numerous users make their choices and thereby shape transport demand.

Disruptions to transportation systems can cause large economic and even human losses. For this reason, the transport sector is often characterized as a CI (Transportation Research Board, 2009); an important pillar of our economy and society. Since most stakeholders may only have a partial perspective of the system they manage or use, it is expected that without any national protection strategy, stakeholders will react autonomously to the challenges of climate change. Given the broad challenges of climate variations and the strong interconnectivity inside the transport sector, such a fragmented approach will potentially lead to great inefficiencies for transport sustainability and resilience to climate impacts.

3.1.3. Impact of Climate Change on Transport Sector

Rising temperatures and extended heatwave periods increase the problems of rail buckling, road pavement deterioration and thermal comfort for passengers in vehicles. Weather extremes generating floods or landslides, which can lead to short term delays and interruptions in all transportation modes, but also long-term interruptions and detouring needs in the event of destroyed land-side infrastructure. Sea level rise can threaten harbors and other transport infrastructure and services in coastal areas. Air transport can be challenged by changing wind patterns, flooding of airport infrastructure, and various extreme weather events. In addition, climate impacts that trigger changes in the organization of society and economy, like different tourist destinations or agricultural productions, can seriously reform transport demand. Table 3.1 presents, in detail, the climatic pressures and risk of climate change for all transport modes, as collected by several literature sources (Committee on Climate Change and U.S. Transportation, 2008; Transportation Research Board, 2009; European Environment Agency, 2014; US EPA, 2015)

Table 3.1: Climate risk and impacts on transport infrastructure

Type		Climatic pressures	Risks
Land Transportation	Rail	Summer heat	• rail buckling • material fatigue • increased instability of embankments • overheating of equipment (e.g. engine ventilation, air-conditioning) • increase in wildfires can damage infrastructure
		Winter cold/ice	• ice on trains and catenary • damage on infrastructure due to low temperatures
		Extreme precipitation	• damage on infrastructure due to flooding and/or landslides • scour to structures • destabilisation of embankment
		Extreme storms	• damage on infrastructure such as signals, power cables, etc. (e.g. due to falling trees, etc.)
		In general:	• reduced safety • increased cost for reparation and maintenance • disruption of 'just in time' delivery of goods and passengers
	Roads (including bridges, tunnels, etc.)	Summer heat	• pavement deterioration and subsidence • melting tarmac • reduced life of asphalt road surfaces (e.g. surface cracks) • increase in wildfires can damage infrastructure • expansion/buckling of bridges
		Extreme precipitation/ floods	• damage on infrastructure (e.g. pavements, road washout) • road submersion • scour to structures • underpass flooding • overstrained drainage systems • risk of landslides • instability of embankments
		Extreme storm events	• damage on infrastructure • roadside trees/vegetation can block roads
		In general:	• speed reduction • road closure or road safety hazards • disruption of 'just in time' delivery of goods • welfare losses • higher reparation and maintenance costs

	Coastal roads	Sea-level rise	• damaged infrastructure due to flooding • coastal erosion • road closure
		Extreme storm events	
	Mountain roads	Permafrost degradation	• decrease of stability • rockfalls • landslides • road closure
Air Transportation	Airports	Summer heat	• greater need for ground cooling • degradation of runways and runway foundations • higher-density altitudes causing reduced engine combustion efficiency • decreased airport lift and increased runway lengths
		Heavy precipitation events	• flood damage to runways and other infrastructure • water run-off exceeds capacity of drainage system
		Sea-level rise	• flooding of runways, outbuildings and access roads
		In general:	• interruption and disruption to services supplied and to ground access, delays and passenger loss of confidence • periodic airport closures • higher maintenance costs
Marine / Shipping	Inland shipping	High river flow (e.g. extreme rain, snow melt)	• problems for the passage of bridges • speed limitations because of dike instability • some restrictions on the height of vessels
		Low river flow (e.g. drought)	• strong restrictions on the loading capacity • navigation problems, speed reduction
		Change in ice cover	In general, shorter periods of ice cover can be expected. Nevertheless, warm and early winters, followed by a rapid decrease in air temperature, may result in thicker ice cover formation and lead to ice jams and damage to infrastructure
		In general:	• disruption of 'just in time' delivery of goods • stopping of inland shipping • welfare losses
	Maritime transport	Sea-level rise	• navigability could be affected by changes in sedimentation rates and location of shoals • more frequent closure
		Change in sea conditions	• more severe storms and extreme waves might affect ships
		Less days below freezing	• reduce problems with ice accumulation on vessels, decks, riggings and docks • occurrence of dangerous ice fog

		Reduced sea ice	• improved access • longer shipping seasons • new shipping routes
	Ports	Extreme storm events	• devastation of infrastructure • interruptions and bottlenecks in the flow of products through ports
		Sea-level rise	
		Floods/landslide	
		In general:	• disruption of 'just in time' delivery of goods • welfare losses • increased cost for reparation and maintenance

The effects of malfunction, disturbance and broken links may stretch far beyond the originally affected area. The transport system is of transboundary character and highly interconnected inside its modes and across modes; hence, disturbances in one part of the network might have a domino effect in other parts too. As such, effects usually extend beyond the transport system, by hindering the ability to deliver reliable services and jeopardizing free movement of people and goods. Depending on the specific case, these interdependencies can result to losses many times higher than direct costs to the transport sector itself.

Adapting the transport system could require substantial infrastructure investments, so mainstreaming of adaptation in infrastructure planning is vital. A study published by the European Joint Research Centre (European Commission, Joint Research Centre, 2016), concerning future climate change impacts, presents a comprehensive quantitative assessment of the impacts of current and future climate extremes on critical infrastructures in Europe. The dynamics of climate hazards were analyzed throughout the 21st century using physical models and adaptation tools (2015, 2020, 2050, 2080 predictions). Regarding the implications of climate change for CIs in Europe, results indicate that damages from climate extremes could triple by the 2020s and amount to more than 10 times the present damages of €3.4 billion/year by the end of the century (European Commission, Joint Research Centre, 2016) as shown in Figure 3.1, economic losses are highest for the industry, transport and energy sectors.

According to this study, heat waves will largely dominate future damages at the transport sector, mainly by impacting roads and rails. These modes of transport will also suffer losses from and coastal flooding, which will drastically increase over time. Inland waterway transport will be impacted by droughts, while sea level rise and increased storm surges will lead to strong increases in damages to ports in the coming century. These projections suggest the need for an adaptation approach with a long-term and systemic perspective, which requires high priority from governance and worldwide adaptation initiatives.

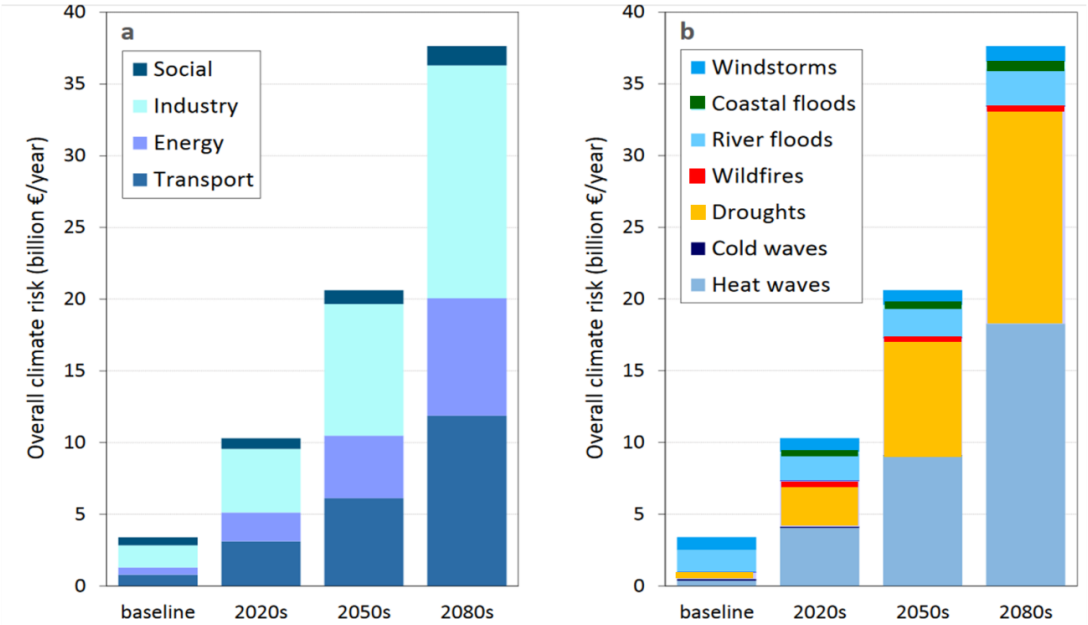


Figure 3.1. Evolution of climate hazard damages to critical infrastructures in the EU (source: EU-JRC)

3.1.4. General approaches to climate change adaptation

In this subsection, adaptation principles are discussed, focusing on adaptation assessment, evaluation and classification of adaptation options, based on conducted literature research. Worldwide adaptation strategies are exhibited and focus on transport sector. Adaptation consists of actions responding to current and future climate change impacts and vulnerabilities (as well as to climate variability that occurs in the absence of climate change) within the context of ongoing and expected societal change. It means not only protecting against negative impacts of climate change, but also building resilience and taking advantage of any benefits it may bring.

Adaptation and disaster risk reduction share the same ultimate goal to reduce vulnerability to hazardous events (Forzieri et al., 2018). There are synergies to be exploited in closely coordinating disaster risk reduction and adaptation policies. Risk reduction and prevention in the short and medium-term will primarily address socio-economic developments and climate variability to reduce the impacts of natural and technical hazards, while adaptation aims at developing longer-term planning to address climate change impacts (European Environment Agency, 2014). Preparedness refers to the readiness of human and natural systems to undergo gradual change through flexibility in practices and governance, thus it is a key common element of adaptation and disaster risk reduction actions.

According to (Willows et al., 2003) adaptation responses and decisions can be categorized as measures and strategies that contribute to: (i) Building adaptive capacity by creating the information (i.e. research, data collecting and monitoring, awareness raising), supportive social structures (i.e. organizational development, working in partnership, institutions), and supportive governance (i.e. regulations, legislations, and guidance) needed as a foundation for delivering adaptation actions; (ii) Identifying adaptation actions that help to reduce vulnerability to climate risks, or to exploit opportunities. These two categories reflect the range of adaptation measures and strategies from which a good adaptation assessment can be developed.

3.1.5. Adaptation assessment

Adaptation assessment is the practice of identifying options to adapt to climate change and evaluating them in terms of criteria such as availability, benefits, costs, effectiveness, efficiency, and feasibility. Approaches used in decision-making to assess potential adaptation options can be broadly categorized according to two main steps of analysis: (a) the identification of adaptation measures and (b) the evaluation of adaptation options.

a) Identification of adaptation measures distinguishes four targets for strategies that contribute to building adaptive capacity and delivering adaptation actions:

1. *Accepting the impacts and bearing losses*, which reflects a conscious decision that no action is needed to address foreseeable climate hazards, either because the hazards themselves represent a small or acceptable risk with existing measures, or because the exposure unit is not judged worth sustaining and alternatives will need to be considered.

2. *Preventing effects or reducing risks*, which involves the introduction of new measures designed to reduce exposure of assets to new or heightened risks. Such an approach pre-supposes that the exposure unit is of sufficient value to warrant some degree of protection.

3. *Offsetting losses* by spreading or sharing risks or losses, which implies using insurance or establishing partnerships or co-operatives to reduce financial or social losses and minimize exposure to risks.

4. *Exploiting positive opportunities*, which might involve the introduction of new activities or behavior to take advantage of reduced climate risks or a move to a new location to exploit favorable climate shifts.

There are limits to adaptation in terms of the time when action can be implemented in, and in terms of geographical space in which the action will be helpful. There are

also inherent limits and uncertainty to the extent to which implemented measures will enhance adaptive capacity and fully protect regions, economic sectors, and communities. Authorities and decision makers face the challenge of deciding which protection level to implement, given their current and expected knowledge of climate change impacts and related damage costs.

b) Evaluation of adaptation options: Once a set of adaptation options have been identified, the next logical step of analysis is to evaluate these options as a basis for guiding decisions on the eventual selection and implementation of adaptation measures. The World Resources Institute and World Bank guidance documents list a number of evaluation criteria for assessing the suitability of an adaptation option for contributing to a stated objective (Transportation Research Board, 2009): (i) Cost analysis, including total costs and cost effectiveness; (ii) Environmental implications; (iii) Secondary or cross-sectoral impacts, externalities or co-benefits; (iv) Social implications, including implications for sensitive and marginalized groups; (v) Short, medium, and long-term efficacy; (vi) Effectiveness at reducing impacts of extreme events; (vii) Effectiveness under different scenarios of future climate; (viii) Limiting factors for implementation or sustainability (e,g., resource constraints); (ix) Consultation with a broad set of stakeholders; (x) Provision for reviewing options based on changing assessments of risk; (xi)Transparency in the process and justification of options selection.

3.1.6. Adaptation Options Classification

According to EEA classification (European Environment Agency, 2014), adaptation measures and actions can be grouped under three broad categories:

- *'Grey'* actions are technological and engineering solutions for infrastructure, corresponding to physical interventions or construction measures and using engineering services to make infrastructures more capable of withstanding extreme events. Examples include building or strengthening of coastal and river flood defenses, dykes and beach 'nourishment'.
- *'Green'* actions are ecosystem-based approaches that use the multiple services of nature. They use the functions and services provided by the ecosystems to achieve a more costs effective and sometimes more feasible adaptation solution than relying solely on grey infrastructures alternatives. When green adaptation actions are integrated into a spatially organized plan, they are called 'green infrastructure'.
- *'Soft'* actions are managerial, legal and policy approaches that alter human behavior and styles of governance. They correspond to design new policies and procedures, land-use controls, information dissemination, and economic

incentives to reduce or prevent disaster vulnerability. Examples include: planning and passing legislation; early warning systems for heat wave risks; natural hazards monitoring; and public information campaigns.

'Green' and 'soft' actions specifically aim at decreasing the sensitivity and increasing the adaptive capacity of human and natural systems to build resilience. These actions are often less resource-intensive and provide multiple benefits. 'Grey' actions and innovative technological solutions typically need more funding, and require more research, experience, and training to be implemented.

Adaptation has an extremely important role in reducing economic costs of Climate Change. While adaptation has a cost, it significantly reduces the costs of inaction and in many cases has benefits that dramatically outweigh costs (European Environment Agency, 2014). Since it is important to enable cost-effective and proportionate adaptation by implementing the appropriate options, there are several viable options that can achieve effective adaptation, minimizing associated risks and uncertainties.

Addressing adaptation risk and uncertainty, UK Climate Impacts Program (UKCIP) (Willows et al., 2003) categorizes options as no-regrets, low regrets, win-win and flexible/adaptive management options that target incremental adaptation. On the opposite side, no effective adaptation actions are characterized as maladaptation, which has to be avoided.

- *No-Regrets Adaptation Options* are adaptive measures that are worthwhile, whatever the extent of future climate change. These types include justified and cost-effective measures under current climate conditions and are further justified when their introduction is consistent with addressing risks associated with projected climate changes.

- *Low-regrets options* are adaptive measures for which the associated costs are relatively low and for which the benefits, although primarily realized under projected future climate change, may be relatively large.

- *Win-Win options* are adaptation measures that have the desired result in terms of minimizing the climate risks or exploiting potential opportunities but also contribute to mitigation or other social and environmental objectives. These types of measures include those that are introduced primarily for reasons other than addressing climate risks, but also deliver the desired adaptation benefits.

- *Flexible or adaptive management options* involve incremental adaptation options, rather than undertaking large-scale adaptation. Measures are introduced through an assessment of what makes sense today, but are designed to allow for incremental change, including changing tack, as knowledge, experience and technology evolve.

- *Maladaptation* options occurs when specific adaptation actions either: (1) do not increase resilience and adaptive capacity or do not reduce vulnerability; (2) are not sustainable from an environmental, economic or social perspective (e.g. over-exploitation of water resources); or (3) conflict with other long-term policy objectives. Maladaptation can be prevented by considering both the climatic and the socio-economic elements that constitute vulnerability to climate change.

Adaptation Initiatives Worldwide

In USA, the Dept. of Homeland Security has developed a Climate Change Adaptation Roadmap and Climate Action Plan, which aligns to the President's Climate Action Plan, preparing the USA for the Impacts of Climate Change. As of 2016, 15 states had completed climate adaptation plans as shown in Figure 3.2. In addition, several states have created sector-specific plans that consider long-term climate change.

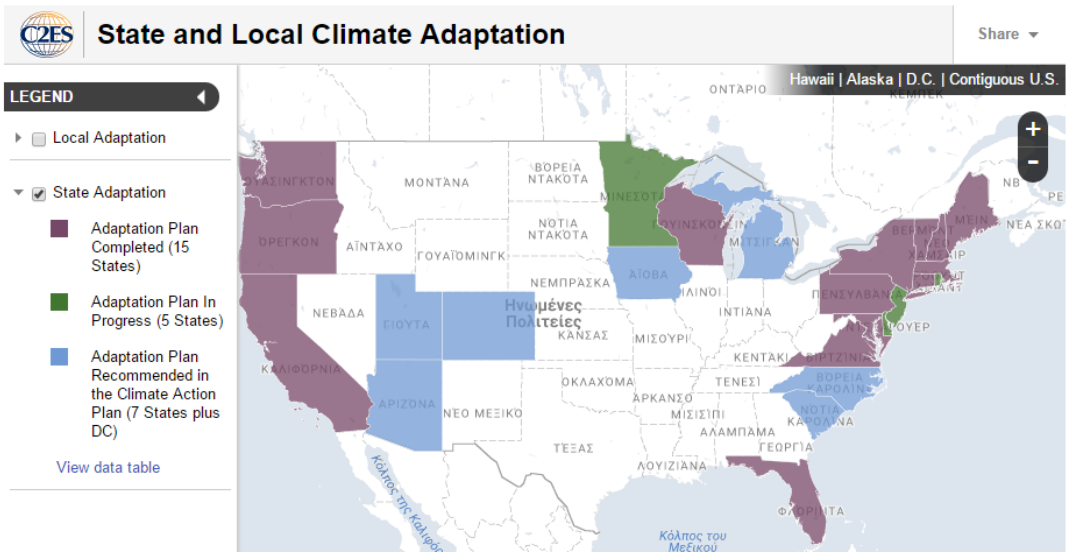


Figure 3.2. USA State Climate Adaptation Plans (C2ES 2016, www.c2es.org)

European strategy (European Environment Agency, 2014) on adaptation to climate change sets out a framework and mechanisms for preparedness for current and future impacts; encouraging and supporting action by EU Member States on adaptation and creating a basis for better informed decision-making on adaptation in the years to come. The majority of EU Member States have adopted national adaptation plans and strategies, outlining their implemented or planned actions to facilitate among other sectors the adaptation of transport to climate change as presented in Figure 3.3.

In Australia, the government has developed the ACT Climate Change Adaptation Strategy (Australian Capital Territory & Environment and Planning Directorate, 2016) to guide efforts in adapting to climate change in a coordinated manner. This strategy identifies the key adaptation policy to help community become more resilient

to the projected impacts by communicating the risks and impacts of climate change and incorporating climate change risk considerations and adaptation actions in ACT Government policies.

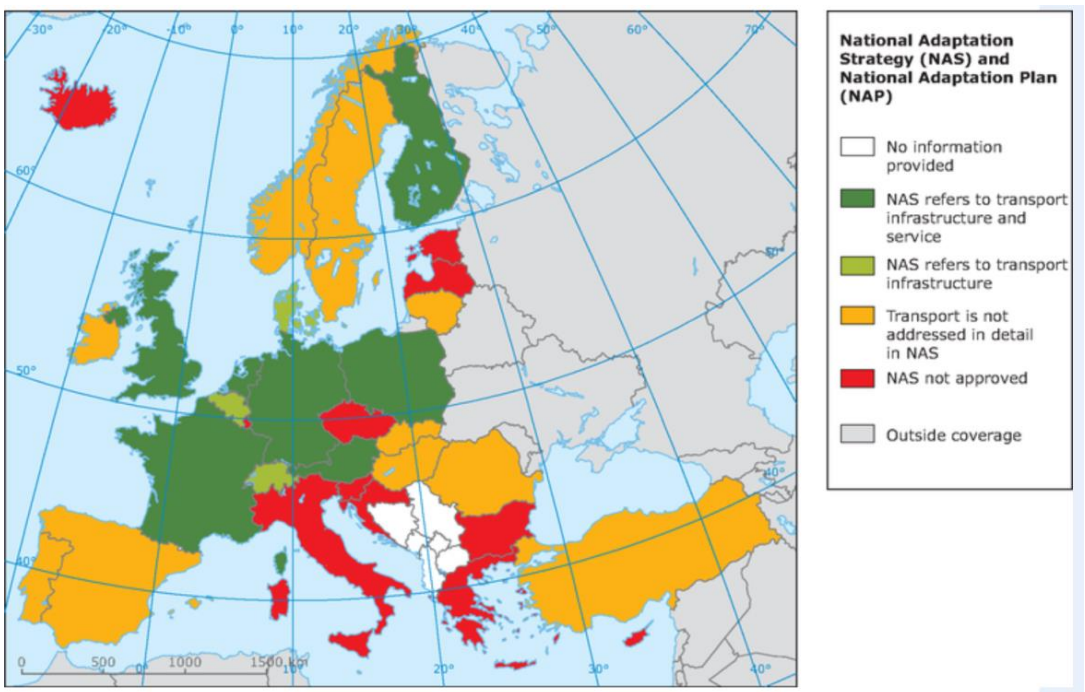


Figure 3.3: EU State Climate Adaptation Plans (source: EEA, 2014)

3.1.7. Adaptation of transport to climate change

In the past, transport has already dealt with extreme events causing interruptions, whether stemming from natural hazards or human impacts like accidents and power cuts, thus it developed strategies to maintain resilience. Therefore, adaptation of transport systems to climate change requires a wide perspective able to embed adaptation into broader transition strategies, rather than leaving it to be implemented by single stakeholders like infrastructure managers, operators or regulating authorities in the transport sector.

The transport sector is specifically addressed with some detail in most national strategies and plans studied in this research (including countries such as Austria, Australia, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Poland, Slovakia, Spain, Switzerland, United Kingdom and USA). Most of the national adaptation strategies and plans focus on transport infrastructure issues, and aspects of transport services, such as development of alternative routes and means of transport,

traffic management, review of technical conditions for vehicles and their operations, or support to operators in the development of their adaptation assessment and actions.

Also, literature research (Wall et al., 2013) has shown that, in particular, bigger transport stakeholders, like rail companies (Palin et al., 2013), airports and port authorities, air traffic control operators (EUROCONTROL, 2013) and others (J. D. Müller & Deutsche Post AG, 2012; DHL, 2013), are aware of climate change impacts and the need to adapt, and have started to take action. The prospects of high re-construction costs, lengthy recovery processes and severe disruptions in the transport system have encouraged infrastructure managers to undertake a comprehensive assessment of the vulnerability of some networks.

In this subsection, we present common and established adaptation measures for transport, using existing adaptation plans and relevant publications from national plans, US general publications and EU directives and all publicly available national adaptation action plans[4]. Presented measures are categorized and analyzed according to the classification systems already discussed. This collection of measures can stimulate further research and discussions among the many different stakeholders concerned with transport adaptation.

This subsection is dealing with different aspects of transport adaptation, which are: (3.1.7.1) Effective governance; (3.1.7.2) Infrastructure planning; (3.1.7.3) Redundancies within and between transport modes; (3.1.7.4.) Operational Contingency; (3.1.7.5.) Early warning systems; (3.1.7.6.) Building Adaptive Ca-pacity; and (3.1.7.7.) Collaboration. For each subsection, adaptation options are presented, followed by a summary table, which resumes our research and classification of adaptation options.

3.1.7.1. Developing effective transport governance for adaptation

The role of governments is mostly enabling adaptation action at local and regional levels by creating an appropriate framework. This includes effective institutions, knowledge, supportive policy, legal framework, and funding. As such, transport should also be a part of national adaptation strategies and action plans.

Since stakeholders, acting at local, regional or company level, are rather the ones who implement measures like climate proofing infrastructure or operations, it is vital for ruling authorities to create synergies and engage all stakeholders within the transport sector. Moreover, enhancing legislation with national standards for earth and public works and requiring climate risk assessment as prerequisite for the design of new plants, can ensure infrastructure integrity and future protection. Funding for new or

[4] Available on www.climate-adapt.eea.europa.eu & www.c2es.org

existing infrastructure reinforcement should incorporate an adaptation assessment to ensure infrastructure sustainability. Effective Governance measures are presented in Table 3.2, categorized per adaptation option type classification.

Table 3.2: Effective Governance measures proposed in adaptation plans

Effective Governance Measures categorized by :	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Strategic planning of Sustainable transport development		X		X			
Create an Adaptation framework so as to engage stakeholders within the transport sector		X				X	
Incorporate Adaptation requirements into Legislation & Regulatory Norms		X			X		
Enhance Standards and National/ Regional Requirements		X			X		
Develop National Adaptation Strategy and Action Plan		X					X
Require as prerequisite climate risk assessment and Environmental Assessment for the design of new plants to ensure integrity		X				X	
Ensure Funding for new infrastructure or existing infrastructure reinforcement			X				X
Coordinate Infrastructure Future Planning		X				X	

As we can notice from Table 3.2, most of measures proposed in effective transport governance for adaptation are ‘soft’ type, expect from funding issues and this is not surprising, since the role of governments is mostly managerial and policy setting, by creating the appropriate framework to enable adaptation action at local and regional

level. From the aspect of risk and uncertainty we can notice a variety of options proposed from cost effective to proportionate adaptive management.

3.1.7.2. Transport Infrastructure planning

The smooth and effective operation of the transport system relies heavily on hard and extensive infrastructures, which are intended to last long term, in some cases beyond 100 years. Investments are usually costly and with long return rates. An anticipatory approach is necessary for planning new infrastructure, renovation improvements or maintenance. Considering future climate trends now, helps in keeping the costs for adaptation bearable and avoiding future unsustainable development path of the transport system.

Climate change adaptation should be included as a criterion to be considered at all the relevant levels, from network planning to project assessment, by providing concrete methodological guidance on how this integration can be effectively implemented (European Environment Agency, 2014). These are so-called 'soft measures' and require relatively low investments. However, further mainstreaming of adaptation into transport infrastructure investments can have substantial implications for the resilience of infrastructure and the costs of adaptation in a long term perspective. In general, it can be expected that adaptation integrated into the design of new and upgraded infrastructure comes at lower cost than adding it at a later stage (McLean et al., 2011b). Infrastructure Design and Planning Measures are presented in Table 3, categorized per Adaptation option type.

As presented in Table 3.3, there is a balanced approach between grey and soft measures that can support transport infrastructure design and planning. On the other side, there is only one green measure proposed, which can be justified from the nature of transport infrastructures and networks, since there is always an environmental impact occurring from transport projects development.

From the aspect of risk and uncertainty we can notice a variety of options proposed, the majority of options are measures that minimize climate risk but also have other

social and environmental benefits (win-win) and measures with incremental actions for flexible adaptation (Adaptive Management).

Table 3.3: Infrastructure Design and Planning measures proposed in adaptation plans

Infrastructure Design and Planning Measures	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Revision of obsolete Design and Infrastructure Standards		x		x			
Create New Standards & Recommended Practices for Resilient Infrastructures		x				x	
Improve site/ earthwork design to combat landslide, subsidence, heave or wind damage.	x					x	
Civil engineering regular checks of infrastructure foundations and measures to protect erosion			x				x
Review piping installation to identify which parts of plant equipment may be vulnerable.			x		x		
Strengthen drainage elements and design and improve storm drain capacity			x				x
Proactively inspecting and maintaining guidance for infrastructure assets		x				x	
Use design limits to explore whether measures for heating, cooling, insulating or drying are required.			x				x
Provide specific information/ guidance for staff on working in extreme temperatures or windy weather.		x				x	

3.1.7.3. Redundancies within and between transport modes

Designing, building, and using redundant infrastructure, like alternative rail links or roads can support transport operation resilience. Build and retain ready to use back-up equipment and vehicles, in case of emergency, and adding backup power/generator capacity in critical facilities are also suggested as redundancy measures. Usually, such a strategy involves extra cost to establish and maintain this redundant infrastructure, which, under normal conditions, might not be necessary. It

has therefore probably been a less preferred option, but it is expected to gain importance, in the face of more extreme weather events due to climate change in the future.

Multimodality offers redundancy potential at different levels. If different modes are available, the user can choose which one best serves his/her transport needs and might switch from one mode to another. Smart and flexible ticketing, which allow passengers to switch operators and modes in the event of disruption, could facilitate this process. Building and retaining ready to use back-up equipment and vehicles in case of emergency and adding backup power/generator capacity in critical facilities can also supports adaptation efficiency. Redundancy Planning Measures are presented and classified in Table 3.4.

Table 3.4: Redundancy planning measures proposed in adaptation plans

Redundancy Planning	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Design and build redundant infrastructure in vulnerable to Climate change or extreme weather areas			x				x
Design and construct resilient vehicles for all transport modes			x			x	
Explore multi-modality opportunities (like multi modal stations, smart and flexible ticketing options, etc.)			x			x	
Build and retain ready to use back-up equipment and vehicles in case of emergency			x				x
Adding backup power/generator capacity in critical facilities			x				x

As listed in Table 3.4 redundancy measures are ‘grey’, since they require more funding and additional resources to establish and maintain this redundant infrastructure. From the aspect of risk and uncertainty options can be categorized either win-win, since redundancy options also offer social benefits for transport users, or measures that offer flexibility and increase adaptive management.

3.1.7.4. Operational Contingency

Transport has traditionally developed approaches to cope with the impacts of extreme weather events, with solutions which might also be valuable options for adapting to climate change. Preparing for a risk situation can be done with contingency planning, business continuity and disaster recovery plans for extreme weather events. Emergency reporting and emergency equipment preparedness, surveillance and maintenance plans can support integrity of critical facilities.

It is also important to locate records, materials and inventory away from potential vulnerable areas, or even relocate critical assets prior to damage or impact. Last but not least, insurance schemes can support key infrastructure funding and restoration in vulnerable areas. Operational Contingency Measures are presented and classified in Table 3.5.

Table 3.5: Operational Contingency measures proposed in adaptation plans

Operating Contigency	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Establish Preparedness and Prevention Plan		x		x			
Business Continuity & Disaster Recovery Plan		x		x			
Emergency Reporting and emergency equipment preparedness			x		x		
Locate records, materials and inventory away from potential vulnerable areas.		x			x		
Provide staff with more/ better PPE e.g. air-flow suits/ helmets for hot weather, heavy snow or storm etc.			x			x	
Relocating critical assets prior to damage or impact			x				x
Surveillance and Maintenance Plans to safeguard integrity		x		x			
Insurance schemes for key infrastructure in vulnerable areas			x				x

From Table 3.5, it occurs that operational contingency measures can be either grey or soft measures, in order support integrity of infrastructure and transport continuity. Green measures are missing, since it is hard to find green solutions to secure transport

contingency. From the aspect of risk and uncertainty we can notice a variety of options proposed from cost effective ones to proportionate adaptive measures.

3.1.7.5. Early warning systems

Early warning systems allow transport managers to prepare for extreme weather events, whether they are induced by climate change or current climate variability. For example, EUROCONTROL Network Manager (EUROCONTROL, 2013) has developed a natural hazards and weather resilience tool, which provides information about the potential vulnerability to such events of airports and en route sectors in Europe. Warning systems can get valuable support through the application of information and communications technology (ICT) to transport management. This is the case of sensors and devices, which provide real time information on traffic conditions on the network, including the distribution of temperature, vehicle speeds, presence of obstacles, deformations and other surface characteristics (Grant-Muller & Usher, 2014). With the support of ICT, this information can be accessed in real time by infrastructure managers, service operators or users.

Table 3.6: Early Warning Systems proposed in adaptation plans

Early Warning Systems	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Fixed warning systems with GPS technology, Meteorological instruments and other sensors to detect extreme weather events			X			X	
Vehicle sensors and devices transmitting real time information			X			X	
User devices which can get or transmit real time information		X		X			
Weather warnings & incident warnings network			X			X	
Warnings and awareness raising for staff on the increased risks during inclement weather.		X				X	

Furthermore, vehicles and users could increasingly serve as data collectors. This would allow infrastructure managers and transport operators to gain unprecedented real-time knowledge about the parts of the transport system they are interested in. Handling these enormous flows of information, requires the deployment of communication technologies linking vehicles to other vehicles and to the infrastructure (Grant-Muller & Usher, 2014). Whilst by their vehicles, transport operators and users can receive the information they need on infrastructure conditions, infrastructure managers can get a more detailed description of the traffic situation from users and communicate to them accordingly. Such exchange of data greatly facilitates traffic management. It also enables passengers to adapt their plans or find alternative transport options. Such measures can also improve the quality of services and have positive co-benefits for all stakeholders (users and operators). Early warning systems are presented in Table 3.6, categorized per Adaptation option type. As we can notice from this table, early warning systems are grey and soft measures, which require technological innovation and engineering support. However, they are win-win measures since they offer many other social benefits to users and travelers.

3.1.7.6. Building Adaptive Capacity

Global Initiatives, Transnational or European level and national adaptation platforms are making efforts in collecting relevant information for all stages of the policy process and making it more easily accessible. For example, the European Climate Adaptation Platform (European Climate Adaptation Platform, 2016) supports Europe in adapting to climate change, by helping users to access and share data and information on expected climate change in Europe, current and future vulnerability of regions and sectors, national and transnational adaptation strategies and actions, adaptation case studies and tools that support adaptation planning.

Information collected on past weather events and their impacts can be a valuable starting point for assessing vulnerabilities and developing strategies to adapt to climate change. Knowledge-sharing on adaptation best practices and benchmarking implementation case studies can create new opportunities for newcomers. Also providing awareness raising communication, education and training on climate change impacts and vulnerabilities could also improve adaptation performance. Building Adaptive Capacity measures are presented and classified in Table 3.7, where we can notice that soft measures, are increasing transport resilience to climate change and are most of the times worthwhile to develop.

Table 3.7: Building Adaptive Capacity measures proposed in adaptation plans

Building Adaptive Capacity	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Create a public adaptation Platform		x		x			
Information Sharing on Adaptation Best Practices		x		x			
Benchmark of best implementation of adaptation measures		x		x			
Documenting and sharing institutional knowledge		x		x			
Build a structure informal dataset to better understand territorial and sectoral vulnerabilities to climate change impacts		x		x			
Provide awareness raising communication, education and training on climate change impacts and vulnerabilities		x				x	

However, our research revealed that the information provided on public informative platforms is of a general nature and specific information on transport is scarce. Transport information on these national platforms could be expanded by adding systematic data collection on transport disruption events at the national level. At this stage, significant problems remain regarding availability of data on impacts of hazards on transport systems, because some stakeholders consider this information as confidential, as it could be used to derive legal responsibilities for service disruptions. Obtaining data on impacts, specifically on transport, available in formats required to cross-check with weather information and with data from other stakeholders is quite important for adaptation planning. Finally, awareness raising communication, education and training on climate change impacts is key success factor for adaptive capacity of stakeholders.

3.1.7.7. Comprehensive collaboration

The collaboration with climate experts can make transport stakeholders aware of the fact that climate-related topics cannot be addressed through traditional, unrealistically deterministic concepts, and that alternative approaches to risk principles would have to be explored. Through closer interaction, transport experts should be able to define

their needs for climate forecasts in more scientific terms, and meteorological experts could better understand transport experts' needs and highlight innovative developments in their modelling practices that could provide useful answers. Through cooperation with experts in other fields, transport stakeholders can increase their flexibility in management and decision-making, thus potentially finding innovative solutions. Collaboration options are presented and classified in Table 3.8.

Table 8 clearly demonstrates that collaboration measures are soft and win-win measures, since cooperation among experts with different backgrounds and expertise have been proved a fruitful and prosperous way to further mainstream adaptation efficiency and transport resilience.

Table 3.8: Collaboration measures proposed in adaptation plans

Collaboration	Measure Type			Risk and Uncertainity			
Adaptation Option Description	**Green**	**Soft**	**Grey**	**No regrets**	**Low regrets**	**Win-win**	**Adaptive Manag.**
Communicating plans and information with the public and stakeholders		x				x	
Cooperation with stakeholders within transport sector to expand knowledge sharing and best practices		x				x	
Interaction of transport experts with other scientists to expand research on adaptation issues		x				x	
Cooperation with experts from other fields to increase knowledge base on climate, science and adaptation		x				x	

3.1.8. Summary of research work

Transport systems are complex. They play a fundamental role in the economy and society, while they are characterized by the long lifespan and high costs of their infrastructure. These characteristics suggest the need for an adaptation approach with a long-term and systemic perspective, thus also preventing unsustainable development paths and maladaptation.

Several states worldwide have started to put into place Adaptation Strategies and Action Plans with a variety of measures to promote the implementation of adaptation measures in all critical sectors, including transportation. These measures include the

provision of information, capacity building, review of technical standards and use of new ICT opportunities. The engagement of all the main stakeholders in the transport sector is of key importance from the perspective of both equity and efficiency, so regulating authorities, policymakers and researchers should make an extra effort to engage stakeholders in their research and information-dissemination activities.

The majority of adaptation measures presented in this survey can be categorized to soft type options (60%), while grey options are also quite popular (38%) in the existing adaptation plans. There is a lack of green measures proposed, which is justified by transport sector infrastructure nature and environmental impact. In general, transport sector low-regret and win-win measures are typically the measures that increase the resilience of transport systems, while providing additional, advantages in terms of smooth operations, quality of services and efficiency.

Sound design and maintenance practices for transport infrastructure, integration of transport systems, revision of obsolete design standards and information sharing are some of the options described. Tools and measures developed to manage risks and disaster from natural hazards, including early warning systems and contingency plans, can be very useful for climate change adaptation too. Most adaptation action focuses on climate-proofing transport infrastructures. Integrating adaptation requirements into the design of new and upgraded infrastructure comes at lower cost than adding them at a later stage. Another way to ensure transport flexibility is through providing functionally redundant option, which offers a higher capacity and enables flexibility in the event of a disaster or other interruption.

It is important that adaptation measures taken in the transport sector are properly monitored and analyzed. This will enable stakeholders to improve their effectiveness and efficiency of future policy. Finally, cooperation between stakeholders inside and outside the transport sector can help to make use of the knowledge gained in other sectors and to find tailored, innovative, and effective solutions for transport adaptation.

3.2. Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning

3.2.1. Introduction [5]

Climate change is an upcoming and unavoidable challenge that all critical infrastructures including transport sector will have to face. Although transport sector and its network substructures are typically designed to withstand weather-related stressors, shifts in climate patterns will greatly increase potential risks. The area of climate adaptation planning is still relatively new, however a variety of processes and methodologies for assessing and reducing the vulnerability to climate change are currently being developed. These processes require and benefit from the use of geospatial analyses, software tools and web portals. In this research, we have focused on climate-related adaptation planning. We provide detailed classification of a set of tools that can facilitate adaptation assessment and risk planning. Our goal is to present a multi-faceted taxonomy and analysis of available Climate Change Adaptation tools which can support transport sector for risk management policies.

Recent modeling studies indicate that climate change is inevitable, thus our society will have to deal with over coming decades. According to IPCC (2014), global warming will have significant implications in climate, population and ecological health, economic development and social stability. Gradual global temperature increase, sea level rise and rainfall regimes along with the projected increase in frequency and intensity of extreme weather events will seriously challenge transportation substructures.

Transport is characterized as a Critical Infrastructure (CI) that greatly supports the smooth functioning of society's prosperity and economy's viability worldwide (Committee on Climate Change and U.S. Transportation, 2008). Most transport substructures being built today are expected to last for decades or even centuries. Integrating adaptation into the design of new and upgraded substructure can enhance stability and life span, while minimizing unplanned outages, failures and maintenance costs (European Environment Agency, 2014).

[5] *Related Publication:* C5. Lykou G., Iakovakis G., Chronis G., Gritzalis D., Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning, in the Procurements of the 12th International Conference on Critical Information Infrastructures Security (CRITIS-2017), Italy, September 2017.

In this research, we have focused on climate-related adaptation planning and we provide detailed information about a set of tools that facilitate adaptation assessment and risk management. We have examined available Climate Change Adaptation tools, with a goal to present a detailed classification and analysis for tools which can support transport sector. The term "tool" has been used to describe a wide variety of planning processes, policies, and analytical approaches, focusing on software and web-based applications that help incorporate data geophysical, environmental, or socioeconomic into the planning process.

The rest of this work is structured as follows: Climate adaptation and planning process is presented in subsection 3.2.2 Adaptation tools analysis takes place in subsection 3.2.3, followed by a sort description for each one. Our main contribution is presented in subsection 3.2.4, where adaptation tools are analyzed and classified in several ways: i) according to type categories and target audience; ii) according to Sectors affected and Climate Impacts; iii) Adaptation Planning Steps; iv) Software Tools Functionality & Mode of Use; and finally, v) Strengths and Weaknesses analysis. subsection 3.2.5 concludes analysis and classification results.

3.2.2. Climate Change Adaptation

Climate Change Adaptation is the evolutionary process of adjusting to new conditions, stresses and natural hazards that result from global warming effects. Thus, adaptation consists of actions responding to current and future climate impacts and vulnerabilities, not only protecting against negative impacts of climate change, but also building resilience and taking advantage of any benefits, it may bring (IPCC, 2014).

Either adaptation can be a spontaneous, autonomous process that takes place depending on existing capacity which is-called '*adaptive capacity*', or it can be well planned and designed. Planned adaptation can take many forms and be driven by decision makers and by policies on a macro scale as well as locally by stakeholders involved. Both autonomous and planned adaptation may require additional outside support in terms of knowledge, financing and technology. According to UKCIP (Willows et al., 2003), adaptation responses and decisions can be categorized as measures and strategies that contribute to: (i) Build adaptive capacity with knowledge spread (i.e. research, data collection and monitoring, awareness raising); (ii) Create supportive social structures (i.e. organizational development, working in partnership), and supportive governance (i.e. regulations, legislations, and guidance); (iii) Identify adaptation actions which help to reduce vulnerability to climate risks, or to exploit opportunities. These three categories reflect the range of adaptation strategies from which a good adaptation assessment can be developed.

Although the field of climate adaptation planning is still relatively new, a variety of processes and approaches are emerging in order to assess and reduce vulnerabilities of CIs to climate change. These processes and approaches require or benefit from the use of geospatial analyses and methodology tools. Basic steps of Adaptation planning processes, as depicted in Figure 3.4, involve:

1. Scope problems, stressors & planning area, information gathering and data inventorying, build working groups and gain stakeholder involvement.
2. Analyze information to elucidate patterns, relationships, and potential future outcomes, conduct vulnerability, impact and risk assessment and set priorities.
3. Establish vision and prioritize adaptation strategies, create action plan based on priorities and schedule implementation.
4. Implement and evaluate the effectiveness of plan, seek funding, adjust to unexpected or novel issues or stressors, revise strategies and priorities as needed.

Figure 3.4: Adaptation Planning Process

Conducting vulnerability and risk assessment is a key analytical step not only for CI protection, as already presented in (Stergiopoulos, Vasilellis, et al., 2016), but also for adaptation planning. Climate change vulnerability assessments identify assets, which may be impacted. In addition, potential sources of vulnerability, risk assessments also consider the likelihood and consequences of potential climate change impacts. Due to the predictive nature of vulnerability and risk assessments, there is a degree of uncertainty in the results (Rozum & Car, 2014). It is important to understand and account for this uncertainty when considering management actions of adaptation, so decision support tools and related software can incorporate data, analyze trends, project evolution, and minimize uncertainty issues.

Transport has already dealt with extreme events causing interruptions, stemming from natural hazards and developed strategies to maintain resilience. In previous work (Lykou et al., 2017) we have analyzed adaptation options for transport sector applied worldwide. Moreover US-TRB (Transportation Research Board, 2009) made the following recommendations: i) Transportation officials should inventory potentially vulnerable critical assets and incorporate climate change into long-range plans for new facilities ii) They should rely on probabilistic techniques to guide decisions and protect assets against the risk and consequences of failure; iii) Research programs should invest in the development of monitoring technologies that can measure stresses and provide warning of potential failures; and iv) Transportation stakeholders should develop procedures to identify and share best practices in managing assets.

All the above recommendations highlight the need for mainstreaming available adaptation tools into planning and critical infrastructure protection, as an essential component of a successful and comprehensive climate adaptation.

3.2.3. Climate adaptation Tools Analysis

The purpose of Adaptation Tools development is to provide the information necessary for stakeholders involved to select appropriate measures and manage risk of their projects. Since there has been an increased demand by governments and international agencies for practical guidance on methods for adaptation assessment, there is a huge development of analytical tools, which are available to support communities, decision makers and stakeholders (Rozum & Car, 2014). The emerging need for multi-model analysis has driven the creation of adaptation toolboxes, which describe the steps to be undertaken for adaptation and risk management process. They also provide access and information on available methods and models to use in such an analysis. The number of tools and guidelines pertaining to climate change has skyrocketed, driven mostly by international aid agencies and NGOs.

In this work, we have extensively searched for open literature adaptation tools, in order to create a useful pool of tools that can be used for CIs adaptation assessment. Although this selection of tools is not exhaustive, we have distinguished the ones who incorporate transport networks and related critical infrastructures. As a result, seventeen tools have been selected and analyzed in this subsection. They allow for a broad range of aspects to be evaluated and provide supportive information for adaptation planning projects in transport sector. These seventeen tools are shortly presented below:

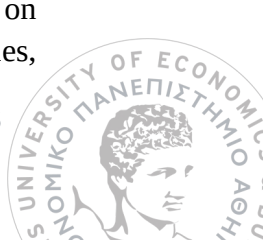
1. **Baltic Climate Toolkit**: is a methodology tool that guides the process of identifying vulnerabilities in the Baltic countries and properly mitigating them. Typical pattern is problem recognition, vulnerability assessment and the mitigation planning. (Abbreviation used in our analysis: BALTIC_CLIM_TOOL. Available via: https://toolkit.balticclimate.org/en/the-project)

2. **Blue Spot Model:** is an analysis methodology used to identify roadways vulnerable to flooding. The method is using Geographical Information System environment and has a complete methodology for vulnerability and risk assessment. (Abbreviation used in our analysis: BLU_SPOT_MODE. Available via: https://climate-adapt.eea.europa.eu/metadata/tools/the-blue-spot-model-a-key-tool-in-assessing-flood-risks-for-the-climate-adaptation-of-national-roads-and-highway-systems)

3. **Climate Vulnerability Monitor:** is a monitoring tool that assesses vulnerabilities and risks and contains detailed information for projected climate related economic damages, deaths, environmental disasters on 184 countries. Additionally, the tool has aggregated findings and recommendations to support decision makers. Data can be viewed either graphical (world map view) or through a monitor table. (Abbreviation used in analysis: CLI_VULN_MONITOR. Available via: http://daraint.org/climate-vulnerability-monitor/climate-vulnerability-monitor-2012/)

4. **Climate Guide: Climate Change Impacts in Finland:** is developed for Finland, where scenarios are built concerning the water resources, potential energy demand and natural ecosystems range from baseline years of 1961-1990 to 2099. Specific climate scenarios are being examined, where observed and projected data are provided for temperature and precipitation, based on different scenarios of carbon emissions. (Abbreviation used in our analysis: CLIMATE_GUIDE_FIN. Available via: http://ilmasto-opas.fi/en/datat)

5. **Climada**: is a software tool available on Github which uses numerical functions to model economic damages from natural hazards. It is based on scenario building and examines type of hazards, related variables,



implemented counter measures etc. It uses natural catastrophe modeling to calculate the impacts and using a simple GUI, it plots assets, damage and benefits on a map. (Abbreviation used is: CLIMADA. Available via: https://github.com/davidnbresch /climada/wiki)

6. **ECONADAPT- Toolbox**: is an EC FP7 research, whose purpose is to support adaptation planning, build the knowledge base on the economics of adaptation and provide practical information for decision makers. It is a library of knowledge related to economics of climate adaptation and methodologies used to assess the economic risks and adaptation strategies. (Abbreviation used is: ECONADAPT. Available via: http://econadapt.eu/)

7. **Ecocities Spatial Portal:** is an interactive platform that displays spatial data and information for understanding climate change vulnerabilities in Manchester area. It provides both decision support making and what-if scenarios. (Abbreviation used in our analysis: ECO_SPAT_PORTAL. Available via: www.ppgis.manchester.ac.uk/ecocities/)

8. **MACC**: is a tool developed by GIZ, which leads project managers through the five steps of the guidebook Adaptation. Each of these steps is monitored by the Excel MACC tool, which provides a spider chart that measures the overall progress of a project of climate adaptation. (Abbreviation used in analysis: MACC. Available via: http://climate-adapt.eea.europa.eu/metadata/tools/monitoring-adaptation-to-climate-change-macc)

9. **ND-GAIN** (Notre Dame Global Adaptation Index) follows a data-driven approach to show which countries are best prepared to deal with global changes. It informs strategic and operational decisions using data since 1995, to create a rank of 181 countries, measuring vulnerability and readiness. The second part of the tool is a matrix that highlights the relative position of the countries' readiness for adaptation. (Abbreviation used in our analysis: ND_GAIN. Available via: http://index.gain.org/)

10. **MOWE-IT:** project identifies best practices and methodologies to assist transport operators and authorities mitigating the impact of natural disasters and extreme weather phenomena on transport system performance. It is a knowledge database-repository and visualization tool, which includes visualization of climatic scenarios, comparison with various cities climatic scenarios and impact on passenger flows. (Abbreviation used in our analysis: MOWE_IT. Available via: http://www.mowe-it.eu/)

11. **Stocktaking for National Adaptation**: is a tool, which provides test questions for assessing the country's capacity to perform adaptation. It works as a decision support tool. (Abbreviation used in our analysis: SNAP. Available via: http://www.adaptationcommunity.net/knowledge/mainstreaming/ tools/ snap/)

12. **Sea Level Rise and Coastal Flooding Impacts Viewer**: This visualization tool creates simulations and graphics of current and potential future conditions to understand and envision consequences of different management decisions. It visualizes potential impacts of sea level rise. (Abbreviation: SLR_ CFI_VIEWER. Available via: https://coast.noaa.gov/digitalcoast/tools/slr.html

13. **HAZUS-MH (Hazards US Multi-Hazard)** is a risk-assessment methodology for analyzing potential losses from floods, hurricane winds, coastal surge and earthquakes. Loss estimates are used anywhere in USA through damage functions and fragility curves. It uses GIS software to map and hazard data, results of damage and economic loss estimates for buildings and infrastructure. Vehicle and traffic data for transportation sector are available. (Abbreviation used is: HAZUS-MH. Available via: https://www.fema.gov/hazus)

14. **NatureServe Vista** is a spatial decision support system for conducting cumulative effects assessment, mitigation planning, and conservation planning. It can help integrate conservation with land use, transportation, energy, and natural resources assessment. (Abbreviation used is: NATURE_VISTA. Available via: http://www.natureserve.org/ conservation-tools/ natureserve-vista)

15. **CommunityViz** is a decision support tool that integrates a variety of analytical models as well as visualization and mapping capabilities to support a variety of planning activities. The software visualizes and analyzes planning and design alternatives and their impacts. It supports scenario building, sketch planning and geodesign, 3-D visualization, suitability analysis, impact assessment, growth modeling etc. It also works as an integration framework connecting to other tools such as Hazus-MH and NatureServe Vista. (Abbreviation used in our analysis: COMMUN_VIZ. Available via: http://communityviz.city-explained.com/communityviz/)

16. **The Urban Adaptation Support Tool**: is a methodology-guide, which takes decision makers gradually through the adaptation process. It provides a quick access guide to data relevant to the process and serves as a decision-making support index. (Abbreviation used in our analysis: URBAN_ADAPT_TOOL. Available via: climate-adapt.eea.europa.eu/tools/urban-ast/)

17. **UKCIP Adaptation Wizard:** is a tool for adapting to climate change, by using a 5-step process that will help assessing vulnerability to current and future climate change. It identifies options for adapting to climate risks and helps developing and implement adaptation strategy. (Abbreviation used in our analysis: UKCIP_WIZARD. Available via: http://www.ukcip.org.uk/wizard/)

3.2.4. Classification of Adaptation Tools

In this subsection, the main contribution of our work is presented, where adaptation tools are analyzed and classified in several ways, aiming to facilitate stakeholders to understand which ones better fit to their adaption planning needs. In 4.1. tools are classified according to typology and target audience, in 4.2. classification is dealing with climate impacts and economy sectors affected, then in 4.3. tools are categorized according to adaptation planning steps. In subsection 4.4, software tools are further classified according to their functionality & mode of use. Finally, in 4.5 Strengths and Weaknesses are evaluated.

3.2.4.1. Classification according to Type of tool and Target Audience

The selected adaptation tools are classified, based on the following three broad categories:

i. *Informative Guidelines* which are tools that offer informational databases on climate change and adaptation planning, through open libraries and repositories, supporting research and knowledge spread.

ii. *Methodologies & Assessments* are those tools that describe climate adaptation though a sequence of steps, which should be followed in order to accomplish a specific task within a larger framework. Vulnerability and risk assessments are also included in this category, to evaluate threats and vulnerabilities.

iii. *Software Tools*: are those tools that offer a calculating platform to facilitate user perform a specific task, model a problem, and enhance his experience by visualizing provided information.

Each tool is designed to support different target audience and this information is presented in Table 3.9. Three main target groups are: i) Designers & Engineers (D); ii) Operators and Managers (O) and iii) Policy Makers (P).

Table 3.9: Tools Categories and target audience

No	Name	Tool Category			Target Group
		Informative Guidelines	Methodology Assessment	Software Tools	
1	BALTIC_CLIM_TOOL	x	x		P- D-O
2	BLU_SPOT_MODE		x		O
3	CLI_VULN_MONITOR			x	P-O
4	CLIMADA			x	D-O
5	CLIMATE_GUIDE_FIN			x	O
6	COMMUN_VIZ			x	P-O
7	ECO_SPAT_PORTAL			x	P
8	ECONADAPT	x	x		D-O
9	HAZUS-MH			x	D-O
10	MACC			x	O
11	MOWE_IT	x		x	P-O
12	NATURE_VISTA			x	P-D-O
13	ND_GAIN			x	P
14	SLR_CFI_VIEWER			x	P
15	SNAP		x		P-O
16	UKCIP_WIZARD			x	P-O
17	URBAN_ADAPT_TOOL	x	x		O

Where P = Policy Makers, D= Designers/Engineers/Developers, O= Operators & Managers

3.2.4.2. Classification of Adaptation Tools according to Sectors and Climate Impacts

In Table 3.10 examined tools have been classified based on geographic scope, affected economy sector and climate impacts. In terms of geographical coverage, there are tools that cover a single state or location, multiple states (e.g., counties belonging to the same continent as EU, USA etc.) and finally those who have a global geographic scope. Sectors affected may be urban areas and communities, agricultural activity, transport or energy sector and earth resources with water and other natural

assets. In terms of climate impacts, there are various weather-related stressors that may impact transport substructure.

Table 3.10: Tools Classification based on Geographic scope, Vulnerabities & Impacts

No	Tool Name	Geographic Scope	Vulnerable Sector					Climate Impacts				
			Urban	Transport	Agriculture	Energy	Water & Resources	Flood	Heat	Cold	Storms	Drought
1	BALTIC_CLIM_TOOL	MS	X	X	X	X	X	X	X			X
2	BLU_SPOT_MODE	G		X				X			X	
3	CL_VULN_MONITOR	G		X	X	X	X	X			X	X
4	CLIMADA	G	X	X		X	X	X		X	X	
5	CLIMAT_GUIDE_FIN	S		X	X	X	X	X	X	X	X	X
6	COMMUN_VIZ	MS	X	X	X	X	X	X	X	X	X	X
7	ECO_SPAT_PORTAL	MS	X	X		X	X	X	X			X
8	ECONADAPT	G	X	X	X	X	X	X	X	X	X	X
9	HAZUS-MH	MS	X	X			X	X			X	
10	MACC	G	X	X	X	X	X	X	X	X	X	X
11	MOWE_IT	MS		X				X	X	X	X	
12	NATURE_VISTA	G	X	X	X	X	X	X	X	X	X	X
13	ND_GAIN	G	X	X	X	X	X	X				X
14	SLR_CFI_VIEWER	MS	X	X			X	X				
15	SNAP	G	X	X	X	X	X	X	X	X	X	X
16	UKCIP_WIZARD	G	X	X	X			X	X	X	X	X
17	URBAN ADAPT TOOL	MS	X	X		X		X	X	X	X	X

Where G = Global Scope, MS= Multi State Area, S= State

We can distinguish that the majority of tools deal with all climate change impacts and all sectors approach. In addition, the most elaborated weather impact is flood. It is evident that multi sector combined with multi hazard approach tools are most

developed since they provide a holistic support for stakeholders to adaptation planning process.

3.2.4.3. Classification of Adaptation Tools according to Adaptation Planning Steps

Another key characteristic of tools is how they support their users to planning process. Different tools perform different functions and are useful at different steps in climate adaption planning, which are: (i) Information, Engagement and Scoping, (ii) Vulnerability Assessment, (iii) Scenario Building, (iv) Adaptation Planning, and (v) Implementation & Monitoring. A key element for selecting the proper tool for a task is to have a well-identified planning process, so for each tool, we have examined which step of adaptation planning serve and results are listed in Table 3.11.

Table 3.11: Tools Classification according to Adaptation Planning Steps

No	Tool Name	Climate Adaptation Steps				
		Information Engagement Scoping	Vulnarability Assesment	Scenario Building	Adaptation Planning	Implement & Monitor
1	BALTIC_CLIM_TOOL	X	X		X	
2	BLU_SPOT_MODE		X			
3	CLI_VULN_MONITOR	X	X			
4	CLIMADA		X	X	X	
5	CLIMATE_GUIDE_FIN	X	X	X		
6	COMMUN_VIZ	X	X	X	X	
7	ECO_SPAT_PORTAL	X	X	X		
8	ECONADAPT	X	X			
9	HAZUS-MH		X	X		
10	MACC				X	X
11	MOWE_IT	X		X		
12	NATURE_VISTA			X	X	
13	ND_GAIN	X	X			
14	SLR_CFI_VIEWER	X	X	X		
15	SNAP				X	X
16	UKCIP_WIZARD	X	X	X	X	X
17	URBAN_ADAPT_TOOL	X	X	X	X	X

Results showed that the tools which have all steps planning approach are rather limited. In our research, we have found only two tools able to cover all five steps. These tools are Urban Adaptation Support tool and UKCIP Adaptation Wizard.

3.2.4.4. Software tools classification

Software tools are further classified according to functionality, mode of use and modeling algorithms, as presented in Table 3.12. They are web-based or standalone applications, and they are further classified into three broad categories according to their functionality:

-Visualization Tools create simulations based on GIS and graphics of current and potential future conditions to help stakeholders understand and envision potential consequences of different management decisions. They are generally easy to use and do not require specialized software or hardware. Increasingly, they are available via Internet.

-Modeling Tools model current and potential future conditions of geophysical and socioeconomic processes. These are generally the most technically challenging tools to use and often require GIS software and appropriate hardware, topical expertise, and training. Models also generally require local data on the process being investigated.

-Decision Support Tools (DSS) help develop scenarios of future conditions resulting from potential climate change effects and management decisions. They can help develop "what if" scenarios that allow users investigate a wide variety of management outcomes.

The majority of software applications integrate with existing GIS software and provide user-friendly interfaces and pre-assembled modeling functions. Most visualization tools are web based, while modeling and DSS tools are downloaded applications.

Table 3.12: Software Tools classified according to Functionality and Mode of Use

No	Tool Name	Software Tools			Mode of Use		Modeling Algorithms Used
		Visualize	Modeling	DSS	Web Based	Download	
1	CLI_VULN_MONITOR	X			X		Data visualization, WordPress, Javascript Framework (jquery)
2	CLIMADA		X			X	Probablistic model, Matlab functions
3	CLIMATE_GUIDE_FIN	X			X		Environmental Data Visualization, OpenLayer maps and Javascript Frameworks (AlloyUI, YUI, jquery)
4	COMMUN_VIZ	X		X		X	3D Visualization, Realtime predictive model, decision tree,
5	ECO_SPAT_PORTAL	X			X		Environmental and Geophysical spatial data visualization on map, openlayer map, jquery
6	HAZUS-MH		X			X	Predictive model
7	MACC		X			X	Excel based tool
8	MOWE_IT	X			X		Data Visualization, Javascript Frameworks and Google Maps
9	NATURE_VISTA			X		X	Decision tree, predictive model
10	ND_GAIN	X			X		Data visualization on maps, Javascript Framework (jquery, node.js, D3, backbone.js, underscore.js)
11	SLR_CFI_VIEWER	X			X		Environmental Data Visualization on map

3.2.4.5. Strengths and Weaknesses of adaptation tools

Finally, after examining tools operation and technical characteristics, we have evaluated strengths and weaknesses of these selected tools, and results are presented in Table 3.13:

Table 3.13: Strengths & Weaknesses Analysis

No	Tool Name	STRENGTHS	WEAKNESSES
1	Baltic Climate Toolkit	•It describes guidelines and methodology easy to understand. • Can be used as a model of regional adaptation planning	• Not enough data to make informed decisions. •Example links stopped working.
2	Blue Spot Model	•Complete protection for any sector and type of hazard. •It can be used for new roads the planning phase. • Potential to expand to other counties	•It requires extensive data related to precipitation, elevation etc. around the targeted road networks
3	Climate Vulnerability Monitor	•Valuable information for all countries worldwide. • Financial analysis and communication on clim.change. • Policy development guidance & resource allocation	•Data classifications of confidence levels • Uncertainty factor
4	Climada	• Wide variety of simulated hazards. • Simulation for natural catastrophes, quantifies costs and damages. •The tool is open source • Allows users to write their own modules	•Some modules might not have been thoroughly tested, but core climada works without limitations. • Uncertainty factor
5	Climate Guide: Clim. Change Impacts	•Comprehensive tool offers a wide range of climate related information. •Can be used in conjunction with the BalticClimate Tool	•Some parts of the tool are available in Finnish only. •Local scope, only for Finland.
6	CommunityViz	• Interactive and highly visual decision-support tool • Versatile, widely used well supported, and updated • Works as an integration framework connecting to Hazus-MH and NatureServe Vista.	• No built-in data and relatively little built-in modeling. • Uncertainty factor • Not free , high cost to obtain
7	Ecocities Spatial Portal	•Wide variety of scenarios presented on a map • Used as a template to assist vulnerability assessment.	•It has a very limited scope, covering only the region of Manchester. • Uncertainty factor

		• Can be combined with Urban Adaptation tool.	
8	EconAdapt	•Rich library of economics of climate change adaptation •Detailed deliverables support decision makers in adaptation process •Easy accessible info on adaptation economic assessment	•Some aspects of the toolbox do not seem to work properly • Uncertainty factor
9	HAZUS-MH (Hazards-United States-Multi-Hazard)	• Results for large-scale events for planning, mitigation, emergency preparedness and response • Intuitive graphic and tabular formats • GIS software to map hazard and economic loss • Vehicle & traffic data • Allows users to estimate the impacts on populations	• Components of default inventory data may not line up on maps, e.g. bridges and roads. • Can run out of memory and fail during coastal floodplain delineation for complex regions
10	MACC	•Useful manual and tutorial videos •The auto-generated indicator and progress charts • The charts and monitoring data can be exported	• As with many Excel-based tools, formula can be deleted or altered • Uncertainty factor
11	MOWE-IT	•Wide variety of information for different stakeholders •There is a library of good practices and methodologies • Visualization tool offers details for transport network	• Not very detailed analysis on results calculations • Uncertainty factor
12	NatureServe Vista	• Integrates information from other tools • Covers integration and modeling assessment • Works well with a variety of other tools • Number of conservation elements, objectives, & multiple land-use	• Raster-based platform • Limited scale • The breadth of functions provided may lead to a slow learning curve • Uncertainty factor
13	ND-GAIN	•A wide variety of sectors on almost every country. •Comparison methods of countries and explanation. •The tool is updated bi-annually	• Incomplete measures of institu-tional and governmental capacity. • Uncertainty factor
14	Sea Level Rise and Coastal Flooding Impacts	• User friendly - GIS analysis for coastal areas • Contains photos and visualize impacts of sea • Diversity of information for different stakeholders.	• Deficient inundation scenarios • Cannot customize outputs

15	SNAP	•It can be used by a variety of stakeholders and in different projects •It can both lay the groundwork for adaptation as well as assess the adaptation process	•It requires preparation that must be conducted outside of the tool and is not supported by it
16	UKCIP Adaptation Wizard	• Captures information on weather events • It assesses organization vulnerability to climate • Range of tools to help user plan his adaptation strategy	• Does not produce a tailor made climate adaptation strategy at the click of a button
17	Urban Adaptation Support Tool	•A complete methodology covering all steps •Feedback system helps tool evolution • Covers a wide range of different regions	•It is more focused on municipality-urban levels

3.2.5. Summary of Research Work

Climate change is already occurring, seriously affecting weather stressors. Adaptation has become a necessity for critical infrastructures. Research work has been done to investigate adaptation tools, suitable for transport sector, with emphasis on methodology assessments and supportive applications, that help stakeholders, make prudent decisions about adaptation planning.

