Security and Resilience for Airport Infrastructure

Corinna Köpke, Louis König, Katja Faist, Mirjam Fehling-Kaschek, Jörg Finger, Alexander Stolz

Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Am Klingelberg 1, 79588 Efringen-Kirchen, Germany. E-mail: Corinna.Koepke@emi.fraunhofer.de

Kelly Burke

DGS S.p.A. - NIS Network Integration & Solutions S.r.l., Via XX Settembre 41, Genova 16121 Italy. E-mail: kelly.burke@dgsspa.com

Eftichia Georgiou, Vasiliki Mantzana, Ioannis Chasiotis

Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection P. Kanellopoulou 4, 101 77 Athens, Greece.E-mail: e.georgiou@kemea-research.gr

Isabel Praça, Eva Maia

GECAD - Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development, School of Engineering (ISEP), Polytechnic of Porto (IPP), R. Dr. António Bernardino de Almeida, 431, Porto, Portugal. E-mail: icp@isep.ipp.pt

Nikolaos Papagiannopoulos

IT&T Data Services, Information Technology & Telecommunications, Athens International Airport S.A, 19019 Spata, Athens, Greece. E-mail: Papagiannopn@aia.gr

Filipe Apolinário, Nelson Escravana

INOV-INESC INOVAÇÃO, Rua Alves Redol, nr. 9 1000-029 Lisboa, Portugal. E-mail: filipe.apolinario@inov.pt

The protection of critical socio-technical infrastructure is a popular research topic that gained particular interest in the last decade. In the age of digitalization, the importance of cyber-threats increases since they can lead to catastrophic consequences especially if combined with physical attacks. A prominent example of a critical socio-technical infrastructure is an airport containing sensitive systems such as the airport operation center, the apron control and the baggage handling system. In general today, airports are well protected against individual cyber-threats and in some cases protected against certain physical attacks on individual systems. A remaining major issue is the vulnerability to combined cyber-physical threats. In the ongoing EU-H2020 project SATIE (Security of Air Transport Infrastructure of Europe), a security toolkit is being developed to face these threats in a coordinated and effective way supported by a shared situational awareness system. The impact propagation simulation, being a part of the project's toolkit, simulates threats in an airport following a network approach to represent the system-of-systems. In this work, we develop a model to represent not only technical components of airport systems but also the social aspect through agent-based modeling (ABM). Performance measures are defined for technical as well as social aspects of the infrastructure to quantitatively analyze the system's resilience under the influence of specific cyber-physical threats.

Keywords: Security, airport, socio-technical infrastructure, agent-based modeling, resilience, system-of-systems.

1. Introduction

Airports play a key role in the transportation of people and goods, as well as in regional, national and international trade. They are a type of Critical Infrastructure (CI), where federal oversight and control intersects with local governments that own and operate most airports (Choi and Hanaoka, 2017; Polater, 2018). Airports Council International (ACI) reported that by 2040 global passengers will double to 20.9 billion, compared to 2017 (8.2 billion) (ACI Media Releases, 2018). To handle this, airports must automate their processes and consequently also increase physical

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0_4026-cd

and cyber-security measures. Furthermore, airports implement several types of security measures and technological solutions to deter, detect and react to physical attacks, such as: (a) fences/walls, (b) guards, (c) building control, (d) intrusion detection and access control, (e) video and audio surveillance systems and (f) Physical Security Information Management (PSIM) systems. In addition, cyber-attacks are emerging, especially with the increasing use of Information Systems (IS), such as electronic tags for baggage handling and tracking, remote check-in, smart boarding gates, faster and more reliable security screening technologies and biometric immigration controls. The continuing advances in the information and communication technologies (ICTs) field, which can benefit the efficiency of the airport, are now also being used as cyber-attacks like the attack to the flight information screens at Bristol Airport in 2018 (Kanyi et al., 2016; Leyden, 2018). Therefore, it is integral for airports to adopt additional cyber-security measures such as: (a) data protection, (b) network monitoring, (c) intrusion response systems, (d) endpoint monitoring, (e) authentication and access control systems and (f) software development based on privacy by design techniques.

