Journal of the Air Transport Research Society 2 (2024) 100011

Contents lists available at ScienceDirect

Journal of the Air Transport Research Society

journal homepage: www.elsevier.com/locate/jatrs

Mitigation of operational impacts on airports by early awareness of malicious events impacting linked critical infrastructures

Florian Piekert[a,*], Meilin Schaper[b], Tim H. Stelkens-Kobsch[c], Andrei-Vlad Predescu[d], Yves Günther[a], Nils Carstengerdes[a]

[a] DLR - German Aerospace Center, Institute of Flight Guidance, Department of Human Factors, Germany
[b] DLR - German Aerospace Center, Institute of Flight Guidance, Department of Controller Assistance, Germany
[c] DLR - German Aerospace Center, Institute of Flight Guidance, Department of ATM Simulations, Germany
[d] Airbus Defence and Space GmbH, Germany

ARTICLE INFO

Keywords:
Security
Resilience
Critical infrastructure
Situation awareness
Airport operational impact
Collaborative decision making

ABSTRACT

This paper introduces to security management that is conducted at infrastructure installations and their corresponding technical assets. Malicious activities at those infrastructures lead to a loss of service provision or can even introduce cascading effects towards other connected infrastructures. If an infrastructure satisfies a significant societal need, it is considered a critical infrastructure. The cascading effects can cause secondary effects at the connected infrastructures, such as airports. Airport operations are central to long-distance societal mobility and even small disruptions have knock-on effects throughout the air transport network. The cascading effects that can affect the airport and that originate at linked infrastructures and real-time use of the corresponding information for airport management and collaborative decision-making purposes in an Airport Operations Center are not well known. In what operational way can an Airport Operations Center make use of early awareness of and information about attacks on linked critical infrastructures? In how far do attacks on separate, but interconnected critical infrastructures have an effect on the operations of an airport? By looking at the existing state of the art and ongoing projects in infrastructure security research, disaster and airport management, this paper conducts a gap identification. The identified weaknesses and limitations are already partially addressed by current research projects. What is still unknown is the necessary airport-centric security management view in order to answer the research question. As a consequence, this paper proposes ideas for future necessary airport-centric infrastructure security research.

1. Introduction

The motivation for this work was driven by the question what operational impact at an airport happens if a connected Critical Infrastructure (CI) fails due to it being a target of malicious activities and how higher-level airport management would be involved to mitigate further cascading effects on airport operations. There are several CIs that an airport is connected to. These can be energy, water, banking and finance, space, data and cloud, communication, transport to and from the airport to name just a few.

CIs include a great variety of different organizations and installations. Aspects that elevate these entities to the level of a CI usually are reflected by the significance of the impact if they fail to operate, Moteff et al. (2003) explain this in detail. For this work it is sufficient to understand that CIs are organizations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences. This includes other linked infrastructures or organizations connected to the CIs and can be applicable to local, regional, national or even multi-national infrastructures. In the case of power plants, their electricity lines that supply power to cities and bigger hubs that provide mobility to citizens or goods like ports or airports this becomes immediately clear.

The recent terroristic manipulation of the North Stream gas pipelines deep in the Baltic Sea or the targeted destruction of the Kachowka dam and its hydroelectric power station in Ukraine[1] are just two very present examples of why it is necessary to physically protect CIs and detect any

[1] https://www.wilsoncenter.org/blog-post/aftermath-kakhovka-dam-collapse

* Corresponding author.
E-mail addresses: Florian.Piekert@DLR.DE (F. Piekert), Meilin.Schaper@DLR.DE (M. Schaper), Tim.Stelkens-Kobsch@DLR.DE (T.H. Stelkens-Kobsch), Andrei-Vlad.Predescu@AIRBUS.COM (A.-V. Predescu), Yves.Guenther@DLR.DE (Y. Günther), Nils.Carstengerdes@DLR.DE (N. Carstengerdes).

https://doi.org/10.1016/j.jatrs.2024.100011

type of targeted malicious act as early as possible in order to mitigate or in the best case entirely prevent such outcomes. Cyber related attacks, e.g. break-in and theft in crypto-currency brokers, can cause financial damage. If control systems of industrial companies or power plants are targeted, cyber-attacks can result in possibly wide-spread physical damage based on a non-physical attack. Another example of this kind could be a cyber manipulation of hub airline systems that impacts the check-in or the entire airline process chain, leaving thousands of passengers stranded. The amount of cyber-attacks in the aviation domain has risen over the past years according to EUROCONTROL EATM-CERT[2] and based on the independent 2022 analysis of KonBriefing.[3]

Going one step further, an attack on one CI may not only affect operations on the targeted CI, but may also impact interrelated CIs. One example for this could be a power plant failing to provide power to an airport or a hospital. This is the reason why recent EU Commission funded security research projects (e.g. PRAETORIAN[4] and PRECINCT[5]) aimed to fill a gap in security research by focusing on interrelated CIs of different domains. The general assumption seems to be that the consideration of possible cascading effects could optimize the way in which such effects can be handled. That is, knowledge about an ongoing attack at another CI as well as its potential consequences might enable a second, linked CI to adapt its response in some way.

Since an airport is a CI itself, the question arises in what way the availability of information about cascading effects at linked CIs would be used by the higher-level airport management within an Airport Operations Center (APOC) if these became available. Further, how the usage of this information would differ from information about e.g. expected weather-related impacts. Operational decision making in an APOC is related to the core problem of balancing available capacity against the demand of flights or corresponding handling activities, as has been explained in varying level of details by e.g. Ball et al. (2007) or as focused on by EUROCONTROL (2013) and Piekert et al. (2017b). Any security related event, either at the airport or coming as a cascading effect from other infrastructures (e.g. manipulation of a fuel pipeline from a refinery to the airport fuel tanks) or as Polater (2018) has analyzed in his survey coming from non-aviation related disasters, has the potential of influencing any of these demand-capacity balancing processes. Further, as climate change continues to develop, corresponding hazards pose threats to airport operations as has been dissected by the Voskaki et al. (2023) survey with the strong suggestion to each airport operator to develop climate hazard risk mitigation plans. Similarly, it is assumed that security related risk mitigation plans exist at airports, possibly for each airport stakeholder organization. While climate impacts could be rather straightforward in identification, the security related assessment understandably is kept from public eyes to not pinpoint on potential target angles.

Security at and within the airport today has to address physical and cyber aspects and units such as the Security Control Center (SOC) are responsible for the procedures. While especially smart airports have to put further emphasis on cyber security (Koroniotis et al., 2020 provide an up-to-date view), all already deal with physical security related situations within the airport and their mitigation means. One example of such a situation is the detection of unattended luggage. Established procedures are already in place to resolve the potential threat and cybersecurity tools can support to detect such situations earlier. Additionally, the impact of the threat (disruptions of the normal airport operations) is communicated to the APOC. Thereby, capacity constraints can be considered in the operational planning of each involved stakeholder, raising individual and mutual situation awareness. In this example, these are caused by the closure (of parts) of the terminal, which leads, for example, to passengers not being able to reach the gates. In the APOC, the planning for the affected flights is adjusted as a result based on the demand capacity balancing approach as mentioned above. While APOC operators are aware of events internal to the airport that might impact local operations, it is questionable whether this is also the case for impacts originating from external events related to CIs that an airport is connected to. The other way around has been in the focus of research by e.g. Sun et al. (2020) regarding impacts on cities due to airport outages or Sun and Wandelt (2021) regarding the impact on the ATM network. Following the Total Airport Management (TAM) notion of airside, landside and ground access, Xu et al. (2023) underline the need for collaborative, multimodal decision-making approaches in case of disruptions in either transport mode due to its interdependencies and this again leads back to the research question since the multimodal transport nodes can be considered as linked CIs.