Tools are classified based on typology and target audience, activity sectors, climate impacts and adaptation planning steps. Moreover, the software tools are classified according to their functionality and mode of use. The majority of tools are developed to deal with all climate change impacts and have an 'all-sectors' approach, in order to provide a holistic support for stakeholders to adaptation planning process.

GIS functionality is incorporated into many decision-making and climate adaptation processes. Seeing that many of the questions raised by climate change planning are landscape-based, they are better addressed by geospatial visualization tools. Stakeholder input throughout the process, is quite critical, since adaptation actions and plans can affect economic prosperity and society's critical services.

Out of the methodology tools examined, the 'Urban Adaptation Support Tool' is a complete methodology-guide, which leads policy makers throughout all adaptation steps, covering all possible climate impacts and the majority of vulnerable sectors. It provides a comprehensive literature database for each step of the adaptation cycle. Also, 'UKCIP Wizard' is very effective, as it provides a variety of functionalities to

help user plan his adaptation strategy and evaluate organization vulnerability to current and future climate.

As far as software tools are concerned, 'Climada' is the most advanced among European initiatives. It uses probabilistic modeling and projects vulnerabilities along with effective-ness evaluation of adaptation measures. Moreover, it is an open-source tool, so it can be modified to adjust to specific needs. From the US developed tools, we have distinguished the 'CommunityViz' software which provides 3D real-time visualization, covers all steps in planning process and works as an interactive decision support tool. It is well maintained and can cooperate with other tools, like 'Hazus' & 'NatureServeVista', which adds up in building adaptive capacity. However, it has a significant purchasing cost, which limits access to those who can afford to pay.

Finally, having examined strengths and weaknesses for each tool, we have collected main strengthful attributes like usability, modeling competencies, future projections, and data visualization. On the other hand, scope limitations, missing data, broken links, and information robustness are listed as main weaknesses. Last but not least, the uncertainty factor, which deals with climate projections, along with impact assessment ambiguity, can be proved as tools' main shortcoming with a decisive role in effective adaptation planning. As a result, adaptation tools should constantly improve their data robustness and modeling algorithms to avoid driving stakeholders to unnecessary measures, costs and complexity on adaptation policies and actions.

Chapter 4: Aviation Sector Cyber-Security Threats

4.1. Smart Airport Cybersecurity: Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience

4.1.1 Introduction [6]

Airports are at the forefront of technological innovation, mainly due to the fact that the number of air travel passengers is exponentially increasing every year. As a result, airports enhance their infrastructure intelligence and evolve as smart facilities to support growth, by offering an enjoyable travel experience. New challenges are coming up, which aviation must deal with and adapt to, such as the integration of Industrial IoT (Internet of Things) in airport facilities and the increased use of smart devices from travelers and employees. Cybersecurity is becoming a key enabler for safety, which is paramount in the aviation context. Smart airports strive to provide optimal services in a reliable and sustainable manner, by working around the domains of growth, efficiency, safety, and security. This subsection exhibits: (a) the implementation rate of cybersecurity measures in commercial airports; (b) malicious threats that evolve due to IoT and smart devices installed; (c) risk scenario analysis for IoT malicious attacks with threat mitigation actions. With the aim to enhance operational practices and develop robust cybersecurity governance in smart airports, we present a systematic and comprehensive analysis of malicious attacks in smart airports, to facilitate airport community comprehend risks and proactively act, by implementing cybersecurity best practices and resilience measures.

Airport operations and business models have evolved dramatically over the last decades to support the explosive growth of the global aviation industry (Raj & Raman, 2017). Regulatory reform in the new air travelling era produced dramatic traffic growth, diversity, and choice for airline passengers. As airlines refine their operating models to align growth to efficiency, airports evolve in parallel to create

[6] *Related Publications:*

I. Lykou G., Anagnostopoulou A., Gritzalis D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", SENSORS, January 2019.

II. Lykou G., Anagnostopoulou A., Gritzalis D., “Implementing cyber-security measures in airports to improve cyber-resilience”, in Proc. of the Workshop on Industrial Internet of Things Security (WIIoTS-2018), IEEE, Spain, June 2018

massive networks of hubs and intelligent systems, which together create an efficient air transportation ecosystem (Gopalakrishnan et al., 2013). Since airports are considered a gateway to the world for travelers and business, they are of great importance for country development and economic growth (Urban, 2016).

In the USA, aviation and airports, as a transportation subsector, constitute a critical infrastructure and key resource sector, according to the U.S Homeland Security Presidential Directive (US DHS, 2013). The same applies in Europe, where critical infrastructures and essential services in air transport facilities should be adequately protected according to NIS (Network and Information Systems) directive, EPCIP (European Program for Critical Infrastructure Protection) and European Community EC/216/2008 regulation.

Securing smart airports and staying ahead of evolving cyber threats is a shared responsibility, involving airlines, airports, vendors and regulators (ENISA, 2016) Identification of cyber-threats challenges, risk assessment approaches and guidelines to enhance cyber security are priorities currently researched by the aviation industry.

In this work, malicious cyber-threats that may influence the operational efficiency of smart airports, when equipped with IoT applications, are developed and analyzed. We present an overview of malicious risks that can affect essential services in airports and interconnected networks. We also illustrate a series of analytical malicious attacks scenarios in critical airport's infrastructures, along with mitigation strategies and resilience measures. The contributions of this study are the following: (i) a research analysis of measures and best practices currently implemented to commercial airports, analyzed based on online survey data; (ii) a detailed identification of malicious threats for IoT applications in smart airports; (iii) scenario analysis of malicious attacks in smart airports assets, including cascading effects, mitigation actions and cyber-resilience measures.

The remainder of this work is structured as follows: subsection 4.1.2 describes the research methodology, while the theoretical framework is presented in subsection 4.1.3. Airports' intelligence classification based on their technological evolution is introduced in subsection 4.1.4, while the online survey and research results are analyzed in subsection 4.1.5. Security practices for smart airports are decomposed in subsection 4.1.6, along with response feedback from the online survey, and then survey results are discussed in subsection 4.1.7. Malicious threats analysis and detailed attack scenarios are developed in subsection 4.1.8. Attackers motives are exhibited and attributed to each attack scenario in subsection 4.1.9. Finally, in subsection 4.1.10 research conclusions are presented.

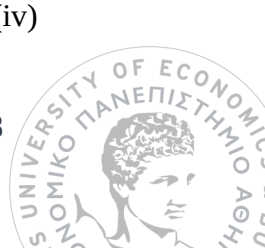
4.1.2. Research Methodology

This work has been developed using a combination of literature research and information received from an online survey about airport cybersecurity. The survey was addressed to European and American busiest airports with the purpose to understand the opinion of airport IT personnel about the introduction of the IoT to their airports and the cybersecurity measures applied. The format of this survey and other details, including questionnaire, are provided in the Appendix B. All survey responses received were promised to be treated with confidentiality and data from this research is reported only in the aggregate.

Our research goal was to define the implementation rate of cyber-security best practices in combination with IoT application status, through IT personnel opinions. Since there was a great diversity of technological evolution in airports examined, we have made an aggregated analysis of responses, combined with airport intelligence classification. Based on survey results, we extended our research and developed threat scenarios for malicious cyber-attacks that may influence the operational efficiency of smart airports.

4.1.3. Theoretical Framework

Cyber security can be defined as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance and technologies used to protect the cyber environment and organizations' assets. Although many airports have robust systems in place to address common hacking threats, they have not always taken a holistic approach to the IT cyber environment or considered the broader threat to the aviation system. In this direction, International Civil Aviation (ICAO) with ICAO/A39 calls on states and industry stakeholders to encourage coordination with regard to aviation cybersecurity strategies, policies and sharing of information to identify critical vulnerabilities that need to be addressed, by developing systematic information sharing on cyber threats, incidents and mitigation efforts. Following this direction, a variety of standards has been developed such as: (i) European Norm (EN) 16495 standard for Air Traffic Management tailored to civil aviation with supporting guidance on Information security for organizations, supporting civil aviation operations; (ii) ISA/IEC-62443 which is a set of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems; (iii) National Institute of Standards and Technology (NIST) - Special Publication 800-53 about Security and privacy controls for Federal information systems and organizations, which is a comprehensive catalogue of controls with much supporting advice; (iv)



NIST 800-82 Guide to Industrial Control Systems (ICS) Security, which provides guidance through typical system topologies, threats and vulnerabilities.

The aviation sector and especially smart airports cybersecurity have attracted researchers in the recent years, as the incorporation of new innovative technologies and their available attack surface has been increased. Civil Air Navigation Services Organization (CANSO) developed a guide for increasing security level to Air Traffic Management (ATM), by presenting cyber threats and risks, as well as threat actors with their motives (CANSO, 2014b). CANSO proposed a model in order cyber security to be addressed, in combination with international standards, NIST Cybersecurity Framework, as well as a risk assessment methodology.

Although significant research has been presented regarding ATM cyber risks, there is a lack of research about threats and vulnerabilities for ground handling IT systems and airport services, especially when equipped with smart applications. Particular to airport cyber security, risks constantly change, as new threats and vulnerabilities evolve, along with ever-changing technology implementations. In 2013, Gopalakrishnan et al. made an analysis about cyber-security in airports, giving a roadmap to secure control systems in the transportation sector, by presenting cyber risks in airport operations and potential targets for cyber-attacks. Existing vulnerabilities in Airport ICS have been evaluated by US Airport Cooperative Research Program and a Guidebook on Best Practices for Airport Cybersecurity has been published in 2011, to mitigate inherent risks of cyberattacks on technology-based systems (K. Sampigethaya et al., 2011). The European Union Agency for Network and Information Security (ENISA) has published its continuing work on communication network dependencies in industrial infrastructures, focusing on ICS/SCADA (Supervisory Control and Data Acquisition) systems and IoT infrastructures. In 2016, ENISA also published a security guidance for smart airports, presenting key stakeholders, asset groups, threats and risk analysis, best practices and security recommendations addressed to airport decision makers, policymakers, and industry stakeholders. Suciu et al. (2018) presented use cases of attacks in airports and explained which prevention methodology can be implemented, in order to improve the security level with the integration of several security tools, services and fields. Afify et al. (2014) focused on analyzing Denial of Service (DoS) attacks that occur in airports and especially in their automation systems by describing how attacks are launched along with effective countermeasures. Moreover, U.S. Department of Homeland Security (Commerce & Security, 2018) published a report which analyzed botnets and other automated, distributed threats, pointing out that such types of attack are a global problem nowadays. Finally, SESAR research addressed cybersecurity issues in Airport Operations Centers including a comprehensive maturity model to

approach to cyber-security within European ATM and to develop a comprehensive response to cyber-threats (SESAR JU, 2016).

Although threats to smart airport's cyber security apply to broad categories of assets (such as communication networks, servers and control systems, internal/sensitive information, authentication, and access control systems), most researchers focus on one or two scenarios of attack, while addressing cybersecurity issues in airports. To the best of our knowledge, no one has presented a complete scenario analysis of malicious attacks that may happen in smart airports, concerning IoT technologies and smart applications, including mitigation actions, resilience measures and impact effects on the information security triad (Confidentiality-Integrity-Availability: CIA).

4.1.4. Airport Intelligence Classification

Increasing their infrastructure complexity, airports have gained more stakeholders nowadays. They have honed their capabilities in interoperability by using Internet of Things (IoT) technology and intelligent applications to achieve on effectiveness.

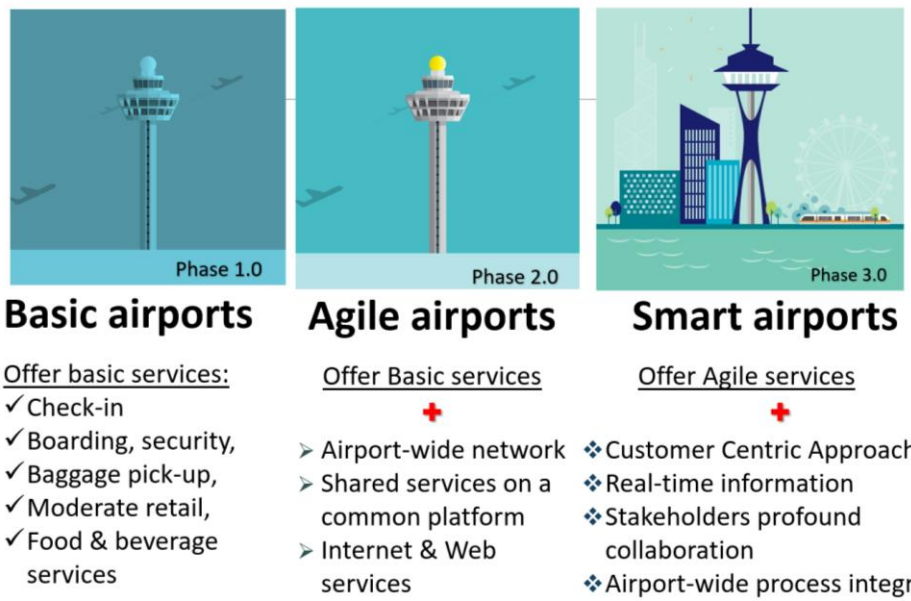


Figure 4.1: Airport Evolution and Intelligence Classification

According to ENISA, smart airports are those who make use of networked, data driven response capabilities that, on the one hand, provide travelers with a better travel experience and, on the other hand, aim to guarantee higher levels of security for the safety of passengers, operators and general public (ENISA, 2016). Since, safety and security are the most significant domains in aviation context, a safe

environment must be ensured by proactively handling difficult cyber challenges, while minimizing operations disruption.

According to (Raj & Raman, 2017), there is an evolution pace in today's airports, which can be classified into three broad categories, as shown in Figure 4.1.

In the **Airport phase 1.0 (Basic Airports),** airports focus on capabilities necessary for safe and efficient management of landings, departures, and other aircraft operations. They offer basic passenger services, including check-in, boarding, security, baggage pick-up, and moderate retail, food, and beverage services.

In the **Airport phase 2.0 (Agile Airports),** airports adapt to this changing digital environment. Technology enabled collaboration is highly evolved throughout these airports and is implemented across business units. Airport-wide, converged network architecture offers shared services on a common platform.

In the **Airport phase 3.0 (Smart Airports),** airports fully exploit the power of emerging and maturing technologies of IoT, with advanced and pervasively deployed sense-analyze-respond capabilities. The digital grid is the airport's nervous system, touching and managing every point of interaction. By enabling the exchange of real-time information, profound collaboration, and airport-wide process integration, smart airports significantly improve operational efficiencies, passenger services, and advanced security capabilities.

Cyber security can be defined as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance, and technologies used to protect the cyber environment and organizations' assets. Although many airports have robust systems in place to address common hacking threats, they haven't always taken a holistic approach to the IT cyber environment or considered the broader threat to the aviation system (IATA, 2015). In this direction, International Civil Aviation with ICAO/A39 calls on states and industry stakeholders to encourage coordination with regard to aviation cybersecurity strategies, policies and sharing of information to identify critical vulnerabilities that need to be addressed, by developing systematic information sharing on cyber threats, incidents and mitigation efforts (*ICAO. Assembly Resolutions A39-19, 2016*).

Particularly in airport cyber security, risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations. A taxonomy of threats to the cyber security of smart airports, including mapping to smart airport assets has been developed by ENISA and makes evident that cybersecurity has a major stake in providing safety. The challenge is to address security issues not only to enhance security but also to ensure safety. According to ENISA, smart airports are those who make use of networked, data driven response

capabilities that, on the one hand, provide travelers with a better travel experience and on the other hand, aim to guarantee higher levels of security for the safety of passengers, operators and general public (ENISA, 2016). Since safety and security are the most significant domains in the aviation context, a safe environment must be ensured by proactively handling difficult cyber challenges, while minimizing operations disruption. In this work, we have concentrated our research on mapping smart airport's threats, initiated from malicious actions, in order to develop a variety of attack scenario analysis, along with recommended mitigations and resilience measures.

4.1.5. Online Survey Results

An online survey questionnaire was addressed to the 200 busiest commercial airports in Europe and USA, although only one third of them had responded to the survey. Among them, we distinguished fully completed and solid questionnaires and we elaborated their results. Answers received from European airports reached 66%, while 34% came from USA as shown in Figure 4.2.a. The airports have been further classified to Basic/Agile/Smart categories, according to their own statement about being or planning to be smart, in combination with the number of IoT applications that they have indicated to use in their facilities. This classification was chosen, in order to better evaluate the cyber-security preparedness level of airports, based on ICT complexity and technological progress. As a result, 16% of airports have been classified in the basic category, 56% were categorized as agile and the rest 28% of airports were ranked as smart airports, as presented in Figure 4.2.b.

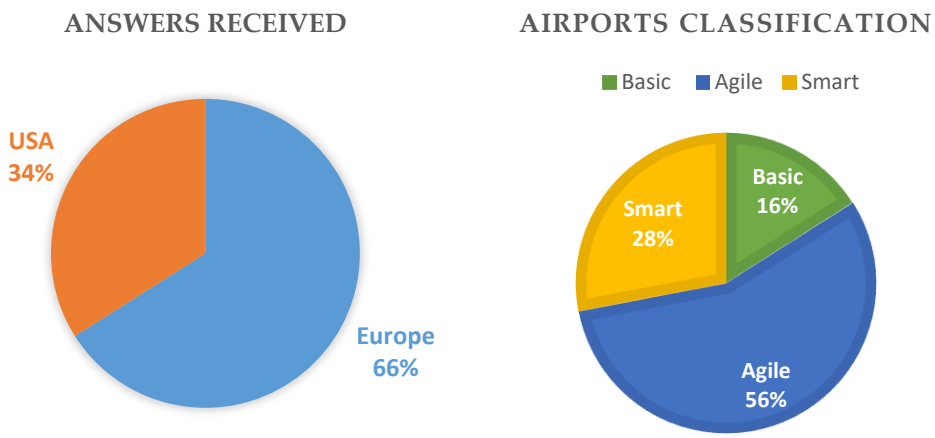


Figure 4.2. a) Origin of airports replies, b) Airports classification based on IoT apps.

Although 59% of responders stated having effective cybersecurity policies for IT assets, when they were asked to rank the risks from IoT devices, the majority (76%) pinpointed the lack of security awareness as the greatest risk, followed by internet connectivity risk (29%), which reveals a controversy in security confidence of responders.

Airports have defined which smart applications are using in their facilities that underpin key airport activities, as listed in Figure 4.1. The percentages, listed on the right side of Figure 4.3, are presenting the overall performance from all airport's answers received, while on the left side, the performance of smart airports is exhibited. As we can see, the most popular smart applications, used in all airports, are passenger check in and boarding services (41%), common use passenger processing systems (41%), while the least used are SCADA applications (6%) and connections with other transport systems (15%).

Especially in smart airports, IoT applications like baggage handling, passenger check in, landside operation controls, common use passenger services and traveler web services are found to be used in frequencies over 70%. Building Management Systems (BMS) and HVAC (Heating, Ventilation, Air Conditioning) equipment controls are also widely used in smart airports (60%). SCADA systems are in their infancy stage overall in airports. Only smart airports have stated to use SCADA with a 20% implementation rate.

Since industrial IoT applications are in their emergence, a great expand is expected to transform mainstream busiest airports to smart airports. Research revealed that this early adoption increases smart airport's interoperability, along with vulnerability exposure to cyber threats.

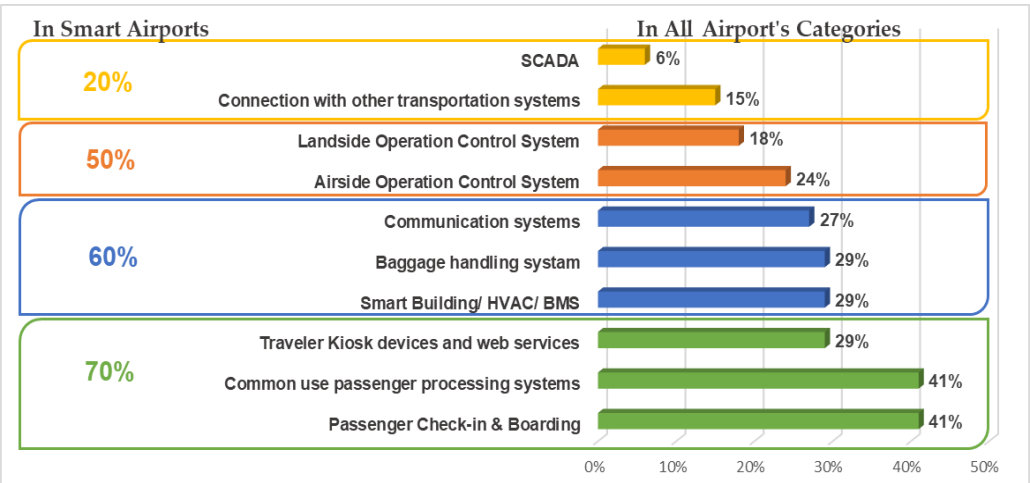


Figure 4.3. IoT applications in airports.

4.1.6. Security Practices for Smart Airports

Securing Smart airports and staying ahead of evolving cyber threats involves proper management from all stakeholders. Security good practices and tools have been developed and published in literature (ENISA, 2015b, 2016, 2017). The identified practices for smart airports have been categorized into three main groups: i) Technical; ii) Organizational and iii) Policies and Standards, as presented in Fig. 4.4.

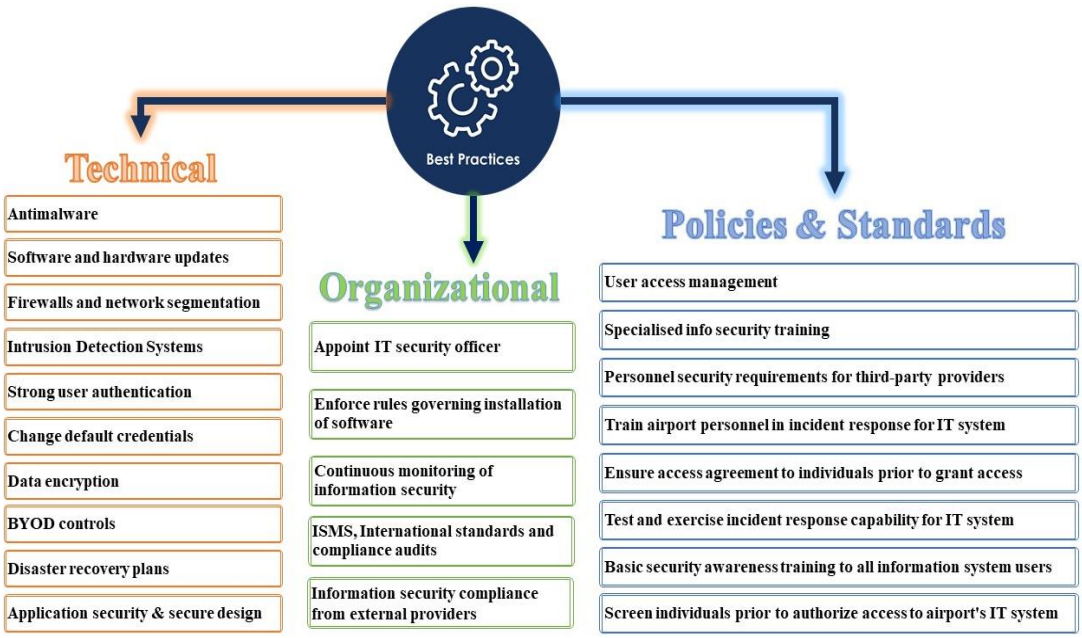


Figure 4.4. Cyber Security Good Practices Classification

4.1.6.1. Technical Good Practices

There are various good practices published for all aspects of airport-based technical practices. Below we provide an overview of ten good practices included in our survey, followed by airport responses analysis.

***Antimalware*:** All computers should run anti-malware software to detect and remove or quarantine malicious software. Smart airports have responded to apply at 60% rate antimalware practices to IT equipment, agile airports are partly implementing with 50% rate, and basic airports poorly implemented antimalware protection reaching only 33%.

***Software and hardware updates*:** Should be regularly performed. Applying security patches prevents cyber criminals exploiting unpatched software and reduces the exposure to known vulnerabilities. This was implemented at 80% rate from smart and agile airports, while only at 33% rate from basic airports.

***Firewalls and network segmentation*:** The border of the airport network infrastructure should be protected by perimeter firewalls to block untrusted connections between networks. A defense in depth approach should be taken to improve network security. Both smart and agile airports fully comply with these practices (100%), while basic airports perform above average with a 67% implementation rate.

Intrusion Detection Systems (IDS): Refers to monitoring of both software and hardware devices over the network. It can be categorized as (i) network-based IDS, focused on the analysis of network traffic and (ii) host-based IDS, able to analyze activities on the host and raise alerts, in case of events like unauthorized access to applications, escalation of privileges, modification of file systems, etc. Smart and agile airports reported to implement IDS at 60% rate, which reveals a security gap, especially for smart airports with many integrated applications and communication ports. Basic airports were found not to implement at all this practice, which creates a serious vulnerability and security risk.

***Strong user authentication*:** Should protect IT devices, while sensitive or remote services should require access only via multifactor authentication and/or biometric identifiers. Smart airports responded to protect IT services using strong authentication (80%), agile airports comply less (60%), while basic airports not at all.

Change default credentials of devices: Devices, connected to the airport network should be properly configured and have default password changed. In addition, when not required, remote access should be disabled to prevent cybercriminal remote-connection attacks. Here the compliance was poor for all airport's categories (smart 40%, agile 50%, basic 33%) which revealed a security gap and a serious vulnerability.

***Data encryption*:** Used to protect sensitive information exchanged in the network from eavesdroppers and to protect data collection and storage. Smart airports satisfactory use encryption methods at 80%, agile airports have lower implementation rate reaching 50%, while basic airports do not use encryption methods, according to IT personnel responses.

Bring your own device (BYOD) controls: Airports should typically prevent employees from connecting their own personal devices to airport systems. Otherwise, effective technical controls should be applied to protect the airport and network infrastructure from compromised devices. All airport categories seem to poorly apply controls for such devices (smart 40%, agile 33%, basic 0%), which reveals the need for security reinforcement with suitable measures to increase cybersecurity protection.

Disaster recovery plans for IT assets: Technical procedures should be in place to restore operation of critical IT assets to an adequate level of service, in case of emergency. Both technical and organizational aspects must be included in disaster recovery plans. People involved must have a clear view of their roles, the sequence of actions to be performed, the actors involved and so on. All smart airports responded positively for this practice with 100% rate, agile airports implementation reached 60%, while for basic airports only one third stated to apply such procedures for IT assets.

***Application security and secure design*:** Secure design should be part of System/Services/Technology Acquisition. It should be combined with airport assets under provisioning risk assessment, privacy by design principle and security criteria requirements. Smart airport responded at 80% to apply secure design procedures, while agile and basic airports had only at one third implemented this practice.

Table 4.1 presents the technical good practices implemented in all airports categories, based on survey answers and airport classification. As we can notice, the most implemented technical based practices for all airports are: i) Firewalls and network segmentation (94%); ii) Software and hardware updates (72%); and iii) Disaster recovery plans (67%). On the contrary, the least implemented technical based practices are: i) BYOD Controls (28%); ii) Change default credentials (44%); and iii) Application security and secure design (44%).

Smart airports have the greatest implementation rate of technical practices, reaching 70% on average. This was an expected result, since advanced complexity of smart applications, requires advanced cybersecurity defense. However, we have found that some practices were poorly implemented by smart airports, such as changing default credentials and BYOD controls, which reveals a security gap and possible areas for cybersecurity amelioration.

Agile airports have an overall lower implementation rate of technical practices, reaching on average 59%. They are all implementing firewalls & network segmentation, while the majority uses strong authentication and software/hardware updates. However, they lack of applying technical practices, like BYOD Controls and secure application design.

Table 4.1: Technical Good Practices

Technical Good Practices	BASIC	AGILE	SMART	ALL
Antimalware	33%	50%	60%	50%
Software and hardware updates	33%	80%	80%	72%
Firewalls & network segmentation	67%	100%	100%	94%
Intrusion Detection Systems	0%	60%	60%	50%
Strong user authentication	0%	80%	60%	61%
Change default credentials	33%	50%	40%	44%
Data encryption	0%	50%	80%	50%
BYOD Controls	0%	30%	40%	28%
Disaster recovery plans	33%	60%	100%	67%
Appl. security & secure design	33%	30%	80%	44%
Average implementation rate	**23%**	**59%**	**70%**	**56%**

Basic airports need to start implementing practices like: Data encryption; Strong user authentication; BYOD controls and IDS, since they have responded not to apply at all. Besides, they need to enforce all the other technical practices. The most implemented measures are firewalls and network segmentation at 67% rate, while the average implementation on technical practices is only 23%.

Research also revealed that airports, who are using IoT and SCADA applications in their facilities, have more technical practices implemented than the other airports. This indicates a higher concern about cybersecurity and effective performance towards cyber resilience achievement.

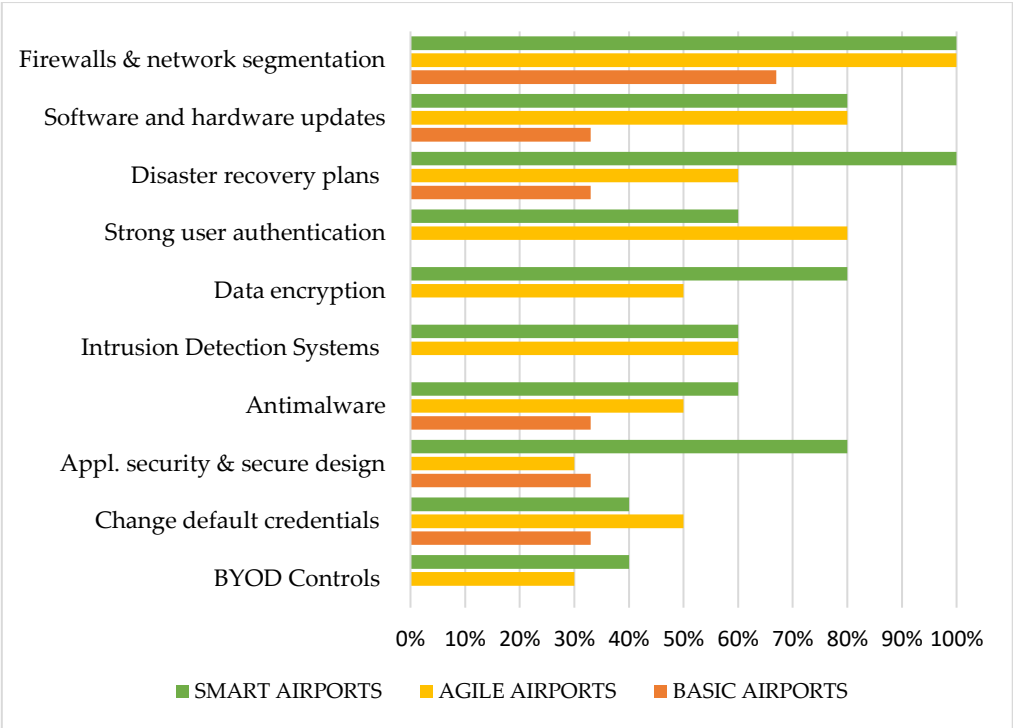


Figure 4.5. Technical good practices implementation analysis

Figure 4.5 exhibits the technical good practices implemented in all airport's categories, based on survey answers and airport classification. As we can observe, the most implemented technical based practices for all airports are: (i) Firewalls and network segmentation; (ii) Software and hardware updates; and (iii) Disaster recovery plans. On the contrary, the least implemented technical based practices are: (i) BYOD: Bring Your Own Device Controls; (ii) Change default credentials; and (iii) Application security and secure design.

4.1.6.2. Organizational Good Practices

A variety of airport-based organizational practices about people and processes exists in literature (ENISA, 2016). Below we provide an overview of each good practice and afterwards we analyze airport responses from our survey about good practices implementation.

User access control and management: Logical and physical access control to airport IT systems should be established along with identity access management system. All airport categories responded to apply such procedures (90-100%), which allies with safety culture already developed, regulated and implemented in airport facilities.

Screen individuals prior to authorizing access to the airport's information system: Requiring airport employees to undergo biometric identification prior to being granted access can be beneficial for mitigating the risk of identity fraud. Smart

airports apply this process at 60% rate, agile at 50%, while basic airports not at all, according to their replies. Privacy and personal data protection restrictions and regulations are possible obstacles for biometric applications.

Ensure individuals requiring access to airport IT systems sign appropriate access agreements: Prior to being given access to airport IT systems, individuals should sign appropriate access agreements, including non-disclosure & acceptable use agreements, rules of behavior and conflict of interest agreements. All airport categories responded to poorly implement this practice with 20-40% application rate.

Establish personnel security requirements for third-party providers, including security roles and responsibilities. 3rd party compliance with such requirements should be also monitored. Smart airports apply such security requirements at 60% rate, while only one third from agile and basic airports comply with such security requirements.

Provide basic security awareness training to all information system users based on the specific requirements of the airport and the IT systems. The majority (60%) of smart airports provides such training to system users, responses from agile airports are at 50% and basic airports need to do more on this area (33%), in order to improve cyber resilience. Security awareness was cross checked with other questions within the survey, where responders claimed that the lack of security awareness was a major risk for IoT devices in airports facilities.

Provide specialized information security training with role-based and security-related training, before authorizing access to IT system. The request for specialized security training is a common need for all airports based on survey responses with low implementation rate (33-40%). IT personnel responses revealed the need for more specialized security training to confront the increasing complexity of cybersecurity threats.

Train airport personnel in their incident response roles with respect to the information system: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources to handle the situation in a way that limits damage and reduces recovery time and costs. The same response attitude from all airport categories with low implementation rate (33-40%) was also found here, which urges for continuous training policies implementation.

Test and regularly exercise the airport's incident response capability system to determine incident response effectiveness and avoid a low level of incident response capability. Airports responded to have a medium implementation of this procedure with smart airports at 60%, agile at 50% rate and basic airports only at 33% compliance.

Table 4.2. Organisational Good Practices

Good practices about people, organization and processes	BASIC	AGILE	SMART	ALL
User access management	90%	90%	100%	95%
Screen individuals prior to autho-rize access to airport's IT system	0%	50%	60%	44%
Ensure access agreement to individuals prior to grant access	33%	20%	40%	28%
Personnel security requirements for third-party providers	33%	30%	60%	39%
Basic security awareness training to all information system users	33%	50%	80%	56%
Specialised info security training	33%	30%	40%	33%
Train airport personnel in incident response for IT system	33%	30%	40%	33%
Test and exercise incident response capability for IT system	33%	50%	60%	50%
Average implementation	**36%**	**44%**	**60%**	**47%**

Table 4.2 summarizes employees' responses about airport organizational practices applied to all airport's categories. The most implemented security process is user access, reaching 95%, while basic security awareness training to all information system users follows with 56% implementation. The least implemented practices are access agreement for third party stakeholders (28%) specialized security training and incident response for airport's personnel (33%).

Smart airports have a good implementation rate of organizational practices reaching 60%, agile airports have on average low implementation rate reaching 44% and basic airports implement them with the disappointing performance of 36%. Moreover, basic airports seem to ignore basic policies and keep low performance to the majority of organizational practices. This can seriously impact their cyber resilience capability, in case of a cybersecurity incident in critical IT processes and services.

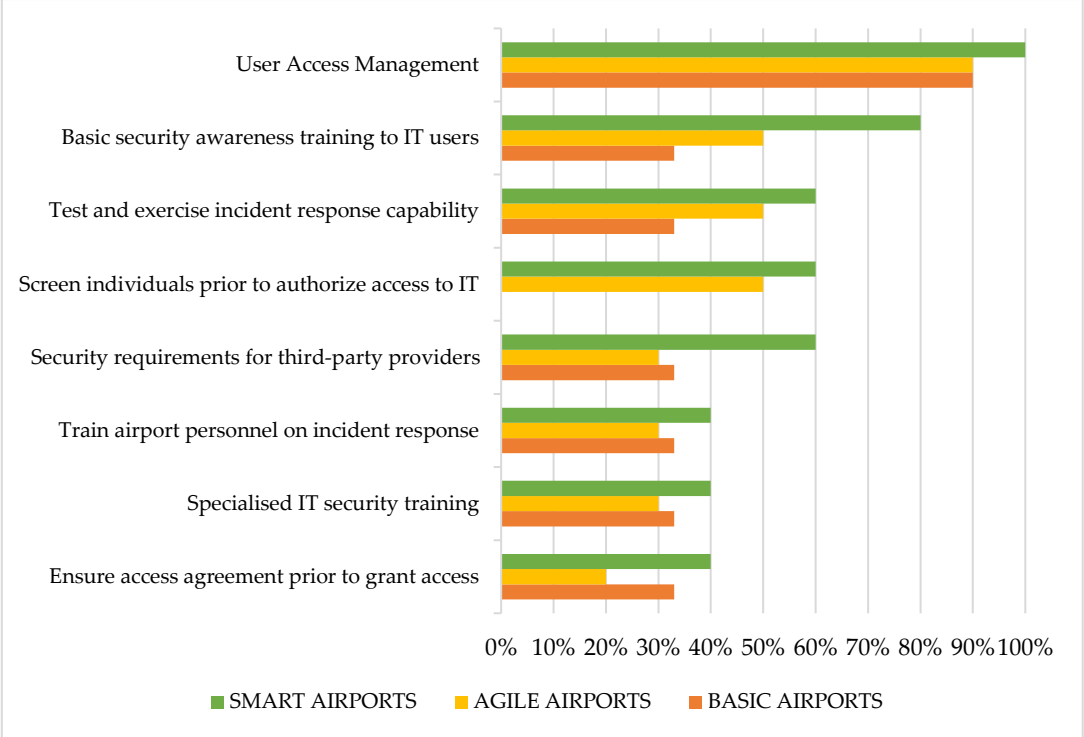


Figure 4.6 Good practices about airport's organization and processes

Figure 4.6 graphically exhibits employees' responses about airport organizational practices, applied to all airport's categories. The most implemented security process is user access, reaching 95% overall performance, followed by basic security awareness training to all information system users. The least implemented practices are: (i) access agreement for third party stakeholders; (ii) specialized security training; and (iii) training on incident response for airport's personnel.

4.1.6.3. Policies and Standards

A variety of airport security policies and standards have been proposed. In this subsection we provide an overview of each good practice, included in our survey and then we analyze airport responses about their implementation.

Appoint an information security officer with the mission and resources to develop, implement and maintain an airport-wide information security program. Smart airports have all (100%) appointed an IT security officer. This is obvious a mandatory policy, in order to successfully protect intelligent applications including SCADA and IoT and meet security requirements. Agile and basic airports have a lower performance at 50% and 33% implementation rate for this essential policy, which reveals a serious security inability.

Enforce explicit rules governing the installation of software, in accordance with contract agreements and copyright laws. Specific rules should be established for the types of software that are permitted and which are prohibited. While smart airports have an acceptable implementation rate of 60%, agile (30%) and basic airports (0%) poorly apply such rules, which increases cyber risks and vulnerabilities.

Continuous monitoring of information security should be established and implemented across the airport. The majority of smart airports implements this practice (80%), while agile and basic airports are performing at 50% and 33% rate accordingly. Monitoring strategy and continuous reporting on the security state of the information system should be included in all airports security practices.

Information security management system (ISMS), implement international standards and demonstrate compliance: Organizations following international standards on ISMS should rely on an information security framework, as well as external audits, for measuring progress, identifying gaps and demonstrating compliance. Smart airports are following such practices with 60% rate, agile airports follow with 40% and basic with 33%.

Information Security compliance from providers of external information services should be also certified against relevant standards. An appropriate chain of trust should be established with external service providers when dealing with information security. Smart airports responded compliance at 80% rate, while agile and basic airports reached accordingly 50% and 33% compliance rate.

Table 4.3. Policies & Standards

Good Practices for Policies and standards	BASIC	AGILE	SMART	ALL
Appoint IT security officer	33%	50%	100%	56%
Enforce rules governing installation of software	0%	30%	60%	33%
Continuous monitoring of information security	33%	50%	80%	56%
ISMS, International standards and compliance audits	33%	40%	60%	44%
Information security compliance from external providers	33%	50%	80%	56%
Average implementation	**26%**	**44%**	**76%**	**50%**

Table 4.3 summarizes IT personnel responses about airport policies and standards applied, according to airport classification and overall. The most implemented security policies are the appointment of IT security officer, continuous monitoring of security, and information security compliance from providers of external IT services. Unexpectedly, the least implemented policy is to enforce rules governing installation of software. This is essential to enhance cybersecurity efficiency, in view of the inc-

rease of personal devices interacting with airport's IT systems, combined with the lack of BYOD security controls.

Figure 4.7 graphically presents IT personnel responses about airport policies and standards applied, according to airport classification and overall.

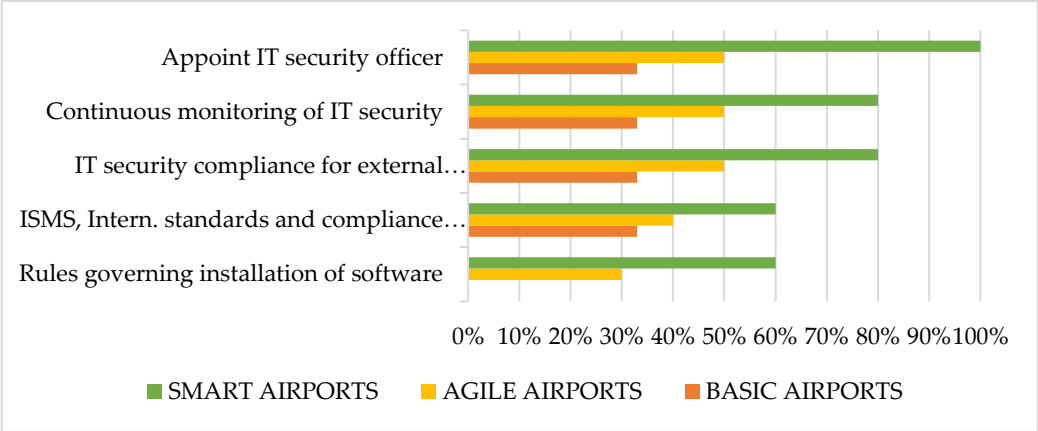


Figure 4.7 Good practices for policies and standards

4.1.7 Results Analysis Discussion

This survey was developed in order to extract information from airport security professionals about their cyber-security efforts and risk management activities. The decline of participants to fully complete the survey and provide information about their cybersecurity implemented practices was a survey limitation. Indeed, although 280 survey visits have been recorded to the online survey-tool, only 34 questionnaires were taken into consideration in our analysis, due to specific filters applied, relevant to participants' position, along with completeness and robustness of answers received.

Moreover, integrity of responses was partially verified by online search for each airport's technological situation. In our view, this response avoidance was attributed mainly to confidentiality precautions from participants and lack of motivation to support this research work.

Although sample size may be considered as small, it was representative from both Europe and US busiest airports, with a good technological variety of airports between basic, agile, and smart categories, so results retain their statistical significance.

4.1.8. Smart Airports Attacks: Scenario Development

4.1.8.1 Cybersecurity Malicious Threats Analysis

Although many security threats may occur either by intentional or unintentional factors, in this work we have focused on cyber security threats that spring from intentional /malicious actions. Various methods can be used by actors with malicious intent to compromise IT assets or to perform elevation of privilege attacks. Each of these attacks may lead to security incidents with breach of confidentiality, integrity, availability and should be considered while assessing the attack vectors for each asset, in order to protect the airport's safety and business continuity. Major cybersecurity threats against IoT applications in smart airports can be segregated into the following categories: (i) Network and communication attacks; (ii) Malicious software; (iii) Tampering with Airport Smart Devices; (iv) Misuse of Authorization; and (v) Social and Phishing attacks. Figure 4.8 presents these malicious threat categories, which are further analyzed afterwards.

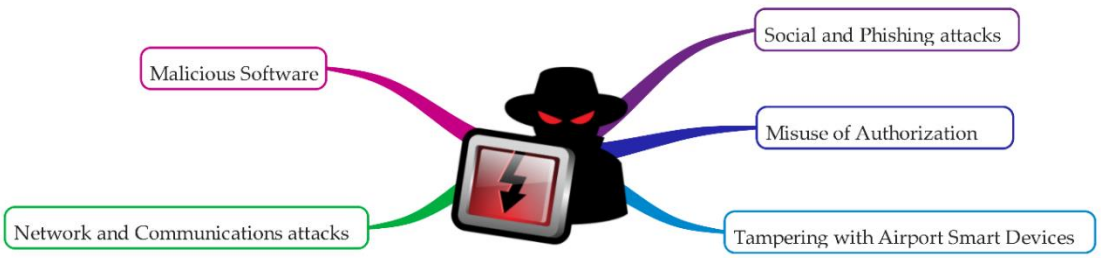


Figure 4.8. Cybersecurity malicious threats categories

Network and Communication attacks: Networks are subject to attacks from malicious sources, divided into two categories: passive attacks, where intruder intercepts data and active attacks, where actor disrupts the network's normal operation and gains access to assets available via this network. Despite the legislation, which prevents communication interception, smart airports remain an attractive target of tampering or network attacks, depending on the attack surface and controls in place. Various kinds of wireless communications may be affected or jammed, such as wireless communications, air traffic management and radio signals, which they can be overshadowed by jamming devices. Denial of Service attacks also enable attackers to disrupt information systems and networks, being able to impact on airport's system availability. As a result, network outages, passenger delays, cancelled flights may have serious imparts to smart airports, along with loss of confidence, damages to reputation, and potential financial damages.

Malicious software: Malware, which is able to infect common information systems, may also compromise smart devices, including passenger and staff portable devices, servers and other smart components, including airport's supervisory control and data acquisition systems. Severe impact on airport's infrastructure occurs, since such software acts maliciously, misusing its ambient authority on the computer it manages to get installed and runs on. Vulnerabilities may exist in smart airport systems, including third party security issues on smart assets, remote sensors, and controls. Any smart airport system with an available attack surface, where security fix has not applied, and system is not running with all the latest security patches is a likely target of malicious software attack.

Tampering with Airport Smart Devices: Airport devices can be tampered with various unauthorized ways. Unauthorized modification includes manipulation of data at central reservation systems, administration IT systems, airport's stored sensor data. The threat of tampering also includes unauthorized modification of hardware or software with data deletion or corruption, which can affect the behavior of airport's self-serving systems like automatic check in machines, passport control gates and smart building management systems. As a result, attackers can potentially gain control over systems, and result in malicious behavior with physical safety breaches and serious impact on airport's security.

Misuse of Authorization: Although, access controls are security features which define how users and systems interact, attackers may be able to obtain credentials and escalate authorization rights. Even employees or contractors, acting as insider threat and possessing authorization rights may be able to misuse their privileges. Such attacks also include credential theft via social engineering, spear phishing or simply insider threats. Provided that attackers can gain access, holding legitimate user's credentials, they can also escalate their privileges, and damage smart airport assets, depending on the level of privilege obtained.

Social and Phishing attacks: Social engineering can manipulate or mislead people in order to perform actions on behalf of the attacker. Social attacks are effective as they can circumvent technical and physical controls. Airport employees who lack security awareness and may not follow procedures, can pose a significant risk to airport cyber security. Email remains a primary method for threat actors to infiltrate a system, enabling the attackers to gain full access to the victims' accounts, identity, and authorization. Even though organizations install filtering capabilities, phishing emails still may get through and trick the victim to perform a malicious action without knowing.

4.1.8.2. Attack Scenarios Analysis with Mitigation and Resilience Measures

In our research we have evaluated various attack scenarios relevant to Smart airports and IoT applications and created a collection of scenario attacks for all malicious threats previously introduced. A more detailed description for each scenario is presented, along with domain and impacted assets, as well as possible escalation to cascading effects on other critical assets. Additionally, a step attack with graphical representation depicts malicious attack phases and related impact on security parameters. In addition, wherever examples of real incidents of cyber-attacks in smart airports have been investigated, are also referenced. Finally, mitigation actions and resilience measures that could be deployed in each scenario are presented, in order airport's cybersecurity and cyber-resilience to be enhanced against malicious attacks.

A) Malicious Attack: Distributed Denial of Service attack

The main characteristic of smart airports is the networked, data-driven response capabilities through smart components and integrated IoT devices. Any smart device connected to airport's network may support crucial key functions of interoperability between aircrafts, airport administration, air traffic control, and other forms of communication. Distributed Denial of Service (DDoS) attack is one of the most interesting and widely seen cyber-attack in the recent times, as presented in Fig. 4.9. In DDoS attack, a hacker temporarily enslaves a number of internet-enabled devices into an arrangement and then make simultaneous requests to a server or an array of servers for a specific service, thereby overwhelming the server and make it ignore legitimate requests from end-users. The Mirai Botnet code is an example of DDoS attack, which infects poorly protected internet devices, to find those that are still using their factory default username and password (Angrishi, 2017). The effectiveness of Mirai is due to its ability to infect thousands of these insecure devices and co-ordinate them to mount a DDoS attack against a chosen victim. Successful DDoS attack can result in either access deny for the legitimate users or system's inability to distinguish legitimate users from fake ones.

Impact Evaluation: Launch of a DDoS attack impacts the availability of smart airport's resources and services. The consequences are varied according to the time needed for recovery of business operations. This type of attack may lead to actions, like cancelation of flights, passenger delays, unavailability of cloud-based services, or even outage of staff communication systems. Such an attack happened in June 2015, at Warsaw Chopin airport, where approximately 1.400 passengers were grounded for five hours, while Polish airline was the victim of a DDoS attack (Reuters, 2015).

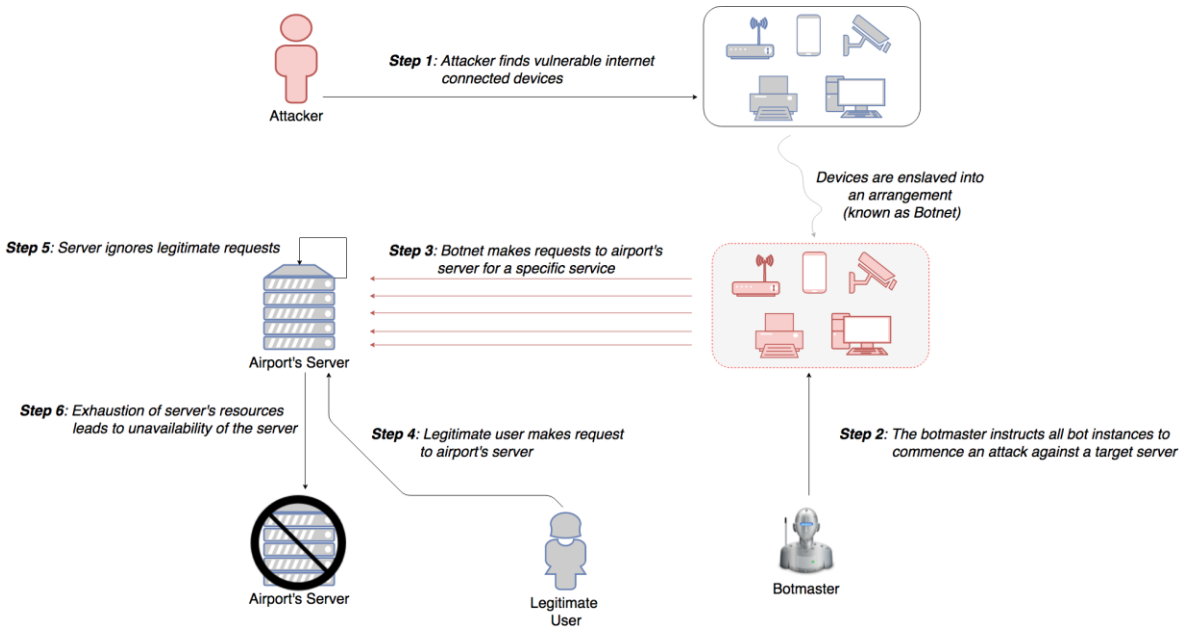


Figure 4.9. DDoS attack using Botnets

Cascading effects: Once a smart airport's network is flooded and non-responsive to requests, many of its functionalities become unavailable. Some of the consequences of such unavailability may refer to the proper operation of passenger management systems, including kiosk devices or passenger check-in and boarding. Moreover, the domains of safety and security, as well as the Airline/Airside Operations may be vulnerable to this attack, as their operations are mainly based on the airport's network. Last but not least, the asset group of IT and Communications may probably be affected as it contains internet-connected assets. Indicative examples of these assets are cloud-based data and application services, passenger-airline communication systems, as well as common communication systems.

Mitigation Actions: Security hardening of airport's smart devices and IoT systems is a quite important mitigation action, as there is need for the reduction of the existing attack surface. This action can be achieved by changing default passwords, disabling services, closing ports, as well as regular patching of systems. Smart airport's network should be protected by firewalls and follow a defense-in-depth approach, in order the traffic between the network segments and hosts to be more restricted. Moreover, another way to protect against DDoS attacks is through volumetric protection from the Internet Service Provider (ISP). Most ISPs have the ability to automatically detect potential DDoS attacks and to filter/throttle back requests from possible sources. The ISP is then able to identify and mitigate abnormal traffic to only deliver 'normal' requests to the final IP address (SESAR JU, 2016). An alternative method of defense could be to have a secondary Internet connection and another IP range, so as to be used in a case of emergency, in order to secure airport operations.

Resilience Measures: In order smart airports to react immediately to a potential DDoS attack, involves the combination of attack detection, classification and response tools, aiming to block illegitimate traffic. Therefore, it is important to regularly exercise preparedness and response time on test incidents, as well as provide incident response capabilities. In addition, communication of anomalous activity and malicious attacks to IT staff, senior management, affected stakeholders, other agencies, and law enforcement personnel can help the airport community to be better prepared and defend against similar attacks.

B) Malicious Attack: Communication Attack to ATM Systems

Automatic Dependent Surveillance –Broadcast (ADS–B) is a recently introduced surveillance technology, where aircraft's navigation system determines its position, using a separate global positioning source (GPS), and periodically broadcasts it together with other data, such as aircraft identity and barometric altitude, enabling it to be seen by any adequately equipped agent (National Academies of Sciences, 2015). The technology has proven particularly attractive in locations, where previously no form of surveillance was physically possible or economically feasible. According to ICAO, ADS-B is now on track to replace conventional radar surveillance systems and become the backbone of next-generation ATM systems.

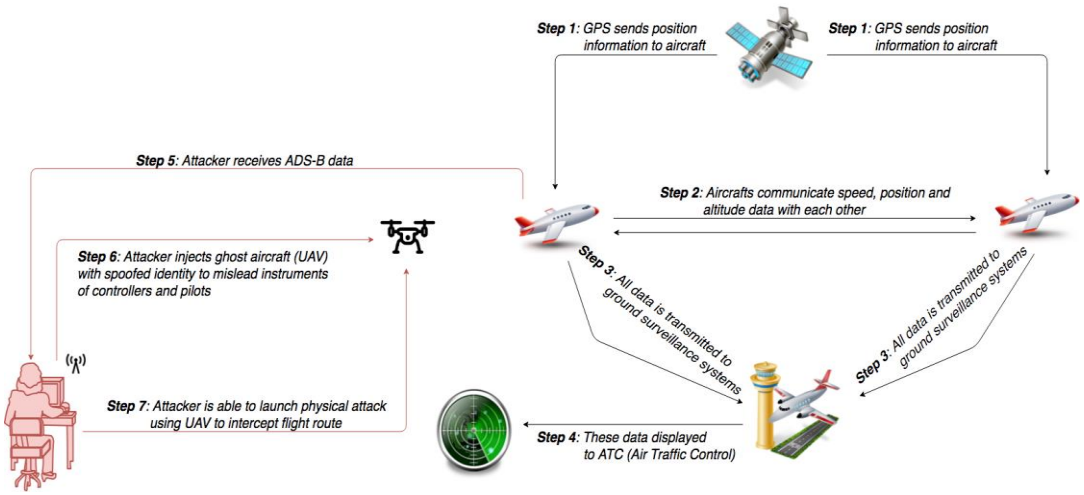


Figure 4.10. Communication attack on ATM systems

ADS-B avionics broadcast unencrypted, error-code protected messages over radio transmission links, approximately once per second, containing the aircraft's position, velocity, identification, and other ATM-related information (Cerchio & Riley, 2011). Since ADS-B signals are unauthenticated and unencrypted, "spoofing" or inserting a fake aircraft into the ADS-B system can be easily accomplished, as shown in Figure 4.10. Therefore, the system is susceptible to hacking, where attacks may range from passive actions (eavesdropping) to active attacks. The attacks can be implemented

using Universal Software Radio Peripheral, a widely available Software-Defined Radio supported by an ADS-B receiver/ transmitter chain with GNU Radio (Riahi Manesh & Kaabouch, 2017). Along with other researchers, Santamatra has recently published a white paper, presenting active attack scenarios that could result from the weak security posture of satellite communications, revealing how hundreds of in-flight aircrafts are accessible and vulnerable to message jamming, replaying of injection and other active attacks (Santamarta, 2018).

Impact Evaluation: With open broadcast data and no encryption there is no confidentiality protection for ADS-B communications. Lack of any authentication provides no integrity and the ability to jam signals brings into question availability. As a result, all security parameters may be impacted during such an incident. With air traffic services compromised, only reduced traffic capacity can ensure minimum safety standards. Such an incident happened in September 2017, at Sydney Airport and drove ATM system software failure at Sydney's Air Traffic Control (Abc Net, 2017).

Cascading effects: The most fundamental security issue with ADS-B is the core idea of broadcasting the identity and precise location of each aircraft, which could open the door for a terrorist to physically attack an aircraft either by using an Unmanned Aerial Vehicle (UAV) to intercept the flight route, or even by using a missile launcher to target aircraft of a specific airline or corporation. This has already happened in the past, like the incident in 2014, with a flight passing over eastern Ukraine, killing all 283 passengers and 15 crew on board (Weaver, 2015).

Mitigation Actions: The use of confidentiality and authenticity features in data traffic becomes mandatory. Therefore, cryptographic protection for ADS-B can be an effective mitigation action. It is also important for ground services to have any received data validated, by using legacy surveillance systems, such as primary radar information. Also, in ATM system's dependability is based on redundancies to ensure efficiency, reliability and continuity of operations. Therefore, Air Traffic Control (ATC) has to maintain in use current network of primary and secondary radars, as backup systems to ADS-B advanced technology. In addition, with the use of Wide Area Multilateration technology (WAM), data that show up on a controller's screen are multi-purpose validated by surveillance systems, so that spoofed targets are filtered out (SESAR JU, 2016).

Resilience Measures: It is important to regularly exercise ATC stuff and systems preparedness, response time and provide incident response capabilities. An effective contingency plan should be developed, implemented and tested, so that ATM resilience to be improved. Finally, communication of anomalous activity and

malicious attacks to Air Traffic Safety Electronics Personnel and law enforcement actions will help the airport to be better prepared and defend against similar attacks.

C) Malicious Attack: Malicious Software on an Airport's Network

Smart airports have complex wired campus networks that allow data access through secondary and tertiary levels of distribution. Having incorporated artificial intelligence systems to their daily functions and by allowing employees and maintenance personnel to use their owned smart devices (BYOD), they became more vulnerable to network malicious attacks. Moreover, aviation and ATM systems have increased the use of IP connections to enhance efficiency and interoperability, which may lead to unauthorized individuals gaining access (Suciu et al., 2018). Research experiments have shown that any malicious passenger or employee, equipped with a smart device infected with malware, may be able to access the aircraft's system and even influence system's integrity (Cerchio & Riley, 2011). Similar attacks can be accomplished with malware installation to the airport's website or intranet, where airport users' devices may be infected, thus giving the opportunity to malicious attackers to access airport's network and critical information system through these infected devices, as presented in Figure 4.11. Such an attack happened in September 2016, at Vienna Airport, where computer servers and employee's computers were infected with malware (The Local, 2017).

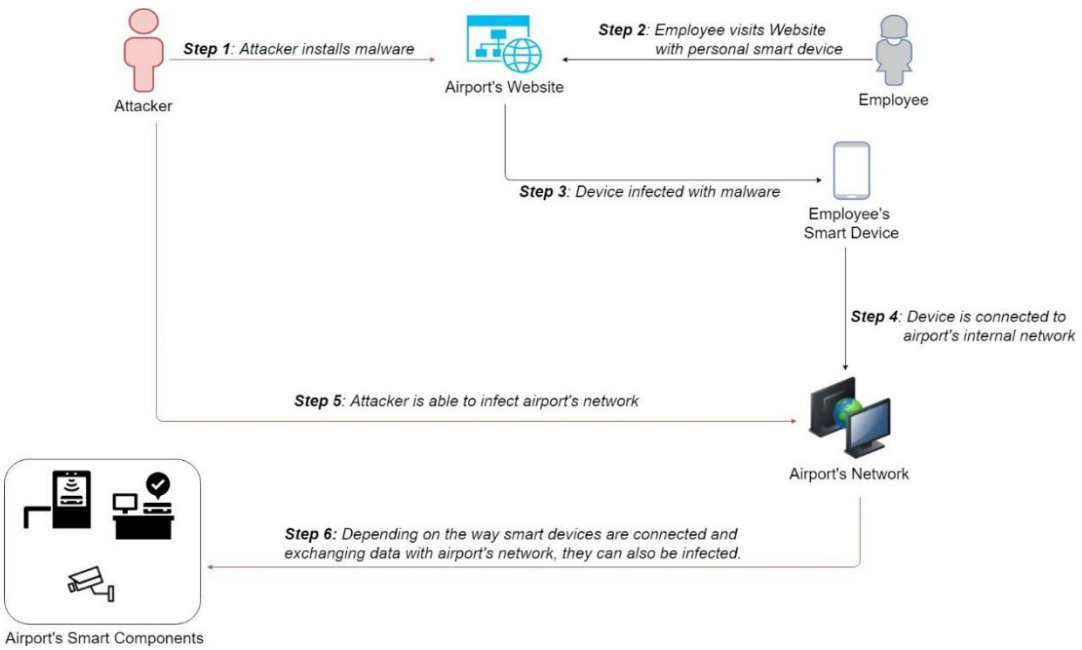


Figure 4.11. Malicious Software Installation

Impact Evaluation: Assuming that BYOD can be inserted in both conventional network and the restricted one of internal systems communication, in order to exchange information, a compromised device can impact airport systems integrity and availability. Since airports systems are interconnected to increase their interoperability, potential attacks on airport's network can cause network outage, flight cancellations, passenger delays, loss of confidence and financial damages. In the unlikely event that aircraft's avionics systems are also infected, attacker may be able to manipulate data from essential functionalities and services, which can jeopardize airplane safety parameters (K. Sampigethaya et al., 2011). While this attack can impact the availability and integrity of information and airport's resources, the impact on confidentiality has a lesser effect on the smooth operation of airport facilities. This does not mean that we should not bear in mind this impact and therefore implement appropriate countermeasures.