The realm of physical assets (like hangars, terminals, baggage conveyors, etc.) is the core business of transportation infrastructure and delivers a broad variety of services (e.g., baggage and passenger screening to detect explosive devices) to end-users that rely on the activities of these services (e.g., passengers, airline companies) (Willemsen and Cadee, 2018). On the other hand, the technological assets that comprise the airport infrastructure (e.g. flight schedule information, passenger passport information, baggage destinations, etc.) give airport staff the technology to effectively manage and supervise the physical assets and to automate tasks in order to deliver airport services (Sampigethaya and Poovendran, 2013; Falvo et al., 2015).

When any of the assets are threatened, possibly by a physical attack, a crisis management plan should immediately be executed in order to manage the problem and minimize the impact. A crisis is defined as an abnormal and unstable condition which threatens the organization's strategic objectives, reputation or viability. In this context, crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises (BS 11200:2014, 2014). Stakeholder management is considered a crucial factor in all phases of crisis management as their actions can increase public awareness, reduce crisis impact and enhance mitigation actions. To that end, mutual aid agreements, clear communication pathways and training of stakeholders should be in place (Harriman et al., 2009). There should always be a balance between increasing an airport's capacity and maintaining their ability to respond efficiently and effectively (Kenar et al., 2007).

Any successful physical or cyber-incident that causes loss of infrastructure, such as natural disasters, terrorist acts, or chemical, biological or radiological hazards could affect airports operation, cause mass casualties, grave economic damage, and attract significant public attention because of the impact on the airport system. Now more than ever, airports must be vigilant in establishing safeguards against physical and cyber-threats, which is why it is imperative to have a solid understanding of the risks and protections available.

Most airport services (e.g., baggage handling) are typically implemented using industrial control system (ICS) security architecture (Stouffer et al., 2011) where physical assets connected to technological assets are separated into three layers of protection (from the most to least critical): a physical, a control and a supervisory layer.

The physical and control layers are the most safety-critical layers, and contain all the necessary mechanisms to implement airport services, namely, control units. The latter are computing devices which serve as interfaces between physical and digital assets of the airport infrastructure and manipulate the physical assets to guarantee airport services.

Given that, the connection between control units and physical assets can have critical consequences to the safety of airport infrastructure (e.g. sabotaging baggage screening machines can bypass bomb detection and successfully place a bomb on an aircraft), attackers often target these control units to hinder the safety and operations of airports. Thus, it is common ICS procedure (Stouffer et al., 2011) to place the IT devices communicating with these units, found in the control layer, on a demilitarized zone (DMZ), and under this DMZ, monitor and restrict network traffic using intrusion detection systems and firewalls.

The supervisory layer is thus connected to this DMZ and is mostly composed of IT devices that supervise the work performed on the control layer and triggers actions to assure the quality of airport services. Most cyber-attacks affecting ICS normally access an IT device in the supervisory layer and attempt to attack the other layers from that device.

Research on how to increase security on cyber-physical ICS systems is a growing trend. Particularly, current research on common threats to ICS security has focused on increasing DMZ protection against cyber-physical attacks (Langner, 2011; Huang et al., 2018) which are capable of infecting IT computers at the supervisory layer with self-spreading malware. The latter disseminates throughout the ICS network bypassing ICS security mechanisms and performing malicious operations over the physical assets. Proposals for novel detection schemes tackling such ICS attacks implement anomaly-based IDS mechanisms with new fingerprinting techniques (Chen et al., 2018; Formby et al., 2016; Cheng et al., 2017), while others have focused on estimating the level of propagation an attack can cause to the organization's IT assets, and identifying which operational objectives and goals (i.e. mission) were compromised by an attack (Lima et al., 2014; Noel et al., 2016; Willemsen and Cadee, 2018; Goodall et al., 2009). Yet, estimating the impact propagation of a cyber-attack throughout the airport services is still an open problem. The increasing capacity of computation and data storage in combination with technological developments - such as machine-learning methods, block-chain and agent-based modeling (ABM) - create opportunities never before seen. Yet frameworks should foster the development with guidelines and proactive measures to address liability, safety, security and privacy of these new technologies.

