Information & Security

W. Matta & A. Cantelli-Forti,
vol. 43, no. 3 (2019): 285-293
https://doi.org/10.11610/isij.4321

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

An Innovative Airport Physical-cyber Security System (APSS)

Walter Matta [a], ***Alessandro Cantelli-Forti*** [b,a] (✉)

[a] *Link Campus University, Rome, Italy, http://www.unilink.it*

[b] *Lab RASS-CNIT, Pisa, Italy, http://labrass.cnit.it*

ABSTRACT:

Considering the number of airports in the world, the 100 of millions of people who work at or pass through them and the relatively small amount of vulnerabilities, which have come to fruition to date, it must be concluded that airports already have a largely adequate level of security and resilience. Recent attacks in Brussels and Paris have, however, indicated that there is still room for improvement. In addition, one should be aware of the increased number of terrorist attacks also exploiting the increased availability of advanced low-cost technology, such as jammers. Thus, we propose to operate the logical division of the airport into physical-cyber security-control, where a multi sensor data fusion is made on two levels: (i) data fusion within each segment, in order to generate the alarms, and (ii) correlation of the "segment alarms" in order to reduce the false (positive and negative) detection rate.

In the proposed solution, data resulting from the two fusion processes are viewed and made available by a Web Portal accessible by security officers and police, increasing the physical-cyber situational awareness and decision making. This approach dramatically increases the confidence level of threat detection, minimizes the false (positive and negative) rate, due to both initial correlation of alarms within the same segment and the final correlation of the alarm coming from different segments. This allows to proactively take countermeasures against such threats.

ARTICLE INFO:

RECEIVED: 01 JUL 2019
REVISED: 05 SEP 2019
ONLINE: 22 SEP 2019

KEYWORDS:

airport security, data fusion, counterterrorism, cybersecurity, cyber-physical systems

✉ Tel.: +39-347-2651552; E-mail: alessandro.cantelli.forti@cnit.it

Introduction

Understanding risk and deciding where to deal with it determines optimal security and resilience in certain environment. The operation of critical infrastructure will always entail risk stakeholders. Considering specifically airports, if they are attacked through intentional physical or cyber threats or seriously compromised through none intentional incidents this can result in direct loss of life[1] (e.g. passengers, air transportation employees, the surrounding population), damage to property (e.g. the airport, air transportation vehicles, other modes of transport) and the environment (e.g. release of harmful compounds, destruction of habitat) and loss of income (cancellation of services connected with air transportation). Indirect losses can include further societal, including economic, damage, e.g. through the inability to travel.[2]

The only way to achieve 0 % risk and accordingly 100 % security in connection with the loss of life and damage to property and the environment would be to not operate airports. This would result in other societal and economic losses which society has to date chosen not to accept. The goal of security must be to reduce risk to as close to 0 % as possible, while evaluating other limitations, such as human, technical and economic.[3] The goal of resilience must be to organise operational and societal systems to ensure that if security is compromised at airports then the operational and societal systems will recover as quickly as possible, having suffered the least loss possible.[4]

In our approach, we call it APSS, the twin goals of security and resilience for the critical infrastructure of airports, their neighbouring populations and environments are to be achieved by clearly understanding the actual or real potential threats they face and their vulnerabilities and finding a balance between reducing the risk of the threat and/or the loss through vulnerability coming to fruition. This requires a thorough and on-going assessment of risk in connection with security and resilience. Risks can then be reduced by implementing actions to prevent, detect, respond and/or mitigate against physical and cyber threats and their combinations to airports, their neighbouring populations and environments.[5]

Analysis of State-of-the-Art Solutions Addressing Current Gaps

Considering the number of airports in the world, the 100 of millions of people who work at or pass through them in any given year and the relatively small amount of vulnerabilities which have come to fruition to date, it must be concluded that airports already have a level of security and resilience, which has been largely adequate. Recent attacks for example in Brussels and Paris and the connected losses have, however, indicated that there is still room for improvement of security and resilience. The resilience of airports' zones with traditionally lower levels of security (e.g., forecourts and check-in areas), as well as their neighbouring surroundings, was in the past also less in focus. In addition, the geopolitical developments in the world as also indicated by the increased number of terrorist attacks and open and/or clandestine wars between nation states in the last 15 years identifies that the probability of physi-

cal and cyberattacks is increasing. The increased availability of advanced low cost technology, such as jammers, also increases the potential of some types of attack or even opens up the possibility of new types of attacks, which can also be compounded through the spread of revised operational methodologies, such as the use of Global Navigation Satellite System (GNSS) signals for landing procedures. The complexity of networked systems, volume of data being transferred and continual technological advancements also identifies the increased probability of cyber-attacks (through availability) and incidents.

