Defending European Airports: Cyber-Physical Threat Analysis in Total Airport Management

Chris Johnson, Matt Shreeve, Piotr Sirko*, Olivier Delain*[†]*, Olivier Ruhlmann*[†]*,*

Eric Vautier[†]*, Bob Graham*[§] *and Marie-Therese Meloni*[§]*,*

School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

**Helios, 29 Hercules Way, Aerospace Boulevard, AeroPark, Fanborough, GU14 6UU, UK.*

[†]*Groupe ADP, 291 Boulevard Raspail, 75014 Paris, France.*

[§]*EUROCONTROL Experimental Centre, BP 15 – 91222, Brétigny Sur Orge. France*

Keywords: Aviation, Airport Operations Centre, Cyber Security, SESAR, Safety.

Abstract

In the past, airports relied on a host of information systems and control applications that were loosely integrated. The software infrastructure components that supported water, heating and lighting systems did not exchange data with baggage handling applications, nor with air traffic management systems. In turn, these infrastructures were isolated from information systems to aid passenger movements through check-in to departures and onto the aircraft. Many airports have, however, begun to implement Airport Operations Plans that improve situation awareness and support collaborative optimisation through increased levels of integration and connectivity. This paper identifies different architectures that support a new generation of Airport Operations Centres (APOC). Subsequent sections summarise the cyber security threats that arise from inter-connection and inter-dependence. The closing paragraphs present mitigations that increase the cyber resilience of APOCs and also address a number of associated safety concerns.

1 Introduction

Airports have traditionally focussed on physical security. Policies and procedures ensure the separation of airside and landside operations. Sensing devices have been deployed to identify unauthorised attempts to cross this divide. The architecture of airports has evolved with physical barriers to prevent attacks similar to that on Glasgow airport in 2007 or in Brussels during 2016. These security mechanisms impose considerable costs in terms of direct investment but also in terms of delays and inconvenience for the travelling public [1,2]. At the same time, airports have become more interconnected [3]. Increasingly complex software systems merge information from, and provide information to, a host of stakeholders including the airlines but also security service providers, facilities management teams and infrastructure subcontractors [4]. This helps optimise throughput for traffic mix and the consequent requirements for baggage handling, for infrastructure support and for physical security screening. Some airports monitor meteorological information and use this data to plan for the knock-on effects of delays and cancellations. There are growing interconnections with Air Navigation Service Providers (ANSPs). Partly in consequence, the International Civil Aviation Organisation (ICAO) has developed the Airport Network information eXchange Model (ANXM), based on ICAO Annex 14 and Doc 4444, enabling the digital exchange of airport information at local, regional, national and international levels [5]. In consequence, airport operations now depend on the close coupling of heterogeneous software systems exchanging data over network architectures. The previous focus on the physical security of staff and passengers is now shifting to consider a range of cyber-related threats. These have the potential to interrupt airport operations and threaten safety – by disrupting critical services. They may also help facilitate physical attacks if attacks compromise the integrity of the screening systems used by security staff.

2. Total Airport Management

The SESAR European programme for the modernisation of Air Traffic Management has promoted the concept of Total Airport Management (TAM), reflecting the evolution towards a performance-based ATM system. The notion of performance management is therefore the cornerstone of the future airport concept, which foresees an integrated airport management framework. The airport operations management concept relies on the creation and maintenance of an Airport Operations Plan (AOP) as the single, common and collaboratively agreed rolling plan used by all involved stakeholders at an airport [6]. This helps optimise flow management of airport demand against existing and future capacity. Airport Demand Capacity Balancing (A-DCB) must be robust against a host of complex, dynamic constraints including the availability of aircraft stands, the impact of weather, as well as noise and environmental restrictions. The airport in the concept can be seen as a ground sector of the ATM Network which will be achieved through the full integration of AOPs with the NOP (Network Operations Plan), supported by SWIM (System Wide Information Management).

The aim of TAM is to steer, monitor, manage and perform post analysis of airport performance. It relies on an airport performance framework based in agreed and refined key performance indicators and airport performance targets. This integrates landside functions, facilitating passengers and cargo operations, with the airside functions that handle aircraft on the ground but also during arrival and departure. The scope of TAM also covers other aspects that may influence the overall airport performance such as transport networks (road access, rail, metro, car parks, etc.), critical networks (electricity, telecom, fuel, etc.) and meteorological aspects. Collaborative decision-making will be optimised through robust and predictive monitoring tools, what-if decision support tools, self-learning business intelligence and user-defined performance dashboards. Benefits include increased predictability and resilience of operations, greater pro-activity and efficiency to cope with both nominal and adverse conditions. In order to support collaborative decision making, it is important to provide an underlying concept of operations and architecture for distributed and scalable information management across these complex socio-technical systems.

