Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P201-cd

Hybrid threats on air traffic

Corinna Köpke

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

Kris Schroven

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

Alexander Stolz

Albert-Ludwigs-Universität Freiburg, Emmy-Noether-Straße 2, 79110 Freiburg im Breisgau, Germany. E-mail: alexander.stolz@mail.inatech.uni-freiburg.de

Air traffic in general is vulnerable to various hazards ranging from natural hazards to technical failures or attacks which can be both cyber and physical. These threats impact on airports but also the air traffic management can be affected to influence the overall air traffic. Here, we analyze the resilience of air traffic by studying performance degradation and recovery in airports due to hybrid threats. An airport consists of many coupled network systems such as public announcement system (PAS), flight information display system (FIDS), access control system (ACS), baggage handling system (BHS), and resource management system (RMS). These systems can be interrelated based on the configuration and setup of the network. Consisting of physical assets such as servers and routers connected through an airport internal network, these systems are vulnerable to physical and cyber threats. In this work, a flexible and modular approach is presented to combine various threats and apply a series of attacks onto the air traffic model by impacting single airports. In contrast to existing work, the nodes of the air traffic model do not reduce their performance to zero but follow pre-estimated resilience curves. Thus, the overall resilience of the air traffic model can be assessed in a dynamic way, here demonstrated for air traffic over Germany.

Keywords: Air traffic, hybrid threats, cyber-physical systems, airport networks.

1. Introduction

Hybrid threats are defined e.g. by Hybrid CoE (2023) as: 'The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level.' Hybrid threats can impact on all kinds of public services and critical infrastructure during war and peace time. A hybrid threat typically combines several attacks of cyber-physical terrorism. This has been presented e.g. in Valenza et al. (2022) where hybrid threats are applied to wind farms considering human, physical and cyber aspects.

A critical infrastructure that faced several terrorist attacks in the past is air traffic. Physical attacks like e.g. suitcase bombs (see e.g. Beauthier et al. (2020)) lead to large damage, also reduced trust in the service itself and reduced well-being in society (Colombo et al., 2022). Cyber attacks harm the processes in a more indirect way, but can lead to immense financial damage. Other aspects of cyber attacks are the spread over systems with the potential to interrupt all services and even turning into physical or safety threats (Kim et al., 2006).

In this work, air traffic is modeled by a multi-layered systems approach similar to (Woods and Branlat, 2010) composed of airports which again are made up of several systems. Air traffic, being a socio-technical infrastructure, consists of physical assets. However, also passengers and employees have to be considered to model attack paths and to understand the spread of threats in the systems and their cascading impacts. Here, we limit our modeling approach to German air traffic and the

German air navigation service provider (ANSP) that manages air traffic over Germany.

To understand how the air traffic performance degrades during a hybrid threat and how it recovers, the resilience of the modeled system of systems is assessed. Generally, resilient behavior of an infrastructure and its engineering (Häring et al., 2016) can be classified into phases, e.g. prepare, prevent, protect, respond and recover (Edwards, 2009; Thoma, 2014). Resilience in the context of hybrid threats has been discussed e.g. by Linkov et al. (2019) analyzing the dependency of society on information systems.

The work presented here mainly builds on Köpke et al. (2021) where airport systems have been represented as network structure to simulate resilience under cyber-physical threats and Köpke et al. (2023) where specifically the impact of cyber threat on rail infrastructure has been assessed. Here, these approaches are extended to generic airport models and hybrid threats impacting on connected airports.

This paper is structured as follows. First, in section 2, the airport layer of the air traffic model is presented and single airports are impacted by cyber attacks. Then, in section 3, the overall air traffic model is presented and coupled hybrid threats are applied to assess the resilience. Finally, in section 4, the work is concluded and an outlook to the next steps of the research is given.

2. Airport systems

A functioning air traffic is dependent on airport operations. Airports typically consist of various assets which can be categorized into different systems with respective functionality. Here, the following systems are considered:

- Through the Public Announcement System (PAS) passengers are informed in the terminal about certain events via speakers. It provides prerecorded messages as well as the possibility to manually pass information.
- The Access Control System (ACS) ensures that passengers and employees only access areas in the airport where they are authorized. It monitors terminals and especially doors via Closed-circuit television (CCTV).
- The Baggage Handling System (BHS) manages all passenger luggage and also checks for dangerous materials.
- Airplanes are distributed through the Resource Management System (RMS) to gates based on availability.
- The Flight Information Display System (FIDS) provides information about status of flights, security checks and gates via screens and its data base is linked to the RMS.