APSS intends to focus on prevention, detection, response and mitigation solutions to actual threats and vulnerabilities and those with a strong potential to increase for which the state of the art and practice has been identified as lacking in terms of performance and/or cost.

Detection Analysis of GNSS Jamming and Spoofing Attacks

The use of GNSS (Global Navigation Satellite System) [6] is becoming a backbone of transportation systems, in particular in civil aviation. GNSS is efficient, precise and available anywhere any time, assuming the service has not been compromised. Civil Aviation is one of the first beneficiaries of these appealing performances. Aircraft are equipped with GNSS receivers, but also the vehicles for ground services, including those from emergency services. Major economic actors of the world (Europe, United States, Russia, China, India) have developed their own augmentation systems on top of GNSS, with the objective to improve the safety of GNSS for civil aviation. Such systems act as a security related enhancement of GNSS. They improve performance and reliability at local, regional, and continental level. The general term for such a system is SABS (Satellite Based Augmentation System), in Europe EGNOS (European GEO Navigation Overlay System). The objective is to allow aircraft to use safely GNSS for travelling and landing. However, GNSS presents some weaknesses that can jeopardize the security of air transportation, including airports and their surrounding areas with potential indirect impacts also on European society. As a global space-based system, GNSS is subject to local degradation due to unintentional interferences or intentional jamming. Existing regulations prohibit the intentional broadcast of any non-GNSS signals on or near the GNSS frequencies. Nevertheless, and despite these protections, those interferences affecting GNSS are observed and their occurrences have significantly increased in the latest years. Almost every day, publications describe cases of GNSS interferences occurring locally.[7] Radio-frequency degradation impacting GNSS use is not handled by any of the GNSS system or GNSS augmentation so far. This is due to the complexity of the surveillance organization that should be deployed since these effects are purely local.

To SBAS regional system augmentations…

Down to local transportation infrastructure….

Figure 1: GNSS Augmentation.

Detection Analysis of Impact of Explosive Attacks

Fortunately present sensing and intelligence techniques within airports and in society more broadly have limited the number of actual attacks. If, however, it is not possible to prevent all attacks with explosives in the future, the resilience of the airport, the people in it, its surroundings and society more broadly would be strengthened if reliable and quantitative data could be provided and analysed in a timely manner to determine the optimal response and mitigation measures. While it is obvious even for inexperienced persons to diagnose the type of attack from the sheer physical destruction obtained in an explosion, currently reliable quantitative data is not available. The proposed APSS exploits the existing network of sensor for detecting, localising and quantifying explosive attacks and modules to determine the impact of the attack in terms of potential casualties and structural damage.

Detection Analysis of Electromagnetic Attacks

Intentional exposure to electromagnetic (EM) radiation is an emerging physical threat. High-power microwave (HPM) is characterized by pulsed wideband or narrowband radiofrequency (RF) emissions at frequencies of up to several GHz, with pulse widths in the range of picoseconds to microseconds and field strengths of up to kilovolts per meter. High power microwave radiation is able to destroy electronic equipment or disturb its function significantly. With the emergence of portable HPM sources in the past years, a new threat arises for all types of infrastructures that critically depend on electronic systems, including airports. Detector systems for HPM are only available for laboratory use. Commercial devices suitable for use in airport infrastructure are not available. Apart from the important capability to be able to detect an electromagnetic attack, just as with explosive attacks, the resilience of the airport, the people in it, its surroundings and society more broadly would be strengthened if reliable and quantitative data could be provided and analysed in a timely manner

to determine the optimal response and mitigation measures. In the APSS approach, the sensors for detecting, localising and quantifying electromagnetic attacks are taken into consideration. Moreover, a module to determine the impact of the attack in terms of destroyed and/or damaged electronical equipment is connected with the core idea.

Cyber-attacks Surface

Airports and organisations within have many networks in connection with different focuses for different processes, including the security process, and which are also networked to third party services, such as Sabre, Amadeus and Travelport, e.g., to distribute real-time flight data and to run internal reservations systems, departure control systems boarding process, last minute bookings and seat assignments. Examples of cyberattacks of particular concern are Denial of Service (DoS) and distributed Denial of Service (DDoS) attacks on network equipment usually through anonymous attackers. Prevention of cyberattacks is to be furthered through continually implementing updated best practices and recommendations, which respond to the fast-moving development of cyber threats.

