SESAR
JOINT UNDERTAKING

Addressing airport cyber-security

Final report

founding members

EUROPEAN UNION

EUROCONTROL

Document information

Document title	Cyber-security application for SESAR OFA 05.01.01 - Final Report
Author	Olivier Delain, Olivier Ruhlmann and Eric Vautier (Groupe ADP) Prof Chris Johnson (University of Glasgow) Matt Shreeve and Piotr Sirko (Helios) Veronika Prozserin (Eurocontrol)
Produced by	Helios
Produced for	This study was undertaken within the context of SESAR Project 06.03.01[1] and led by SESAR member, Eurocontrol, in collaboration with Helios, Groupe ADP and Professor Chris Johnson from the University of Glasgow.
Produced under contract	16-220098-C
Version	V1-00
Date of release	15 November 2016
Document reference	P2232D003 (Internal) / OFA 05.01.01- D3 (External)

[1] The study supports the SESAR Operation Focus Area 05.01.01 "Airport Operations Management" and SESAR Project 06.03.01 "The Airport in the ATM environment".

Revision history

Version	Date	Author	Description of the changes
0-01	13/6/16	Matt Shreeve	Initial structure for internal review
0-02	18/8/16	Matt Shreeve	Initial collated version
0-10	19/8/16	Matt Shreeve	Draft for review by EUROCONTROL
0-20	30/9/16	Matt Shreeve	Draft for review by EUROCONTROL
0-30	11/10/16	Matt Shreeve	Draft for internal review
0-40	19/10/16	Matt Shreeve	Draft for review by EUROCONTROL
0-50	31/10/16	Matt Shreeve	Final draft for approval
1-00	15/11/16	Matt Shreeve	Release

Approval

Date	Name	Role
15 November 2016	Eric Vautier	Group ADP CISO
	Prof Chris Johnson	Cyber-Security Expert
	Matt Shreeve	Study Manager and Cyber-Security Expert

Executive summary

The APOC is critically important…

The compromise of the availability and/or integrity of information systems will have a profound impact on the CDM (Collaborative Decision Making) that is at the heart of APOC (Airport Operations Centres) and TAM (Total Airport Management). Even with a downtime of two hours of the APOC (or key components like the Airport Operations plan (AOP) or Local Area Network (LAN)) flights will be delayed or even cancelled. The impact of such disruptions can be huge, given the importance of airports for the economy. For instance, according to ACI Europe (2015) Paris Charles De Gaulle airport directly contributes €9.5 billion to France's GDP – which amounts to approximately €26 million per day and over €1 million per hour.

But may be built on insecure legacy infrastructure…

Given current legacy systems and services, airports may well decide to build APOC and CDM on top of untrustworthy, unauthenticated data sources and insecure networks and industrial control systems. With an insecure foundation establishing trust in the APOC and the underlying supply chain is impossible.

… and extended supply chains may increase security risks

System integration increasingly results in extended supply chains where each stakeholder relies on services provided by their partners, but which might be delivered by third party companies. An extended supply chain inherently means more people having physical and/or digital access to core systems and infrastructure, which poses security risks.

A compromised APOC could 'pollute' the European ATM Network

Data exchange between airports and the wider network (e.g. the synchronising AOP and Network Operations Plan (NOP)) means that the NOP will not be updated from the AOP if the AOP is disrupted. In the worst case scenario, the NOP will be updated with incorrect information and propagate this to other parts of the network.

Two future scenarios exist: dystopian where cyber-security is not a priority…

If cyber-security is not prioritised and remains unaddressed, we will face a dystopian future with high cyber-risk and will fail to exploit the modernisation and benefits that SESAR promises. This will adversely impact European aviation as a whole. The worst case is that with increasingly skilled attackers, airports are frequently disrupted.

… or utopian where APOCs are 'secure by design', a more cost-effective approach

Fortunately, the opportunity exists to fix these problems and achieve a more utopian future in which technology and data drives performance improvements for all. Most directly this means building in the right security requirements into APOC solutions and projects from the very start. Furthermore, work and coordination on common and harmonised security architectures will improve industrialisation and deployment.

Efforts must therefore be made to protect APOCs

Key technical controls required for an APOC include intrusion prevention/detection, data diodes (to protect read-only data, such as relating to passengers), logging and audit capabilities, device and service authentication and data validation tools (which will also support general robustness for airports).

Trust will need to come from a range of sources

As well as technical measures, APOC partners will need to trust each other. Trust is enabled by security assurance, which comes from the actions of developers, implementers and assessors of security functionality, and in particular through structured design processes, documentation and testing. Assurance will come from global and European legislation/regulation, as well as from national and local level activity.

Information sharing and common cyber-situational awareness will be needed too

While it is premature to build an APOC-specific taxonomy for the exchange of cyber-incident data, given that the Network and Information Security (NIS) Directive is moving towards implementation, a framework for cooperation between each European state and Europe is necessary. The combination of organisational cyber-maturity assessments, together with more detailed metrics for the cyber-situational awareness of key APOC stakeholders – at the individual and team level – is one promising approach.

Fortunately, airports can and should, start their preparations now

Cyber-security capabilities take time to implement and mature. Airports can start now by assessing their cyber-security maturity and identifying areas for priority improvements. Cyber-exercises can be run to test the practical readiness of existing arrangements and learn lessons.

Contents

List of figures

List of tables

1 Introduction

1.1 General

This deliverable is the final report (D3) from a study that analysed cyber-security issues relating to the Airport Operations Centre (APOC) and Total Airport Management (TAM).

The APOC is the heart of the airport information network and is the central organisation unit responsible for airport operations. It is the 'nerve centre' of all decision-making processes between stakeholders, including airport management, airlines, air traffic control, MET, air traffic flow management and ground handlers. On the one hand, the development of these centres creates new vulnerabilities – through the integration of heterogeneous data sources. On the other hand, it creates important opportunities for improving mutual cyber-security. Because it creates a more complete picture of operations at the airport, it is essential that both the input and output data are reliable and resistant to manipulation, and that different partners are aware of, and can mitigate, cyber-threats together. Enhanced cyber-situational awareness in anticipation of cyber-attacks, and effective collaborative decision making during and following a cyber-attack, is key, especially since attacks - including some successful - are inevitable and consequently cyber-resilience is critical.

The study was undertaken by Aéroports de Paris (Groupe ADP), Prof Chris Johnson of the University of Glasgow and Helios, for EUROCONTROL under contract number 16-220098-C.

1.2 Objectives and scope of the study

This study contributes to the OFA05.01.01 final OSED and act as preparatory material for SESAR 2020. The study's objectives are to:

1) identify potential weaknesses in SESAR APOC / TAM;
2) investigate accreditation and assurance for building trust;
3) investigate and assess information sharing and threat mechanisms;
4) investigate common cyber-situational awareness and collaborative decision making.

The focus of the study is the SESAR APOC concept – i.e. the APOC of the future, rather than today's preliminary APOCs. However, the study is informed by the practical considerations of the concept at Groupe ADP, thereby providing a real-life insight into how the concept will develop.

1.3 Approach

The approach taken to meeting the study's objectives is outlined in Table 1 below:

Objective	Approach
Potential weaknesses in the SESAR APOC / TAM	We used scenarios to capture possible cyber-security threats and ways of mitigating them. We produced a visual 'map' of systems to establish the context. These included Business Impact Analysis on assets (systems and data). We also consider the integration of novel systems into a legacy architecture.
Accreditation and assurance as a way to build trust	We identified current and future EU and national legal considerations relating to both aviation and critical infrastructure. We then reviewed existing accreditation and assurance building measures across a range of sectors and industries to identify the best practices which could be applicable to APOC. Finally, we established appropriate principles and requirements for APOC by determining their applicability to Groupe ADP and the stakeholders it partners with.
Information sharing	We analysed the information resources existing within the APOC concept using use cases. This enabled us to determine the best ways of sharing information regarding security concerns and alerting relevant stakeholders to long term as well as short term security threats. This led to dissemination and escalation strategy for information sharing, as well as guidance on the appropriate format to support Cooperative Decision Making (CDM) given different priorities of APOC. We also included example applications of information sharing mechanisms.
Common cyber-situational awareness	Drawing on our experience in improving cyber-situational awareness we determined the best and most feasible methods of sharing cyber-security information with multiple stakeholders across national boundaries. We achieved this by developing appropriate KPI performance measures for means of displaying information such as Cyber-Security dashboards. This includes qualitative and quantitative techniques for assessing cyber-situational awareness.

Table 1: Approach to completing the study.

The study was completed between June and October 2016.

1.4 SESAR and cyber-security context

The Single European Sky (SES) initiative consists of a number of policy instruments including the Performance Scheme, Functional Airspace Blocks, Network Manager, extension of EASA and SESAR. SESAR is the technological arm of the SES, delivering new operational concepts, procedures and systems to support the SES objectives. The SESAR contribution to the High Level Goals, through Performance Ambitions, is defined in the European ATM Master Plan, which acts as the blueprint for the future European ATM system.

Cyber-security is about the prevention of and/or reaction to deliberate malicious acts undertaken via cyber-space to either compromise the system directly or wherever systems plays a key role in the prevention or response to threats to other parts of the business. While there is no standard definition of cyber-space it refers to the domain of information flow and communication between computer systems and networks and includes physical as well as purely virtual elements. Airport and ATM cyber-security is aimed at limiting the effects of such cyber-threats and the impact on airport organisation and operations and the overall ATM network.

As the SESAR Programme will deliver new procedures and systems that provide a much tighter integration of stakeholders within the European ATM system, there is a need to

address security concerns during the development and deployment of SESAR. Indeed, with SESAR, and the US equivalent, NextGen, the future looks very different to current specialised and isolated ATM systems. Early cyber-work in SESAR investigated the challenges ahead, illustrated by SWIM, and produced a cyber-security target framework and roadmap for SESAR (SESAR, 2015b). Of particular relevance are:

- The increasing interconnectivity of ATM means that the impact of an attack may extend across a growing number of interconnected systems.
- Increased reliance on integrated data means a high potential for operational disruptions if connectivity is lost.
- The migration toward common and Commercial-Off-The-Shelf (COTS) components, underpinned by industry standard protocols such as Internet Protocol (IP), with published vulnerabilities means that more people will have the technical background to launch attacks and more people will have access to core infrastructures through extended supply chains.
- Constraints on system and stakeholder complexity, including accommodating different levels of trust, plus specific constraints, such as safety timeframes on software patching, presents many challenges.
- Integration increasingly results in extended supply chains where each stakeholder relies on services provided by their partners but which might be delivered by third party companies.
- New methods of attack stemming from either criminal activities and/or state sponsored actors, of increasing levels of sophistication.

It is important to implement appropriate cyber-security measures. In particular, cyber-security must be incorporated in the design from the earliest stages in order to avoid the escalating costs when it only becomes considered as an afterthought. It must also support legacy applications given the longevity of many existing ATM components. There are increasing areas of concern – especially the integration of cyber-physical systems – where physical control systems are accessible through various forms of corporate networks. Using best practices from other sectors where applicable, and progressively building cyber-security capabilities, is key.

Of course, an APOC sits within an airport and both general and specific cyber-security guidance is available. General guidance on Security Management Systems and controls includes the ISO 27001 series, the NIST series of publications, and European standard EN 16495. Specific airport guidance is available from ACRP and the ENISA Securing Smart Airports work, and is supported by tools such as ACI World's IT Airport Cybersecurity Benchmarking tool. The study's standalone summary gives more detail on sources of guidance.

To-date SESAR has not addressed cyber-issues for TAM and APOC; that is the purpose of this study. SESAR APOC and TAM depend on the information that they are supplied with. Any changes affecting raw data, processed data or even how this data is sent to those systems will adversely affect APOC and TAM effectiveness. Cyber-security needs to be a primary consideration when designing and implementing SESAR APOC and TAM systems. Risks caused by potential vulnerabilities and their impact on SESAR developments need to be thoroughly investigated so that the necessary mitigation measures can be identified and put in place. The need for this study is therefore clear: without addressing cyber-security, the success of TAM and APOC are at risk.

1.5 Document structure

Table 2 below briefly describes the remaining sections in this document:

Section or Annex	Short description of content
2	Context for the study and the importance of the APOC and TAM
3	APOC cyber-security weaknesses and potential cyber-attack scenarios. In addition, contains a brief description of possible utopian and dystopian futures and how these might affect the cyber-security threats present.
4	Trust between APOC partners: why it's necessary and how it might be achieved
5	Information sharing mechanisms which could be established to share trusted information between APOC partners
6	Methods of establishing common cyber-situational awareness between APOC partners
7	Conclusions and recommendations
A	Abbreviations
B	References

Table 2: Document structure

2 APOC context

This section first introduces the SESAR APOC and related concepts in more detail, before analysing them to better understand their criticality within a future airport.

2.1 APOC, A-DCB and TAM: at the heart of airport performance

The SESAR European programme for the modernisation of ATM has promoted the concept of 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. This helps optimise flow management of airport demand against existing and future capacity. This 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 as a whole. 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 TAM scope additionally 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 MET aspects. Collaborative Decision-Making (CDM) 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 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. The APOC 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.

In order to achieve these aims it is important that stakeholders trust the information and services that they can access through the APOC. We return to this issue in Section 4 since security is a prerequisite for the maintenance of trust.