To this end, a multi-national project called SATIE has been funded by the European Commission with the goal of assessing the most threatening risks in airports, creating a holistic plan to improve cyber-physical security and implementing an up-to-date airport security management cycle that will cover security, safety, maintenance and information sharing processes. Thus, an interoperable security toolkit will be developed to improve cyber-physical correlations, forensics investigations and dynamic impact assessment at airports. This toolkit will be based on a complete set of semantic rules that will improve the interoperability between existing systems and enhanced security solutions, in order to ensure more efficient threat prevention, threat and anomaly detection, incident response and impact mitigation, across infrastructure systems, populations and the environment. Moreover, the collaboration between security practitioners and airport managers will also be enhanced, enabling a more efficient crisis resolution. Different threat scenarios combining cyber- and physical threats against airports will be defined and integrated in a simulation platform to validate the efficiency of the toolkit. In addition to simulations, different possible threat demonstrations will be conducted at different airports in distinct locations across Europe.

In this paper, the simulation of impact propagation which is part of the SATIE toolkit is described. It evaluates the impact of certain threats on a system-of-systems and describes cascading effects beyond the borders of single systems. Here, an agent-based approach is employed to simulate the impact of cyber-physical threats on passengers in an example simulated airport which will be integrated into the impact propagation tool for SATIE. This paper is structured as follows: In section 2 the approach is described about the agent-based representation of airport passengers and how this is embedded into the SATIE project. Further, section 3 presents the application of our approach to an example problem and the results are visualized. Finally, in section 4 the findings of this work are summarized and an outlook is provided.

2. Approach

2.1. *The SATIE toolkit*

The SATIE toolkit aims to strengthen the protection against cyber-physical threats at airports. To accomplish this, the SATIE project will improve the state of the art by addressing pre-identified conceptual, technical, economical and societal limitations. The SATIE toolkit is composed of several solutions that will be deployed in the critical areas of the airport, in order to prevent and detect potential threats. For example, in the air traffic control tower, voice communication and traffic status will be monitored and correlated to decrease the detection time of security threats and support the decision about the mitigation procedures. Due to the increasing amount of heterogeneous systems at the airport, combining internet-of-things (IoT) devices and industrial control systems, a module to ensure security of communications will also be developed. The baggage handling system will be used as an example application for this module. However, it might be reused for other assets in the airport. In the context of the baggage handling system, a link between passenger and baggage will be created, considering baggage as an extension of the passenger's identity. This way it will be possible to identify unusual characteristics of passengers' data to highlight potential cyber- and/or physical threats related to their baggage or vice versa.

All information and alerts from the devices and systems will be gathered by the correlation engine (see Figure 1). It will be the central part of the SATIE toolkit, which stores all the information and processes it in real time. The processing phase will allow the detection of inconsistent information or even a combination of cyber- and physical security events, that trigger real-time alerts which are sent to the incident management portal.

An impact propagation simulation will contribute to the information in the incident management portal. Relying on an interdependency model between IT assets, airport information and airport operations, it will provide impact assessments and decision support for both the security operation center (SOC) and airport operation center (AOC). An investigation tool will also be a source of information for the incident management portal. It will unify the physical and cybersecurity investigations, by performing a deep analysis of activities and threats over a long time frame. It will be very useful not only for completing and better predicting the real-time analysis of

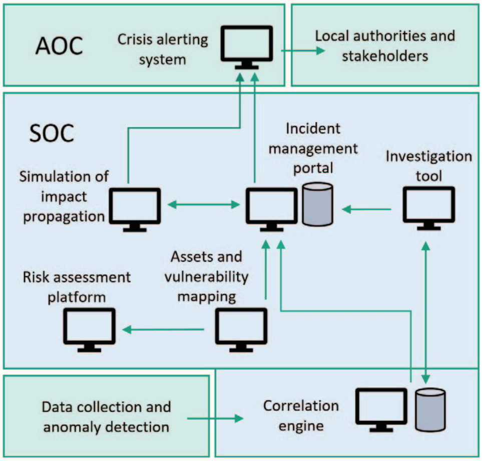

AOC
Crisis alerting system
Local authorities and stakeholders
SOC
Incident management portal
Investigation tool
Simulation of impact propagation
Assets and vulnerability mapping
Risk assessment platform
Data collection and anomaly detection
Correlation engine

Fig. 1. Interrelations between the tools in SOC and AOC.

the correlation engine, but also for supporting the fast recovery in case of an incident. It will analyze additional security details, providing contextual and semantic data, to identify causes for security events and threats started by an alert, and will feed the correlation engine with new and/or improved rules.