The following section will provide an overview of the state-of-the-art in higher-level airport operational management in order to convey a more detailed idea of an APOC's manner of functioning and the different processes it is connected to and that it manages.

2. Total airport and performance based airport management

Airport management is required to operate an airport. Consequently, airport management has to deal with any event that the airport is subjected to, including any malicious activity on physical or cyber level. The degree of involvement in countering, mitigating or recovering after such an incident is probably different based on the event outcome and target.

The airport management has evolved especially for the big hub airports in Europe over the past decade, driven by the need to optimally use existing capacity and to compete with future challenges of deeply interlinked operations. The topic has also been taken up in the international context and is included in various European research and development programs. One of these is SESAR, which is the technological pillar of the Single European Sky (SES).[6] It aims to improve ATM by defining, developing, validating and deploying innovative technological and operational ATM solutions (Undertaking, 2015). Piekert et al. (2017a) in depth explained SESAR's approach for a harmonized European airport management development. Following the TAM philosophy (Eriksen & Meier, 2006; Günther et al., 2006), the management of big hubs will be organized on a higher level by the APOC, which will provide the Airport Operations Plan (AOP) and where decisions are taken in a collaborative manner between the stakeholder representatives with a longer lead time (e.g. one hour until the next day). On a physical level it is housing stakeholder representatives of various operating entities, including e.g. airlines, the airport itself, air traffic control, security/border control and more (see Fig. 1). As such though, the APOC does not directly interrelate to infrastructure or cyber-security measures taken in ad-hoc situations or on operational level, but its involvement is required to resume operations in the recovery phase after security related or critical events. Further, the APOC itself could be the target of a directed attack on either level, rendering it inoperative or by manipulation of the provided AOP information creating impacts in the connected organizations.

In case of events that threaten to impact the airport's overall performance (usually focused on flight operations and corresponding key metrics; Helm et al., 2015; Kosanke & Schultz, 2015), the APOC stakeholders jointly decide via suitable collaborative decision-making procedures and tool support (Papenfuss et al., 2017; Piekert et al., 2023; SESAR, 2020) on the best mitigation approach. Such events include weather related, capacity shortage due to staffing, construction work or equipment issues, breaches of security inside the terminal and on the apron

[2] https://www.aviationtoday.com/2021/07/12/new-eurocontrol-data-shows-airlines-increasingly-becoming-targets-cyber-attacks/

[3] https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html

[4] https://praetorian-h2020.eu/

[5] https://www.precinct.info/

[6] https://transport.ec.europa.eu/transport-modes/air/single-european-sky_en

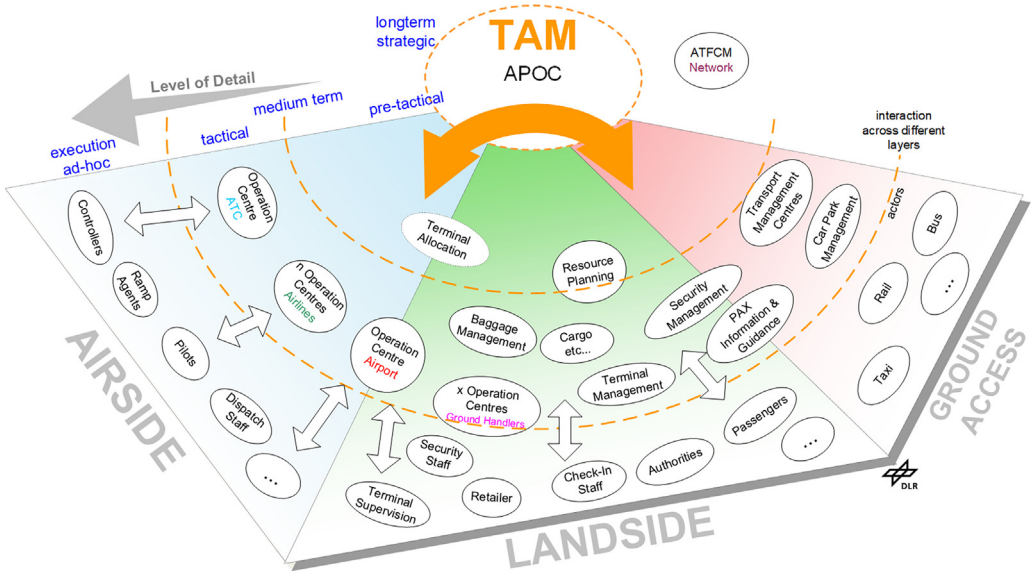

Fig. 1. Total Airport Management operational processes pyramid (Fig. 1 in Piekert and Strasser (2010)).

Fig. 2. Simplified chain of security management.

area, left behind baggage or even accidents/incidents. This high-level decision taken in the APOC how to operate the airport is then broken down in the individual stakeholder operation centers, down to the individual flight or process step. Depending on the types of events, tool support offers prediction capability. This capability can show the anticipated impact of adverse weather or disruptions of landside operations. This allows for a more homogeneous information and reliability level than just relying on personal experience of the different team members. Input to the predictions are operational data of the various processes coming from the different stakeholders and all this data is stored in the AOP.

The management of small and medium type airports does not require such a sophisticated APOC infrastructure element and predictions most often are based on the experts' judgement that are in control of the operations during their shifts. Nevertheless, based on the airports' needs, collaborative decision making does happen between those airport stakeholders, with less complex tool support and with a "light" version of the AOP. Since airports are not isolated nodes in the air transport network, their (in-)direct dependency upon each other (sink and source of flight operations) is very obvious. The controlling entity that governs and regulates the traffic flows is the Network Manager (European Commission, 2011). In close collaboration with the national Air Navigation Service Providers (ANSPs) it issues and maintains flow predictions of the various aerial sectors or airport destinations and ensures their adherence. In this regard the airports and the ATM network build a dependency network of CIs on an ATM operational service level, not necessarily on a physical link level. ATM events at one airport may impact others, but possibly the effect can be anticipated sufficiently and predicted reliably by these actors. Physical attacks on an airport CI do not necessarily introduce cascading physical effects in other airports, but maybe on the ATM layer.

The following section will describe the state of the art regarding security research for and among CIs, as well as more recent research dealing with interconnected CIs. Gaps in this research are identified and the need for future research in the context of airports is discussed.

3. Research on security - state of the art

In this section, we will address the state of the art in security management research. In order to establish a general understanding of what the term security management entails, Fig. 2 illustrates a simplified chain of steps typically incorporated in security management systems (adapted from National Institute of Standards and Technology, 2023). First of all, sensors are required in order to detect events that are possibly related to an attack (e.g. cameras or cyber sensors). Secondly, the gained information of an ongoing or already occurred event on singular or multiple seemingly unrelated or linked elements needs to be analyzed according to criteria. Not all detected events by the sensors are malicious, only if they fulfil previously defined criteria. In the case of a positive detection of non-authorized activity, responsible operators need to be informed in a meaningful way. This is then followed by a reaction or countermeasure and lastly, recovery and prevention. This last step is highly specific to each project and CI and therefore not further addressed in this work.