For more information on the systems see e.g. Köpke et al. (2021), Apolinário et al. (2023) and Abie et al. (2001).

2.1. *Network model*

To model the different airport systems, they are represented by information networks. Dependent on the network setup and also the size of the airport, there is either one network containing all systems with their IT components or several dedicated networks.

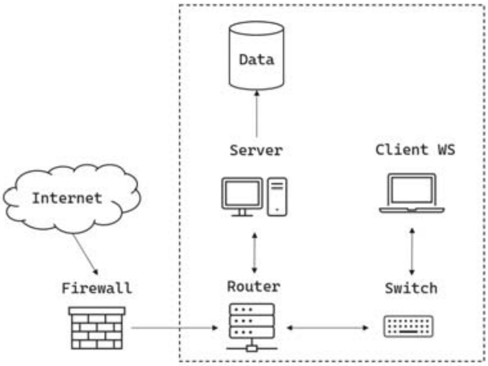

Fig. 1. Schematic of a simple company network that is used to model the airport systems, i.e. box containing router, server, data, switch and workstation (WS).

Here, we follow the latter approach and represent the overall airport network as a system of systems. Each system consists of a router, a switch, a sever linked to data and a client workstation (Secure Networks ITC, 2023). Through the overall firewall and the respective router, the system is connected to the internet (see Fig. 1). The connection to the internet is optional for the systems as they could be in an isolated environment.

For each of the airport systems, a representative network is established with additional components such as CCTV, monitors, speakers, baggage, passengers and employees, respectively (see Table 1).

Table 1. Asset list for the airport systems.

ID	Component	System
1	Firewall	IT
2 - 6	Fig. 1	BHS
7 - 11	Fig. 1	ACS
12 - 16	Fig. 1	PAS
17 - 21	Fig. 1	FIDS
22 - 26	Fig. 1	RMS
27	Passengers	People
28	Security	People
29	CCTV	ACS
30	Monitor	FIDS
31	Speaker	PAS
32	Baggage	BHS
33	Aircraft	RMS
34	Security check	ACS

The systems are presented with a color code in Fig. 2. The edges within the systems are based on the network presented in Fig. 1 and they are connected through common components such as passengers and employees.

The network setup enables the representation of both cyber and physical attacks. These attacks impact on single or multiple nodes in the network and propagate along edges with a specified probability. They impact further nodes with an impact delay. The impacted nodes recover based on the restoration time and return to full performance.

2.2. *Cyber-physical threat propagation*

A catalog of specific man-made threats to air traffic has been investigated, which can be combined into hybrid threats scenarios. It was found that each threat has very specific characteristics and the resilience assessment needs, dependent on the requirements, a very detailed threat modeling. For combined cyber-physical threat scenarios, the network model is well suitable. Thus, in this work, we consider two main scenarios, i.e. (A) a security breach via social engineering on one workstation of the FIDS and (B) a denial of service (DOS) attack that overloads all routers and thus the servers.

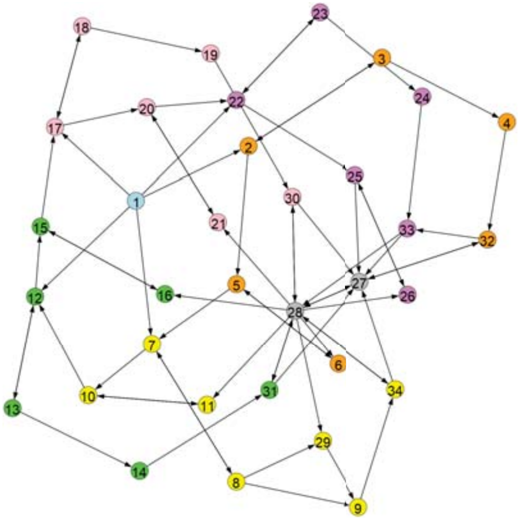

Fig. 2. Airport overall directed network with systems in color codes: BHS: Orange, ACS: Yellow, PAS: Green, FIDS: Pink, RMS: Violet, People: Grey, Firewall: Blue.

For scenario A, we assume that an attacker has gained access to a workstation in the airport via social engineering for obtaining a key card and credentials. The attacker thus gains access to the workstation of the FIDS, i.e. node #21 in the network model (see Fig. 2). Having access, the attacker has the option to manipulate information or disable the FIDS monitors which will then impact on the passenger behavior and finally on all operations in the airport. For scenario B, we assume an overload of requests through all routers in the network (nodes #2,7,12,17 and 22) that disables all communication to the servers and thus stops all services.