TAM objectives are delivered through an AirPort Operations Centre (APOC), as the heart of airport performance. It is a platform / operational structure which pro-actively manages the performance of present and short-term airport operations, giving relevant airport stakeholders a common operational overview of the airport, and allowing them to communicate, coordinate and collaboratively decide on their progress. It is intended to monitor airport performance and help identify situations that require operator intervention in response to external events, including bad weather but also disruptions across complex, integrated supply chains. APOC operations must:

- Maintain performance during nominal conditions, degraded modes and recovery, especially when this involves cooperation between the airport and air traffic network management;
- Encourage and sustain collaborative information sharing and cooperative procedures in the planning of routine, atypical and adverse operations.
- Help real-time recover management in response to adverse weather and ‘exceptional’ operating conditions;

A number of different approaches have been taken to the physical implementation of APOCs. For example, a scalable APOC has been implemented at Paris Charles De Gaulle airport supported by digital integration and information exchange between distributed teams that are not located within the same control room. Depending on the situation, the APOC can be reconfigured to cover airport stakeholders' need and situations, linking with airport centralised functions and command centres (parking and access, terminals, airside operations, de-icing) and with police, customs, Grouped ADP headquarters, civil aviation authority (French DGAC). As an example, 68 disruptive situations were pro-actively managed in 2014 (storms, strong wings, strikes, technical failures etc.) in Paris Charles de Gaulle APOC, limiting the impact on their customers and preventing these disruptions to escalate in crises. This approach offers a flexible and cost-effective solution. In contrast, Heathrow opened a bespoke APOC in 2014 where airlines, the ANSP NATS, the UK Border Force, the Metropolitan Police and the Highways Agency all sit within the same control room.

The benefits and challenges of TAM can be illustrated through recent validation exercises for Time Based Separation (TBS) at Heathrow. Aircraft during final approach are routinely expected to maintain fixed separation minima this distance is intended to ensure that following aircraft do not encounter the wake vortex of preceding flights. However, strong headwinds will reduce the ground speed of an aircraft on final approach leading to a reduced landing rate with delays and cancellations. TBS reduces the separation between aircraft because stronger winds will help dissipate a wake vortex. Initial trials have shown that TBS could allow up to five extra aircraft per hour in strong wind conditions, and reduce holding times up to 10 minutes at Heathrow. However, safe landing rates are also determined by the aircraft’s final approach speed and deceleration profile. In consequence, the use of such optimisation techniques will only succeed if the landside infrastructures are tuned to respond to changing traffic patterns. Stakeholders must work together to ensure that stands are available, that ground handlers are ready and that outbound aircraft are prepared to make use of the available departure slots.

3. The Challenge of TAM Cyber Security

The interconnectivity of airport operations increases concerns over cyber-security [7]. Many of the initiatives, cited in previous sections, focus on cost reduction not information integrity. In consequence, the associated protocols and networks are vulnerable. Many are unauthenticated and some existing traffic is unencrypted.

There are important differences between airport operations and more conventional safety-related applications. In particular, there are cyber-physical threats where an attack on information infrastructures can expose or leverage vulnerabilities in physical security. For example, undermining the integrity of digital systems can be used to compromise the level or protection offered by CCTV installations and access control cards. These concerns are not 'science fiction'. A recent attack on information systems in Antwerp was able to hide the importation of drug and weapons through the port [8].

Cyber security concerns for Total Airport Management extend well beyond the conventional enterprise architectures that characterise many other information systems. Airports are unusual because they also integrate Industrial Control Systems (ICS)/ Supervisory Control And Data Acquisition (SCADA) infrastructures. Power, heat and lighting distribution also rely on relatively low-level sensors and Programmable Logic Controllers (PLCs) rather than conventional mass-market processors. Automated, baggage-handling systems are controlled by similar devices that operate over Profibus and Modbus rather than TCP/IP. SCADA devices are vulnerable because most were designed and deployed in an era before cyber security was an explicit concern for system procurement. An attack on PLCs and sensors controlling air conditioning units would undermine higher-level enterprise information systems and the digital interfaces to physical security networks.