A considerable number of research projects on European and national level have dealt with the protection of CIs (covering the above chain in different levels of intensity) and, judging from existing (European Commission, 2023a) and anticipated research calls, more are necessary. It is good practice for new research projects to consider previous project results in order to take over promising approaches. Predescu et al. (2023) conducted an analysis of different approaches for security management systems so far used in previous security projects. Most of the analyzed projects addressed the entire attack and mitigation chain for e.g. a specific CI or business process chain. This includes the detection of an attack by sensors, the data correlation and analysis, the appropriate information provision to operators and possibly the support in countering this event. The knowledge and implementations based on these previous projects can be considered state-of-the-art for this area.

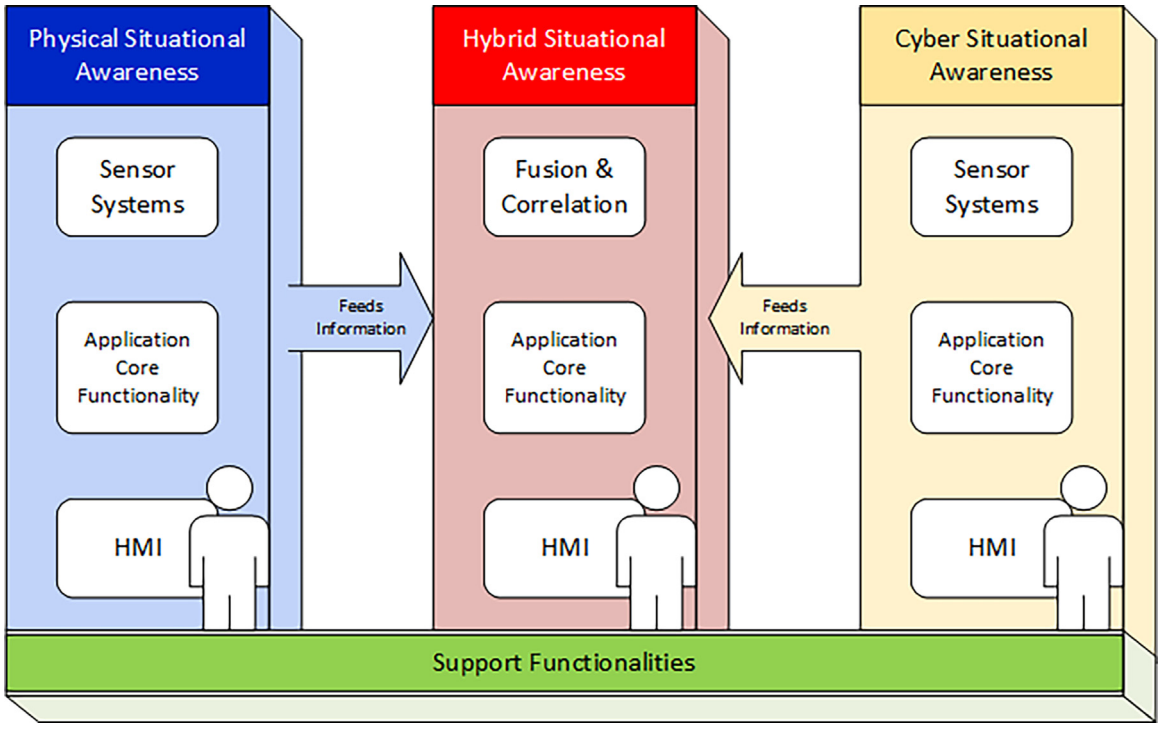

Fig. 3. Functional pillars and link between PSA, CSA, HSA and support functions.

Other, not less important projects were conducted even in previous European Commission funded programs, e.g. the GAMMA (Global ATM Security Management) project[7] or the security related projects in the SESAR[8] (Single European Sky ATM Research) work program mentioned. These will be incorporated later in this section Security Research in Air Traffic Management. The domain categories that had been addressed by 21 of the 22 projects analyzed by Predescu et al. (2023) were:

- Port/Maritime
  - SAURON (König et al., 2019),
  - PIXEL (Široka et al., 2021),
  - MITIGATE (Duzha et al., 2017), and
  - MEDUSA (Papastergiou et al., 2018).
- Airport
  - SATIE (Burke et al., 2021; Stelkens-Kobsch et al., 2021).
- Railway
  - SAFETY4RAILS (Crabbe et al., 2022).
- Energy/Water
  - DEFENDER (Di Orio et al., 2020),
  - SECUREGAS (Mantzana et al., 2021), and
  - STOP-IT (Ugarelli et al., 2021).
- Medical
  - SAFECARE (Atigui et al., 2020).
- IT/Comms
  - RESISTO (Neri et al., 2020),
  - FINSEC (Dattani et al., 2020),
  - 7SHIELD (Gkotsis et al., 2023),
  - ENSURESEC (Francaviglia et al., 2021),
  - HYRIM (Busby et al., 2016), and
  - PREVISION (Demestichas et al., 2020).
- Industry
  - InfraStress (Caleta et al., 2020).
- Overarching
  - PRECINCT (König et al., 2022),
  - LETS-CROWD (Dambra et al., 2019),
  - DroneWise[9], and
  - FORTRESS (Pescaroli & Alexander, 2016).

3.1. Main pillars of security management

The majority of the analyzed projects recognized the need to correlate externally sourced physical with cyber-attacks in a hybrid approach. The term hybrid only refers to the civil perspective in this work and refers to combined cyber and physical attacks. Four main pillars (see Fig. 3) of security management can be identified from the above projects, following the SAURON nomenclature:

- Physical Situational Awareness (PSA),
- Cyber Situational Awareness (CSA),
- Hybrid Situational Awareness (HSA), and
- Support Functionality (e.g. Emergency Population Warning Systems EPWS or Impact Propagation Simulation IPS or Decision Support Systems DSS).

The aforementioned projects addressed the four pillars according to their needs and focal areas. In general, each pillar (except the support functionality pillar) has either sensors and/or fusion/correlation as input, some sophisticated core functionality and varying human-machine interfaces (HMI).

Sensors are directly linked to situation awareness as they are the means of detection. Physical sensors can, e.g., include proximity, noise or smoke detectors or cameras. Cyber sensors can include, e.g., intrusion detection, anti-malware, firewalls, or customized survey scripts. In case information between physical and cyber events is correlated, this is referred to as a hybrid sensor.

Regarding data analysis and attack identification (i.e. the identification of meaningful events or the correlation of events), different

[7] https://www.gamma-project.eu/
[8] https://transport.ec.europa.eu/transport-modes/air/welcome-sesar-project_en
[9] https://dronewise-project.eu/

projects have developed correlation functionalities. For example, a Reasoning Engine (STOP-IT) or cyber-physical event correlators (e.g. RESISTO, SAURON, SATIE, FINSEC, InfraStress, 7SHIELD) that address intra-physical (PSA only), intra-cyber (CSA only) and/or hybrid (HSA) events. Simply put, what they have in common is the correlation of events happening at the same time or in timely sequence that could be related to an attack. The individual correlation approaches differ based on e.g. architecture, used sensor systems and asset models.