Finally, the crisis alerting system will combine the information from both the correlation engine and the impact propagation simulation to understand the security and safety status of airport systems. It will also be responsible for triggering real-time notifications and alerts for all actors involved at every level of coordination, in order to improve the collaboration and coordination of the security and safety responses. As already mentioned, all systems described above will be integrated in a simulation platform. Thus, using specific threat scenarios that exploit target systems' vulnerabilities, the effectiveness of prevention, detection, and response of the SATIE toolkit will be validated.

2.2. *Simulation of impact propagation*

The simulation of impact propagation for the anticipated impact assessment in the SATIE toolkit is based on a simulation tool named CaESAR (Cascading Effects Simulation in urban Areas to assess and increase Resilience). CaESAR is a simulation tool for computing cascading effects within critical infrastructure and especially across infrastructure borders (i.e. in interdependent infrastructure systems) (Hiermaier et al., 2017). The overall target of the CaESAR tool is to model impact propagations in interdependent infrastructure systems, to find weaknesses, to identify optimized strategies to overcome the weaknesses and to increase the resilience of those interdependencies. In SATIE, CaESAR will be used to implement the model of different assets (e.g. IT assets, physical assets or humans), employing ABM. Based on this model, CaESAR will simulate the propagation of threats, evaluate the consequences on the airport infrastructure and identify possibilities to increase the resilience.

2.3. *Agent-based modeling*

ABM is a bottom-up modeling approach that consists of agents such as individual objects or groups, an infrastructure, and rules of interactions. The latter are very important to guide the agents in the infrastructure and in groups. Agents have specific properties that lead to individual behaviors such as needs (to eat and drink), emotions, memories and relations to other agents (Helbing and Balietti, 2011). To develop a simulation environment based on ABM, the programming language, platform, boundary conditions, time discretization and noise need to be defined. In the case that the simulations should provide quantitative outputs, validation of the ABM is crucial (Helbing and Balietti, 2011).

ABM has been applied in various disciplines such as archaeology (Guedes et al., 2016; Romanowska et al., 2019), tumor research (Ozik et al., 2019), train logistics (Othman et al., 2014), air traffic management (Stroeve et al., 2013) and evacuation in case of fire (Kasereka et al., 2018). Even whole languages and platforms have been developed to facilitate the application of ABM to scientific questions (Kravari and Bassiliades, 2015; Wilensky and Rand, 2015). The application of ABM to socio-technical systems such as airports enables to reflect human behavior in the infrastructure, to observe what happens under specific conditions and to explore possible states of the system (Van Dam et al., 2012).

In this work, we focus on the representation of the interdependency between human individuals in an airport environment and the technical components of the infrastructure. This approach helps to better understand the interrelations between human behavior and technical functionality and to offer decision support in incident situations (Van Dam et al., 2012). An object-oriented approach using the programming language C++, enables the representation of the infrastructure and the individual passengers as agents. Through the simulation environment, incident scenarios can be analyzed and impacts can be quantified.

3. Application

As already introduced in section 2.3, in this work single passengers in an airport are simulated as agents. The path of a passenger in the airport is individual and passes Flight Information Display System (FIDS) monitors, check-in counters,

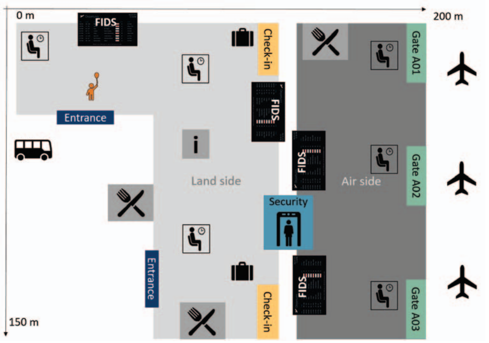


Fig. 2. Airport layout for the scenario described in section 3.1. The layout is employed to simulate passenger flow in the land-side and air-side airport areas.

security check points and gates. The passengers choose their path based on their own decisions and move with their individual velocity. The only rule that is predefined is that once they enter the air-side they cannot return to the land-side area of the airport anymore. Besides that, the individual situation of the passengers such as online check-in and number of check-in bags influences their path in the airport area. If and when they want to get information from the FIDS (e.g. number of check-in counter and gate corresponding to their flight), the agents can decide on their own.