2.2 APOC Criticality

APOCs provide at least one physical centre that gathers representatives of all the key airport stakeholders, informed by advanced support tools and communication means. The APOC enables these representatives to exchange information in an effective way in order to manage airport performance. The APOC is a potential target for cyber-attackers and before looking at the weaknesses and potential cyber-attacks on the APOC, it must first be established how important this ‘nerve centre’ is and what the impact of compromise actually is.

It is already clear that airport disruption is expensive, both in terms of immediate loss of revenues and wider economic impact, and so the costs of a successful cyber-attack could easily run into millions of Euros if operations are paralyzed. Two approaches are taken to examine criticality: first using the SESAR risk assessment framework, and then Business Impact Analysis. It should be noted that for both, the SESAR APOC concept is the focus, not the earlier forms of APOC seen today.

2.2.1 SESAR Security Risk Assessment Methodology

An initial consideration of the SESAR Security Risk Assessment Methodology (SecRAM) impact levels[2] indicates that:

- **Worst case loss of integrity and/or availability** (i.e. with aggravating factors such as already snow-disrupted operations or very busy periods) would have a 'catastrophic' impact on capacity (loss of 60-100% of capacity) for the period of disruption, with a similarly 'catastrophic' branding impact (government and international attention) if at a major European airport. Performance and economic impacts are likely to be 'critical' (major quality abuse that makes major system - i.e. APOC - inoperable, and a serious loss of income, respectively).
- **Worse case loss of confidentially** is less severe, but with two main factors. Firstly, the AODB contains near-term aeronautical billing data, which is commercially sensitive (airlines loading factors, etc.). Compromise would be embarrassing (especially with airlines), but without major financial impact. Secondly, there may be passenger and staff personal data in the AODB, though passenger data is likely to be not detailed (only names, accessibility needs, etc.) and staff data may be based on roles (rather than individual names). However, even from names there would be some privacy impact if compromised; it should be noted that financial penalties are increasing with the EU's new General Data Protection Regulation (e.g. up to 5% of turnover for a breach) and also that the problem of extortion attacks is growing.
- **No safety impact is necessarily foreseen** from a worst-case compromise of confidentially, integrity and/or availability. The APOC is essentially a performance management system. The airport's control tower, not the airport operational system,

[2] Note that this is not a full-blown risk assessment - but preliminary work that should be developed further in SESAR 2020, as recommended later.

manages Navaids, lighting, etc. that are clearly safety critical. Of course the APOC may be on an attack path (i.e. on the route from entry point to target system), but an attack on APOC cannot directly affect safety critical systems. The only conceivable way this would change is with a move to integrated facilities management (with IP networked Programmable Logic Controllers (PLC) and Industrial Control Systems (ICS)) would change this (as the cyber-attack scenario in sub-section 3.4.5 shows).

The conclusion from this is clear – damaging cyber-attacks on an implementation of a SESAR APOC concept are most likely to come from manipulating data or from partial or full denial of service. Business Impact Analysis, in the next sub-section, assesses impact from a more finely-grained, asset-based perspective.

2.2.2 Business Impact Analysis

Business Impact Analysis (BIA) is a method that determines and evaluates the potential effects of an interruption, or a malfunction due to the wrong data, to critical business operations. The interruption can be the result of a disaster, accident or emergency.

BIA is an essential component of an organisation's business continuity plan. The analysis helps to compile a document that highlights critical assets that need to be secured in a business continuity plan.

The assets considered here are derived from the ENISA Smart Airports Functions and Assets document (Anon., 2016), however, the BIA is this study's, led by Groupe ADP and so is rooted in reality. The following categories are used:

- An asset is vital if its disruption cannot last more than 2 hours because too many flights would be immediately delayed and then cancelled,
- An asset is critical if its disruption cannot last more than 24 hours because too many flights would be delayed,
- Otherwise, an asset is useful or not applicable (N/A).

The following table assesses the business criticality of both airport and APOC assets.

Function	Asset	Criticality to the Airport	Criticality to the APOC
Airline/Airside Operations	Air Traffic Control and Management (ATM), Navigational Aids and Approach	Vital	Useful
	Meteorological Information Systems	Critical	Useful
	Airport Operation Plan (AOP)	Vital	Vital
	Network Operation Plan (NOP)	Critical	Critical
	Departure Control Systems (DCS)	Critical	N/A
	De-icing Systems	Critical	Critical
	Airfield Lighting Control Systems	Vital	N/A
	Runway Monitoring System	Vital	N/A
	Communication, Navigation and Surveillance (CNS)	Vital	N/A
Landside Operations	A-SMGCS	Vital	Critical
Safety and	Access Control Systems	Vital	N/A

Function	Asset	Criticality to the Airport	Criticality to the APOC
Security	Authentication Systems	Vital	Critical
	Badging Systems	Vital	N/A
	Baggage Screening Systems	Vital	N/A
	Smart Surveillance Systems e.g. Smart CCTV, Camera and Video	Vital	Critical
	Customs and Immigration	Vital	Critical
	In-line Explosive Detection Systems (IEDs)	Vital	N/A
	Passenger Screening Systems	Vital	N/A
	Perimeter Intrusion Detection Systems (PIDS)	Vital	N/A
	Emergency Response System	Vital	N/A
IT and Comms	Local Area Network Systems (LAN)	Vital	Vital
	Communications Systems (e.g.) Radio Spectrum Management Systems	Vital	N/A
	IT Equipment Hardware and Software	Critical	Critical
	Global Positioning System	Critical	Critical
	Network Security Management	Critical	N/A
	Wide Area Network (WAN)	Critical	Critical
	SITA Enabled Common Communications Network	Critical	Critical
Staff Management	Staff Authentication System e.g. Biometric Identification System	Critical	N/A
Passenger Management	Flight Information Display System (FIDS)	Critical	N/A
	Baggage Handling Systems	Critical	N/A
	Passenger Check-in and Boarding	Critical	N/A
Facilities and Maintenance	Energy Management	Critical	N/A

Table 3: Criticality of airport and APOC assets

2.2.3 Most critical APOC assets

As the preceding analysis shows, assets vital or critical to the whole airport do not necessarily carry the same importance for an APOC.

The following table sorts APOC assets by criticality in order to help understand which assets are important for the APOC. Other assessments are possible depending on the infrastructure at particular airports:

Functions	Assets	Criticality to the APOC
Airline/Airside Operations	Airport Operation Plan (AOP)	Vital
IT and Comms	Local Area Network Systems (LAN)	Vital
Airline/Airside Operations	De-icing Systems	Critical
	Network Operation Plan (NOP)	Critical
IT and Comms	Global Positioning System	Critical
	IT Equipment Hardware and Software	Critical
	SITA Enabled Common Communications Network	Critical
	Wide Area Network (WAN)	Critical
Landside Operations	A-SMGCS	Critical
Safety and Security	Authentication Systems	Critical
	Customs and Immigration	Critical
	Smart Surveillance Systems e.g. Smart CCTV, Camera and Video	Critical

Table 4: Criticality of potential APOC assets

Table 4 shows that the APOC is comprised of vital and critical assets for airport business continuity, so that any loss of integrity or availability would soon have a detrimental impact on airport operations.

2.3 Cost of airport disruption

The two hour threshold used above to identify vital APOC assets is based on potential costs to the airport in terms of losing APOC functionality due to cyber-attacks. This amount of time has also been chosen because it is a plausible duration for an incident to be identified and rectified.

The potential cost of airport disruption resulting from cyber-attack is difficult to estimate. There is no known actual data. Economic data relating to non-cyber disruption/losses is relevant, but will never be directly comparable. For example, data from the Eyjafjallajökull volcanic eruption in 2010 (€250m in lost European airport revenue alone for a six-day closure based on ACI figures) are not directly comparable because airports and all stakeholders had to stop their activities. After 9/11 Ronald Reagan Washington Airport remained closed for an extensive amount of time even though other airports were re-opened and the total daily impact of its closure on the economy was estimated to be in excess of 350 million US dollars a day (Chang, et al., 2003) – noting that this is the cost to the economy, not just airport, and that full airport closure due to a cyber-attack on an APOC is unlikely.

Though difficult, prior work on such economics such as (Langhe, et al., 2013) provides some guidance on how costs of airport disruption/closure might be calculated:

- If delays or cancellations are present, the airport will lose revenue stemming from passenger charges on cancelled flights or other passenger components of landing fees.
- Revenue stemming from non-aviation sources like retail stores or parking fees will be lost as well. One rule of thumb is that each passenger is worth €1 per minute in the departures lounge; noting of course that if flights are delayed then some types of expenditure will actually increase.
- The closure might negatively affect the image of the airport and lead to further long-term losses, and missed opportunities, which again are hard to quantify.
- Beyond the airport itself, closure will negatively affect a diverse set of stakeholders:
  - Airlines, due to passenger reimbursement, cancellations and accommodation costs. In addition, airlines might incur costs of rescheduling aircraft and staff as well as lose cargo clients due to delays.
  - Cargo businesses and mail services, due to the time sensitive nature of the cargo, costs of storage and mail rerouting.
  - Passengers, due to the cancellations or delays and especially if travelling on business. Passengers might also be affected by increased transportation costs if they choose to complete their journey via alternative means.
  - Service providers, as closure will also affect multiple parties such as airport shop operators, transportation companies and companies working with airlines.
- Some airports have military significance, and therefore contribute to national security.
- Most broadly, airport closure will affect the wider economy, such as the tourism sector, if passengers cancel their travel arrangements or are diverted elsewhere.

Crucially, the costs of airport closure for airport stakeholders might be carried over to the airport as airlines have to give compensation to passengers when their flights are significantly delayed or cancelled (EC, 2004). This quickly mounts up so that the airport holds significant liability in the event of successful cyber-attack.

Following successful a cyber-attack there are direct costs for clean-up, re-certification and implementation of new security controls. Liability, and wider economic costs, are likely to outweigh these – but they may be significant in areas where the airport already has a low profit margin.

Total economic losses due to airport closures remain very difficult to quantify. However, even if a loss of revenue is hard to evaluate - and data will hopefully will sparse since such a situation occurs rarely - we can assume there is potentially very significant costs in a dystopian future and that consequences will be more severe than today.

2.4 Beyond an individual APOC: the Network level impact

Compromise of an individual APOC (or specific functions therein) will not only negatively affect operations at a particular airport but will have repercussions network-wide. This comes not only from knock-on flight delays, but very conceivably through the network management. If the Airport Operations Plan (AOP) is not available to update the Network Operations Plan (NOP) then the data for network management becomes out-of-date.

A worse scenario, is where false information could be fed into the NOP, and this information subsequently feeds incorrect and misleading data and instructions to other airports. This possibility is explored in cyber-attack scenarios in the next section. In short, the loss of integrity at a single APOC could ‘pollute’ the network with much broader consequences.

3 Potential weaknesses and future trends

3.1 Introduction

This section identifies potential vulnerabilities of the Airport Operations Centre (APOC) and of the airport that owns it. Even though APOC implementations might differ between airports, as they will be optimised to the local conditions and operational philosophy, they will share the same objectives. The following pages begin by looking at future attack trends and identifying types of potential cyber-attacker. We then use a scenario-approach to illustrate how an attacker could manage to get inside an airport system and how they may prepare and conduct their attack.

3.2 Future attack trends

The aviation industry relies now on multiple data sources that were not available 10 years ago: Airports have become regulated with a departure sequence that introduced the concept of Targets (TOBT, TSAT, ASAT, etc.). New systems have been designed and implemented to improve the passengers' experience (Automatic luggage drop, self-boarding, quicker passport authentication using body's biometric properties, etc.). Weather forecasts are more scrutinised than ever, while security issues have grown since September 2001 with an increasing number of systems checking luggage and their owners.

While it is very difficult or even impossible, to forecast what the aviation industry will be in the future, we can contrast dystopian and a utopian scenarios and try to predict the types of cyber-security threats that will be present.

3.2.1 Airports utopian and dystopian shared futures

Today many existing systems are isolated (i.e. still air gapped, like SCADA[3] systems). In order to optimise future airport performance, this data must be integrated into real-time dashboards. Air-gapped systems will not exist in an interconnected future.

Systems within airports, and systems across airports will be interconnected. For instance, Passenger Name Record (PNR) system and Network Operation Plan (NOP) will be connected to the Airport Operation Plan (AOP).

We can also predict that airports will rely more on their IT systems than today. The trend for increased interconnectivity using standard commercial technologies is well exemplified by ACI's Aviation Community Recommended Information Services (ACRIS) specifications for standardised web services, including those for A-CDM. The end-goal is to facilitate integration and data exchange between companies working within the aviation domain, and also end consumers.

It is also likely that in the future airports might get greater fines in case of successful cyber-attacks, especially if passengers' data is compromised or if stakeholders press charges against the airport operator.

[3] Supervisory Control And Data Acquisition (SCADA) systems are a type of Industrial Control System (ICS). SCADA devices are used for remote monitoring and control of industrial processes. SCADA devices often refer to centralized systems which monitor and control individual sites, or complexes of systems spread out over large areas. SCADA devices control many basic processes, examples include the transmission of electricity, air conditioning and water distribution.

3.2.2 Airports' dystopian future

Dystopia: An imagined place or state in which everything is unpleasant or bad.

In a dystopian future, cyber-security is not taken into account. An increasing number of services are interconnected without appropriate security. The attack surface expands and it becomes easier to have significant business impacts through cyber-attack.

In this future, attackers are increasingly skilled, funded and are more numerous. Increasing fragmentation of Europe and aggressive police forces of foreign countries heighten the probability that state-backed attackers will target European airports and the ATM network.