Once such events are identified, responsible operators get informed. The projects foresee different methods of displaying this information, these range from log excerpts by email to more complex and sophisticated HMIs, allowing dynamic interaction with the provided information.

Some projects take this further, paying tribute to the fact that any detected attack might be the entry key to follow-up attacks on other assets of the same CI or possibly even act as a decoy. Based on modelling of the relationship of assets, their (inter-)dependencies and known relevance to operations as a whole, risk probability models allow to guesstimate possible follow-up targets as cascading effects. The functionality differs between the individual projects, but the overall approach is similar. From Risk Predictor (RESISTO), via Threat Propagation Engine (TPE; e.g. SAURON, HYRIM) to impact propagation tools (e.g. SATIE, SAFECARE, FORTRESS, MITIGATE, MEDUSA), such tools provide additional information about possible future consequences to the operators, allowing preparation, mitigation or counter-measures appropriately. SATIE proposed an ontology to harmonize understanding technically (e.g. attributes and structural elements in exchanged messages) for the correlation as well as the used vocabulary - when interpreting the results (Canito et al., 2020) and helps to prevent misunderstandings when communicating across CI boundaries with other responsible operators.

The support functionality pillar is more diverse. It can include tools for e.g. disclosing information to the public, tools that provide decision support or integration of first responder teams. Some projects foresee an emergency population warning system (e.g. SAURON, STOP-IT) or suitable interfaces for transmitting information to the local/national authorities that are responsible for the information dissemination to the public based on the applicable regulations (e.g. distribution via first responders). Some provide decision support functionality (e.g. RESISTO, SAFECARE, 7SHIELD, SAFETY4RAILS) to operators, tapping on internal databases that contain, e.g. lessons learned from previous events, crisis or emergency procedures easily accessible, or guidance on the best choice for risk treatment. Sometimes the boundary between one of the awareness pillars and the transversal support functionality does not exist as functionality is directly implemented into the former.

3.2. Intra- and inter-CI security management

Most of the analyzed projects focused on a specific type of CI or digital service and stayed more or less within the boundaries of that CI or directly connected systems, e.g. intra-industrial, intra-space, intra-port, intra-airport, intra-financial or intra-commercial systems or intra-healthcare related infrastructures. Some projects targeted the provision of enhanced cyber-crime fighting capabilities for Law Enforcement Agencies. Several projects introduced cross-CI supply-chain risk assessment methodologies (e.g. MEDUSA, MITIGATE or PIXEL). Predescu et al. (2023) state that from the point of industrial suppliers and infrastructure operators only SATIE focused on the airport critical infrastructure, while the others focused on non-airport critical infrastructure-specific solutions. A few projects looked beyond the addressed single CI's physical or IT boundary, not limited to a local or regional perspective. E.g. SECUREGAS covered the value-chain from production to distribution with focus on the European gas network beyond regional CI influence and FINSEC addressed the cyber-physical security of the financial supply chain, while MITIGATE looked at the cyber security of the supply chain from a port-oriented point of view, stretching beyond the port CI.

Two projects addressed multiple CIs beyond regional aspects and, to a degree, their inter-dependencies or relationships. PRECINCT focusses on multimodal transport, energy, water, and ICT/telecoms with digital twins. The goal of PRECINCT is to supervise and control complex interdependent networks and cyber-physical systems of systems with distributed ownership and management structures. This project can be considered PRAETORIAN's sister project, as both started in parallel and ended in autumn 2023. The other project that extends its view beyond a single CI's boundary is FORTRESS. Crisis situations are difficult to overcome on their own, but things can easily turn for the worse and lead to higher magnitude consequences. The FORTRESS project aimed to gain a greater understanding of these cascading effects and provide stakeholders (crisis managers and infrastructure providers) with tools to cope better with these complex phenomena during possible crises across European borders. That incidents in CIs can develop into crisis is self-explanatory, however the cascading effects are a factor that can make events even worse.

SATIE (Georgiou et al., 2019) addressed interconnected CIs as external stakeholders to the airports' crisis management, whereas crises could be caused intentionally (e.g. by attacks). The interconnected CIs could participate in the AOC/APOC during the crisis response step. The recovery phase shall be used to stabilize operations, which could be seen as a step toward pre-tactical planning in the TAM/Performance based-airport management (done in the APOC), which in consequence impacts the ATM network.

3.3. Security research in air traffic management

In ATM and aviation in general, the need to consider security on another level started with the devastating 9-11 attacks in 2001. This changed air transportation forever - it also changed the way to look on and deal with security. Security began to receive increased attention and research was intensified to secure air transport. In contrast to the physical protection of CIs introduced above, a focus of the ATM related security research was the protection of ATM services. The organizations providing these services and their physical infrastructures are subject to the application of the above approaches.

The European 7th Framework Program (FP7; 2007-2013) project GAMMA spotted at cyber security, communication navigation and surveillance security, physical infrastructure security and crisis management, all in the ATM domain. Detected events were sent to so-called Local GAMMA Security Operations Centers (LGSOCs) and correlated based on rules. Each LGSOC could send the information to the corresponding National GAMMA Security Management Platform (NGSMP). These NGSMPs are provided with advanced functions and additional control capabilities, which are not available at the local level. The NGSMP operators can share information with the European GAMMA Coordination Center (EGCC) (Montefusco et al., 2016). Schaper et al. (2017) indicate benefits of fusing local security data on national level as well as incident management on national level; nevertheless, there shall be the possibility to sanitize data before sharing. From our understanding sanitization could include, e.g., removal of state or business confidential data.

As SESAR is the technological pillar of the SES, it is responsible to provide innovative solutions for ATM security as well. The European Commission has already established common rules in the field of civil aviation security aimed at protecting persons and goods from unlawful interference since 2002. This has been taken up by SESAR from its first program installment (SESAR 1, 2004–2016). However, the foundations to foster security as such in SESAR has been laid merely at the end of the first SESAR cycle when the SESAR ATM Security Risk Assessment Methodology (SecRAM) was developed and postulated initially by one of the dedicated projects of SESAR.

This methodology was further improved by the SESAR cyber security task force in 2017 and developed to its current version 2.0 (Le Fevre et al., 2017). Projects being funded by SESAR 2020 (2016 – 2024) had to conduct a security risk assessment following the guidance of SecRAM

2.0 and take measures accordingly to assure a secure set up of their architecture and processes as well as operations. This ensured that all new developments followed a kind of security-by-design approach and that had to be considered even by already existing solution in retrospect. This had the positive side-effect that all participants of SESAR 2020 received training on how security aspects have to be considered and are now sensitized to apply this for further developments. This so-called security culture will also be beneficial for the developments, innovations and deployments which will follow in the SESAR 3 multi-annual work program (2021–2031; SESAR 3 Joint Undertaking, 2022).

It is worth noticing that the current Horizon Europe work program for civil security research (European Commission, 2023a) does not mention airports at all. The topic airport is included in the "Climate, Energy and Mobility" research program (European Commission, 2023b), however this does not include security research aspects of linked CIs and the SESAR 3 program is a sub program of this Horizon Europe program. The airport as a node in a network of linked CIs is not addressed in the SESAR 3 program. However, SESAR 3 still addresses the need to provide cyber-security to the aviation infrastructure as a CI, showing that previous and ongoing efforts are not closing all possible gaps.