Data Fusion Engine (DFE) and Web Portal

The proposed solution exploits a DFE, which incorporates the latest technologies, is scalable and empowered with the flexibility to expand and enrich the system by adding new sensors and applications according to specific requirements and future needs. The scope of a DFE is to monitor each airport security sector by tailored technologies which are incorporated into the system, creating a multisource fusion logic, alert prioritization and impact analysis which enables situational awareness and decision making of the airport anytime, anywhere. A Web portal transforms the process into a user- friendly interface and presents alert information and impact analysis result to the operator in a straightforward and clear manner. This enables an advanced, more accurate decision-making process in the face of the growing multitude of threats and dangers each airport is faced with on a daily basis.

The APSS Approach

The proposed architecture of APSS is provided in Figure 2.

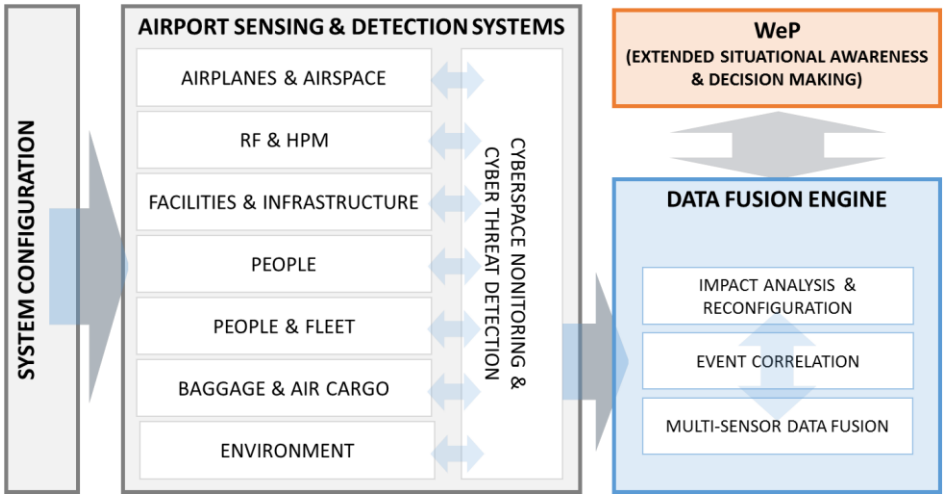

Figure 2: APSS Logical Architecture.

In this architecture the airport sensing and detections systems are divided into major sectors, which can be briefly described as follows:

- Airport facilities control: Perimeter and inbound sensitive areas surveillance, both indoor and outdoor (terminals, hangars, turf, parking areas, fuel storage and pipelines, storage areas, peripheral and surrounding areas, etc.);
- People control: Passengers and air-crew acting as terrorist operatives (both witting and unwitting involvement), airport personnel, visitors, suppliers etc. including people access and boarding control. The technologies in this segment will not be sensed by the passengers and will not interrupt the passengers' smooth flow.
- Fleet control: All airport fleet vehicles, automobiles and truck control;
- Cargo control: Carry-on baggage, checked, hold baggage, air-cargo and air-food/beverages control including their access and boarding control;
- Airplanes and airport-air-space access control, including physical damage to aircraft;
- Environmental control: Air-quality and drinking water monitoring for chemical and biological agents;
- Cyberspace: cyber monitoring for cyberattacks and response actions.

Results in the previous TASS EU-project,[8] indicated that the division of sensing and detection sectors is a method to leverage protection against physical and cyber threats and incidents. The APSS approach is proposed to fuse data from detection and sensing systems already used by airports. In APSS detection, localisation and quantification systems will be developed for GNSS Interference, explosive, electromagnetic (EM) and cyber-attacks and incidents.

In the Data Fusion Engine (DFE) each of these sectors are monitored in real time and the data generated by the different technologies will be processed in a series of steps, in overview:

- Fusion of "homogeneous" data generated by sources and technologies within the same sector;
- Fusion of "heterogeneous" data generated after the first step (correlation) and detection of anomalies;
- Analysis of the actual or potential impact of the threats detected on airport functions, neighbouring populations and the environment;
- Determination of proposed mitigation and response measures for either automatic or manually supervised implementation.

The fused technologies are already used by airports (in-place technologies), yet in a "stand-alone mode." This mode is less effective in creating a comprehensive intelligence system compared to the "fused mode." The APSS approach brings the capability to integrate these in-place technologies (mobile and fixed) and eventually also novel detection technologies and to fuse their collected data into a central point where it will be analysed together with data from external sources.

The potential impact on the quality of service of airport functions and the ability to make reconfiguration/mitigation proposals requires that both the relevant technical systems architectures and business processes within the airport are part of the information behind the rules implemented in DFE. The potential impact on the neighbouring populations and surrounding environment also requires that the key and critical characteristics are defined. In PASS approach, impact analysis modules foresee for (i) explosive attacks – structural and human impact, (ii) HPM on airport equipment, (iii) GNSS interference, (iv) Space weather; and cascading effects.