In the worst case scenario, an airport and its APOC could be frequently disturbed or even disrupted since the airport will rely entirely on its systems.

3.2.3 Airports' utopian future

Utopia: An imagined place or state of things in which everything is perfect.

In a utopian future, cyber-security is taken seriously by APOC stakeholders; who work together for mutual protection. The benefits of integration are realised. Harnessing many sources of data means that data is cross-checked and validated and there is high confidence in the data.

Since more and more services are interconnected, security systems are fully deployed, such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), segregation/zoning and access control. A security architecture would offer depth and resilience. Since some AOP data sources can be read-only, then data diodes[4] can be used. Audit and penetration tests are performed regularly.

In an airport's utopian view, the threats still exist but do not come from other states, which means that the likelihood of a successful attack is lower compared to the dystopian future.

Finally, even if an attack succeeds, the response will be swift: Diagnosis and repair will be fast enabling efficient recovery. In order to avoid attack propagation, all stakeholders connected to the same network will be made aware of the threat.

3.3 Potential cyber-attackers

Potential cyber-attackers can be summarised as follows:

- Insiders (employees, contractors, etc.) who have legitimate access to the APOC, either by accidental or deliberate misuse (e.g. when threatened by terrorists)
- Hacktivists, who have a cause to fight for (such as political or ideological motives)
- Hackers or virus writers, who find interfering with computer systems an enjoyable challenge
- Business competitors and foreign intelligence services, interested in gaining an economic advantage for their companies or countries
- Cyber-criminals, who are interested in making money through fraud or from the sale of valuable information
- Terrorists, who are interested in obtaining and using sensitive information to launch a conventional attack

[4] A data diode is a network device that allows data to travel only in one direction.

- Organised crime, who are interested in obtaining financial reward or ransom in exchange for not provoking cancellations or flight disruptions
- State Cyber-Forces, who have large amount of resources at their disposal, state backing and are very highly skilled

In most attacks, without specific, detailed insider knowledge, the APOC and TAM would not be directly targeted. Instead, it seems likely that attacks would be launched against the airport as a whole from Hacktivists that are not organised enough to sustain long engineering and deployment steps before they start attacking.

To directly disturb APOC operations requires significant domain knowledge, funds and skills: It could be done by groups motivated by money (e.g. organised crime) or by states intending to disrupt national critical infrastructure (i.e. State Cyber-Forces).

3.4 APOC cyber-attack scenarios and APOC weakness

Potential APOC vulnerabilities – and more generally airport vulnerabilities – are illustrated using five different attack scenarios. They have been specifically selected because they can undermine the coordinated decision-making that is the main objective of APOC operation. « The APOC […] is seen as the principle support to the airport decision-making process » (cf. OFA 05.01.01). For example, although an attack on the baggage system is without doubt a serious incident it is not included in our analysis because it does not affect APOC decision making-processes. Of course, the APOC is not just a vulnerability in itself - the APOC could help resolve such an incident by helping all relevant stakeholders focus on recovery.

3.4.1 Scenario 1: Distributed Denial of Service attack on the Airport's internet connection

Description

A group of attackers wants to blackmail large companies into paying a ransom by threatening them with a volumetric distributed denial of service attack (DDoS). The attackers have identified that an airport operating company could be a great target since it relies on its Internet connection and controls significant financial resources.

In order to prepare the offensive, the attackers need to identify the IP addresses owned by the airport authority. These are not difficult to determine: they can be found by checking the main website's DNS entries or by finding the IP address(es) used by web-services on mobile applications.

In order to conduct an efficient DDoS attack, the attackers need to find several emitting sources with which to conduct the attack. Their first choice could be to acquire a network of infected machines that would be managed by them, such as a Botnet. It is possible to hire such services. Alternatively, they could gather people who share a common objective for instance, to disturb the air industry by using a website like PasteBin to coordinate their attack.

If the airport does not meet the blackmail demands, the attack will be launched and will overload the airport's Internet connection.

Why this scenario?

More and more companies are being targeted by DDoS attacks. In the past, these were mainly conducted to disrupt an Internet site and were used by Hacktivists. More recently such attacks have become a way for cybercriminals to obtain income, especially since it is possible to buy time on large quantities of infected computers (botnets) that will send data to the target. This provides a degree of indirection that makes it hard to trace the identity of the attackers. Airports hold an added attraction for some attackers – the impact of a DDoS attack would not just be focussed on digital resources but might also impact the physical operation of core services.

Although this scenario focuses on blackmail, a similar attack method might be used by hacktivists. For instance, if they oppose airport operations/expansion.

Impact on the APOC

Once it is accepted that the airport's Internet connection might be compromised, consequences need to be studied:

Based on the SESAR 2020 APOC concept we can assume that stakeholder representatives will not only have AOP access but will also be connected to their own systems, run at their headquarters, and accessed via a VPN network over the airport's internet connection. They could also use Voice Over IP (VoIP) technology to call their HQ or other partners. Since the Internet connection will be cut, or severely compromised, the stakeholder representatives could still make decisions but these will be hard to communicate within their organisation or across the airport. The APOC will stand but will be isolated from airport operations.

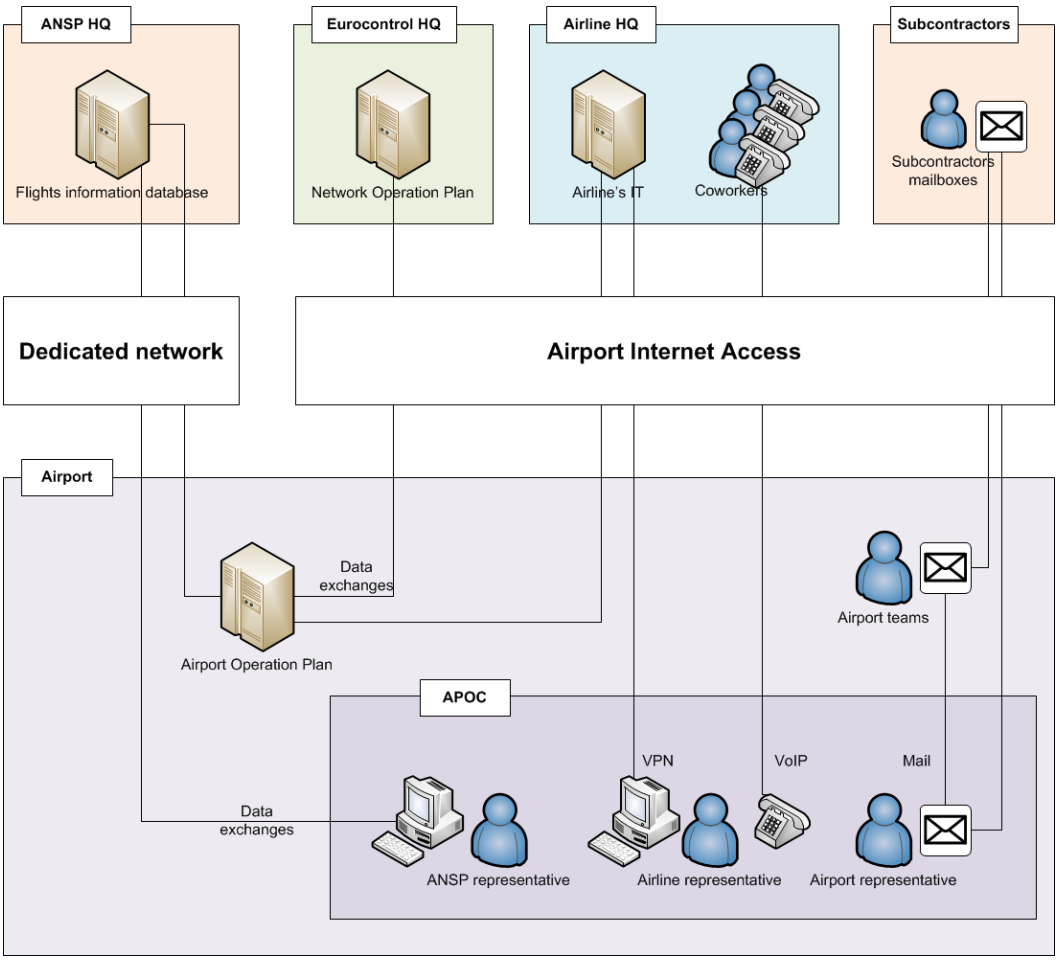


Figure 1: Connectivity diagram

Data such as weather forecasts are critical to airports and are delivered through the Internet. If a DDoS attack succeeds, the airport will not have up-to-date forecasts, which could be very critical in case of low visibility or snowy conditions.

Finally, dedicated networks could also be disturbed by the attack as they may share some physical hardware resources that will be busy and become unavailable.

Impacts on the Airport

The Internet connection may be used by the airport to exchange data between partners. If it breaks, the AOP won't be updated by these partners. Later sections will discuss further vulnerabilities with these alternative communications channels.

Impacts on the Network

If the Internet connection breaks, the NOP won't be updated. Therefore the Network would rely on outdated data from the targeted airport that are needed by other European airports.

Weaknesses

Categorised according to the ISO27005:2008 Annex D, the identified vulnerabilities in this scenario are:

Types	Vulnerabilities
Network	Single point of failure
Network	Inadequate network management (resilience of routing)

Table 5: DDoS attack vulnerabilities

Mitigation

One way to protect against DDoS attacks is through volumetric protection from the Internet Service Provider (ISP). Most ISPs have the ability to automatically detect potential DDoS attacks and to filter/throttle back requests from possible sources. The ISP is then able to identify and mitigate abnormal traffic to only deliver 'normal' requests to the final IP address.

IP address ranges can be whitelisted or blacklisted. However, the incoming traffic will only be blocked after having been received, which means that a large part of the incoming bandwidth (that merges normal and abnormal traffic) will be discarded. This method is also inefficient if the attackers choose IP ranges close to those of customers, partners, etc. since any throttling might also affect the connection of legitimate customers. This could happen if computers of legitimate customers are hijacked and used to conduct a DDoS volumetric attack.

A last method of defence would consist of having a secondary Internet connection and another IP range that will only be used in a case of emergency to secure airport operations.

3.4.2 Scenario 2: Deep and Slow infiltration to steal data

Description

A group of highly motivated and skilled cybercriminals wants to infiltrate an airport network in order to steal data. The final part of their attack is to clean their tracks by destroying some of the airports IT systems.

The scenario begins with spear phishing attacks targeting key decision makers in the APOC. Their computers are comprised via an attachment or URL to a compromised website that hosts the malware's payload. Once launched, the malware will try credential escalation and pivoting to gain control over host computers.

The infected machines will then map the network and post the results on a Twitter account that acts like a Command & Control server.

To avoid detection, data exchanges between infected equipment will be layer-encrypted in a way that some equipment will act like a proxy without being able to decipher the information.

Once the Active Directory is infected, attackers will gain full access to the APOC systems. Mass data can be exfiltrated to be analysed or sold, including operational data relating to flights and intelligence on the airport stakeholders.

Finally, the attackers will cover their tracks by destroying the workstations and servers operating the APOC's systems.

Why this scenario?

This scenario is an extension of an attack carried out on TV5Monde (one of the top three most available global television networks available around the world) in 2015 within the context of an APOC. In this incident a group of hackers managed to take down the TV station with an attack that ran for several months and used a large array of cyber-attack skills.

Impact on the Airport

Data that will be extracted may be related to flights and thus contain critical information for instance about delays, flight load factors and passenger personal information. These can lead to large penalties if passengers or airlines press charges, and a loss of confidence. The General Data Protection Regulation (GDPR) (EU, 2016) extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for severe penalties of up to 5% of worldwide turnover.

The airport website could also be defaced to promote an ideology or to publicise compromising information.

Once the hackers attain their goals and access the information they require they can remotely launch secondary attacks to damage the IT infrastructure, which will result in long-term disruption to the AOP that will disrupt the airport for a long time as the AOP is a mandatory asset. Without it, a major European airport will only be able to continue operating for a few hours before all ground movement will have to cease. This would, of

course, result in loss of confidence and major revenue loss for the airport operator and airlines.

Impact on the APOC

Since the AOP is a mandatory asset for the APOC, it means that its disruption is sufficient to disrupt the APOC as well. Further, leaked data could be used against APOC stakeholders, and hence help conduct further attacks on the aviation industry.

Impact on the Network

Once the AOP is down, the NOP will not be updated. It means that the Network will rely on outdated data from the targeted airport to update other European airports.

Weaknesses

The TV5Monde attack has been studied by the ANSSI (French National Authority for IT Security), which identified weaknesses that were used to conduct this attack.

Categorised according to the ISO27005:2008 Annex D, the identified vulnerabilities in this scenario are:

Types	Vulnerabilities
Hardware	Lack of periodic replacement schemes
Software	Well-known flaws in the software
Software	Poor password management
Network	Unprotected communication lines
Personnel	Insufficient security training
Personnel	Lack of security awareness
Organization	Lack of formal process for access right review (supervision)
Organization	Lack of fault reports recorded in administrator and operator logs
Organization	Lack of records in administrator and operator logs

Table 6: Infiltration attack vulnerabilities

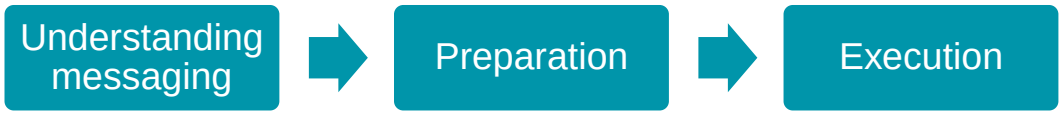
Mitigation

Very significant resources are needed to shield against such an attack: the economic case vs. the security case might have to be considered. In an airport context this means first identifying the critical IT assets that have to be secured and then evaluating the associated costs. If the loss of confidence and revenue is higher than the cost of mitigation, the resources have to be allocated. However, this is an imprecise judgement given the difficulty of anticipating the eventual costs of any future attack.