4. Weaknesses or limitations of state of the art

Each of the security research activities and projects aforementioned had contributed greatly towards the goal of increasing the resilience and protection of CIs. Many of these addressed the challenge with unique approaches and built on previous research results. However, as research is a continuous activity in which the knowledge is pushed beyond the boundaries of the state of the art, it can be understood that certain limitations may exist as laid out by Predescu et al. (2023).

The current state of the art research had mostly been considering the challenge of protecting the CIs only within the context defined by each type of infrastructure (e.g. communications, transportation or healthcare). This approach provides a good coverage of the threats posed to each individual CI, while also considering their specific industry particularities, therefore allowing an efficient development of associated threat mitigations and defense measures. Nevertheless, it can be argued that this approach is limited in some sense when threats posed by failures in protecting adjacent CIs are not considered. In current times, CIs are widely interconnected through the supply of critical services from one to another. The lack of consideration of cases in which the disruption of a critical service in one CI results in a cascading effect in another is a limit that needs to be overcome.

With respect to cascading effects caused by disruptions in interconnected CIs, the geographical context is also of high concern and not emphasized enough in current state of the art as very few research efforts have considered this aspect. CI protection and threat landscape definition should not be limited to geographical borders. When the CI is near a border region between countries, the threats of cross-border nature should be very much taken under consideration. Further consideration should be given to events that impact critical infrastructures of any kind on a cross-border level. This matter can be considered as a weakness and it should be taken into account with more in the future research activities and projects.

In the aviation sector, security research is well implemented regarding the protection of the individual Air Traffic Management related services. This includes e.g. the manipulation of essential data exchange or detection of malicious use of the voice radio channels in airport vicinities giving commands or confirmations that could develop into threat situations (Schaper et al., 2017). Whether such an occurrence leads to an operational impact on the airport, e.g. the extend of flight operations flow reduction, is yet unknown and hence, no automatic correlation and impact prediction exists. Only the knowledge of operational experts, which is highly specific to each airport, can answer this eventually. However, for more often occurring security related events that happen at the airport, these introduce an operational impact that is well known to the airport management and the operation centers involved. These events comprise e.g. left along baggage in the terminal or a passenger passing security control without being checked or some person appearing on the apron area without permission. In contrast, what is missing is the operational impact of attacks on CIs outside the airport and that introduce cascading effects into the airport, e.g. if gas or fuel pipelines from refineries in the airport vicinity to refuel airport-based tanks are the target. It is apparent that at some time after these events occur the cascading effects will impact airport operations due to refueling capacity or failing to refuel issues.

From the ATM network flow perspective, e.g. weather situations sometimes develop in such a dynamic way that operational predictions with sufficient lead time are not possible and traffic partners (airlines flying to this particular airport) are forced to adapt and possibly take an aerial holding or land at an alternate destination airport and prepare follow-on steps. Depending on the sophistication of the employed airport management approach, mitigation and recovery might be differently effective and efficiently. This could be similar to security related events and their impacts, where the time to prepare might not be sufficient enough to optimally adapt the operational plans and where the recovery needs to address these shortcomings.

The concept of TAM/PBAM (Performance Based Airport Management) is still rather new. Consequently, the APOC has to be considered as a new asset of the airport, included in all of the security risk plans. As a consequence, it means that a threat and risk assessment needs to be performed, focusing on all APOC services.

5. Most recent security research contributions

Previous security projects did important work in innovating security research. Nevertheless, Predescu et al. (2023) identified some gaps in the state of the art. For example, the recent PRAETORIAN project addressed interconnected CIs of a large set of heterogeneous sectors. This involves, for example, transport, energy and healthcare sectors. The toolset is specific and scalable according to the needs of individual CIs. Still, the calculation of possible cascading effects also for interrelated CIs enables to respond in a unified, coordinated way, e.g. by enabling communication between CIs in the context of both national and cross-border attack scenarios.

For example, one potential attack scenario including an airport was developed within the project (PRAETORIAN, 2023) and involves the theft of a sample from a laboratory which is transported to an airport across the border. The attackers plan to spread the sample at the airport with the help of a drone and inside the terminal building. Without a support system providing information about this correlation, an operator at the airport would not get notified about the stolen sample already before the attackers arrive at the airport, neither would the operator be aware that the airport has a link to the other CI. The information received includes video footage of one of the laboratory attackers, which enables airport's video analytics tools to later recognize the attacker's face in the airport area.

To achieve this cross-CI visibility of ongoing events at other CIs, the aforementioned project integrated tools already developed in other research projects like the EPWS (from SAURON, STOP-IT), a DSS (from RESISTO, SAFECARE, 7SHIELD, SAFETY4RAILS), the Threat Propagation Engine (from SAURON, HYRIM) and Impact Propagation Tools (from SATIE, SAFECARE, FORTRESS, MITIGATE, MEDUSA). This integrated system was applied to a variety of different CIs and into a CI-network and validated by a scenario-based established methodology (Stelkens-Kobsch et al., 2023).

To summarize, the PRAETORIAN project's contribution to the state-of-the-art is a holistic approach that considers cascading effects for heterogenous and geo-distributed interrelated/ interconnected/ linked CIs. Although the project addressed the airport as part of the to be protected CI network in one of the attack scenarios, the selected scenario is not

taken to the point where possible operational impacts become visible. Further, the research suggestions about APOC inclusion in security related events as reported by SATIE (Georgiou et al., 2019) were not taken aboard by it. A reason for this seemed to be that the security orientation of the project did not foresee this need to include operational airport expertise beyond security representatives for the envisaged orientation of the project. However, the project helped creating the links between different CIs (e.g. by communication means), but what the airport will do with the information is still kept open.

6. Conclusions and future research needs

Looking at the individual pieces, it is possible to state that there exists profound knowledge of security and security management when considering single CIs. Similarly, this has been developed for inter-CI relationships and even entire process chains in various domains. Further, threat impact prediction and escalation models and mechanisms for intra- and inter-CI aspects exist and have been shown by recent research projects.

On the airport and ATM side, the conducted research brought aspects of the security management research into this domain (ATM network and airport) and supports secure transport. ATM domain related predictions of operational problems exist to a large degree (e.g. weather impact or closure of runways due to maintenance, climate hazard or non-aviation disaster related influences). However, predictions of operational impacts based on security related events exist only for a few typical and well-known intra-CI security events at the airport (e.g. security events inside the airport terminal). Future research could as complimentary knowledge using the suggestions by Sun and Wandelt (2021) address the cascading effects from the airport into the ATM network based on the node's importance and network functionality. Depending on the relevance, known security events and beyond them (full picture approach) should be assessed regarding the network information needs and their operational utilization at other network nodes. As an example, it is easy to understand that the power outages at a large hub airport due to powerplant failures have a greater disruption potential than a road blockage near a small regional airport. But if this information is helpful for other network nodes needs to be assessed in subsequent research and was not in focus of our work.

Looking again at the research question "what operational impact at an airport happens if a connected Critical Infrastructure (CI) fails due to it being a target of malicious activities and how higher-level airport management would be involved to mitigate further cascading effects on airport operations", we can conclude from the above deduction that there is no operational impact prediction based on external threats coming from linked CIs outside the airport yet, although in airports' undisclosed risk assessment and mitigation plans very high-level mitigation measures might exist. Literature does not reveal whether airport operational experts have experienced such situations already and if yes, if they were sufficiently aware of the reasons why some connected CIs did not maintain their regular services. Without proper information and knowledge, they can only take assumptions on the potential impact on the CI and hence on airport operations, possibly by guidelines of those risk mitigation plans. Based on this, it is apparent that no support systems for such situations exist yet either.