To simulate these impacts and to assess the resilience the following parameter specifications for nodes are employed:

- Restoration time mean: 60 minutes
- Restoration time standard deviation: 10 minutes
- Impact delay time mean: 3 minutes
- Impact delay time standard deviation: 1 minute

The mean and standard deviation are used to draw for each iteration / repeated simulation random values for restoration time and impact delay for each node, respectively. For the general simulation the following variables are specified:

- Number of iterations: 100
- Propagation probability: 0.75
- Time of attack: in minute 5
- Time steps: 150

Note, uncertainty can also be introduced for the propagation probability by e.g. defining a uniform distribution between a minimum and a maximum probability. The attack time is fixed in this case but it is also possible to initiate attacks at random times. Further, all these variables are set globally for all nodes but they can also be specified for each node individually to enable the simulation of a broad set of possible situations.

Based on the airport network topology and the parameters, the suggested simulation environment implemented in Python, propagates the impacts of the attack scenarios through the network along the edges. The impacted nodes stop their operation and with a certain probability transfer the impact to adjacent nodes. This also includes cascades from one airport system to another. The impact probability is very difficult to estimate as data for calibration is sparse. Thus, a value below one is assumed in this work to enable a certain variability in the results. Once the restoration time has passed, the nodes start to be operational again. The simulation results are presented in Fig. 3 and 4.

The overall time for degradation and full recovery is almost the same for both scenarios as they are based on the same assumptions. However, the minimum performance for scenario B is much lower as for scenario A. This is due to the larger number of systems which are affected at the same time for scenario B.

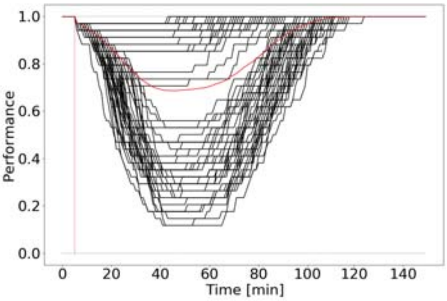

Fig. 3. Resilience assessment for scenario A (security breach on workstation). Black lines are repeated simulation results with varying restoration and impact delay times, the red vertical line shows the time of attack and the red solid line gives the mean performance.

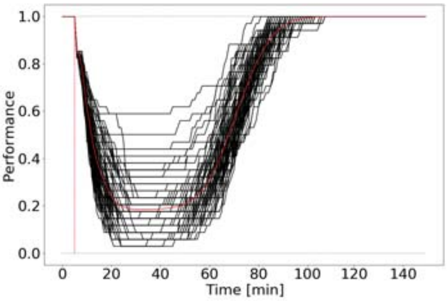

Fig. 4. Resilience assessment for scenario B (DOS-attack). Black lines are repeated simulation results with varying restoration and impact delay times, the red vertical line shows the time of attack and the red solid line gives the mean performance.

Note, even if only two specific cyber-related threat scenarios have been presented in this work, many more scenarios can be assessed with this method, especially as the computational load of running the associated Python scripts is very low (approximately 1 second for 100 repeated simulation runs on a standard notebook).

3. Air traffic model

Based on the single airport networks, consisting of different airport systems, an overall air traffic model is constructed. It consist of 15 airports distributed over Germany and based on the locations with towers operated by the German ANSP (DFS, 2023). All airports are connected and it is assumed that airplanes circulate between all airports along these edges (see Fig. 5). If one airport degrades in performance, all other airports get a certain percentage of reduced performance as well because only a reduced number of flights can be operated to the impacted airport. The degradation of performance of a single airport is given by specific mean resilience curves as presented in Fig. 3 and 4 that serve as input for the resilience assessment of the overall air traffic model.

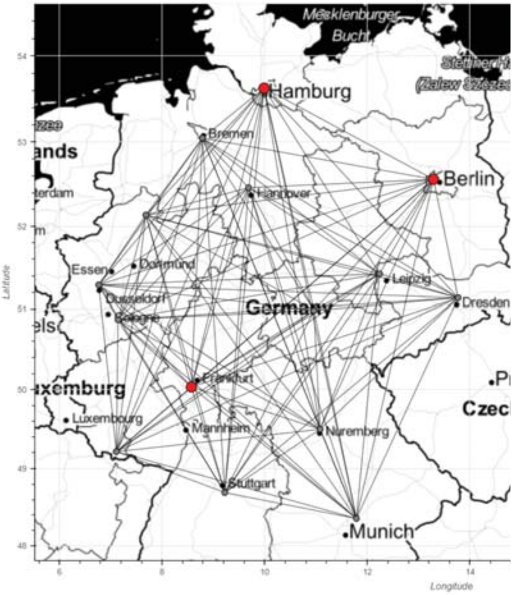

Fig. 5. Air traffic model. Red airports are impacted by hybrid threats in the examples considered. Map tiles by Stamen Design under CC BY 3.0. Data by OpenStreetMap under ODbL.