- Potential prevention and mitigation measures include:
- Zoning of connections and one-way information transfer,
- Educating to make staff are aware of cyber-security issues,
- Traffic profiling and understanding what traffic is expected on the network,
- Using white-lists and identification as well as scanning of networks,
- Establishing relations with cyber-security authorities that would send Indicators of compromise (IoC) to be searched for on the network.

3.4.3 Scenario 3: Major integrity loss

Description



A highly motivated group wants to disrupt operations at the airport and, if possible, operations at any other European airports. In order to do this, they send incorrect flight information to the targeted airport using a major messaging service deployed around the world used by airlines, airports, handlers and other businesses related to aviation. It is, therefore, relatively easy for an attacker to gain physical or digital access to a connection by compromising one of these legitimate businesses.

The next step is to send the wrong information to the right target. The targets address could easily be found on a proprietary search engine by searching for the targets name and the name of the messaging service.

Flight information sent to an airport are formatted following the IATA message specifications. Attackers have to know how to write the false messages they intend to send: This could be easily done since all relevant information is illegally stored on several public servers around the globe. These documents explain the Aircraft Movement Message (MVT) specification, which is enough to disturb an airport.

Finally, a list of incoming and outgoing flights needs to be created so that the attacker can alter critical information on genuine arrivals/departures. The necessary information can be obtained either from the airports own web site or other freely available sites such as FlightRadar24. The attackers now have everything in place: They can now write a script which sends information related to flights in a correct IATA syntax.

Once the attack begins, the AOP will receive incoherent updates but will not be able to blacklist the sender because it is not mandatory to put a sender address in a message. Using another stakeholder address is also possible.

Why this scenario?

Although not an attack, a similar scenario happened when a software company based in the United States of America sent a major European airport false information on real flights. They also used the wrong address in the signature field of the messages. It led the airport to be more careful with handling messages from the messaging community. This scenario can happen again and affect a larger selection of flights as part of a coordinated cyber-attack.

A single compromised source is enough to carry out a major attack for several hours. Each connection within the network independent of the type of organisation (airline, handler, airport, ANSP, etc.) could be targeted or be the origin of the attack.

Impact on the Airport

The messages transmitted from the hackers will introduce false data into the AOP. This will result in the following effects:

- Flights will be delayed since plane parking spot schedules will be disturbed by messages stating that the planes need to stay longer. These delays will also disturb the departing flights sequence.

- Meanwhile, real data will be sent by the stakeholders IT systems and become interspersed by incorrect data sent by the attackers. This could lead to a situation where the AOP is significantly slowed down by the amount of information that need to be processed.

Impact on the APOC

The numerous updates invoked by the attackers on the AOP will trigger alerts in the APOC. At worst, it will be impossible to distinguish legitimate alerts from false ones.

Each stakeholder will ask its IT to send the correct data which will generate more messages to be processed by the AOP, making it slower.

Impact on the Network

Flight data from the AOP will be sent to the NOP, which will send these to other AOPs, spreading false information across Europe.

It is also possible that the NOP becomes too busy updating data from the targeted airport.

Weaknesses

Categorised according to the ISO27005:2008 Annex D, the identified vulnerabilities in this scenario are:

Types	Vulnerabilities
Network	Single point of failure
Network	Lack of identification and authentication of sender and receiver
Personnel	Lack of monitoring mechanisms

Table 7: Integrity loss vulnerabilities

Mitigation

One way of mitigating such an attack would be to confirm all messages with an operational impact via secondary means. However, such duplication would be potentially very expensive, and need to be carefully implemented with sufficient separation so that if the endpoint is compromised then both primary and secondary means are not compromised.

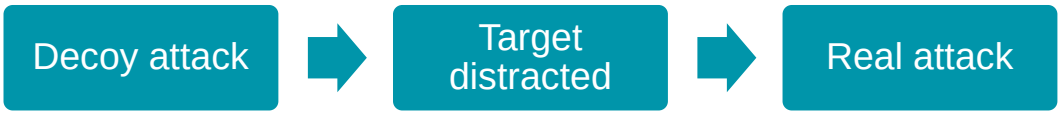
XML messages could also be used instead of plain-text: Since the XML structure contains several fields, one of which could contain a certificate confirming that a message was emitted from an allowed source. If the endpoint is known to have been digitally compromised, it can be blacklisted since its identity is known through XML structure. It might still take some time, however until someone identifies the source. If using plain-text, the messaging service operator will have to be contacted to identify the sender and block the messages. This could take several hours.

The use of an APOC itself might help identify inconsistencies quicker, since stakeholder representatives know which information is correct.

In case of major integrity loss, a temporary mitigation would be to cut the messaging service connection. This means, however, that the AOP will not be updated by legitimate messages.

3.4.4 Scenario 4: Blended attack

Description



A group of hackers wants to disturb an airport but without being noticed too rapidly.

They could achieve this by modifying flight information using the method described in Scenario 3 however this type of attack is too obvious. Instead, to reach their goals they use a blended attack that consists of several attacks with one being obvious, intended to divert attention, and a main attack intended to be conducted in such a way as to remain undetected.

An initial DDoS attack, similar to the one presented in Scenario 1 but less intense, will be launched in order to disturb operations at the APOC, but not disrupt them. Meanwhile, flight messages will be sent which will be targeting a limited number of flights with minor changes designed to be small enough to remain undetected.

IT and engineering staff inside the APOC will then be distracted by trying to rectify the effects of the first attack and their attention will be diverted from the main attack: Since the first attack is a light one, it gives the illusion that the situation is under control and that the APOC is still safe whereas the real threat is obscured by the first attack.

Why this scenario?

This scenario demonstrates several previous scenarios used together as a blended attack. This kind of attack has already happened, for example, it resembles elements of the attack on the Ukrainian power system in 2015. It should be addressed in this cyber-security study because such hybrid techniques may become more prominent in the future.

The threat of blended attacks also exemplifies why APOC stakeholders should be aware of cyber-security issues, and especially the possibility of diversionary attacks. This will enable them to react in an appropriate way when such situations occur.

Especially in the case of a blended attacks it is important to understand that the illusion of safety is a real threat. APOC stakeholders might let their guard down if they think APOC integrity is still 'safe', when in fact it may well be insecure.

Impact on the Airport

Minor changes, like small delays, will be sent regarding flights a few minutes before they arrive or before they leave. For instance, if a flight has to arrive earlier than expected, people in charge of handling it will have to be available earlier. If the information is incorrect, they have to wait until the plane arrives whereas they could have been handling another flight elsewhere. If an arriving flight is handled too late, it is possible that the plane's next departure will be delayed since the fuelling, cleaning or luggage handling will not be finished on time.

Impact on the APOC

The stakeholders will have difficulties understanding that a major attack is being masked by a smaller one and will not necessarily focus on the delays that are created: The

decision making process will be focused on the first and obvious attack instead of the second.

Impact on the Network

Since delays on outgoing flights will take place, those will impact other European airports that consider these flights as incoming ones.

Weaknesses

Categorised according to the ISO27005:2008 Annex D, the identified vulnerabilities in this scenario are:

Types	Vulnerabilities
Network	Single point of failure
Network	Lack of identification and authentication of sender and receiver
Network	Inadequate network management (resilience of routing)
Personnel	Lack of security awareness
Personnel	Lack of monitoring mechanisms

Table 8: Blended attack vulnerabilities

Mitigation

People inside the APOC should be aware that one attack might mask another more serious threat. It is also important to understand that attacks may also coincide with routine equipment failures or upgrades. Any time engineering staff are preoccupied with other tasks, can provide the attackers with opportunities to hide their work.

An alert could be triggered every time more than [x] flights are delayed during a duration of time [t]

3.4.5 Scenario 5: Low Level Attack on APOC ICS/SCADA infrastructure

Description

Programmable Logic Controllers (PLCs) are simple devices that can be used to control physical processes. There are hundreds of thousands of them at every airport, but they are often 'invisible' because they are conventional, stand-alone components controlling everything from power distribution through air-conditioning and baggage handling. They run bespoke firmware and do not use conventional operating systems. There is typically no logging or forensic capability for these devices in European airports nor do they have any intrusion detection facility. They have however been the targets of recent attacks (Stuxnet, Ukrainian power plant). APOCs increase the integration of these devices through IP interfaces that enable stakeholders to monitor their behaviour.

In the past, PLCs were 'air gapped' and the only way malware might have been inserted would have been through very infrequent firmware updates via field devices. However, existing Supervisory Control And Data Acquisition (SCADA) components are very vulnerable – for instance some PLC's have firmware updates distributed from web servers whose URL is in plain text on the installation packages – hence they can be spoofed.

Alternatively, there is pressure from suppliers to use IP bridges so that operators can maintain and interact with PLCs and the associated sensor/actuators over conventional APOC networks. This creates new possibilities for coordinated attacks.

Stuxnet included a state machine, when it attacked the Iranian SCADA infrastructures it concealed its behavior by altering the effects of the malware over time – first doing nothing for 20 days, then setting the speed of devices slightly fast, hiding again and then setting the speed too slow. This prevents diagnosis, especially when airports have no Industrial Control Systems (ICS) forensic capability. In the air gapped case, there is no need to synchronize the state machine stages but this could be done over APOC cyber-physical networks.

Why this Scenario?

APOCs are at the forefront of cyber-physical integration. The data exchanged between stakeholders enables the optimized deployment of physical resources, however APOC, and Total Airport Management to a much greater extent, depend upon the provision of accurate data through sensors (heating, power, water, aircon, security cameras) and on the delivery of automated services through actuators (physical protection, doors, voltage relays etc.). These devices are very different from conventional office-based systems and they have been exposed to a growing number of attacks (Ukraine, Stuxnet).

This scenario reminds us that not every system runs Linux or uses IP – but they can be attacked with significant effects on APOC / Total Airport Management. The likelihood of such a scenario might be relatively low now but the intelligence communities across member states have stressed the need to be aware of this threat in the next 3-5 years.

Impact on the APOC

SCADA components are widely distributed across all airport infrastructures. It would be sufficient for the attacker to focus on one or two subsystems to impact on the APOC

stakeholders. The attackers might reprogram upper permissible voltage levels so that the APOC networks are continually starved of power. The attacks would undermine confidence in the supply chain.

Impact on the Airport

It would be hard to have a direct impact on safety but very easy to have an impact on the quality of service to end users. Indeed, the attackers might alter the temperature settings on building management systems using the APOC networks as the distribution and coordination vector. Field engineers seldom consider the possibility of malware; mutual situational awareness would be undermined as engineers struggle to resolve the source of the problem.

There are some scenarios where these effects might be exacerbated – by leaking information about the attack to the media or through a focus on specific components which do have safety related functions (PLCs and SCADA components are part of runway lighting systems, security screening applications etc.).

Impact on the Network

Only if delays are present at the targeted airport.

Weaknesses

Categorised according to the ISO 27005:2008 Annex D, the identified vulnerabilities in this scenario are:

Types	Vulnerabilities
Hardware	Lack of efficient configuration change control
Software	Lack of audit trail
Software	Uncontrolled downloading and use of software
Network	Transfer of passwords in clear

Table 9: Low Level Attack vulnerabilities

Mitigation

A range of techniques can be used to verify the authenticity of firmware – some manufacturers offer stronger certification and digital signing of their updates hence steps can be taken during procurement to select those devices that offer the greatest level of version control. It is important to consider the integrity of the supply chain given that many airport operators will outsource the handling of these devices which are embedded within the power distribution and air conditioning systems that are the lifeblood of their operations.

However, airports rely on thousands of legacy PLCs and SCADA components, a risk assessment can be used to identify both safety and business critical components and greater steps taken to ensure their integrity. These measures may include attempts to protect the air gap – through physical barriers to prevent field devices from being attached to SCADA components – with only a small number of trusted devices/updates permitted. Similarly, companies can introduce local hashing techniques to ensure that firmware versions conform to the canonical copies that are supplied direct from the device manufacturer.

Given the technical sophistication of recent attacks on SCADA components, it is also important to consider the use of forensic techniques that might be able to detect and isolate any potential problem. The logs that are usually protected for high-level information systems are typically not provided for these lowly level devices. Hence, in the medium term steps can be taken to ensure that sufficient information is available to help a CERT or other response team to assist the recovery of an APOC after an attack.

3.5 Attackers' targets

The table below indicates which entities are likely to conduct attacks described in the five scenarios:

Entities	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Insiders			✓		✓
Hacktivists, Cyber-criminals and Terrorists	✓				
Hackers					✓
States and Organised crime	✓	✓	✓	✓	✓

Table 10: Entities likely to conduct the attacks described in the scenarios

3.6 Vulnerabilities list

The following table gives an overview of the vulnerabilities identified for each of the attack scenarios described above.