Independent from the above confirmed gaps, another central question that needs to be asked is: what makes an external threat event different in handling from an event that happens inside the inter-airport-network or from an adverse weather-based event local to the airport? Will an external event's impact on airport operations be dealt with differently on operational level by the APOC decision makers?

Once research has identified suitable cascading effects' models (what e.g. can induct effects at the airport), the models can be analyzed from an operational point of view. And once this is achieved, suitable operational prediction models can be derived. The literature has already some sophisticated solutions for the airline perspective, but the holistic airport view does not exist.

Further, the way existing predictions of operational impacts are made available are not incorporated into support systems (e.g., providing all information in digital form or even decision support for the operators) or available in a complete manner. New additions based on research output should be harmonized with and incorporated into then-existing solutions. Depending on the airport size and its needs, appropriate scaling needs to be conducted. Since bigger airports have more sophisticated tools available that provide management support, consequently these predictions should be incorporated into these management tools. For smaller airports, suitable stand-alone solutions could be envisaged.

Taking the already developed ideas described above into a more specific direction, these ideas may be combined in an even more holistic approach than it was done in recent security research projects and along the envisaged SATIE gap idea. It is imaginable to collect security information from different sources belonging to different CIs, classify them according to an ontology, correlate them, predict possible impacts – in detail within the CI, on a higher level of detail to other CIs – and share the information accordingly. Related open questions, especially when information is shared cross-border, concern e.g. data protection, legislation, internal policies (e.g. CI internal or national) as well as means of filtering and appropriate visualizations. One option might be, that an operator responsible for the security at that CI has to categorize the information as an incident or an attack which would trigger automatic sharing of that incident/attack information. Since an ontology is used, every recipient would be aware of the significance of transmitted messages. The operator of the receiving CI or some centralized distribution service may have to filter whether the received information is just nice to know or if explicit actions should be triggered in response.

Tools for estimating cascading effects and impact propagation may not only be useful for other CIs but – in the airport domain – also for the APOC decision makers as a simple awareness mechanism of an ongoing threat or attack. The impacts that manifest at the airport need to be identified by the SOC in collaboration with affected operation centers and then the APOC decision makers need to be duly informed. For the planning of mitigation and recovery of operations, the APOC needs to conduct demand and capacity balancing correspondingly and then update the Airport Operations Plan (AOP) in an appropriate manner (see Fig. 4) and follow established information distribution flows.

Concluding, a lot of unanswered questions remain. Do the APOC decision makers need the information about ongoing attacks at external CIs for situation awareness? How specific and detailed does the information need to be in order to be useful in an APOC? Or do the operators only want to get involved when the end of the impact is becoming visible and the recovery phase will start and how to best restart operations again needs to be planned? Above we mainly discussed the instances in which the APOC might utilize information about security events for its own work. But what if the APOC itself is the CI asset under attack? How does this cascade into the ATM network and connected CIs? Sun and Wandelt (2021) do not entirely answer this, as maybe not an entire failure to provide operations occurs, but undetected fraudulent information exchange spoils the network. As was explained above, the information regarding malicious activities at linked CIs is currently neither available at the airport nor in the APOC. Therefore, it is not possible to achieve an early awareness about such events and as a consequence it limits the mitigation means an APOC can take on operational impacts. All in all, it becomes evident that airport operations would benefit from research approaches that combine aspects of critical infrastructure security and airport operations beyond the current state-of-the-art and literature.

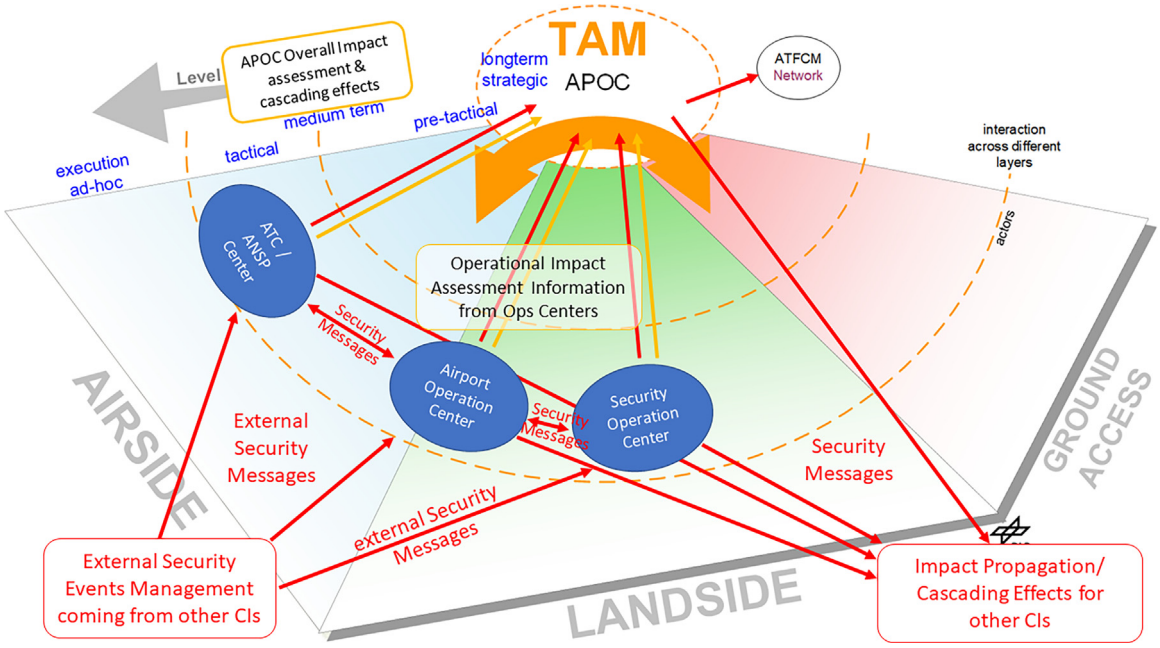

Fig. 4. Research needs for the exchange of security and operational impact messages.

CRediT authorship contribution statement

Florian Piekert: Writing – original draft. **Meilin Schaper:** Writing – original draft. **Tim H. Stelkens-Kobsch:** Writing – original draft. **Andrei-Vlad Predescu:** Writing – original draft. **Yves Günther:** Writing – review & editing. **Nils Carstengerdes:** Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Florian Piekert: Writing – original draft. **Meilin Schaper:** Writing – original draft. **Tim H. Stelkens-Kobsch:** Writing – original draft. **Andrei-Vlad Predescu:** Writing – original draft. **Yves Günther:** Writing – review & editing. **Nils Carstengerdes:** Supervision, Writing – review & editing.

Acknowledgement

This work has received funding by the EU H2020 research and innovation program under grant agreement No. 101021274 (PRAETORIAN project, https://praetorian-h2020.eu/).