3.1. *Hybrid threats*

A dynamic approach is suggested for several threats impacting on airports and all connected airports receive additional shared performance reduction. Thus, hybrid threats can be constructed by specifying input vectors that contain the time of attacks, target airports and types of attack.

In the following, two examples for hybrid threats are presented, which combine scenario A (security breach on workstation) and B (DOS-attack). First, scenario A impacts on Frankfurt airport in time step 100 and scenario B impacts on Berlin airport in time step 150 (see Fig. 6). Second, scenario B impacts on Berlin airport in time step 125 and on Hamburg airport in time step 150, followed by scenario A impacting on Hamburg airport in time step 200 (see Fig. 7). For the latter hybrid threat example, the attacker benefits from the degradation of systems due to the DOS-attacks to prevent the systems from recovering by the additional security breach.

These two examples demonstrate the flexibility of the approach and how threats accumulate. A single attack on one airport is still well compensated by the other airports and air traffic is only minimally impacted. However, if threats are coupled, which is often the case for hybrid threats, severe damage to the infrastructure and thus to society can be observed. The actual status of the derived approach is still simple but offers a tool to stress test infrastructure for various coupled hybrid threat scenarios and can be easily modified to a more complex system by adding e.g. more informed performance functions, threat types and coupled infrastructure grids.

4. Conclusion

In this paper, a flexible approach has been presented for stress testing critical infrastructure facing hybrid threats. It has been applied to German air traffic management by considering cyber-physical threats. The approach is based on a multilayered systems model, where air traffic is based on a grid composed of airports and the airports are made up of several systems which consist of several assets. The approach enables to define hybrid threats as a combination of single threats on airports. The advantage over existing approaches is, that the airports in the overall air traffic model are not only turned on or off by a threat impacting, but single resilience curves can be introduced to represent the status of each airport in a quantitative manner. From this quantified status the overall performance of the system can be derived.

To estimate the overall performance of air traf-

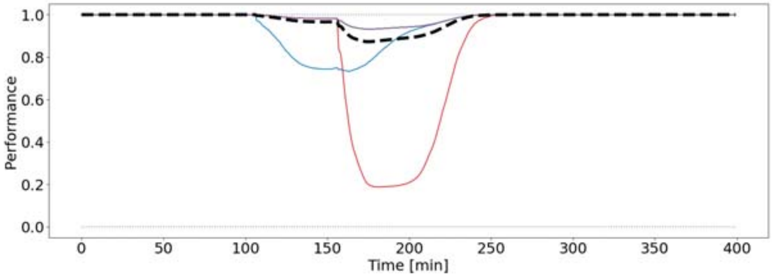

Fig. 6. Air traffic performance under hybrid threats: security breach in Frankfurt airport at time step 100 (blue), DOS attack in Berlin airport at time step 150 (red), all other airports (purple), mean (black dashed).

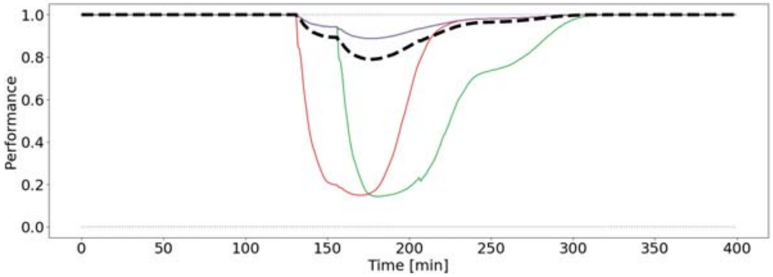

Fig. 7. Air traffic performance under hybrid threats: DOS attack in Berlin airport at time step 125 (red), DOS attack in Hamburg airport at time step 150 (green), security breach in Hamburg airport at time step 200 (green), all other airports (purple), mean (black dashed).

fic in future developments of the suggested approach, an agent-based model will be considered where airplanes move along the edges of the overall air traffic model between airports. Passengers spawn/are created at random times with random start and target airports. They choose a connection of flights to get to their target (for more information see (Köpke et al., 2023)). This will enable a more detailed and realistic quantification of the overall system performance. It is also intended to expand the system by including international airports as the German air traffic is not isolated but depends on the international air traffic.