Types	Vulnerabilities	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Hardware	Lack of periodic replacement schemes		✓			
Hardware	Lack of efficient configuration change control					✓
Software	Well-known flaws in the software		✓			
Software	Lack of audit trail					✓
Software	Poor password management		✓			
Software	Uncontrolled downloading and use of software					✓
Network	Unprotected communication lines		✓			
Network	Single point of failure	✓		✓	✓	
Network	Lack of identification and authentication of sender and receiver			✓	✓	
Network	Transfer of passwords in clear					✓
Network	Inadequate network management (resilience of routing)	✓			✓	
Personnel	Insufficient security training		✓			
Personnel	Lack of security awareness		✓		✓	

Types	Vulnerabilities	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Personnel	Lack of monitoring mechanisms			✓	✓	
Organization	Lack of formal procedure for user registration and de-registration		✓			
Organization	Lack of formal process for access right review (supervision)		✓			
Organization	Lack of fault reports recorded in administrator and operator logs		✓			
Organization	Lack of records in administrator and operator logs		✓			

Table 11: Overview of the vulnerabilities identified for each of the attack scenarios

3.7 Summary

Several types of attacks could at the very least disturb operations at the APOC. In the most extreme scenarios airport operations could be disrupted completely. Vulnerabilities have been identified for each of the attack scenarios. These should be fed into a business impact analysis to build a set of prioritised actions to protect the APOC. A dystopian future, where cyber-security is unaddressed, is contrasted with a utopian future.

4 Trust between APOC partners

4.1 Introduction

This section first explains why trust between APOC partners will be critical to the effective and efficient use of the APOC. It identifies the means to build, and maintain trust, by reviewing how this need is fulfilled in similar situations elsewhere. The APOC context is then described, before a set of principles and requirements for APOC trust are articulated. These partly come from legal and regulatory requirements, which are identified, but will very likely be augmented through negotiation with national authorities. Some promising mechanisms for achieving this trust are then discussed, with a particular focus on APOC supply chain management.

The literature for securing and trusting multi-party processes and systems is rich, and this study draws on key references, most notably:

- **ISO/IEC 15443 Security assurance framework** - which defines terms and organises concepts for understanding IT security assurance. Its objective is to present a variety of assurance methods and to guide selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given system satisfies its stated assurance requirements.
- **EUROCAE ED-201 Aeronautical Information System Security Framework Guidance** - which is a recent standard. At its core is the concept of a standardised External Agreement which covers the cyber-risks around an external interface and/or use of third-party products, in order to manage the shared risks which are created by a shared resource, such as an APOC. It addresses airworthiness issues, and is therefore designed to provide high-levels of assurance.
- **EN 16495 Information security for organisations supporting civil aviation** - which is a European Standard defining guidelines and general principles, structured in line with ISO 27002 (ISO/IEC, 2013b), for the implementation of an information security management system. It highlights that service delivery in aviation is greatly defined by the cooperation of the individual participants - directly relating to an APOC - and this needs sharing the results of risk assessments along the business process chain, agreement on the required level of trust, and agreement on the required security controls and their implementation. To this end, a series of trust levels are defined, with the intent that that aviation organisations working in partnership agree that these levels of trust, backed by reasonable evidence, be recognised in further shared business processes.

The key concepts and ideas used in this section are:

- Trust defined by EN 16495 (CEN, 2014) as a situation where one party is willing to rely on the actions of another party.
- Assurance, which has various relevant definitions (see later), but the preferred one used here is from ED-201 which is 'the planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements'.

4.2 The need for trust

The APOC will be the 'nerve centre' for decision-making. The Airport Operator therefore needs to be willing to rely on actions of itself, and its partners and suppliers, including that:

- Critical data supplied by itself and others is accurate and timely
- Connections to external systems/processes do not introduce security weaknesses into its own systems/processes (and partners/suppliers need to trust in the Airport Operator in this too)
- APOC function behaves as intended to deliver its intended benefits

Given its role in decision-making, the APOC is a trusted function, in that its stakeholders trust it to perform critical operations, but the key question in this section is **how do we know that the APOC is trustworthy?** If the APOC is being trusted to handle, process and present critical data, but does not deserve this trust (i.e. is untrustworthy) then there is a major problem. In asking 'how do we know that the APOC is trustworthy?', the 'we' includes the Airport Operator, partners and suppliers, customers, the regulator and other third parties such as the Network Manager (as the NOC relies on APOCs) - i.e. a wide range of stakeholders, with varying interests, but all relying on the APOC and/or needing confidence in its operation. It should also be stressed that if any individual stakeholder within an APOC cannot be trusted then the impact will undermine the trust of EVERY stakeholder – including ultimately the travelling public.

4.3 Where trust comes from

NIST SP800-39, a federal standard on cyber-security risk management, identifies two factors affecting the trustworthiness of information systems:

- **Security functionality** (i.e., the security features/functions employed within the system), which needs a combination of management, operational and technical security controls; protective controls are discussed in the previous section, and the information sharing and cyber-situational awareness is described in the next sections.
- **Security assurance** (i.e., the grounds for confidence that the security functionality is effective in its application); this is the critical enabler for trust in this section.

EN 16495 also identifies assurance, in the context secure external connection and data exchange, when saying that the "organisation must assess the trust it can place in the connection and in the data being received, and assure itself that the trust assessment is validated". (Security) assurance therefore enables trust - and the challenge is to deliver sufficient assurance for APOC such that it is trusted.

We offered a definition of assurance earlier that centres on confidence. Other definitions adopt a similar approach:

- The grounds for justified confidence that a claim has been or will be achieved (ISO, 2015).
- A measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy (NIST, 2011).
- An attribute of an information system that provides grounds for having confidence that the system operates such that the system security policy is enforced (EUROCAE, 2015).

- Confidence [of a user (or accreditor)] that the system works as intended, without flaws or surprises, even in the presence of malice (Snow, 2005)

So the question is now: where does assurance come from and how much is needed for APOC purposes? Again prior work points the way for sources of assurance:

- Assurance comes from "actions taken by developers and implementers with regard to the design, development, implementation, and operation of the security functionality" (NIST, 2011)
- Assurance also comes from "actions taken by assessors to determine the extent to which the functionality is implemented correctly, operating as intended, and producing the desired respect to meeting the security requirements for information systems and their environments of operation" (NIST, 2011)
- Assurance comes through structured design processes, documentation and testing (Snow, 2005)
- Assurance obtained for a system/process is usually a blend or composition of different assurance methods applied at various stages through-out the system's life cycle (EUROCAE, 2015)

Cyber-security assurance can seem abstract. Physical security is visible and auditable in a way that cyber is not, and with cyber-security it is difficult to run standardised tests, such as those used to audit passenger screening. This results in reliance on wider range of assurance methods.

ISO 15443 (ISO/IEC, 2012) is a security assurance framework for information systems, and identifies three types of assessment to gain assurance: namely assessment of **systems, processes and environments**:

- Assessment of a **system** involves an examination of the system itself (or product, service or other deliverable). These assurance methods examine the system and its associated security design documentation independent of the development processes. Direct system assessments include the Common Criteria scheme for products[5] and penetration testing of deployed systems. Indirect system assurance methods include supplier declarations and warranties.
- Assessment of a **process** involves an examination of the organisational processes used in the production and operation of the system throughout its lifecycle (i.e., development, deployment, delivery, testing, maintenance, disposal). Assurance is gained through the inference that if a defined process is followed the deliverable will be developed and implemented to a certain quality. This should yield security assurance when applied to systems. Examples include quality management processes (e.g. ISO 9000 (ISO, 2015)) and secure systems engineering processes (e.g. ISO/IEC 21827 (ISO/IEC, 2008)).
- Assessment of the **environment** involves an examination of the environmental factors that contribute to the quality of the processes and the production of the systems (it does not examine a deliverable or process directly). These factors include personnel and physical facilities. Examples include vetting of staff and third-party review of facilities.

[5] Common Criteria (standardised by ISO/IEC 15408) is a certified product scheme in which vendors' products are evaluated against functional and assurance requirements by testing labs. It provides assurance of a rigorous and standard and repeatable manner fit for the target environment for use, and is often used in critical infrastructure.

Some assurance approaches combine multiple types of assessment. For example, security management through the ISO/IEC 27000 series looks at system, process and environment aspects. Typically, a 'security assurance case' is used to make the case for sufficient security and links the claim to supporting evidence. The 'security assurance case' is an overall package of security assurance related to the system, demonstrating how, and with what confidence, the security assurance requirements for a system have been met (ISO/IEC, 2012).

Whilst assurance methods attempt to minimise subjectivity over levels of confidence, by being rooted in the evidence produced by assessment processes, ISO 15443 (ISO/IEC, 2012) usefully highlights that the reputations of the operators, suppliers and assessors are significant in establishing confidence because their qualifications and experience may or may not be acceptable. By their differences in individual perception, stakeholders may have different degrees of confidence after the performance of a given assurance method. This hints at the difficulty of building trust across and between a large number of APOC stakeholders.

4.4 Real-world examples of assurance mechanisms

Building assurance in the real world can take various forms, for example a process of certifying that a supplier is capable of providing a secure and resilient service or system, or a process of accepting residual security risks associated with the deployment and operation of a system and granting approval to operate. In other industries, these measures are supported by regulatory audit to ensure compliance is not simply a paper or tick-box exercise.

Four examples of assurance methods applied in the real-world are described below:

- The Galileo Security Accreditation Board (SAB) leads security assurance for European GNSS systems and ensures suppliers have ISO 27002 (ISO/IEC, 2013b) controls (system/process/environment) and that systems are ‘certified’ against a set of common requirements (system). Technical recommendations to stakeholders appear unclear at times, perhaps due to sensitive vulnerability insight, however a central authority empowered to mandate requirements and oversee compliance provides a strong, common level of assurance.
- UK government accreditation is a process of accepting residual security risks associated with the deployment and operation of a system, before granting approval to operate. It is mandatory for government systems with a through-life method, ISO 27002-aligned controls, certified products, etc. (system/process/environment). It is thoroughly documented in a 'Risk Management and Accreditation Documentation Set (RMADS)' that is built up over time. Typically, there is a professional 'accreditor' scrutinising each step of the system lifecycle so that there is a somewhat adversarial approach. CESG, as the UK's national technical authority on cyber-security, can be involved where necessary. Ultimately the business owner can decide to accept residual risks, so that a preferred balance of business benefit and cyber-risk can be achieved.
- CBEST in the UK banking sector is an industry-specific framework of intelligence-led pen testing for core banking services (system). It is voluntary but encouraged by the regulator, and supported by CESG. It was launched in recognition that the banking sector was likely unable to provide assurance against more sophisticated attacks on critical assets. A security testing authority (CREST) approves and certifies commercial

organisations supplying cyber-threat intelligence, penetration testing, cyber-incident response and security architecture services.

- ANSSI Certification Center in France includes first level evaluations and EAL evaluations (system) in accordance with Common Criteria (ANSSI, 2002). Certificates issued by the ANSSI by delegation from the Prime minister certify that the certified products comply with a technical specification referred to as the security target. This is product and component-level rather than whole system or process assurance.

The common denominator here is third-party scrutiny by a competent authority. This suggests that the APOC should undergo the same process. The four approaches have been applied in different ways: e.g. component-level or system-level, and the degree of centralised authority (e.g. the Galileo SAB can be much more unilateral than the voluntary CBEST scheme). A CBEST-style scheme at the European Network-level, with appropriate involvement of national authorities, may be more politically acceptable. Some of these differences are explored in more detail in subsequent sections looking at architectures for cyber-information exchange across European APOCs.

4.5 Key APOC security features relating to trust and assurance

Fundamentally:

- As the 'airport nerve centre' APOCs directly impact airport (and network) performance (especially improved efficiency and return from non-nominal conditions) and so is a 'core' function. This means that the APOC is likely to require medium/high levels of trust and assurance to deliver its full set of benefits. This is explored in more detail later.
- The AOP, as realised by an AODB (much extended from today's AODBs[6]), is the single source of truth for near-term airport operations (i.e. today and tomorrow's operations[7]) and so cannot be allowed to go stale or lose its validity. It is a both a single source of truth, but by implication a potential single point of failure.
- As a set of integrated processes, with many connections/interfaces with external systems (including different types of systems: ICS, business systems, etc.) it involves multiple stakeholders, with a range of trust requirements (and very likely a range of trustworthiness). This implies assuring the APOC is non-trivial and without one-size-fits-all solutions.
- The concept of pivoting raises significant questions; this tactic involved the escalation of privileges during a cyber-attack. An initial breach might involve a less critical/less trusted component of the supply chain. Access rights and sensitive data obtained from this attack can then be used to mask further attacks on more trusted stakeholders – hence any assessment of the trust associated with different parties must also consider the risks from coordinated escalation of initial attacks.
- Furthermore, the APOC emphasises information sharing and coordination; this is at odds with cyber-security where the emphasis is on separation.

[6] The AOP handles airport operational management info (flight schedules, etc.), resource allocation (staff, stand allocations, etc.), aeronautical billing, baggage reconciliation and more.

[7] It is also long-term in order to manage airport slots for the next IATA season.

- Fall back to manual processes is increasingly difficult with increased automation, especially as 'skills fade' means that fall back to manual processes becomes less viable.
- Airport and APOCs' link to NOP/NMOC creates a pan-European dimension for cyber-security issues.

Also of note, on a more practical basis:

- Many airports are currently integrating existing systems, which tend to be from multiple suppliers and few airports have taken a whole “TAM” suite from a single supplier. This indicates that confidentially of information to be disclosed may be an issue.
- As TAM solutions mature, then airports could be expected to take a selection of products or services from a small number of preferred suppliers. This indicates that responsibilities for assurance could change as market matures (e.g. a single supplier may take greater responsibility for assurance as an intrinsic part of its offering, or a value-added service).
- TAM solutions and modules can be hosted locally or remotely, and can be shared across multiple airports. This implies that an overarching assurance model needs to accommodate centralised and distributed, and physical and virtual APOCs, and hybrids.
- Suppliers view TAM (and presumably APOC) in different ways, and it is not as structured as EUROCONTROL and SESAR's concept. This indicates that the flexibility of an assurance model is important.