References

Atigui, F., Hamdi, F., Hannou, F.-Z., Lammari, N., Mimouni, N., & Si-Said, S. (2020). Managing cyber-physical incidents propagation in health services. In *Research challenges in information science: RCIS 2020* (p. 385). Springer. https://hal.science/hal-02957720

Ball, M., Barnhart, C., Nemhauser, G., & Odoni, A. (2007). Air transportation: Irregular operations and control. *Handbooks in Operations Research and Management Science, 14*, 1–67.

Burke, K., Carstengerdes, N., Hrastnik, S., Predescu, A.-V., Papagiannopoulos, N., & Branchini, E. (2021). Demonstration of cyber-physical security solutions in SATIE–validation and lessons learned,.

Busby, J. S., Gouglidis, A., Rass, S., & König, S. (2016). Modelling security risk in critical utilities: The system at risk as a three player game and agent society. In *2016 IEEE International conference on systems, man, and cybernetics (SMC)* (pp. 001758–001763). IEEE. https://doi.org/10.1109/SMC.2016.7844492

Caleta, D., Jovanovic, A., Romano, L., & Sutton, L. (2020). InfraStress: Enhancing resilience of industrial plants against cyber-physical threats. *ITASEC 2020 - Italian conference on cybersecurity*. Ancona, Italy

Canito, A., Aleid, K., Praça, I., Corchado, J., & Marreiros, G. (2020). An ontology to promote interoperability between cyber-physical security systems in critical infrastructures. In *2020 IEEE 6th International conference on computer and communications (ICCC)* (pp. 553–560). Chengdu, China: IEEE.

Crabbe, S., Roß, K., Köpke, C., Faist, K., Medina, E. V., Siebold, U., Cazzato, E., Mádi-Nátor, A., Ben-Yizhak, E., Peled, I., et al., (2022). Safety4rails information system platform demonstration at madrid metro simulation exercise. In *Proceedings of the 32nd European safety and reliability conference, copyright*. https://doi.org/10.3850/978-981-18-5183-4_S06-14-470-cd

Dambra, C., Gralewski, A., & Arias, J. (2019). LETSCROWD: Dynamic risk assessment for mass gatherings. In *Proceedings of the 16th ISCRAM conference*. http://inis.iaea.org/search/search.aspx?orig_q=RN:53037610

Dattani, I., Mamelli, A., Polyviou, A., Soldatos, J., & Troiano, E. (2020). A reference architecture for securing infrastructures in the finance sector. *Cyber-physical threat intelligence for critical infrastructures security: A guide to integrated cyber-physical protection of modern critical infrastructures*. https://doi.org/10.1561/9781680836875.ch2

Demestichas, K., Alexakis, T., Peppes, N., Remoundou, K., Loumiotis, I., Muller, W., & Avgerinakis, K. (2020). Prediction and visual intelligence platform for detection of irregularities and abnormal behaviour. *Detection Machine Learning for Trend and Weak Signal Detection in Social Networks and Social Media, 2606*, 25–30.

Di Orio, G., Brito, G., Maló, P., Sadu, A., Wirtz, N., & Monti, A. (2020). A cyber-physical approach to resilience and robustness by design. *International Journal of Advanced Computer Science and Applications, 11*(7), 70–78. https://doi.org/10.14569/IJACSA.2020.0110710.

Duzha, A., Gouvas, P., & Canepa, M. (2017). Mitigate: An innovative cyber-security maritime supply chain risk management system. In *ITASEC* (pp. 248–252).

Eriksen, P., & Meier, C. (2006). Total airport management. http://www.bs.dlr.de/tam/Dokuments/TAM%20Leaflet%20-%20print.pdf.

EUROCONTROL (2013). *Airport CDM implementation*. EUROCONTROL. http://www.eurocontrol.int/documents/airport-cdm-implementation-manual-version-4

European Commission (2011). Commission decision of 7.7.2011 on the nomination of the network manager for the air traffic management (ATM) network functions of the single european sky, 6 1. http://ec.europa.eu/transport/modes/air/single_european_sky/doc/32011d4130.pdf.

European Commission (2023). Horizon europe work programme 2023-2024. *6. Civil security for society*. European Commission. https://research-and-innovation.ec.europa.eu/document/download/ed4ea470-af89-49d7-85c1-f9bb3039ccbd_en

European Commission (2023). Horizon europe work programme 2023-2024. *8. Climate, energy and mobility*. European Commission. https://research-and-innovation.ec.europa.eu/document/download/5d031a89-7e76-45b2-83f2-ae85e7238791_en

Francaviglia, G., Sousa, L., Theodoropoulos, C., Diaz, R., Kozik, R., Milánkovich, A., Lukács, D., Dimakopoulos, N., Nati, M., Signoles, J., Lemesle, A., Gliga, R., Daskalakis, M. T., Emmanouil Khan, & Rademacher, R. (2021). D3.4-ENSURESEC architecture. https://doi.org/10.5281/zenodo.6108384.

Georgiou, E., Mantzana, V., Chasiotis, I., Gkotsis, I., Lancelin, D., Köpke, C., Faist, K., Papagiannopoulos, N., Stelkens-Kobsch, T., Schaper, M., Déchelle, F., Branchini, E.,

Oudin, T., Perlepes, L., Hrastnik, S., Burke, K., Mangini, M., & Hervé, E. (2019). Satie d7.7 - specification of a holistic security management cycle. http://satie-h2020.eu/?smd_process_download=1&download_id=1456.

Gkotsis, I., Perlepes, L., Aggelis, A., Valouma, K., Kostaridis, A., Georgiou, E., Lalazisis, N., & Mantzana, V. (2023). Solutions for protecting the space ground segments: From risk assessment to emergency response. In *European symposium on research in computer security* (pp. 291–307). Springer.

Günther, Y., Inard, A., Werther, B., Bonnier, M., Spies, G., Marsden, A., Temme, M., Böhme, D., Lane, R., & Niederstraßer, H. (2006). *Total airport management (operational concept and logical architecture)*. DLR Ph.D. thesis.. http://www.bs.dlr.de/tam/Dokuments/TAM-OCD-public.pdf

Helm, S., Loth, S., & Schultz, M. (2015). Advancing total airport management–an introduction of performance based management in the airport context. In *Proceedings of the 19th ATRS world conference, Singapore* (pp. 2–5).

König, S., Connolly, L., Schauer, S., O'Connor, A., Carroll, P., & McCrum, D. (2022). Combining cascading effects simulation and resilience management for protecting cis from cyber-physical threats. In *Proceedings of the 32nd european safety and reliability conference (ESREL 2022). dublin*.

König, S., Rass, S., Rainer, B., & Schauer, S. (2019). Hybrid dependencies between cyber and physical systems. In *Intelligent computing: Proceedings of the 2019 computing conference: 2* (pp. 550–565). Springer.

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access, 8*, 209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728.

Kosanke, L., & Schultz, M. (2015). Key performance indicators for performance-based airport management from the perspective of airport operations. *5th International air transport and operations symposium (ATOS 2015)*. http://www.lr.tudelft.nl/fileadmin/Faculteit/LR/Organisatie/Afdelingen_en_Leerstoelen/Afdeling_C_O/Aerospace_Management_and_Operations/ATOS/Papers/2015/CATO2015_4_2_1.pdf

Le Fevre, M., Gölz, B., Flohr, R., Stelkens-Kobsch, T., & Verhoogt, T. (2017). SecRAM 2.0 security risk assessment methodology for SESAR 2020; 02.00. 00 SESAR joint undertaking: Brussels. https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf.