Cascading effects: Once an attacker gains access to airport network or even aircraft avionics systems, he may be able to control other components or applications connected to this system. Indicative examples are air navigation and air traffic control management systems, communications, aircraft collision avoidance systems and other aircraft management systems. Compromising either airport's or aircraft systems puts at serious risk essential services and facilitates further attacks that may lead to fatal accident and loss of human lives.

Mitigation Actions: For the adequate protection of smart airports, some of the basic countermeasures and BYOD controls, including antimalware and Intrusion Detection & Protection Systems (IDS/IPS), should be implemented. Moreover, smart airports should establish technical controls and organizational policies, in order to protect the infrastructure from potential risks coming from the employees' personal devices. In addition, strict control measures and severe access restrictions for BYOD on airport's critical systems or SCADA systems should be applied. Personnel security training and awareness is also vital for the ones, who are allowed to bring and connect their own devices, such as smartphones or tablets, to airport's systems. Finally, it is quite important that all the airport systems are designed and developed according to international security standards and best practices that drive at organization's sufficient security.

Resilience Measures: It is important all the software patches and hardware updates to be done on time, so as smart airport's systems to be kept up-to-date, with reduced exposure to common vulnerabilities. Moreover, the monitoring and audit of systems and log files are also crucial for the resilience of smart airports, because any unauthorized changes by malicious insiders should be immediately detected. IT stuff should always be efficiently trained and prepared to isolate infected systems, remove

malicious software, recover from new attack vectors, and gain experience from lessons learned.

D) Malicious Attack: Tampering with Airport Self-Serving Systems

Airline companies foster the use of Common Use Passenger Processing System (CUPPS) to facilitate 24 h/7 days a week customer support and speed up check-in and passenger control processes via automated smart devices. Self-serving check-in infrastructures are being installed nowadays, being used and shared by multiple airlines, along with third parties which also have started to operate common services. The majority of these devices run commonly used operating systems, firmware or proprietary software. Although these devices leverage intranet connectivity for accessing only content to company servers, they often provide remote management functionalities and they may be subject to tampering attacks, as they are exposed in public spaces. An attack scenario is exhibited in Figure 4.12. Such attacks can also affect various airport systems and SCADA equipment, from baggage handling and access control to air-conditioning and power distribution systems, which are widely distributed across airport infrastructures. While in the past these systems were air gapped, nowadays are networked and interdependent. Thus, smart airports are more likely to be victim of tampering attack, due to their adoption of IoT technologies. Los Angeles Airport has experienced a number of cyber incidents in the past, related to malware that targeted networked baggage systems (Gopalakrishnan et al., 2013).

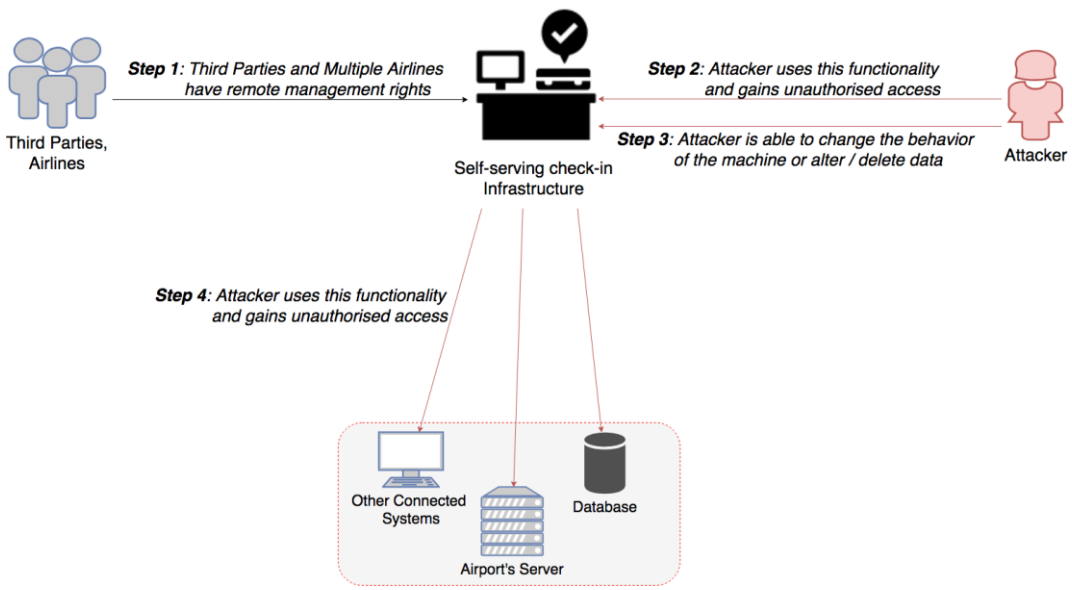


Figure 4.12. Tampering with airport self-serving systems

Impact Evaluation: Successful tampering can result in the attacker having unauthorized access to the machine and potentially lead to privilege escalation. This enables attacker to change the behavior of the machine, both in terms of the customer facing actions and the interactions with other connected systems. Such an attack happened at Iran's Mashhad Airport, in May 2018, where hackers took control of the airport's monitors, in order to express their support to Iran Protests (The Times of Israel, 2018). Disruption of CUPPS or SCADA systems may create inconvenience to passengers and impact airport's services availability and operational efficiency, such as creating flight cancellations, long passenger waiting queues and longer boarding times . It can also impact integrity of information, for example facilitate the boarding of unknown passengers into the plane and lead to more serious security risks involving safety. Last but not least, tampering on airport devices may impact privacy and data protection, where privilege escalation can lead to loss of personal or sensitive passenger's data, such as passport, identity or credit card details.

Cascading effects: Once an airport CUPPS or SCADA devices are compromised, the attacker may be able to infect other interconnected systems and related databases. The lack of logging and forensic capabilities of such systems prevents early diagnosis and response, undermining trust on system's provided services. Except from any interruption of the provided service operation, a threat that arises here is the alteration of data, aiming at whatever act can compromise the safety of passengers, including potential terrorist facilitation. Although the majority of airports use segregated networks, depending on the effectiveness of the controls, cascading effects have the potential to impact the secure operation of Airside and Landside operations.

Mitigation Actions: The most important mitigation action is to restrict usage of external media drives or wireless connections, disable unused services, so as to minimize equipment communication ports. Also, it is vital to provide along with network segmentation, the adequate physical security. Users shall ensure that unattended equipment has appropriate protection either with security guards, video monitoring or surveillance systems. Moreover, data encryption can minimize privacy risks, while Intrusion Detection & Prevention Systems (IDS/IPS) can support early detection and prevent further impacts on airport operational systems.

Resilience Measures: It is important to provide backup systems, which can be activated to support business continuity in case of such an incident. Basic security awareness training to all airport employees could prevent unauthorized access to these devices, while incident response capacity building for ground staff should be introduced and regularly tested. Finally, an effective contingency plan should be developed, implemented and tested to improve airports operational resilience.

E) Malicious Attack: Network attack to CCTV systems

Digital surveillance systems are integrated nowadays with new ways to speed up airport processes and detect threats, including radio frequency identification (RFID) tags for tracking purposes, new thermal imaging scanning devices, intelligent closed-circuit television (CCTV) programs that identify unusual behavior and devices to detect chemical substances. Digital surveillance and CCTV developments include video analytics nowadays, to increase the functionality and effectiveness of both CCTV and access control systems, while solving the inherent difficulties caused by the sheer size of airports and their perimeters. CCTV systems are becoming increasingly interconnected and interdependent with other airport information systems, introducing additional vectors of attack, due to their interconnectivity. Thus, CCTV systems can be exposed to similar vulnerabilities as computers and networked devices. Specifically, weak network security may allow attackers to open a backdoor and exploit software vulnerabilities, which can enable the attacker to gain unauthorized access, as presented in Figure 4.13. Malware could also be uploaded during patching and with the collaboration of compromised employees (i.e. insider threat). A successful attack on CCTV systems would then allow an attacker to monitor all physical airport infrastructures.

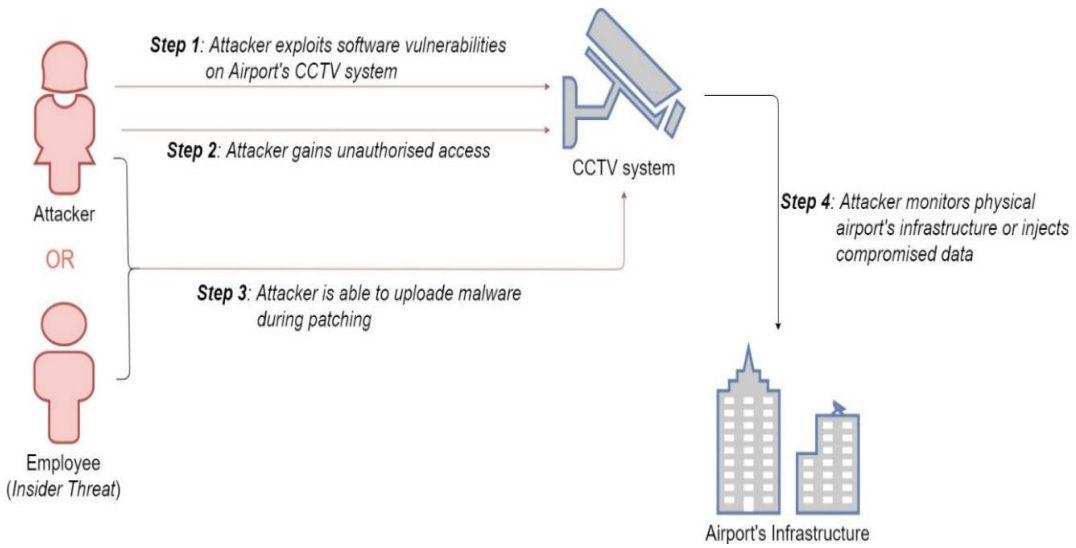


Figure 4.13. Network attack on CCTV systems

Impact Evaluation: Compromised CCTV systems impact airport operation safety both in landside and airside areas, which affects all security parameters: confidentiality, integrity, and availability of security systems. In addition, in case that system administrators had to wipe the infected systems and reinstall the CCTV

software, it is possible that a good deal of footage to be lost and the system will be rendered inoperable for a time, which creates a serious safety handicap.

Cascading effects: Once a malicious actor has gained control of any CCTV device, this could lead to catastrophic impacts on airports safety. After a hacker has gained control, he could use the camera for hostile reconnaissance, or inject his own video stream, or even he could use the device to pivot into other devices on the same network; all of which would cause serious problems in airport security and airside operations safety.

Mitigation Actions: The first mitigation measure is to avoid connecting any CCTV device directly to the Internet, since cameras or CCTV systems, which can be remotely accessible with port forwarding all inbound traffic, are quite vulnerable to malicious attacks. Effective measures are the use of VPN (Virtual Private Network), use of non-standard network ports, while enabling dual factor authentication controls, when using a remote access service. Change of default passwords in all devices is one of the basic precaution actions, along with disabling unused services and closed equipment communication ports. Also, it is vital to provide adequate physical security to remote devices with security guard patrols especially in the perimeter of the airport installations, which can be the Achilles heel (weak point) for airport's safety.

Resilience Measures: It is important to provide redundancies, by keeping legacy systems in standby mode, being activated when needed to support any relevant incident. Efficient security training to all airport employees could make difficult any attempt to interfere with CCTV systems, while incident response capabilities for security staff should be developed and regularly tested. Finally, an effective contingency plan should be developed, implemented and tested to improve airports resilience.

F) Malicious Attack: Misuse of Authorization

Disgruntled employees, contractors or business associates having in possession access credentials may are able to misuse their authorization privileges and act as insider threat, aiming to steal information for personal gain or to benefit another organization. In addition, an intruder may gain access to airport's network, using Advanced Persistent Threat (APT) as presented in Figure 4.14, remaining undetected for an extended period, while escalating authorization privileges. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization. To maintain access to the targeted network without being discovered, threat actors use advanced methods, including continuously rewriting malicious code to avoid detection and other sophisticated

evasion techniques (Reis, 2016). Some APTs are so complex that they require full-time administrators to maintain and restore the compromised systems and software in the targeted network.

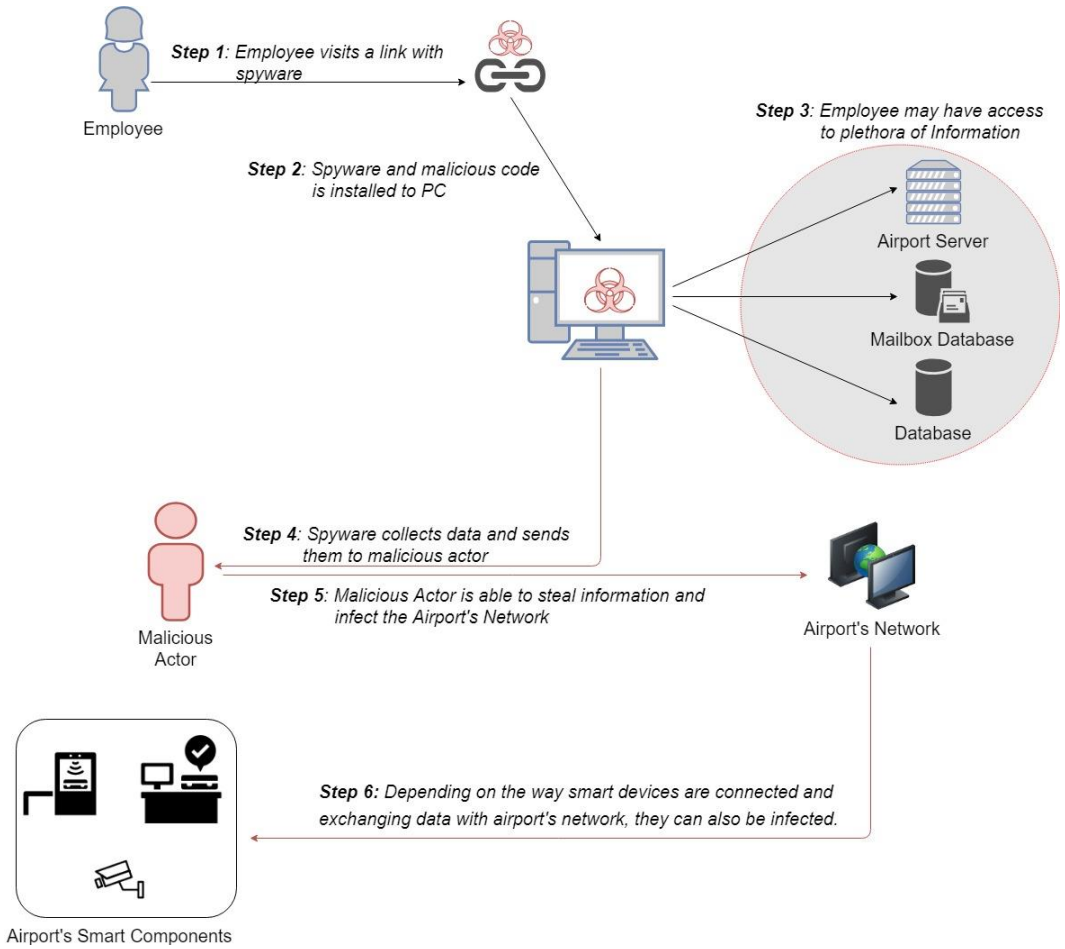


Figure 4.14. Misuse of authorization with APT

Impact Evaluation: Data which may be extracted are related to airport management and thus containing critical information for instance about airport vulnerabilities, airlines operation data or even passenger personal information. This can lead to large penalties, fines and loss of confidence. Data protection laws applicable worldwide, like the European General Data Protection Regulation (GDPR), provide severe penalties of up to 4% of company's global turnover. Such an incident happened in 2018 with British Airways, where personal and financial data of approximately 380.000 customers were exposed. The airline admitted this data breach, while claiming that between those data weren't any passport details or other sensitive personal data (USA Today, 2019). With compromised airport's administration

systems, there is a serious impact on operational safety both in landside and airside areas, which affects all security parameters: confidentiality, integrity and availability of airport's essential services and operational systems.

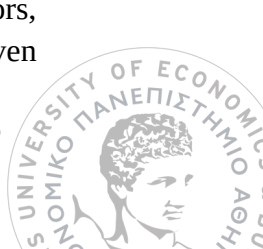
Cascading effects: Since the infected device may have access to plethora of information, privilege escalation from threat actors, who have breached their target systems, including gaining administrator rights, offer them the ability to move around the enterprise network at will (Suciu et al., 2018). Additionally, they can attempt to access other servers, as well as other secure areas of the network, facilitating their malicious indents and targets. Compromising airport's systems puts at serious risk essential services and facilitates security attacks, causing civilian fatalities and serious financial losses.

Mitigation Actions: An effective user access management should be in place for granting and revoking access to all information systems and services. In addition, the use of utility programs that might be able to override system and application controls shall be restricted and tightly controlled. A variety of countermeasures are also necessary, including data encryption and antimalware, in order to mitigate such attack's impacts (Stergiopoulos, Vasilellis, et al., 2016b). Airport's cybersecurity team should focus on detecting anomalies in outbound data to see if the network has been the target of any APT attack.

Resilience Measures: The continuous monitoring and audit of systems and log files are crucial for the resilience of smart airports, since the data loss prevention is enhanced. Thus, any unauthorized action made by malicious insiders is immediately detected and appropriate actions are implemented. Moreover, airport's employees and business associates should be granted the least level of privilege, and should be able to access only information that is needed, according to their working position and duties. Efficient security awareness and training to all airport employees could harden authorization misuse attempts, while incident response capabilities for security staff should be developed and regularly tested.

G) Malicious Attack: Email Phishing and Social Engineering Attacks

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. It is a confidence trick for the purpose of information gathering, fraud, or system access (Reis, 2016). Phishing is typically carried out by email spoofing or instant messaging, which often directs users to enter personal information at a fake website, identical to the legitimate one. Social Engineering and communications, purporting to be from social web sites, banks, online payment processors or IT administrators, are often used to lure victims. Such a scenario attack is presented in Figure 4.15. Even



though organizations can install filtering capabilities, phishing emails still may get through, since phishers can use images instead of text to make it harder for anti-phishing filters to detect them. Hackers are spoofing email sender addresses from major companies and services, tricking recipients into thinking the malicious message is from a known source. Also, evil-twins is a phishing technique, where phisher creates a fake wireless network, that looks similar to a legitimate public network. This can be found in an airport and whenever someone logs on to the bogus network, fraudsters try to capture passwords and/or credit card information.

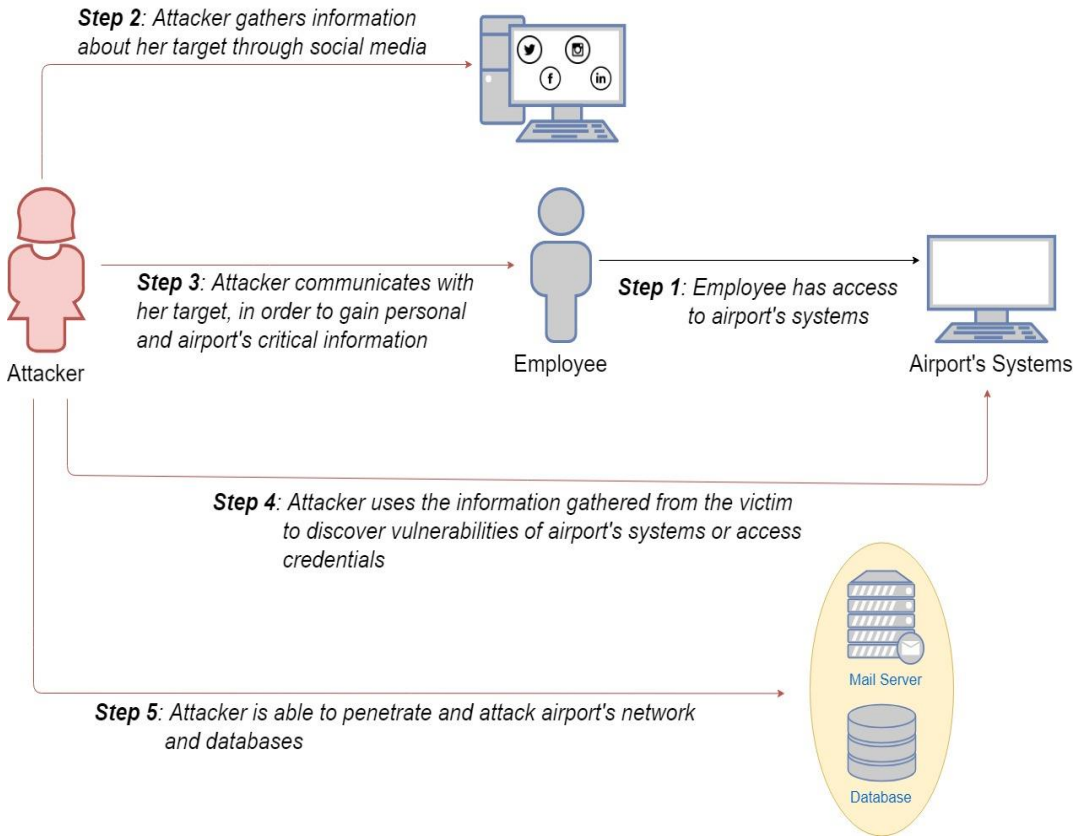


Figure 4.15. Social engineering attack scenario

Impact Evaluation: Depending on the network privileges of IT devices all security factors can be serious impacted such as confidentiality, integrity and availability of airport operations. The degree of harm phishing attack is likely to cause is dependent on attacker's motivation and victim's organizational position and access privileges. A recent cyber-attack example, where ransom was attacker's motive, happened in September 2018, at Bristol Airport. As a result, the airport's information screens failed to operate for two days (Adams, 2018).

Cascading effects: Once airport's authorization clearances and user access systems are compromised, the attacker depending on his motives can penetrate and attack other connected systems. Data alteration aims at whatever malicious act can compromise airport administration systems, where Airside and Landside operations may be infected causing passenger delays, cancelled flights and finally can jeopardize civilian's safety, including potential terrorist facilitation.

Mitigation Actions: The mitigation actions require a combination of technological, process, and people-based approaches. These actions include anti-spoofing control, filtering, dual authentication, malware protection and other technical security measures. In addition, user training, security awareness, encouraging employees to "Think before clicking a link" and being suspicious regarding emails that look strange or very attractive, including invitations from social media. Email addresses should be carefully examined and filtrated, while IT security team should be notified accordingly. It is obvious that many infiltration attempts could be stopped as a result of recipients being suspicious, mistrustful and paying more attention.

Resilience Measures: Phishing and social attacks work by exploiting weaknesses in human psychology and organizational culture. With security awareness and employees' training, it is feasible to create an environment, which empowers users to report incidents for helping and increase the reporting rate of suspicious emails. These incidents can be further investigated with the use of virtual environments and sterile sandboxes, so as to inform and alert all airport stakeholders, as well as increase systems cyber resilience.

Smart Airport's Malicious Attack Scenarios Synopsis

In order to facilitate airports stakeholders and cyber-security researchers to aggregate information exhibited in these cyber-attack scenarios, we have condensed information into a synoptic table. Table 4.4 summarizes this collection of malicious attack scenarios, presenting for each malicious threat which categories of assets may be affected, cascading effects, along with mitigation actions and resilience measures that can be taken, in order to improve airports cyber security and cyber resilience.

Table 4.4. Smart Airport's malicious attack aggregate analysis

Malicious Attacks for Smart Airports				
THREAT DESCRIPTION	**Assets Infected**	**Cascading Effects**	**Mitigation Actions**	**Resilience Measures**
DDoS	- Web Services - Network Services - ATM communication -Wireless communications -Mobile telephony	-Airline/Airside Operations -Landside Operations -Airport Interoperability -IT and Comms	-Intrusion Detection/Protection (IDS/IPS) -Security hardening of systems -Firewalls, network segmentation - Volumetric protection from ISP	-Provide incident response & contingenc plan - Regularly exercise preparedness - Communicate anomalous activity to airport stakeholders
TeleCom Attacks	-Air Traffic Control (ATM) -Communications, Navigation and Surveillance -Global Positioning System -Geographic Information Systems (GIS)	-IT and Comms -Airside Operations -Management of flight operations	- Intrusion Detection/Protection -Anti spoofing Control -Strong user authentication - WAM for ATM systems - Law enforcement in case of incident - Data encryption	-Provide incident response capabilities f airports (including airlines) -Maintain Communication BackUp Alternatives fully operational
Malicious Software	-Network and IT systems -SCADA Systems -Staff smart devices -Passenger IT devices -Operational Servers	-Airline/Airside -Landside Operations -Passenger Management System -IT and Comms -Safety and Security	-Intrusion Detection/Protection (IDS/IPS) -Antimalware & technical control -BYOD controls -Least privilege access manag. -Software and hardware updates -Application security and secure design according to Inter.Stds	-Provide incident response & contingenc plan -Develop forensic analytic capabilities - Regularly exercise preparedness and response time on test incidents - Security Awareness and Training
Tampering with Airport Devices	-Common Use Passenger Processing Systems -Baggage Handling -Passenger Ticketing System	-Local Area Network -Landside Operation Systems -Passenger Management	-Resctrict Usage of Ext. Devices - Intrusion Detection/Protection - Data Encryption - Enhance Physical Security and Surveillance systems	- Provide BackUp Alternatives - Monitor risk effectively - Regularly exercise incident response of airport staff - Implement Contigency Plan
Network Attacks	-ICS SCADA -CCTV systems -Baggage handling -Landside Operations	-Facilities and Maintenance -Airside Operations -Landside Operations -Baggage handling -IT and Comms	-Firewalls, network segmentation and defence in depth - Intrusion Detection/Protection -Strong user authentication -Change default administrator credentials of devices -BYOD controls -Data encryption	- Provide BackUp Alternatives - Monitor risk effectively -Develop forensic analytic capabilities - Provide incident response capabilities f airports - Implement Contigency Plan - Security Awareness and Training
Misuse of Authorisation	-SCADA systems -Air Traffic Management -Enterprise Management System -Access Control & Surveillance -IT Systems	-Facilities and Maintenance -Airport Administration -Airline/Airside Operations -Landside Operations	-Change default credentials of devices -BYOD controls -Software and hardware updates -Least privilege and data classification -Data encryption -Strong user authentication -User access management	-Provide incident response capabilities -Develop forensic analytic capabilities - Regularly exercise preparedness and response time on test incidents - Implement Contigency Plan - Security Awareness and Training

4.1.9. Malicious Attacks Motives

In this section, we introduce the attacker's motivation into our scenario analysis, since people, while performing a malicious action, may fall on a subjective spectrum of good and evil. According to Safe Skies research (PARAS, 2019) motives of cyber attackers fall into four general categories, all of which can reduce airport's operational efficiency, as listed below:

1) Political or Military: Foreign military or intelligence-related sources have the competences to conduct the most serious and harmful attacks. Their purpose is to gain some military, political, or strategic insight, affecting confidentiality, integrity and availability of systems to undermine public trust. Airports are highly symbolic and attractive targets for such attacks, where any disruption, impacts confidence in air traveling and national airspace safety.

2) Commercial Espionage: Attackers with commercial espionage motivations are usually aligned to steal or damage confidential or proprietary information in order to gain commercial intelligence from private and public companies. This kind of attack aims to defraud, blackmail, obtain financial gains or targets corporate strategic goals. Examples of such commercial espionage targets are airports' administration documents, including planning, construction, budget, financial, legal and government-related documents.

3) Peer Group Disruption: Peer groups such as vandals, activists, or outsiders, along with a wide variety of individuals may engage in cyber-attacks, in order to disrupt or disable access to resources. They usually claim to have political reasons such as to protest, create economic harm, or rise status within their peer group. Distributed denial-of-service attacks are common examples in the airport environment, where attackers strive to prevent access to airport's website or disrupt online services.

4) Cybercrime: Attackers usually target networks and systems directly for data, in order to steal and resell valuable data, such as customer identification, credit card, or banking information. This is one of the most rapidly growing areas of attacks nowadays. Airports that handle credit card information for paying services, such as baggage fees or parking allotments could be prime targets for these attackers. Although these attacks may be less sophisticated than the other types, cybercrime techniques and tools have been recently improved and become easier to obtain and use. For example, by using ransomware or destructive malware, attackers are able to encrypt or even destroy data and afterwards threaten their victims to pay a great amount of ransom (usually in bitcoins), in order to unlock data or refrain from exposing sensitive information.

Table 4.5. Malicious attack motives analysis

Scenario No	Malicious Attack Scenario	Impact on			Malicious Attack Motives			
		Confidentiality	Integrity	Availability	Political or Military	Commercial Espionage	PeerGroup Disruption	Cybercrime
1	Distributed Denial of Service attacks			√	√		√	√
2	Communication attack to ATM systems	√	√	√	√	√	√	√
3	Malicious Software on Airport's Network	√	√	√	√	√		√
4	Tampering with airport self-serving systems	√	√	√	√		√	√
5	Network attack to CCTV systems	√	√	√	√	√	√	√
6	Misuse of Authorization		√	√	√		√	√
7	Email Phishing and Social Engineering Attacks	√	√	√	√	√		√

Table 4.5. attributes to malicious threat scenarios discussed, the cybersecurity impact on assets according to the CIA triad (Confidentiality-Integrity-Availability) and the categories of cyber attackers who may be evolved in such malicious actions, according to their motives.

4.1.10. Summary of Research Work

In this research, we have outlined how technological advances and IoT technologies may change the security threat models in aviation and influence the operational efficiency of smart airports. In order to extract information from airport security professionals, about their cyber-security efforts and risk management activities, we started our research with an online survey for airport's cybersecurity.

However, we confronted a decline from participants to fully complete the survey and provide detailed information about their cybersecurity implemented practices. This was a survey limitation, therefore, online desktop research for each airport's technological situation and related work on cybersecurity best practices have also been investigated.

This study focused on cyber-attacks that may occur from malicious actions as the incorporation of smart applications in airports introduces new vulnerabilities. With the motive to increase cyber security awareness to all airport's stakeholders, we have tried to expose in a simple and understandable way, key issues of cyber security in smart airports.

Commercial airports are required to develop their own policies to enhance cyber security, nowadays, since our survey has revealed that there is a large variation in the way airports implement measures to protect networked infrastructures and design cybersecurity solutions. Due to the fact that each airport has a variety of ICT applications, being operated within the airport perimeter, the resulting cyber security landscape has become very large and complicated.

Our research also revealed the disparity amongst airports in the methods and the degree of applying cyber security best practices. While smart airports are having a more mature cyber security posture, basic airports seem to have limited resources dedicated to cyber defense and resilience. Technical based cybersecurity practices have a better implementation rate for all airport categories, while organizational practices, policies and standards keep lower levels of implementation, including low levels of cyber security awareness and training prioritization.

Although smart airports perform the majority of good practices examined in our survey, security gaps have been revealed. Besides, the rapid advance of IoT technologies, along with the slower pace of the required regulatory processes, may lead to serious legal gaps for confronting malicious threats in smart airports. These gaps might pose challenges to smart airports for addressing security and safety.

Ultimately, as our survey revealed, main security concern to all responders was security awareness. To this conclusion adds the fact that most malicious attacks are launched, due to untrained personnel in security issues. Therefore, the above analysis of attack scenarios, based on malicious intentions, can be supportive to airport community and aviation stakeholders to understand the meaning of acting proactively by implementing best cybersecurity practices.

There is a need for identification and development of airport trust framework, helping operators navigate their trust relationships and indicate how smart devices and operators exchange data and operate together. Another important finding of our research was the growing need of educating IT experts and providing specialized advanced training in cybersecurity areas, in order to increase cybersecurity preparedness. Moreover, promoting security awareness of passengers and airports' personnel on the risks posed by new IoT technologies is essential.

Securing Smart airports, against evolving cyber threats, is a shared responsibility for all aviation stakeholders, including commercial airports, airlines, business associates and regulators. As a result, a collaborative cyber-resilience model, which defines the appropriate cyber security posture for airports, is quite important nowadays. Airport operators ought to prioritize cyber security initiatives, in order to ensure safety of operations for airlines, passengers and public in general. Cyber threats and related risks will continue to grow, along with technological developments, while the relationship between safety and security in the aviation context will become more interdependent.

4.2. Aviation cybersecurity and cyber-resilience: assessing risk in Air Traffic Management

4.2.1. Introduction [7]

Civil aviation is the safest transport mode in the world and probably also the most interconnected system of information and communication technology. Cyber-attacks are increasing in quantity and persistence, so the consequences of a successful malicious cyber-attack on civil aviation operations could be severe nowadays. New technologies, extension of connectivity and their integration in the aviation industry, especially in the field of Air Traffic Management (ATM), increase the risk to these critical assets. This subsection examines cyber security challenges and interoperability in ATM systems. We propose an extended threat model for analyzing possible targets and risks involved. We also introduce and analyze cyber resilience aspects in the aviation context and the need for holistic strategy of defense, prevention and response. Under the resilience umbrella, all actors should work on collaborative, risk-based framework to address security threats and increase the aviation systems resilience against future attacks.

Security threats to civil aviation operations have become more sophisticated and challenging. One that is emerging in the recent years and arguably even more advanced and complicated to manage is cyber-attack. Today, the global civil aviation community is relying on computer based and information technology (IT) systems for their daily frontline and backroom operations. This reliance is expected to grow as new and modern airports are developed, new aircraft introduced into service and stakeholders seek to meet the growing demand of the more IT-savvy passengers with new passenger facilitation processes, using digital and IT-based systems.

Aviation is a key foundation for international trade, tourism, and investments crucial to the global economy development. The air transport industry supports 2.7 trillion dollars or 3.5% of the world's gross domestic product (GDP) providing 9.9 million direct jobs within the air transport industry (Industry High Level Group, 2017). According to the latest traffic forecasts, by 2034, both air passenger and air freight traffic are expected to double, compared to 2016. Passenger traffic is expected to

[7] *Related Publication:* Lykou G., Iakovakis G., Gritzalis D., "Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management", in Critical Infrastructure Security and Resilience, Gritzalis D. et al. (Eds.), pp. 245-260, Springer (Advanced Sciences and Technologies for Security Applications), 2019.

overpass 14 trillion revenue passenger-kilometres (RPKs) with a growth of 4.5 per cent per annum, and freight will expand by 4.2 per cent annually over the same time period, reaching 466 billion freight tonne-kilometres (FTKs) (Industry High Level Group, 2017).

The use of Information Technology in civil aviation has also increased exponentially in the last years. Digitalization, technological tools and systems often connected to the internet increase intelligence and interoperability on one hand, while on the other they may constitute serious risks for aviation cyber security. Therefore, it is necessary to keep a high level of attention and awareness on possible future developments of the cyber threat (Zan et al., 2016).

The overall aim is to reduce the vulnerability to cyber-related risks, to strengthen the air transportation systems resilience against cyber threats, which is seen as the capability of an organizational and technical system to protect itself from failures or losses, to mitigate impacts by adapting to changing conditions and to recover from degradation after the incident (Kiesling & Kreuzer, 2017).

This work looks at some of the challenges and concerns about cyber security threats in the aviation sector. While in previous work (Lykou et al., 2018b) we have focused our concerns on the ground, analyzing cybersecurity measures and best practices to improve airports cyber resilience, in this research we present advanced services in surveillance systems of Air Traffic Control with the aim to address existing vulnerabilities and dependencies. Our purpose was to introduce and analyze resilience aspects in the aviation sector and then classify already proposed resilience recommendations, based on their technical, organizational, social, and economic dimensions.

The remainder of this work is organized as follows: Subsection 4.2.2 examines ATM interoperability and recent advances in surveillance systems. Subsection 4.2.3 briefly presents related work on aviation cybersecurity and introduces an extended model with cyber-threat agents in the aviation sector. Security measures are presented in subsection 4.2.4, while subsection 4.2.5 introduces resilience aspects within the aviation context and analyzes existing in literature resilience proposals on several dimensions. Finally, subsection 4.2.6 concludes resilience analysis and benefits for the aviation sector.

4.2.2 Understanding ATM Interoperability

In order for Air Traffic Control (ATC) to safely manage airspace, each ground located air traffic controller needs to understand the status of each aircraft under their control. Traditionally, Primary and Secondary Surveillance Radar in various layouts have

supported air traffic surveillance and management for decades. Both systems were designed at a time when radio transmission required a great financial investment and expertise. Hence, no security thought was given to these legacy systems, since it was presumed that they would remain out of reach. The rise of Software Defined Radio (SDR) voided this assumption and marked the shift from potential attackers being well resourced to those with much less resource and capability (Strohmeier et al., 2014).

The ongoing move from traditional air traffic control systems, such as radar and voice, towards enhanced surveillance and communications systems using modern data networks, has caused a substantial shift in the security of the aviation environment. Implemented through Aviation research programs like the Single European Sky ATM Research (SESAR) and the US American NextGen programs, several new air traffic control and communication protocols are currently being rolled out that have been in the works for decades (Strohmeier et al., 2016).

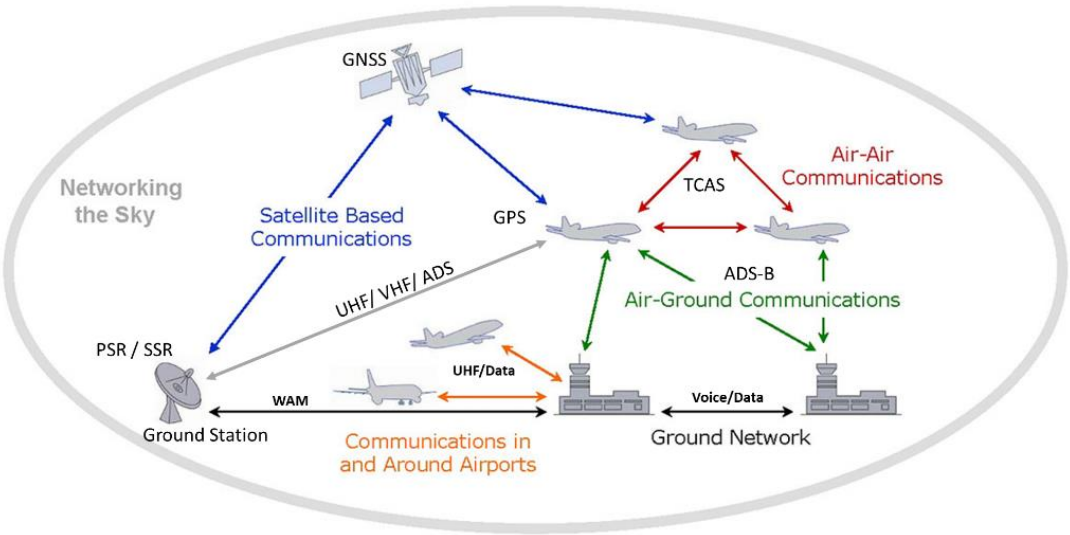


Fig. 4.16. ATM interoperabilities

In this section, we briefly describe the basic ATM systems serving surveillance and interoperability, used for air traffic control such as: Primary and Secondary Surveillance Radar, Automatic Dependent Surveillance-Broadcast, Traffic Collision and Avoidance System, and Wide Area Multilateration. All these systems interact with each other as graphically presented in Figure 4.16. Then we discuss how recent advances in wireless technologies have changed the threat landscape in the aviation context.

Primary Surveillance Radar (PSR) describes non-cooperative radar localization systems. In civil aviation, these typically employ a rotating antenna radiating a pulse position-modulated and highly directional electromagnetic beam on a low GHz band. Potential targets in the airspace reflect the pulses and measurement of the bearing and round-trip time of these reflections provides the target's position. Whilst PSR is not data-rich, it is relatively hard to attack as it relies on physical properties (Strohmeier et al., 2017).

Secondary Surveillance Radar (SSR) is a cooperative technology with modern communication versions, including the so-called transponder modes. SSR provides more target information on ATC radar screens compared to PSR. Ground stations interrogate aircraft transponders using digital messages on the 1030 MHz frequency, which reply with the desired information on the 1090 MHz channel. Commodity hardware can receive and transmit on these frequencies, making them accessible to attack (Costin & Francillon, 2012). Mode S is a particularly important for the current SSR system. It supports systems of increasing significance in modern aviation surveillance, in conjunction with multilateration techniques to provide redundancy. Being intentionally designed with lack of confidentiality, all SSR systems are subject to eavesdropping attacks by passive observers.

Automatic Dependent Surveillance-Broadcast (ADS-B) is a protocol in which aircrafts continually broadcast their own ID, position and velocity as well as further information such as intent or urgency codes. These broadcasts do not require interrogation but independently send the aircraft's position and velocity twice a second and unique identification every 5 seconds; ADS-B is currently in the roll-out phase and it is mandated for use by all aircraft from 2020 in all European and American airspace (Strohmeier et al., 2016).

Traffic Collision and Avoidance System (TCAS) allows aircraft to interrogate nearby aircraft, in order to resolve airspace conflicts. For example, should another aircraft come within some predefined range, TCAS will initially produce a Traffic Advisory notifying the pilot of traffic nearby. Should the intruder enter the immediate airspace of the aircraft, an alarm will be produced which instructs one of the aircraft to change course. Since the 1st December 2015, TCAS is mandated for inclusion on civil aircrafts carrying more than 19 passengers or with a minimum take-off weight of 5,700kg (EASA -EU, 2011).

Wide Area Multilateration (WAM) is particularly useful for ATM since it allows location estimation of an aircraft using 1090 MHz messages over large areas. WAM, combined with ADS-B, will form a key part of the next generation surveillance technologies and can help to detect unusual ADS-B reports. Due to the number of

sensors and data processing equipment required to cover large areas, the cost of installation is very high, which makes WAM quite hard to attack.

To aggregate information, all the above surveillance systems of Air Traffic Management with discussed characteristics, dependencies and vulnerabilities are presented in Table 4.6.

Table 4.6 Main characteristics, dependencies and vulnerabilities of ATM systems

System	Ground/Air Dependent	Deployment Status	Technology	Dependency	Vulnerability
Primary Surveillance Radar (PSR)	Ground	In use	Measure the bearing and distance of targets using the detected reflections of radio signals	Airplane target independent	Not IT related
Seconday Surveillance Radar (SSR)	Ground	In use	Requests additional info from aircraft like identity, altitude, speed	Targets equipped with transponder	Eavesdropping
Traffic Collision and Avoidance System (TCAS)	Air	In Use / Mandatory since 2015	Target identity interogation	Targets equipped with transponder	Eavesdropping, jamming, spoofing
Automatic Dependent Surveillance-Broadcast (ADS-B)	Air	Mandate by 2020	Targets broadcast infromation about identity, altitude, speed	Targets equipped with transponder	Eavesdropping, jamming, spoofing
Wide Area Multilateration (WAM)	Ground	In deployment	Combines ADS with RSR SSR Data for robustness	Central Proccesing IT based information	Data proccesing and IT related

4.2.3 Aviation Cyber Threat Agents

Although air transportation has a long history of risk management with a special focus on safety and physical security, the field of cyber risks has recently introduced a new landscape of threats. In 2016, at the 39th Assembly, International Civil Aviation Organization (ICAO) has announced preparation works on cybersecurity and cyber resilience. In this direction, Chapter 18 of the Aviation Security Manual which deals with cyber threats has been updated in September 2017. Moreover, Aviation Security Manual (Doc 8973) was enhanced to provide guidance, including minimum measures, to protect critical information systems against unauthorized access and use (ICAO, 2017).

In addition, recent research studies revealed that cyber threat will most likely be one of the main security issues in aviation, since according to SESAR and NextGen programs the overall air transport system will massively migrate to an IP based infrastructure and operate in accordance with network centric operations concept, with real-time information sharing. As a critical resource, information must be treated like any other critical asset which is essential to the efficiency and successful delivery of ATM systems.

In the area of aviation cybersecurity, research work has shown that complexity and criticality of information security and its governance demand the highest organizational security level. Civil Air Navigation Services Organization has issued in 2014 a guidance for Cyber Security (CANSO, 2014a) explaining how air navigation service providers should take into account for cyber security in air traffic management, including cyber threats and risks, motives of threat actors, as well as some considerations to managing cyber risks and implementing a cyber-security program. A vulnerability assessment framework for wireless threats in Aviation Cyber-Physical Systems (ACPS) has been proposed by (Kumar & Xu, 2017) evaluated the tools and used them in their framework to assess the various threats associated with ACPS. Sampigethaya et al. (2009) presented a comprehensive survey of security of the e-enabled airplane with applications such as electronic distribution of loadable software and data, as well as future directions such as wireless networked control and airborne ad hoc networks..

During their study, Stander & Ophoff (2016) found that steps are taken by aircraft manufacturers and controlling bodies to prevent the occurrence of incidents as to compromise the information systems of an aircraft. The key to ensuring security would be to keep up with the developments thereby being in a position to confront the threats rather than evoking responsive action after its occurrence.

Strohmeier et al. (2016) have presented a realistic threat model based on the up-to-date capabilities of different types of threat agents and their impact on a digitalized aviation communication system, where threat agents are classified based on their motivation and capabilities. We have extended this model by adding a new threat: “the insider”. We strongly believe that this actor remains a considerable threat agent, not to be neglected from the scheme. We have also estimated risk exposure, taking into account implemented security controls and available security solutions and countermeasures, already proposed in literature. Table 4.7 presents this extended taxonomy applicable to wireless security in aviation ATM systems and we briefly describe each threat agent characteristics:

Passive observers exploit the open nature of air traffic communication protocols. They use public and private websites and mobile applications, which display air traffic and its communications in real time, to gather information about private or secret air traffic movements. Alternatively, they can employ cheap SDR receivers to gather their own undistorted picture of all air traffic in their vicinity, in real time or stored for later analysis. The information collected can be exploited in many ways, ranging from privacy concerns to the detection of military operations. The risk exposure of ATM systems in such threat agents is rather low, due to no offensive capabilities in the aviation industry.

Activists and hobbyists are the lowest active threat in our model, based on their abilities concerning both hardware and knowledge. Their aim is to exploit security holes with existing, easy-to-use attacks with typically low sophistication and they are able to monitor and interfere to aviation communication channels. Their motivation is regularly not rational, instead any identifiable impact is sought for publicity, thrill and recognition (Stouffer, Pillitteri, et al., 2015). The risk exposure of ATM systems in such threat agents is considered low, since they can be detected and mitigated with the use of back-up surveillance systems.

Insiders can be a serious threat and are often disgruntled employees, former employees, contractors, or even business associates. These users have inside information of the organization's security practices, data, and computer systems. Insiders can be be greedy, malicious or unpredictable in their motivations. The fact that an insider has access to key applications and other critical systems makes him potentially even more dangerous than third-party cybercriminals who try to break in through malware and other mechanisms. Therefore, risk exposure of ATM systems is medium since it is really hard to promptly detect insider's malicious intent or actions.

Cyber-crime attackers usually seek to attack systems for monetary gain, having a sufficient knowledge, using software-defined radios, and even small unmanned aerial vehicles (UAV), being able to inject new messages or modify existing ones in such ways that they are not flagged by current detection systems. They try to cause maximum damage and exert credible threats, as a pre-requisite for blackmail or to take advantage of inside knowledge. Consequently, they are seeking to exploit any possible and effective way to attack Air Traffic Control and aircraft systems. The risk exposure of ATM systems is medium and should be seriously taken into consideration in regular performed risk assessments.

Table 4.7. Threat Agents in Aviation systems

Threat	Resources	Goal Motivation	Capabilities	Hardware Cost	ATM Target	Risk
Passive Observers	Very low	Information collection Financial or personal interest	Eavesdropping, use of website & mobile apps.	Internet access, SDR receiver stick ($10)	ADS-B	Low
Hactivists & Hobbyists	Low	Any noticeable impact Thrill and recognition	Eavesdropping, replay attacks, denial of service.	COTS SDR transmitter ($300-$2.000)	ADS-B	Low
Insiders	Low - Medium	Disgruntlement, Revenge, Maximise financial gains selling proprietary information	Resources for specific impact on operatios, based on proprietary kwonledge	Low cost, enforced by inside use of tools and info on security gaps	SSR, PSR, ADS-B, TCAS	Medium
Cyber Crime	Medium - High	Maximising impact Financial gains using e.g. blackmail or valuable information	Resources for large-scale operations with sophisticated transponders.	Directional antennas, small UAVs with SDR transmitters (~ $5.000)	SSR, PSR, ADS-B, TCAS	Medium
Cyber Terrorism	Low - Medium	Political or religious motivation Massive disruption and casualties	Resources for specific high-impact ops, though usually on a limited scale	As with cyber crime, potentially on a smaller, more targeted scale	SSR, PSR, ADS-B, TCAS	High
Nation State	Unlimited	Weapons Targeting specific, potentially military objects	Anything physically and computationally possible	Military-grade radio equipment, capability for electronic warfare	SSR, PSR, ADS-B, TCAS, WAM	High

Cyber-terrorists seek to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence in aviation systems (Stouffer, Pillitteri, et al., 2015). By exploiting the vulnerabilities in wireless aviation communications, terrorist groups, which traditionally hijack or crash planes using physical weapons, could mount attacks on planes from the ground and from safe distances. The risk exposure of ATM systems is high, due to the increased capacity of terrorists and extremists nowadays to use of IT and cyber technologies for their

illegal purposes. This tendency is on the rise around the world, attributed to political and social instability in Middle East, North Africa and other conflict areas.

Nation state actors can be part of the electronic warfare threat model, although traditionally this is outside the scope of securing civil aviation (Strohmeier et al., 2016). With sufficient knowledge of intrusion detection systems and near-unlimited resources, it is possible to bypass plausibility checks and redundancy-based defenses even in the ATM sector. The risk exposure of ATM systems is considered high and depends rather on specific political circumstances.

4.2.4 Security Measures in ATM

Since ATM Security is major component of Aviation Security, it plays a key role in the prevention and response to threats aimed at all parts of the aviation system including national and international high-value assets. In addition, ATM Security has an interface with Airspace Security revolving around national security and defense requirements, providing technological security and interoperability between civil and military systems. Security threats may be directed at aircraft or through them to targets on the ground. The international dimension imposes the uniform and effective application of suitable measures. ATM has to support national security in respect of the identification of flights entering a State's national territory and Air Defense organizations have to be provided with all ATM information relevant to their task (Zan et al., 2016).

In general, security measures in aviation range across a number of security disciplines. It does not matter if the asset to protect is an aircraft, an airport, a control center or an information network, all security elements apply at a certain degree, as already referenced in Security Standards (ISO, NIST, ISA) and literature recommended practices. In Table 4.8 we brief these basic security measures & disciplines.

While the above security principles can be implemented to a certain efficiency degree, there is a need for a 'holistic view' covering all challenges of aviation security for all phases of air transport, both on the ground and in the air, since the weakest link in the chain is the one likely to break.

Especially the last security element for operational continuity aims to handle degradations of the ATM system. Although it may encapsulate more managerial aspects, is an essential part of the overall aviation security cycle. It highlights the need for a holistic strategy of defense, prevention and response and introduces the need for resilience management. The idea of resilience and its related aspects is introduced and analyzed in the next chapter section.

Table 4.8. Basic security measures & disciplines in ATM systems

Security Discipline	Security Measures
Physical security	Access control, perimeter protection, screening, control checks, assets responsibility, redundancies, enviromental protection
Personnel security	User Access managent, security clearances, segragation of duties, recruitment policy, staff regulations, vetting, staff awarness and trainning
Information security	Rrotection of information CIA: Confidentiality, Availability, Integrity; Cryptography, Media handling, Backups, Software updates and patches
Communication security	Network segregation, security management, intrusion detection management, event logging, teleworking and mobile devices policies
Intelligence support	Security without intelligence is meaningless; intelligence support is a transverse requirement for threat assessments, threat watch and security alert levels declaration
Security information exchange	Information exchange between national authorities, security and intelligence organizations and ATM security managers, security warnings, threat and alert levels, incident identification and notification, reporting and incident resolution follow-up
Operational continuity	Emergency response, Buisiness continuity management and contigency plans

4.2.5 Cyber Resilience in the aviation context

The idea of cyber-resilience in ICT, in its most basic form, is the evaluation of what happens before, during and after a digitally networked system encounters a threat. Resilience is not event-specific: it accrues over the long term and should be included in overall business or organizational strategy. The different understandings of resilience are described in IMPROVER project taking into account a combination of different properties (Theocharidou et al., 2016). Some definitions target on foresight, robustness, resourcefulness, redundancy, rapid recovery and adaptability. Others take prevention, preparedness, respond and recovery into consideration. According to IMPROVER, Resilience concepts encompass several dimensions, such as technical, organizational, social, and economic ones, as presented below:

The *technological* dimension refers primarily to the physical properties of infrastructure components and systems and refers to the characteristics and behavior of these in the case of a change or incident.

The *organizational* dimension, as it relates to the organizations and institutions that manage the physical components of the systems, i.e. CI operators or owners. It covers aspects such as culture, people, business continuity, risk and disaster management at the organizational level.

The *social* dimension encompasses population and community characteristics that render social groups either more vulnerable or more adaptable to hazards and disasters.

The *economic* dimension focus on reducing both direct and indirect economic losses resulting from disasters, in various levels.

In aviation context, Eurocontrol Research program uses for resilience the following definition: "*Resilience* is the ability to prevent disruptions, to prepare for and adapt to changing conditions and to respond and recover rapidly from disruptions to ensure the continuity of services at an acceptable performance level". The aim of this definition is to achieve the understanding that caring for resilience is more affiliated to the management of risks rather than to the elimination of them (EUROCONTROL, 2012).

Being resilient implies minimizing reductions in performance (acceptable drop of performance) in the face of a successful attack. This means to be able to work properly also in several levels of degraded mode, while healing measures and repair works can be undertaken. It is therefore essential to provide methods and means to allow the solution to recover, as quick as possible from such degraded modes, achieving minimum recovery time.

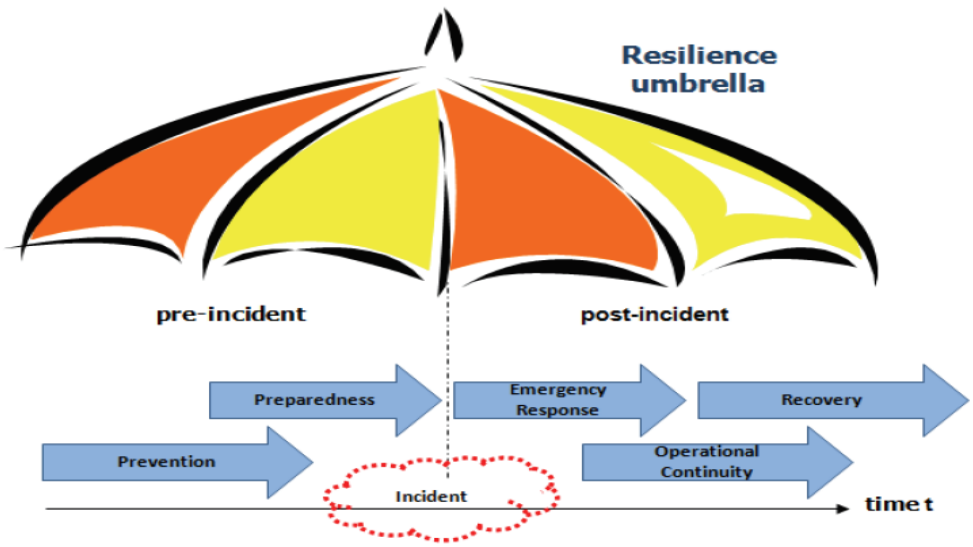


Fig. 4.17 The resilience umbrella (source: EUROCONTROL)

As presented in Figure 4.17, under the resilience umbrella, the whole set of measures, which are required for sufficient resilience against cyber-attacks, is a combination of different actions and proper behavior before, during and after the incident (EUROCONTROL, 2009) The flow of cyber resilience actions already starts when the services, tools or systems under concern are in the development phase, which is related to the "security by design". When taking this into account, the first step of "*Prevention*" is profound established. Controls may have to be put in place to address potential risks emanating from other parts of the system or "system of systems". Another pillar of resilience is "*Preparedness*" for possible attacks, which can be achieved by procedures and training of staff. Being prepared for any cyber-attack begins with thinking about daily activities and the way work is organized and conducted. This also includes the knowledge about the fastest and most secure ways of de-coupling software tools from the system or network and safely/securely shutting down infected systems.

When being under attack the "*Emergency Response*" to the attack is also important. The first response focusses on identifying the problem, containing it, eradicating it. Responsive measures may also include the restriction of services or the unwinding of trained sequences. The focus shall be kept on the secure delivery of services and data whilst being aware of the attack in progress. This supports and enhances "*Operational Continuity*". The response phase needs to be continued until the cause and even the cascading effects of the attack have been eliminated, accounted for or phased out. When at any point in time this can surely be confirmed the phase of "Recovery" may be initiated. This phase again needs to be as short as possible in order to have all services, tools and systems in full operation after a cyber-attack.

Although resilience engineering has been introduced in the aviation mainly for enhancing safety sector, it has not been thoroughly expanded to the cybersecurity aspects and resilience in the air traffic management area. Resilience in aviation sector has been partially discussed in previous research (EUROCONTROL, 2009; Kiesling & Kreuzer, 2017; Lykou et al., 2018b). However, in our work we have studied a recent research, the ARIEL project for Air Traffic Resilience, which aimed to perform a holistic risk analysis and evaluation of critical infrastructures in aviation.

According to ARIEL (Kiesling & Kreuzer, 2017), resilience is seen as the ability of a system to absorb or avoid damage without suffering complete failure and integrates the aspects of protection, mitigation and recovery. It proposes a continuous dynamic and model-based cyber risk analysis process, in order to establish persisting capabilities of cyber resilience in the air transportation system. Project report identified the following recommendations, as essential for resilience implementation in the aviation sector, which are listed and briefly explained below:

R-1) ***Develop the structural and procedural basis for continuous intra- and inter-organizational cyber resilience analysis***: Combining classical information security and newly developed cyber operational resilience approaches. Establishing an organizational structure that brings together the personnel of all relevant disciplines inside and across air traffic organizations to cope with the evolving cyber threat landscape in a holistic way. This should be combined with suitable continuous processes aligned with the existing information security norms and standards.

R-2) ***Develop and manage interdisciplinary cyber risk analysis teams:*** To facilitate the establishment of interdisciplinary collaborating teams, there is a need to develop and apply the necessary methods and management approaches comprising elements of a common language; knowledge management and transfer; ignorance management for balanced evaluation of findings; widespread basic IT knowledge and security awareness by personnel of all disciplines including middle and top management.

R-3) ***Develop and maintain a portfolio of cyber threat scenarios:*** In contrast to the currently applied ad hoc way of threat scenario development and utilization, the introduction of a structured continuous process for the development and evolution of air-traffic cyber threat scenarios is recommended. This is to be combined with suitable methodology to develop scenarios and to apply them in the areas of knowledge development, training as well as verification and validation.

R-4) ***Ensure the interoperability of cyber-relevant models and data:*** Developing standardized meta-models for computer-based data exchange and collaboration of different models is needed. The integration and comparison of cyber-relevant results and findings in tool-based analysis and decision support is also essential. To enable interdisciplinary or even inter-domain collaboration based on a comprehensive approach, data sharing concepts are needed for a reuse of existing data, which include technical, methodological and organizational aspects.

R-5) ***Refine and Evolve Dynamic Risk Analysis Methods:*** Additional effort into the further evaluation and evolvement of the model-based dynamic risk analysis method should be developed. This semi-automated analysis method enables to dynamically model and analyze cyber risks in complex systems, large organizations or even in between several interconnected organizations. The high potential of this approach enables a comprehensive, dynamic cyber risk assessment in the aviation sector.

R -6) ***Safety & Security – Ensure consistency and enable synergies:*** Since cyber threats and potential cyber-attacks can have a direct impact on safety-critical system functions. Therefore, the development of a comprehensive risk management approach aligning the formerly separated considerations of safety and security under a common roof is requested.

R-7) ***Enhance design methodologies to ensure resilient system characteristics throughout a complete lifecycle:*** The restructuring of architectures of sociotechnical systems could support cyber resilience in addition to protective measures. Existing approaches of resilience engineering, which focus mainly on human factors in complex systems, should be extended in a technical sense towards integration of cyber resilience capabilities. Some of the more important aspects to be considered are: the preparation of architectures for ongoing changes; the consideration of mitigation and recovery strategies in the system design; and the addition of system functions supporting the detection of cyber-attacks.

R-8) ***Exploit simulation methodologies to support cyber threat and risk analysis of complex systems:*** To achieve a holistic understanding of the effects of potential cyber-attacks in complex systems, simulation is a valuable method to complement more traditional analysis methods. A widespread application of simulation models for processes and systems should be identified by cyber threat and risk analysis to be critical for system operation. Simulation increases the understanding of the impact of identified cyber threats and supports the validation of risk analysis results. Besides using existing simulation models as standalone tools, it is important to develop simulation models "from gate-to-gate" to support holistic analysis of aviation processes. Finally, using human-in-the-loop simulation is vital with operational staff to research the fundamentals of human factors in the face of potential cyber-attacks.

Based on the ARIEL recommendations, we have analyzed the resilience dimensions which are encompassing, according to IMPROVER Resilience concepts (technical, organizational, social, and economic) and the results of this analysis are presented in Figure 4.18.

Resilience Dimension	Technological	Organizational	Social	Economic
ARIEL Resilience Recommendation				
R – 1		✓	✓	
R – 2		✓	✓	
R – 3	✓	✓		
R – 4	✓	✓		
R – 5	✓	✓		
R – 6	✓	✓		
R – 7	✓	✓	✓	
R – 8	✓	✓	✓	✓

Fig 4.18: Resilience Dimension in ARIEL Recommendations

What we can comprehend from the above table analysis is that most recommendations cover at least two resilience dimensions with the technological and organizational ones to be the most common used. There is a core difference of resilience recommendations from cybersecurity disciplines, which usually handle a single dimension at a time. Resilience measures appear to be a synthesis of interactions, collaboration and evolution of current cybersecurity approaches.

The organizational dimension is common to all recommendations, since cyber resilience is really a matter of effective risk management, combined with collaborative working and interdisciplinary strategies to ensure contingency and efficient business continuity.

While there is a lack of recommendations that enforce the economic dimension of aviation resilience, the social dimension is also less developed. The only recommendation that covers all four resilience dimensions is the last one, about achieving a holistic understanding of the effects of potential cyber-attacks with simulation methodologies using human in the loop, which better support cyber risk analysis of complex systems.

For promoting an overall cyber-resilience approach in the aviation sector, long- term strategy should combine all resilience dimensions that is technological, organizational, societal, and economic. This cyber-resilience approach can ensure greater performance and readiness, making systems more efficient and effective.

4.2.6 Summary of Research Work

Recent developments to increase capacity and efficiency of the existing air traffic system have led to an enormous effort of transition towards digitalization and automation. As a result, formerly separated IT systems get connected via newly established networks for information and data exchange.

Due to a growth of complexity, the attack surface of the overall aviation system is increasing, and previously unknown interdependencies are being created. Limiting security risk management to “traditional” physical aspects like air terrorism is no longer sufficient to ensure a stable and robust operation of the air transportation system. The component of cyber-security has to be expanded from traditional risk mitigation approaches to more resilient focused approaches.

The domains of air transportation and cybersecurity are organized with a strong focus on protective mechanisms, in terms of their operational and technical implementation. To fulfil the requirements of continuous adaption to a rapidly changing threat environment, the architectures of operational and technical systems have to be restructured based on the results and dynamic simulation risk analysis. According to

that, we strongly recommend balancing the cost and performance-driven development and prioritize a sustainable, comprehensive, and continuous improvement in order to improve the overall systems cyber resilience.

As both safety and security are drivers for the determination of resilience requirements, it is sensible to take an integrated view on both subjects to foster the consistency of resilience concepts in aviation.