4.5.1 Assurance levels required

Especially due to the potential impacts on capacity and reputation, strong security levels are needed and such strong security requirements call for a high degree of assurance. This will, however, be expensive, and to consider if security investment can be prioritised it is beneficial to consider if there are some services, systems or data that are more/less critical than others and can be separated for protection purposes. For example, can APOC be separated from CDM? If so, then APOC has marginal performance uplift only (i.e. its about optimising rather than step-change in performance) and so is less critical. However, CDM is perhaps more rightly seen as at the heart of APOC?

Understanding the required assurance levels allows for a security architecture to be designed that accommodates the levels. Different approaches, identified in prior SESAR work (SESAR, 2015c) include:

- **Least common denominator** – security level corresponds to lowest level appropriate across the different users, on top of which different users have to apply their own additional security measures (e.g. at the application layer) to fulfil their security requirements and policies.
- **System-high** – security level corresponds to the highest level needed across the different users, so that no additional security measure is required. The whole APOC supports this high level of security.
- **Optimised** – somewhere between ‘least common denominator’ and ‘system-high’, where the security level is optimised to meet a particular objective (e.g. cost minimisation). Network segregation and zoning are used. Some parties will need to

apply their own additional security measures, but these will be fewer in number than in the least common denominator.

- **Multi-level security** – there are multiple security levels, that are securely separated, so that each user has an appropriate level.

These approaches are illustrated below, in a simplified form with six operational services (A to F) each with a simplified security level and one or sets of control (coloured, rounded boxes).

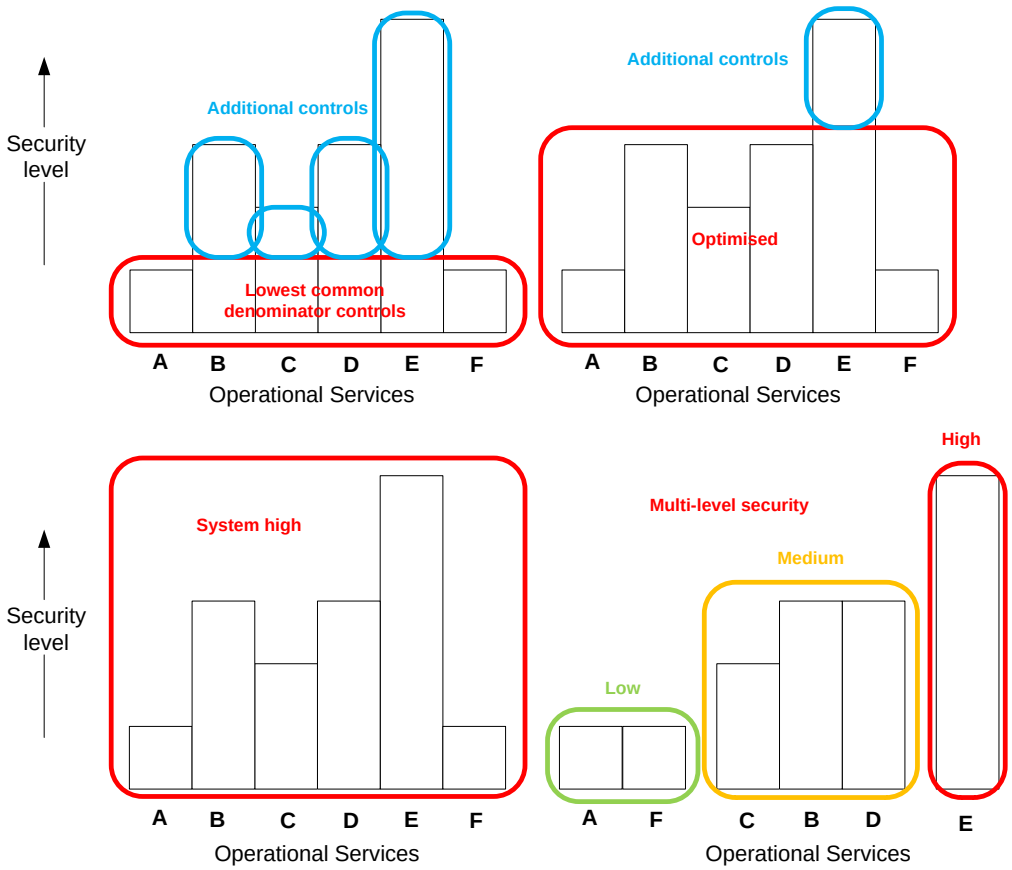


Figure 2: Different approaches to applying controls to different security levels

The actual mix of APOC services is key to determining the correct approach. For example, if all services have a similar level apart from one, then it would typically be best to design for the common level and ensure that the exception establishes additional controls. If the services vary in security level, then a multi-level security approach might be more appropriate, especially if the economic overhead of multiple levels can be minimised.

Taking the SESAR OFA 05.01.01 Consolidated OSED (SESAR, 2015a) as a reference, a rough logical architecture of services, systems and data can be identified.[8] Figure 3 shows this, in standard ArchiMate notation, with their relative expected security levels overlaid in colour.

[8] Note that further real-world considerations such as onward data warehousing is not considered in this logical architecture.

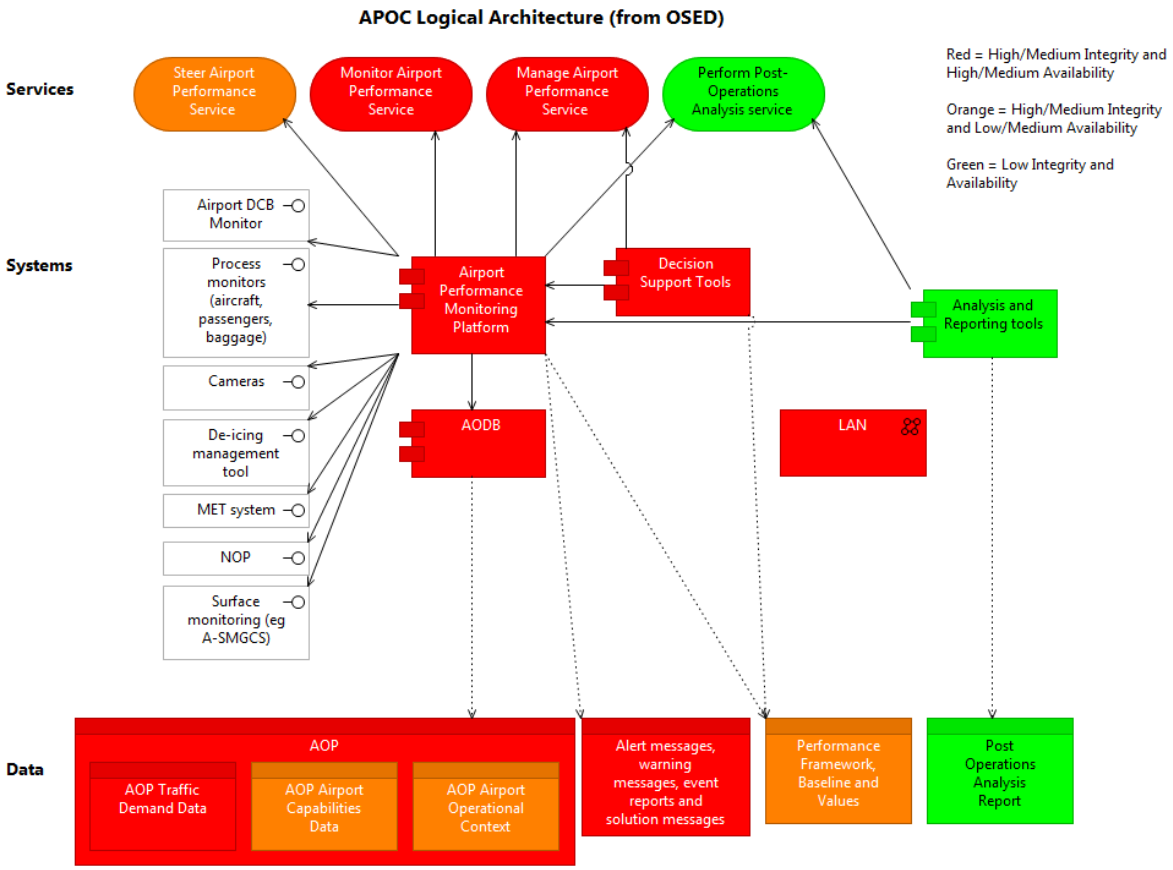


Figure 3: APOC Logical Architecture (from OSED)

The central conclusion is that the APOC is one logical and physical data repository, with lots of interfaces. So whilst, data and services can be split into different security levels, the system cannot be easily split. This indicates that a 'System High' approach is likely. This limits opportunities for segregation, zoning, etc. However, due to the high number of APOC interfaces, one important application of the separation principle is to look at which data feeds are 'read only' (as opposed to 'read and write') and to use data diodes to isolate and protect these feeds. This, and the general initial assessment in this sub-section, should be explored in further work on APOC security architectures.

4.6 Assurance principles and requirements for APOC

4.6.1 Assurance principles

Review of the literature identifies a core set of cyber-security assurance principles that are applicable to APOC:

1) Level of assurance depends on existing and required trustworthiness (i.e. proportionate to risk)
2) Assurance needs to fit the security environment (i.e. no one size fits all)
3) Assurance is a blend or composition of different assurance methods (and expert judgement is required to combine them)
4) Assurance provided is related to the effort expended, but since because it is intangible it is often hard to justify

5) Assurance is built progressively through a lifecycle approach

6) Component-level assurance builds to system-level assurance, but the integration of one or more systems into a final target environment generally has a negative impact on the resulting security assurance.

7) Assurance degrades with time, and with new systems and data, and so needs to be dynamic and needs effective cyber-situational awareness

8) Third party involvement can add credibility and expertise, and avoid insular thinking, and so strengthen assurance

9) Assurance is facilitated by auditable requirements

10) When risks are shared, assurance needs to be mutually understood and accepted

At a practical-level, the following inter-related characteristics help engender trust:

- **Technical competence**: An ability to identify vulnerabilities/weaknesses and mitigations, which implies the involvement of respected experts and authorities. For example, if assessed by a well-resourced national security agency, with both offensive and defensive capabilities, then more assurance can be taken than if assessed by an untrained, inexperienced airport systems engineer turned security manager.
- **Openness and transparency to external assessment and criticism**: This is indicated by a desire to (pro-actively) seek external judgement and letting others see for themselves. For example, inviting a third party, especially a national authority, to assess key systems indicates a greater level of maturity than solely using internal assurance methods.
- **Self-awareness**: A willingness to acknowledge weaknesses as well as strengths. For example, knowing that certain controls are still under development or are not as strong as they need to be would give more assurance than blindly believing that everything is fine and then having an obvious vulnerability exposed.
- **Honesty**: A willingness to reveal truths that need to be known. For example, voluntarily disclosing the weaknesses above or a willingness to report incidents pro-actively and fully.

4.6.2 Lifecycle approach

A lifecycle approach is important, as assurance should be progressively built-up over time as an initial concept and requirements (with much uncertainty over implementation) becomes a reality (with fewer unknowns). At each stage the understanding of cyber-risk is refined and additional measures can be established to control the risk and assurance methods used to build confidence. Conversely, as ISO 15443 (ISO/IEC, 2012) points out, human error, equipment failures, new vulnerabilities, and threats can occur in any lifecycle stage. The following diagram illustrates this lifecycle approach, along with example assurance methods that are appropriate for each stage. The evidence from each stage can be added to the Assurance Case. ISO/IEC 15026-2:2011 (ISO/IEC, 2011) specifies the minimum requirements for the structure and contents of an assurance case.

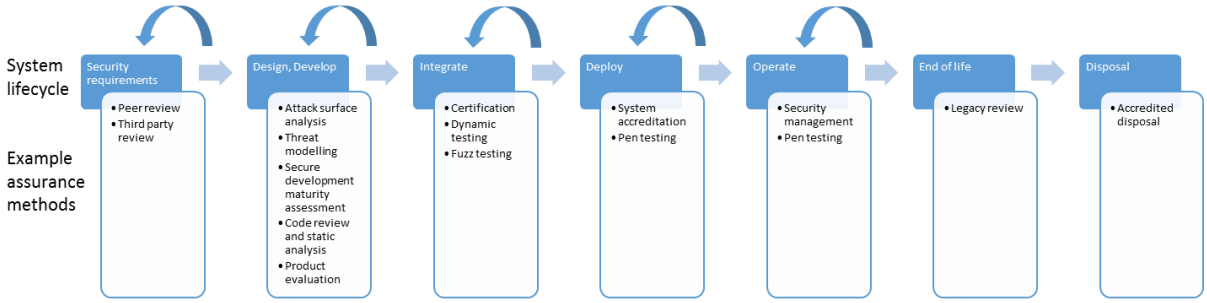


Figure 4: A lifecycle approach to building assurance

Particular examples are:

- **Static analysis**: Analysing binary software files using algorithms to measure the security hygiene of code, so-called 'static' because it looks at code without executing it. Examples of good security hygiene include whether the compiler used to convert the source code into binary inserted common protective features, and minimising the number of branches in a program (as more branches mean more complexity and more potential for error).
- **Fuzz testing**: Throwing a lot of data at a program to see if it does something it shouldn't do. The program is monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. If it behaves badly then it's an indicator of potential vulnerabilities. Again this is usually automated or semi-automated.
- **Pen testing**: Attempting to gain access to resources without knowledge of passwords and other normal means of access. The goal is to find holes in the security and understand them (e.g. what damage could be inflicted) in order to fix them. Typically a penetration tester will be given basic user-level access with the goal to elevate the status of the account or user other means to gain access to additional systems or data. Pen testing can be semi-automated, but relies on human expertise.
- **Security management system certification**: Certifying that an organisation meets the requirements set in a standard, for example ISO 27001 on Information System Management Systems. Certification provides written assurance (a certificate) by an independent Certification Body that a management system (a) conforms to the specified requirements, (b) is capable of consistently achieving its stated policy and objectives, and (c) is effectively implemented, and thereby provides value to the organisation, its customers and interested parties. It addresses management system processes as much as the systems themselves.