3.1. *Airport use case*

Here, passenger movement is simulated in a small representative airport (see Figure 2). The airport layout and passenger behavior are mainly developed with the expertise of Athens International Airport (see Table 1).

Table 1. Data that has been developed with the expertise of Athens International Airport to design the airport and the simulation environment.

Number of flights per hour	5
Check-in treatment time	3-8 min
Number of passengers per hour	1875
Number of check-in counters	18
Time to walk from entrance to check-in	1-5 min
Time to walk from check-in to security	4-8 min
Time to walk from security to gate	5-20 min

To test and demonstrate the ABM approach, a scenario has been developed based on scenarios of the SATIE project. The FIDS is the target of a cyber-attack, and as consequence, it displays the wrong information. Instead of displaying correct check-in desks and gates, every passenger in the public area of the airport is directed only to a single check-in counter. Some passengers go directly to the designated check-in desk, while others do not know where to go and search for help, and finally, others do not care about FIDS information and remain at security. This creates crowds in the public area, which can be a potential target for physical attacks (for example, a suitcase bomb placed respectively).

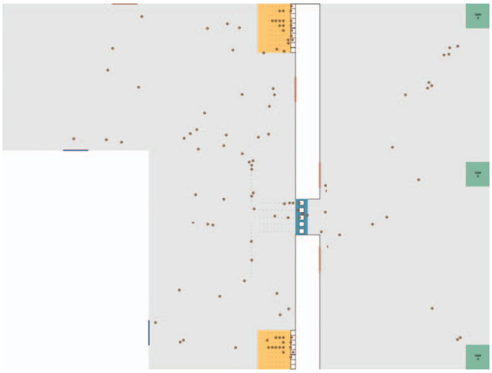


Fig. 3. A screenshot of passenger movement in the airport area during normal operation. Passengers (orange circles) move in the airport from the entrance (dark blue lines) to check-in (yellow), to security (blue) and to the gates (green) getting information at FIDS monitors (red lines).

3.2. *Results and visualization of the ABM approach*

The developed tool enables to simulate the passenger flow in the airport area. Without any disturbance, passengers walk from the entrance, to check-in, to security and finally to their gate (see Figure 3). They decide on their own when they take a look at the FIDS to get information about their flight. Note, that not all features of the airport are implemented yet. In contrast, in the case of a cyber-attack on the FIDS, all passengers are directed to one single check-in counter and it is assumed that all passengers follow the request. The formation of the resulting crowd can be represented by the simulation tool. Further, the crowd formation simulation will be dependent on the number of passengers land-side and the time it takes to restore the FIDS after the attack.

To analyze the performance of the airport before and during the cyber-attack, the number of passengers air-side and the estimated mean waiting time at the security check-point has been chosen as performance measures. These two measures are plotted as a function of time in Figure 4(a). In the beginning, from minute 1 to around 10, the airport opens its doors and passengers begin to enter first the land-side and later the air-side areas of the airport. From minute 10 to 40 a constant mean number of air-side passengers during normal operation can be observed. In minute 40 the cyber-attack occurs and all FIDS monitors direct the passengers to the specific check-in counter. In minute 50 the FIDS is restored and the passengers are distributed over all check-in counters again.