A web portal will alert and display the collected data of each operational area, its analysis and actions taken and/or proposed to respond and mitigate against the attacks and/or incidents. Information will be provided to all relevant stakeholders, including, but not limited to monitoring teams, security teams, rescue teams and the general public. One of the major advances introduced by APSS is the use of web-portals as hubs for real-time, actionable information. The WeP will include an interoperable service support environment that will allow the integration of new data access or data processing services at run time, i.e., the portal can be tailored at run time to the current situation. Additionally, and in contrast to existing applications, the "thin client" use will be supported, implying users will need little more than a web browser and no especially installed software to operate the portal.

The initial correlation of alarms within the same segment and the final correlation of the alarm coming from different segments dramatically increase the confidence level of the threat detection, minimizing the false (positive and negative) rate and allowing the proactively impact analysis of such threats and

the consequent protection countermeasures. This is the real innovation aspect of the APSS concept.

Conclusions

It is rather obvious that critical infrastructure protection, i.e., of airports, cannot be carried out anymore with traditional concepts.

Considering the interconnections and networks between the various parts of the "airport system" as a whole, we have to take into account a high number of independent information sources in order to have a real-time, complete operational overview of the system's status and suspect threats. An extended fusion of this information to enable threat detection involves high false (positive and negative) rates, so it is very difficult to tune the security systems and permit the normal operational activities of the airport. *This is a crucial point to ensure that the security system is not a weak point in security per-se.*

APSS is a completely new concept and the proposed methodology has never been used so far. APSS is an innovative methodology to design physical-cyber airport security systems able to dramatically increase the threat detection power, minimizing the false (positive and negative) rate. The key idea is to:

- divide the airport security in multiple security-control segments (i.e., facility control, person control, vehicle control, cargo control, aircraft control, air/water environment control);
- fuse the data coming from all sensors (legacy and new) within each segment and correlate the different alarms within the same segment for generating the detection events ("*single-segment detection events*");
- correlate the different single-segment detection events coming from two or more segment for generating the "multi-segment detection events";
- analyse the impact of each multi-segment detected threat on airport security;
- carry on the countermeasure against the detected threats.

According to this approach, it is possible to tune the sensing and detection systems within each segment in order to minimize the false rate and, consequently, to correlate detection events having good confidence level coming from different segments. This correlation further increases the confidence level of the threat detection, allowing a proactive countering of such threats.

It must be stressed that the proposed methodology and its outcomes are not tailored toward any critical infrastructure (i.e. airport) in particular, as we believe that it should be applicable to any critical infrastructure system protection with minimal or no effort.

References

[1] Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon, "The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel," *The Journal of Law and Economics* 50, no. 4 (2007): 731-755, available at https://ssrn.com/abstract=1007534 or http://dx.doi.org/10.2139/ssrn.677563.

[2] COPRA (FP7-SEC-2011-261651) EU research project, "Aviation Security Research Roadmap," D5.1 (2013).

[3] Peer Schouten, "Security as Controversy: Reassembling Security at Amsterdam Airport," *Security Dialogue* 45, no. 1 (January 2014): 23-42.

[4] H. George Frederickson and Todd R. LaPorte, "Airport Security, High Reliability, and the Problem of Rationality," *Public Administration Review* 62 (2002): 33-43.

[5] Clifford Sweatte, "Method and System for Airport Security," U.S. Patent No. 6,335,688, January 1, 2002.

[6] E.g. Global Positioning Service (GPS), Europe's Global Satellite Navigation System (Galileo).

[7] See, for example, Guy Buesnel, "GPS Spoofing Is Now A Real Threat – Here's What Manufacturers of GPS Devices Need to Know," *Spirent blog*, September 14, 2015, http://www.spirent.com/blogs/positioning/2015/september/gps_spoofing_is_a_real_threat.

[8] Total Airport Security System, TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities, https://cordis.europa.eu/project/rcn/94264/factsheet/en.

About the Authors

Walter **Matta** received the Degree in Electrical Engineering (with honours) in 1994 from the University of Cagliari, Italy. He has worked in Aerospace, Security and Defence since 1996, covering roles of increasing responsibility in big companies and in national and European organizations. Currently, he is full professor at Link Campus University.

Dr. Alessandro **Cantelli-Forti** is a computer engineer with a Ph.D. in information technology engineering with a doctoral thesis titled "Mitigation and Incident Management Methodologies for Critical Infrastructure Protection." He is currently a researcher and an accident investigator in critical transportation systems.