Given its high criticality, a high-level of assurance is needed in the APOC, and all of the assurance methods in the system lifecycle Figure 4 are applicable. One should expect these to be used progressively and systematically, with scrutiny as needed to satisfy stakeholders that the residual risks are tolerable. Assurance is then on-going, for example with an audit schedule, and reviewed on a regular basis, or whenever there is a major change (e.g. in systems, in airport operations, threat level, etc.).

Of course nothing, especially a complex APOC, will ever be as simple as a linear process or lifecycle, so assurance methods need to be used iteratively as well. ISO 15443 notes that functional deficiencies, changes in requirements, and new vulnerabilities will affect security assurance and would require earlier lifecycle stages to be entered again. It should

also be emphasised that maintenance, system enhancements and decommissioning are massively important, and end-of-life 'twilight' legacy components/systems are a real problem as they may not have been designed or developed securely originally or the means to manage vulnerabilities disappears with loss of technical support.

4.6.3 How SESAR will help with APOC assurance

The best time to influence APOC trustworthiness is early in its life cycle. It is critically important to consider security and assurance concerns carefully during the development and design phases since it is always costlier to 'bolt-on' security afterwards. SESAR plays a key role in identify security and assurance requirements. Of course, what SESAR does is not sufficient, as the lifecycle principle demonstrates.

In SESAR, the security validation and verification process defines the steps/activities to be performed into a general validation process in order to provide evidence that SESAR concept satisfies the SESAR high-level security objectives (as defined by P16.06.02 in SESAR 1). A SecRAM defines how to undertake a security risk assessment that will help identify the level(s) of assurance needed, associated security functionality requirements and assurance requirements. It will help prioritise investments and design an appropriate security architecture.

In SESAR 2020 there is likely to be increased emphasis on projects establishing clear plans to demonstrate assurance, including creating an initial security case (similar to a safety case) and generating initial evidence. SESAR Solution packs then contain the Security Cases demonstrating that the solution can be deployed in a secure and resilient manner. If done in this way, APOC Assurance Cases can include SESAR Security Cases as an early input.

4.6.4 Likely legal and regulatory context for APOC security assurance

Assurance requirements may be easy to identify. One extreme assurance is a legal or regulatory requirement, and the assurance methods may be tightly defined, while at the other extreme it may only be subject to negotiation through an external agreement. This sub-section examines current and future EU and national legal considerations relating to both airport and critical infrastructure to identify where there may be mandatory requirements on an APOC.

Airport security in the EU is regulated on national, EU and international level. The main actors for creating rules in this domain are ICAO, the European Commission, ECAC and national authorities. As a result of multiple actors being involved in the rule-making process, international, EU and national regulatory requirements often overlap.

- **International Civil Aviation Organization (ICAO)**: ICAO's Annex 17 to the Convention on International Civil Aviation, Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference, sets minimum standards for aviation security worldwide and creates a global policy and legal framework, which has been constantly updated since 1974, based on the current policy and threat landscape. These standards are the basis of national civil aviation security programmes and are binding for contracting States. ICAO Aviation Security Manual (ICAO, 2015) provides guidance, including on minimum measures are to protect critical information systems against unauthorised access and use.
- **European Civil Aviation Conference (ECAC)**: ECAC is an international organisation of States which was formed with the assistance of ICAO. Its work consists of agreeing

and issuing resolutions, recommendations, and policy statements. ECAC's role in aviation security is twofold. It not only sets standards in the form of policy recommendations, resolutions, etc., but also aims to ensure that security equipment used at European airports meets the minimum security requirements of the EU. ECAC sets out aviation security standards in its Aviation Security Handbook. However, the standards are only recommendations without a legally binding effect on contracting states. The basis for European security measures is the ECAC Document 30[9] ('Doc. 30') (ECAC, 2009) that builds upon ICAO Annex 17 (ICAO, 2014) but often defines higher standards. Even though ECAC Doc. 30 currently does not address cyber-security, appropriate amendments (overarching principles in Chapter 14, and prescriptive annexes, as well as supporting guidance material) are expected to be developed and included within the next couple of years. This will include assurance and testing requirements - for example, prescriptions on third party certification or equivalent self-certification. In addition, ECAC auditing is expected to move towards including cyber-vulnerability security assessments at national level.

- **European Commission (EC)**: On the European level, the EU framework for aviation security is the main framework that sets common standards for every aspect of airport security. The EU framework for aviation security aims to create a common understanding of ICAO's Annex 17 that provides for minimum standards to ensure the security of civil aviation and is based on recommendations of the ECAC Document 30. The initial framework, established after 9/11, has been replaced by Regulation (EC) No 300/2008[10] (EC, 2008). The detailed and general measures for the implementation of basic standards set out by the framework are binding and member states are obliged to comply with the minimum standards but they can also implement more stringent measures if necessary. In 2016, the Network and Information Security (NIS) Directive (EU, 2016) has been adopted and will shortly come into force. This is legislation aimed at establishing minimum standards for critical national infrastructure, and should be applicable to airports, but mainly addresses a risk managed approach, information sharing and incident reporting, without specific assurance requirements.
- **National level**: Under EU legislation, Member States are obligated to designate a single authority responsible for the coordination and the monitoring of the implementation of common basic standards for aviation security. States also have to set up national civil aviation security programmes and national quality control programmes. Additionally, operators must define and maintain airport security programmes, air carrier's security programmes. As mentioned previously, member states are obliged to implement the minimum standards defined by the EU (and ICAO); however, more stringent measures can also be applied if necessary - for example if the threat level warrants it. National security agencies are likely to be involved, and undertake assessments and provide intelligence-led recommendations. Under the new NIS Directive Member States are required to adopt national strategies that set out concrete policy and regulatory measures to maintain a level of cyber-security. This includes designating a national competent authority for information

[9] European Civil Aviation Conference (ECAC) Doc 30 or "ECAC policy statement in the field of civil aviation facilitation" contains requirements relating to security within the airport. As of the date of writing of this report (October 2016) these do not yet extensively cover cyber-security.

[10] Note that EC 272/2009 supplements 300/2008 with further common basic standards on civil aviation security, and EU 18/2010 amends 300/2008 with specifications for national quality control programmes. Finally EU 72/2010 details the procedures of conducting inspections at airports and applying aviation security standards to ensure the correct implementation of regulation 300/2008.

security and setting up a team responsible for handling incidents and risks. However it is too soon to say what effect the Directive will have when implemented at national levels.

In addition, EASA, through a new cyber-security centre, will have a role - but this is expected to essentially be a clearinghouse for confidential incident information, and so only of relevance for the next section.

This analysis indicates that there are currently extensive, often overlapping, regulations with a harmonised approach to compliance monitoring: common basic standards for methodology, a reporting system and a baseline for mutual acceptance of equipment. However, there are no harmonised certification programmes, which reveal a lack of common approach to security equipment approval, which hinders assurance-building efforts.

Based on this research, neither current, nor envisaged, legal and regulatory requirements tightly define assurance methods nor a level of assurance required for APOCs. Changes to ECAC Doc 30 should introduce a set of auditable requirements for airport cyber-security that would apply to APOCs (an audit scheme will be present as well). This will include some guidance on assurance, but will likely still place the onus on national authorities to consider whether the measures in place effectively satisfy identified risks. This will not tightly define assurance requirements.

It is clear that national sovereignty concerns limit mutual recognition of security requirements. One issue is that threat levels are always different, another are the disclosure laws in certain states', which might mean that if vulnerability/intelligence information is disclosed to a particular country, it might have to be disclosed publicly. Furthermore, some national cyber-security authorities may have already defined methodologies; for example, France has the ANSSI First Level Security Certification CSPN, and the UK use CESG Cyber-Risk Reviews of airports considered to be critical national infrastructure. In general, international comparability of cyber-security assurance is very hard, and has only been achieved (at a limited level) at a product-level. Mutual recognition is not the case today, nor can it realistically be expected.

A final consideration is that airports are focused on supporting transport – they are not specialist cyber-security agencies. They will therefore need external support to respond and cope with (hopefully) rare attacks. This could be done at a regional, national or European level by supporting an aviation specific CERT etc.

4.6.5 Voluntary mechanisms

If legal and regulatory requirements are unlikely to provide a harmonised assurance regime, then voluntary mechanisms based on standards are needed. From those currently available, the ED-201 approach is a good fit, and was recently tested at a UK Airport. It is specifically geared to aviation with a risk managed approach:

1) Address internal security, including processes for measuring assurance of SecMSthe Information Security Management System (ISMS)
2) Address external security, by identifying partners, risk assessing and sharing results, modifying practices, etc.
3) Agree that shared risks have been identified and addressed, including apportioning shared risk

Its concept is based on sharing comparable risk assessments, to support discussions around the security of interfaces and to promote common understanding of impacts, risks and the appropriateness of controls. The results of the risk management process are embodied in an External Agreement between organisations.

It should be stressed, however, that existing security standards tend to be poorly integrated with the safety requirements in ED-153 etc. They offer different definitions of risk; there are no common agreed criteria for software safety/security assurance levels.

ED-201 assumes that the organisations involved have formal security management systems and risk assessment methods, although these may not follow the same standard. Hence the first issue for organisations is to establish the comparability of their formal methods (e.g. against ISO 27005 framework). Once comparability has been established, organisations are better able to compare risks that may be shared by virtue of the interfaces with partner organisations.

4.7 Summary

Trust is enabled by security assurance, which comes from the actions of developers, implementers and assessors of security functionality, and in particular through structured design processes, documentation and testing.

A high level of security assurance is required for APOCs as they are business critical. Therefore, a comprehensive approach is needed – addressing processes, systems and the operating environment. Practical-level characteristics that engender trust are technical competence, openness and transparency to external assessment and criticism, self-awareness and honesty.

Current and envisaged legal and regulatory requirements do not tightly define security assurance methods nor does a level of assurance for APOCs. However, impending changes to ECAC Doc 30 should introduce a set of auditable requirements for cyber-security that should eventually provide a strong mandate for airports, including APOCs, to adequately address the majority of cyber-risks. Addressing nation state threats (i.e. very capable and persistent attackers) would require additional support from national authorities. The (NIS) Directive makes this more likely.

A key question is the extent to which pan-European harmonisation can occur. Specific assurance requirements will be subject to negotiation and agreement with regulators (and other national authorities), partners/suppliers, customers, etc., and therefore vary across APOCs – but harmonisation would be beneficial to encourage mutual trust and to facilitate efficiency. Common rules are needed, and whilst full harmonisation of security assurance across Europe is desirable, it is unlikely due to national sovereignty concerns and differences in threat levels. Instead, assurance requirements will be subject to negotiation and agreement with regulators (and other national authorities), partners/suppliers, customers, etc., and therefore vary across airports and APOCs.

Where legal and regulatory needs fall short of providing sufficient assurance, a voluntary, standards-based approach would be helpful. Looking a variety of comparable schemes and mechanisms shows that third-party scrutiny, from a competent authority, is common denominator. The CBEST scheme in the UK banking sector is a useful model. In either cases, consistent interpretation of regulations/standards absolutely key.

As a single logical platform and data repository, a 'system high' approach is more applicable than multiple-levels of assurance. A security architecture that offers depth and

resilience is crucial. Since some AOP data sources can be read-only, then data diodes can be used. However, segregation, zoning, etc. will be limited, as will opportunities to prioritise security investment in the APOC.

A multi-lateral External Agreement, as defined in EUROCAE Standard ED-201, is the most promising way of building and documenting trust with and across APOC partners. A key challenge will be to enable flexible accommodation of new requirements in an evolving environment (e.g. when new services are introduced and new threats emerge).

The concept of security assurance cases is also relevant here. A security assurance case is an overall package of security assurance demonstrating how, and with what confidence, the security assurance requirements for a system have been met. Such a case is needed to present to, and convince others, to get the trust required for APOC operations.

5 Information sharing and dashboards

5.1 Introduction

This section first sets out use cases for the sharing of information about cyber-incidents and 'leading practices' to mitigate the risks of future attacks. Subsequent sub-sections then present a number of desktop visualisations that might be used to support/implement these use cases.

The approach used extends existing practices, such as the reporting techniques already used by ENISA under the Telecoms Directive. This is appropriate because it is likely that the same use cases will be incorporated into Air Traffic Management as a result of the NIS Directive; where ENISA will guide the implementation likely based on their existing practices. Similarly, the information dashboards are derived from existing applications with a focus on low cost and open source applications. It should be noted that further work is required to trial a number of these systems with APOC stakeholders, especially where they require the further instrumentation of local area networks.