Since cyber resilience is really a matter of risk management, there is not a single point at which it begins or ends. Instead, it comes from building strategy and working to ensure that the risk-transfer mechanisms that work for more traditional threats are also brought to bear on new cyber threats.

Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and mitigating risks. While it is everyone's responsibility to cooperate, in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible and have increasingly been held accountable for including cyber resilience in organizational strategy.

4.3. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies

4.3.1. Introduction [8]

As the fastest growing segment of aviation, unmanned aerial systems (UAS) continue to increase in number, technical complexity, and capabilities. Numerous civilian and commercial uses are drastically transforming civil protection, asset delivery, commercial and entertaining activities. However, UAS pose significant challenges in terms of safety, security, and privacy within society. An increasing phenomenon, nowadays, is drone-related incidents near airport facilities, which are expected to proliferate in frequency, complexity, and severity, as drones become larger and more powerful. Critical infrastructures need to be protected from such aerial attacks, through effective counteracting technologies, risk management and resilience plans.

In this subsection, we present a survey on drone incidents near airports and a literature review on sensor technologies, able to prevent, detect, identify, and mitigate rogue drones. We exhibit benefits and limitations of available counter-drone technologies (C-UAS), however, defending airports against misused drone activity is a hard problem. Therefore, we analyze three realistic attack scenarios from malicious drones and propose an effective C-UAS protection plan for each case. We discuss applicability limitations of C-UAS in the aviation context and propose a resilience action plan for airports stakeholders for defending airborne threats from misused drones.

Unmanned Aircraft Systems (UAS), Unmanned Aerial Vehicles (UAV), or Remotely Piloted Aircraft Systems (RPAS) are all different ways of referring to what are most known as Drones. They provide a game-changing technology, transforming commercial industries, media, and entertainment, while future opportunities in the field are limitless. A decade ago, drones were considered a technology restricted only to official authorities, such as the military, police, etc. However, many sectors have begun to use UAVs for delivering goods and services. The US Federal Aviation Administration (FAA) predicts that more than 2 million drones will be operated in the USA by 2020 (FAA, 2020a).

[8] *Related Publication:* G Lykou, D Moustakas, D Gritzalis, Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies, Sensors 20 (12), MDPI.

On the other hand, UAS pose a significant challenge in terms of safety, security and privacy for our society and many drone related incidents are frequently reported, affecting Critical Infrastructures (CIs), especially around airport facilities. According to United Nations Security Council, the increased accessibility to drones, combined with their technological evolution, has led to renewed attempts by malicious actors, including organized crime and terrorist groups, who exploit UAS for nefarious purposes (Wells, 2019). There have been several examples of terrorists using weaponized UAS to conduct attacks, or support surveillance, reconnaissance, and other illegal activities. These incidents have created the need to detect and disable rogue drones, therefore a new area of research and development has emerged in counter drone technologies (C-UAS).

The remainder of this work is structured as follows: In subsection 4.3.2, we present drone technological evolution, while in subsection 4.3.3 we present our survey on worldwide drone incidents, threatening airports and its critical infrastructures. In subsection 4.3.4, we review methods and sensor technologies, able to detect, identify and mitigate rogue drones. In subsection 4.3.5, we analyze three different categories of attack scenarios against aviation assets and airport's CIs, while in subsection 4.3.6, C-UAS protection plan is proposed for each scenario. Finally, in subsection 4.3.7, we discuss applicability limitations of C-UAS in the aviation context and propose a resilience action plan for defending airports from misused drones. Findings and conclusions of our research are resumed in subsection 4.3.8.

4.3.2. UAV Technological Evolution

UAVs are multi-rotor or fixed wind aircrafts, autonomously piloted or operated by remote controller. They come in many shapes and sizes, ranging from insect-like types to large ones, that weight several tons. Different organizations (NATO, DoD, NASA, Regulatory Authorities) have defined main UAS categories. Most of these classifications are based on weight, operating altitude, or speed. Table 4.9 shows UAV categorization based on weight, altitude, range, endurance, payload capabilities, and some examples of available commercial UAV models.

In this work, we analyze threats from the lightweight class of micro, mini and small UAVs (sUAS, NATO Class I) weighting less than 150 kg. Such drones can navigate quite far from center of command, up to a range of 50km, with an average speed of 15m/s. They are able to carry heavy payloads up to 50kg and provide video piloting and communication link based on radio signals.

Table 4.9: UAV classification based on weight, altitude, range & payload

Category	NASA UAS class	Weight (in kg)	Normal Operating Altitude (in m)	Mission Radius, Range (in Km)	Typical Endurance (in hrs)	Payload (in kg)	Available UAV models in market
Micro	sUAS Class I	<2	<140	5	<1	<1	DJI Spark, DJI Mavic, Parrot Bebop2
Mini		2-25	<1000	25	2-8	< 10	DJI Matrice600 DJI Inspire2, Airborne Vanguard
Small		25-150	<1700	50	4-12	< 50	AAI Shadow 200, Scorpion 3 Hoverbike
Medium	Class II	150-600	<3300	200-500	8-20	< 200	Griff 300, Ehang 216
Large/ Tactical	Class III	>600	>3300	>1000	>20	> 200	Boeing X-45A UCAV

Moreover, live video stream can be sent from the drone's video camera to the pilot (operator) via a GCS (ground control station), which can be a dedicated controller, smartphone, VR glasses, etc. While classification group nomenclature differs among these organizations, some specific weight limits are commonly used, as presented in Table 4.9.

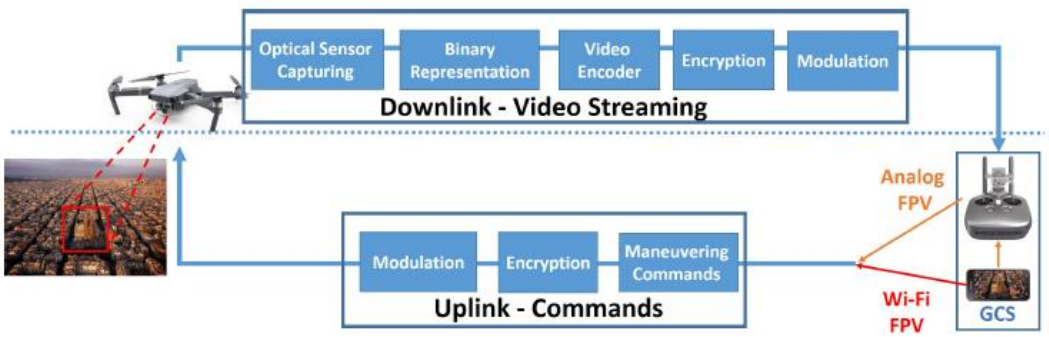


Fig. 4.19: UAS Communication channel – downlink & uplink

A typical communication channel, also called First-Person View (FPV) consists of a downlink and an uplink, as presented in Figure 4.19. There are two types of technologies for Command and Control (C2) communication: Wi-Fi and analog. A

Wi-Fi FPV drone is basically a flying router with no Internet connectivity. Such drones open a network, as an access point, which allows the drone and its controller to communicate from many kilometers far away. Moreover, live video stream can be sent from the drone's video camera to the pilot (operator) via a GCS (Ground Control Station), which can be a dedicated controller, smartphone, VR glasses, etc. (Nassi et al., 2019). For this category of commercial-off-the-shelf sUAS, new innovative control interfaces have been recently developed and the emerging field of Human-Drone Interaction (HDI) was surveyed by Tezza and Andujar (2019), who discussed how HDI goes beyond control modalities, enhancing human interaction.

The recreational and commercial uses of drones have expanded in evolving smart cities, where UAVs perform multiple activities. Alsamhi et al. (2019) have reviewed the collaboration of drones and Internet of Things (IoT) for improving intelligence and quality of life in smart cities. Moreover, in rural areas and critical infrastructures, new uses for UAVs fulfill operational, safety and environmental monitoring tasks, which include taking physical, chemical, electromagnetic and radiochemical measurements. They extend human safety capabilities, by monitoring in environments where humans cannot reach (Calantropio, 2019). In the security sector, UAVs can expand the deployment of traditional security detection (e.g., sensors and cameras) with perimeter monitoring systems in CIs, including airport facilities. Furthermore, within airport perimeter, UAS can provide faster response to security alarms, track threats, inspect or patrol facilities, as presented in (PARAS, 2019).

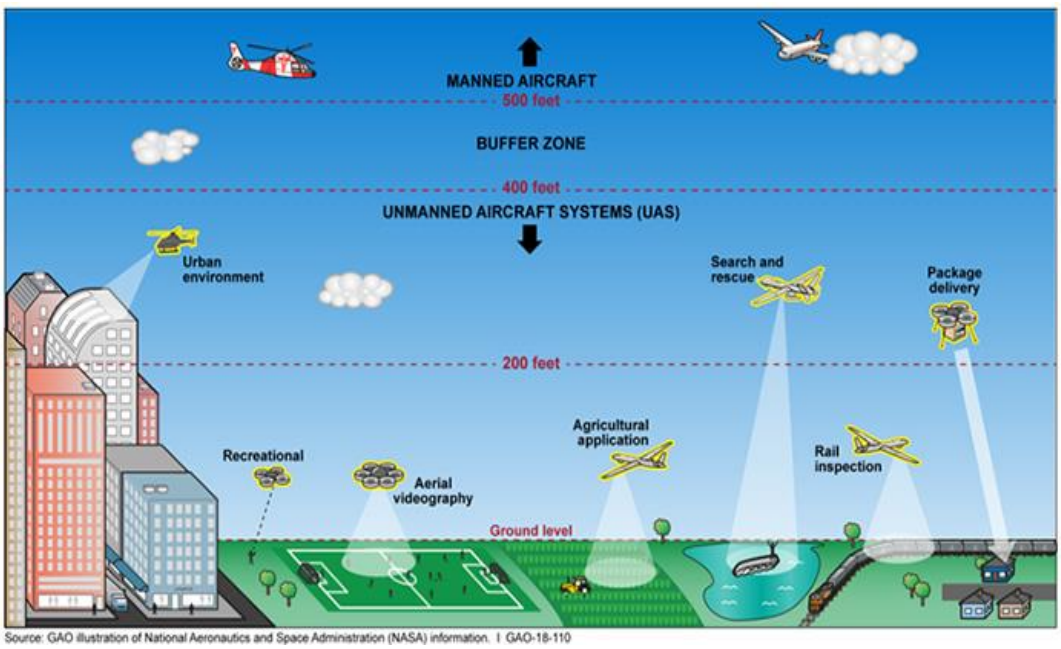


Figure 4.20: Potential Civilian and Commercial Uses for Small UAS

Figure 4.20 graphically represents potential civilian and commercial uses for UAVs and interaction with aviation activities, as published in GAO report (U.S. Government Accountability Office (GAO), 2018). In the drawing, we can distinguish drones performing package delivery, aerial videography and other recreational activities in urban areas. They are also used in agricultural applications and critical infrastructure inspection in rural areas and support search and rescue activities, while flying in lower airspace up to 400 feet from ground level.

Although advances in UAV technology found numerous applications and brought multiple benefits to society in general, the potential threat of technology misuse should not be discounted. Nassi et al. (2019) describe societal threats to security and privacy created by drones, while Altawy & Youssef (2016) have identified both physical and cyber threats of such systems. In our research, we have distinguished asymmetric threats, which can exploit sUAS capabilities to attack against CIs, including airports, in an obscure or unusual fashion, providing unfair advantage to perpetrator. These have been aggregated into the following three categories:

- Spying and tracking points of interest, conducting unauthorized mapping and surveillance.
- Carrying CRBNE payloads (Chemical, Radiological, Biological, Nuclear and Explosive materials) towards fixed installations or moving targets.
- Intercepting wireless networks, breaching computer systems and conducting cyberattacks by hovering or landing on buildings.

In this subsection, we present a survey on drone incidents and counter measures, focusing our research on airport facilities and surrounding critical infrastructures. We continue with a literature review on C-UAS sensors and technologies, which includes both academic publications and industry developments in countering drone systems. Benefits and limitations of each detecting and counteracting technology are also presented, along with applicability challenges of C-UAS systems in the complicated aviation environment. In addition, we have developed various attack scenarios against airport's CIs with the use of UAVs, based on the three categories of asymmetric threats listed above. A detailed description for each scenario is presented, along with affected assets and impact analysis. Graphical attack representations depict malicious attack phases, on step-by-step basis, while related impacts on security parameters are also examined. Finally, we propose preventing measures, detection, and mitigation technologies, which could be deployed in each scenario, in order to counteract and protect airport's CIs from UAS malicious attacks.

The principal aim of our research is to develop an overview of the available risks from misused UAVs and make recommendations on the design of effective C-UAS in airport facilities. To the best of our knowledge, no study has presented analytical attack scenarios, which can be launched inside and outside airport perimeter (in eight potential attack-launching spots). For each attack scenario, a proposed C-UAS

protection plan is designed, aiming to increase airport resilience and business continuity.

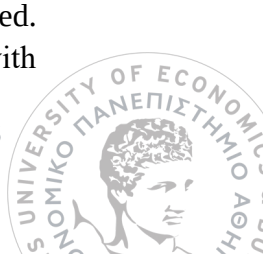
Research's contribution is to: i) alert airport community and aviation researchers about safety and security risks revealed from nefarious drones, ii) analyze benefits and limitations of available C-UAS technologies and iii) propose a resilience action plan that supports airport operators and aviation stakeholders to increase robustness of critical assets and infrastructures against airborne malicious threats.

4.3.3 Worldwide incidents with UAS

Since 2016, the number of security incidents, involving UAVs near airports and other CI facilities, has dramatically increased worldwide. It is obvious that drones can pose a potentially severe threat to aviation activities (Altawy & Youssef, 2016). The major problem with drones operating near airports and air-controlled space is collision hazard between manned aircrafts and drones, which raises safety risks of human and material losses. Tests conducted by UK government found that a 400g drone could smash a helicopter's windscreen, while a 2kg drone could cause critical damage to a passenger jet's windscreen (Jones, 2016). While cheap UAV versions have barely enough power to fly for half an hour, sophisticated models can stay airborne for hours at a time. As a result, whenever an unauthorized drone is detected around airports and its facilities, runways, or even close to the security perimeter, the entire airport may be closed, for safety reasons. And this is translated into unnecessary costs, time delays and potentially negative reputation for the airport, the Air Traffic Control (ATC) and Civil Aviation Authority. In this section, we present our survey on UAV incidents affecting aviation activities, which includes UAS sightings and verified UAV incidents near airport facilities with quantified impacts.

Although UAS incident reporting is not mandatory yet, we have examined and exhibit drone incidents witnessed over the last 4 years, by using open publicly available sources and databases, which report UAVs incidents like NASA, FAA, Dedrone, ASN and others (Dedrone, 2020; FAA, 2020b; NASA, 2020; Wild et al., 2016). We have distinguished 10 serious incidents in heavy traffic airports worldwide, with serious impacts to safety, security, reputation, and quantified economic loss, and we present this collection of events below:

1. UK: A serious incident happened between 19-21 December 2018 in London, when Gatwick Airport has stopped operations due to drone attack. Police investigators said that it was a planned attack, involving someone with inside knowledge of the airport's operational procedures. It is estimated that 140,000 passengers were affected with around 1,000 flights either diverted or cancelled. The attack cost the airport approx. £1.4m, but airlines were hit even harder, with



EasyJet said to have lost £15m through the 3-day attack. A similar disruption took place one month later at Heathrow Airport in January 2019, although with limited duration.

2. Ireland: Flight operations at Dublin airport were suspended for half an hour in February 2019, due to the confirmed sighting of a drone over the airfield, despite drone's prohibition within 5 km (3 miles) around Irish airports.
3. Germany: Frankfurt airport was shut down for an hour on 9 May 2019, as operators halted flights over a drone sighting. Overall, 143 take-offs and landings were cancelled, while 48 aircrafts were diverted to other airports among a total of 1,500 scheduled flights.
4. Singapore: Two incidents occurred, where unauthorized drone flying affected flights at Changi Airport, twice in one week during June 2019. Overall, 52 flights were delayed and 8 were diverted due to these drone sightings.
5. UAE: Dubai International Airport (DXB) was closed 3 times (an accumulated 115-minute closing) in 2016, due to illegal drone activities near the airport. Emirates Authority for Standardization and Metrology estimates the financial losses to be $95,368 per minute due to shutdowns caused by drones. The total loss of DXB in 2016 was approx. $11M due to drones.
6. Japan: A drone spotted flying near Osaka's Kansai International Airport in October 2019 led to the temporary closure of the major hub, despite the fact that flying drones near Kansai Airport and bringing drones inside the airport are prohibited.
7. Canada: A Beech King Air A100 of Skyjet Aviation collided with a UAV in October 2017, while approaching at Jean Lesage Airport near Quebec City. The aircraft landed safely despite being hit on the wing. Neither the UAV, nor the operator had been found. UAV had been flying at 1,500ft, i.e., 5 times the maximum altitude that UAVs are permitted to fly in Canada.
8. New Jersey, USA: Newark airport was closed due to a drone spotted in the vicinity for 90 minutes, in January 2019. Estimating a cost of $1M per minute for the airport closure, the incident caused $90M of economic loss. Airplanes were diverted to other airports, using extra fuel consumption and adding to the economic loss for the airlines.
9. New York, USA: A civilian UAV collided with a Black Hawk helicopter over the eastern shore of Staten Island in September 2017. The helicopter was able to continue flying and landed at Linden Airport. Nobody was hurt, but part of the UAV was found at the bottom of the main rotor system.
10. South Carolina, USA: A helicopter's crash has been triggered by a civilian drone in February 2018. This was the first drone-linked aircraft crash. Helicopter's tail

struck into a tree, while trying to evade small drone triggering a crash landing. Student and instructor pilots were uninjured, according to Charleston Police Dep. Report.

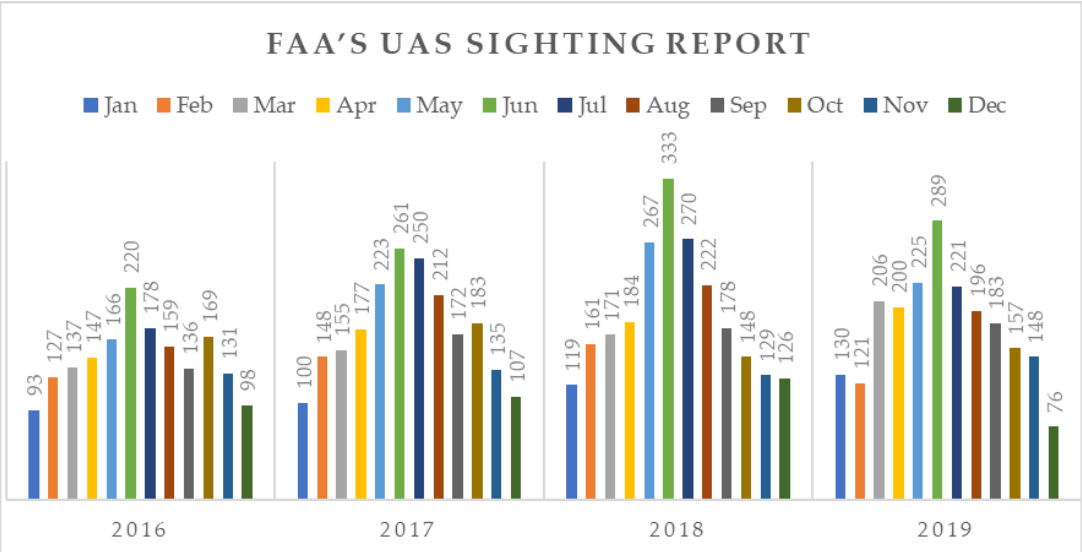


Figure 4.21: FAA's UAS Sighting Report Database

In addition to the above incidents with quantified impacts, encounters and near-misses between manned and unmanned aircrafts are becoming increasingly common events, despite the existing restrictions around air-controlled spaces and geofencing measures. Since 2016, US Federal Aviation Administration (FAA) has collected 8,344 reports from airmen, about UAS sightings of potentially unsafe use. In Figure 4.21, these sightings of non-compliant sUAS operations are graphically analyzed, where we can distinguish the occurrences seasonality in summer months and the gradual annual increase of sightings.

Despite FAA's efforts and initiatives to regulate and contain the risks of unsafe or non-compliant sUAS operations in aviation sector, the problem seems to be accelerating with more than 2,000 near-miss sightings per year, being reported by airplane pilots, air traffic controllers and other aviation stakeholders (FAA, 2018). Although these events cannot be outright verified, so that to be reported as incidents, the FAA's UAS Sighting Report Database provides a barometer of unsafe UAS operations.

The increasing number of occurrences near airports has led to serious safety concerns, being raised for drone violations of aviation safety rules. All these occurrences, combined with the rapid development of UAV technology and the uncontrolled spread of drone's usage, has motivated our survey for counter-drone sensing technologies and methodologies proposed by the academic sector and applied by industry.

4.3.4 Literature Review on Counter Drone (C-UAS) Technologies

The need to protect critical infrastructures from misused drones has brought advances in C-UAS academic research and commercial applications. Countering a drone is a complex, multi-step process, involving interaction between several distinct sensors and methodologies, along with interaction with human operators. In this subection, we provide a literature review of major C-UAS sensor technologies that can be used in airports, classified into three main categories: i) preventing actions, ii) detection sensors & technologies and iii) mitigation countermeasures against rogue drones.

Since 2014, an increasing interest to C-UAS academic research has led to more than 950 scientific publications. In Table 4.10, the number of new publications, which included the term "C-UAS" in their title is presented, excluding patents and citations, based on Google scholar's search. Moreover, from January and up until March 2020, another 47 related publications were published.

Table 4.10: Number of new publications based on Google scholar search

Year	2014	2015	2016	2017	2018	2019
Num. of Scientific Publications	99	124	134	182	178	234

This proliferating trend in the number of related publications confirms the growing stimulus of the research community in this area, related to drone detection sensors and mitigation technologies, as exhibited in figure 4.22.

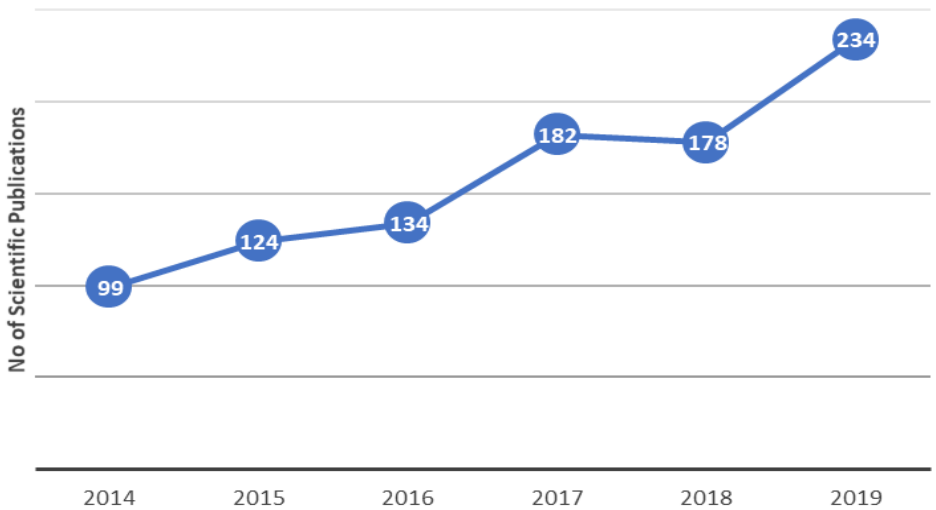


Figure 4.22: Number of new publications using the term "C-UAS" based on Google scholar search

4.3.4.1. Preventing Actions

The use of UAS is generally regulated by national civil aviation authorities and national institutions. In many countries, legislation proposes a set of rules to control the effects of small UAV on peoples' safety, security and privacy. Such regulation frameworks complemented by geofencing technologies can act as preventive measures to forestall drone operators from entering restricted airspace by mistake or by ignorance.

Geofencing is the creation of virtual fences around areas or points of interest to keep drones away from No-Fly Zones (Stevens & Atkins, 2018). Substantial work has already been published to define and realize geofencing systems for small UAS (Stevens & Atkins, 2016, 2018; Zhu & Wei, 2016). Popular autopilot systems currently offer simple containment volume geofences over critical areas, including airports (Hayhurst et al., 2015). A geofence could be dynamically generated, as in a radius around a location point with predefined set of boundaries. It is an effective preventing measure, when built into UAV's navigation software. As a result, drones using Global Positioning System (GPS) or Global Navigation Satellites Systems (GNSS), combined with autopilot software, can interact with a geofence and avoid restricted areas.

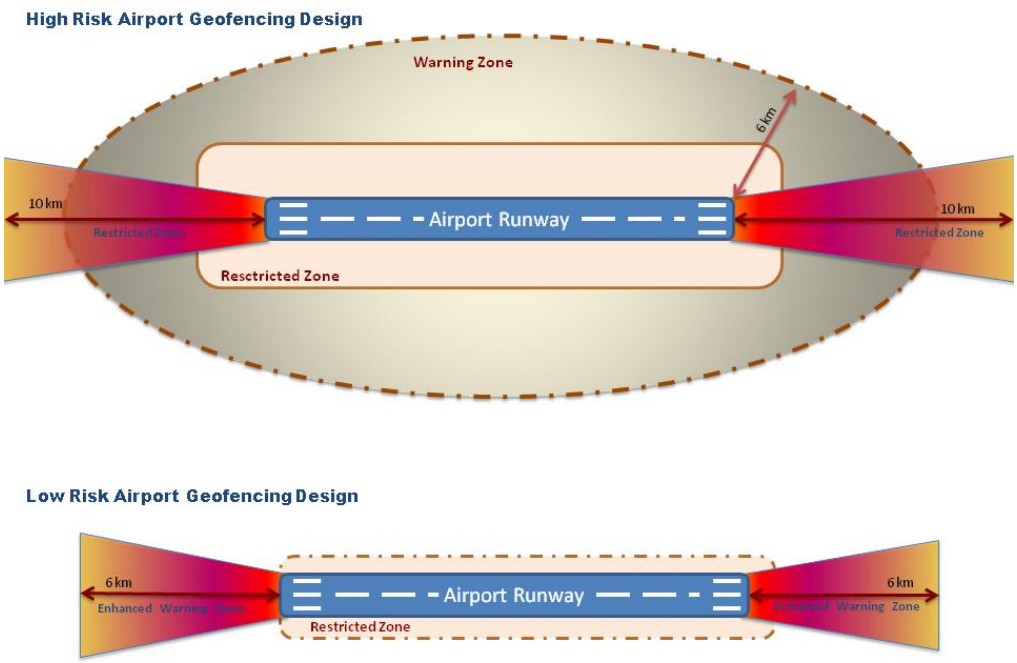


Figure 4.23: Detailed three-dimensional Geofencing solutions around airports

Furthermore, geofencing software can be regularly updated by UAV manufacturers to include new and temporary restricted zones. Some manufacturers have also expanded the airport restricted zones to enhanced safety zones, which prevent UAVs from entering into a three-dimensional bow-tie geofence shape (DJI, 2019). This protects approach and departure pathways and prevents misused drones from interfering with airplanes, while departing from or landing to airports. Risk-based airspace principles can categorize airports virtual fences to high and low risk design, as presented in Figure 4.23. In lower-risk areas, drone's operations may be permitted, for example, when authorized UAVs are allowed to conduct drone inspection activities in locations parallel to runways.

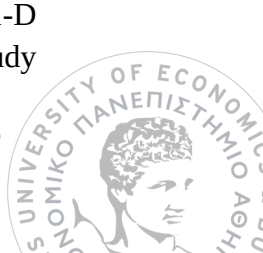
Geofencing can play a major role in ensuring that careless and clueless UAS operators are prevented or alerted, when interfering with airport airspace. However, it cannot stop malicious users from manually disabling UAV geofencing functionality, in order to intrude into restricted areas. Therefore, detecting and interdicting C-UAS measures for nefarious drones in Non-Fly Zones are also needed.

4.3.4.2. Detection sensors & technologies

In this subsection we present a literature review on detection sensors and technologies, using various types of sensors like: i) radar detection sensors; ii) radio frequency detection sensors; iii) acoustic sensors; and iv) visual sensors. Afterwards, we make a comparison of benefits and limitations of each technology sensor, while commercially available detection systems are also exhibited and analyzed at the last part of this section.

Radar detection

A surveillance radar is designed with single or multiple antennas to detect and track multiple objects simultaneously. It sends out a signal, in order to receive aircraft's reflection, measuring spatial coordinates and optionally velocity, acceleration and direction. According to Skolnik (1990), no other sensor can measure range to the accuracy possible with radar, at such long ranges and under adverse weather conditions. In recent years, it has been an active area of research in the field of C-UAS radar applications. Monostatic radars work with collocated transmitter and receiver. Several studies analyzed monostatic radar working either at 35 GHz, or at 9.4 GHz to detect and track nearby drones (Drozdowicz et al., 2016). The most employed radar signal characteristic for automatic target classification is the micro-Doppler (m-D) signature (Samaras et al., 2019). The intrinsic rotation movements of UAV rotor blades can define the type of drone, while the propulsion turbine of a jet or the flapping wings of a bird can be statistically described by the radar m-D signature (Harmanny et al., 2014; Ritchie et al., 2015; Wit et al., 2012) Another study



showed that distinguishing between a drone and a bird can be accomplished, using machine learning algorithms, by extracting features from m-D signatures (Molchanov et al., 2014). Several methods suggested the use of bistatic radar, where transmitter and receiver are not collocated, or multi-static radars in order to increase accuracy of UAV detection (Fioranelli et al., 2015; Hoffmann et al., 2016; Zhang et al., 2017). Compared to other technologies, radar can provide long-range detection up to several hundred kilometers, depending on the target Radar Cross Section (RCS). Its performance is almost unaffected from adverse light and overcast conditions (Knott et al., 2004). On the other hand, challenges about the use of radar include the lack of automation and the high dependence on trained radar operators (Michel, 2019). Moreover, radar is the most expensive equipment of all available drone detection sensors, while it requires national frequency spectrum licensing and environmental compatibility study.

In airports, radar sensors are designed for detecting standard sizes of manned aircraft, with relatively large RCS and high velocity, thus they are not suitable for detecting very small and slow-moving objects, flying at low altitude such as s-UAV (Joint Air Power Competence Centre, 2019). Radar sensors are usually tuned for identifying small targets at short, medium or long ranges; therefore, multiple radars with different detection ranges may be necessary to cover the areas of detection in airports (MyDefence, 2019). Another drawback of radar sensor for tracking drones is the lack of geo-localization of GCS and pilot of the invading UAV, thus this surveillance technology is commonly used in combination with other detection sensors (Birnbach et al., 2017).

Radio Frequency detection

Radio Frequency (RF) scanners use passive detection technology and provide a cost-effective solution for detecting, tracking, and identifying UAVs, based on their communication signature. They explore algorithms to scan known radio frequencies, find and geolocate RF-emitting drones despite weather and day/night conditions. Many studies have used RF scanners, either for locating a drone in space, or classifying FPV (First Persons View) channel transmissions. Nguyen et al. (2018, 2016) analyzed RF signals, captured by Software Defined Radio (SDR) and found that the RF signatures of commercial Wi-Fi drones can be detected with high accuracy from a distance up to 600m. They could also identify the detected drone type with variable accuracy (64-89%), depending on the drone. The received signal strength indication patterns of Wi-Fi signals were analyzed for the detection of approaching and spying Wi-Fi drones. This method can be applied using a Wi-Fi receiver, but its effectiveness depends upon line of sight between receiver and UAV.

However, detection accuracy in environments with many Wi-Fi signals and among other emitting smart devices has not been validated. Scheller (2017) investigated drone detection in heavy RF environments, where RF drone's signature at a distance more than 100m away, could not be observed. Two studies (Peacock & Johnstone, 2013; Shi et al., 2017) used machine learning algorithms to classify drone transmissions, while Peacock suggested detecting the presence of a drone by analyzing the MAC addresses of known drones.

Nevertheless, attackers can evade the suggested detection method by changing a drone's MAC address. RF scanners can be very effective at detecting the presence of a drone and identifying its type by comparing them to known used bands (Mototolea & Stolk, 2018). Some high-end systems can triangulate the drone and its GCS, when using multiple RF scanners spread far apart (Kim et al., 2017). Moreover, RF detection can provide early-warning, through the fact that drone and controller transmit radio signals, when the system is turned on, allowing adequate detection time, even before the drone takes off. On the other hand, RF-based UAS detection sensors can detect only a few airborne objects at a time. Their accuracy can be affected by numerous sources of potential interference, particularly when line of sight obstacles degrade detection performance (Blue Ribbon Task Force, 2019). Their effectiveness is valid, as long as the UAS transmit a signal. However, malicious drones may flight autonomous, without emitting RF signals, in order to avoid RF detection, or even transmit to a dedicated band that is not popular for FPV use.

Acoustic detection

Drone propellers transmit an audio pattern that can be detected and used for drone positioning and classification by acoustic sensors. Usually, a microphone detects the sound made by a drone and calculates location, using Time Difference of Arrival (TDOA) technique, while more sets of microphone arrays can be used for rough triangulation of UAVs (Bernardini et al., 2017). In most cases, acoustic sensors have a short detection range, less than 300m. They are subject to interference limitations with other audible noise, which is quite significant around airports. Regarding the field of audio-based detection of UAV, researchers have exploited utilizing micro-phone arrays with single board computers for the digital signal processing tasks (Chang et al., 2018). Other researchers proposed drone detection frameworks using audio fingerprints and correlation for comparison. Acoustic signature collection is a major issue for acoustic detection, however factors such as wind, temperature, time of day, obstacles, and other sounds can bend the sound waves, changing the direction of the sound (Chowdhury, 2016). The collection of a sound signal on a hot day with little wind in open plain areas will be significantly different than collection of the signal on a cold, windy night in a forest (Mezei & Molnár, 2016). Several studies suggested methods that triangulate sounds obtained from centralized (Bernardini et

al., 2017) and distributed microphone arrays, in order to detect drone's direction of arrival and location. Kim et al. (2017) introduced a real-time drone detection and monitoring system, using one microphone and increased the classification accuracy of their proposed system from 83- 86%, using an artificial neural network. They created a background noise class to separate the drone sounds using the UrbanSound 8K dataset (Salamon et al., 2014). Jeon et al. (2017) presented a binary classification model that used audio data to detect the presence of a drone. Acoustic sensors are not considered as primary detection source and are generally combined with other detection tools. Park et al. (2015) proposed a system that used a combination of radar and acoustic sensors and a feed-forward neural network, in order to detect and track identifiable rotor-type UAVs.

Acoustic sensors can detect autonomous flying UAVs, with lower system cost, medium probability of detection with a higher false alarm rate (due to increasing number of drone models), while geolocation of the operator is not provided. Finally, acoustic sensors rely on a database of sounds emitted by known drones and might be deaf to drones not covered by the library. Algorithms can also identify the type of UAS and even differentiate between authorized and unauthorized UAS. However, in airport heavy noise environments, where aircraft noise is enormous and overlapping, the use of acoustic sensors cannot be considered as a reliable detection method.

Visual detection

Imaging systems and cameras can be used both in the visual and infra-red spectrum to detect and classify drones. Not typically a primary detection source, electro-optical sensors use a visual signature to detect UAS, while infrared sensors use a heat signature. High performance camera systems provide images as forensic evidence. They are often equipped with a high zoom capability to show small objects at a distance; however, they have range limitations. Based on cameras that detect visible frequencies, several studies suggested methods to detect a drone and its trajectory from video stream by detecting motion cues, visual marks, and shape descriptors. With the advancements in neural networks and deep learning algorithms, optical data are a valuable source of information and provide significant cues to a UAV detection system, as presented in (Saqib et al., 2017). Rozantsev et al. (2017) have used multiple fixed ground cameras for dynamics-based recovery of UAV trajectory. Opromolla et al. (2018) used traditional computer vision techniques for UAV detection, using template matching and Normalized Cross-Correlation metrics. UAV detection with optical cameras that make use of traditional techniques are proposed by Gokcce et al. (2015) who employed traditional features such as Histogram of Gradients (HOG) to describe small UAVs. Researchers have also achieved detection and objects classification, by using hyperspectral images. The methods can accurately locate and identify drones. They suffer from false positive detections, due to the similarities

between movements of drones and birds. They also suffer from high false negative rates, due to the increasing number of drone models, the use of non-commercial ones and ambient darkness.

Unlike optical sensors, thermal sensors operate in the non-visible electromagnetic spectrum. Thermal cameras are able to capture the infrared radiation, emitted by all objects in the form of heat. They are sensitive to the long-infrared range of the electromagnetic spectrum, with a wave length between 9-14μm (Samaras et al., 2019). In order to address drone detection in dark conditions, several studies suggested using thermal cameras. Muller (2017) suggested using short-wave infrared (SWIR) for night detection, while Birch and Woo (2017) performed a comparison of drone detection at various distances using SWIR, mid-wave infrared (MWIR), and long-wave infrared (LWIR) imagers. In (Thomas et al., 2019) authors propose a localization method via 2D and 3D triangulation for already detected UAV targets, when considering images from multiple thermal cameras. The main advantage, when using a thermal camera in a security related application, is the ability to visualize the surrounding environment, regardless of the external lighting or weather conditions and even in total darkness. Furthermore, compared to traditional RGB cameras, thermal cameras offer increased robustness against illumination changes. On the downside, thermal cameras usually produce lower resolutions images, while being more expensive. Finally, Church et al. (2018) analyzed the detection of drones using a LiDAR sensor and found good detection accuracy, within a range of a few hundred meters. Nonetheless, infrared cameras and LiDAR cannot identify drones, due to low resolution of captured images. Typically, cameras that capture visible and invisible wavelengths are combined to support detection throughout the day and night. It's hard to be used for detection alone, therefore they are often paired with radar and RF options, as an additional tool for UAS detection, verification and forensics analysis.

Comparison of detection technologies

Based on literature review of academic work on C-UAS, we have summarized in Table 4.11, advantages and drawbacks on detection sensing technologies. It is obvious that adopting a single sensor technology for UAV detection in airports cannot provide the desired situational awareness. Utilizing different sensors in a system is considered more efficient for drone detection systems, especially in the airport complex environment. Therefore, in airports, detection can be implemented in different ways, either as a distributed system on the airport perimeter, or as a single point of detection capability.

Table 4.11: Comparing C-UAS detection technologies

Method	Benefits	Limitations
Radar	Long Range primary surveillance detection system up to 100 km, depending on RCS & altitude	Detection range dependent on drone size and Radar Cross Section (RCS).
		Radar systems designed for manned aviation cannot detect small flying objects.
	Can track most of drone types, regardless of autonomous flight	High acquisition and installation cost.
	When combined with machine learning algorithms can distinguish birds from drones	Requires transmission license and frequency check to prevent interference with other RF transmissions
	High accuracy tracking, while in angle range of observation	Hard to detect low altitude flying, slow moving or hovering UAVs
	Able to track multiple targets simultaneously, when using multi-tracking coverage	No Pilot tracking capability or Ground Control Geolocation
	Bistatic and multi-static radars increase accuracy of UAV detection	Lack of automation and high dependence on trained radar operators
	Independent of visual conditions (day, night, overcast weather etc.)	Fault positives with similar shape objects (like birds, clouds, etc.)
	No need for RF or acoustic signal	Environmental compatibility study is needed
RF detection	Lower cost than radar sensors with Medium Range up to 600m	RF signal required, can't detect autonomous flying drones
	Detects certain radio frequency bands, where UAV and GCS communicate for command and control (C2)	Electromagnetic interference and loss of sight degrades detection capabilities
	Can capture RF emitted by UAV and able to locate UAV and controller	Variable detection accuracy depending on drone type & frequency band
	Can capture WiFi emitting drones	Attacker can spoof MAC address
	High accurancy detection	Can detect only a few UAVs at a time
	Early warning capability even before UAV takes-off (when turned on)	Less effective in heavy RF environments with range less than 100m
	Triangulation is possible with multiple RF sensors	Detection limitations for swarm of drones
	Machine learning algorithms can classify drone transmissions	Some passive systems may emit RF signals, despite being characterized as passive systems
	Passive detection, no license required	

Acoustic	Classification based on acoustic signature	Depends on available library of already capture sound signatures
	Can differentiate between authorized and unauthorized UAS	Higher false positives, due to increasing number of drone models
	No need for RF signal for detection. Can detect autonomous flying UAVs	Unreliable detection at range >300-meters
	UAVs detection can extend beyond Line of Sight	Doesn't work as well in noisy environments
	Classification based on UAV's acoustic signature	Detection limitations for swarm of drones
	Time Difference of Arrival (TDOA) technique is used for UAV localization while triangulation is possible with an array of distributed sensors	Detection performance is affected by wind direction, temperature, line of sight and signal reflections due to obstacles
	Low cost sensors	Not used as primary detection source
	Can provide drone direction or rough estimation	No Pilot tracking capability or Ground Control Geolocation
Visual	Detects visual signature for electro-optical (EO) cameras to classify UAVs	Need for human interference or artificial intelligence to efficiently detect UAVs
	Detects heat signature infrared spectrum for thermal (IR) cameras	Not used as primary detection source (both EO & IR cameras)
	Can distinguish drone from birds, especially with IR sensors	Both have detection limitations based on resolution capabilities. Hard to capture swarm of drones
	No need for RF signal emitted by UAVs to capture	IR & EO cameras need direct Line of Sight to detect UAVs
	IR cameras visualize surrounding environments, regardless of the external lighting or weather conditions and even in total darkness	EO Cameras depend on daylight and outdoor illuminance conditions (Overcast, darkness etc)
	Can record sightings and use for further investigation	May confuse UAV with a bird or similar shape small airplane
	Can record incidents as forensic evidence for legal actions	Range limitations depending on weather conditions (clouds, rain, fog, mist etc)

Considering the fact that UAVs may be requested to perform specific tasks, in the airport premises, it is important to be able to distinguish authorized UAV operations from misused drone flights. The type of device permitted to flight around airports should be identified, in as much detail as possible, with registration mark (if available), size, color, number of rotors, direction of travel, etc. Identifying the drone type and main characteristics, in case of nefarious use, will provide security team with information about drone's endurance time and which countermeasure is best suited for response.

In the near future, USA, Europe, and other states are planning to develop and implement Unmanned Aerial System Traffic Management (UTM) systems and Remote Identification requirements for civilian drones, which will enable airspace authorities to segregate compliant with non-compliant drones. UTM, as traffic management ecosystem for UAV operations, will be separated from manned aviation ATM systems. However, services, roles and responsibilities, data exchange protocols, infrastructure and performance requirements are under development for enabling the management of low-altitude uncontrolled drone operations. Since, this initiative is under design, counter drone technologies are essential for protecting airports from misused UAVs.

4.3.4.3. Mitigation Countermeasures

There is a number of technological solutions for mitigating threats from malicious UAS, when approaching critical infrastructures. However, adopted mitigation options should be legal, proportionate and properly risk assessed. Two types of C-UAS technologies exist: electronic and kinetic. Electronic countermeasures can defeat UAV by using communications link manipulation, RF jamming, or GPS spoofing. Kinetic interdiction refers to intercepting UAS by physical means. Both technologies are reviewed, in order to examine their applicability in the airport environment. The analysis is resumed with a comparative table for benefits and limitations of each mitigation technology.

Electronic interdiction or Signal Jamming is the intentional use of RF transmission, in order to block signals and disrupt communications between the GSC operator and the flying UAV. Radio Frequency jammer is a static, mobile, or handheld device, which transmits a large amount of RF energy towards the drone, masking the controller signal. This results in the following reactions, depending on the drone's design: i) drone makes a controlled landing in its current position; ii) drone returns to user-set home location; iii) drone falls uncontrolled to the ground; and iv) drone flies off in a random uncontrolled direction. Several studies have suggested disrupting incoming/outgoing communication for disabling UAVs. By using applied radio jamming against a video link channel, the FPV functionality can be disabled, preventing the operator from maneuvering the drone. A jammer's ability relies on the strength of its radio transmitter; however, the effective range cannot exceed a radius of few kilometers (Birnbach et al., 2017).

Another option is GPS Jamming, when UAVs use GPS navigation systems, however mitigating a satellite navigated drone is a much larger challenge, than jamming the RF controlled drone. In order to effectively jam a satellite navigation signal, a new stronger signal is sent to the drone, replacing GPS communication, which the drone

uses for navigation. Applying GPS jamming to drones, results in vehicle's drifting, increases difficulty to control the drone, and prevents the return to home functionality from working. Mitch et al. (2011) surveyed the signal properties of 18 commercially available GPS jammers, based on experimental data, and presents measurements of the attenuation of jamming efficiency. By dynamically altering the GPS coordinates in real-time, the drone's position can be controlled and the drone can be directed to another landing zone.

Protocol manipulation of a UAS refers to a third party taking over a UAS remotely by impersonating its remote control. The emitted signal instructions are designed to confuse the UAS, so that it operates as though the manipulated instruction is the legitimate signal. Many studies demonstrated methods for hijacking a drone using replay attacks applied from a malicious GCS against weak uplinks of FPV channels. Rodday (2016) presented in Asia Black Hat Conference techniques for hijacking a $30k drone, used by police departments, by exploiting the XBee 868LP protocol and using replaying maneuvering commands that are sent over 868 MHz from the GCS to the drone. Highnam et al. (2016) showed that amateur drones whose uplinks are based on the MAVLink protocol and can be found on amateur drones (e.g., 3DR IRIS+, Erle-Copter) can also be hijacked using a replay attack. Davidson et al. (2016) demonstrated a method of hijacking a drone by spoofing its downward camera. He influenced the stabilizing algorithm, by directing a laser and projector to the surface of a flying drone. Some studies presented methods for hijacking and disabling a drone using GPS spoofing of No-Fly Zones, during autonomous navigation to a target (He et al., 2019; Kerns et al., 2014). Protocol employs algorithms, often enhanced with artificial intelligence, to take control of the UAS with a new communication link, that removes the UAS from the threat environment. The manipulating signal gives a third party the opportunity to neutralize the UAS, by taking over the flight and downloading its data. However, this method may not be effective, when command and control communications are encrypted, or when using proprietary protected protocol.

Kinetic Interdiction

Many types of kinetic options are being proposed by researchers and industry. Their deployments have been tested mainly: i) on the battlefield in military missions; ii) for the security of executive and government officials; iii) in high-level special events. Such kinetic measures include:

- Net Capturing: is the attempt to physically capture a drone. An enforced and hardened UAV flies toward the intruding drone and carries attack nets, in order to seize and bring back targeted UAS. Such systems work on relatively short distances and are effective when the nefarious drone navigates with a low speed or it does not maneuver.

- Birds of Prey: are trained birds with protective gear, which are used to attack and grab UAS, when entering into a restricted area. However, birds are also restricted and pose hazards, when flying around airport areas, due to possible conflicts with arriving and landing aircrafts.
- High Power Microwave (HPM) or Laser Fire: Using high-power electromagnetic pulse or laser weapons, security teams are able to target and shoot down UAVs. HPM or laser high energy destroys electronic circuits and other vital segments of the drone's airframe. It often causes UAV's crash to the ground.

However, outside military use, kinetic techniques may not be a viable option for use, especially in crowded areas, due to the risk drone's uncontrolled crashing or triggering the deployment of CRBNE payloads. In most cases they are not suitable for airports and surrounding airspace, due to collateral hazards to aviation operations. Therefore, all these kinetic interdiction measures may not be legal, depending on civil aviation rules.

Benefits and limitations of mitigation measures against misused drones are summarized in Table 4.12, where we can notice common drawbacks for all measures in their legitimate applicability into airport complicated environments.

Table 4.12: Comparing C-UAS mitigation measures

Method		Benefits	Limitations
Electronic Interdiction / Signal Jamming	RF Jamming	Use RF transmission to block signals and disrupt C2 between the GSC operator and UAV	RF interference in crowded RF areas. May also jam and interrupt other communication signals
		Medium range up to few kilometers, depending emitting power	Can't affect autonomous driven drones (without an active RF link)
		Static, mobile, or handheld device	Illegal use for many countries.
		Programmable based on RF sensor scanning	May cause uncontrolled UAV flight and crash
		Disrupts Radio Frequency (RF) communication link Can include WiFi links	Needs special licensing for approval use, based on Electromagnetic compatibility regulations
		Use of directional Jamming to minimize interfering	A jammer's ability relies on the strength of its radio transmitter
	GPS Jamming	Replaces GPS communication, increases difficulty to control the drone	Can't work if UAVs disable GPS, or use of encrypted GPS (military mission)
		Medium to short range, depending on satellite constellation	Dangerous when used near airports, because airplanes also use Satellite Navigation
		Disrupts Global Positioning Satellite communication link	Illegal procedures in many countries. Needs special licensing for approval use
		Prevents the return to home functionality	May cause uncontrolled UAV flight and crash

Method		Benefits	Limitations
	Protocol Manupulation	Replaces communication link and takes control of drone operation	Illegal procedure for civilian use, against computer fraud and abuse act
		Employs algorithms enhanced with Artificial Intelligence	Not always successful, especially when encryption is used for C2 links
		Can drive malicious UAV to designated area	Complicated method, not always successful.
		Low cost tecnique, based on attackers ability	Can't affect autonomous driven UAVs not using GPS
Kinetic Physical	UAV Net Capturing or Birds of Prey	Active and aggressive counter measures	May cause collateral fatalities to other aircrafts. Not appropriate for airports
		Net Capturing: Enforced and hardened UAVs physically capture a drone	Net capturing efficiency depends on UAVs flight behavior, reaction time etc.
		Birds of Prey are used to attack and grab UAS	Birds also pose hazards, when flying around airports
		Captures & drives UAV in specific area.	Depends on speed or maneuver capabilities of rogue UAV
Kinetic Electronic	High Power Microwave or Laser Guns	Aggressive & Long Range countermeasures	Can have negative effects other passing aircrafts with fatal consequences
		Destroys electronic systems of UAVs	May cause uncontrolled UAV flight and cash
		Disables drone flight	Illegal in civil aviation context. Violated Aviation Security Laws

In many countries worldwide, mitigation counter-drone systems are not allowed to be used in civilian environments, but only when applied by police and military operations. There is some confusion and ambiguity to legal liabilities of C-UAS technology use, subject to numerous overlapping laws (such as Aviation Security Laws, Computer Security and Electromagnetic Compatibility Regulations). Adding to this ambiguity is the fact that most governments have not yet established comprehensive C-UAS-specific policies for protecting aviation assets, while airspace regulators continue to develop regulations for UAVs integration into commercial and civilian uses.

4.3.5. Counter UAS Applied technologies in commercial systems

In addition to academic research publications, in this subsection, we have collected information about available C-UAS products and counter drone technologies applied in commercial systems. Searching open source databases for marketed counter drone systems, we have investigated their technical characteristics and present a statistical analysis of sensor's technology used. There are at least 545 counter-drone products, based on open-source information, commercial publications and press releases. C-UAS systems have been divided into three main categories, as presented in table 4.13, where 178 systems (or 33%) have been designed only for detection purposes, using a variety of detection sensors. The majority of C-UAS products, which are 218 systems

(or 40%), provide mitigation technologies with interdicting UAV capabilities, while 149 systems (or 27%) are capable of both detection and mitigation.

Table 4.13: C-UAS Products available in the market or under development

Number of C-UAS Products	545	%
Systems Capable of Detection	178	33%
Systems Capable of Mitigation (Interdiction)	218	40%
Systems Capable of Both Detection and Mitigation	149	27%

Basing our analysis on C-UAS technical characteristics, in Figure 4.24 (a) we have plotted the percentages of C-UAS systems, which are capable of detection and mitigation, while in Figure 4.24 (b) the number of sensors used for detection purposes in every system are exhibited. As shown in graph 4b, the majority of C-UAS systems (52%) use a single sensor for detection and mainstream method is RF scanning, mainly due to cost-benefit advantages. More advanced and expensive systems are using a combination of two or more sensor types (36%), usually combing primary surveillance methods with visual sensors. A minority of C-UAS systems (12%) employs a combination of 4-5 different sensor types, integrating RF sensors with visual cameras (both optical and infrared) and acoustic sensors.

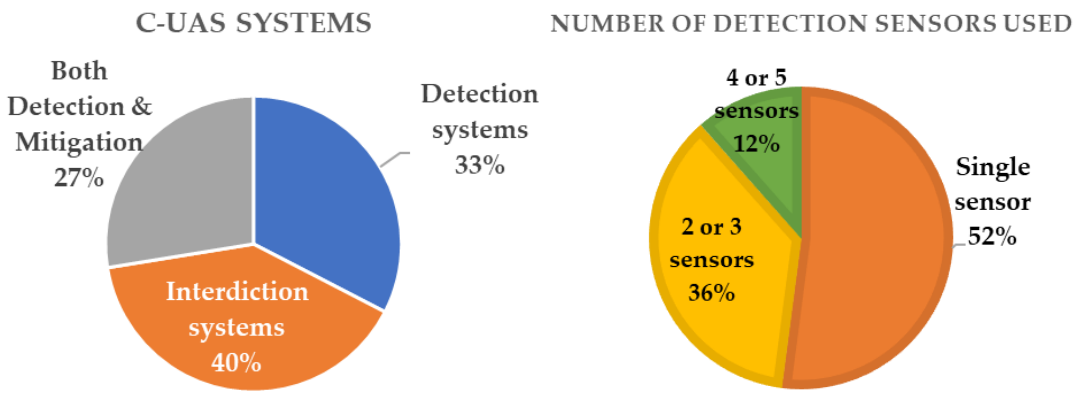


Figure 4.24: (a) Detection/Mitigation Technologies, (b) No of Detection Sensors

Radio Frequency scanners and Radars are the most commonly used detection elements as shown in in Figure 4.25. Radars are used in 159 (28%) systems, while RF in 147 (26%) ones. Visual systems are also popular with 40% of systems employing cameras for supporting RF detection. Electro-optical cameras and Infrared systems, which are often used in conjunction, equally applied in C-UAS systems,

with a percentage of 20% each. Acoustic sensors are less common in use with 6% application in products and mostly in conjunction with other detection technologies.

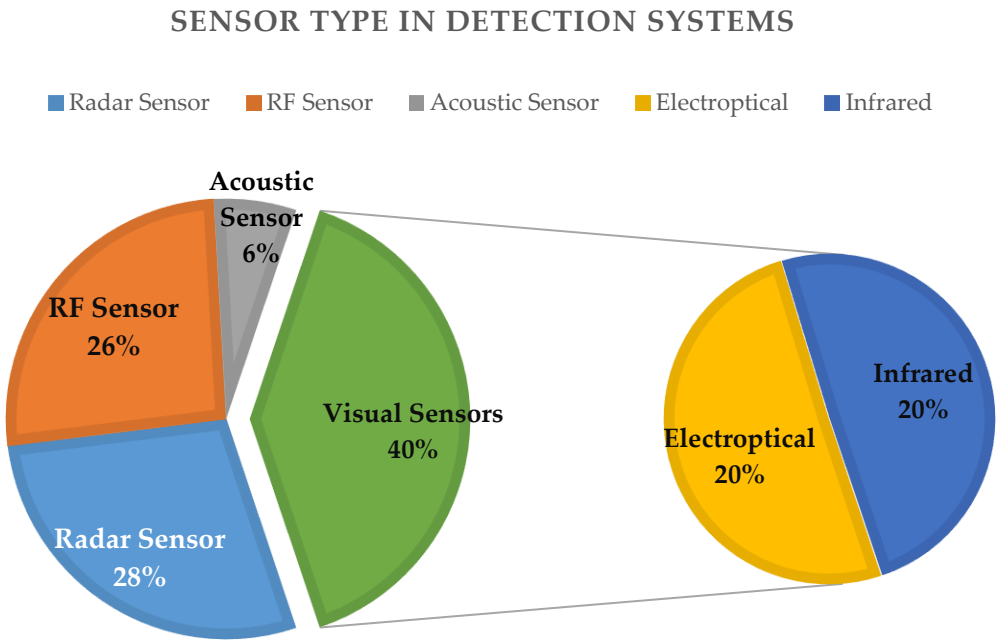


Figure 4.25. C_UAS systems: Type of sensors used for detection

From the 367 available systems, which have mitigation capabilities (either stand-alone or combined with detection sensors), 147 (or 40%) rely on a single mitigation technique, while 215 (or 58%) rely on two or more techniques. In Figure 4.26, types of sensors used for mitigation purposes are presented. RF and GNSS jamming techniques are counted distinctly, although they are often used in conjunction. Signal Jamming (both RF and GNSS) is the most common interdiction method with a percentage of 76% use in systems. Nine per cent of systems have spoofing capabilities, while kinetic methods are used in 15% of systems examined. Among kinetic methods, 18 (or 8%) involve lasers, 27 (or 5%) employ nets, and 8 (or 2%) use a sacrificial UAV able to attack against intruding drones. Jammers are most commonly used for disabling drones. Some anti-drone jammers are directional RF transmitters in the form of mobile shooting guns that apply jamming to GPS signals and ISM bands, known to be used by drones (ISM bands are frequencies reserved internationally for Industrial, Scientific, and Medical purposes).

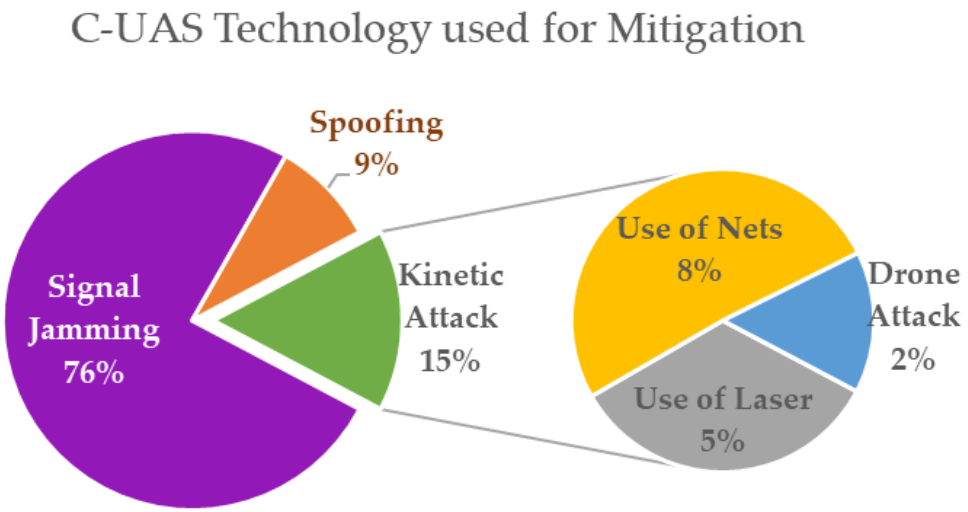


Figure 4.26. C_UAS systems: Type of Sensors used for Mitigation Purposes

4.3.6. Attacks with Drones in Airport Critical Infrastructures: Scenario Analysis

Having examined the available sensor technologies and counter measures for defending misused drones (both in industry and academia), in this section we extend previous research on Airports Cybersecurity (Lykou et al., 2018a) and Aviation Cyber-resilience (Lykou et al., 2018b). Therefore, in this work we present and analyze various attack scenarios, using s-UAVs (small drones) against airport facilities. Our main purpose is to exhibit security and safety risks from misused drones and propose appropriate C-UAS and counteractions, which are efficient and applicable in airports and support aviation resilience against airborne threats.

In Figure 4.27, a typical Airport Layout is presented, which includes: i) airport runways; ii) aircraft parking areas; iii) passenger terminal buildings; iv) near to airport installations, supporting air traffic management; and v) connecting public transport infrastructures. In this layout, we have marked with spot numbers {1, 2, 3} locations, which are open to public and may be used as spots for launching UAV attacks. Each spot number is associated with the number of scenarios presented below. The following three categories of attacks have been analyzed:

- **Scenario (1):** Drone attack to remote located or unmanned sites nearby airports, which support Air Traffic Management (ATM) Critical Infrastructures
- **Scenario (2):** UAS attack against airport wireless systems, information systems and data links
- **Scenario (3):** Drone Attack to ATM Systems, jeopardizing flight safety of manned aviation.

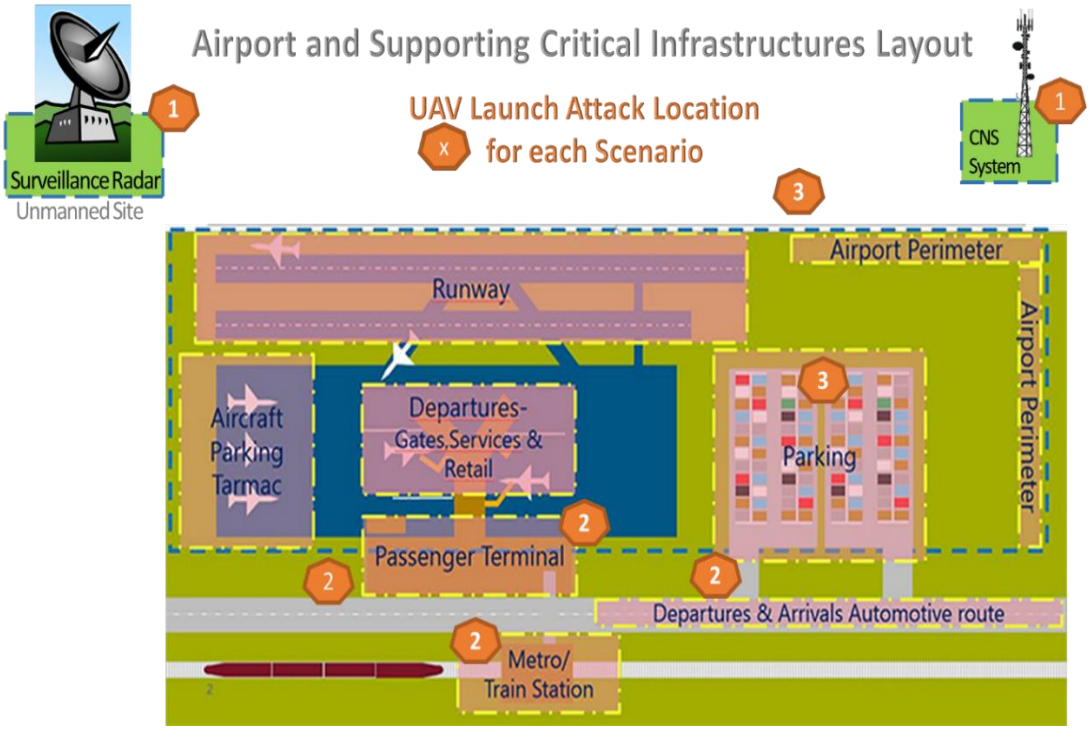


Figure 4.27: Typical Airport Layout and possible locations for launching a UAV attack on Airport CI *(where each location spot number is connected with the no. of scenario presented)*

Each attack scenario is complimented by the following: a) Attack Target Background, which presents vulnerabilities and related research on similar attacks; b) Graphical Representation of attack scenario c) Attack Analysis on step-by-step basis; d) Impacted Assets; and e) Impact evaluation with resuming impact analysis table.

As we can notice in figure 4.27, these three attack scenarios may be launched from different spot locations (inside and outside airport premises) which are: a) near or inside passenger terminal area; b) in parking area; c) near public transport connections (bus/metro/train station); d) near or outside airport perimeter; and e) in peripheral ATM sites, which are located outside airport perimeter. These eight spots are public locations accessible to all, often overcrowded and often with less strict security measures. As a result, the scenario analysis presented below, as escalated on a step by step basis, covers almost all possible attacks, which can be performed by malicious actors, exploiting UAS capabilities inside and around airport facilities.

Scenario 1: Drone attack to Unmanned Sites, supporting ATM CIs

Attack Target Background: Spying Aeronautical Telecommunication systems for vulnerabilities and information gathering is the first step for target reconnaissance, when preparing a malicious attack. Drone's FPV channel provides an excellent tool for a malicious operator to spy any target without being detected, since the operator can maneuver the drone and collect information from miles away. UAV's attached camera can capture data, obtain high quality pictures, record video and send back information gathered about vulnerabilities scanned, in order to prepare a successful attack. Several studies have shown that drones equipped with radio transceivers can be used for extracting unencrypted information from radio transmissions, or even create RF noise or telecommunication interference (Nassi et al., 2019). Besides, drones can cause a significant damage to unmanned sites, which supports Aeronautical Telecommunication systems, by carrying explosive payloads and even by self-exploding, while targeting into antennas, navigational aids and other critical infrastructures. Such incidents had already occurred in the past, in many airports like in S. Arabia and Middle East Areas, causing serious fatalities.