The number of air-side passengers and the waiting time at the security are correlated with a time delay. After peaks in waiting time, a larger number of passengers moves into the air-side area (see e.g. Figure 4(a) from minute 30 to 35). Further, once the cyber-attack happens, people continue to move to the air-side area. After around 5 minutes the impact of the cyber-attack in the land-side area also affects the passenger movement into the air-side area. The number of air-side passengers and the waiting time at security drops to a minimum around minute 55 because most passengers are crowded at the indicated check-in counter, which slows the flow of passengers to security. Once the passenger movement restores from minute 50 on, the impact can be observed air-side around minute 55 when passengers arrive again in the air-side area. The latter finding is further visualized with slopes approximated by linear regression from minute 40 to 55 and from minute 55 to 65. The corresponding values can be found in Table 2.

Table 2. Slope calculated for passengers arriving air-side for both simulations with the FIDS being restored a) in minute 50 and b) in minute 60 corresponding to Figure 4.

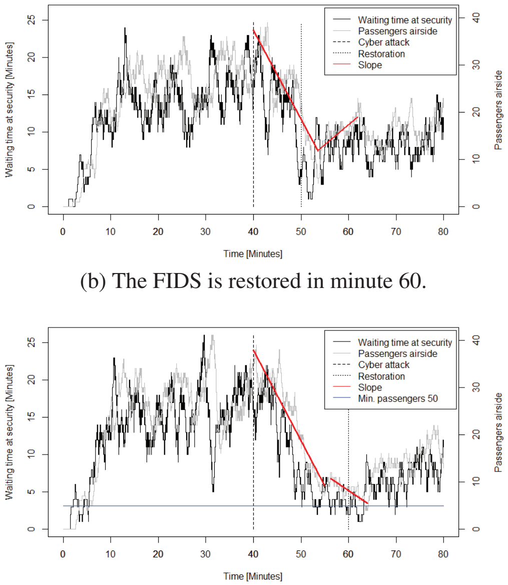
	Slope: minute 40-55	Slope: minute 55-65
(a)	-1.87	0.85
(b)	-1.91	-0.67

If the restoration takes longer, the impact of the cyber-attack on performance functions in the airport will increase. This is shown in Figure 4(b) where the attack occurs again in minute 40 but the restoration begins in minute 60. In this case, the number of passengers arriving at the air-side area decreases almost exponentially and reaches a minimum at around minute 65. The slope of passengers arriving at the air-side area is again approximated by linear regression and the results are presented in Table 2.

Comparing Figure 4(a) and (b), the slope of air-side passengers from minute 40 to 55 is almost the same which means that the initial impact of the cyber-attack is similar. However, if a fast recovery is possible and the FIDS is repaired after minute 50, the slope becomes positive again and the system is able to recover. If the recovery takes only 10 minutes longer and the FIDS is operable in minute 60, we observe a negative slope for air-side passengers also from minute 55-65. The performance does not yet recover and the number of passengers air-side drops to four which is lower than in the fast recovery case (see blue line in Figure 4(b)).

Here, we mainly discuss the degradation of the system's performance due to the cyber-attack. The recovery can be partially observed in Figure 4 but the simulation tool is not yet able to represent every detail of the recovery phase mainly because the crowd that formed in front of the check-in counter does not resolve anymore and also blocks adjacent check-in counters which limits the restoration capabilities. For this reason, the peak in waiting time at security and the return to normal performance cannot be observed which would be expected during and after the recovery phase. Note, that the number of land-side passengers as a function of time is not presented here because they mainly accumulate in the land-side area especially when the cyber-attack happens. Further, the passengers' velocities and waiting times are scaled to reduce computation time and might not exactly reflect reality.

(a) The FIDS is restored in minute 50.



(b) The FIDS is restored in minute 60.

Fig. 4. Airport performance visualization during normal and disturbed operation due to a cyber-attack on the FIDS (which happens in minute 40). Estimated waiting time at the security check-point (black line) and the number of air-side passengers (gray line) are given as a function of time. Additionally two dashed black lines show the time when the cyber-attack starts and ends. Red lines indicate the slope of the degradation of performance. In (b), the blue line represents the minimum number of passengers air-side when the FIDS is restored in minute 50.