TAM concepts must also consider a host of safety concerns that do not arise from the cyber-security of many more conventional office-based systems. For example, APOC stakeholders include representatives of local ATC and airspace users who ensure the safe and efficient movement of aircraft on taxiways and runways. Their performance affects all other aspects of the APOC hence there is a need to integrate data from their applications with the wider information ecosystem. Many of the software tools used by the Tower crew are safety-related, for instance, controlling sectional lighting to help coordinate aircraft movement. It is conceivable that some cyber threats might trigger loss of life, by exploiting vulnerabilities in the sectional taxiway lighting systems. However, system diversity and human monitoring make this relatively unlikely – aircrew and Tower personnel will notice abnormal behaviour. However, other concerns focus on denial of service (DoS) attacks. Traditionally, these overwhelm network components with spurious requests. In safety-critical systems, operators will intervene to halt a service if they suspect that it has been the target of an attack. For instance, Tower staff will reduce traffic and eventually close the skies if they cannot trust the integrity of data from arrivals and departure management.

4. Potential Attackers?

As mentioned in previous sections, this paper summarises the initial phase of a cyber security threat assessment for the TAM concept of operations. Some airport stakeholders still question whether anyone would deliberately target the infrastructures that they operate. This attitude is gradually fading as more information is disseminated in the aftermath of STUXNET, DUQU, the Ukrainian attacks etc. There is a growing awareness of the range of potential attackers with an interest in disrupting airport operations, these include but are not limited to:

- Individual hackers - the intellectual interest and potential for personal gain by being associated with such a global and high-profile mode of transportation;
- (H)activists - local and policy interests in the environmental, safety and economic factors of aviation are high, with the European dimension giving added interest;
- Insiders (employees, contractors, etc.) - the trusted-insider-turned-attacker is always concerning simply due to their level of authorised access. With TAM, increasing collaboration and industrialisation means more contract engineers having more access, and individual circumstances or events (sometimes linked with broader factors such as tough economic times) can lead to them posing a threat;
- Business competitors - those seeking a competitive advantage through industrial espionage of technologies, operational insight, business plans, etc, can pose a threat;
- Terrorists: as aviation has long been the target of serious and symbolic attacks, and the public is already sensitive to safety fears, terrorists could aim to attack through solely cyber-means, or perhaps are more likely to use sensitive information obtained through a cyber-attack to launch a more conventional attack such as a hijacking or bombing based on the cyber-physical scenarios identified in previous paragraphs
- Organised crime- the sheer costs of cancelling or disrupting flights could elicit financial reward if held to ransom, or through the theft of intellectual property. Airports are also centres for a host of high high-value operations – ranging from commercial on-site operations through to the transport and storage of cargo items;
- State cyber-forces: any country's airport infrastructure is an important economic and social target, as well as being a critical national infrastructure and potentially a means to achieve geo-political advantage, particularly during times of high regional tensions. Disruption to hub airports would have an impact not only on local business but also in many countries macro prosperity.

The distinctions between these different groups are blurred – for example, terrorist groups might leverage an attack using zero day exploits that can be purchased from criminal peer to peer networks. Groups such as ISIL have trained airport engineers within their territories; these individuals have the knowledge necessary to leverage future threats so that they resemble an insider attack [9].

5. Cyber-Strengths and Vulnerabilities

The particular vulnerabilities of an APOC depend on the technologies used, on their deployment and operation as well as associated maintenance. However, like many aspects of both the US NextGen and European SESAR movement, TAM creates a common set of concerns:

- New attack propagation vectors: The increased number of interconnections between TAM stakeholders and between business and operational systems increases the attack surface and creates new attack propagation vectors. Cyber-attack payloads could be propagated across common services;
- Increased level of exposure: The use of open public internet network may be chosen by stakeholders as low-entry means of communication and thus might increase the level of exposure of particular components within an APOC;
- Increased transactions: Whereas limited data is exchanged today between some APOC components and between stakeholders across Europe, the implementation of TAM will drastically increase the number of data types exchanged between stakeholders in support of CDM. More opportunities will be offered to attackers to alter the integrity of multiple data types;
- Possibilities of multi-target cyber-attacks: Openness and net-centric architecture create opportunities for multiple, coordinated cyber-attacks enabling more systemic or European-wide impacts, especially with APOC architectures supporting multiple airport operators;
- Publication of vulnerabilities: Whether explicitly through Computer Emergency Response Teams (CERTs) or through public leaks of common vulnerabilities in APOC components such as the SWIM protocols and communications stacks may facilitate attack planning and design;
- Varying levels of cyber-security maturity across the numerous APOC stakeholders' may create weak links in the cyber-security supply chain.