Graphical Attack Representation of drone attack to unmanned ATM CIs is shown in Figure 4.28.

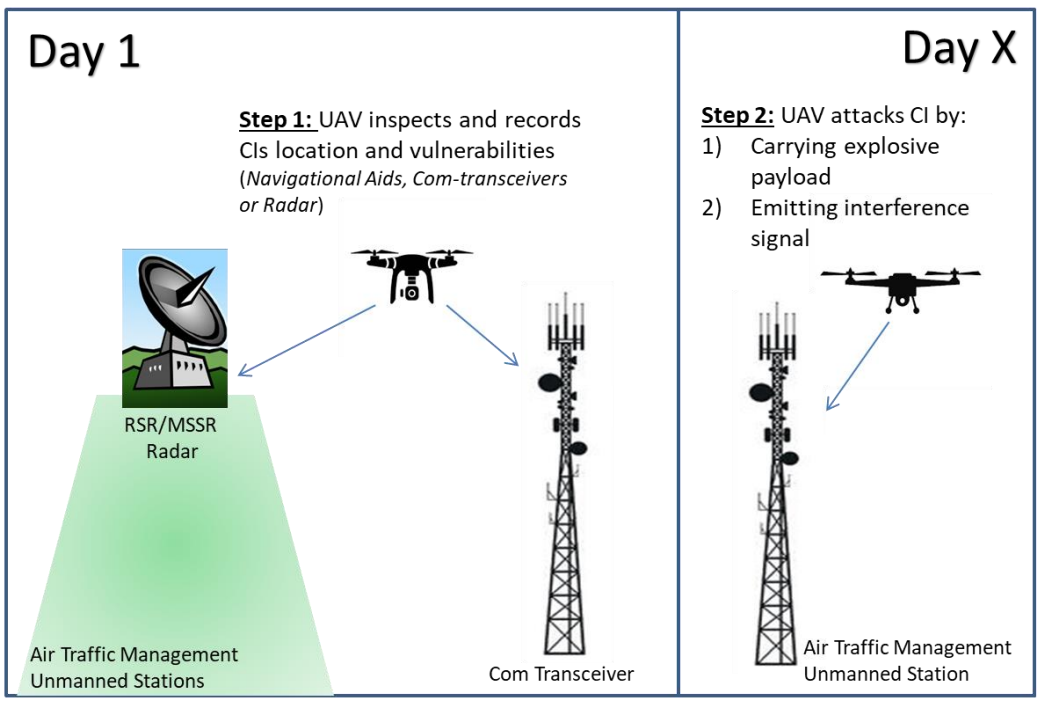


Figure 4.28: Drone attack to unmanned Air Traffic Management (ATM) CIs

Attack Scenario Analysis

Step 1: A UAV driven by malicious user can perform a reconnaissance flight above and nearby Aeronautical Telecommunication systems, in order to monitor and record site vulnerabilities, with the intent to prepare an attack after a period of time. The drone can be equipped either with video-camera, optical sensors with night vision capabilities (for after dark flights) or Radio Frequency (RF) analyzer to detect wireless communication and RF signals.

Step 2: If step 1 is successful, after a period of time, having elaborated all information gathered about the attack target, the UAV can realize: i) a physical attack by carrying either explosive payload against physical integrity of CI facility, or ii) a cyber-attack by using RF jamming equipment to interfere with existing ATM communication systems.

Impacted Assets: Communication, Surveillance and Navigation (CNS) systems which are often unmanned sites, far away from airports main establishment. These systems include: a) Aeronautical Telecommunication systems; b) Navigational aids which provide guidance, location, and direction to airplanes; c) Surveillance systems (Primary and Secondary Surveillance Radars), which detect and report the position of aircrafts for air traffic control purposes. Very-high frequency Omnidirectional Ranges (VOR), which are often located nearby airports and provide a bearing to and from the station, along with magnetic direction. Non-directional beacons (NDB) which broadcast a signal on an AM frequency to support the pilot's direction and orientation. In addition to CNS, supporting equipment may be affected like: Power Supply & HVAC (Heating Ventilation Air-Conditioning) stations, where stopping or downgrading their operation may create cascading operational problems to main CNS systems and airport CIs operation. All the above assets, which are often located in distant areas from airport security systems (in unmanned sites), may be vulnerable to aerial attacks.

Impact Evaluation: CNS systems are exposed and, when assaulted by a malicious UAVs, may lose integrity and their operational efficiency. This results in ATM services degradation and traffic flow slowdown for safety precautions. Moreover, air space capacity limitations, flight delays or cancelations may also occur. Economic losses to air navigation service providers and aircraft operators, due to downtime for repair and integrity checks. Material or service loss and additional legal liability to air navigation providers and/or airport facilities. Table 4.14 presents impact evaluation for each step of attack scenarios analyzed. The table includes impacted assets and description of areas impacted (Economic, Legal, Reputation, Human or Material/Service loss), along with information security impacts, affecting Confidentiality, and/or Integrity, and/or Availability.

Table 4.14: Impact Analysis of Scenario 1

Threat/ Hazard	Impacted Assets	Impact Analysis		
		Description & Impact Areas(*)		on CIA(**)
Spying Aeronautical CNS systems for vulnerabilities and information gathering	Air Traffic Management Communication, Surveillance and Navigation (CNS) systems, such as: - Navigational aids (VOR, NDB, DME) - Surveillance systems (RSR, MSSR) - Aeronautical Telecommunication systems. - Power Supply & HVAC remote stations	Site and System Vulnerabilities exposure	R, L	C
The drone equipped with Radio Frequency (RF) analyzer detects wireless communication and RF signals.		RF signals exposure	R, L	C
UAVs carry RF jamming equipment to interfere to existing RF signals communication systems		CI operation interference, signal jamming and com loss. Air space capacity limitations	E, M, R, L	I, A
UAVs carry explosive payload against physical integrity of CI facility		CI physical damage. Loss of operational efficiency. Air traffic flow slowdown for safety precautions. Human Injuries	E, H, M, R, L	I, A

(*) Impact Areas: E= Economic, H= Human, M= Material/Service Loss, R= Reputation, L= Legal.
(**) Impact on Information CIA: C=Confidentiality, I=Integrity, A=Availability.

Scenario 2: UAS attack on Airport's Wireless Network and IT Infrastructures

Attack Target Background: Airport operations center, supported by a central information network, connects airport facilities and serves as an interaction point for all airport community stakeholders. It manages processes from airside and flight control systems to landside operations and ground handling systems. As a result, in modern airports, operations center acts as the central point of command, effectively managing every data interchange and information sharing. Information is extracted from a series of sensors and smart devices and communicated though wireless LANs (802.11) or wide area wireless networks (WiMax, Lorawan), using ground-based line of sight data-links, due to expanded airport borders. Drones equipped with wireless antennas and software can take advantage of access point communications and can sniff and capture data packages, sent between wireless connected devices. Recent research (SESAR JU, 2016), has proven that drones can be used, in order to monitor an access point, capture the communication packets and record detailed network

information. According to Gittleson (2014), malicious software can be installed on a drone (called Snoopy) to harvest personal information and to track and profile smartphone users. Snoopy can also sniff RFID, Bluetooth, and IEEE 802.15. A Snoopy drone can exploit the WiFi, impersonate the identified network and trick smart devices into joining it, so as to collect all the information entered on this disguised network. In addition, UAVs can perform 3D through-wall mapping, leak data from air-gap computers, or even carry traditional spying devices to eavesdrop on conversations (Nassi et al., 2019). With the use of RFID tags, attack targets can be traced by a RFID reader at distances varying from one up to few hundred meters. As a result, UAV equipped with RFID reader can trace RFID tags, navigate and locate themselves via specific points and identify attack targets. All the above attacks to wireless networks can be performed by a sUAS in an airport environment, which is overcrowded with passengers, airport community employees and various commercial activities, full of wireless communications and smart applications.

Graphical Attack Representation of drone attack in airport facilities assisted by an insider is shown in Figure 4.29.

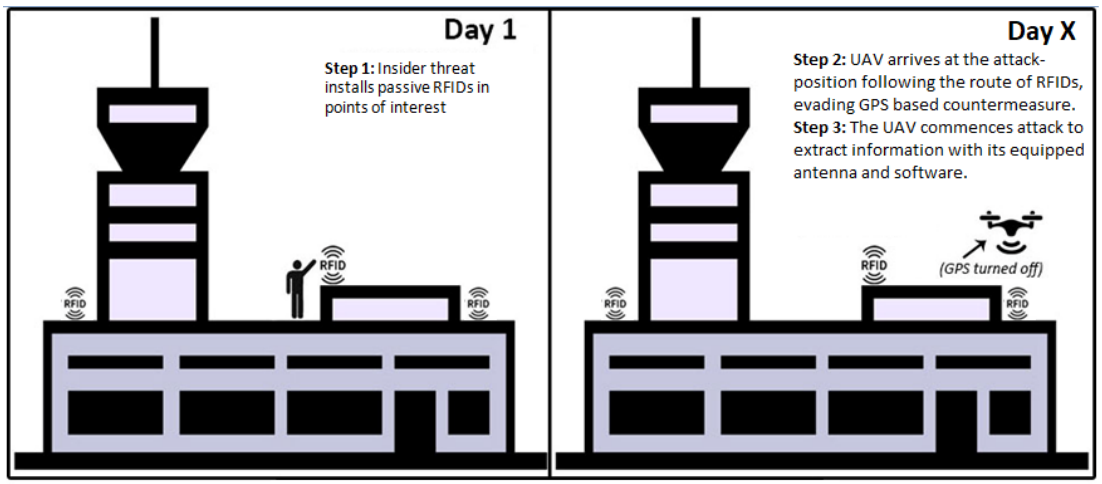


Figure 4.29: Drone attack in airport facilities assisted by insider

Attack Scenario Analysis

Step 1: An insider takes advantage of free entrance on the rooftop of the building and/or nearby facilities and infrastructures, without being noticed by security controls. He is able to distribute RFID tags, in order tomark sensitive locations, e.g. airport server rooms, wireless routers, array of integrated smart sensors, or security cameras network.

Step 2: A mini UAV performs an attack some days later, targeting distributed RFID tags. Assuming that airport has counter measures against drones and in order to avoid

geofencing, the UAV turns off GPS navigation system and follows the route identified by distributed RFID tags, towards its attack-position. As a result, the drone requires fewer energy to be guided at its destination, relative to a GPS-navigation, so this expands its flight endurance time. Its small size and low altitude flight can make the UAV untraceable for ground surveillance radars, while anti-drone protection, based on GPS-spoofing, cannot affect its route towards attack target.

Step 3: If not traced, the UAV identifies its target and while equipped with wireless antenna and supportive software, it can take advantage of vulnerable access point communication. As a result, it can sniff and capture the packages sent between Wi-Fi connected devices and wireless sensors, extract information and send it back to its malicious center of command. Likewise, a drone can perform an acoustic attack to capture and record voice communications and reveal sensitive information. Even worse, it can also perform a physical attack, by carrying an explosive payload.

Table 4.15: Impact Analysis of Scenario 2

Threat/ Hazard	Impacted Assets	Impact Analysis		
		Description & Impact Areas(*)		CIA(**)
An insider installs passive RFID in the location above a server room, router, array of integrated sensors or data center	Airport Operations Centre, the central network which handles all the decisions and processes from flight control to ground handlers. Such Assets include: -Server rooms - WI-FI routers - Integrated sensors used for airport smart monitoring - Airport data center - Passenger handling systems, -Automated vehicle identification and RFID based asset tracking systems	Airport sensitive information and critical infrastructure exposed	R, L	C
UAV equipped with wireless antenna accesses communication links and captures data packages sent between Wi-Fi connected devices and wireless sensors to extract information towards a malicious center of command.		Confidentiality Breach, Data exposure. Passengers' and personnel' personal information can be stolen	E, R, L	C, I
UAV performs an acoustic attack recording valuable private information.		Confidentiality Breach	R, L	C
UAV performs physical attack against CIs, if carrying an explosive payload		CI physical damage. Human injuries or Loss of life. Air traffic flow & Airport stops for safety precautions	E, H, M, R, L	I, A

(*) Impact Areas: E= Economic, H= Human, M= Material/Service Loss, R= Reputation, L= Legal.
(**) Impact on Information CIA: C=Confidentiality, I=Integrity, A=Availability.

Impacted Assets: Server rooms, Wi-Fi routers, smart sensors used for airport operations monitoring and airport data center security may be put in jeopardy. Passenger handling systems, automated vehicle identification, RFID based asset tracking systems may be impacted. Communication confidentiality, including ground-based line of sight datalinks and ATM signals may be compromised.

Impact Evaluation: Information, communication, surveillance system can be disrupted, downgrading airport services. Airport's operation can be disorganized or forced to close certain services, if data leak is detected. Passengers and employee's personal information can be disclosed or stolen, leading to legal liabilities, economic fines and reputation loss. Airport sensitive corporate information may be exposed to malicious actors. Airport operations will be forced to stop operations for safety reasons, if UAV is detected in restricted air space areas. Table 4.15 presents impact analysis for each step of attack in scenario 2 and impacted assets.

Scenario 3: CyberPhysical Attack to Air Traffic Management Systems & Manned Aircrafts

Attack Target Background: ADS-B (Automatic Dependent Surveillance - Broadcast) system is an emerging surveillance technology, recently introduced in aircraft navigation, as the cornerstone of airspace management modernization. ADS-B transponder periodically broadcasts information about aircraft's current position and enables to be tracked from surveillance systems. The information can be received by ATC ground stations and by other aircrafts, in order to provide situational awareness, allowing self-separation and supporting Traffic Collision Avoidance Systems (TCAS).

However, according to many researchers, a plethora of active attack scenarios and serious security breaches have been presented, posing at risk integrity of surveillance systems. The system is susceptible to hacking, where attacks may range from passive actions (eavesdropping) to active attacks with the use of malicious drones. ADS-B and ATM radio technologies are broadcasted unencrypted. As a result, a well-equipped attacker can receive and send messages, or overshadow existing signals. In addition, due to weak security posture of satellite communications, hundreds of in-flight aircrafts are accessible and vulnerable to message jamming, replaying of injection and other active attacks.

Graphical Attack Representation of communication attack on ATM systems is shown in Figure 4.30.

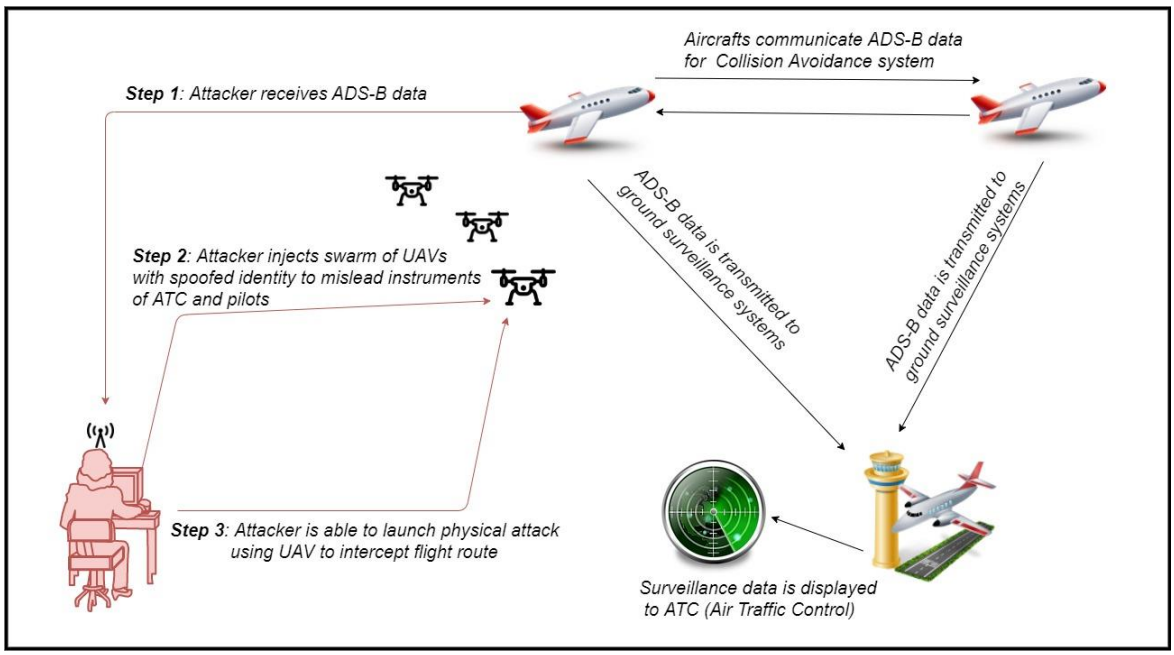


Figure 4.30. Communication attack on ATM systems

Attack Scenario Analysis

Step 1: Attacker is located near the airport facility and he is equipped with Software-Defined Radio supported by an ADS-B receiver/transmitter chain with GNU Radio. Based on this equipment, he receives ADS-B data from passing over aircrafts. As a result, malicious user is able to collect air traffic information about aircrafts traversing the area and transmitting their position (aircraft type, identification mark, position coordinates, altitude, speed, direction, destination etc.), in order to prepare his attack.

Step 2: Attacker launches into designated airspace a single UAV or a swarm of drones, equipped with ADS-B transponders. Their identity is spoofed, based on data collected on step 1 (replay attack). Hence, malicious drones transmit false ADS-B data, pretending to be commercial aircrafts. As a result, confusion is created to airport's surveillance system and ATM, which forces Air Traffic Control to stop air flights in the impacted area for safety reasons.

Step 3: Even worst, attacker may escalate, by launching a physical attack against approaching aircrafts, since data collection about airplane's position, destination and technical data, enable him to calculate airplane's position in future time, so that to target and send a UAV towards this aircraft. This midair collision hazard can cause safety issues with serious fatalities and damage to both aircrafts, especially during take-off or landing.

Impacted Assets: Air Traffic Control, Secondary Surveillance System (ADS-B Data), Aircraft Safety during Take-Off or Landing Phases, aircraft safety and separation minima can be violated. Airport's infrastructures and manned aircrafts may be seriously damaged from uncontrolled UAV flight and crash, in case of mid-air collision hazard. Last but not least, human loss or injuries are also intolerable.

Impact Evaluation: Surveillance integrity is threatened and air traffic can be disrupted, or downgraded for safety reasons. ATC operations should immediately close violated airspace. Aircrafts safety is jeopardized, standard routes may be deviated, flights are cancelled and air traffic is diverted to other airports. A serious accident with aircraft may cause fatalities, serious material loss and destruction of airport's CIs. The airport will close for further incident/accident investigations with serious economic losses and negative reputation. Table 4.16 presents impact evaluation for each step of attack in scenario 3, along with impacted areas analysis.

Table 4.16: Impact Analysis of Scenario 3

<table>
<tr><th rowspan="2">Threat/ Hazard</th><th rowspan="2">Impacted Assets</th><th colspan="3">Impact Analysis</th></tr>
<tr><th colspan="2">Description & Impact Areas(*)</th><th>CIA(**)</th></tr>
<tr><td>Attacker is equipped with ADS-B tracing system and receives traffic data from passing over aircrafts.</td><td rowspan="4">Air Traffic Control, Secondary Surveil-lance System (ADS-B Data), Aircraft Safety during Take-Off or Landing Phases, Se-paration Minima, Aviation Safety Rules</td><td>Surveillance and ATM systems confidentiality is compromised</td><td>L</td><td>C</td></tr>
<tr><td>Attacker injects into airspace single UAV with ADS-B spoofed identity to create confusion to airport's surveillance system and ATM.</td><td>Surveillance integrity is compromised and air traffic can be disrupted, or downgraded for safety reasons</td><td>E, H, M, R, L</td><td>I, A</td></tr>
<tr><td>Attacker injects a SWARM of drones equipped with ADS-B systems to create confusion to airport's surveillance system and ATM.</td><td rowspan="2">Aircraft safety is jeo-pardized and separation minima are violated. A serious accident with aircraft may cause fatalities and serious destruction in airport's CI</td><td>E, H, M, R, L</td><td rowspan="2">I, A</td></tr>
<tr><td>Attacker launches a physical attack against passing over aircrafts, during take-off or landing</td><td>E, H, M, R, L</td></tr>
</table>

(*) Impact Areas: E= Economic, H= Human, M= Material/Service Loss, R= Reputation, L= Legal.
(**) Impact on Information CIA: C=Confidentiality, I=Integrity, A=Availability.

4.3.7. Proposed counter measures for airports

Airports may differ in size, design layout, air traffic flow and capacity, proximity to populated areas, etc. However, some hazards associated with UAVs are common to all airports, overpass standard security measures and should be addressed in priority, while examining UAV integration in airports operations. In civilian airspace, drones aren't yet required to carry transponders, so they cannot be detected and tracked with existing air traffic control systems. Relying on visual observation to detect drones is equally ineffective, since s-UAV can become invisible to the naked eye. Although detection methodologies for tracking drones have been developed, the small size of drones and the variety of design and material used in UAVs pose challenges to detection systems. In this subsection, we propose countermeasures for preventing, detecting and defending misused drones from invading into airport premises. For each scenario, a proposed C-UAS protection plan is designed and graphically presented, aiming to increase airport's resilience and robustness.

Scenario 1: Drone attack to Unmanned Sites that support ATM Critical Infrastructures

CI vulnerability is higher, when an asset is remotely located, in unmanned sites. In the first scenario, with inadequately secured ATM sites, it is important to establish geofencing barriers, as standard preventing measure. Due to lack of physical protection measures from airborne threats, enhanced safety geofencing zones of 6-10km around ATM sites, are required. They should be designed, legislated and communicated to all aviation stakeholders and UAV industry, while being integrated into publicly available Aeronautical Information Packages (AIP). In addition, a sensor detection system must be installed, able to track, identify and locate any incoming drone, which may overpass Geofencing areas. A wide-area surveillance radar or RF detectors are proposed, as primary detection method. Moreover, secondary sensors, such as electrooptical or infrared cameras, may support detection system and confirm the type of intruding UAV, while also providing additional information about its payload. For example, a PTZ (Pan-Tilt–Zoom) camera may be able to show, whether a drone appears to be carrying explosives, or simply a video camera for information gathering and record keeping. Installation of video surveillance systems, with remote monitoring connection to airport's security operations center is also proposed, instead of enhanced physical protection of unmanned sites with security guards. However, security operators may only have a limited window of time, to make decision and take countermeasures, whenever an incoming drone is considered malicious. In our case, assuming that: a) the incoming drone is travelling with an average speed of 10-20m/s, and b) a geofencing perimeter

of 6km exists; the available response time is between 5-10 minutes, from invasion time into restricted zone, before target is reached. The proposed C-UAS protection plan for Scenario 1 is graphically presented in Figure 4.31.

Finally, regular integrity checks and calibration of ATM equipment performance, backup and redundancy design for critical assets, along with contingency operational plans for ATM services are also effective resilience measures. These will enhance integrity and availability of aviation services, in case of emergency or failure and prevent Air Navigation Service Providers (ANSP) from service degradation, while being under attack.

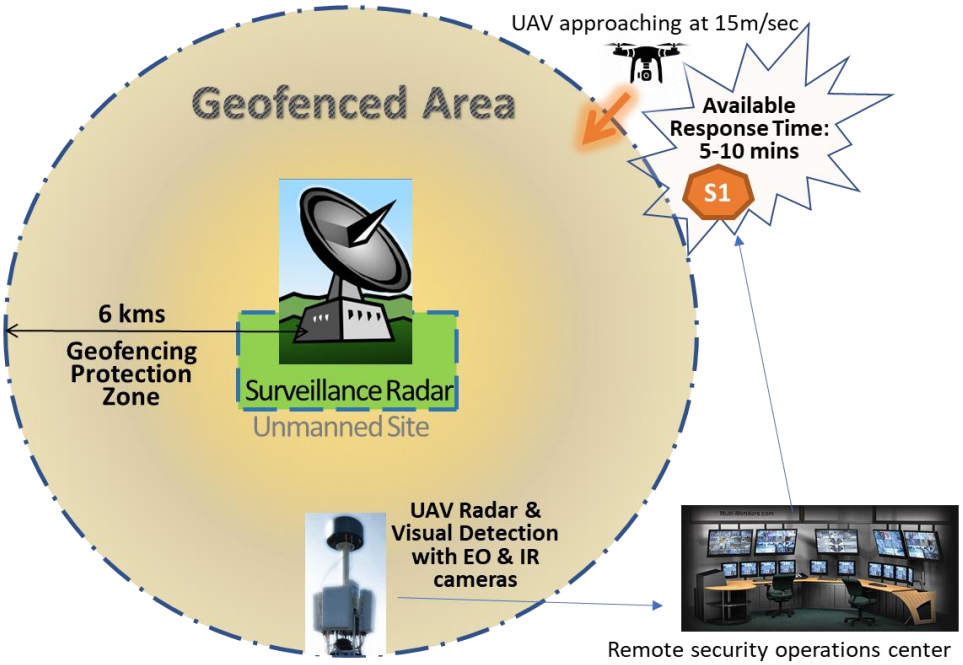


Figure 4.31. C-UAS protection plan for Scenario 1

Scenario 2: UAS attack on Airport's Wireless Network and IT Infrastructures

In the aviation context and according to national and international regulations, almost every airport has built appropriate airspace limitations and prohibited areas, according to state Aeronautical Information Packages (AIP). These restricted areas are usually protected by Geofencing shell, acting as a virtual security shield that keeps drones away, when their navigation is based on programmed GPS data. In our scenario, since malicious actor has turned-off GPS, to avoid geofencing, only detection sensors can protect airport from such nefarious drone flights. Surface surveillance radar system in airport premises should be able to track sUAS, slow-moving or hovering over airport critical infrastructures. When systems are supported by secondary sensors, such as electrooptical or infrared cameras, C-UAS can monitor

and record any unauthorized UAV flight. They can also provide additional information about drone's payload. These detection sensors should be distributed around airport perimeter and especially covering public access areas, based on security expert's risk assessment. However, it is more important to be able to locate and capture UAV pilot, than chasing any flying object, while approaching airport facilities. Therefore, security guards should be adequately trained, in order to perform regular security patrols, carry mobile RF scanners and be able to forestall any UAV illegal flight, even before starting. Some kinetic counter measures could also be applied by security trained personnel, (e.g., launching net capturing drones, or using directed RF jammers), provided they are compatible with aviation rules and authorized by civil aviation.

The potential of insider threat, exposing airport vulnerabilities should be eliminated. Airport community and employees should be well informed and discouraged with appropriate measures. They have to be alerted, act as spotters and inform security agencies, in case of any suspicious drone sighting. In addition, Close Circuit Television System (CCTV) for 24h surveillance will discourage malicious insiders from mis-performing, or when considering any action opposed to airport security. The proposed C-UAS protection plan for Scenario 2, with detection sensors distributed around the airport perimeter and close to public accessible areas, is graphically presented in Figure 4.32.

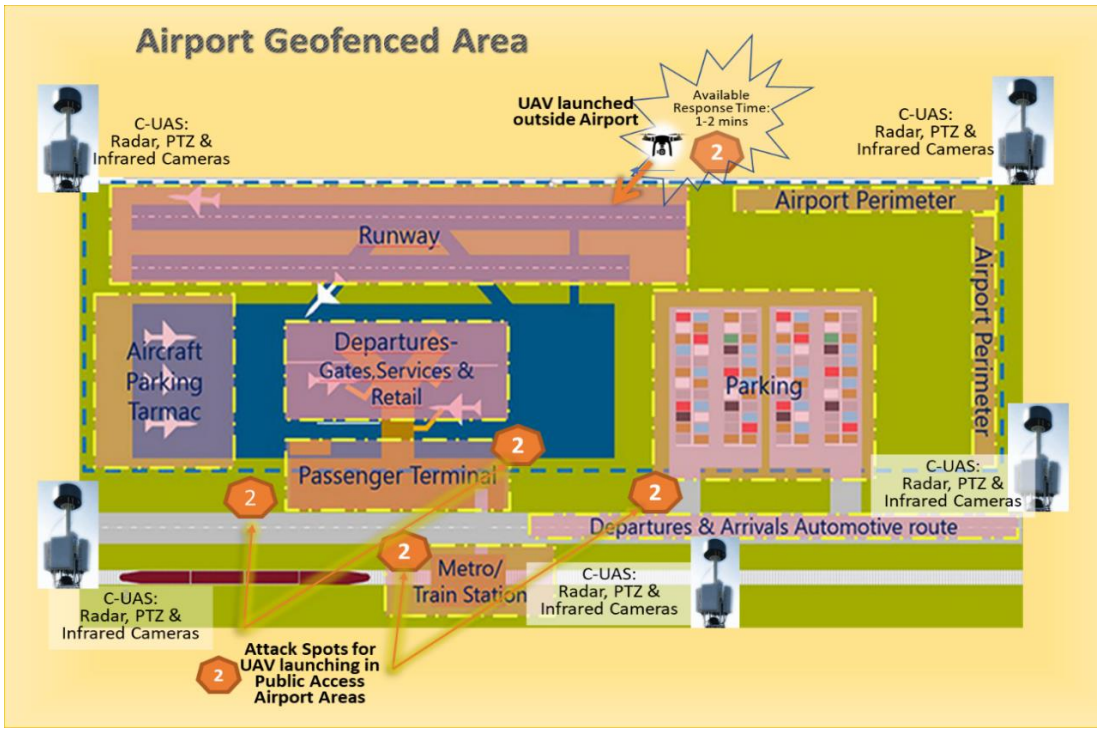


Figure 4.32. C-UAS protection plan for Scenario 2

Scenario 3: CyberPhysical Attack to Air Traffic Management Systems & Manned Aircrafts

Terminal airspace is required to be adequately protected and cleared by mitigating any airborne hazard. It is obvious that uncontrolled flying, landing or crashing of UAV with area obstacles or land is an unacceptable situation in the aviation context. If an attack is launched, outside Airport Perimeter, response time may vary in minutes, depending on launching spot distance and average UAV navigation speed. However, in case the attack is launched inside airport premises, available response time is only few seconds, so it is vital for security teams to immediately react and prevent such actions, as proposed in scenario 2. Enhanced geofencing, using a 3-dimensional bow-tie shape to create virtual fences, according to airport's risk management suggestions, is an effective preventing measure. Thus, geofencing warning zone expands available response window for both ATM controllers and security guards, to detect, identify and react to incoming misused drones, from few seconds to few minutes, as presented in Figure 4.33.

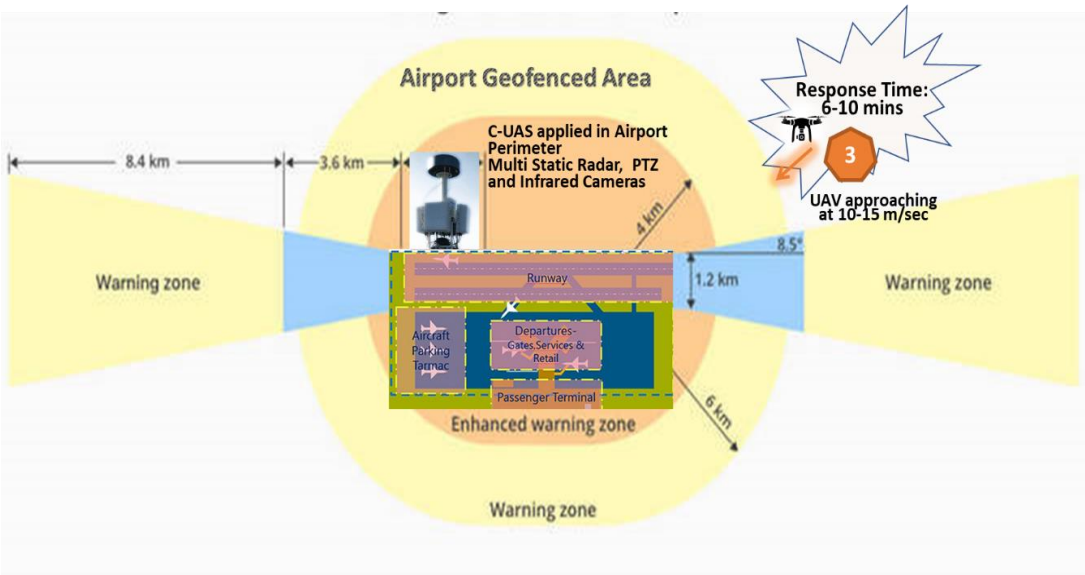


Figure 4.33. C-UAS protection plan for Scenario 3

Moreover, detection measures including surface surveillance radar, RF detectors and visual sensors should be expanded in the vicinity of airport, provided that they are compatible with aviation rules and they are legally authorized. Air traffic control should receive data validated and multilaterated by surveillance radar systems, so as to be able to distinguish malicious drones from airplanes, if their identity is spoofed. Confidentiality and authenticity features in data traffic should be enhanced with cryptographic protection for ADS-B systems. ANSPs have to upgrade surveillance

technologies used by current network of primary and secondary radars, in order to support and complement ADS-B technology.

Last but not least, public awareness with safety promotion campaigns of UAS No Fly Zones, along with educational leaflets and advertisements will minimize uninformed or ignorant drone enthusiasts from flying UAVs in the vicinity of airports. Drone registration, remote pilot training and licensing requirements, are crucial elements that need to be specified, with clear financial & legal consequences, for violating aviation rules and intruding into restricted airspace.

4.3.8. Discussion on C-UAS applicability in Airports and Resilience Plan

Although there is a number of technological C-UAS solutions, as discussed in previous sections, no International Standards exist for the proper design and use of C-UAS systems in airports and its critical infrastructures. The applicability of UAV interdicting measures remains an open challenge to the complicated airport environment. According to FAA, airports seeking to deploy UAS detection systems, should be aware of deployment hazards of such systems, since they may implicate provisions of law, even when C-UAS are marketed as passive detection systems.

Terminal airspace should be adequately protected, however the risk of interference with legitimate communications is a serious concern. Especially in the airport approach area, it is vital to eliminate any interfere with other important radio signals for aviation, such as Instrument Landing Systems (ILS), surveillance approach radars, radio communications etc. Moreover, RF jamming for civil use is illegal in many countries worldwide (EU, Canada, USA, Australia) and as such, jamming cannot be used as a mitigation option in many airports. Likewise, jamming GPS/GLONASS signals near an airport are also considered dangerous for civil aviation, since many airplanes nowadays rely heavily on satellite navigation for take-off and landing procedures.

Airfield operators must remain within the law, when using C-UAS technologies, and the risks on the wider community should be fully assessed and understood. A clear decision-making process should be established to allow the airport operator to make the most appropriate decisions, based on solid and accurate information. As exhibited in previous sections, in most cases aggressive mitigation measures cannot be implemented in civilian airports, due to existing aviation laws and legal restrictions. Therefore, it is recommended for airport operators to establish coordination channels with security agencies, such as the police, military, and Civil Aviation Authority, in order to strengthen their defense capabilities and ensure a more joined-up response. In case a drone falls within the airfield boundaries, the operator should also consult

the police and legal authorities before approaching it, as it may contain vital forensic and digital evidence that could be used for investigation and legal prosecution.

Aiming to enhance Airport Resilience and robustness, when confronting UAV attacks, aviation stakeholders have to develop efficient contingency plans with clear safety and security measures to protect their critical assets. While planning their strategy for increased resilience and robustness, airport operators have to take into consideration the following:

i) Implement an effective UAS detection system and create an internal reporting point for drone sightings. It is imperative to understand which part of a facility's airspace has been infringed upon and locate the drone at all times, during the incursion.

ii) Identify the drone and understand the type of UAV being used, what threat may pose to the airport operator or airspace management and which mitigation options are available.

iii) If any mitigation options are adopted, they must be legal, proportionate and properly risk assessed, so as not to create any other hazard to the wider airport community.

iv) Appropriate liaison with security partners and legal agencies (police, civil protection authorities etc.) should be established, in order to coordinate response, when an incident takes place.

v) Whenever a drone interrupts airport's operation, and before resuming flights schedule, the operator should confirm that the airspace is clear, the drone is disabled and it is safe for operations to restart.

vi) Ensure that business continuity plan, developed for airport operations, has included such type of UAV disruptions, while regularly exercise preparedness scenario, involving all aviation stakeholders.

4.3.9. Summary of Research Work

Ranging from insect-sized to several tons in weight, drones are extremely versatile and can perform a large variety of tasks, transforming civil protection, security patrols, asset delivery, commercial and entertaining activities. Among the advantages of commercial drones are their relatively low cost, easy reach, great work productivity and capacity to reduce risk to human life. These features have led to their mass commercialization. Nevertheless, regulatory and oversight challenges remain immature, particularly regarding dual use of civil drones, that can be easily turned into armed drones or weaponized for criminal purposes.

Drone-related incidents at critical infrastructures, including airport facilities, are expected to rapidly proliferate in frequency, complexity and severity, as drones become larger and more powerful. The use of drones can appeal to nefarious actors, since they are relatively inexpensive and provide means to attack a target with low risks for perpetrators. Critical Infrastructures need to be protected from such aerial attacks, through effective vulnerability assessment, risk management and resilience actions.

Although airport environments are complicated with a variety of sizes and design features, they have similar security requirements for protecting their facilities, detecting and identifying misused drones, as well as taking effective counter measures. Based on extensive literature survey on C-UAS technologies, we have developed three categories of attack scenarios in airport premises and proposed an efficient C-UAS protection plan for each case. Geofencing as preventing measure and a variety of detection sensors can be implemented in different ways, depending on risk appetite, either as a distributed system on the airport perimeter, or as a single point detection capability. Multiple radars with different detection ranges provide the necessary primary surveillance method in airports. Since it is important to identify the type and payload of invading drone, we proposed a combination of radio frequency sensors with visual detection sensors (electro-optical and infrared cameras), which provide supplementary surveillance around airport's extended perimeter.

However, defending airports against unwanted drone activity is a wide and deep problem set. Despite the variety of technological mitigation solutions available, airfield operators must remain within the law, when using disruptive technologies, and the risks on the wider community should be fully assessed and understood. A clear decision-making process should be in place, to allow the airport operator to make the most appropriate decision, based on solid and accurate information.

Clearly, safety is the priority within the aviation context. Any decisions against a flying object should be appropriate, proportionate and necessary, with documentation and the rationale for making it.

Furthermore, appropriate responses taken by operators before, during and immediately after any UAV incident should be developed in a contingency action plan to minimize the impact on key stakeholders. Airports should rely on support and co-ordination from official security services, the military and industry partners to increase resilience and robustness.

C-UAS technology poses a wide range of practical, legal, and policy challenges in airport's environment. A lack of common standards in the C-UAS industry means that there is a wide variance in the effectiveness and reliability of available systems. Efforts to identify new methods that will protect airspace and coordinate manned with unmanned aviation are ongoing, with Unmanned Aerial System Traffic Management (UTM) systems and Remote Identification requirements for civilian drones being under design. After all, further development of civilian and commercial UAVs and their integration into evolving smart cities, is dependent on the ability of drones to operate in various areas of the airspace, especially at very low level, without posing any risk to safety, security and privacy within society and its critical infrastructures.

4.4. Assessing Interdependencies and Congestion Delays in the Aviation Network

4.4.1 Introduction [9]

Concerning air traffic delays, air transport networks appear to have variable performance and stochastic nature. A delay incident in one airport may affect the operational efficiency of others and generate various side effects to the whole aviation network. Flight delays are a widespread phenomenon nowadays, costing billions to the air transportation economy and degrading passenger's quality of service. Dependency graphs have been proposed in the past to understand the delay propagation phenomenon and analyze such cascading events by using dependency chains. In this work, we propose a risk-based method to analyze interdependencies and congestions in the aviation network. The methodology and the developed tool can assess delay incidents in airports and produce weighted risk dependency graphs, presenting how a delay that occurred in one airport may affect other interconnected airports. Based on data collected from the US Bureau of Transportation Statistics, we analyze how flight delay risk propagates inside the aviation network. In addition, using historic flight performance data we provide predictions for flight chains, which are prone to delays. We implement a tool that can detect the most critical airports and congested connections based on their delay contribution in dependency chains. It also proposes the n-order dependency chains, which should be avoided by airline flight planners, to reduce delay impacts in the aviation network.

The US Department of Homeland security identifies aviation as a critical subsector of the transportation system (CISA, 2019). Aviation provides a swift worldwide transportation network, which generates economic growth and facilitates international connectivity, trade, and tourism (ICAO, 2019). With increasing globalization, the aviation industry has been growing at a fast pace, while on the other hand, flight delay problems have become a serious challenge degrading traveler's quality of service.

The United States is the world's largest aviation market, while future air transport growth requires improved traffic flow to reduce congestion (IATA, 2018). High airport delays can cause negative impacts on several aspects, such as passengers, airlines, and the air transport economy. Delays impact the aviation industry's efforts to maintain

[9] *Related Publication:* G. Lykou, P. Dedousis, G. Stergiopoulos and D. Gritzalis, "Assessing Interdependencies and Congestion Delays in the Aviation Network," in IEEE Access, vol. 8, pp. 223234-223254, 2020, doi: 10.1109/ACCESS.2020.3045340.

high levels of customer satisfaction, increased productivity while maintaining disruption's resilience. Unnecessary flight delays are often the result of outdated technology and procedures, which cost the US more than 25B$/year (ICAO, 2019).

A flight delay is usually reported as the late arrival or late departure of an inbound or outbound flight. It can be attributed to several reasons, such as air carrier or airport handling organizational issues, aircraft technical problems, extreme weather, air traffic control, security, etc. (Bureau of Transportation Statistics, 2020). As a result, a propagated delay may occur due to interconnected resources, while the most important resource is aircraft which flies multiple flight legs, very often more than five flight segments per day (Kafle & Zou, 2016a). Hence, a delay of an earlier flight can affect subsequent flights. Waiting for transit passengers from delayed connecting flights is also known to cause delays to upcoming flights (Zou & Hansen, 2014). Flight crew switches between aircraft may also cause further delays to the network (Wang et al., 2017). For these reasons, a small initial delay may cause cascading effects, creating larger delays and inducing worse situations in the downstream flight connections. Thus, research on the mechanism of delay propagation is a challenging area.

Researchers have studied dependency modeling, simulation, and analysis of infrastructures extensively. Several methodologies and tools that focus on dependency analysis estimate the impact (Franchina et al., 2011; Robert, 2004) or the risk derived from the dependencies within a critical infrastructure or among interdependent infra-structures (Kjølle et al., 2012; Kotzanikolaou et al., 2013a, 2013b; Stergiopoulos et al., 2017a, 2018a). Risk usually depends on two factors: i) the likelihood (or probability) of a negative event occurring and ii) the impact (consequences) of that negative event, usually called a disruption. Such impact may result in incomplete operations (flight cancelations) or service degradation (flight delays) due to dependencies in infrastructure networks.

In this work, we use a previous time-based dependency analysis methodology for critical infrastructure dependency modeling (Kotzanikolaou et al., 2013a, 2013b), to analyze delay risk propagation in the US aviation network. We apply the proposed methodology, and the developed tool in a dataset of commercial flight routes and delays reported per flight for years 2018-19, as provided by US Bureau of Transportation Statistics (BTS) (Bureau of Transportation Statistics (BTS), United States Department of Transportation, n.d.). Our contributions are:

1) A methodology able to analyze congestion in aviation networks, as follows: i) model aviation networks as dependency graphs; ii) assess the dependency risk of delay incidents between interconnected airports; iii) produces weighted risk dependency chains, to present how a delay occurred in one airport may affect other inter-connected airports; and iv) calculates impact and likelihood of delays in congested airports using various methods such as min-max algorithm, standard

deviation timeframes, and statistical dynamic averages.

2) A comparison analysis of airplane arrival on-time performance data of US domestic flights as provided by BTS (Bureau of Transportation Statistics (BTS), United States Department of Transportation, n.d.) for two consecutive years. Specifically, we provide a risk congestion analysis during summer months (July-August) for years (2018-19) detecting the worst n^{th} order dependencies and worst airports in terms of congestion delay propagation. Moreover, we detect the most congested paths, schedules, and airports to be evaded by flight planners, airline marketing managers, and other air transportation stakeholders.
3) A software implementation of the proposed methodology, which can:
   a. Indicate the flight connections with the highest delay risk for the period defined.
   b. Identify the worst n-order airport dependencies by calculating the overall risk of cascading congestions.
   c. Indicate airports that are frequently part of the worst n-order airport dependencies and introduce delays to the downstream flights
   d. Analyze what-if scenarios for the congested airport's connections.
   e. Propose the n-order dependency chains, which should be avoided by flight planners, to reduce delay impacts in the aviation network.

To the best of our knowledge, a risk-based methodology and software implementation for analyzing flight interdependencies of congested aviation networks and indicating worst dependency connection chains has never been introduced before.

The remainder of this research is structured as follows: in subsection 4.4.2, related work in modeling infrastructure interdependencies and flight delay propagation is presented. In subsection 4.4.3, the dependency analysis methodology is presented, while in subsection 4.4.4, the dataset details, which were used for airport congestion analysis, are explained. The results from the implementation of the proposed methodology and software tool are analyzed in subsection 4.4.5. Finally, the conclusion and evaluation of results are exhibited in subsection 4.4.6.

4.4.2 Related work

During the past decade, modeling of critical infrastructures along with the flow of information and risks between them has been a major topic of interest in scientific research. This subsection summarizes models and methodologies already proposed and focuses on similar work on aviation networks and critical air transportation infrastructures.

Several approaches exist in modeling infrastructure dependencies and information flow. Generally, infrastructure modeling appears to be associated with simulation techniques and mathematical models, such as (i) continuous time-step simulation; (ii) discrete time-step simulation; (iii) Monte Carlo simulation; (iv) decision trees; (v) geographical information systems; and (vi) risk management tools (Stergiopoulos, Vasilellis, et al., 2016a). According to Ouyang (Ouyang, 2014a), critical infrastructure protection methodologies and tools are categorized as: (i) Empirical; (ii) System Dynamics; (iii) Agent-based; and (iv) network-based. Empirical models are based on historical events. System Dynamics utilize top-down methods such as stock and flows to manage and analyze complex adaptive systems with interdependencies. Agent-based approaches model components of infrastructures as agents and analyze agent interaction based on sets of rules, while network-based approaches model infrastructures as network graphs whose nodes represent infrastructure components.

Our approach is purely network-based, driven by historical data and applying a risk management model for simulating airport dependencies. A graphical dependency model of the worst performing airports in the US aviation network is developed. Airports are modeled as nodes, while flight routes between airports are portrayed as graph links, using the methodology previously presented for urban and maritime transportation networks to predict high-risk nodes and propose traffic congestion mitigation mechanisms (Stergiopoulos et al., 2017a, 2018a).

Academic literature on flight delays can be classified into three main categories: i) statistical models, which explore the effects of various components of travel time, ii) econometric models that analyze the economic drivers of flight delays, and iii) operations management models, which investigate the operational impacts of delays in air transportation.

Since the nature of air transportation is highly stochastic, different aspects of flight scheduling issues have been explored in the past. Several researchers have developed statistical models for forecasting different components of air-travel time.

Deshpande and Arıkan (Deshpande & Arıkan, 2012a) analyzed empirical flight data to model total travel time distribution without dividing it into individual segments and developed a model of total travel time for all flights flown in the United States at all airports, using the BTS dataset. Wang et al. (Wang et al., 2017) used empirical statistics of departure delays to form complementary cumulative distribution functions (CCDF), along with transmission delay functions and proposed a novel approach to interpret big temporal data. Takeichi (Takeichi, 2017a) proposed a mathematical model delay analysis to estimate the delay accumulation by using arrival delay statistics and nominal flight time optimization formulas for aircraft arrivals at an airport.

In econometric models, the impacts of various factors on the initiation and progression of propagated delay are quantified. Kafle & Zou (Kafle & Zou, 2016a) developed a joint discrete-continuous econometric model to reveal the effects of various influencing factors, considering the buffer time that airlines insert into flight schedules. As a result, they were able to quantify propagated, and newly formed delays that occur to each sequence of flights that an aircraft flies in a day.

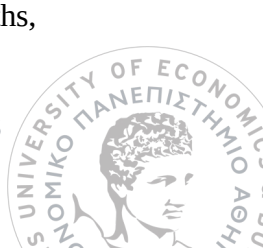
Quantitative approaches such as statistical (Wang et al., 2017), (Deshpande & Arıkan, 2012a), (Takeichi, 2017a), and econometric (Kafle & Zou, 2016a) methods focus mainly on flight delays in a single airport. Furthermore, although the series of flights are taken into account by some (Kafle & Zou, 2016a), (Takeichi, 2017a), others (Wang et al., 2017), (Deshpande & Arıkan, 2012a) neglect the sequence of the predecessor flights from the upstream airports. In either way, the process of delay propagation needs to be analyzed from a broader and network-based perspective since flight scheduling for airlines and airport operations are oriented towards network performance optimization.

Pyrgiotis et al. (2013a) investigated how the delay is propagated and how delays mitigate daily airport operational efficiency and push more demands into late evening hours. The approximate network delays (AND) model which computes the delays to the 34 busiest US airports was thus introduced. Zhang and Nayak (Nayak & Zhang, 2011a) used the multivariate simultaneous equation regression (MSER) model to study the impact of one airport on others and concluded that major airports have a higher impact on the average delay. Hao et al. (Hao et al., 2014) used the MSER model to quantify the impact of New York's airports on delays throughout the airport network. They concluded that the delays in NY airports, being analyzed by two different models, were lower than expected. Fleurquin et al. (Fleurquin et al., 2013) developed the maximum connected subgraph of congested airports for assessing the level of delays across the entire system. Campanelli et al. (Campanelli et al., 2016a) compared the modeling of the US and the European air traffic networks to assess the effect of delay disruptions and proposed how slot reallocation and swapping can mitigate flight delay propagation in the US aviation network. A comparative analysis of models for predicting delays in air transportation has been presented by (Gopalakrishnan & Balakrishnan, 2017), comparing the performance of different approaches to predict delays in air traffic networks. The authors consider three classes of models: i) dynamics network models using Markov jump linear system (MJLS); ii) classical machine learning techniques like classification and regression trees (CART); iii) Artificial neural network (ANN) architectures, utilizing classification factors such as time of day, day of the week, season, and previously realized delays.

Despite the advances in understanding flight delay propagation, few studies have investigated delay propagation by considering the interdependence relationship of delay. These approaches focused on the propagation processes between sequence flights and congestion in airports while ignoring actual relationships among airports, the network structure, and airport properties. Moreover, the factors used to analyze delay propagation are often limited in the sense that the delay time is calculated directly from the difference between the actual and scheduled travel time (Rupp, 2007) or by analyzing arrival and departure delays times separately (Campanelli et al., 2016a; Deshpande & Arıkan, 2012a; Fleurquin et al., 2013; Hao et al., 2014; Kafle & Zou, 2016a; Pyrgiotis et al., 2013b) while others consider either departure delays (Wang et al., 2020) or arrival delays (Nayak & Zhang, 2011b; Takeichi, 2017b), thus not representing the actual congestion delay of a flight caused by both origin and destination airports. Finally, approaches like those presented in (Campanelli et al., 2016b; Deshpande & Arıkan, 2012b; Kafle & Zou, 2016b; Pyrgiotis et al., 2013a) use multivariate simulation methods to analyze the social and economic impacts of delays in operational performance of airports examined. These methods are more complicated and need a variety of data to be provided by airlines, inside business information and airport authorities, to produce results.

Since the air transportation system is also a typical large-scale complex system, the mechanisms of delay propagation are not fully understood, especially for the interdependencies of different airports, thus creating a growing interest in the inference of causal interactions in complex systems (Wahl et al., 2017). Du et al. (2018a) proposed a delay causality network (DCN), based on the Granger causality test to analyze the topological and temporal properties of the DCN and better understand the mechanism of flight delay propagation at the system level. The proposed approach in (Du et al., 2018b), considers delay propagation problem from the perspective of delay interdependences utilizing network analysis. While this method can capture the interaction patterns of delay, it is limited in identifying them between airport pairs. Also, the majority of studies regarding air traffic networks focus on using network graph theory to classify the topology of the network (Bagler, 2008; Han et al., 2007; W. Li et al., 2006), while other network based theories use measures to consider the importance of individual airports (Guimera et al., 2005) or focus on the optimization and efficiency of the network (Gillen et al., 2015; Z.-C. Li et al., 2010; Silva et al., 2014).

Our approach is different from the majority of studies regarding air traffic congestion delays since it introduces a risk-based approach to assess the inter-dependencies of delay propagation in the aviation network. The presented implementation similar to (Stergiopoulos et al., 2017a, 2018a), is considered to be a cyber-physical, deterministic, long-term optimization model that uses risk assessment, statistical analysis, and graph theory to promote decision making by proposing the n-order dependency chains, paths,



and airports which should be avoided by flight planners, to reduce delay impacts in the aviation network.

Our model relies on congestion delays created by both origin and destination airports. Also, it uses all airports and all flights approach, similar to (Campanelli et al., 2016a; Deshpande & Arıkan, 2012a; Fleurquin et al., 2013) while others focus on a single airport (Hao et al., 2014; Takeichi, 2017a), specific airlines (Kafle & Zou, 2016a), (Wang et al., 2017), or only the busiest US airport hubs (Pyrgiotis et al., 2013b), (Nayak & Zhang, 2011a). We use data exclusively from the BTS database to analyze historic data from a selected period of aviation traffic on US airports, while other methods (Campanelli et al., 2016b; Deshpande & Arıkan, 2012b; Kafle & Zou, 2016b; Pyrgiotis et al., 2013a) require data from airlines, inside business information, and airport authorities, to produce results. Utilizing statistical analysis, our model converts time delays to risk impact and frequency of delay occurrence into likelihood, calculating the risk of congestion for each flight route.

Finally, our approach utilizes network graph theory similar to (Bagler, 2008; Gillen et al., 2015; Guimera et al., 2005; Han et al., 2007; W. Li et al., 2006; Z.-C. Li et al., 2010; Silva et al., 2014). While the aforementioned studies utilize graph theory either to classify the topology of the network, measure the importance of the individual airport, or for optimization, we utilize known graph theory algorithms for computing all possible paths of an aviation network, thus calculating all possible n-order airport dependencies, in order to assess the cumulative congestion risk of the aviation network dependency paths.

From the related work presented, prediction methodologies are developed in (Campanelli et al., 2016a; Du et al., 2018b; Fleurquin et al., 2013; Hao et al., 2014; Pyrgiotis et al., 2013b) while none of them produces a projection of worst dependency chains of flight connections like our model does. Understanding flight delay propagation is a hard problem while few studies have investigated delay propagation by considering the interdependence relationship of delay time-series, and none has ever explored the delay propagation and congestion analysis through airport chains (n-order airport dependencies) in large-complex aviation networks. Therefore, our efforts to produce dependency graphs, to assess congestion risk and delay propagation to interconnected airports, introduce a new approach to this stochastic problem. To the best of our knowledge, there is currently no solution able to calculate the individual risk (in terms of delay impact and the likelihood of a flight delay to occur) of interdependencies between airports in wide aviation networks, along with the cumulative risk of n-order airport dependency chains.

4.4.3 Dependency Analysis Methodology

Our methodology expands a previously presented multi-risk dependency analysis, developed in (Stergiopoulos et al., 2017b), to model the traffic flow of automobiles in the UK transportation system. The same team has also analyzed congestion interdependencies of ports and container ship routes in the maritime network infrastructure in (Stergiopoulos et al., 2018b).

Our implementation is based on the CIDA tool (Stergiopoulos, Kotzanikolaou, et al., 2016), which we modified and expanded in functionality to model and analyze aviation congestion interdependencies between airports.

The methodology uses five fundamental building blocks:

A. An algorithm that models historic air traffic data into a dependency airport graph.

B. A congestion delay calculation methodology for aircraft flights.

C. A likelihood calculation algorithm for graph connections.

D. An impact calculation algorithm that uses two different methods for calculating the delay impact.

E. A multi-risk dependency analysis methodology for assessing the risk of the graph's dependency paths.

Each building block is briefly presented below.

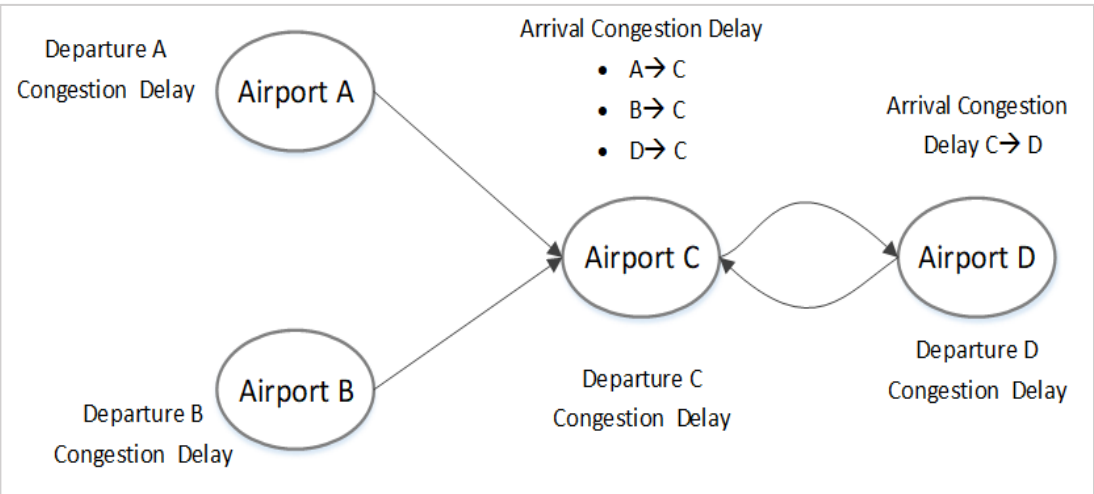


Figure 4.34. Airport's Departure and Arrival Congestion Delay

AIRPORT DEPENDENCY GRAPHS

In this methodology, we denote as:

A: the set of airports in the aviation network,

C: the set of connections between airports, and

F: the set of flights among airport nodes for each connection (i.e., aircraft flights that connect these airports).

Dependencies are modeled in directed, weighted graphs $G = (V, E)$, where the nodes V represent airports of the network system and edges E represent connections between them (Fig. 4.34). The graph is directional to represent a flight dependency from one destination to another within the aviation network. An edge $A_x \rightarrow A_y$ depicts a connection $C_{x \rightarrow y}$ from Airport A_x to Airport A_y, and each connection is related to many connecting flights F_i, performed by various commercial carriers, using different aircraft types.

Daily, from every airport A_x scheduled flights depart from A_x or arrive to A_x, based on the submitted Flight Plans (FP) and commercial carriers' Computerized Reservations Systems (CRS). Each aircraft has a unique Tail Number (TN) that indicates the aircraft's type/model, load capacity, and speed performance. It usually serves several flights to many airports in a single day. By modeling all possible connections, we create chains of multiple flight legs, forming n-order dependencies $A_0 \rightarrow A_1 \rightarrow A_2 \rightarrow \cdots \rightarrow A_n$ of connected airports.

CONGESTION DELAY CALCULATION

Based on FP and CRS, every flight has a predefined departure time and an arrival scheduled time. Arrival performance is based on the aircraft's arrival time at the airport's gate (in-block time). Departure performance is based on the aircraft's departure time from the gate (off-block time). We define as congestion delay, the arrival delay that exceeds 15 minutes from scheduled in-block time, caused by any delay cause (air carrier, extreme weather, NAS, late-arriving aircraft, etc.).

For each tail number TN, performing a connection flight F_i, congestion delay is split between arrival and departure part. For every flight, F_i we calculate arrival congestion delay CA and departure congestion delay CD as follows:

Procedure CalculateCongestionTimes ( )
Inputs:
Arrival Delay (mins): $\boldsymbol{A}$
Departure Delay (mins): $\boldsymbol{D}$
Output:
Arrival Congestion Delay (mins): $\boldsymbol{CA}$
Departure Congestion Delay (mins): $\boldsymbol{CD}$
If $A \leq 15$ mins **then**
$CA = 0$ (Flight considered On Time)
Else
If $D \leq 0$ then
$CA = A$
Else
$CA = A - D$
$CD = D$
End If
End if

CONNECTION DELAY LIKELIHOOD CALCULATION

Each relationship is assigned with a likelihood value, which declares, how likely the route is to be delayed or congested. Intuitively, this value is a probability, based on which we can make predictions about each airport's congestion state, at different times. For each route $C_{x \to y}$ from an airport A_x to an airport A_y every flight $F_{x \to y}$ is rated either as "Good" or as "Bad" as follows:

Procedure EvaluateConnectionFlight ( )
Inputs:
Arrival Congestion Delay (mins): $\boldsymbol{CA}$
Departure Congestion Delay (mins): $\boldsymbol{CD}$
Output:
Connection Flight Evaluation: $\boldsymbol{F_{x \to y}}$
If $CA > 0\ mins$ **Or** $CD > 0$ **then**
$F_{x \to y} =$ "Bad"
Else
$F_{x \to y} =$ "Good"
End if

Based on the above, the delay likelihood of connection $C_{x\to y}$ from airport Ax to airport Ay is calculated, taking into account all connection flight routes, as following:

$$L_{x\to y} = \frac{Number\ of\ times\ F_{x\to y}\ marked\ as\ "Bad"}{Total\ number\ of\ times\ F_{x\to y}\ appears} \qquad (1)$$

$$L_{x\to y}\ \epsilon\ [0,1]$$

$L_{x\to y}$ refers to connection likelihood, and it is calculated based on all individual flights Fi, departing from airport Ax and arriving at airport Ay.

IMPACT CALCULATION

Each flight F(x→y) is assigned with an impact value. This metric asserts how severe the congestion delay is and how much it will affect a flight connection's punctuality and airport's operational efficiency. Since there is no standard available for evaluating arrival delay time and social-economic impact level to passengers in the US, we proposed two different methods for impact calculation. The first (Min-Max Method) is proportional, by defining for each connection the min and max delay performance and then rescaling this range to a 10-steps scale with equal size of time frames. The method e-valuates the relational delay performance of each connection. As a result, the upper and the lower range limits are evaluated based on actual performance data of all flights in this connection during the period examined. For example, if all aircrafts have arrived on-time while flying this connection route or have never been delayed more than one hour, the impact is scaled to take its max value for this one-hour delay time. On the other hand, for a connection where flights are always on delay (sometimes more than 15 hours delay), we evaluate impact based on min and max delay's deviation that takes place for the specific connection. As a result, in this method impact values are not assigned with fixed delay intervals and maximum impact may represent different delay performances.

The second method (Standard deviation timeframes method) is based on specific deviation time intervals, identifying with the lowest value for impact (I=1) when flight arrival is on-time, while impact gets its higher rating when arrival delay exceeds 900 min (or being late for more than 15 hours). In this impact rating, delay timeframes are in accordance with traveler's tolerance against delays, because as the duration of flight delay increases, passenger dissatisfaction intensifies. However, this evaluation method exerts the same objective criteria for all flights performed in the US domestic aviation, based on the deviation in minutes from the scheduled arrival time. Since air travelers use aviation as the fastest transportation mean, they expect to reach their destination on scheduled time. So, while they may tolerate delays less than 1-2 hours, higher delays may impact the airline's reputation, while economic liabilities may be claimed by

dissatisfied passengers. The following paragraphs describe in more detail the impact calculation of the proposed methods.

D.1. Min-Max Method

For each connection C(x→y) from an airport Ax to an airport Ay a congestion delay may occur, during either departure or arrival phase, and its impact is calculated based on the best and worst-case congestion delay of each connection, as following:

$$MinDelay_{x\to y} = \text{MinDepartureCongestionDelay} + \text{MinArrivalCongestionDelay} \quad (2)$$

$$MaxDelay_{x\to y} = \text{MaxDepartureCongestionDel}ay + \text{MaxArrivalCongestionDelay} \quad (3)$$

Min and Max Departure Congestion Delay are calculated taking into account all flights departing from airport A_x to airport A_y. The same definition applies for Min and Max Arrival Congestion Delay, considering all flights arriving to airport A_y from airport A_x.