4. Conclusion

In this paper, the security situation of airports in Europe is discussed and respective issues are raised. The EU-H2020 project SATIE is presented and how it addresses security issues in airports such as the handling of combined cyber-physical attacks. The SATIE toolkit addresses this through a novel, multi-faceted approach to augment the separation and security of the physical layer, control layer, and supervisory layer of the security architecture found in airports. Video-captured biometric credentials aid anomaly detection algorithms which are fed information linking passengers to their baggage. All of this information is used in a model of the connections between assets (both physical and informational), which can quantitatively represent the propagation of a negative impact through the airport infrastructure and demonstrate how performance measures would be affected. The focus in this paper is on the impact assessment simulation, using ABM to model airport processes. The current focus is less on technical components and more on passenger movement and their interactions with technical components such as the FIDS.

The agents in the simulation tool presented here move individually based on their personal situation such as whether they checked-in online, how much baggage they have and their individual velocity. However, some decisions are still guided or simply made by random generators, which will be improved by additional individual properties such as needs and personal preferences. For example, some passengers could be hungry and buy some food in a shop, some passengers try to avoid crowds or they have different comfort zones. Further, a next step is to include different types of people in the airport such as airport employees, security staff or attackers additionally to the passengers.

The airport representation is simplistic and further features will be introduced. Information counters, shops, restaurants and waiting areas will enable the agents to choose their paths in the airport area based on their needs and personal situations. The airport layout and agent movements need to be further validated with airport operators and data.

Also the scenario needs to be further developed and validated. The reaction of passengers and employees in the case of disturbed operation needs to be well understood and represented in the simulation. This will enable more advanced and combined attack scenarios to be considered. Still, as already mentioned in section 3.2, to study more advanced attack scenarios and to analyze the system's resilience the recovery phase needs to be studied in more detail.

Finally, the simulation tool that is presented here is able to simulate individual passenger movement in the airport in normal and disturbed operations. The simulation results show a crowd formation in the case of a cyber-attack on the FIDS and performance functions represent the impact of the attack on the airports functionality. Further, inertial effects can be observed in the performance measures as a function of time. It also enables to analyze and compare quantitatively the system's degradation for different recovery situations. This simulation tool will contribute to the SATIE project to better understand the impact of combined cyber-physical attacks on airport infrastructure.

The SATIE toolkit offers a holistic, comprehensive approach to airport security, addressing the unquestionable issue that physical attacks and cyber-attacks are highly interconnected and often permit one another to occur. Airports face a daily challenge to ensure business continuity and passenger safety and this innovative project improves cyber-physical correlations, forensics investigations and dynamic impact assessments, resulting in better threat prevention, detection, response and mitigation.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein. For more information on the project see: http://satie-h2020.eu/.

References

ACI Media Releases (2018). ACI's world airport traffic forecast reveals emerging and developing economies will drive global growth.

BS 11200:2014 (2014, May). Crisis management – guidance and good practice. Standard, The British Standards Institution.

Chen, Y., C. M. Poskitt, and J. Sun (2018). Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system. In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 648–660. IEEE.

Cheng, L., K. Tian, and D. D. Yao (2017). Orpheus: Enforcing cyber-physical execution semantics to defend against data-oriented attacks. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, pp. 315–326. ACM.

Choi, S. and S. Hanaoka (2017). Diagramming development for a base camp and staging area in a humanitarian logistics base airport. *Journal of Humanitarian Logistics and Supply Chain Management 7*(2), 152–171.

Falvo, M., F. Santi, R. Acri, and E. Manzan (2015). Sustainable airports and nzeb: The real case of rome international airport. In *2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*, pp. 1492–1497. IEEE.

Formby, D., P. Srinivasan, A. Leonard, J. Rogers, and R. A. Beyah (2016). Who's in control of your control system? device fingerprinting for cyber-physical systems. In *NDSS*.

Goodall, J. R., A. D'Amico, and J. K. Kopylec (2009). Camus: automatically mapping cyber assets to missions and users. In *MILCOM 2009-2009 IEEE Military Communications Conference*, pp. 1–7. IEEE.

Guedes, J. A. d., S. A. Crabtree, R. K. Bocinsky, and T. A. Kohler (2016). Twenty-first century approaches to ancient problems: Climate and society. *Proceedings of the National Academy of Sciences 113*(51), 14483–14491.