Conversely, the development of TAM concepts and their delivery through APOC architectures also provides opportunities for mitigation:

- Cyber-security coordination that improves the sharing of information (risk assessments, vulnerabilities assessments, threat assessments, etc) and provides coordinated incident response. This is particularly important between APOCs across Europe but also within the stakeholders of TAM. Depending on the nature of an incident, it will be important to coordinate forensic support and available resources to aid recovery;
- Coordinated approach or security management. APOCs and the associated management structures help to pool resources and to ensure that all partners meet their obligations – for instance, in ensuring the application of security patches;
- Standardised interfaces for services, in particular, for security applications to reduce the potential for abuse and subversion. More specifically common formats support the use of whitelist intrusion detection which relies on network and systems managers being able to recognise valid processes;
- Sharing with other sectors fixes, advances and investments in cyber-security for COTS components. A key concern with the development of APOC infrastructures is to benefit from economies of scale and move away from high-cost bespoke applications;
- Reducing complexity and overheads, thereby reducing mistakes and unauthorised configurations. This is important because, typically, the more security features that are embedded within a system then the more important it is to ensure that they are correctly configured when deployed within an airport environment.

Particular implementation architectures also offer particular benefits for cyber-security. For example, the use of virtualised or service oriented APOC architectures means that application processes can be clustered on common servers. Redundancy and diversity can then be used to increase the resilience of centralised computational resources. It is arguably easier to manage the cyber-security of these implementations than ensure thousands of distributed machines are correctly configured and patched across airport infrastructures. Other APOC infrastructures, associated with SCADA components cannot be virtualised in this way. In such situations there is a tension between the use of 'air gaps' that isolate PLCs and sensors from networked attacks and the need to enable ICS integration with the TAM concept of operations.

6. Cyber Threat Scenarios

Previous sections have argued that cyber risk assessments for Total Airport Management must consider an evolving range of potential attackers. It is also important to take a balanced approach to both the strengths and the weaknesses derived from APOC architectures as we move from basic research to initial deployment [10]. Scenarios and use cases provide important tools in this work. The intention is not to enumerate every possible cyber threat to airport infrastructures. Instead, the aim is to expose existing vulnerabilities that can have a credible impact on safe and successful operation. They provide a focus for discussion between multiple stakeholders and across national borders. The following paragraphs present an initial subset of these TAM scenarios.

6.1 Unauthorised Disclosure of Operational Data

In this scenario, an activist group is campaigning against the expansion of an airport. Their aim is to highlight environmental damage by launching a cyber-attack on the APOC information systems. They use a spear-phishing attack on junior airport management that is then used to leverage access to the long and medium term planning data held within an APOC. The hackers begin to selectively exfiltrate a range of sensitive information – this includes personal details about airport staff home addresses so that they can become targets for direct action. They place company financial information on externally facing web sites; revealing data about the financial remuneration of key staff and also the sums paid to sub-contractors.

The activists export data about the airport's environmental impact – including the violation of night curfews. By identifying high-level APOC KPIs, the compromised systems yield safety performance data that is leaked to media and regulatory organisations. The activists find evidence of situations where minimum separations were violated over densely populated areas on approach or departure – threatening the communities that play a key role in the future expansion of the airport. Their analysis is missing many elements (e.g. air-ground data-link and radio communication records) to provide a distorted but plausible story, which is amplified on social media. Politicians and the public begin to question stakeholders about the cyber-security of APOC operations. The material is reformatted to undermine confidence in the airport and, especially to stress the apparent lack of cyber-security in an organisation that plays an important role in the preservation of public safety.

6.2 Ransomware Attacks through the Supply Chain

In the second scenario, the pressure for improved productivity alienates a software engineer at a major APOC systems supplier. They are rushing to meet a deadline and breaking company policy, decide to integrate unattributed source code from a public repository into their modules. Time pressures mean that this is not identified during Verification and Validation. In any case, their company will only use independent reviews for safety critical software. Months later when integrated into an operational system, code that is hidden within the public source is now executed. The malware is modelled on the attack vector that was embedded within STUXNET. Initially it does nothing. However, after some days it begins to send corrupted packets onto shared network infrastructures. The intention is not to force a collapse or to launch a DoS attack but to undermine confidence in the engineers from several sub-contractors who must diagnose the source of the problem. The APOC implementation is not designed to support forensic analysis nor are the engineers trained to consider anything other than more routine bugs. The malware then hides itself by halting any network communication. Engineers fail to find the cause of the problem and normal operations are resumed – hence there is a huge loss of confidence when the problem returns again some time later. This leads to massive disruption, undermining trust in the APOC and the associated ATM systems. There are calls for root-to-branch review of critical code but there is insufficient expertise available to do this and the APOC is not supported by sufficient logging or by the necessary IPR agreements to identify the source of the problem.