Based on $MinDelay_{x\to y}$ and $MaxDelay_{x\to y}$ values, an impact scaling is calculated in equal timeframes, ranging from 1 to 10, where the maximum impact denotes the maximum occurred congestion delay. For each connection flight $F_{x\to y}$, we assign an impact value based on its $CongestionDelay_{x\to y}$ impact range.

Table 4.17. Relation between standard deviation timeframes and Impact

Arrival Delay (mins)	Impact
0-15	1
16-30	2
31-60	3
61-120	4
121-180	5
181-270	6
271-400	7
400-600	8
601-900	9
>900	10

D.2. Standard deviation timeframes method

We calculate the delay impact on standard deviation timeframes between actual arrival time and estimated CRS arrival time (Tab. 4.19). If the arrival delay is less than 15 min, the flight is considered on time and the impact gets its minimum value (I=1).
On the downside, if a flight arrives later than 900 min (i.e., delay >15 hours) after its scheduled arrival time, the impact takes its maximum value (I=10) indicating an unacceptable delay situation for air transportation service. The interval steps are presented in Tab. 4.19. Due to the lack of standards for setting the arrival delay time intervals, we divided the arrival delays up to 180 minutes to the first half of the impact scale. After 3 hours delay, compensation liabilities may arise, depending on current aviation law. The time intervals thereafter are increased by a multiplier of 1.5 until the maximum impact value is reached.
No method takes into account cancellations, although a flight leg may be canceled, due to previous congestion delays. Having calculated impact for each individual flight, we evaluate the total impact value of a connection $C_{x\to y}$ from airport A_x to airport A_y as the average impact of the flights F_i, performed by various commercial carriers in that connection, using different aircraft types as defined by their TN.

CONGESTION - DEPENDENCY ANALYSIS

The proliferation of impact and likelihood values indicate the Delay Risk $R_{x\to y}$ for a connection $C_{x\to y}$ from an airport A_x to an airport A_y as follows:

$$\mathrm{R}_{x\to y} = \mathrm{Impact}_{x\to y} \cdot \mathrm{Likelihood}_{x\to y} \quad (4)$$

Potential congestion delay is transferred from the previous connection to the next flight leg, where late arrival of one flight may be propagated to late departure of the next scheduled one for the same aircraft. To calculate the dependency risk of delay propagated in a series of airports, we use the following method:
Let $A_0 \to A_1 \to A_2 \to \cdots \to A_n$ be a chain of n^{th} airport dependencies, based on specific aircraft routes, where $L_{A_0,\cdots,A_n}$ is the likelihood of the n$^{\text{th}}$-order cascading congestion and I_{A_{n-1},A_n} is the impact of the $A_{n-1} \to A_n$ dependency, then the cascading risk of the chain $R_{A_0,\cdots,A_n}$ due to the n$^{\text{th}}$-order dependency is computed based on (5).

$$R_{A_0,\cdots,A_n} = L_{A_0,\cdots,A_n} \cdot I_{A_{n-1},A_n} = \left(\prod_{i=1}^{n} L_{A_{i-1},A_i}\right) \cdot I_{A_{n-1},A_n} \quad (5)$$

The cumulative dependency risk considers the overall risk exhibited by all the critical infrastructures in the sub-chains of the n^{th}-order dependency, denoted as $DR_{A_0,\cdots,A_n}$. It is defined as follows, representing the overall risk produced by n^{th}-order dependency.

$$DR_{A_0,\cdots,A_n} = \sum_{i=1}^{n} R_{A_0,\cdots,A_i} = \sum_{i=1}^{n} \left(\prod_{j=1}^{i} L_{A_{j-1},A_j} \right) \cdot I_{A_{i-1},A_i} \quad (6)$$

Equation (6) computes the overall dependency risk, as the sum of the dependency risks of the affected nodes in the chain, due to delay incidents realized in the origin airport A_0 of the dependency chain. Interested readers may refer to (Kotzanikolaou et al., 2013b) and (Kotzanikolaou et al., 2013a) for additional details about dependency risk estimation.

4.4.4 Data Set Details & Validation

Since 2010, the US Department of Transport (DOT) has been publishing a list of air traffic data sets on their website (Bureau of Transportation Statistics (BTS), United States Department of Transportation, 2020). We have collected US Flight data for two consecutive years (2018-19), focusing our analysis on July and August. These months have the highest traffic, due to the summer holidays season, while the arrival on-time performance degrades compared to other months all year round. Moreover, these summer months are more likely to suffer from late-arriving aircraft and air carrier delays, besides weather delays introduced, either as extreme weather events or indirectly reported in National Aviation System (NAS) delays. Therefore, July and August seem to better reflect aviation stake-holders' efficiency to manage heavy traffic in airports. We refrained from using 2020 data in our analysis, since in summer 2020 aviation traffic dramatically shrunk, due to Coronavirus global health crisis (Covid-19 Pandemic). As a result, on-time performance has significantly improved.
From the data set retrieved from the BTS database we exploited in our experiments the following information:

- FL_DATE: Date of flight
- TAIL_NUM: Airplane tail number (unique per plane)
- OP_CARRIER_FL_NUM: Flight number
- ORIGIN_AIRPORT_ID: Unique airport origin/source ID (IATA CODE)
- ORIGIN: Airport origin/source code
- DEST_AIRPORT_ID: Unique airport destination ID
- DEST: Unique airport destination code
- DEP_DELAY_NEW: Difference in minutes between scheduled and actual departure time (0, if arrived early)
- ARR_DELAY_NEW: Difference in minutes between scheduled and actual arrival time (0, if arrived early)
- CRS_SCHED_TIME: Scheduled flight time as shown in Computerized Reservations Systems (CRS) (min)
- ACTUAL_ELAPSED_TIME: Actual flight elapsed time in minutes.

Table 4.18. Valid Data Set Rows used in Delay Risk Analysis

Year	Month	Data Rows	Canceled Flights	Invalid Data	Valid Data
2018	July	645,299	11,083	198	634,018
	August	644,673	12,353	185	632,135
2019	July	659,029	12,928	159	645,942
	August	658,461	11,298	165	646,998

To ensure the quality of the dataset, we removed rows where data entries appeared with inconsistencies, like flights without information about arrival time, arrival delay and actual elapsed time, etc. These flights were considered as canceled flights due to missing data from arrival reporting fields.
In addition, canceled flights reported in the dataset were excluded from our experiments, since they could not cause any congestion to airports, although these cancelations may have occurred due to enormous flight delays from previous flight con-nections, which sometimes exceeded the amount of 1440 minutes (i.e., 24 hours delay). The validated data used for each month in our experiments are presented in Tab. 4.20

4.4.5 Results

The tool was developed in the Java language using the Neo4J graph database (Webber, 2012). The tool accepted as input the collected US Flight data for two consecutive years 2018-2019 for July and August. It modeled all US airports as nodes and flight connections as edges. For each connection of the modeled graph, all flights performed by various aircraft were processed and assigned with an impact and a likelihood value based on the presented methodology.
The tool generated all dependency chains for the worst performing aircraft and each airport and flight route. Output was then imported into a Neo4J graph database for risk dependency chain analysis.
We ran the experiments for the two alternative methods proposed for calculating impact and connection's delay risk to evaluate which method best fitted to congestion delay analysis. The results are analyzed below and involve the busiest US airports, where we use the 3-digit IATA code to de-note them.
For readers not familiar with IATA codes, all US airports discussed in this subsection are listed in Appendix C. The table in Appendix C provides details about official airport's name, the main city served, along with annual passenger traffic, which indicates an airport's importance in the aviation network.

IMPACT CALCULATION METHODS COMPARISON

The first step of our analysis was to present the differences between the two methods proposed for impact calculation. In Fig. 4.35, we present the variations of average risk calculation between the Static Impact method and the Min-Max Impact calculation for all connections arriving at New York airport (JFK). This airport is one out of three airports serving NY city, and it is connected with another 64 US airports for serving domestic flights. The average risk of each airport connected to JFK is the fraction of total risk accumulated from all flights in the same connection, divided by the number of flights. Thus, it denotes the risk tendency for delays in each JFK connection with other airports.

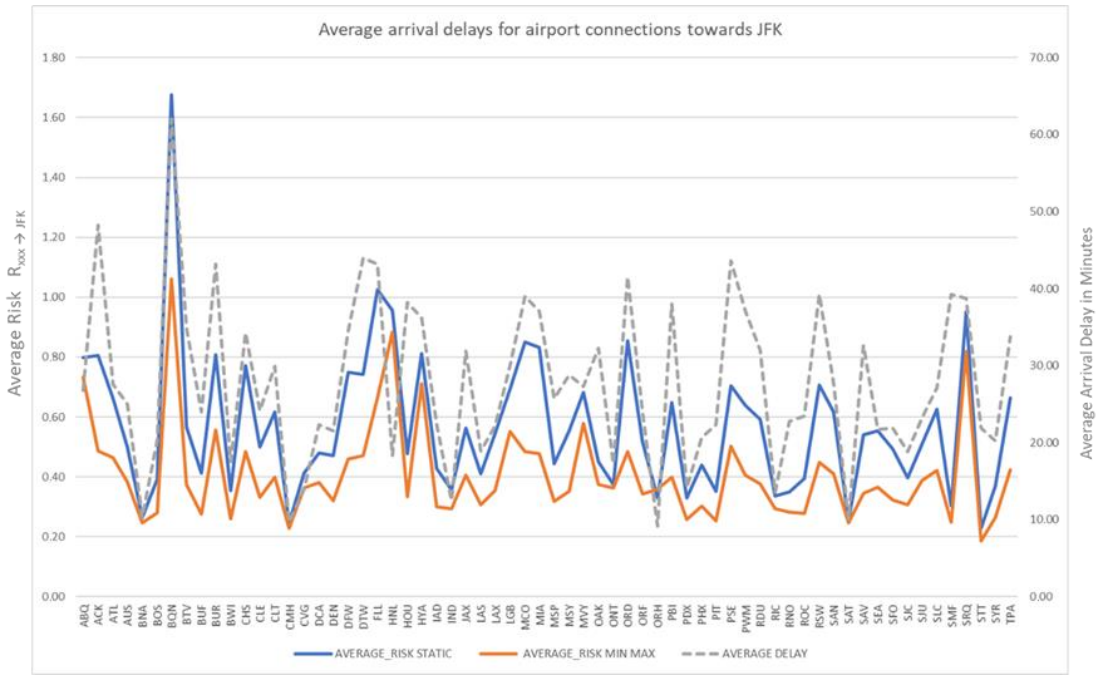


Fig. 4.35. Average Risk calculation for static and Min-Max method in JFK airport

The graph in Fig. 4.35 depicts:

1) Delay Risk calculated based on the static method represented by the blue line.

2) Delay Risk calculated based on the Min-Max method, represented by the orange line.

3) The average arrival delay in minutes for each route directing to JFK, shown in the grey dashed line. Grey line values are reported to the right-hand secondary axis.

The average risk of each connection for the Static method (blue line) is more representative and proportional to the average arrival delay of each flight landing at JFK. The Min-Max method (orange line) is more subjective than the Static method since the impact scaling is self-adjusted for each connection to its minimum and maximum delay performance. Although it can capture airport perfor-mance variations and provide a differential analysis of deteriorations and improvements of airport's connection examined, it can be relatively unfair, since impact values assigned do not indicate the same delay deviation from scheduled arrival time. For example, I=10 may indicate a delay of 30 min, for a connection with no delays, while the same impact value may be attributed to a connection, with major delays more than 1000 minutes.
On the other hand, the Static method is more objective, evaluating all connections impact with the same criteria regarding the deviation in minutes of actual performance versus scheduled arrival time. As we have concluded from all experiments we performed, both methods were able to distinguish very congested airports, simulate the hierarchy of worst airports, and produce similar aggregated risk values for heavy traffic connections.
However, for the rest of our analysis and graph production, we decided to use the static method as a more objective for calculating airport delay performances.

AIRPORT CONGESTION RISK ANALYSIS

The results of the average risk analysis for the 30 busiest US airports are graphically presented in Fig. 4.36. We depict the average connection's risk for heavy traffic airport connections during peak traffic months (July-August) of the year 2019. Graph depiction is in GIS format, where the reported avia-tion hubs served overall 788 domestic flight connections. In this graph, with red lines are represented the connections which have a higher average risk for a delay (>0.6) while with orange and green color the connections with risk lower average risk below 0.6 and 0.4 values respectively.
For the examined period, these airports have handled 439,846 domestic flights, while they account for 34% of national flights reported. In other words, 8% of US airports served one-third of commercial domestic flights. The most interconnected airports, presented in Fig. 4.36, are Atlanta (ATL with 160 connections), Dallas (DFW:179), Chicago (ORD:174) and Denver (DEN:165), while the least inter-connected busiest airport is Portland Airport (PDX), with 47 domestic connections with other airports in the USA.
In Figure 4.36, the airports with the highest average risk include the following destinations: BOS, EWR, FLL, JFK, LGA, and MCO. It is evident that congestion delays seem to cluster on eastern coast airports. Specifically, delay risk is detected to be higher for air-traffic departing from south-east destinations (MIA, FLL, MCO)

towards north-east airports like the ones in New York, Philadelphia, and Washington, and vice versa.

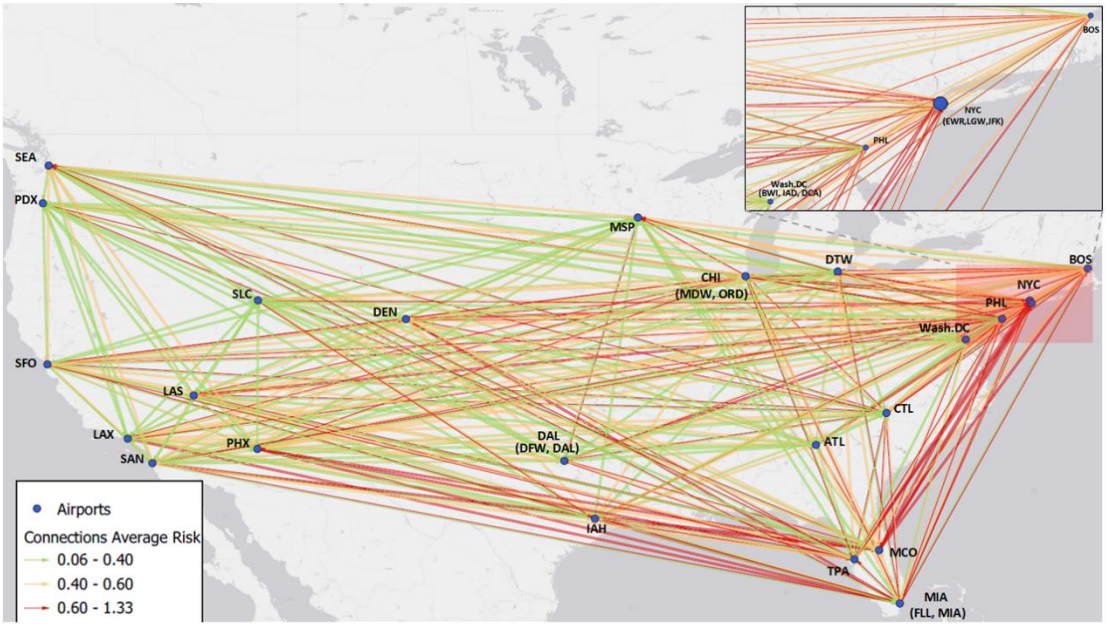


FIGURE 4.36. Risk Connection Analysis for 30 US busiest airports for 2019

The higher average risk value is 1.33 for the CLT→ PDX connection (worst connection with 67% delay probability), while the lowest risk value is 0.06 for SLC→TPA connection (best connection with only 5% delay probability). The average likelihood value is 0.37 for both summer months, which means that 37% of flight connections are likely to arrive with delay (>15 min later than scheduled arrival) during July and August.

Furthermore, we also examined the 30 busiest US airports for i) incoming congestion risk, which occurs based on arrival delays, and ii) outgoing congestion risk based on departure delays occurred for July and August in 2018. Afterward, we compared 2018 data with the same period in 2019, and results are graphically presented in Fig. 4.37 and 4.36 respectively. The data are also provided in a table format in Appendix D (Tab. D1).

Fig. 4.37 depicts average congestion risk for the 30 busiest airports in 2018. For each airport, we present its inbound delay risk (expressed by average arrival delay risk of all flight connections arriving at this airport) and outbound delay risk (expressed by average departure delay risk off all flights departing from the airport) plotted in blue and orange bars respectively. On the right-side secondary axis, the number of connections with other domestic airports are shown in the red line and depict the airport's degree centrality. In graph theory, degree centrality is equivalent to the edge count of a node; airports with high degree centrality generally are more central and of greater importance in the aviation network.

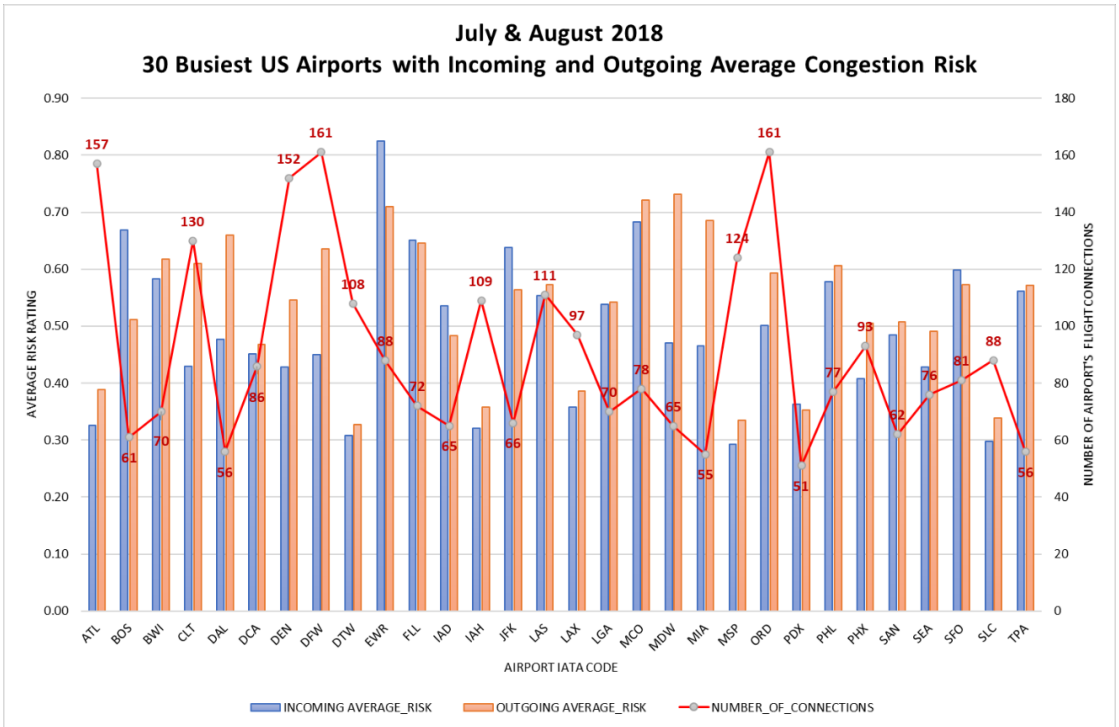


FIGURE 4.37. 30 Busiest Airports with Incoming & Outgoing Delay Risk for July-August 2018

As one can notice in Fig. 4.37, there are airports that create more departure delays than arrival delays occurred, therefore for these airports, the outbound average risk exceeds the inbound average risk. Such airports are: ATL, CTL, DAL, DEN, DFW, DTW, MDW, MIA, MCO, MDW, MIA, ORD, PHX, SEA, SLC, etc. On the other hand, there are airports that manage to mitigate occurred arrival delays, like the BOS, EWR, JFK, IAD, SFO. These airports perform better in their operations handling, mitigate occurred arrival delays, and propagate fewer delays to the downstream connections. Overall, the best performing airports for avoiding delay risks are ATL, DTW, IAH, MSP, and SLC, which have the lowest average ingoing and outgoing risk. On the downside, the most congested airports are EWR, FLL, and MCO.

In Fig. 4.38, the same 30 busiest airports for 2019 are presented, with blue and orange bars for inbound delay risk and outbound delay risk, respectively, while the number of connections with other airports is shown in the red line. By comparing Figure's 4.38 diagram to the previous one, we see an increase in airport connections during 2019 vs. 2018, for the majority of airports. This is in accordance with the reported flight's increase, as reported by BTS. Moreover, it is evident from this graph that all airports have improved on-time performance and decreased delay risk versus previous year, despite the fact that airport connections to most airports have increased on average by 2.5% (2797 more flights vs. 2018). The airports, where departure delays are exceeding arrival delays, have slightly changed. The airports that manage to mitigate occurred

arrival delays are: BOS, EWR, FLL, JFK, SAN, SFO, TPA. The best performing airports for avoiding delay risk remain: ATL, DTW, MSP, SLC, while the most congested ones remain EWR, FLL, and MCO. Despite the improvement in on-time performance, the airports that propagated more delays in the aviation network remain the same.

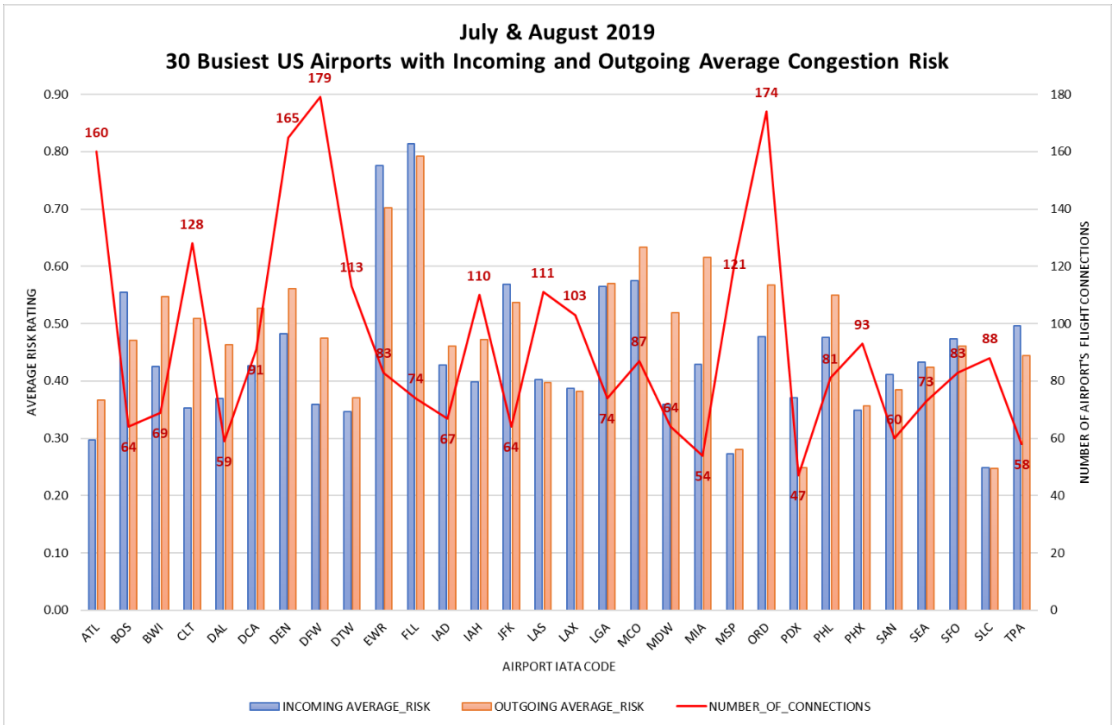


FIGURE 4.38. 30 Busiest Airports with Incoming & Outgoing Delay Risk for July-August 2019

To reveal the most congested routes, we sorted the airports that concentrated the higher total risk in descending order. To do so, we utilized the proliferation of delay impact with delay likelihood, as shown in equation (2).

In Fig. 4.39, we present the average risk of the eighty most congested connections between airports for July and August in 2018. These connections between airports have at least 10 flights per day, by all commercial carriers who provide scheduled flights in the connection. It is worth mentioning that there are airport connections that are served by 35-40 flights per day (like the connections between LAX-SFO, LGA-ORD, and LAX-JFK).

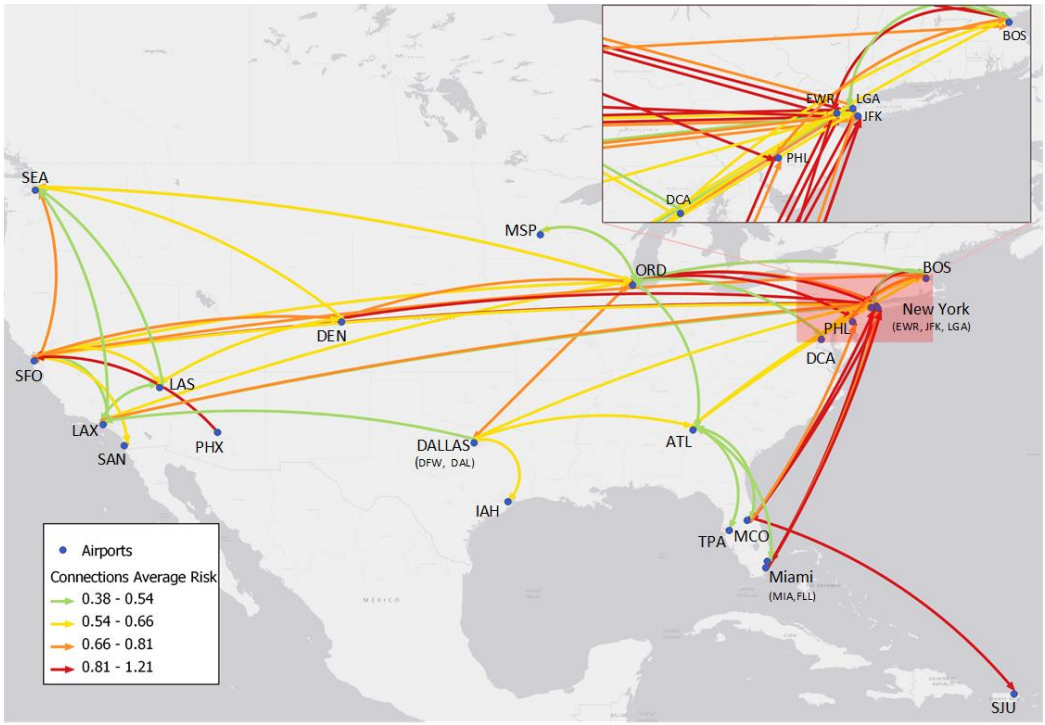


FIGURE 4.39. Most Congested Connections with Higher Average Delay Risk (2018)

In addition, in Fig. 4.39 we depict the most congested connections, which have higher average delay risk as occurred for peak traffic months (July-August) of the year 2018, while the data in detail are given in Tab. D2 of Appendix D. The most congested routes depart/arrive between the airports: DEN, EWR, JFK, LGA, FLL, MCO, ORD, LAX, SFO. Especially the routes with higher average risk are: DEN→EWR, ORD→EWR, MIA→JFK, FLL →JFK, MCO→JFK, SFO→ EWR, EWR→ FLL, which involve New York area airports (EWR, JFK, LGA), either as the origin or as destination airport. This graph was also produced for the same period in the year 2019. In Fig. 4.40, we exhibit the most congested connections with heavy traffic and high average delay risk, while the data in detail are given in Tab. D3 (Appendix D). As one can notice, although the flight movements have increased in 2019, there is a slight improvement in congestion's performance with lower average risk values in many airports. The most congested routes still include the airports DEN, EWR, JFK, LGA, FLL, MCO, MIA, FLL, and ORD, while new airports have appeared on the map, like CLT, DTW, ANC, etc.

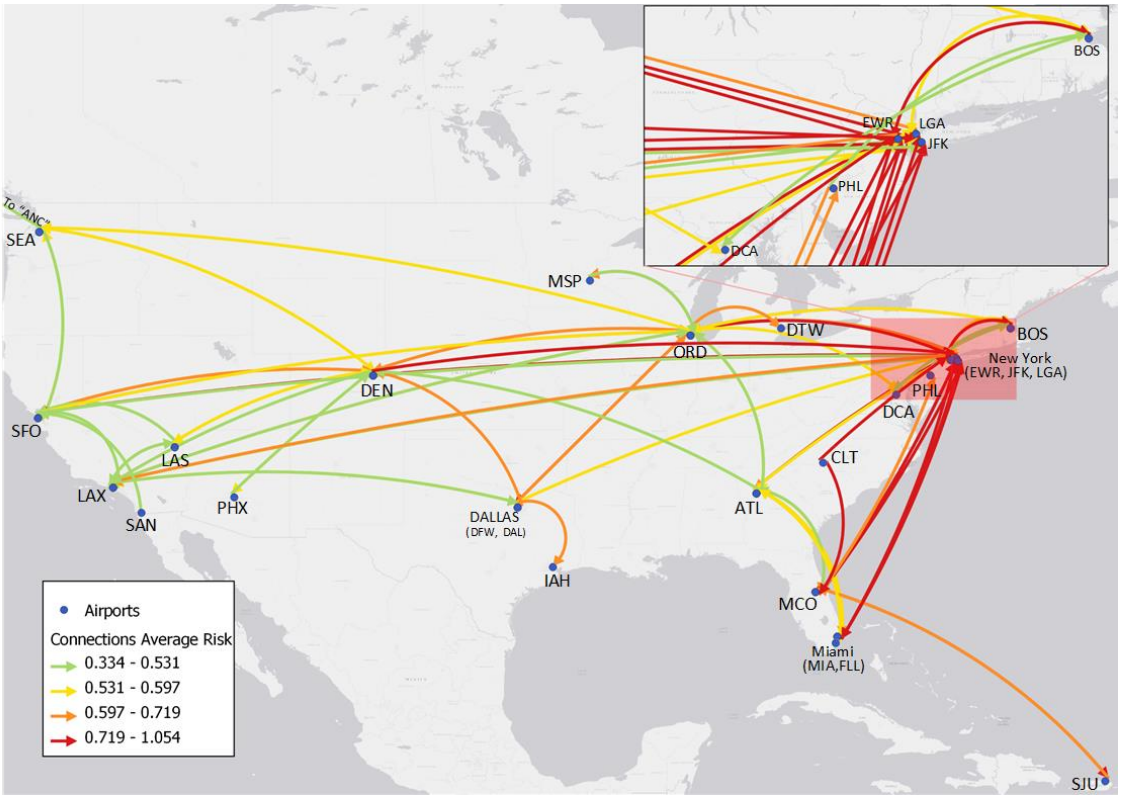


FIGURE 4.40. Most Congested Connections with Higher Average Delay Risk (2019)

DEPENDENCY CHAIN ANALYSIS

Our tool generated all dependency chains for each aircraft's TN and for each route traveled within the same day. The tool accepted all airports as nodes and flights as edges. All data were imported as CSV files into Neo4J graph database for risk path calculation. First, we used our tool to find out the aircraft chains that accumulated higher dependency risks. The results are presented in Tables 4.19 and 4.20, for years 2018-19, respectively, where we indicate: i) the worst aircraft routes visiting 3-6 airports in a single day; ii) the dependency risk values; and iii) the accumulated arrival delays, counted in minutes.

Although an aircraft can fly up to 9 destinations in a day, depending on destination distance and airport's congestion, results indicated that the worst aircraft were those who visited congested airports, usually with fewer flight legs. Findings also showed that the cascading effects beyond the fifth order could rarely affect the consequent infrastructures. Since the product of likelihood tends to zero, so does the cascading congestion risk after 5 flight legs.

Table 4.19. Dependency Chain Risk Analysis for (2018)

AIRCRAFT TN	RISK	1st AIRPORT	R1	2nd AIRPORT	R2	3rd AIRPORT	R3	4th AIRPORT	R4	5th AIRPORT	R5	6th AIRPORT	Sum of delays in minutes
N342AN	7.43	PHL	4.97	SJU	2.45	PHL							679
N410UA	6.23	MCO	4.54	EWR	1.69	MCO							1673
N938FR	7.10	ATL	3.82	COS	2.41	PHX	0.87	DEN					1229
N949FR	7.97	TUL	2.47	IAD	3.37	COS	2.13	PHX					328
N993JB	6.75	EWR	3.56	RSW	2.15	EWR	1.04	FLL					909
N350DN	5.77	JFK	4.07	MCO	0.86	JFK	0.55	MIA	0.28	JFK			1807
N807JB	6.50	EWR	3.56	RSW	1.84	EWR	0.73	RSW	0.38	EWR			573
N939FR	7.35	SJC	2.06	TUL	2.26	IAD	1.85	COS	1.17	PHX			374
N263SY	6.30	ORD	4.55	LGA	1.25	PIT	0.38	LGA	0.12	ORD	0.03	LGA	1767
N324FR	6.49	JAX	2.50	SAT	2.35	JAX	1.04	STL	0.46	JAX	0.14	LAS	446

The top 10 worst dependency aircraft routes for July and August of the year 2018 are presented in Tab. 4.21. Data inside the table distinguish aircraft that accumulate higher delay risk when flying between congested airports (e.g. PHL↔SJU, JFK/ EWR↔MCO, ORD↔LGA). In some circumstances, delays exceeded 24 hours and finally, the aircraft arrived the day after. For example, TN: N410UA delayed for 483 minutes in the first leg, while in the next leg it delayed for another 1190 minutes, to sum up 1673 minutes of delay. It is obvious that the aircraft could not fly to other destinations on the same day, due to accumulated delays. For TN: N342AN the delays were fewer (679 min), however, the congestion likelihood for the connections involved was significantly higher for each flight leg. Thus, the dependency risk of this flight chain took a higher value.

Moreover, in Tab 4.21 we can notice that aircraft with 3-4 connections per day accumulate high delays when passing through congested airports of New York (EWR, JFK, LGA).

To analyze further what went wrong with these worst performing dependency routes, we provide a causal delay analysis. For all TN presented in Tab. 4.21, accumulated arrival delays and delay causal analysis are exhibited in Tab. 4.22. Results in tab.4.22 indicate that most delays were at-tributed to late-arriving aircraft, followed by air carrier deficiencies, while extreme weather delays are negligible and NAS delays less important.

Table 4.20. Delay Causal Analysis for Aircrafts with Higher Dependency Risk (2018)

FLIGHT DATE	TAIL NUM	ACCUMULATED ARRIVAL DELAYS	LATE AIRCRAFT DELAY	CARRIER DELAY	NAS DELAY	EX. WEATHER DELAY
30/7/2018	N342AN	679	90%	9%	2%	0%
24/7/2018	N410UA	1673	29%	49%	22%	0%
9/8/2018	N938FR	1229	100%	0%	0%	0%
25/7/2018	N949FR	328	29%	9%	63%	0%
29/7/2018	N993JB	909	66%	27%	3%	4%
11/8/2018	N350DN	1807	0%	43%	57%	0%
15/8/2018	N807JB	573	67%	33%	0%	0%
28/7/2018	N939FR	358	63%	32%	5%	0%
23/7/2018	N263SY	1663	41%	55%	4%	0%
26/8/2018	N324FR	446	97%	2%	1%	0%

Table 4.21. Dependency Chain Risk Analysis for (2019)

AIRCRAFT TN	DEPENDENCY RISK	1st AIRPORT	R1	2nd AIRPORT	R2	3rd AIRPORT	R3	4th AIRPORT	R4	5th AIRPORT	R5	6th AIRPORT	Sum of delay in minutes
224NV	7.12	FLL	3.75	GSP	3.37	FLL							360
N658JB	5.70	EWR	3.43	SJU	2.27	EWR							1023
N990AN	5.89	CLT	4.79	MIA	0.94	DFW	0.15	MIA					1104
N375JB	4.77	MCO	2.70	HPN	1.39	TPA	0.67	HPN					832
N566JB	6.46	FLL	3.82	HPN	1.54	RSW	0.67	HPN	0.44	FLL			1300
N703JB	6.42	SJU	3.61	EWR	1.84	FLL	0.64	SJU	0.33	BOS			1092
N794JB	5.73	SJU	3.09	EWR	1.52	SJU	0.78	EWR	0.33	PBI			834
N996JL	5.32	BQN	3.87	JFK	0.93	MCO	0.39	JFK	0.13	SJU			428
N974JT	4.81	FLL	2.87	JFK	1.06	FLL	0.61	JFL	0.27	FLL			794
N918US	6.02	CLT	4.03	PDX	1.65	CLT	0.30	RDU	0.02	CLT	0.01	RDU	654

See Appendix C for Airport names

The top 10 worst dependency chain routes for the same summer period in the year 2019 are presented in Tab. 4.23, to compare congestions and delay risk performances versus previous year. As one can notice, the worst flights with two legs have accumulated lower delays in minutes, comparing with the previous year, while the same busiest airports appear in dependency chains. When comparing the worst dependency chains with more flight legs in Tab. 4.23, we can notice that there is a lower aggregated dependency risk than the previous year, and so does the sum of accounted delays. However, in both years, the same airport hubs are included in worst chains, as congested ones, such as New York airports (EWR, JFK) and Florida airports (MCO, MIA).

Table 4.22. Delay Causal Analysis for Aircrafts with Higher Dependency Risk (2019)

FLIGHT DATE	TAIL NUM	ARRIVAL DELAY	LATE AIRCRAFT DELAY	CARRIER DELAY	NAS DELAY	EX. WEATHER DELAY
9/8/2019	224NV	360	49%	45%	6%	0%
22/7/2019	N658JB	1023	30%	46%	3%	21%
14/8/2019	N990AN	1104	77%	19%	5%	0%
14/7/2019	N375JB	832	66%	34%	0%	0%
1/7/2019	N794JB	834	93%	4%	3%	0%
9/8/2019	N566JB	1300	75%	22%	2%	0%
9/8/2019	N703JB	1092	94%	3%	3%	0%
23/8/2019	N996JL	428	77%	2%	21%	0%
7/8/2019	N13248	1866	57%	0%	33%	11%
24/7/2019	N974JT	794	85%	8%	3%	5%
22/8/2019	N918US	445	86%	1%	2%	10%

In Tab. 4.24, percentages of causal delay analysis for each TN are provided, to analyze the cause of delays for the worst-performing dependency aircraft routes in the year 2019. As one may notice, most of the delays were attributed to late aircraft arrivals and air carrier deficiencies, while extreme weather delays and NAS delays introduce fewer disruptions in the aviation network.

We can also notice that both dependency analysis experiments include some of the routes of worst-performing connections, as presented in red in Fig.4.36.

Comparing the chains presented in both tables, we can distinguish the improved delay performance in summer months for years 2019 and 2018. When delays are shorter the likelihood of lateness is lower, so does the accumulated dependency risk. Out of 370 airports we examined, some appeared more often than others in congested routes and seemed to greatly affect the network, in terms of adding delays. Overall data calculated are hard to be presented in detail, therefore indicative results for worse performing aircraft are presented.

In the last phase of our analysis, we used our tool to detect future airports' congestions, owed mainly to interdependencies by extracting patterns and trends, based on the historic flight data analyzed. For calculating dependency risk, we used for each connection the average impact of all flights examined during the summer period in 2019. In the experiments, we have distinguished two major airports categories: i) the busiest airports, which serve from 300-1500 flights per day; and ii) the regional airports which usually have lower daily traffic, but due to summer seasonality, they serve more flights than their year ave-rage performance.

In order to evaluate the worst dependency chains for the busiest airports, we used total risk performance and we distinguished the eighty worst dependency paths to present them in the graph shown in Fig. 4.41.

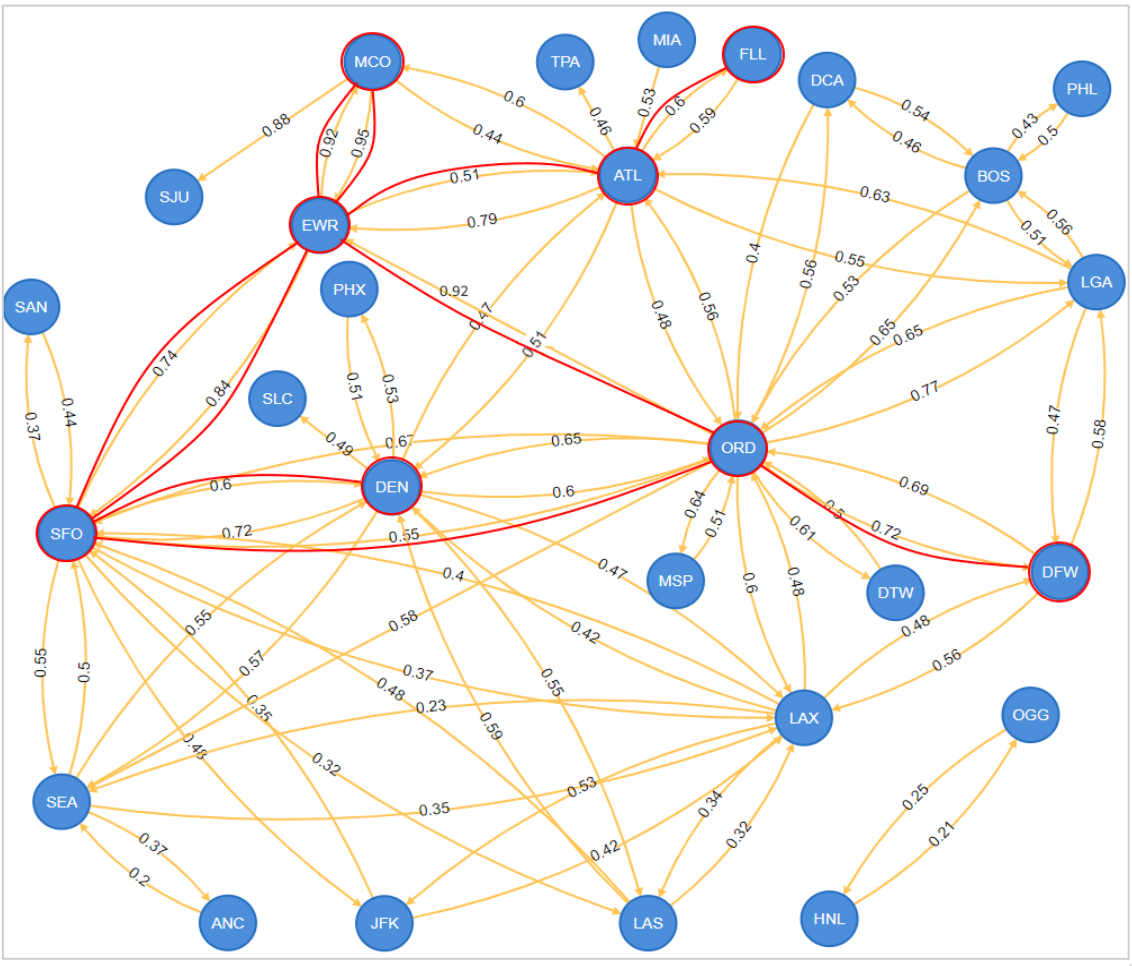


FIGURE 4.41. **Graphical representation of worst dependency chains produced based on top 80 highest *total* risk connections**

In the graph depicted in Fig. 4.41, one can distinguish the airports which can produce greater delays in the aviation network, and these are ATL, EWR, DFW, ORD, LAX, MCO, SFO. The connections presented in the graph are more likely to introduce delays in the aircraft's scheduled flight routes. The lines marked with red color represent the worst dependency flight connections, with higher cumulative risk, which are analytically presented in Tab. 4.23.

Table 4.23. Top 5 worst dependency routes from the dependency risk output of airports with highest total risk connections

Paths	Cumulative Risk
(ORD)→(EWR)→(MCO)→(EWR)→(SFO)→ (DEN)	1.63
(ORD)→(EWR)→(MCO)→(EWR)→(SFO)→ (EWR)	1.63
(EWR)→(MCO)→(EWR)→(SFO)→(EWR)→ (ATL)	1.59
(EWR)→(MCO)→(EWR)→(SFO)→(ORD)→ (DFW)	1.58
(MCO)→(EWR)→(SFO)→(EWR)→(ATL) →(FLL)	1.53

On the other hand, to evaluate the worst dependency chains for the regional airports, we used average risk performance, (instead of total risk used for the busiest ones) and distinguished the eighty worst dependency paths. These flight connections are presented in the graph shown in Fig. 4.42.

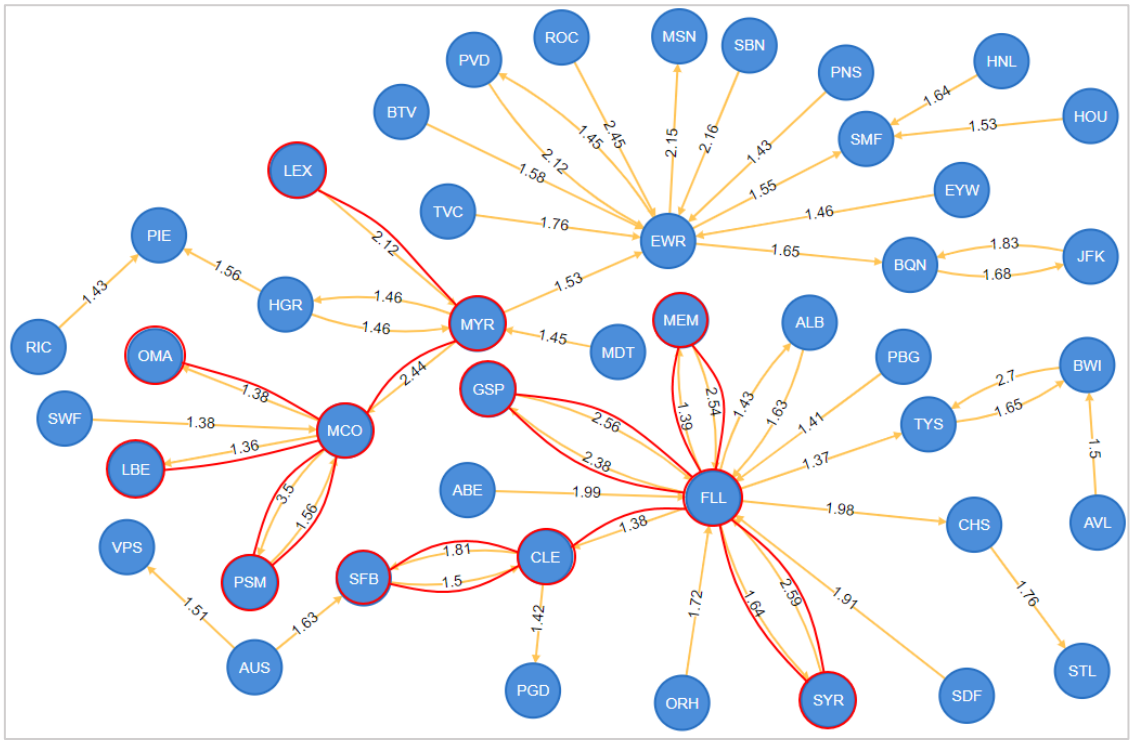


FIGURE 4.42. Graphical representation of the examined graph produced based on top 80 highest *average* risk connections

In the graph, we can distinguish the airports which can produce greater delays in the aviation network, and work as hubs to the regional airports propagating delays in the aviation peripheral network due to summer seasonality in traveling. These airport hubs are EWR, FLL, and MCO. The connections presented in the graph are more likely to introduce delays in the aircraft's scheduled flight routes. The lines marked with red color represent the worst dependency connections, which are analytically presented in Tab. 4.24.

Table 4.24. Top 5 worst dependency routes output from the dependency risk analysis for highest average risk connections

Paths	Cumulative Risk
(MYR)→(MCO) →(PSM)→(MCO)→(OMA)	8.06
(LEX) → (MYR) → (MCO)→(PSM→ (MCO) → (LBE)	7.97
(SYR) → (FLL) → (GSP) → (FLL))→ (MEM) → (FLL)	7.77
(MEM) → (FLL) → (GSP) →(FLL) → (SYR) → (FLL)	7.66
(SYR) → (FLL) → (GSP) → (FLL) → (CLE) → (SFB)	7.53

Finally, comparing the worst dependency paths in Tab. 4.25 and 4.26, one can notice a big difference in aggregated dependency risk between the paths involving the connections of busiest airports, versus the ones of regional airports. This makes sense, since large airports, which serve domestic aviation traffic as the nation's hubs, may introduce significant delays in the network. |However, they are more competent to handle heavy traffic, minimize average delay risk, and be resilient when unexpected delays occur, especially during the summer period.
So, their on-time performance is better than the performance of regional airports, and this is reflected in connection chains with lower cumulative dependency risk values.

4.4.6 Summary of Research Work

In this work, we propose a risk-based dependency method to analyze congestions in the aviation network. The methodology and the developed tool can assess the risk of delay incidents in airports and produce weighted risk dependency graphs, presenting how a delay that occurred in one airport may affect other interconnected airports. By using real data collected from US Bureau of Transportation Statistics, we analyzed how flight delay risk propagates into the aviation network. Based on historic flight performance data, we also provided a prediction for congested connections and higher dependency risk chains.

We were able to detect the worst airports, in terms of affecting the aggregated delay of an aircraft route, along with airports that perform better and mitigate delay propagation in the aviation network. The tool, we have developed for congestion analysis, can be used to identify key airports inclined to delays with great influence on the network due to: (i) the number of connections; (ii) the likelihood of congestions; and (iii) the airports that get affected the most by delays occurred in previous airports.

Between the two consecutive years examined, which included two summer months in 2018-19, simulation results indicated that significant delay risk mitigation was achieved in summer 2019 versus the previous year. The results were cross validated with BTS air travel consumer reports issued for the same period to verify the performance and the efficiency of the developed tool.

Generally, our tool can detect: i) the flights with the highest overall risk to be congested and create major impact with propagation delays to downstream flights in the aviation network; ii) dependency paths with highest overall impact for specific connections per period of calculation (week, month, year); iii) the airports which create delays in the aviation network and exert higher influence on other airports in terms of both impact (how much delay they introduce to other flight connections) and centrality (how many other flights they may affect), and iv) the worst n-order airport dependency chains.

Simulation results can aid airlines and operators, flight planners, and decision-makers to assess congestion risks of routes towards busy airports and analyze large-scale congestion scenarios. The model can also be used to run specific scenarios of interest to airlines concerning specific airport connections. These include "what-if" scenarios that only consider delays that affect one or some of the airports. By analyzing nth-order dependency paths, we can: i) identify which dependencies should have a high priority for applying mitigation controls for risk reduction in the aviation network; ii) propose alternatively connection paths; and iii) indicate flight connections to be avoided or rescheduled.

Chapter 5: A new methodology toward effectively assessing data center's sustainability

5.1. Introduction [10]

Data centers are found in nearly every sector of the economy, such as financial and commercial services, media and communications, academic and governmental institutions. Day to day, there is an increasing demand for data processing and storage, thus cloud computing has been evolved, supported by the continued growth of internet services worldwide. This has led to significant energy consumption, accompanied with serious environmental impacts, such as earth resources spending, greenhouse gas emissions, electronic equipment waste and environmental pollution. Various metrics have been proposed to evaluate efficiency in data centers, aiming to develop energy conscious behavior and resources savings, however they are falling short, when assessing sustainability of a data center in a holistic view. Sustainability aims at preserving the environment, along with economic, operational, and social longevity. The creation of sustainable data centers, using renewable energy, optimizing energy efficiency, and minimizing resources waste, makes both environmental and business sense. In this chapter, we present a new methodology, for assessing sustainability based on five major quantifiable elements, composed by different influencing factors, with the aim to obtain a holistic approach. By introducing a new sustainability scoring model, we can evaluate in a spherical way the environmental impact and operational efficiency of data centers.

The Information and Communication Technology (ICT) industry has a broad impact on our economy and society, due to the wide spread of ICT services in every commercial and almost every human activity. In addition, the evolution of cloud computing, provided nowadays as a service, contains thousands of Data Centers (DCs) trying to fulfill every customer demand online and on time. These DCs span in hundred to thousand square meters of area, thus huge amount of power is required for running these server farms, feeding with energy processors, monitors, network equipment, lighting, air distribution fans and cooling systems. Supported by the continued growth in internet-based services, DCs facilities can consume large amounts of electricity and put an increasing strain on utility grids and energy resources (Yuventi & Mehdizadeh, 2013).

According to International Energy Agency (2016) and recent publications (Bawden, 2016; Nieuweling, 2016; Shehabi et al., 2016), data centers have mushroomed from virtually nothing ten years ago, to consuming about three per cent of the global electricity supply and accounting for about two per cent of total greenhouse gas emissions (GHG).

[10] *Related Publication:* Lykou G., Mentzelioti D., Gritzalis D., "A methodology for effectively assessing Data Center sustainability", *Computers & Security* (Special Issue), 2018

That gives the same carbon footprint as the whole international aviation industry, or equally total electricity consumption of highly developed countries like UK and France. Even worst the amount of energy consumed by these DCs is expected to treble in the next decade, seriously increasing its environmental footprint and jeopardizing efforts to contain global warming.

The main concept of dealing with the green ICT services nowadays, principally focuses on reducing energy consumption. However, green computing should include energy saving efforts, along with GHG emissions reduction and innovative methods of effectively reused and recycled resources, minimizing environmental footprint (Jain et al., 2013). Taking into account the fact that renewable energy industry has reached maturity, as a utility power generation technology, maximizing onsite renewable power usage can be a cost-effective green computing opportunity (Chinnici & Quintiliani, 2013). Furthermore, there are countries, where more than half the total energy generated, comes from renewable sources (Eurostat, 2017) e.g Scandinavian Countries in Northern Europe. Combining favorable cold climate with green energy utilities has a great significance, when selecting the appropriate location for installing a green data center.

While significant research has been focused on energy efficiency and optimized performance in the design and operation of ICT systems, very little has been reported towards assessing Data Center sustainability, in a holistic view, using a quantitative modeling approach.

Many metrics have been proposed to evaluate and communicate DC performance. Some focus on energy efficiency, water efficiency, carbon footprint, others on data productivity. However, all these metrics have certain shortcomings, since they evaluate a single parameter of resources consumed by DC operation and not sustainability of the system as a whole. To the best of our knowledge, sustainability scoring model has never been proposed for evaluating DCs performance despite the fact that DCs have tremendously increased their environmental footprint nowadays.

The purpose of this work is to introduce a holistic sustainability evaluation model that can be applied to data centers, using a scoring system and taking into account all necessary components, in order to discover how green, how efficient, and how social friendly this data center is. This model can help DCs owners and operators to evaluate the sustainability of their facilities and make prompt decisions on their management choices, increasing their operating efficiency, while reducing their environmental footprint.

The rest of this study is structured as following: A short presentation of DCs facilities design, machinery, and associated equipment in given in subsection 5.2. Best practices for achieving DCs Energy Efficiency are collected from literature and presented in subsection 5.3, followed by already developed metrics for assessing energy efficiency and resources utilization in subsection 5.4. Then, subsection 5.5 presents the main contribution of this work, where a new sustainability framework for DCs is introduced and analyzed. Subsection 5.6 tests the application of this methodology in already

operating data centers and results are presented. Finally, subsection 5.7 concludes our research and proposes further work.

5.2. Data Center in a snapshot

Data centers apply to spaces specifically designed and equipped to meet the needs of high-density computing equipment such as server racks used for data storage and processing. Typically, these facilities require dedicated uninterruptible power supplies and cooling systems (ENERGY STAR, 2012). DCs functions may include traditional enterprise services, on-demand enterprise services, high performance computing, internet facilities and/or hosting facilities. Often data centers are free-standing, mission-critical computing installations, autonomous located or within a larger corporate building.

As presented in Figure 5.1, data centers primarily contain electronic equipment used for data processing (Servers), data storage (Storage) and communications (Network). Collectively, this equipment processes, stores and transmits digital information using Software and Information Technology (IT) Services. DCs are served by specialized power conversion (Power Generator & Power Transformer) and backup equipment (UPS) to maintain reliable, high-quality, energy supply for the whole installation.

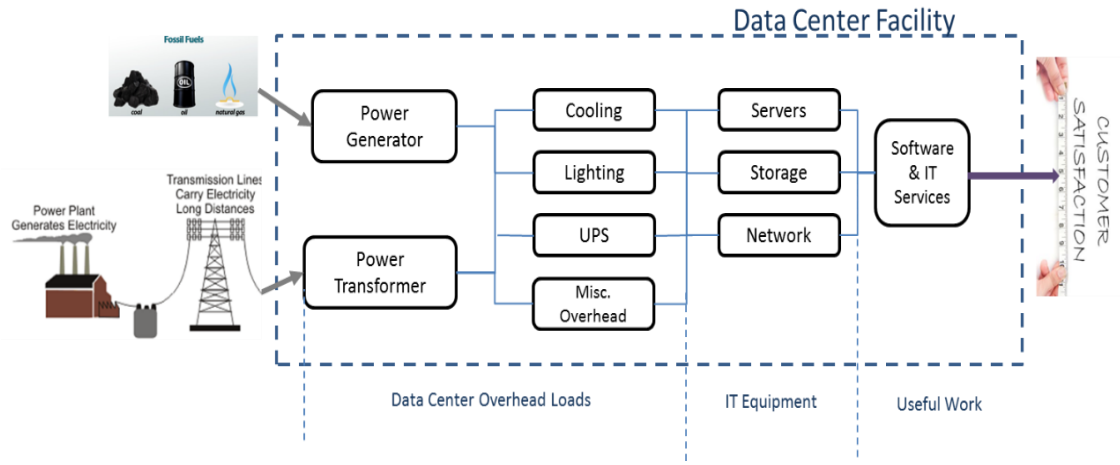


Figure 5.1: Data Center power structure and energy loads

Data center facility is also equipped with redundant equipment for robustness, air conditioning (Cooling) and Lighting. Environmental control equipment maintains the proper temperature, humidity, and appropriate indoor air quality conditions for efficient operation, usually through sophisticated electronic controllers and Building Management Systems (BMS).

It is obvious that DCs business approach and main concern focus on supporting information society, around the clock, 365 days a year, striving to develop advanced, high

quality services that ensure customer satisfaction and loyalty. Their operation needs to ensure four key properties: i) security: assurance of integrity, authenticity, and confidentiality of information; ii) safety: avoidance of hazards; iii) resilience: ability to provide and maintain an acceptable level of service in the face of failure or disruption; and iv) sustainability: maintenance of long-term operation by optimizing performance, while minimizing environmental impact (Banerjee et al., 2012).

5.3. Best Practices for Energy-Efficient Data Centers

Several international initiatives have started addressing energy efficiency in data centers. For example, EU-Code of Conduct for data centers (Avgerinou et al., 2017), Green Grid (2010) and Energy Star Program (2012) have launched energy efficiency criteria and benchmarks, along with best practice measures and efficient product technologies, in order to support DCs efficiency both at IT hardware level and infrastructure level.

In a typical data center with an energy efficient cooling system, ICT equipment loads can account for more than half of the entire facility's energy use (The Green Grid, 2010). Providing efficient IT equipment can significantly reduce energy loads within the data center and downsize the equipment needed for cooling. Purchasing servers equipped with energy-efficient processors, fans and power supplies, high-efficient network equipment, consolidating storage devices, consolidating power supplies, and implementing virtualization are the most advantageous ways to reduce ICT equipment loads within a data center.

In this work, we present Best Practices applied to increase energy-efficiency for the design and operation of DCs, as collected from several literature sources. Therefore, we focus on best practices for ICT equipment, while we expand guidance to a variety of energy efficiency measures for the whole DCs installation (Data Center Facility), which support robust and reliable operation.

5.3.1. Efficient ICT Equipment

ICT equipment best practices have been proposed to increase energy efficiency both for hardware, like rack servers, storage devices, network equipment, power supply and for software like virtualization techniques.

Servers: Rack servers are the main perpetrators of wasting energy and represent the largest portion of the IT energy load in a typical data center. Improvements in the internal cooling systems and processor devices manage to minimize this wasted energy. Variable speed fans are used for the internal component cooling and power management devices can reduce energy consumption on idle processors. Multi-core processor chips allow simultaneous processing of multiple tasks, leading to higher efficiency and improved performance.

Storage Devices: Power consumption is linear to the number of storage modules used. Although storage redundancy offers reliability, it needs to be rationalized and right sized. Maximizing storage capacity utilization by drawing from a common pool of shared storage can provide significant energy savings.

Network Equipment: As network demand varies, there are active energy management measures which can be applied to reduce energy usage, such as idle state logic, gate count optimization, memory access algorithms and Input / Output buffer reduction. Ethernet network energy efficiency can be substantially improved by quickly switching the speed of the network links to the amount of data that is currently transmitted.

Power Supplies: Using higher-quality components and advanced engineering, it is possible to find power supplies with efficiencies up to 95%, which can lower power energy consumption and indirectly reduce cooling system cost and rack overheating issues.

Software Techniques: Virtualization is a method of running multiple independent virtual operating systems on a single physical computer. Instead of operating many servers at low CPU utilization, virtualization combines the processing power onto fewer servers, that operate at higher utilization. Virtualization can drastically reduce server power and consequently the size of the necessary cooling equipment. Some overhead is required to implement virtualization, but this is minimal compared to the savings that can be achieved.

5.3.2. Efficient DC Installation

Energy efficiency measures for facility overheads, focus on cooling systems, air supply management, lighting and other electrical systems serving the facility, like plug-in loads and energy consuming devices.

Air and Cooling Management: Effective air management minimizes the bypass of cooling air and the recirculation of heat exhaust around rack intakes, which can reduce operating costs, increase the data center's power density, and reduce heat related processing interruptions or failures. When selecting the appropriate cooling systems, it is important to consider initial and future loads, in particular part-load and low-load conditions. A high-efficiency chiller is the most common cooling option for large facilities equipped with variable frequency driven compressors, high evaporator, and low entering condenser water temperatures.

Lighting: Since data center spaces are not uniformly occupied, they do not require full illumination during all hours. Therefore, zone-based occupancy sensors can have a significant impact on reducing the lighting electrical use. Careful selection of an efficient lighting layout, lamps and ballasts can also reduce not only the lighting electrical usage but also the heat load on the cooling system.

Electrical Systems: Similar to cooling systems, it is important to always consider initial and future loads, along with low-load conditions, when designing and selecting plug-ins and electronic equipment for minimizing data center's overheads.

All these measures and best practices should be applied and properly evaluated by using suitable metrics and performance measurements. Various studies have shown that there is significant opportunity to conserve energy in the data center by improving the energy efficiency of infrastructure equipment. This could allow energy savings of 20-60% or even higher.

5.4. Metrics for energy efficiency assessment in data centers rooms

Following the motto "You can't manage, what you cannot measure", metrics are key drivers towards energy efficiency of DC facilities. They should meet specific requirements like ease of use, low cost to implement, accuracy, objectivity, so as to be acceptable and used by DCs operators and ICT industry.

Energy efficiency metrics are typically used for benchmarking the energy consumption of single products or systems, hence covering equipment or facility-level. The complexity of a data center, as a system, is without doubt a challenging factor. As a result, a variety of metrics have been introduced with the intention to quantify selected aspects of the data center performance. They are distinguished into two main categories:

- The first type is intended for the evaluation of energy efficiency of the IT equipment. This type is typically a test bed benchmark, which measures the energy consumption and efficiency of the IT equipment, based on a defined workload managed in a certain time frame. Such comparison of different technical concepts and solutions is used as a basis for purchasing decisions and represents an ex-ante assessment of energy efficiency with various metrics, which are presented in subsection 5.5.1.
- The second type of metrics supports continuous monitoring of total DC facility efficiency and operation. This type of metrics premise specific requirements regarding measurements and system boundaries. These metrics are analyzed in subsection 5.5.2.

Both types of metrics are suitable for DC operators to evaluate efficiency and they are potentially capable of cross comparison among different DCs. However, these metrics have some limitations which are presented and discussed in subsection 5.5.3.