Further, the resilience curves per threat can not only be represented by their mean behavior. The uncertainty should be considered by e.g. introducing the standard deviation. Also, more threats will be investigated in future work such as drone disorder, usage of lasers, bombing threats and attacks. For physical attacks and structural damage, finite element methods are much more suitable than network based models (see e.g. (Köpke et al., 2023)). Thus, various simulation approaches will be employed along with crime scene investigations to improve the threat-specific resilience estimates. In future work, the modular approach can be easily extended to different threat scenarios, systems and infrastructure.

Acknowledgement

The authors like to thank Johannes Walter for the production of one of the Figures and the reviewers for their comments that helped to improve this paper.

References

Abie, H., D. Ferrario, E. Troiano, J. Soldatos, and F. Di Peppo (2001). Projekt presentations. In H. Abie, D. Ferrario, E. Troiano, J. Soldatos, and F. Di Peppo (Eds.), *Consolidated Proceed-*

ings of the first ECSCI Workshop on Critical Infrastructure Protection. Steinbeis-Edition.

Apolinário, F., J. Guiomar, É. Hervé, S. Hrastnik, N. Escravana, M. L. Pardal, and M. Correia (2023). Comsec: Secure communications for baggage handling systems. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers*, pp. 329–345. Springer.

Beauthier, F., W. Van de Voorde, P. Lefevre, and J.-P. Beauthier (2020). Belgium experience in disaster victim identification applied in handling terrorist attack at brussels airport 2016. *Forensic Sciences Research 5*(3), 223–231.

Colombo, E., V. Rotondi, and L. Stanca (2022). The day after the bomb: Well-being effects of terrorist attacks in europe. *Social Indicators Research*, 1–18.

DFS (2023). Deutsche flugsicherung. `https://www.dfs.de/homepage/de/`. Accessed: 2023-03-28.

Edwards, C. (2009). Resilient nation demos.

Häring, I., S. Ebenhöch, and A. Stolz (2016). Quantifying resilience for resilience engineering of socio technical systems. *European Journal for Security Research 1*, 21–58.

Hybrid CoE (2023). Hybrid threats as a concept. `https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/`. Accessed: 2023-03-29.

Kim, Y., T. Lee, H. In, Y. Chung, I. Kim, and D. Baik (2006). A probabilistic approach to estimate the damage propagation of cyber attacks. *ICISC 2005 3935*, 175–185.

Köpke, C., J. Mielniczek, C. Roller, K. Lange, F. S. Torres, and A. Stolz (2023). Resilience management processes in the offshore wind industry: schematization and application to an export-cable attack. *Environment Systems and Decisions*, 1–17.

Köpke, C., K. Srivastava, L. König, N. Miller, M. Fehling-Kaschek, K. Burke, M. Mangini, I. Praça, A. Canito, O. Carvalho, et al. (2021). Impact propagation in airport systems. In *Cyber-Physical Security for Critical Infrastructures Protection: First International Workshop, CPS4CIP 2020, Guildford, UK, September 18, 2020, Revised Selected Papers 1*, pp. 191–206. Springer.

Köpke, C., J. Walter, E. Cazzato, C. Linguraru, U. Siebold, and A. Stolz (2023). Methodology for resilience assessment for rail infrastructure considering cyber-physical threats. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers*, pp. 346–361. Springer.

Linkov, I., F. Baiardi, M.-V. Florin, S. Greer, J. H. Lambert, M. Pollock, J.-M. Rickli, L. Roslycky, T. Seager, H. Thorisson, et al. (2019). Applying resilience to hybrid threats. *IEEE Security & Privacy 17*(5), 78–83.

Secure Networks ITC (2023). How to: Small business network setup. `https://securenetworksitc.com/small-business-network-setup/`. Accessed: 2023-03-27.

Thoma, K. (2014). *Resilien-Tech:Resilience by Design: a strategy for the technology issues of the future*. Herbert Utz Verlag.

Valenza, F., E. Karafili, R. V. Steiner, and E. C. Lupu (2022). A hybrid threat model for smart systems. *IEEE Transactions on Dependable and Secure Computing*.

Woods, D. D. and M. Branlat (2010). Hollnagel's test: being 'in control'of highly interdependent multi-layered networked systems. *Cognition, Technology & Work 12*, 95–101.