Harriman, S. L., R. O. Fanjoy, and D. A. Petrin (2009). Small general aviation airport emergency preparedness and the perceived risks of very light jet operations. *Journal of Aviation/Aerospace Education & Research 19*(1), 25–36.

Helbing, D. and S. Balietti (2011). How to do agent-based simulations in the future: From modeling social mechanisms to emergent phenomena and interactive systems design why develop and use agent-based models? *Santa Fe Institute Working Papers* (11), 1–55.

Hiermaier, S., S. Hasenstein, and K. Faist (2017). Resilience Engineering-how to handle the unexpected. In *7th REA Symposium*, pp. 92.

Huang, B., M. Majidi, and R. Baldick (2018). Case study of power system cyber attack using cascading outage analysis model. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*, pp. 1–5. IEEE.

Kanyi, P. M., P. Kamau, and C. Mireri (2016). Assessment of the appropriateness and adequacy of the existing physical infrastructure in mitigating aviation risks at wilson airport, kenya. *IOSR Journal Of Humanities And Social Science (IOSR-JHSS) 21*(7), 51–62.

Kasereka, S., N. Kasoro, K. Kyamakya, E.-F. D. Goufo, A. P. Chokki, and M. V. Yengo (2018). Agent-based modelling and simulation for evacuation of people from a building in case of fire. *Procedia Computer Science 130*, 10–17.

Kenar, L., T. Karayilanoglu, M. Eryilmaz, M. Ortatatli, and H. Yaren (2007). Chemical release at the airport and lessons learned from the medical perspective. *Journal of hazardous materials 144*(1-2), 396–399.

Kravari, K. and N. Bassiliades (2015). A survey of agent platforms. *Journal of Artificial Societies and Social Simulation 18*(1), 11.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy 9*(3), 49–51.

Leyden, J. (2018). Brit airport pulls flight info system offline after attack by 'online crims'. *The Register*.

Lima, J., N. Escravana, and C. Ribeiro (2014). Bpids-using business model specification in intrusion detection. In *Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014, Proceedings*, Volume 8688, pp. 479. Springer.

Noel, S., E. Harley, K. H. Tam, M. Limiero, and M. Share (2016). Cygraph: graph-based analytics and visualization for cybersecurity. In *Handbook of Statistics*, Volume 35, pp. 117–167. Elsevier.

Othman, N. B., E. F. Legara, V. Selvam, and C. Monterola (2014). Simulating congestion dynamics of train rapid transit using smart card data. *Procedia Computer Science 29*, 1610–1620.

Ozik, J., N. Collier, R. Heiland, G. An, and P. Macklin (2019). Learning-accelerated discovery of immune-tumour interactions. *Molecular Systems Design & Engineering*.

Polater, A. (2018). Managing airports in non-aviation related disasters: A systematic literature review. *International journal of disaster risk reduction 31*, 367–380.

Romanowska, I., S. A. Crabtree, K. Harris, and B. Davies (2019). Agent-based modeling for archaeologists: Part 1 of 3. *Advances in Archaeological Practice 7*(2), 178–184.

Sampigethaya, K. and R. Poovendran (2013). Aviation cyber–physical systems: Foundations for future aircraft and air transport. *Proceedings of the IEEE 101*(8), 1834–1855.

Stouffer, K., J. Falco, and K. Scarfone (2011). Guide to industrial control systems (ics) security. *NIST special publication 800*(82), 16–16.

Stroeve, S. H., T. Bosse, H. A. Blom, A. Sharpanskykh, and M. H. Everdij (2013). Agent-based modelling for analysis of resilience in atm. *Proceedings of the Third SESAR Innovation days. Stockholm (Sweden), Novermber*.

Van Dam, K. H., I. Nikolic, and Z. Lukszo (2012). *Agent-based modelling of socio-technical systems*, Volume 9. Springer Science & Business Media.

Wilensky, U. and W. Rand (2015). *An introduction to agent-based modeling: modeling natural, social, and engineered complex systems with NetLogo*. MIT Press.

Willemsen, B. and M. Cadee (2018). Extending the airport boundary: Connecting physical security and cybersecurity. *Journal of Airport Management 12*(3), 236–247.