5.4.1. Metrics for IT Equipment

Many researchers and industrialists have introduced methods to optimize data center designs for energy considerations and metrics to benchmark efficiency. The most

commonly used energy related metrics for IT equipment as a system are Performance per Watt, Compute Power Efficiency and EnergyStar Score, which are briefly analyzed below.

Performance per Watt: quantifies the energy efficacy of individual computer architecture or computer hardware. It is the processing rate that can be remitted by a processor for each watt of power absorbed by it. Normally it is measured in FLOPS (floating-point operations per second) and MIPS (million instructions per second).

Compute Power Efficiency (CPE)*:* It is a measure of the computing efficiency of a datacenter and is defined as following:

CPE = (IT Equipment Utilization * IT Equipment Power) / Total Facility Power (1)

This metric is unit-less and has a maximum value of 1.0 or 100%. This allows the CPE of two different data centers to be compared, since there is no need to convert the units of measurement. However, the metric face serious difficulties in application, since it uses "utilization" as a measure of useful work and there is no clear definition of utilization that works for all IT equipment in all applications.

ENERGY STAR score: provides a fair assessment of the energy performance of a DC, taking into account the climate, weather and business activities. To identify the aspects of building activity, a statistical analysis of the peer DC building is performed. The result of this analysis is an equation that can predict the energy use and then prediction is compared to its actual energy use to yield a 1 to 100 percentile ranking of performance, relative to the national population.

5.4.2. Metrics for Data Center Facility

Various metrics, in terms of energy or resources used to serve the whole facility of examined data center have been introduced to measure efficiency, like the popular PUE (Power usage Effectiveness), or its inverse fraction DCiE (Data Center infrastructure Efficiency), the GEC (Green Energy coefficient), the ERF (Energy Reuse Factor), the CUE (Carbon usage Effectiveness) and the WUE (Water usage Effectiveness). All these metrics are introduced and analyzed in this section.

Power Usage Effectiveness (PUE) has been introduced by Green Grid for the comparison of energy used by computing application and infrastructure equipment with the energy wasted in overhead loads. Value of PUE depends on building location and construction characteristics of datacenter facility. The PUE can be described as the ratio of overall electricity consumed by the facility of a data center to the overall electricity consumed by IT equipment with the following equation:

PUE = Total Facility Energy / IT Equipment Energy (2)

where:

IT Equipment Energy can be described as the energy that data center has taken for the management of IT equipment, processing of IT equipment and storing the data in disk drives or routing the data within the datacenter.

Total Facility Energy is IT equipment power plus power needed by uninterrupted power supply (UPS), generators (needed to provide power in case of power failure), batteries, cooling system and lighting.

Perfect efficiency would give datacenter a PUE of 1.0. An average data center has a PUE of 2.0, however, several recent super-efficient data centers have been known to achieve a PUE as low as 1.1. If a datacenter has PUE 1.5 then it means when IT equipment has consumed 1kWh, data center has consumed 1.5 kWh of energy and 0.5 kWh energy has wasted in unfruitful work, such as IT equipment cooling, grid power conditioning, lighting and other overhead consumptions.

The PUE metric is the most popular method of calculating energy efficiency and it is the most frequently used metric for operators, designers, and facility managers to determine how energy efficient their data centers are.

Data Center infrastructure Efficiency, *DCiE:* is the inverse fraction of PUE. It is defined as:

DCiE = IT Equipment Energy / Total Facility Energy	(3)
or equally: DCiE = 1 / PUE	(4)

Although PUE and DCiE are the most commonly used metrics designed for the efficiency comparison of datacenters, it is evident that their approach only allows the assessment of energy efficiency of the DC infrastructure (including cooling and power supply) but does not provide any information on the energy efficiency of the IT services themselves. In addition, they do not account for the location climate and different normal temperatures outside the data center. For example, a data center located in Alaska cannot be effectively compared to a data center in Miami, since colder climate results in a lesser need for cooling.

Green Energy coefficient *(GEC):* is a metric that quantifies the portion of a facility's energy that comes from green and renewable energy sources. GEC is computed as the green energy consumed by the data center divided by total energy consumed by the data center. It is a measure for evaluating the energy mix and environmental footprint of a data center and it is defined as:

GEC = Green Energy / Total Facility Energy	(5)

where:

Green energy is any form of renewable energy, like solar energy through photovoltaic panels, or heat energy by solar panels, wind energy powered by wind turbines, hydro powered energy, biofuels powered energy, fuel cells production and others. Green energy

can be either produced nearby the facility or purchased by the data center management through a utility provider with green energy certificate.

Energy Reuse Factor, *ERF:* is a metric that identifies the portion of energy that is reclaimed and exported for reuse outside of the data center. Data centers always have a heat surplus resulting from the conversion of electrical energy into heat within the IT equipment. This heat surplus can be reused in different ways depending on local circumstances, like heat demand for heating offices, preheat water and other facilities nearby the data center. Although it isn't always easy to quantify the amount of energy being reused, it does provide opportunities for increasing economy and improving energy efficiency. ERF is the defined as:

ERF = Reused Energy / Total Facility Energy (6)

where:

Reused energy is measured as it exits the data center control volume and

Total energy consumed by the data center is the total source energy, calculated identically to the numerator of PUE.

Carbon usage effectiveness, *CUE:* is a recently introduced metric by Green Grid to address carbon emissions associated with data centers. It enables the assessment of the total GHG emissions of a data center, relative to its IT energy consumption and it is computed as the total carbon dioxide emission equivalents (CO2eq) from the energy consumption of the facility divided by the total IT energy consumption. It is defined as:

CUE = Total GHG emissions / IT Equipment Energy (7)

where:

Total GHG emissions are greenhouse gases emissions from total energy absorbed by the facility of a data center, including carbon dioxide gases (CO_2), methane (CH_4) and refrigerant fluids that can be emitted in atmosphere. This value is calculated on annual basis.

CUE adds information about the data center's ecological footprint. If the data center has multiple energy sources, like a combination of grid-sourced electricity and on-site renewable sources, the partial contribution of both should be considered. Adopting the CUE metric will incite the industry to choose low impact energy sources, like on-site renewables.

Water Usage Effectiveness, WUE: is a metric introduced by Green Grid to address water usage in data centers. The WUE metric – combined with the PUE and CUE metrics – enables data center operators to quickly assess the water, energy and carbon sustainability aspects of their data centers, compare the results and determine if any energy efficiency and/or sustainability improvements need to be made.

The WUE is a ratio of the annual water usage to how much energy is being consumed by the IT equipment and servers, defined as:

WUE = Water Used Annually / IT Equipment Energy (8)

Water is needed: a) for cooling the facility of a data center, b) for humidification, c) for apparatus associated power generating and energy production, d) for serving other DCs facilities installations. Like CUE, the ideal value of WUE is zero, for no water needed, nor used for data center operation.

5.4.3. Data center efficiency metrics - Existing Limitations

The above introduced metrics are the basis to support energy efficiency of IT-equipment and infrastructure in data centers. It is obvious that the process of measuring and reporting such efficiency factors has provided a focus and comparable performance measurements, which has allowed many DCs operators to make substantial efficiency improvements. However, there is still no generally accepted metric for IT sustainability efficiency. Most efficiency metrics have certain shortcomings particularly regarding modeling the real-life conditions of the entire data center. They are falling short when assessing sustainability of IT services provided by the data center.

Despite the fact that PUE metric has become an industry's standard for reporting energy performance of data centers, it remains an incomplete metric, failing to address hardware efficiency, energy productivity, green energy sourcing and environmental performance of DC facility. Therefore, concepts beyond PUE are sought intensely to relate the energy consumption to the actual environmental impact. DCs industry is challenged to minimize its environmental footprint by adopting and systematically reporting their efficiency performance based on a holistic assessment.

Based on these drawbacks, our proposal introduces a new model for sustainability performance scoring, which evaluates data center environmental impact by combining some of the already established and widely used metrics with qualitive attributes and performance factors. This proposed assessment obtains a holistic view of DCs sustainability performance.

5.5. Proposed Methodology for DCs Sustainability Assessment

This section presents our main contribution, where a sustainability framework for DCs is proposed, considering operational efficiency and performance metrics for the whole data center installation, in order to evaluate in a spherical way, the environmental impact and sustainability performance of data center facility.

Since 2005, sustainability framework has identified three main sustainable goals, such as economic development, social development, and environmental protection. The Three Pillars of Sustainability are a useful tool for defining sustainability problem, as shown in

figure 5.2. It is expressed using three overlapping ellipses, indicating that these elements are not mutually exclusive. In fact, the three pillars are interdependent and in the long run none can exist without the others.

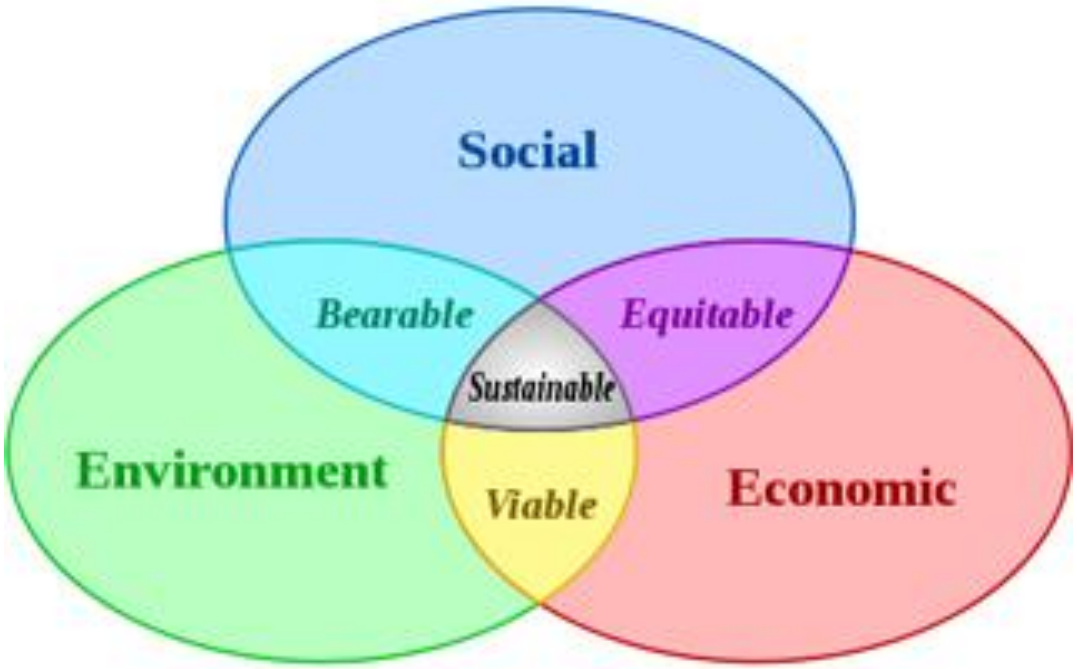


Figure 5.2: The three pillars of sustainability

In our proposal for Corporate Sustainability Assessment, we have enriched this framework, introducing five major "Sustainability Elements", in order to evaluate DCs efficiency with a holistic approach. These five elements are: i) DCs environmental impact, ii) Resource utilization and Economy, iii) DCs operational efficiency, iv) Resources Recyclability and v) Societal Impact. The proposed five elements sustainability assessment is graphically presented in Figure 5.3 and each element is further analyzed in the following subsection.

The purpose for introducing five elements in corporate sustainability that differ from the conventional three broad categories (environment, society and economy), was to capture values and criteria that are significant for DCs corporate governance. Thus, operational efficiency and economic growth are key success factors for such a high technological and competitive environment, where sustainability goes beyond environmental efficiency.

With the introduction of these sustainability elements and corresponding influencing factors, a new framework has been developed to measure the level of sustainability of DCs, either while in design stage, or in operating stage. The inputs of the model consist of data available from well-established and already used metrics and the output is a weighed score that indicates sustainability performance of the DC.

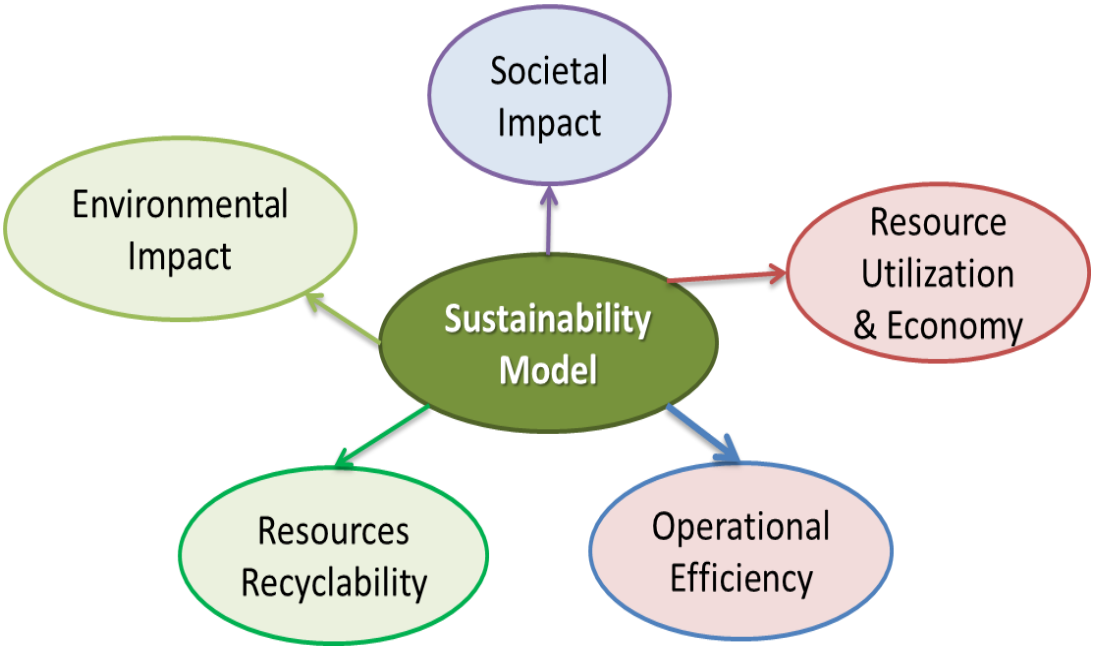


Figure 5.3: Data Center Sustainability Elements Model

5.5.1 Sustainability Elements Analysis

In this subsection, we analyze the five sustainability elements, describing the influencing factors for each element and how they can be evaluated. Most of these factors were selected among the efficiency metrics already presented, focusing on those able to create a holistic aspect for assessing sustainability. It is important for the factors introduced to be fair and applicable to different types of DCs operator, so as to create more positive than obstructive incentives.

5.5.1.1. Environmental Impact examines the environmental footprint of the DC taking into account: i) the usage of Green energy used to power the DC's facilities which contributes to the reduction Greenhouse gas emissions and climate change and ii) Green Material Use, green purchasing inititatives and recycling policies.

Green materials are built aided by green chemistry and technology. They require less resources, eliminate hazardous substances in the design, reduce packaging waste and minimize carbon footprint. The use of certified green materials remains an important driver for sustainability. For example, using of recycled paper, purchasing ecological certified products, requiring RoHS (Restriction of Hazardous Substances) compliance in electronic equipment add up to accounting green material use.

In order to evaluate the DCs environmental impact the following influencing factors are examined and presented in table 5.1:

Table 5.1: Data Center Environmental Impact Factors

Sustainability Element	Influencing Factor	Factor Description
Environmental Impact	GEC	Green Energy / Total Energy Consumed
	GMU	Green Material + Recycled products /Total Material use, ROHS compliance

Green Energy Consumed (***GEC)*** metric was already presented in subsection 4.2, so equation (5) is used to quantify this metric.

Green Material Use (***GMU)*** calculates the use of green material purchased goods relative to total annual purchases. It is defined as:

$$GMU = \text{Green Product Purchases} / \text{Total Annual Purchases} \quad (9)$$

where:

Green Product includes recycled goods (e.g. recycled paper, refilled toners etc), equipment made by environmental friendly materials and green certified products according to local regulations for environmental protection and circular economy principles.

Both influencing factors, as expressed by equations (5) & (9) are ratios with value range between 0-1 and they are expressing DCs environmental footprint.

5.5.1.2. Resource Utilization & Economy uses two metrics to evaluate DC energy efficiency the DCiE and ERF, as listed in table 5.2:

Table 5.2: Data Center Resource Utilization & Economy Factors

Sustainability Element	Influencing Factor	Factor Description
Resource Utilization & Economy	DCiE or 1/PUE	IT Equipment Energy / Total Facility Energy
	ERF	Resused Energy / Total Energy Consumed

DCiE expresses the energy efficiency efforts of DC operation towards resource utilization & economy, while the ERF demonstrates company's efficiency to reuse wasted energy from DC spaces, by converting it to a useful energy that serves other nearby facilities, like heating offices using heat recovery options. It is expressed by equation (3) or (4).

Despite its popularity, PUE wasn't used in our scoring methodology, since PUE is always greater than the unit (ranged between 1 and 3+). Instead, we have chosen to use DCiE, because we prefer to have all incorporated metrics with values rated between 0-1 and with maximum value at maximum efficiency. The same applies for ERF metric, which is defined by equation (5) and is rated between zero and one. When all wasted energy is reused, ERF value is maximized to the unit.

5.5.1.3. Resources Recyclability is evaluated based on two influencing factors which are Waste Recycle Ratio and Water Reuse Ratio. These factors aim to motivate DC operators to minimize waste and increase recycling initiatives in DC facilities. They are presented in table 5.3:

Table 5.3: Data Center Resources Recyclability Factors

Sustainability Element	Influencing Factor	Factor Description
Resources Recyclability	Waste Recycle Rate	Waste recycled/Total waste produced
	Water Reuse Rate	Water conservation /Total Water Used

Waste Recycle Rate: Recycling is the process of converting waste materials into new products, preventing the waste of potentially useful materials. It can reduce energy usage, air pollution (from incineration) and water pollution (from landfilling). Recyclable materials include many kinds of glass, paper and cardboard, metal, plastic, tires, textiles, batteries and electronic equipment. The composting or other reuse of biodegradable waste (such as food or garden waste) is also considered recycling. Therefore, Waste Recycle Rate is defined as the ratio of Recyclable Materials sorted and collected within the DCs facility divided by Total Waste produced.

Water Reuse Rate: water conservation relies on any beneficial reduction in water loss, use and waste. Improving water management practices can reduce the use or enhance the beneficial use of water. One strategy in water conservation is rainwater harvesting, where collected and filtered rain water can be used for toilets, gardening, lawn irrigation and firefighting services. Reuse of graywater for flushing toilets or watering gardens and sustainable use of groundwater is also essential in water conservation. All these measures can be evaluated by the Water Reuse Rate, which is defined as the ratio of Water conservation and reuse efforts, divided by Total Water Used.

Both influencing factors are analogic ratios with value range between 0-1 and they are expressing resources and recyclability efforts.

5.5.1.4. Operational efficiency

Operational efficiency can be defined as the ratio between outputs gained from business and input of resources spent. It is a key aspect for all DC operations and business development, and it is achieved, when offering reliable and valuable services according to customer needs. The most important factor for evaluating DC efficient operation is the IT equipment performance. It can be evaluated with Energy efficiency metrics, which benchmark the energy consumption of data center as presented in subsection 5.5.1.

In addition to standard quantitative metrics, this sustainability element is enhanced by other qualitative and important influencing factors for operational efficiency such as: i) DC Security & Resilience Plans, ii) Effective maintenance, iii) Building Energy Management System and iv) Innovation initiatives. These factors can contribute to particular aspects of service provided (including quality, availability, responsibilities) as agreed between the service provider and the service user, according to Service-Level Agreement (SLA).

It is obvious that, since reliable services can lead to customer satisfaction and loyalty, the above listed factors contribute to Operational efficiency in a sustainable DC. Both qualitative and quantitative influencing factors for operational efficiency are presented in table 5.4:

Table 5.4: Data Center Operational Efficiency Factors

Sustainability Element	Influencing Factor	Factor Description
Operational Efficiency	IT Equipment Efficiency	Performance per Watt / CPE / Energy Star Score
	Security & Resilience	Risk Management, Security & Resilience Planning
	Effective Maintenance	Organizing Efficient Maintenance Plan
	BEMS	Building Energy Management System
	Innovation Research	Research & Development Initiatives

Since the first factor, which is IT equipment efficiency, was already presented in subsection 5.5.1, we will briefly introduce the other four influencing factors and the importance for driving DCs companies to include such options into their operating efficiency portfolio.

Security & Resilience: Data centers have a mission critical nature of their own and in addition they often serve mission critical applications. Therefore, any security compromise of either the cyber system or the physical environment of DCs can have profound consequences. This also makes them more likely targets for cyberattacks. In a

world, which is becoming increasingly dependent upon DCs to provide automated, efficient management of essential services, care has to be taken to ensure that they are effectively protected and secured.

Security management reduces the risk of DCs critical operations by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization and deciding what countermeasures to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. In addition, Business Continuity Plan (BCP) is critical to the transparent and continuous operation of data center businesses. Business continuity and resiliency plans create systems of prevention, recovery, and deal with potential threats to a company. Any event that could negatively impact operations is included in the plan, such as supply chain interruption, loss of or damage to DCs critical infrastructure (major machinery or computing /network resource). As such, BCP is a subset of risk management.

Effective Maintenance can achieve operational efficiency with better planning (spare parts, people, etc.), timely identifying and preventing problems, thus increasing plant availability and resilience. Data Centers are critical infrastructures, which are required to provide ceaselessly the desired services over an extended period of time with minimal maintenance intervals. Utilizing resources with efficiency and proactive approach can enable DCs operation to have a long operational lifetime.

Building Energy Management System (BEMS): is a sophisticated method to monitor and control the building's facilities and its energy needs, while efficiently controlling the whole installation. BEMS can control and monitor a large variety of DC functions and achieve considerable operational benefits.

Innovation Research and R&D management is creating and commercializing inventions, promoting excellence of technology and state of the art performance within the sector, so it is vital for DC operators to offer corporate resources and create incentives for promoting innovation.

While IT Equipment Efficiency is an analogic influencing factor with value range between 0-1, the rest four influencing factors are qualitative discrete values that means that DC either has developed or not such qualitive attributes to achieve operational efficiency.

5.5.1.5. Societal Impact

Societal Impact is the fifth element in the sustainability framework. Obviously, a sustainable business should have the support of its employees and stakeholders, along with public acceptance from surrounding community. The approaches able to secure and maintain this support may vary, however it includes employees' fairly treatment, being a good neighbor and community member, caring for the environment both locally and globally.

In our assessment, societal impact is evaluated with the following influencing factors: i) Corporate Social Responsibility, ii) Employee Satisfaction iii) Employee Health and Safety, iv) Green and public transport Initiatives, as presented in table 5.5:

Table 5.5: Data Center Societal Impact Factors

Sustainability Element	Influencing Factor	Factor Description
Societal Impact	Corporate Social Responsibility	Effective Plan & Commitment
	Employee Satisfaction Performance	Annually Survey Performed and Rating
	Occupational Health & Safety	Health and Safety Programme
	Sustainable Transport	Green Vehicles /Bicycles/ Public Transit Initiatives

Corporate Social Responsibility (CSR) is a form of corporate self-regulation integrated into business model, which goes beyond compliance and statutory requirements and engages actions that offer social good, including philanthropy and volunteering initiatives. This sense of responsibility towards the community and environment can be expressed through environmental protection actions, contributing to educational programs and society enforcing initiatives.

Employee Satisfaction Performance: Employee satisfaction is typically measured using an employee satisfaction survey. These surveys address topics such as compensation, workload, perceptions of management, flexibility, teamwork, resources, etc. It is an inside dialog, which provides important feedback for organizations who want to keep their employees happy and reduce turnover. Employee satisfaction is quite an important factor, especially in technological companies like DCs, who rely on highly qualified personnel for keeping high operational excellence standards.

Occupational safety and health (OSH) is a multidisciplinary field concerned with the safety, health and welfare of people at work. Occupational health aims at the promotion and maintenance of the highest degree of physical, mental, and social well-being of employees in all occupations. In a high technological environment such as a data center facility, health and safety is an important factor for corporate sustainability.

Sustainable transport promotes environmentally friendly policies beyond DC boundary. Green transportation initiatives, including fuel efficiency improvements and vehicle emissions controls, can migrate transportation from fossil-based energy to other alternatives for corporate sustainable transportation. The greenest and most sustainable forms of transportation are electric vehicles, trains, bicycles, and walking habits. Such initiatives for encouraging employees to daily use green transportation modes should be

awarded for promoting sustainability. Therefore, companies should be accountable for their green transportation initiatives.

All these societal influencing factors are discrete qualitive values, which either exist or not as societal policies adopted by DC management.

The overview of the proposed model for evaluating data center sustainability, with all influencing factors previously discussed, is graphically presented in figure 5.4.

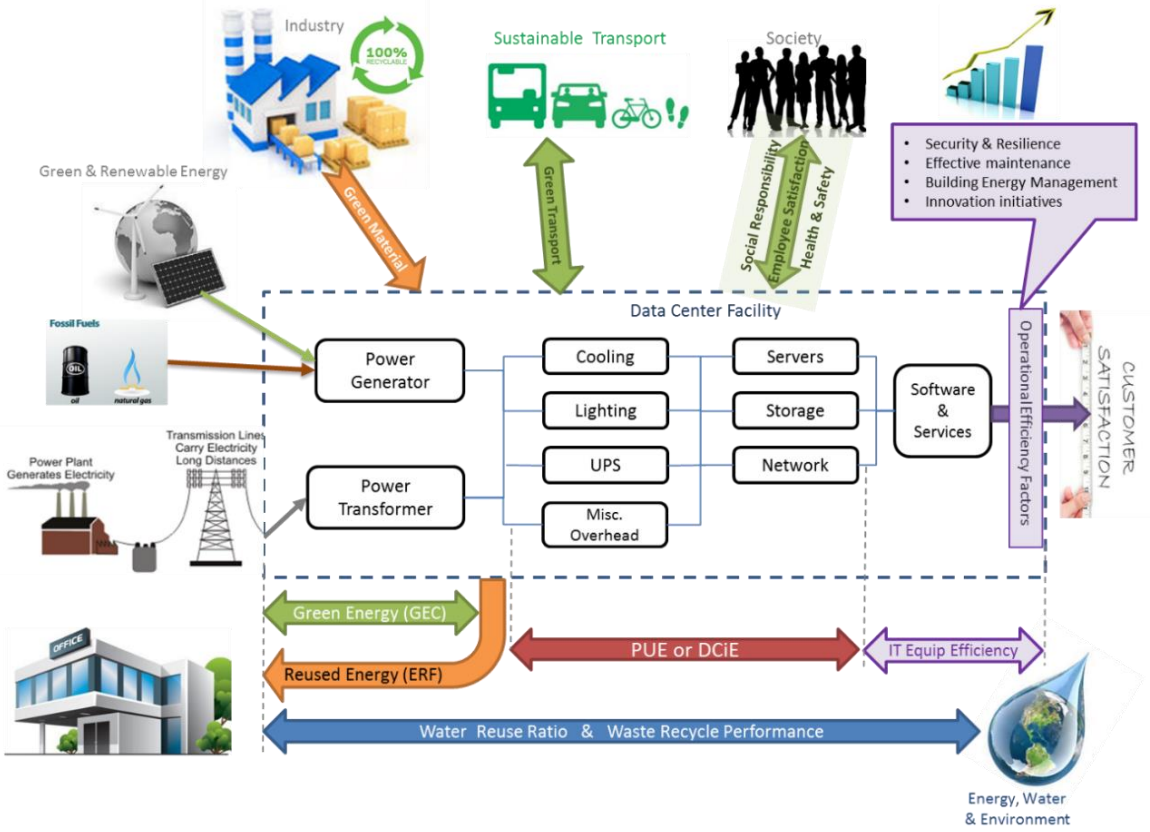


Figure 5.4: Data Center Sustainability Model Overview

5.5.2. Weighting of Influencing Factors

As presented in subsection 5.5, in our model we have used these fifteen Influencing Factors for the evaluation of sustainability, where seven of them are metrics with value range between 0-1. These are weighted for the 75 points out of a 100 points total score, and they are namely GEC, GMU, DCiE, ERF, Waste Recycle Rate, Water Reuse Rate and IT Equipment Efficiency.

The other eight factors are qualitative ones, weighted for the 25 points, which highlight operational efficiency and social responsibility with attributes that promote sustainability, equity, and solidarity. These are namely Corporate Social Responsibility, Security & Resilience, Effective Maintenance, Innovation & Research, Employee Satisfaction, Health and Safety, Greener Transport Initiatives. These factors are also important for any

company who wishes to gain customer confidence and loyalty, self-engaging in actions that combine social good with company's prosperity and resilience.

The summary of the sustainability elements presented in our methodology for assessing data centers sustainability, with each influencing factor characteristics and weighting is listed in Table 5.6. As we can notice from table 6, 75% of scoring value comes from environmental and energy efficiency metrics, which are quantifiable and represent main aspects of the environmental performance of DC facility. The other 25% of scoring value comes from qualitative attributes, that satisfy social and operational efficiency needs that compliment DCs sustainable development.

Table 5.6: Data Center Model Weighting Factors

a/a	Sustainability Element	Influencing Factor (Fi)	Range	MAX Rating (Wi)	%
1	Environmental Impact	GEC	0 ~ 1	15	75
2		GMU	0 ~ 1	10	
3	Resource Utilization & Economy	DCiE	0 ~ 1	15	
4		ERF	0 ~ 1	10	
5	Resources Recyclability	Waste Recycle Rate	0 ~ 1	5	
6		Water Reuse Rate	0 ~ 1	5	
7	Operational Efficiency	IT Equipment Efficiency	0 ~ 1	15	
8		Security & Resilience Plan	Y/N	4	25
9		BEMS	Y/N	4	
10		Effective Maintenance	Y/N	4	
11		Innovation Research	Y/N	3	
12	Societal Impact	Corporate Social Responsibility	Y/N	3	
13		Employee Satisfaction Index	Y/N	2	
14		Health and Safety	Y/N	3	
15		Green Transport	Y/N	2	
TOTAL SUSTAINABILITY SCORE				**100**	**100**

For evaluating the overall Sustainability score of a DCs, the weighted sum model, has been used in our assessment, which is the most widely used multi-criteria decision analysis method in literature. The overall score is given by the following equation:

$$\text{Total Sustainability Score} = \Sigma\{W_i * F_i\} \qquad (10)$$

where W_j denotes the relative weight of importance of the influencing factor F_i. For the maximization case, the most sustainable DCs is the one that yields the maximum total performance value. Based on the above sustainability scoring table we have tested and validated our proposed model, using already operating data centers and results are presented in next section.

5.6. Methodology Implementation and Scoring Results

We have tested and validated our methodology with various case-studies from DC located all over the world. In this subsection, we present the results from four existing hyper-scaled data centers, some of them being advertised for their energy efficiency performance. All data on energy efficiency metrics, construction details and corporate performance were collected from publicly available information. We have chosen four different locations around the world with the aim to compare the effects of various efficiency strategies applied and evaluate the performance scoring of our assessment. The four Data Centers were located in USA, UK, Finland and Turkey and a short description of their installation facilities is given below.

F Data Center located in Prineville, Oregon with 31 MW installed power, includes features such as rainwater reclamation, partial solar energy installation for providing electricity to the office areas and reuse of heat created by the servers to heat office space. Several new technologies are used in the design and operation of the data center and include energy efficient server design, specialized software to optimize server capacity and a low-energy evaporative cooling system to eliminate traditional air conditioners. Although it is one of the most energy efficient in the world with PUE metric rated at 1.07, green energy used is accounted only 10% of the total energy consumption, while the rest 90% is powered by fossil fuels and this has a negative impact to its sustainability performance.

G Data Center located in in Hamina, Finland with 22 MW installed power is one of the most advanced and efficient data center with high-tech chiller-free cooling system, which uses sea water from the Bay of Finland, drastically reducing energy use, with PUE at 1.12. In addition, having a collaboration with a Swedish wind-farm developer, G has managed to purchase green energy for the next 10 years, achieving very low carbon footprint for this facility.

H Data Center located in Wynyard, UK with 19 MW installed power has an eco-friendly design by using 100% renewable energy, built-in resiliency and a PUE rating of 1.2. Main energy saving features include an innovative airflow scheme for cooling, but no measures for water recycling have been reported and there is a medium waste recycle ratio.

The fourth Data Center examined is a virtual one, named V, located in Turkey with 10 MW. It is using convectional energy from utility grid and PUE performance is on industry's average rated at 2.0. There are no reported measures for water recycling, waste recycle ratio for the area is low and we have also assumed some drawbacks in social responsibility plans, green transport, and innovation initiatives.

In our analysis, we have presumed that all DCs are using IT equipment with the same efficiency performance rated at 94%, since IT Equipment Efficiency was not referred to any publicly available information. We adopt the same performance ratio in all data centers, as our purpose was to highlight how total score is affected by all the other parameters, beyond the IT equipment performance. Since energy consumption has a

critical role in the cost structure of any data center during its lifecycle performance, DCs manager of such an energy intensive facility always seek to reach maximum performance of IT equipment installed.

The data inputs for each Data Center examined and the output of our assessment scoring, with detail of characteristics taken into account are presented in table 5.8, where V.I is the Input Value entered in the model, according to DCs characteristics and S.O is the Scoring Output from each influencing factor. S.O value results by multiplying VI with MAX Rating Value which was presented in table 5.6. All Technical Characteristics of examined Data Centers are summarized in table 5.7:

Table 5.7: Technical Characteristics of examined Data Centers

DC Name	**F**	**G**	**H**	**V**
Location	**Oregon USA**	**Finland**	**UK**	**Turkey**
Max Power	**31 MW**	**22 MW**	**19 MW**	**10 MW**
Green Energy	10%	100%	100%	0%
Green Material	40%	70%	50%	20%
PUE	1,07	1,12	1,20	2,00
DCiE	0,93	0,89	0,83	0,50
Energy Reuse	60%	60%	25%	0%
Waste Recycle Rate	60%	70%	40%	20%
Water Reuse Rate	70%	90%	0%	0%
IT Equipment Efficiency	94%	94%	94%	94%
Security & Resilience Plan	YES	YES	YES	YES
BEMS	YES	YES	YES	YES
Maintenance	YES	YES	YES	YES
Innovation Research	YES	YES	YES	NO
Corp. Social Responsibility	YES	YES	YES	NO
Employee Satisfaction Index	YES	YES	YES	YES
Heath and Safety	YES	YES	YES	YES
Green Transport	NO	YES	NO	NO

So, from the outputs of this analysis we can notice that although F data center has the highest energy efficiency with PUE at 1.07, it does not get the highest sustainability score (69,1/100), since most energy used is sourced from grid utility with high carbon intensity and only 10% is reported as green energy use. Furthermore, green material purchasing polices are lower than competitors and no green transportation initiatives have been implemented.

On the other hand, H company, although it has lower PUE performance at 1.2, all energy used comes from renewable sources and that improves its sustainability performance, still it lacks in water conservation efforts and energy reuse rate, so final score is at 74,1/100.

Table 5.8: Scoring Results of examined Data Centers

DC Name		**F**		**G**		**H**		**V**	
DC Location		**Oreg. USA**		**Filand**		**UK**		**Turkey**	
a/a	**Influencing Factor**	**V.I**	**S.O**	**V.I**	**S.O**	**V.I**	**S.O**	**V.I**	**S.O**
1	GEC	0,10	1,5	1,00	15,0	1,00	15,0	0,00	0,0
2	GMU	0,40	4,0	0,70	7,0	0,50	5,0	0,20	2,0
3	DCiE	0,93	14,0	0,89	13,4	0,83	12,5	0,50	7,5
4	ERF	0,60	6,0	0,60	6,0	0,25	2,5	0,00	0,0
5	Waste Recycle Rate	0,60	3,0	0,70	3,5	0,40	2,0	0,20	1,0
6	Water Reuse Rate	0,70	3,5	0,90	4,5	0,00	0,0	0,00	0,0
7	CPE	0,94	14,1	0,94	14,1	0,94	14,1	0,94	14,1
8	Security & Resilience	1	4,0	1	4,0	1	4,0	1	4,0
9	BEMS	1	4,0	1	4,0	1	4,0	1	4,0
10	Maintenance	1	4,0	1	4,0	1	4,0	1	4,0
11	Innovation Research	1	3,0	1	3,0	1	3,0	0	0,0
12	Corp.Social Responsibility	1	3,0	1	3,0	1	3,0	0	0,0
13	Employee Satisfaction	1	2,0	1	2,0	1	2,0	1	2,0
14	Heath and Safety	1	3,0	1	3,0	1	3,0	1	3,0
15	Green Transport	0	0,0	1	2,0	0	0,0	0	0,0
Total Score		**69,1**		**88,5**		**74,1**		**41,6**	

Best performance is achieved by G Data center with total score 88,5/100, which uses 100% green energy and implements more environmental conscious policies on water conservation, waste recycling and green material purchases than its competitors, as presented in tables 5.7 & 5.8. Also, G has location competitive advantage, since Finland's climate is favorable cold and country promotes green and environmental policies.

Worst performance occurs for V data center with 41,6/100 score, since the company uses energy from utility grid with high carbon intensity, does not reuse energy exploiting heat recovery options, lacks on water conservation and waste recycling policies. In addition, on the qualitative metrics evaluation, company hasn't announced any corporate social responsibility programs, or innovation research efforts and there are no green transport initiatives. That is why its sustainability performance is below average, although PUE energy efficiency is rated on industry's average performance.

From the results presented we can notice that although some hyper-scaled data centers have achieved high-energy efficiency performance (using mainly PUE metric as an indicator), on accounting their sustainability scoring results, significant deviations exist, leaving plenty of room for improvements and further minimization of environmental impact and sustainability performance.

5.7. Summary of Research Work

As one of the fastest growing sectors, both economically and in energy consumption, Data Centers have a tremendous opportunity and unique responsibility to take greater control of their operational efficiency, energy consumption and environmental footprint management.

Data center sustainability assessment can be a function of multiple variants, where each one carries a corresponding, weight depending on the severity or the priority proposed by stakeholders and regulators. Since, no metric alone can provide a holistic approach about the environmental footprint of a data center, the sustainability evaluation should include a variety of factors both quantitative and qualitative, as proposed in this work.

After careful examination of available DCs efficiency metrics and best practices proposed for energy efficiency improvements, we have introduced a holistic sustainability evaluation model that can be applied on data centers, using a scoring system, and taking into account all necessary components for evaluating how green, how efficient and how social friendly such a facility can be.

Our proposed model intends to enrich and update the existing sustainability assessments based on the new requirements and performance metrics introduced. We have analyzed environmental footprint based on green energy consumed and green material used, waste and water recyclability. Since data centers have become very critical infrastructures, operational efficiency measures that increase performance, security and resilience could not be excluded from this model. Last but not least, societal impact is also incorporated, through corporate social responsibility factors.

After having implemented the above evaluation model to several data centers around the world, we have concluded that even if certain, undisputedly important metrics, show impressive results, however the overall sustainability score may not be so satisfactory.

Given the energy-intensive nature of data centers, the decision about where to build the installation is of critical importance, since access to significant amounts of electricity and network stability is a key factor for data center operation. By making better energy choices towards energy efficiency and green energy supply, data center companies have the opportunity to become a catalyst in driving utilities and governments toward the development of cleaner electricity generation that will ensure long-term sustainability.

Chapter 6: Conclusions

6.1 Summary and discussion

Critical Infrastructures are highly interconnected, whether they manifest as processes, systems, facilities, assets, or services. The modeling and analysis of CI interdependencies are relatively new research fields with increasing interest. The effective implementation of the CI protection plans depends on the degree to which CI operators, government and private sector partners engage in systematic risk assessment, effective risk management, and multi-directional information sharing. In this thesis we have identified, classified, and compared various tools and methods that have been developed to analyze CIs and support CI risk management. Emphasis has been given on the comparison of similar tools from the perspective of their purpose and modeling approach.

Adequate security of information in Industrial Control Systems (ICS) that support Critical Infrastructures (CIs) is a fundamental for their efficient operations. ICS operators should be constantly aware of the status of their information security controls, to make informed judgments and appropriately mitigate risks to an acceptable level. Self-assessment tools provide a tailored assessment for assessing cyber vulnerabilities of ICS. Based on a selectable set of cybersecurity standards, these tools provide structured questionnaires to build organizational knowledge and create a cybersecurity compliance report with compiled statistics and security recommendations. Since self-assessment tools do not generate a complex risk assessment, they cannot provide a detailed architectural analysis of the network or detailed hardware/software configuration review. Therefore, periodic onsite reviews and inspections should also be conducted, using a holistic approach including facility inspection, interviews, examination of facility practices, and penetration testing.

Researching the field of physical threats against CIs, we explored how projected climate change, such as increases in temperature, sea level rise and extreme weather events, have come to challenge CIs operation. The transport sector belongs to CIs, as it is an important pillar of our economy and society. Transportation systems are quite complex, their majority of infrastructures are greatly exposed to weather impacts, while they are characterized by the long lifespan and high building costs for their substructures. These characteristics suggest the need for CI managers to adopt an adaptation approach with a long-term and systemic perspective. Several states worldwide have started to implement Adaptation Strategies and Action Plans with a variety of adaptation measures in all critical sectors, including transportation. These measures include the provision of information, capacity building, review of technical standards and use of new ICT opportunities.

Adaptation tools, already proposed by academic community, have been surveyed and classified based on their typology and target audience, activity sectors, climate impacts, and adaptation planning steps. Moreover, the software tools were classified according to their functionality and mode of use. Most tools were developed to deal with all climate

change impacts and have an ‘all-sectors’ approach, in order to provide a holistic support for stakeholders to adaptation planning process. However, especially for the transport sector, the engagement of all stakeholders is of key importance for ensuring adequate resilience, thus regulating authorities should make an extra effort to engage them all. It is important that adaptation measures taken in the transport sector are properly monitored and analyzed, so as to improve their efficiency and robustness of future design and resilience policies for climate adaptation.

Aviation sector remains the safest transport mode in the world and probably also the most interconnected transport system in terms of information and communication technology. Cyber-threats are increasing in quantity and persistence, so the consequences of a successful malicious cyber-attack on civil aviation operations could be severe nowadays. New technologies introduced, the extension of connectivity in the aviation industry, especially in the field of Air Traffic Management (ATM), may increase the risk to the aviation sector & its critical assets.

Focusing our research in the Aviation sector, we have explored how technological advances and IoT technologies may change the security threat models in aviation and influence the operational efficiency of smart airports, through an online survey questionnaire. The study focused on cyber-attacks that may occur from malicious actions as the incorporation of smart applications introduces new vulnerabilities in airports. There is a large variation in the way airports implement cyber-physical measures to protect networked infrastructures. Our survey revealed the disparity amongst airports regarding to the methods and the degree of applying cyber security best practices. While smart airports have a mature cyber security posture, basic level airports seem to have limited resources dedicated to cyber-defense and cyber-resilience. Technical based cybersecurity practices have a better implementation rate for all airport categories, while organizational practices, policies and standards keep lower levels of implementation, including low levels of cyber security awareness and training prioritization.

By presenting and analyzing various attack scenarios, based on malicious intentions of unruly actors, airport community and aviation stakeholders can better understand the importance of acting proactively and implementing best cybersecurity practices. There is a need for identification and development of airport trust framework, supporting operators explore their trust relationships and indicate how smart devices and operators can exchange data and enhance interoperability. Another important finding of our research was the growing need for educating IT experts and providing specialized advanced training in cybersecurity areas, to increase cybersecurity preparedness. Moreover, it is essential to promote security awareness for passengers and IT personnel on the risks posed by new IoT technologies.

Securing Smart airports, against evolving cyber threats, is a shared responsibility for all aviation stakeholders, including commercial airports, airlines, business associates and regulators. As a result, a collaborative cyber-resilience model, which defines the appropriate cyber security posture for airports, is quite important nowadays. Airport

operators ought to prioritize cyber security initiatives, to ensure safety of operations for airlines, passengers, and public in general.

Cyber threats and related risks will continue to grow, along with technological developments, while the relationship between safety and security in the aviation context will become more interdependent.

In the area of Air Traffic Management, the increase of capacity and efficiency has led to an enormous effort of transition towards digitalization and automation. As a result, formerly separated IT systems get connected via newly established networks for information and data exchange. Due to a growth of complexity the attack surface of the overall aviation system has increased, thus previously unknown interdependencies have been created. Limiting security risk management to "traditional" physical aspects like air terrorism is no longer sufficient to ensure a stable and robust operation of the air transportation system. The component of cyber-security should be expanded from traditional risk mitigation approaches to more resilient focused approaches. As both safety and security are drivers for the determination of resilience requirements, it is vital to take an integrated view on both subjects to foster the consistency of resilience concepts in aviation.

Drone-related incidents at critical infrastructures, including airport facilities, are expected to rapidly proliferate in frequency, complexity and severity, as drones become larger and more powerful. The use of drones can appeal to nefarious actors and provide means to attack a target with low risks for perpetrators. Critical Infrastructures need to be protected from such aerial attacks, through effective vulnerability assessment, risk management and resilience actions. Although airport environments are quite complicated with a variety of sizes and design features, they have similar security requirements for protecting their facilities, detecting, and identifying misused drones, as well as taking effective counter measures. Based on extensive literature survey on C-UAS technologies, we have developed three categories of attack scenarios in airport premises and proposed an efficient C-UAS protection plan for each case. Geofencing as preventing measure and a variety of detection sensors can be implemented in different ways, depending on risk appetite, either as a distributed system on the airport perimeter, or as a single point detection capability. Multiple radars with different detection ranges and applied technologies provide the necessary primary surveillance method in airports. Since it is important to identify the type and payload of invading drone, we proposed a combination of radio frequency sensors with visual detection sensors (electro-optical and infrared cameras), which provide supplementary surveillance around airport's extended perimeter. However, defending airports against unwanted drone activity is a wide and deep problem set. Despite the variety of technological mitigation solutions available, airfield operators must remain within the law, when using disruptive technologies, and the risks on the wider community should be fully assessed and understood. A clear decision-making process should be in place, to allow the airport operator to make the most appropriate decision, based on solid and accurate information.

Concerning the whole aviation network and its interdependencies, we proposed a risk-based dependency model to analyze congestions in the aviation network. The methodology and the developed tool can assess the risk of delay incidents in airports and produce weighted risk dependency graphs, presenting how an incident causing a delay in one airport may affect other interconnected airports. By using real data collected from US Bureau of Transportation Statistics, we have analyzed how flight delay risk propagates into the aviation network and provided a prediction for congested connections and higher dependency risk chains. We were able to detect the worst airports, in terms of affecting the aggregated delay of an aircraft route, along with airports that perform better and mitigate delay propagation in the aviation network. The tool, we have developed for congestion analysis, can be used to identify key airports inclined to delays with great influence on the network due to: (i) the number of connections; (ii) the likelihood of congestions; and (iii) the airports that get affected the most by delays occurred in previous airports.

Finally, in the last section of our research, we have presented a new methodology, for assessing sustainability based on five major quantifiable elements, composed by different influencing factors, with the aim to provide a holistic approach. By introducing a new sustainability scoring model, we have evaluated in a spherical way the environmental impact and operational efficiency of CIs and its data centers. As one of the fastest growing sectors, both economically and in energy consumption, IT facilities and data centers have a tremendous opportunity and unique responsibility to take greater control of their operational efficiency, energy consumption and environmental footprint management.

6.2 Publications

Our contribution is published in peer-reviewed journals, conferences, and book chapters, namely:

A) Publications in peer-reviewed, academic journals:

J1. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., **Lykou G.,** Gritzalis D., "*Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures*", International Journal of Critical Infrastructure Protection, March 2016.

J2. Stergiopoulos G., Gritzalis D., Kotzanikolaou P., Magkos M., **Lykou G.,** "*Holistic Protection of Critical Infrastructures*", Maritime Interdiction Operations Journal, Vol. 14, No. 1, pp. 29-41, September 2017.

J3. **Lykou G.,** Mentzeloti D., Gritzalis D., "*A new Methodology towards effectively assessing Data-Center sustainability*", Computers & Security, Elsevier, January 2018.

J4. **Lykou G.**, Anagnostopoulou A., Gritzalis D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", SENSORS, January 2019.

J5. **Lykou, G.,** Moustakas, D., Gritzalis, D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies", Sensors, Vol. 20, No. 12, 2020.

J6. **Lykou G.,** Dedousis P., Stergiopoulos G., Gritzalis D., "Assessing Interdependencies and Congestion Delays in the Aviation Network", IEEE Access, December 2020

B) Publications in peer-reviewed, international conferences:

C1. Stergiopoulos G., Vasilellis E., **Lykou** G., Kotzanikolaou P., Gritzalis D., "*Critical Infrastructure Protection tools: Classification and comparison*", in Proc. of the 10th International Conference on Critical Infrastructure Protection (CIP-2016), USA, March 2016

C2. Faily S., **Lykou** G., Partridge A., Gritzalis D., Mylonas A., Katos V., "*Human-Centered Specification Exemplars for Critical Infrastructure Environments*", in Proc. of the 30th British Human Computer Interaction Conference (HCI-2016), July 2016

C3. Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magkos E., **Lykou** G., "*Critical Infrastructure Protection: A Holistic Methodology for Greece*", in Proc. of the Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (in conjunction with ESORICS-2016), Springer, Greece, September 2016

C4. **Lykou** G., Stergiopoulos G., Papachrysanthou A., Gritzalis D., "*Climate adaption: Addressing risks and impacts of climate change on Transport Sector*", 11th International Conference on Critical Infrastructure Protection (CIP-2017), USA, March 2017

C5. **Lykou G**., Iakovakis G., Chronis G., Gritzalis D., "*Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning*", in Proc. of the 12th International Conference on Critical Information Infrastructures Security (CRITIS-2017), Italy, September 2017

C6. **Lykou G**., Anagnostopoulou A., Gritzalis D., "*Implementing cyber-security measures in airports to improve cyber-resilience*", in Proc. of the Workshop on Industrial Internet of Things Security (WIIoTS-2018), Spain, June 2018

C7. **Lykou G.**, Anagnostopoulou A., Stergiopoulos G., Gritzalis D., "*CYBERSECURITY SELF-ASSESSMENT TOOLS: Evaluating Importance for Securing Industrial Control Systems in Critical Infrastructures*", in Proc. of the 13th Intern. Confer on Critical Information Infrastructures Security, CRITIS-2018, Kaunas, September 2018.

C) Publications in peer-reviewed book chapters:

Lykou G., Iakovakis G., Gritzalis D., "*Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management*", in Critical Infrastructure Security and Resilience, Gritzalis D. et al. (Eds.), pp. 245-260, Springer (Advanced Sciences and Technologies for Security Applications), 2019.

6.3 Future Work

The research presented in this dissertation can be set as a basis for further investigation on the scientific area of Aviation Sector and its Critical Infrastructures Protection. The research results demonstrate that there is a long way ahead for further research contribution in the field of risk assessment and risk management of aviation assets, in order to enhance their cyber-protection and cyber-resilience.

We plan to further survey cyber resilience aspects in the aviation context and the need for holistic strategy of defense, prevention, and response, so as to contribute how all aviation actors should work on a collaborative and risk-based framework, in order to address security threats and further increase the aviation systems resilience against future attacks.

Moreover, as the fastest growing segment of aviation, unmanned aerial systems (UAS) continue to increase in technical complexity and capabilities, so our research will focus on the development of new counter drone technologies and methodologies which could prevent, detect, identify, and mitigate malicious drones.

Future work will focus on the incorporation of machine learning and data mining techniques, in order to produce a data model that will allow a comprehensive understanding of cyber-attacks and its classification in airside and landside areas within airport facilities, enabling aviation stakeholders to effectively respond to increasing cyber-physical threats, which pose significant challenges in terms of safety, security, and privacy.

Regarding physical threats, climate change is an unavoidable challenge that aviation sector will have to face in the near future. It is important that resilience and adaptation measures taken in the aviation sector should be further developed and analyzed, so as to improve their efficiency and robustness of future design. We plan to further develop and analyze resilience policies for climate adaptation and environmentally friendly development of new and existing aviation critical infrastructures, which are key success factors for the sustainable development of transportation sector and planet's longevity.

Appendices

Appendix A

As presented in Chapter 2, sixty-eight (68) CIP tools and methodologies have been examined. In the table below full description of the examined tools is presented.

Summary Table of 68 CIP Tools and Methodologies

TOOL	DEVELOPER	ORIGIN	DESCRIPTION	SECTOR	WEB LINK
ActivitySim	Los Alamos National Laboratories (LANL)	USA	Activity representation of the US population	CF	http://public.lanl.gov/sunil/pubs/simx.pdf
AIMS (Agent-based Infrastructure Modelling and Simulation)	University of New Brunswick (UNB)	CAN	Interdependency modeling and survivability of Canada's critical infrastructures	E, C, WWS, IT	http://ebagheri.athabascau.ca/papers/ijbpim.pdf
AIMSUN (Advanced Interactive Microscopic Simulator for Urban and Non-Urban Networks)	TSS-Transport Simulation Systems	ESP	Traffic modeling	TS	https://www.aimsun.com/
AMTI : Advanced Modeling & Techniques Investigation (Loki Toolkit)	Sandia National Laboratories	USA	Quick formulation and application of network models of complex systems	E, TS, FS	http://www.sandia.gov/casosengineering/amti.html
AT/FP (Anti-Terrorism / Force Protection)	Naval Postgraduate School	USA	Planning waterside security for ships in a port	DIB, ES, HPH, TS	https://savage.nps.edu/RobotTelemetry/DonCioXmlWgNpsSlides/NPSATFPProjectFlyer.2007Apr19.pdf
Athena	On Target Technologies, Inc.	USA	Interdependency modeling and analysis	C, CF, CM, DIB, E, FS, IT, NRMW, WWS, TS	https://inldigitallibrary.inl.gov/sti/3489532.pdf
ATOM (Air Transportation Optimization Model)	Sandia National Laboratories / Los Alamos National Laboratories	USA	Consequence assessment of a partial or complete outage at a major airport or set of airports for an extended period of time	TS	http://www.sandia.gov/nisac/capabilities/network-optimization-models/
BIRR (Better Infrastructure Risk and Resilience)	U.S. Department of Homeland Security	USA	Vulnerabilities assessment and risk reporting	All sectors	http://www.dis.anl.gov/projects/ri.html
CAPRA Comprehensive Approach for Probabilistic Risk Assessment	CEPREDENAC sponsored by WORLD BANK & UN	LATIN AMERICA	RVA tool for assessing, understanding and communicating disaster risk	WWS, HPH, TS, FS	www.ecapra.org/
CARVER 2 (Criticality Accessibility Recoverability Vulnerability Espyability Redundancy)	National Infrastructure Institute Center for Infrastructure Expertise	USA	Threat and potential terrorist targets prioritization	HPH	http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

CASCADE	DNV GL (Det Norske Veritas)	Norway	Analyzation of catastrophic disruptions of large, interconnected infrastructure systems due to cascading failures	All sectors	
CI³ (Critical Infrastructure Interdependencies Integrator)	Argonne National Laboratories (ANL)	USA	Emulation of time and cost needed for restoration purposes	C, CM, E, NRMW, WWS	http://www.ipd.anl.gov/anlpubs/2002/03/42598.pdf
CIDA (Critical Infrastructure Dependency Analysis tool)	Infosec Lab, Athens University of Econ. And Business	EU	Dynamic assessment of the evolution of cascading failures over time. Interdependency analysis and risk mitigation.	All sectors	https://github.com/geostergiop/CIDA/wiki/
CIMS (Critical Infrastructure Modeling System)	Idaho National Laboratories	USA	Visualization of cascading consequences of infrastructure perturbations	C, CF, E, TS, HPH	https://inldigitallibrary.inl.gov/sti/3578215.pdf
CIMSuite: Critical Infrastructure Modeling	Idaho National Laboratories	USA	Preparation for man-made and natural disasters	All sectors	http://www4vip.inl.gov/factsheets/docs/cimsuite.pdf
CIP/DSS (Critical Infrastructure Protection Decision Support System)	LANL, SNL, Argonne National Laboratories	USA	Dynamic simulation of individual infrastructures	All sectors	http://www.systemdynamics.org/conferences/2005/proceed/papers/LECLA332.pdf
CIPDSS-DM (Critical Infrastructure Protection Decision Support System Decision Model)	LANL, SNL, Argonne National Laboratories	USA	Decision making proposal under conditions of uncertainty and risk	All sectors	http://www.ipd.anl.gov/anlpubs/2008/12/63060.pdf
CIPMA (Critical Infrastructure Protection Modeling and Analysis)	Government of Australia	Australia	Critical infrastructure resilience enhancement	C, E, IT, TS, FS	http://www.polymtl.ca/crp/doc/GREGSCOTT-CIPMABriefingforCanada.pdf
CISIA (Critical infrastructure simulation by interdependent agents)	University of New Brunswick (Canada)	CAN	Interdependency and system analysis	C, CM, E, WWS, C	http://www.chiarafoglietta.com/wp-content/uploads/2015/04/Cisia.pdf
CommAspen (Agent-based simulation model of the U.S. economy)	Sandia National Laboratories (SNL)	USA	Simulation of interdependent effects of market decisions and disruptions in the telecommunications infrastructures	FS, C, E	http://www.inf.uniroma3.it/autom/LabRob/Projects/CISIA/home.html
Counteract (Generic Guidelines for Conducting Risk Assessment in Public Transport Networks)	UITP, International Association for Public Transport	EU	Risk reporting	TS, E, HPH	http://www.transport-research.info/sites/default/files/project/documents/20120719_145438_7577_COUNTERACT_Guidelines_lr.pdf
DECRIS (Risk and Decision Systems for Critical Infrastructures)	SAMRISK research programme	Norway	All-hazard generic RVA methodology suitable for cross-sector infrastructure analysis	E, WWS, TS, C, IT	https://www.sintef.no/projectweb/samrisk/decris/
DemandSim	Los Alamos National Laboratories (LANL)	USA	Geographically demand computation on each of the CI sectors	All sectors	http://www.lanl.gov/

EMCAS (Electricity market complex adaptive system)	Argonne National Laboratories (ANL). Sponsored by ADICA Consulting	USA	Simulation of complex power systems for operational and economic impact consequence calculation	E	http://www.energyplan.eu/othertools/national/emcas/
EpiSimS	Los Alamos National Laboratories (LANL)	USA	Analyzation of disease spread within the United States	HPH	http://public.lanl.gov/sdelvall/p556-mniszewski.pdf
EPRAM (Electric Restoration Analysis: Tools)	NISAC	USA	Impact determination of network-level damage on electric power restoration	E	http://www.mssanz.org.au/modsim2013/D2/stamber.pdf
EURACOM (European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks)	Directorate-General for Enterprise and Industry (DG ENTR) - Seventh Framework Programme (FP7)	EU	Contingency planning	All sectors	http://cordis.europa.eu/result/rcn/53099_en.html
FAIT (Fast analysis Infrastructure Tool)	Sandia National Laboratories (SNL). Sponsored by U.S. Department of Homeland Security	USA	Economic analysis tool for conducting economic impact assessment across multiple sectors	E, ES, FS, TS, WWS	http://www.sandia.gov/casosengineering/docs/Stochastic%20Mapping%20of%20Food%20Distribution%202011%20NGI%20conference.pdf
FastTrans	Los Alamos National Laboratories (LANL)	USA	Route simulation of vehicles on real-world road networks	TS	http://www.lanl.gov/programs/nisac/fasttrans.shtml
FEPVA (Framework for Electricity Production Vulnerability Assessment)	Los Alamos National Laboratories (LANL)	USA	Impact assessment of natural disasters or malicious attacks for both response and preventative purposes	E	http://www.lanl.gov/
FINSIM (Financial System Infrastructure)	Los Alamos National Laboratories (LANL)	USA	Modeling of cash and barter transactions that are dependent on contractual relationships and a network at the federal reserve level	FS, E, C	http://cnls.lanl.gov/annual26/abstracts.html
Fort Future	US Army Corps of Engineers (US.A.C.E.)	USA	Simulation for testing plans for Department of Defense (DoD) installations	C, CF, CM, E, ES, FS, HPH, IT, NRMW, TS, WWS	http://www.usace.army.mil/
HCSim (Healthcare Simulation)	Los Alamos National Laboratories (LANL)	USA	Impact assessment of mass-casualty incidents on hospital capacity	D, HPH, NRMW	http://www.osti.gov/scitech/biblio/1084564
HURT (Hurricane Relocation Tool)	Los Alamos National Laboratories (LANL)	USA	Hurricane relocation	HPH	http://www.lanl.gov/
HYDRA Population and Economic Modeling	Los Alamos National Laboratories (LANL)	USA	Development of a service-oriented architecture for integrated Web-based access of LANL agent-modeling capabilities	HPH, FS	http://www.bwbush.io/projects/hydra.html

I2SIM (Infrastructures Interdependencies Simulation)	University of British Columbia, UBC Faculty of Electrical and Computer Engineering	CAN	Simulation of a disaster response scenario at the system level, showing the impacts of the events that occur	CF, TS, CM, HPH	http://www.ece.ubc.ca/~jiirp/
IEISS (Interdependent Environment for Infrastructure System Simulations)	LANL, University of Virginia (USA)	USA	Electric power flow model that simulates service and outrage areas, outrage duration, and critical system components	E, TS, WWS	https://inldigitallibrary.inl.gov/sti/3489532.pdf
IIM (Inoperability Input–Output Model)	UV, Sandia National Laboratories and Los Alamos National Laboratories	USA	Analyzation of economic impacts	FS, E, C, IT, TS, FS	https://inldigitallibrary.inl.gov/sti/3489532.pdf
IntePoint VU	Intepoint LLC	USA	Analyzation of complex environments and modeling system-wide interdependencies across physical, virtual and social networks	C, E, CF, TS	http://intepoint.com/products/index.html
IRRIIS (Integrated risk reduction of information-based Infrastructure Systems)	FP6-IST - Information Society Technologies	EU	Interdependency analysis and management of critical infrastructures	All sectors	http://www.irriis.org/
Knowledge Management &Visualization	Carnegie Mellon University (CMU)	USA	Analyzation of vulnerabilities associated with delivery of fuel	E, TS, WWS	https://inldigitallibrary.inl.gov/sti/3489532.pdf
LogiSims	Los Alamos National Laboratories (LANL)	USA	Planning preparation for a disaster and real-time response to a disaster	HPH, E	http://public.lanl.gov/rbent/bent-pes.pdf
LS-DYNA	Livermore Software Technology Corporation (LSTC)	USA	Behavior analysation of structures as they deform and fail	CM, D, TS	http://www.lstc.com/products/ls-dyna
MBRA (Model-Based Risk Assessment)	Naval Post Graduate School Center for Homeland Defense and Security	USA	Resilience analyzation of the crude oil pipeline network	FS, TS, E	https://www.chds.us/ed/items/2164
MIITS (Multi-Scale Integrated Information and Telecommunications System)	Los Alamos National Laboratories (LANL)	USA	Realistic simulation of internet packet traffic on a national or global level	C, IT	http://www.lanl.gov/programs/nisac/miits.shtml
MIN (Multi-layer Infrastructure Networks)	Purdue	USA	A Simulation tool of automobile, urban freight, and data network layer	CF, TS	https://inldigitallibrary.inl.gov/sti/3489532.pdf
MSM (MIT Screening Methodology)	Massachusetts Institute of Technology (MIT)	USA	Prioritization of vulnerabilities	E, WWS, HPH	
MUNICIPAL (Multi-Network Interdependent Critical Infrastructure	Rensselaer Polytechnic Institute (RPI)	USA	Interdependency analyzation of civil infrastructure systems	E, C, IT, TS	http://eaton.math.rpi.edu/faculty/Mitchell/papers/decisiontechnologies.pdf

Program for Analysis of Lifelines)					
N-ABLE (National agent-based laboratory for economics)	Sandia National Laboratories (SNL) and Los Alamos National Laboratories (LANL)	USA	Analyzation of economic factors, feedbacks and downstream effects of infrastructure interdependencies	E, FS, TS	http://www.sandia.gov/nisac/capabilities/nisac-agent-based-laboratory-for-economics-n-able/
NEMO (Net-Centric Effects-based operations Model)	Sparta, Inc	USA	Modeling of cascading effects of events across multiple infrastructure networks	C, E, WWS, TS, DIB	http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf
Network-Centric GIS	York University	USA	Decision making proposal using GIS (geographical information system) interoperability	TS, WWS, ES	https://inldigitallibrary.inl.gov/sti/3489532.pdf
Nexus Fusion Framework	IntePoint, LLC	USA	Visualization of intended and unintended effects and consequences of an event across multiple infrastructure models	E, C, TS, DIB	https://inldigitallibrary.inl.gov/sti/3489532.pdf
NG Analysis Tools (Natural Gas)	Argonne National Laboratories (ANL)	USA	Modeling of the natural gas pipeline infrastructure	E	https://inldigitallibrary.inl.gov/sti/3489532.pdf
NSRAM (Network security risk assessment model)	James Madison University (JMU)	USA	Analyzation of large interconnected multi-infrastructure networks to determine how the systems respond and interact to various kinds of accidents and attacks	E, IT, C	http://www.jmu.edu/iiia/wm_library/NSRAM_Application_to_Municipal_Electric.pdf
PC Tides	Neptune Navigation Software	UK	Wind speed and flood surge analysis	HPH, ES	http://www.neptunenavigation.co.uk/tides.htm
PFNAM (Petroleum Fuels Network Analysis Model)	Argonne National Laboratories (ANL)	USA	Hydraulic calculations of pipeline transport of crude oil and petroleum products	E, TS	http://www.gss.anl.gov/publications-2/
PipelineNet	EPA	USA	Hydraulic and water quality models integration using existing databases for providing emergency managers real time information and for estimating the risks to public water supplies	WWS, HPH	http://files.waterky.org/aamastrrefs/Bahadur%20et%20al.%202003.%20PipelineNe.%20a%20model%20for%20monitor%20introd%20contam%20in%20a%20dist%20syst.%20World%20Water%20Congr.%202003..pdf
QualNet	Scalable Network Technologies, Inc	USA	Telecommunication analysis	C	http://web.scalable-networks.com/
Restore	Argonne National Laboratories (ANL)	USA	Estimation of time and cost needed to achieve an intermediate stage of completion, as well as overall completion of a goal	CM, E	http://www.anl.gov/egs/group/resilient-infrastructure/resilient-infrastructure-capabilities

R-NAS (Railroad Network Analysis System)	Sandia National Laboratories (SNL). Los Alamos National Laboratories (LANL)	USA	Studying and understanding the flow of commodities over the U.S nation's rail infrastructure	FA, TS	http://www.sandia.gov/nisac/capabilities/network-optimization-models
RTDS (Real Time Digital Simulator)	RTDS Technologies	CAN	Testing the dynamic behavior of the power systems in real time	E	https://www.rtds.com/
SessionSim	Los Alamos National Laboratories (LANL)	USA	Generation of data traffic between communication of individuals	C	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5429274&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5429274
SIERRA (System for Import/Export Routing and Recovery Analysis)	Sandia National Laboratories (SNL). Los Alamos National Laboratories (LANL)	USA	Flow diversions estimations between U.S. ports	TS	http://www.sandia.gov/nisac/tag/system-for-importexport-routing-and-recovery-analysis/
TEVA (Threat Ensemble Vulnerability Assessment)	EPA	USA	Vulnerability assessment of a water utility to a large range of contamination attacks	HPH , WWS	http://ascelibrary.org/doi/abs/10.1061/40737%282004%29482
TRAGIS (Transportation Routing Analysis Geographic Information System)	Oak Ridge National Laboratories	USA	Calculation of highway, rail, or waterway routes within USA	TS, WWS	http://web.ornl.gov/sci/gist/TRAGIS_2005.pdf
TRANSIMS (Transportation Analysis Simulation System)	Los Alamos National Laboratories (LANL)	USA	Evaluation of transportation consequences of urban evolution scenarios. Simulation of every vehicle movement through a large metropolitan area	TS, CF	https://code.google.com/p/transims/
UPMoST (Urban Population Mobility Simulation Technologies)	NISAC	USA	Provides the common interface for the flow of information between multiple UIS domain-specific models	CF	https://scs.org/magazines/2012-01/index_file/Files/MoonAndLee.pdf
VISAC (Visual Interactive Site Analysis Code)	Oak Ridge National Laboratory is managed by UT-Battelle for the Department of Energy	USA	Prediction and analyzation of outcomes of different accidents/incidents at various nuclear and industrial facilities	CH, NRMW	http://computing.ornl.gov/cse_home/about/VISAC_FactSheet.pdf
WISE (Water Infrastructure Simulation Environment)	Los Alamos National Laboratories (LANL)	USA	Evaluation of water infrastructure in terms of both infrastructure specific and interdependency issues	CS, TS, WWS, HPH	http://cedb.asce.org/cgi/WWWdisplay.cgi?146772

Appendix B

This appendix presents the questionnaire addressed to Cyber Security in Smart Airports, which has been sent to the busiest 200 commercial European and American airports. This survey was addressed to both Smart airports or not. Its main purpose was to understand the opinion of Airport IT personnel about the introduction of the IoT technology to Airports and whether they have the appropriate security awareness. This online survey took place in 1st semester of 2017 and invitation was sent through email to IT personnel.