A variant on this scenario is that instead of consuming critical resources such as network bandwidth, the hidden code might attack configuration data. This would again undermine the stability of the APOC. Without appropriate recovery mechanisms it might take a significant amount of time to detect and diagnose the cause of the problem. Another observed method of attack focuses on the integration of VOIP communications into APOC architectures. Previous attackers have introduced code that either jams all communications within the APOC by mass calling of their numbers or incurs huge financial costs by using the internal VOIP code to place unintended premium calls on behalf of the APOC stakeholders.

The motivation for this attack might be financial gain through the increasing prevalence of sophisticated and embedded ransomware. APOC stakeholders would continue to suffer until either they found the source of the malware embedded in the sub-contractors code or transferred ledger-based payment.

6.3 Advanced Persistent Threats

A third scenario focuses on a dispute between two neighbouring states. This leads to sanctions being imposed, which exacerbates tensions and triggers further reactions. Not wanting to provoke a military response, an antagonistic cyber-attack campaign is planned. This is focussed on high-value infrastructure operations; including power distribution but also the major airports. The antagonist has access to engineers and technicians who have been trained by the same suppliers as the other APOC operators. However, they have been combined into the offensive arm of the nation's intelligence agencies with the remit to first map out and then potentially exploit weaknesses in cyber infrastructures.

The antagonists have access to a national testbed for SCADA systems and the associated sensing devices. They are then able to mimic aspects of the Ukrainian attack, cited earlier, for instance infecting the firmware on ICS components without being detected on the field devices that are used throughout the airport. In this case, the application of conventional security management practices means that maintenance teams act in a rigorous manner to upload the infected malware through system patches even on air gapped devices. Initial tests are conducted through TCP/IP interfaces to the control system protocols – for instance, forcing a collapse of the power system by triggering firmware faults in voltage relays immediately after unusual levels of solar activity. The intention is not to disrupt operations but to conduct a weapons test in such a way that the true nature of the intrusion is masked by a secondary event.

The implications of this form of attack on national security are immense – the activation of poisoned firmware might be triggered in a random and distributed fashion to undermine confidence as in the second scenario. Again forensics would be hard because of the proprietary nature of SCADA Devices in APOCs and the present tendency simply to rip and replace failed devices rather than conduct lengthy code debugging cycles. A more malicious alternative would be to trigger the code during the escalation of physical attacks, as was seen during the Russian conflict in Ossetia [11].

7. Mitigations

These scenarios are based on previous incidents that have affected other industries. They can be criticised because they focus on the particular impact for TAM but they stem from more general methods of attack. However, they are justified because each one is grounded in evidence from previous occurrences and it seems unreasonable to assume that aviation will be immune from the troubles that have affected other industries. In some cases, we can address these concerns by transferring lessons from other domains. For example, there is a clear need from all three scenarios to ensure that engineers have the forensic evidence necessary to identify and diagnose potential attacks. There are, unfortunately, particular challenges in re-using the lessons of other industries. For instance, many of the APOC/TAM concepts have not considered process and resource profiling, the importance of authentication and access control, the need to train staff to distinguish between 'normal' degraded modes and cyber incidents or provided means of preserving the chain of evidence. It is important to reiterate that the aim of these vignettes is not to conduct an exhaustive risk assessment given the huge differences in APOC architectures and the evolving nature of APOC services – however, these scenarios are important because they provide a focus for discussion and help to ensure that cyber-threats are considered when stakeholders work with project sponsors to refine the high level concepts that were introduced at the start of this paper.

It is important to stress that the examples in this paper are a subset of the concerns that have guided our work and from them we identify the following mitigations that seem essential for the future integrity of APOC/TAM implementations:

- Supply chain management – APOCs are specifically intended to bring together groups of stakeholders who previously operated isolated systems. This integration unifies many different supply chains; the subcontractors and suppliers vary enormously in terms of their cyber maturity.
- Resource profiling – even new APOCs integrate many different legacy systems. The operators often lack the intellectual property rights to access process and memory structures for those systems hence it can be hard to support intrusion detection.
- Incident reporting – if we cannot yet accurately profile all of the admissible processes in our network, we might support APOC intrusion detection by identifying malware using information about previous attacks. This depends on sharing attack signatures especially between APOCs that operate similar, specialist applications not covered by existing security firms.
- Forensic support – all of the scenarios raise questions about the evidence that can be obtained in the aftermath of a suspect intrusion. TAM requires that stakeholders consider whether they have enough data logged to identify the causes and extent of an intrusion.
- Regulatory interfaces – many APOC services are safety related. In consequence, operators need to know whether they should immediately halt operation when an incident is detected. This would have a huge impact on availability given the clear possibility of false alarms. Regulatory support is also required to determine when it is safe to resume operation given the persistent threat are deliberately hard to identify.
- CERT assistance – it is likely that a European-wide aviation Computer Emergency Response Team will be developed. The future integrity of TAM implementations will benefit greatly from closer interaction between their operators and this future organisation.
- KPI interaction – the APOC concept is intended to meet a wide range of KPIs through airport information system integration. Increased levels of cyber-security are likely to have an impact on those KPIs – for example in response to false alarms within an intrusion detection system or through increased costs of supply chain management. Hence, some help needs to be provided to APOC operators when they draw up a business case to consider the costs and benefits of investing in cyber-resources.

As can be seen, some of the mitigations are APOC specific while others are more generic, however, all can influence and shape the emerging TAM concepts of operation.

8. Conclusions

This paper has introduced the twin concepts of Airport Operations Centres (APOCs) and Total Airport Management (TAM). Together, these provide a vision of greater efficiency, increased levels of safety and reduced environmental impact through collaborative decision making that is informed by the integration of information systems.

These objectives will be undermined if we cannot ensure the cyber security of future implementations. This paper has identified a range of possible vulnerabilities and has used three scenarios with different actors, different levels of technical sophistication and different consequences on airport operations. Each is based on previous attacks on other industries – this is important if we are to show that the threats are credible. However, each scenario has been reinterpreted in the context of APOC operations with the aim of ensuring that detailed and specific cyber concerns are considered as TAM infrastructures move from research to deployment. The closing sections have identified a number of mitigations – some generic and other specific to airport systems. It remains to be seen whether these concerns inform future systems or whether we are left to pick up the pieces after deployment.

Acknowledgements

This work was supported by the SESAR Joint Undertaking Programme under Operational Focus Area ‘ Airport Operations Management (OFA 05.05.01).

References

[1] Wong, Solomon, and Nina Brooks. "Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry." Journal of Air Transport Management 48 (2015): 60-64.

[2] Sakano, R., K. Obeng, and K. Fuller. "Airport security and screening satisfaction: A case study of US." Journal of Air Transport Management 55 (2016): 129-138.

[3] Choi, Jin-Ho, and Jin-Woo Park. "A study on factors influencing ‘CyberAirport’usage intention: An Incheon International Airport case study." Journal of Air Transport Management 42 (2015): 21-26.

[4] Marks, Adam, Kees Rietsema, and AL-Ali Maytha. "Airport Information Systems—Landside Management Information Systems." Intelligent Information Management 7.03 (2015): 129.

[5] EUROCONTROL, Airport Network Information Management: Draft ANCM/ANXM Models, Brussels, December 2007.

[6] EUROCONTROL, Airport Operations Centre, http://www.eurocontrol.int/articles/airport-operations-centre-apoc, last accessed June 2016.

[7] Smith, Wayne. "Cyber security in airports." Journal of Airport Management 9.3 (2015): 232-238.

[8] EUROPOL, European Cybercrime Centre, Hackers Deployed to Facilitate Drugs Smuggling, Notification 004, June 2013, last accessed June 2016. https://www.europol.europa.eu/sites/default/files/publications/cyberbits_04_ocean13.pdf

[9] C.W. Johnson, Cyber Security and the Future of Air Traffic Management: Identifying the Challenges for NextGen and SESAR. In C. Sandom, C. Johnson, P. Casely, M. StJohn-Green and R. Piggin (eds.), 10th IET System Safety and Cyber Security Conference 2015, The IET, Savoy Place, London, 2015.

[10] C.W. Johnson, Innovation vs Safety: Hazard Analysis Techniques to Avoid Premature Commitment in the Early Stage Development of National Critical Infrastructures. In Don Swallom (ed.), Proceedings of the 32nd International Systems Safety Society, Louisville, USA 2013, Unionville, VA, USA, 2014.

[11] C.W. Johnson, Anti-Social Networking: Crowdsourcing and the Cyber Defence of National Critical Infrastructures, Ergonomics, (57)3:419-433, 2014.