Mantzana, V., Georgiou, E., Gazi, A., Gkotsis, I., Chasiotis, I., & Eftychidis, G. (2021). Towards a global CIs' cyber-physical security management and joint coordination approach. In *International workshop on cyber-physical security for critical infrastructures protection* (pp. 155–170). Springer.

Montefusco, P., Casar, R., Koelle, R., & Stelkens-Kobsch, T. H. (2016). Addressing security in the ATM environment: from identification to validation of security countermeasures with introduction of new security capabilities in the ATM system context. In *2016 11th International conference on availability, reliability and security (ARES)* (pp. 532–541). IEEE.

Moteff, J. D., Copeland, C., Fischer, J. W., Resources, S., & Industry, D. (2003). *Critical infrastructures: What makes an infrastructure critical?*. Congressional Research Service, Library of Congress Washington, DC.

National Institute of Standards and Technology (2023). Framework for Improving Critical Infrastructure Cybersecurity. *Cybersecurity Framework 2.0 Initial Public Draft*. Gaithersburg, MD, USA: National Institute of Standards and Technology.

Neri, A., Neri, A., et al., (2020). RESISTO - Resilience enhancement and risk control platform for communication infrastructure operators. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security*.. https://doi.org/10.1561/9781680836875.ch17.

Papastergiou, S., Polemi, N., & Kotzanikolaou, P. (2018). Design and validation of the medusa supply chain risk assessment methodology and system. *International Journal of Critical Infrastructures, 14*(1), 1–39.

Papenfuss, A., Carstengerdes, N., Schier, S., & Günther, Y. (2017). What to say when: Guidelines for decision making. In *An evaluation of a concept for cooperation in an APOCg, twelfth USA/europe air traffic management research and development seminar (ATM2017)* (pp. 26–30). https://elib.dlr.de/111849/

Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards, 82*, 175–192. https://doi.org/10.1007/s11069-016-2186-3.

Piekert, F., Carstengerdes, N., Schier, S., Suikat, R., & Marsden, A. (2017). A high-fidelity artificial airport environment for SESAR APOC validation experiments. *Journal of Air Transport Studies, 8*(1), 31–50. http://etem.aegean.gr/index.php/en/etem-en/publications/itemlist/category/10-journa

Piekert, F., Carstengerdes, N., Schier-Morgenthal, S., Günther, Y., & Suikat, R. (2023). Metrics to evaluate multi-stakeholder decision-making processes – a critical discussion AHFE. *AHFE (2023) International conference on human factors in transportation*: vol. 95. Elsevier. https://openaccess.cms-conferences.org/publications/book/978-1-958651-71-1/article/978-1-958651-71-1_59

Piekert, F., Delain, O., Martín Domínguez, E., & Marsden, A. (2017b). Europe's next step in total airport management research. *Atrs 2017*. Antwerp, Belgium. http://elib.dlr.de/110860/

Piekert, F., & Strasser, M. (2010). Potential impact of data variance on the prediction of key performance indicators (KPI) as a decision variable for airport pretactical decision making within a total airport management (TAM) airport operations center (APOC). *2nd ENRI Int. workshop on ATM/CNS (EIWAC 2010)*. Tokyo, Japan. http://www.enri.go.jp/eiwac/2010/pdf/gaiyo/EN-001.pdf

Polater, A. (2018). Managing airports in non-aviation related disasters: A systematic literature review. *International journal of disaster risk reduction, 31*, 367–380. https://doi.org/10.1016/j.ijdrr.2018.05.026.

PRAETORIAN. *Croatian scenario #2 overview*. https://praetorian-h2020.eu/wp-content/uploads/2023/04/PRAETORIAN_Croatian_2_Scenario_Overview.pdf

Predescu, A.-V., Piekert, F., Stelkens-Kobsch, T. H., Günther, Y., Carstengerdes, N., Schaper, M., Demestichas, K., Papadopoulos, L., Remoundou, K., Alexakis, T., Masouros, D., Dose, M., Muñoz, E., Caillière, R., Helies, E., Leslous, M., Rychkov, V., Levak, J., Markarian, G., et al., (2023). *PRAETORIAN D2.1 Instantiation of previous project results*: vol. 1. European Commission. https://praetorian-h2020.eu/documents/

Schaper, M., Stelkens-Kobsch, T. H., & Carstengerdes, N. (2017). From preparation to evaluation of integrated ATM-security-prototype validations. In *2017 IEEE/AIAA 36th digital avionics systems conference (DASC)* (pp. 1–8). IEEE.

SESAR 2020 PJ.04 Project Partners (2020). *Solution PJ.04-02: V2 Data Pack. 733121*. Brussels, Belgium: European Commission. https://doi.org/10.2829/60154

SESAR 3 Joint Undertaking (2022). *MULTIANNUAL WORK PROGRAMME 2022-2031* (1.0 ed.). Publications Office of the European Union. https://doi.org/10.2829/60154

Široka, M., Piličić, S., Milošević, T., Lacalle, I., & Traven, L. (2021). A novel approach for assessing the ports' environmental impacts in real time–the IoT based port environmental index. *Ecological Indicators, 120*, 106949. https://doi.org/10.1016/j.ecolind.2020.106949.

Stelkens-Kobsch, T. H., Boumann, H., Piekert, F., Schaper, M., & Carstengerdes, N. (2023). A concept-based validation approach to validate security systems for protection of interconnected critical infrastructures. In *Proceedings of the 18th international conference on availability, reliability and security* (pp. 1–10). https://doi.org/10.1145/3600160.3605025

Stelkens-Kobsch, T. H., Carstengerdes, N., Reuschling, F., Burke, K., Mangini, M., Lancelin, D., Georgiou, E., Hrastnik, S., & Branchini, E. (2021). Security challenges for critical infrastructures in air transport. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security*, 232. https://doi.org/10.1561/9781680838237.ch10.

Sun, X., & Wandelt, S. (2021). Robustness of air transportation as complex networks: Systematic review of 15 years of research and outlook into the future. *Sustainability, 13*(11), 6446. https://www.mdpi.com/2071-1050/13/11/6446

Sun, X., Wandelt, S., & Zhang, A. (2020). Resilience of cities towards airport disruptions at global scale. *Research in Transportation Business & Management, 34*, 100452. https://doi.org/10.1016/j.rtbm.2020.100452.

Ugarelli, R., et al., (2021). Cybersecurity importance in the water sector and the contribution of the STOP-IT project. In *Cyber-physical threat intelligence for critical infrastructures security: Securing critical infrastructures in air transport, water, gas, healthcare, finance and industry* (pp. 145–158). https://doi.org/10.1561/9781680838237.ch6.

Undertaking, S. J. (2015). Sesar 2020 multi-annual work programme. In *SESAR Joint Undertaking, Brussels, Belgium* (p. 565). http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/jtis/h2020-wp-multi-annual-sesar-ju_en.pdf

Voskaki, A., Budd, T., & Mason, K. (2023). The impact of climate hazards to airport systems: a synthesis of the implications and risk mitigation trends. *Transport Reviews*, 1–24. https://doi.org/10.1080/01441647.2022.2163319.

Xu, Y., Wandelt, S., & Sun, X. (2023). IMMUNER: Integrated multimodal mobility under network disruptions. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 1480–1494. https://doi.org/10.1109/TITS.2022.3224413.