Also, it is worth mentioning that all survey responses that we received are strictly confidential and data from this research are reported only in the aggregate. Although, in this online survey we have counted 280 visits to our online questionnaire, we have finally received only 34 fully completed answers and we elaborated these results.

Online Survey Questionnaire

The questionnaire was available in the following link:
https://survey.zohopublic.eu/zs/uiCChZ.

The questions were the following:

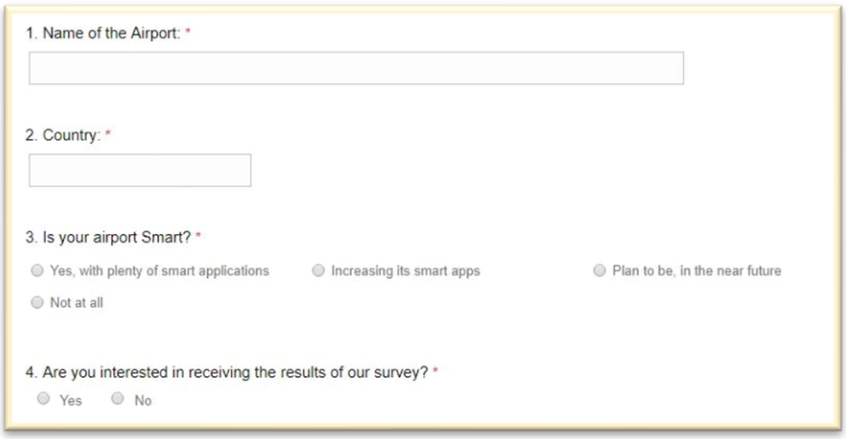


Figure B1. Questions about the airport's details.

In case that the responder answers yes in question No 4, then he should fill some contact details. Otherwise, the responder will continue answering the rest questions, starting with the Question No 8 (Figure A3).

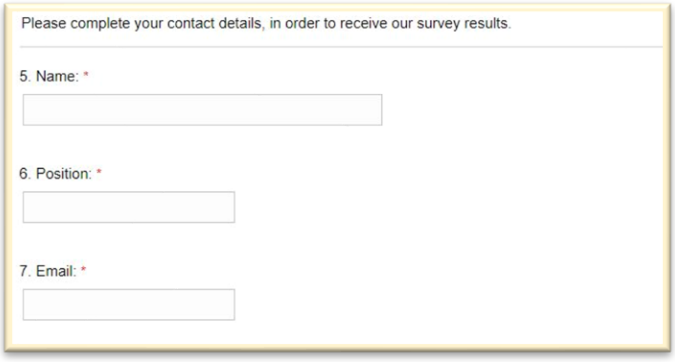


Figure B2. Questions for contact details.

Figure B3. Question No 8.

Figure B4. Question No 9.

Figure B5. Question No 10

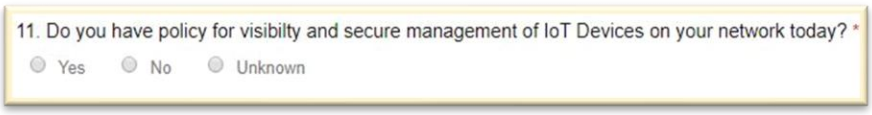


Figure B6. Question No 11.

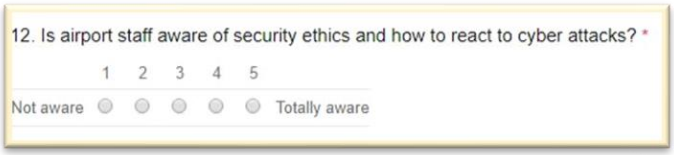


Figure B7. Question No 12.

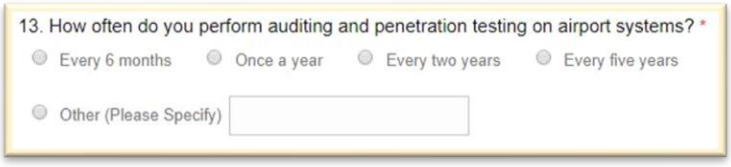


Figure B8. Question No 13.

Figure B9. Question No 14.

Figure B10. Question No 15.

Figure B11. Question No 16.

Online Survey Questionnaire Answers and Related Statistics

Table B1. Origin of airports' answering & airport's classification.

Airport's Location	Answers Received	
Europe	66%	22
USA	34%	12
TOTAL	100%	34

Airport's Classification	Answers Received	
Basic	16%	5
Agile	56%	19
Smart	28%	10
TOTAL	100%	34

Table B2. Answers to Question 8.

Question: What Types of Internet of Things (IoT) Applications is Your Organization Providing?		
IoT Applications in Airports	**Answers Received**	
SCADA	6%	2
Connection with other transportation systems	15%	5
Landside Operation Control System	18%	6
Airside Operation Control System	24%	8
Communication systems	27%	9
Baggage handling system	29%	10
Smart Building / HVAC / BMS	29%	10
Traveler Kiosk devices and web services	29%	10
Common use passenger processing systems	41%	14
Passenger Check in & boarding	41%	14

Table B3. Answers to Question 14.

Question: Which of the Following Technical/Tool-Based Good Practices are You Implementing in Your Organization?				
Technical Good Practices	**BASIC**	**AGILE**	**SMART**	**ALL**
Antimalware	2	10	6	18
Software and hardware updates	2	15	8	25

Firewalls & network segmentation	4	19	10	33
Intrusion Detection Systems	0	11	6	17
Strong user authentication	0	15	6	21
Change default credentials	2	10	4	16
Data encryption	0	10	8	18
BYOD Controls	0	6	4	10
Disaster recovery plans	2	11	10	23
Appl. security & secure design	2	6	8	16

Table B4. Answers to Question 16.

Question: Which of the Following Policies and Standards for Mitigating Risks are You Implementing in Your Organization?				
Good Practices for Policies and Standards	**BASIC**	**AGILE**	**SMART**	**ALL**
User access management	2	10	10	22
Screen individuals prior to authorize access to airport's IT system	1	6	6	13
Ensure access agreement to individuals prior to grant access	2	10	8	20
Personnel security requirements for third-party providers	2	8	6	16
Basic security awareness training to all information system users	2	10	8	20

Table B5. Answers to Question 15

Question: Which of the Following Policies and Standards for Mitigating Risks Are You Implementing in Your Organization?				
Good Practices About People, Organization and Processes	**BASIC**	**AGILE**	**SMART**	**ALL**
User access management	5	17	10	32

Screen individuals prior to authorize access to airport's IT system	0	10	6	16
Ensure access agreement to individuals prior to grant access	2	4	4	10
Personnel security requirements for third-party providers	2	6	6	14
Basic security awareness training to all information system users	2	10	8	20
Specialised info security training	2	6	4	12
Train airport personnel in incident response for IT system	2	6	4	12
Test and exercise incident response capability for IT system	2	10	6	18

Appendix C

As presented in Chapter 4, IATA codes for all US airports are listed in the table below as discussed and examined in our research results.

LIST OF US AIRPORTS WITH IATA CODE AND CITY/STATE SERVED

IATA CODE	MAJOR CITY SERVED	AIRPORT NAME	ANNUAL PASSENGER BOARDINGS
ATL	Atlanta	Hartsfield–Jackson Atlanta Int. Airport	50,501,858
LAX	Los Angeles	Los Angeles International Airport	39,636,042
ORD	Chicago	Chicago O'Hare International Airport	37,589,899
DFW	Dallas	Dallas/Fort Worth International Airport	31,283,579
JFK	New York	John F. Kennedy International Airport	29,533,154
DEN	Denver	Denver International Airport	28,267,394
SFO	San Francisco	San Francisco International Airport	25,707,101
MCO	Orlando	Orlando International Airport	24,562,271
LAS	Las Vegas	McCarran International Airport	22,833,267
SEA	Seattle / Tacoma	Seattle–Tacoma International Airport	21,887,110
CLT	Charlotte	Charlotte/Douglas International Airport	21,511,880
MIA	Miami	Miami International Airport	21,421,031
PHX	Phoenix	Phoenix Sky Harbor International Airport	20,896,265
IAH	Houston	George Bush Intercontinental Airport	20,062,072
EWR	New York	Newark Liberty International Airport	19,923,009
MSP	Minneapolis	Minneapolis–St. Paul International Airport	18,123,844
FLL	Fort Lauderdale	Fort Lauderdale–Hollywood Int. Airport	17,950,989
BOS	Boston	Edward Lawrence Logan Int. Airport	17,759,044
DTW	Detroit	Detroit Metropolitan Airport	16,847,135
PHL	Philadelphia	Philadelphia International Airport	15,285,948
LGA	New York	LaGuardia Airport (&Marine Air Terminal)	14,614,802
BWI	Baltimore	Baltimore/Washington Int. Thurgood Airport	13,371,816
DCA	Washington, D.C.	Ronald Reagan Washington National Airport	11,470,854
SLC	Salt Lake City	Salt Lake City International Airport	11,143,738
MDW	Chicago	Chicago Midway International Airport	11,044,387
TPA	Tampa	Tampa International Airport	10,941,173
IAD	Washington, D.C.	Washington Dulles International Airport	10,596,942
SAN	San Diego	San Diego International Airport	10,340,164
PDX	Portland	Portland International Airport	9,071,154
DAL	Dallas	Dallas Love Field	7,554,596
STL	St. Louis	St. Louis Lambert International Airport	6,793,076
RDU	Raleigh	Raleigh-Durham International Airport	5,401,714
SJC	San Jose	Norman Y. Mineta San José Int. Airport	5,321,603
RSW	Fort Myers	Southwest Florida International Airport	5,044,024
PIT	Pittsburgh	Pittsburgh International Airport	4,670,954
SAT	San Antonio	San Antonio International Airport	4,179,994
CLE	Cleveland	Cleveland-Hopkins International Airport	4,083,476
JAX	Jacksonville	Jacksonville International Airport	3,479,923
PBI	West Palm Beach	Palm Beach International Airport	3,100,624
ANC	Anchorage	Ted Stevens Anchorage International Airport	2,563,524
OMA	Omaha	Eppley Airfield	2,127,387
MEM	Memphis	Memphis International Airport	2,016,089
SFB	Sanford	Orlando Sanford International Airport	1,601,614
TUL	Tulsa	Tulsa International Airport	1,342,315
SYR	Syracuse	Syracuse Hancock International Airport	1,013,149
GSP	Greenville	Greenville-Spartanburg International Airport	991,276
MYR	Myrtle Beach	Myrtle Beach International Airport	944,849
HPN	White Plains	Westchester County Airport	759,334
COS	Colorado Springs	City of Colorado Springs Municipal Airport	657,694
LEX	Lexington	Blue Grass Airport	638,316
PSM	Portsmouth	Portsmouth International Airport at Pease	73,247

Appendix D

Research results from Chapter 4 are presented below with tabular form in tables D1-D3

TABLE D1. 30 BUSIEST AIRPORTS WITH INCOMING & OUTGOING DELAY RISK FOR JULY-AUGUST 2018-19

YEAR	2018			2019		
AIRPORT CODE	INCOMING AVERAGE RISK	OUTGOING AVERAGE RISK	NUMBER OF CONNECTIONS	INCOMING AVERAGE RISK	OUTGOING AVERAGE RISK	NUMBER OF CONNECTIONS
ATL	0.33	0,39	157	0,30	0,37	160
BOS	0.67	0.51	61	0.56	0.47	64
BWI	0.58	0.62	70	0.43	0.55	69
CLT	0.43	0.61	130	0.35	0.51	128
DAL	0.48	0.66	56	0.37	0.46	59
DCA	0.45	0.47	86	0.43	0.53	91
DEN	0.43	0.55	152	0.48	0.56	165
DFW	0.45	0.64	161	0.36	0.47	179
DTW	0.31	0.33	108	0.35	0.37	113
EWR	0.82	0.71	88	0.77	0.70	83
FLL	0.65	0.65	72	0.81	0.79	74
IAD	0.54	0.48	65	0.43	0.46	67
IAH	0.32	0.36	109	0.40	0.47	110
JFK	0.64	0.56	66	0.57	0.54	64
LAS	0.55	0.57	111	0.40	0.40	111
LAX	0.36	0.39	97	0.39	0.38	103
LGA	0.54	0.54	70	0.57	0.57	74
MCO	0.68	0.72	78	0.58	0.63	87
MDW	0.47	0.73	65	0.36	0.52	64
MIA	0.47	0.69	55	0.43	0.62	54
MSP	0.29	0.34	124	0.27	0.28	121
ORD	0.50	0.59	161	0.48	0.57	174
PDX	0.36	0.35	51	0.37	0.25	47
PHL	0.58	0.61	77	0.48	0.55	81
PHX	0.41	0.50	93	0.35	0.36	93
SAN	0.48	0.51	62	0.41	0.38	60
SEA	0.43	0.49	76	0.43	0.42	73
SFO	0.60	0.57	81	0.47	0.46	83
SLC	0.30	0.34	88	0.25	0.25	88
TPA	0.56	0.57	56	0.50	0.44	58

TABLE D2. AIRPORT'S CONNECTIONS WITH HIGHER AVERAGE DELAY RISK (2018)

ORIGIN	DEST	RISK	ORIGIN	DEST	RISK
DEN	EWR	1.21	SEA	ORD	0.66
ORD	EWR	1.18	SFO	DEN	0.66
MIA	JFK	1.16	DFW	LGA	0.64
FLL	JFK	1.15	SFO	ORD	0.63
MCO	JFK	1.06	JFK	SFO	0.63
SFO	EWR	1.05	ATL	BOS	0.63
EWR	FLL	1.02	DAL	HOU	0.63
MCO	EWR	0.97	ORD	LAX	0.62
EWR	MCO	0.96	ORD	DCA	0.6
MCO	SJU	0.96	SFO	LAS	0.59
ORD	LGA	0.92	EWR	ATL	0.59
ORD	BOS	0.88	DCA	BOS	0.58
ORD	PHL	0.88	LAS	DEN	0.58
JFK	MCO	0.87	ATL	LGA	0.57
DEN	SFO	0.86	DEN	LAS	0.57
PHX	SFO	0.84	LAX	ORD	0.56
PHL	MCO	0.84	DEN	SEA	0.55
ATL	EWR	0.81	DFW	ATL	0.55
EWR	SFO	0.81	LAX	SFO	0.54
BOS	EWR	0.81	SFO	SAN	0.54
EWR	BOS	0.81	ORD	MSP	0.54
MCO	PHL	0.81	ORD	ATL	0.52
SFO	BOS	0.79	LAS	SEA	0.52
ORD	DFW	0.77	LGA	ATL	0.5
SFO	JFK	0.77	ATL	MCO	0.5
SFO	SEA	0.76	BOS	ORD	0.49
MIA	LGA	0.74	MSP	ORD	0.49
SEA	SFO	0.73	SFO	LAX	0.48
LAS	SFO	0.73	DCA	ORD	0.46
DFW	ORD	0.73	SEA	LAX	0.45
LGA	ORD	0.72	MCO	ATL	0.45
ORD	SFO	0.72	LAS	LAX	0.44
BOS	PHL	0.72	LAX	SEA	0.44
ORD	SEA	0.71	ATL	FLL	0.44
LAX	EWR	0.71	BOS	LGA	0.42
LAX	JFK	0.68	FLL	ATL	0.42
SAN	SFO	0.68	LGA	BOS	0.4
ORD	DEN	0.67	LAX	LAS	0.39
PHL	BOS	0.67	JFK	LAX	0.38

TABLE D3. AIRPORT'S CONNECTIONS WITH HIGHER AVERAGE DELAY RISK (2019)

ORIGIN	DEST	RISK	ORIGIN	DEST	RISK
EWR	FLL	1.05	DFW	DEN	0.6
FLL	JFK	1.03	FLL	ATL	0.59
FLL	EWR	1	LAS	DEN	0.59
MCO	EWR	0.95	DEN	SEA	0.58
EWR	MCO	0.92	DFW	LAX	0.58
ORD	EWR	0.92	ORD	SEA	0.58
LGA	FLL	0.9	SFO	SEA	0.56
MCO	SJU	0.88	LGA	BOS	0.56
MCO	JFK	0.85	ATL	LGA	0.56
EWR	SFO	0.84	ORD	ATL	0.56
CLT	MCO	0.84	ORD	DCA	0.56
EWR	BOS	0.82	DEN	LAS	0.56
FLL	LGA	0.8	SEA	DEN	0.55
ATL	EWR	0.79	SFO	ORD	0.55
ORD	LGA	0.77	LAX	JFK	0.54
SFO	EWR	0.74	DCA	BOS	0.54
BOS	EWR	0.74	BOS	LGA	0.53
CLT	EWR	0.74	BOS	ORD	0.53
ORD	DFW	0.72	MIA	ATL	0.53
DEN	SFO	0.72	DEN	PHX	0.53
EWR	LAX	0.71	PHX	DEN	0.53
DFW	ORD	0.69	MSP	ORD	0.51
PHL	MCO	0.68	ATL	DEN	0.51
ORD	SFO	0.67	SEA	SFO	0.5
LGA	ORD	0.65	PHL	BOS	0.5
ORD	BOS	0.65	LAX	ORD	0.49
ORD	DEN	0.65	ATL	ORD	0.49
ORD	MSP	0.64	SFO	JFK	0.49
SJU	MCO	0.64	LAS	SFO	0.48
LGA	ATL	0.63	LAX	DFW	0.48
ATL	FLL	0.62	DEN	LAX	0.47
DFW	IAH	0.62	BOS	DCA	0.46
ORD	DTW	0.61	MCO	ATL	0.44
MCO	PHL	0.61	JFK	LAX	0.42
ATL	MCO	0.6	LAX	SFO	0.4
ORD	LAX	0.6	SFO	LAX	0.37
DEN	ORD	0.6	SEA	ANC	0.37
SFO	DEN	0.6	LAX	LAS	0.34
DFW	LGA	0.6	LAS	LAX	0.33

References

Abc Net. (2017, September 25). *Cyber attack ruled out as Sydney Airport attempts to clear chaos*. https://www.abc.net.au/news/2017-09-25/sydney-airport-delays-begin-clearing-after-radar-fixed/8984862

Adams, C. (2018, September 16). Bristol Airport blames cyber attack for taking departure boards offline for two days. *The Telegraph*. https://www.telegraph.co.uk/news/2018/09/16/bristol-airport/

Alsamhi, S. H., Ma, O., Ansari, M. S., & Almalki, F. A. (2019). Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEEAccess*, *7*, 128125–128152. https://doi.org/10.1109/ACCESS.2019.2934998

Altawy, R., & Youssef, A. M. (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2), 7:1-7:25. https://doi.org/10.1145/3001836

Angrishi, K. (2017). Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. *ArXiv:1702.03681 [Cs]*. http://arxiv.org/abs/1702.03681

Australian Capital Territory & Environment and Planning Directorate. (2016). *ACT climate change adaptation strategy: Living with a warming climate*. https://www.yoursay.act.gov.au/application/files/3615/1252/3571/ACT-Climate-Change-Adaptation-Strategy.pdf

Avgerinou, M., Bertoldi, P., & Castellazzi, L. (2017). Trends in Data Centre Energy Consumption under the European Code of Conduct for Data Centre Energy Efficiency. *Energies*, *10*(10), 1470. https://doi.org/10.3390/en10101470

Bagler, G. (2008). Analysis of the airport network of India as a complex weighted network. *Physica A: Statistical Mechanics and Its Applications*, *387*(12), 2972–2980. https://doi.org/10.1016/j.physa.2008.01.077

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. (2012). Ensuring safety, security, and sustainability of mission-critical cyber-physical systems.

Proceedings of the IEEE, *100*(1), 283–299. https://doi.org/10.1109/JPROC.2011.2165689

Bawden, T. (2016). *Global warming: Data centres to consume three times as much energy in next decade, experts warn*. The Independent. https://www.independent.co.uk/environment/global-warming-data-centres-consume-three-times-much-energy-next-decade-experts-warn-a6830086.html

Bernardini, A., Mangiatordi, F., Pallotti, E., & Capodiferro, L. (2017). Drone detection by acoustic signature identification. *Electronic Imaging*, *2017*(10), 60–64. https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168

Birch, G. C., & Woo, B. L. (2017). *Counter Unmanned Aerial Systems Testing: Evaluation of VIS SWIR MWIR and LWIR passive imagers.* (No. SAND2017-0921). Sandia National Lab. (SNL-NM), Albuquerque, NM (United States). https://doi.org/10.2172/1342469

Birnbach, S., Baker, R., & Martinovic, I. (2017). *Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones*. Internet Society. https://ora.ox.ac.uk/objects/uuid:c74a2aa9-1950-4f97-992e-89406a6fdf8f

Blue Ribbon Task Force. (2019). *Blue Ribbon Task Force on UAS Mitigation at Airports, Interim Report*.

Bureau of Transportation Statistics. (2020, March 5). *Airline on-time performance and causes of flight delays*. https://www.bts.gov/explore-topics-and-geography/topics/airline-time-performance-and-causesflight-delays

Bureau of Transportation Statistics (BTS), United States Department of Transportation. (n.d.). *Reporting Carrier On-Time Performance (1987-present).* Retrieved July 28, 2020, from https://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=236

Calantropio, A. (2019). The Use of UAVs for Performing Safety-Related Tasks at Post-Disaster and Non-Critical Construction Sites. *Safety*, *5*(4), 64. https://doi.org/10.3390/safety5040064

Campanelli, B., Fleurquin, P., Arranz, A., Etxebarria, I., Ciruelos, C., Eguíluz, V. M., & Ramasco, J. J. (2016a). Comparing the modeling of delay propagation in the US and European air traffic networks. *Journal of Air Transport Management*, *56*, 12–18. https://doi.org/10.1016/j.jairtraman.2016.03.017

CANSO. (2014b). Cyber Security and Risk Assessment Guide. *CANSO*. https://canso.org/document/cyber-security-and-risk-assessment-guide/

Cerchio, R. D., & Riley, C. (2011). Aircraft systems cyber security. *2011 IEEE/AIAA 30th Digital Avionics Systems Conference*, 1C3-1-1C3-7. https://doi.org/10.1109/DASC.2011.6095969

Chang, X., Yang, C., Wu, J., Shi, X., & Shi, Z. (2018). A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays. *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, 573–577. https://doi.org/10.1109/SAM.2018.8448409

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Chinnici, M., & Quintiliani, A. (2013). An Example of Methodology to Assess Energy Efficiency Improvements in Datacenters. *2013 International Conference on Cloud and Green Computing*. https://doi.org/10.1109/CGC.2013.78

Chowdhury, A. S. K. (2016). Implementation and Performance Evaluation of Acoustic Denoising Algorithms for UAV. *UNLV Theses, Dissertations, Professional Papers, and Capstones*. https://doi.org/10.34917/10083129

Church, P., Grebe, C., Matheson, J., & Owens, B. (2018). Aerial and surface security applications using lidar. *Laser Radar Technology and Applications XXIII*, *10636*, 1063604. https://doi.org/10.1117/12.2304348

CISA. (2018a). *Assessments: Cyber Resilience Review (CRR)*. https://us-cert.cisa.gov/resources/assessments

CISA. (2018b). *CYBER SECURITY EVALUATION TOOL*. https://us-cert.cisa.gov/ics/Assessments

CISA. (2019, May 9). *Transportation Systems Sector*. https://www.cisa.gov/transportation-systems-sector

Commerce, U. S. D. of, & Security, U. S. D. of H. (2018). *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (pp. 38–38). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final

Committee on Climate Change and U.S. Transportation. (2008). *Potential Impacts of Climate Change on U.S. Transportation: Special Report 290*. https://doi.org/10.17226/12179

Costin, A., & Francillon, A. (2012). *Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices*.

Critical Infrastructure Sectors | CISA. (2013). https://www.cisa.gov/critical-infrastructure-sectors

Davidson, D., Wu, H., & Jellinek, R. (2016). Controlling UAVs with Sensor Input Spoofing Attacks. *In Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT)*, 11. https://www.usenix.org/system/files/conference/woot16/woot16-paper-davidson.pdf

Dedrone. (2020). *Map of World Wide Drone Incidents—Dedrone*. https://www.dedrone.com/resources/incidents/all

Deshpande, V., & Arıkan, M. (2012a). The Impact of Airline Flight Schedules on Flight Delays. *Manufacturing & Service Operations Management*, *14*(3), 423–440. https://doi.org/10.1287/msom.1120.0379

DHL. (2013). *The World in 2050—A Scenario Study*. DHL. https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/case-studies/logistics-2050.html

DJI. (2019). *DJI Improves Geofencing To Enhance Protection of European Airports and Facilities*. DJI Official. https://www.dji.com/ae/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities

Drozdowicz, J., Wielgo, M., Samczynski, P., Kulpa, K., Krzonkalla, J., Mordzonek, M., Bryl, M., & Jakielaszek, Z. (2016). 35 GHz FMCW drone detection system. *2016 17th International Radar Symposium (IRS)*. https://doi.org/10.1109/IRS.2016.7497351

Du, W.-B., Zhang, M.-Y., Zhang, Y., Cao, X.-B., & Zhang, J. (2018). Delay causality network in air transport systems. *Transportation Research Part E: Logistics and Transportation Review*, *118*, 466–476. https://doi.org/10.1016/j.tre.2018.08.014

EASA -EU. (2011). *Commission Regulation (EU) No 1332/2011*. EASA. https://www.easa.europa.eu/document-library/regulations/commission-regulation-eu-no-13322011

ENERGY STAR. (2012). *Harmonizing global metrics for data center energy efficiency*. https://www.energystar.gov/buildings/tools-and-resources/measurement-protocol-gec-erf-and-cue

ENISA. (2015a). *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors* [Report/Study]. https://www.enisa.europa.eu/publications/maturity-levels

ENISA. (2015b). *Threat Landscape of Internet Infrastructure* [Report/Study]. https://www.enisa.europa.eu/publications/iitl

ENISA. (2016). *Securing Smart Airports* [Report/Study]. https://www.enisa.europa.eu/publications/securing-smart-airports

ENISA. (2017). *Baseline Security Recommendations for IoT* [Report/Study]. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

EUROCONTROL. (2009). *White Paper on Resilience Engineering for ATM*. https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf

EUROCONTROL. (2012). *Manual for National ATM Security Oversight*. https://www.eurocontrol.int/publication/manual-national-atm-security-oversight

EUROCONTROL. (2013). *Challenges of growth 2013*. https://www.eurocontrol.int/publication/challenges-growth-2013

European Climate Adaptation Platform, D. C. (2016). *Climate-ADAPT*. DG Joint Research Centre. https://climate-adapt.eea.europa.eu/

European Commission. (2011). *Roadmap to a Single European Transport Area—Towards a competitive and resource efficient transport system -White paper* [Text]. Mobility and Transport - European Commission. https://ec.europa.eu/transport/themes/european-strategies/white-paper-2011_en

European Commission, Joint Research Centre. (2016). *Resilience of large investments and critical infrastructures in Europe to climate change.* Publications Office. https://data.europa.eu/doi/10.2788/232049

European Environment Agency. (2014). *Adaptation of transport to climate change in Europe—EEA Report No 8/2014*. https://www.eea.europa.eu/publications/adaptation-of-transport-to-climate

Eurostat. (2017). *Energy from renewable sources—Statistics Explained*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_from_renewable_sources

FAA. (2018). *Integration of Civil Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS) Roadmap*. https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf

FAA. (2020a). *FAA Aerospace Forecasts*. https://www.faa.gov/data_research/aviation/aerospace_forecasts/

FAA. (2020b). *UAS Sightings Report*. https://www.faa.gov/uas/resources/public_records/uas_sightings_report/

Fioranelli, F., Ritchie, M., Griffiths, H., & Borrion, H. (2015). Classification of loaded/unloaded micro-drones using multistatic radar. *Electronics Letters*, *51*(22), 1813–1815. https://doi.org/10.1049/el.2015.3038

Faily S., Lykou G., Partridge A., Gritzalis D., Mylonas A., Katos V. (2016). Human-centered specification exemplars for critical infrastructure environments, in Proc. of the 30th Intern. Human Computer Interaction Conference, BCS, United Kingdom.

Fleurquin, P., Ramasco, J. J., & Eguiluz, V. M. (2013). Systemic delay propagation in the US airport network. *Scientific Reports*, *3*(1), 1159. https://doi.org/10.1038/srep01159

Forzieri, G., Bianchi, A., Silva, F. B. e, Marin Herrera, M. A., Leblois, A., Lavalle, C., Aerts, J. C. J. H., & Feyen, L. (2018). Escalating impacts of climate extremes on critical infrastructures in Europe. *Global Environmental Change*, *48*, 97–107. https://doi.org/10.1016/j.gloenvcha.2017.11.007

Franchina, L., Carbonelli, M., Gratta, L., Crisci, M., & Perucchini, D. (2011). An impact-based approach for the analysis of cascading effects in critical infrastructures. *International Journal of Critical Infrastructures*, *7*(1), 73. https://doi.org/10.1504/IJCIS.2011.038958

Gillen, D., Hasheminia, H., & Jiang, C. (2015). Strategic considerations behind the network–regional airline tie ups – A theoretical and empirical study. *Transportation Research Part B: Methodological*, *72*, 93–111. https://doi.org/10.1016/j.trb.2014.09.001

Gökçe, F., Üçoluk, G., Şahin, E., & Kalkan, S. (2015). Vision-Based Detection and Distance Estimation of Micro Unmanned Aerial Vehicles. *Sensors*, *15*(9), 23805–23846. https://doi.org/10.3390/s150923805

Gopalakrishnan, Govindarasu, M., W. Jacobson, D., & M. Phares, B. (2013). CYBER SECURITY FOR AIRPORTS. *INTERNATIONAL JOURNAL FOR TRAFFIC*

AND TRANSPORT ENGINEERING, *3*(4), 365–376. https://doi.org/10.7708/ijtte.2013.3(4).02

Gopalakrishnan, K., & Balakrishnan, H. (2017). *A comparative analysis of models for predicting delays in air traffic networks*.

Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magkos E., Lykou G. (2016). Critical infrastructure protection: A holistic methodology for Greece, in Proc. of the Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (in conjunction with ESORICS-2016), pp. 19-34, Springer, Greece.

Grant-Muller, S., & Usher, M. (2014). *Intelligent Transport Systems: : The propensity for environmental and economic benefits*. https://doi.org/10.1016/J.TECHFORE.2013.06.010

Guide, & Governance, E. O. (2006). *Good Practice Guide Process Control and SCADA Security*. /paper/Good-Practice-Guide-Process-Control-and-SCADA-Guide-GOVERNANCE/0f542323ba6c208b685dc65ab5aef1e0cab838a2

Guimera, R., Mossa, S., Turtschi, A., & Amaral, L. A. N. (2005). The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proceedings of the National Academy of Sciences*, *102*(22), 7794–7799. https://doi.org/10.1073/pnas.0407994102

Han, D. D., Qian, J. H., & Liu, J. G. (2007). Network Topology of the Austrian Airline Flights. *ArXiv:Physics/0703193*. http://arxiv.org/abs/physics/0703193

Hao, L., Hansen, M., Zhang, Y., & Post, J. (2014). New York, New York: Two ways of estimating the delay impact of New York airports. *Transportation Research Part E: Logistics and Transportation Review*, *70*, 245–260. https://doi.org/10.1016/j.tre.2014.07.004

Harmanny, R. I. A., Wit, J. J. M. de, & Cabic, G. P. (2014). Radar micro-Doppler feature extraction using the spectrogram and the cepstrogram. *2014 11th European Radar Conference*, 165–168. https://doi.org/10.1109/EuRAD.2014.6991233

Hayhurst, K. J., Maddalon, J. M., Neogi, N. A., & Verstynen, H. A. (2015). A case study for assured containment. *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*, 260–269. https://doi.org/10.1109/ICUAS.2015.7152299

He, D., Qiao, Y., Chen, S., Du, X., Chen, W., Zhu, S., & Guizani, M. (2019). A Friendly and Low-Cost Technique for Capturing Non-Cooperative Civilian Unmanned Aerial Vehicles. *IEEE Network*, *33*(2), 146–151. https://doi.org/10.1109/MNET.2018.1800065

Highnam, K., Angstadt, K., Leach, K., Weimer, W., Paulos, A., & Hurley, P. (2016). An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture. *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, 222–225. https://doi.org/10.1109/DSN-W.2016.63

Hoffmann, F., Ritchie, M., Fioranelli, F., Charlish, A., & Griffiths, H. (2016). Micro-Doppler based detection and tracking of UAVs with multistatic radar. *2016 IEEE Radar Conference (RadarConf)*, 1–6. https://doi.org/10.1109/RADAR.2016.7485236

IATA. (2015). *Aviation Cyber Security*. https://www.iata.org/en/programs/security/cyber-security/

IATA. (2018, October 24). *IATA Forecast Predicts 8.2 billion Air Travelers in 2037*. https://www.iata.org/en/pressroom/pr/2018-10-24-02

ICAO. (2017). *Aviation Security Manual (Doc 8973 – Restricted)*. https://www.icao.int/Security/SFP/Pages/SecurityManual.aspx

ICAO. (2019). *Aviation Benefits Report*. https://www.icao.int/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf

ICAO. Assembly Resolutions A39-19, 2016. (n.d.). Retrieved January 3, 2021, from https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf

Industry High Level Group. (2017). *Aviation Benefits—IHLG Report*. https://www.icao.int/sustainability/Pages/IHLG.aspx

International Energy Agency. (2016). *Energy, Climate Change and Environment 2016 Insights – Analysis*. IEA. https://www.iea.org/reports/energy-climate-change-and-environment-2016-insights

IPCC. (2014). *AR5 Climate Change 2014: Impacts, Adaptation, and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change, Cambridge Univ. Press, Cambridge, USA*. https://www.ipcc.ch/report/ar5/wg2/

Jain, A., Mishra, M., Peddoju, S. K., & Jain, N. (2013). Energy efficient computing-Green cloud computing. *2013 International Conference on Energy Efficient Technologies for Sustainability*, 978–982. https://doi.org/10.1109/ICEETS.2013.6533519

Jeon, S., Shin, J., Lee, Y., Kim, W., Kwon, Y., & Yang, H. (2017). Empirical study of drone sound detection in real-life environment with deep neural networks. *2017 25th European Signal Processing Conference (EUSIPCO)*, 1858–1862. https://doi.org/10.23919/EUSIPCO.2017.8081531

Joint Air Power Competence Centre. (2019, August 16). A Comprehensive Approach to Countering Unmanned Aircraft Systems. *Joint Air Power Competence Centre*. https://www.japcc.org/portfolio/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/

Jones, D. (2016). Small Remotely Piloted Aircraft Systems (drones), Mid-Air Collision Study. *The Department for Transport, the Military Aviation Authority and British Airline Pilots' Association*, 18.

Kafle, N., & Zou, B. (2016a). Modeling flight delay propagation: A new analytical-econometric approach. *Transportation Research Part B: Methodological*, *93*, 520–542. https://doi.org/10.1016/j.trb.2016.08.012

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics*, *31*(4), 617–636. https://doi.org/10.1002/rob.21513

Kiesling, T., & Kreuzer, M. (2017). *Recommendations to Strengthen the Cyber-Resilience of the Air Traffic System* (ARIEL, Air Traffic Resilience). SESAR JU.

Kim, J., Park, C., Ahn, J., Ko, Y., Park, J., & Gallagher, J. C. (2017). Real-time UAV sound detection and analysis system. *2017 IEEE Sensors Applications Symposium (SAS)*, 1–5. https://doi.org/10.1109/SAS.2017.7894058

Kjølle, G. H., Utne, I. B., & Gjerde, O. (2012). Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, *105*, 80–89. https://doi.org/10.1016/j.ress.2012.02.006

Knott, E. F., Schaeffer, J. F., & Tulley, M. T. (2004). *Radar Cross Section*. SciTech Publishing.

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013a). Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures*, *9*(1/2), 93. https://doi.org/10.1504/IJCIS.2013.051606

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013b). Cascading Effects of Common-Cause Failures in Critical Infrastructures. In J. Butts & S. Shenoi (Eds.), *Critical Infrastructure Protection VII* (pp. 171–182). Springer Berlin Heidelberg.

Kumar, S. A. P., & Xu, B. (2017). *Vulnerability Assessment for Security in Aviation Cyber-Physical Systems* (pp. 145–150). IEEE Computer Society. https://doi.org/10.1109/CSCloud.2017.17

Lee, K. A. (2008, January 1). *CS2SAT: THE CONTROL SYSTEMS CYBER SECURITY SELF-ASSESSMENT TOOL* (Article INL/CON-07-12810). ISA EXPO 2007,Houston, TX,10/02/2007,10/04/2007; Idaho National Laboratory. https://digital.library.unt.edu/ark:/67531/metadc897337/

Li, W., Wang, Q. A., Nivanen, L., & Le Méhauté, A. (2006). How to fit the degree distribution of the air network? *Physica A: Statistical Mechanics and Its Applications*, *368*(1), 262–272. https://doi.org/10.1016/j.physa.2005.11.050

Li, Z.-C., Lam, W. H. K., Wong, S. C., & Fu, X. (2010). Optimal route allocation in a liberalizing airline market. *Transportation Research Part B: Methodological*, *44*(7), 886–902. https://doi.org/10.1016/j.trb.2009.12.013

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018a). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, *19*(1), 19. https://doi.org/10.3390/s19010019

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018b). Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience. *2018 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2018.8534523

Lykou G., Anagnostopoulou A., Stergiopoulos G., Gritzalis D. (2018c) Cybersecurity self-assessment tools: Evaluating importance for securing industrial control systems in critical infrastructures, in Proc. of the 13th International Conference on Critical Information Infrastructures Security (CRITIS-2018), pp. 129-142, Springer, Lithuania.

Lykou G., Dedousis P., Stergiopoulos G., Gritzalis D. (2020) Assessing Interdependencies and Congestion Delays in the Aviation Network. IEEE Access, vol. 8, pp. 223234-54.

Lykou G., Iakovakis G., Chronis G., Gritzalis D. (2017). Analysis and classification of adaptation tools for Transport Sector adaptation planning, in Proc. of the 12th Intern. Conference on Critical Information Infrastructures Security (CRITIS-2017), pp. 37-47, Springer, Italy.

Lykou G., Mentzeloti D., Gritzalis D. (2018). A new methodology towards effectively assessing Data-Center sustainability, Computers & Security, Vol. 76, pp. 327-340.

Lykou G., Moustakas D., Gritzalis D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies, Sensors, Vol. 20, No. 12:3537.

Lykou G., Stergiopoulos G., Papachrysanthou A., Gritzalis D. (2017). Protecting the Transportation Sector from the negative impact of climate change, in Proc. of the 11th International Conference on Critical Infrastructure Protection, pp. 3-21, Springer (Critical Infrastructure Protection XI), USA.

McLean, C. R., Lee, Y.-T. T., Jain, S., & Hutchings, C. W. (2011a). *Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications*. https://www.nist.gov/publications/modeling-and-simulation-critical-infrastructure-systems-homeland-security-applications

Mezei, J., & Molnár, A. (2016). Drone sound detection by correlation. *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 509–518. https://doi.org/10.1109/SACI.2016.7507430

Michel, A. (2019). Counter Drone Systems. *Center for the Study of the Drone at Bard College*, 45.

Mitch, R. H., Dougherty, R. C., Psiaki, M. L., Powell, S. P., O'Hanlon, B. W., Bhatti, J. A., & Humphreys, T. E. (2011). Signal Characteristics of Civil GPS Jammers. *Radionavigation Laboratory Conference Proceedings*, 13. https://repositories.lib.utexas.edu/bitstream/handle/2152/63304/Signal%20Characteristics%20Civil%20GPS%20Jammers_Mitch.pdf?sequence=2

Molchanov, P., Harmanny, R. I. A., Wit, J. J. M. de, Egiazarian, K., & Astola, J. (2014). Classification of small UAVs and birds by micro-Doppler signatures. *International Journal of Microwave and Wireless Technologies*, *6*(3–4), 435–444. https://doi.org/10.1017/S1759078714000282

Mototolea, D., & Stolk, C. (2018). Detection and Localization of Small Drones Using Commercial Off-the-Shelf FPGA Based Software Defined Radio Systems. *2018*

International Conference on Communications (COMM), 465–470. https://doi.org/10.1109/ICComm.2018.8484827

Müller, J. D., & Deutsche Post AG (Eds.). (2012). *Delivering tomorrow: Logistics 2050 ; a scenario study* (1. ed). Deutsche Post AG.

Müller, T. (2017). Robust drone detection for day/night counter-UAV with static VIS and SWIR cameras. *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*, *10190*, 1019018. https://doi.org/10.1117/12.2262575

MyDefence. (2019, February 14). Protecting airports against drones. *MyDefence Counter UAS*. https://mydefence.dk/2019/02/mydefence-publishes-white-paper-on-airport-drone-protection/

NASA. (2020). *ASRS Database Online—Aviation Safety Reporting System*. https://asrs.arc.nasa.gov/search/database.html

Nassi, B., Shabtai, A., Masuoka, R., & Elovici, Y. (2019). SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps. *ArXiv:1903.05155 [Cs]*. http://arxiv.org/abs/1903.05155

National Academies of Sciences, E. (2015). *Guidebook on Best Practices for Airport Cybersecurity*. https://doi.org/10.17226/22116

Nayak, N., & Zhang, Y. (2011). Estimation and Comparison of Impact of Single Airport Delay on National Airspace System with Multivariate Simultaneous Models. *Transportation Research Record: Journal of the Transportation Research Board*, *2206*(1), 52–60. https://doi.org/10.3141/2206-07

Nguyen, K., Cheriet, M., Lemay, M., Savoie, M., & Ho, B. (2013). Powering a Data Center Network via Renewable Energy: A Green Testbed. *IEEE Internet Computing*. https://doi.org/10.1109/MIC.2012.125

Nguyen, P., Ravindranatha, M., Nguyen, A., Han, R., & Vu, T. (2016). Investigating Cost-effective RF-based Detection of Drones. *Proceedings of the 2nd Workshop*

on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, 17–22. https://doi.org/10.1145/2935620.2935632

Nguyen, P., Truong, H., Ravindranathan, M., Nguyen, A., Han, R., & Vu, T. (2018). Cost-Effective and Passive RF-Based Drone Presence Detection and Characterization. *GetMobile: Mobile Computing and Communications*, *21*(4), 30–34. https://doi.org/10.1145/3191789.3191800

Nieuweling, C. (2016, November 14). *Code of Conduct for Energy Efficiency in Data Centres* [Text]. EU Science Hub - European Commission. https://ec.europa.eu/jrc/en/energy-efficiency/code-conduct/datacentres

NIPP. (2013). *National Infrastructure Protection Plan, CISA*. US Department of Homeland Security. U.S. Department of Home Security. https://www.cisa.gov/national-infrastructure-protection-plan

NIST, CYBERSECURITY FRAMEWORK. (2018, April 12). *The Five Functions* [Text]. NIST. https://www.nist.gov/cyberframework/online-learning/five-functions

Opromolla, R., Fasano, G., & Accardo, D. (2018). A Vision-Based Approach to UAV Detection and Tracking in Cooperative Applications. *Sensors*, *18*(10), 3391. https://doi.org/10.3390/s18103391

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

Palin, E., Thornton, H., Mathison, C., Mccarthy, R., Clark, R., & Dora, J. (2013). Future projections of temperature-related climate change impacts on the railway network of Great Britain. *Climatic Change*, *120*. https://doi.org/10.1007/s10584-013-0810-8

PARAS. (2019). *Guidance for Integrating Unmanned Aircraft Systems (UAS) into Airport Security*. https://www.sskies.org/images/uploads/subpage/PARAS_0012.UASAirportSecurityIntegration.FinalGuidebook.pdf

Park, S., Shin, S., Kim, Y., Matson, E. T., Lee, K., Kolodzy, P. J., Slater, J. C., Scherreik, M., Sam, M., Gallagher, J. C., Fox, B. R., & Hopmeier, M. (2015). Combination of radar and audio sensors for identification of rotor-type Unmanned Aerial Vehicles (UAVs). *2015 IEEE SENSORS*, 1–4. https://doi.org/10.1109/ICSENS.2015.7370533

Peacock, M., & Johnstone, Michael. N. (2013). Towards detection and control of civilian unmanned aerial vehicles [PDF]. *Proceedings of the 14th Australian Information Warfare Conference*, *Edith Cowan University*, 2013. https://doi.org/10.4225/75/57A847DFBEFB5

Pyrgiotis, N., Malone, K. M., & Odoni, A. (2013). Modelling delay propagation within an airport network. *Transportation Research Part C: Emerging Technologies*, *27*, 60–75. https://doi.org/10.1016/j.trc.2011.05.017

Raj, P., & Raman, A. C. (2017). *The Internet of Things: Enabling Technologies, Platforms, and Use Cases*. CRC Press.

Reis, D. (2016). *Cybersecurity: Issues of Today, a Path for Tomorrow*. Archway Publishing.

Reuters. (2015, June 21). *Hackers ground 1,400 passengers at Warsaw in attack on airline's computers*. The Guardian. http://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot

Riahi Manesh, M., & Kaabouch, N. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *International Journal of Critical Infrastructure Protection*, *19*, 16–31. https://doi.org/10.1016/j.ijcip.2017.10.002

Ritchie, M., Fioranelli, F., Griffiths, H., & Torvik, B. (2015). Micro-drone RCS analysis. *2015 IEEE Radar Conference*, 452–456. https://doi.org/10.1109/RadarConf.2015.7411926

Robert, B. (2004). A method for the study of cascading effects within lifeline networks. *International Journal of Critical Infrastructures*, *1*(1), 86. https://doi.org/10.1504/IJCIS.2004.003798

Rodday, N. (2016). *Hacking a Professional Drone*. 27.

Rozantsev, A., Sinha, S. N., Dey, D., & Fua, P. (2017). *Flight Dynamics-Based Recovery of a UAV Trajectory Using Ground Cameras*. 6030–6039. https://openaccess.thecvf.com/content_cvpr_2017/html/Rozantsev_Flight_Dynamics-Based_Recovery_CVPR_2017_paper.html

Rozum, J., & Car, S. (2014, February 14). *Tools for Coastal Climate Adaptation Planning: A guide for selecting tools to assist with ecosystem-based climate planning*. NatureServe, Arlington, Va. https://www.natureserve.org/biodiversity-science/publications/tools-coastal-climate-adaptation-planning-guide-selecting-tools

Rupp, N. G. (2007). *Further Investigations into the Causes of Flight Delays*.

Salamon, J., Jacoby, C., & Bello, J. P. (2014). A Dataset and Taxonomy for Urban Sound Research. *Proceedings of the 22nd ACM International Conference on Multimedia*, 1041–1044. https://doi.org/10.1145/2647868.2655045

Samaras, S., Diamantidou, E., Ataloglou, D., Sakellariou, N., Vafeiadis, A., Magoulianitis, V., Lalas, A., Dimou, A., Zarpalas, D., Votis, K., Daras, P., & Tzovaras, D. (2019). Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review. *Sensors*, *19*(22), 4837. https://doi.org/10.3390/s19224837

Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., & Royalty, C. (2011). Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond. *Proceedings of the IEEE*, *99*(11), 2040–2055. https://doi.org/10.1109/JPROC.2011.2162209

Sampigethaya, Krishna, Poovendran, R., & Bushnell, L. (2009). Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes. *Proceedings of the IEEE*, *96*, 1992–2007. https://doi.org/10.1109/JPROC.2008.2006123

Santamarta, R. (2018). *Last Call for SATCOM Security*. 72.

Saqib, M., Khan, S. D., Sharma, N., & Blumenstein, M. (2017). A study on detecting drones using deep convolutional neural networks. *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 1–5. https://doi.org/10.1109/AVSS.2017.8078541

Scheller, W. (2017). Detecting drones using machine learning. *Graduate Theses and Dissertations*. https://doi.org/10.31274/etd-180810-5839

SESAR JU. (2016). Addressing airport cyber-security. *Final Report*, 94.

Shehabi, A., Smith, S., Sartor, D., Brown, R., Herrlin, M., Koomey, J., Masanet, E., Horner, N., Azevedo, I., & Lintner, W. (2016). *United States Data Center Energy Usage Report*. https://eta.lbl.gov/publications/united-states-data-center-energy

Shi, Z., Huang, M., Zhao, C., Huang, L., Du, X., & Zhao, Y. (2017). Detection of LSSUAV using hash fingerprint based SVDD. *2017 IEEE International Conference on Communications (ICC)*, 1–5. https://doi.org/10.1109/ICC.2017.7996844

Silva, H. E., Verhoef, E. T., & van den Berg, V. A. C. (2014). Airline route structure competition and network policy. *Transportation Research Part B: Methodological*, *67*, 320–343. https://doi.org/10.1016/j.trb.2014.05.012

Skolnik, M. I. (Ed.). (1990). *Radar handbook* (2nd ed). McGraw-Hill.

Stander, A., & Ophoff, J. (2016). Cyber security in civil aviation. *Imam Journal of Applied Sciences*, *1*, 23–26.

Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G., & Gritzalis, D. (2016). Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection*, *12*, 46–60. https://doi.org/10.1016/j.ijcip.2015.12.002

Stergiopoulos, G., Valvis, E., Anagnou-Misyris, F., Bozovic, N., & Gritzalis, D. (2017a). Interdependency analysis of junctions for congestion mitigation in Transportation Infrastructures. *ACM SIGMETRICS Performance Evaluation Review*, *45*(2), 119–124. https://doi.org/10.1145/3152042.3152078

Stergiopoulos, G., Valvis, E., Mitrodimas, D., Lekkas, D., & Gritzalis, D. (2018). Analyzing Congestion Interdependencies of Ports and Container Ship Routes in the Maritime Network Infrastructure. *IEEE Access*, *6*, 63823–63832. https://doi.org/10.1109/ACCESS.2018.2877659

Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., & Gritzalis, D. (2016). Classification and Comparison of Critical Infrastructure Protection Tools. In M. Rice & S. Shenoi (Eds.), *Critical Infrastructure Protection X* (Vol. 485, pp. 239–255). Springer International Publishing. https://doi.org/10.1007/978-3-319-48737-3_14

Stergiopoulos G., Gritzalis D., Kotzanikolaou P., Magkos M., Lykou G. (2017). Holistic protection of critical infrastructures, Maritime Interdiction Operations Journal, Vol. 14, No. 1, pp. 29-41.

Stevens, M. N., & Atkins, E. M. (2016). Multi-Mode Guidance for an Independent Multicopter Geofencing System. In *16th AIAA Aviation Technology, Integration, and Operations Conference* (Vol. 1–0). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2016-3150

Stevens, M. N., & Atkins, E. M. (2018). Geofencing in Immediate Reaches Airspace for Unmanned Aircraft System Traffic Management. In *2018 AIAA Information Systems-AIAA Infotech @ Aerospace* (Vol. 1–0). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2018-2140

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication (SP) 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82r2; p. NIST SP 800-82r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

Strohmeier, M., Schäfer, M., Lenders, V., & Martinovic, I. (2014). Realities and challenges of nextgen air traffic management: The case of ADS-B. *IEEE Communications Magazine*, *52*(5), 111–118. https://doi.org/10.1109/MCOM.2014.6815901

Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., & Martinovic, I. (2017). On Perception and Reality in Wireless Air Traffic Communication Security. *IEEE Transactions on Intelligent Transportation Systems*, *18*(6), 1338–1357. https://doi.org/10.1109/TITS.2016.2612584

Strohmeier, M., Schäfer, M., Smith, M., Lenders, V., & Martinovic, I. (2016). Assessing the impact of aviation security on cyber power. *2016 8th International Conference on Cyber Conflict (CyCon)*, 223–241. https://doi.org/10.1109/CYCON.2016.7529437

Suciu, G., Scheianu, A., Vulpe, A., Petre, I., & Suciu, V. (2018). Cyber-Attacks – The Impact Over Airports Security and Prevention Modalities. In Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *Trends and Advances in Information Systems and Technologies* (pp. 154–162). Springer International Publishing. https://doi.org/10.1007/978-3-319-77700-9_16

Swanson, M. M., & Lennon, E. B. (2001). *Security Self-Assessment Guide for Information Technology Systems*. https://www.nist.gov/publications/security-self-assessment-guide-information-technology-systems-0

Takeichi, N. (2017). Nominal flight time optimization for arrival time scheduling through estimation/resolution of delay accumulation. *Transportation Research Part C: Emerging Technologies*, *77*, 433–443. https://doi.org/10.1016/j.trc.2017.01.025

Tezza, D., & Andujar, M. (2019). The State-of-the-Art of Human–Drone Interaction: A Survey. *IEEE Access*, *7*, 167438–167454. https://doi.org/10.1109/ACCESS.2019.2953900

The Green Grid. (2010). *Carbon Usage Effectiveness (CUE): A Green Grid Data Center Sustainability Metric | The Green Grid* (Christian Belady, Microsoft, Ed.). https://www.thegreengrid.org/en/resources/library-and-tools/241-WP

The Local. (2017, February 28). *Turkish suspect identified in Vienna airport cyber attack*. https://www.thelocal.at/20170228/suspect-identified-in-vienna-airport-cyber-attack

The Times of Israel. (2018). *Screens at Iran airport said hacked with anti-regime messages*. https://www.timesofisrael.com/screens-at-iran-airport-said-hacked-with-anti-regime-messages/

Theocharidou, M., Melkunaite, L., Eriksson, K., Winberg, D., Honfi, D., Lange, D., Guay, F., & Lin, L. (2016). *IMPROVER D1.3 Final lexicon of definitions related to Critical Infreastructure Resilience*. http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-38983

Thomas, A., Leboucher, V., Cotinat, A., Finet, P., & Gilbert, M. (2019). UAV Localization Using Panoramic Thermal Cameras. In D. Tzovaras, D. Giakoumis, M. Vincze, & A. Argyros (Eds.), *Computer Vision Systems* (pp. 754–767). Springer International Publishing. https://doi.org/10.1007/978-3-030-34995-0_69

Transportation Research Board. (2009). *A Transportation Research Program for Mitigating and Adapting to Climate Change and Conserving Energy: Special Report 299*. https://doi.org/10.17226/12801

Urban, J. (2016). *Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry* (SSRN Scholarly Paper ID 2787476). Social Science Research Network. https://doi.org/10.2139/ssrn.2787476

US Department of Energy. (2007). *21 Steps to Improve Cyber Security of SCADA Networks*. The IT Law Wiki. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

US DHS. (2013). *ISC PPD-21 Implementation White Paper | CISA*. https://www.cisa.gov/publication/isc-ppd-21-implementation-white-paper

US EPA, O. (2015, September 10). *Carbon Pollution from Transportation* [Overviews and Factsheets]. US EPA. https://www.epa.gov/transportation-air-pollution-and-climate-change/carbon-pollution-transportation

U.S. Government Accountability Office (GAO). (2018). *Key Issues: Unmanned Aircraft Systems*. https://www.gao.gov/key_issues/unmanned_aerial_systems/issue_summary

USA Today. (2019). *British Airways hack: Credit card details of 380,000 stolen*. Associated Press. https://www.usatoday.com/story/travel/flights/todayinthesky/2018/09/07/british-airways-hack-credit-card-details-stolen/1223887002/

Wahl, B., Feudel, U., Hlinka, J., Wächter, M., Peinke, J., & Freund, J. A. (2017). Conditional Granger causality of diffusion processes. *The European Physical Journal B*, *90*(10), 197. https://doi.org/10.1140/epjb/e2017-80015-x

Wall, T. A., Meyer, M. D., Technical Activities Division, Transportation Research Board, & National Academies of Sciences, Engineering, and Medicine. (2013). *Risk-Based Adaptation Frameworks for Climate Change Planning in the Transportation Sector* (p. 22462). Transportation Research Board. https://doi.org/10.17226/22462

Wang, Y.-J., Cao, Y.-K., Zhu, C.-P., Wu, F., Hu, M.-H., Barzel, B., & Stanley, H. E. (2017). Characterizing departure delays of flights in passenger aviation network of United States. *Scientific Reports*, *10*(1), 6890. https://doi.org/10.1038/s41598-020-62871-6

Wang, Y.-J., Cao, Y.-K., Zhu, C.-P., Wu, F., Hu, M.-H., Barzel, B., & Stanley, H. E. (2020). Characterizing departure delays of flights in passenger aviation network of United States. *Scientific Reports*, *10*(1), 6890. https://doi.org/10.1038/s41598-020-62871-6

Weaver, M. (2015, October 13). MH17 crash report: Dutch investigators confirm Buk missile hit plane - live updates. *The Guardian*. https://www.theguardian.com/world/live/2015/oct/13/mh17-crash-report-ukraine-live-updates

Webber, J. (2012). A programmatic introduction to Neo4j. *Proceedings of the 3rd Annual Conference on Systems, Programming, and Applications: Software for Humanity - SPLASH '12*, 217. https://doi.org/10.1145/2384716.2384777

Wells, D. (2019). *CTED TRENDS ALERT*. 7.

Wild, G., Murray, J., & Baxter, G. (2016). Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters. *Aerospace*, *3*(3), 22. https://doi.org/10.3390/aerospace3030022

Wilkinson, G. (2014). *Digital Terrestrial Tracking: The Future of Surveillance*. Undefined. /paper/Digital-Terrestrial-Tracking%3A-The-Future-of-Wilkinson/07a508ddd6cc3eadd1f0743e7acf8a38db467703

Willows, R., Reynard, N., Meadowcroft, I., & Connell, R. (2003). *Climate adaptation: Risk, uncertainty and decision-making. UKCIP Technical Report* [Publication - Report]. Climate Adaptation: Risk, Uncertainty and Decision-Making; UK Climate Impacts Programme. http://www.ukcip.org.uk/wordpress/wp-content/PDFs/Risk.pdf

Wit, J. J. M. de, Harmanny, R. I. A., & Prémel-Cabic, G. (2012). Micro-Doppler analysis of small UAVs. *2012 9th European Radar Conference*, 210–213.

Yuventi, J., & Mehdizadeh, R. (2013). *A critical analysis of Power Usage Effectiveness and its use in communicating data center energy consumption*. https://doi.org/10.1016/J.ENBUILD.2013.04.015

Zan, T. D., Fabrizio, d'Amore, & Federica, Di Camillo. (2016). The Defence of Civilian Air Traffic Systems from Cyber Threats. *Istituto Affari Internazionali (IAI)*, 67.

Zhang, P., Yang, L., Chen, G., & Li, G. (2017). Classification of drones based on micro-Doppler signatures with dual-band radar sensors. *2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL)*, 638–643. https://doi.org/10.1109/PIERS-FALL.2017.8293214

Zhu, G., & Wei, P. (2016). Low-Altitude UAS Traffic Coordination with Dynamic Geofencing. In *16th AIAA Aviation Technology, Integration, and Operations Conference* (Vol. 1–0). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2016-3453

Zou, B., & Hansen, M. (2014). Flight delay impact on airfare and flight frequency: A comprehensive assessment. *Transportation Research Part E: Logistics and Transportation Review*, *69*, 54–74. https://doi.org/10.1016/j.tre.2014.05.016