A key concept is the distinction between periodic (monthly/annual) and ad hoc information exchange. Periodic reports are useful because they provide a structured, statistical summary when there may be a large number of low impact threats. They may also provide a summary digest of lessons learnt. They help to ensure that Chief Information Security Officers (CISOs) are not overwhelmed by a mass of less relevant warnings. In contrast, ad hoc reporting takes place as soon as a high-impact incident is suspected and provides immediate warning to other potential victims. As we shall see, ad hoc and periodic reports may be exchanged within an APOC, between stakeholders that include airport operators, airlines, ANSPs, security companies, retail organisations, network and infrastructure companies, police agencies etc. At a higher level they may also be distributed through national regulatory organisations and onto European bodies including the Network Manager Operations Centre (NMOC).

The objectives for this section are to:

1) Enable timely and consistent CDM across APOC stakeholders.
2) Extend the information push concepts embedded within APOC to cyber-incidents BUT avoid information overload.
3) Provide designs for an information dashboard building on leading practice from other industries (e.g. nuclear cyber-security and military cyber-information sharing systems).
4) Integrate the above with existing H2020/FP7 projects on ATM cyber-incident reporting (especially GAMMA and ECOSSIAN).

The following pages analyse the information resources existing within the APOC concept using use cases. This is intended to determine the best ways of sharing information regarding security concerns and alerting relevant stakeholders to long term as well as short term security threats. This will lead to a dissemination and escalation strategy for information sharing, as well as guidance on appropriate format to support A-CDM given different priorities of APOC (compared to ATFCM, ATC, Ground Handling, Airport Ops and Airline OCC). We include example applications of information sharing mechanisms.

We are sensitive to the trade-offs in this area – imposing undue security constraints may reduce the benefits from increased information sharing. Any security measures must be

proportionate both to the nature of the threat and to the business requirements of our stakeholders.

5.2 More Detailed Approach

As mentioned, the following sections build on an approach to cyber-incident reporting that has been used for almost three years across member states by the European Network and Information Security Agency in support of the Telecoms directive (Johnson, 2015) and (Johnson, 2015). The intention is to integrate the use case approach already applied in the SESAR APOC role documents with similar techniques developed by ENISA – thereby ensuring high-level consistency.

A secondary aim is to integrate with existing European projects, in particular GAMMA and ECOSSIAN. The goal of both projects is to independently develop cyber-information sharing structures for en route ATM and wider aviation communities. We can build on the hierarchical concepts of Security Operations Centres (SOCs) developed within those projects with the notion of logical and virtual APOCs described in the SESAR outline documents. This will ensure that our use cases build on previous work but also reflect the particular challenges in an Airline Operations Centre.

The following stages were used to complete this work:

1) **Develop use case diagrams for information sharing between APOC stakeholders**: Our use cases consider the frequency of communication – to ensure prompt transfer of relevant details without overloading the recipient with irrelevant information. It is critical that a mass of low threat information does not overwhelm the patience and situational awareness of CISOs within an APOC. It is also important to consider the legal consequences of reporting; where disclosure potentially violates national security requirements or the IP concerns of particular participants. These issues can be addressed in a number of ways – including filtering through national or APOC specific points of contact and through appropriate levels of redaction. These were considered and supported within the case studies, presented below, again building on an APOC specific adaptation of the existing ENISA systems;

2) **Identify information requirements and formats**: The second stage identified key data to be exchanged between APOC stakeholders. This is non-trivial. In the immediate aftermath of an attack it is often only possible to identify the symptoms that were observed without countermeasures or the forensic analysis of underlying causes. These details must be added over time. There is far less agreement over security incident taxonomies than there are over the descriptions used in safety related incidents. We also consider the level of abstraction to be provided in cyber-incident reports – in many cases, vulnerabilities emerge from detailed interactions between software that is unique to a particular APOC stakeholder. Providing this level of detail has the potential to disclose vulnerabilities without supporting other member states. Alternatively, a higher level of abstraction focussing on intrusion detection measures or supply chain concerns can provide more general insights.

3) **Develop Initial Concepts for Information Dashboards Supporting CDM**: The final stage was to prototype desktop summaries based on the growing number of existing cyber-situational awareness tools. The focus here is not on developing an optimal solution – this is premature given the need for additional operational expertise in the deployment of these technologies. Instead, the intention is to provide initial proposals

that can be shown to other agencies and can trigger a more sustained dialogue around what is needed in the future SESAR work programme.

In preparation we consulted with ENISA's cyber-security for Smart Airports project team – taking part in teleconferences and supporting their work through structured interviews. We participated in periodic reviews of both the GAMMA and ECOSSIAN projects on European frameworks for aviation cyber-incident reporting. Our case studies were also validated by consultation with EASA at director level- ensuring that this work is broadly in line with their strategy.

5.2.1 Key Issues

The following key issues are at the heart of this section:

- How can we leverage the existing information resources within the APOC concept to automatically identify security concerns and alert appropriate stakeholders?
- How can we maximise the information presented to stakeholders in periodic reports to retain interest, to avoid information overload and to improve cyber-security maturity levels over time?
- How can we maximise the information presented to stakeholders in ad hoc reports to optimise our response (Johnson, 2014), contain and counter an incident, thereby speeding recovery and minimising disruption?

5.3 Relevant ATM cyber-incident reporting mechanisms / Threat and intelligence sharing requirements for APOC

The exchange of information about threats and mitigations against cyber-attacks falls within the scope of security management. Figure 5 shows how Security Management System (SecMS) for cyber-security and information security (ISMS) share many of the features of more traditional safety management systems. As can be seen, 'Monitoring and Incident Reporting' provides means of validating the risk and threat assessments that guide design and implementation.

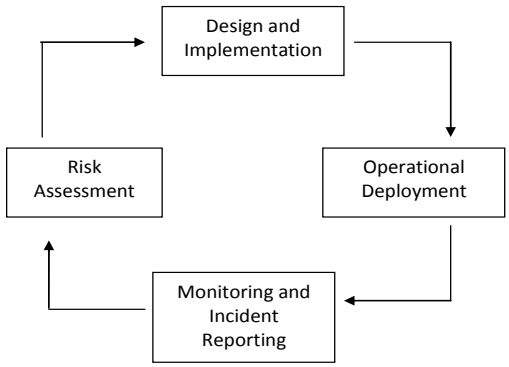


Figure 5: Conventional Safety Management Systems

ENISA extends Figure 6 to illustrate the core concepts within a cyber-security Management System – as can be seen incident reporting fills the same roles in both safety and security. Unfortunately, a number of differences complicate the implementation of sharing mechanisms across these different areas. In safety, it is widely accepted that information should be shared as widely as possible and in a timely fashion to prevent the recurrence of previous accidents. Things are more complicated within cyber-security. For example, the disclosure of information about an attack can motivate future attacks or help

an adversary refine their techniques – police agencies will also use knowledge of an incident as an indication of potential involvement in an incident. There are further concerns about reputational damage and about national sovereignty.

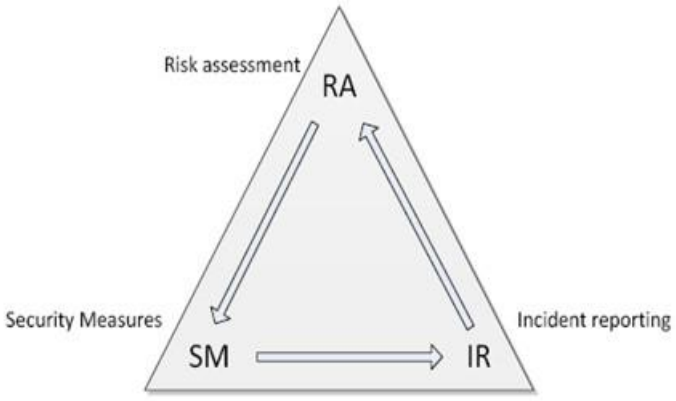


Figure 6: ENISA High-Level Architecture for Security Management Systems (SecMS)

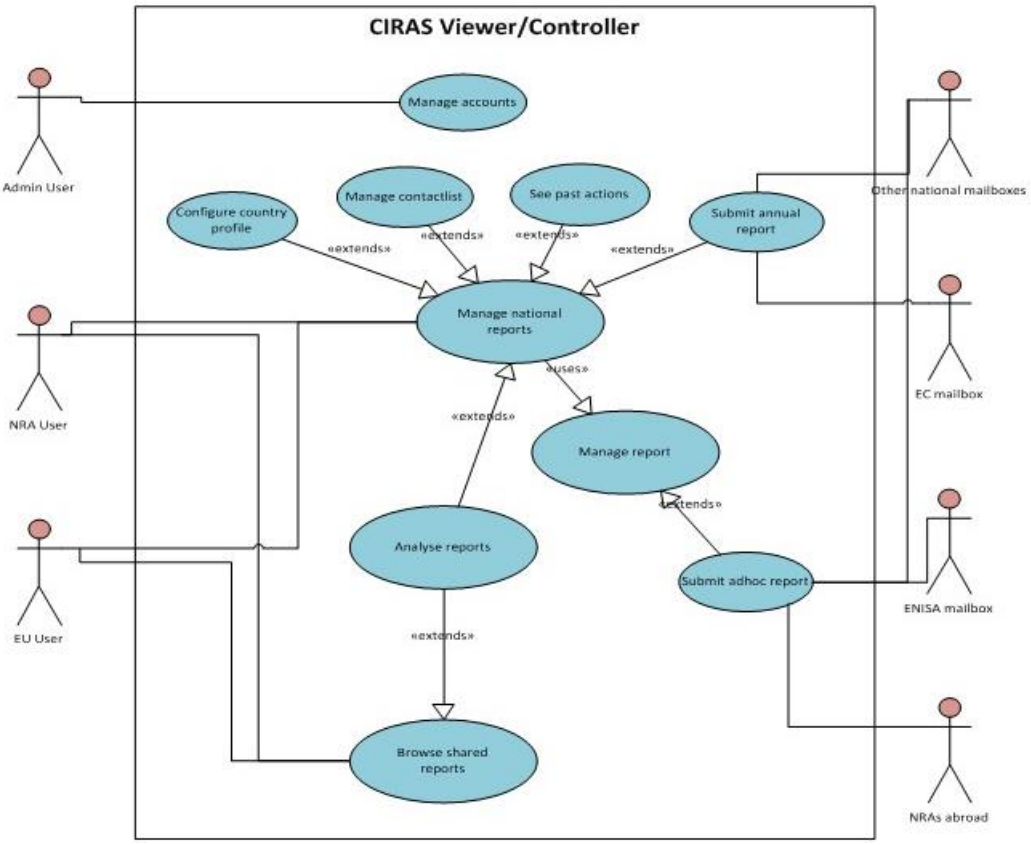
This leads to a number of key concerns in cyber-information sharing that are discussed in the following section:

1) **What information can be shared?** This is important because in previous European reporting systems, the intention has been to provide high-level statistical data across member states on the distribution of attacks and then to provide more immediate short-term warnings about high-risk threats. Provisions are in place to anonymise this information so that other users of the system will not be able to tell which country suffered the attack. This will be problematic for APOCs compared to existing reporting systems for ISPs – there are far fewer airport operators meaning that it will be easier to infer the subject of an attack once information is provided to other states. This is arguably less of concern for the exchange of good practices or pre-emptive threat intelligence, although this might conceivably compromise security sources.

2) **Who safeguards the system?** In existing European reporting systems, the regulator in each member state coordinates the provision of data and reports through a web interface to ENISA who then distribute the reports to other member states. This avoids the situation where ENISA might be seen to side-step national regulatory provisions. We would recommend a similar scheme across Europe's airports – given that in many member states there is a legal requirement on operators to report safety (and security) concerns to the national regulator before any European agencies. This creates a framework for cooperation between each state and Europe.

3) **What should be reported?** Under the existing reporting systems within the Telecoms directive, there is a taxonomy of information to be provided about specific incidents – including the number of users affected, whether a cyber-attack affected critical infrastructures etc. Again, any European system should build on this – however, it is premature to build an APOC specific taxonomy given that the Network and Information Security Directive is moving towards implementation. The Directive will enter into force in August 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services. This places a requirement on airport operators to report cyber-incidents; it is highly likely (certain) that ENISA will coordinate the information requirements for the implementation of this directive and any APOC specific taxonomy should be consistent with this.

F



Information Sharing 'Use Case' Diagram

4) To begin with, we can identify use cases/critical roles in the exchange of cyber-incident information. Figure 7 illustrates the CIRAS (Critical Incident Reporting and Analysis) approach that ENISA used to sketch the high level concept behind Europe's existing system for sharing cyber-security information across member states. In the context of this project, ENISA might be replaced by EASA or EUROCONTROL. The National Regulatory Agency (NRA) is ambiguous–existing European cyber-reporting systems depend upon Telecoms rather than aviation regulators; in the UK cyber-incidents go via Ofcom to ENISA and the Commission rather than the CAA. The implementation of the NIS Directive needs to resolve this – it is clearly important that the national receiving agency has aviation expertise within the context of APOCs, equally, the Telecom regulator may also be receiving warnings of similar attacks on infrastructures (VOIP, GPS, Linux etc.) that are common between aviation, maritime, rail etc. Figure 8 is used by the EC GAMMA project (see next section) to illustrate the interdependencies that make it critical to integrate APOC cyber-incident reporting with other industries covered in the Network and Information Security Directive.

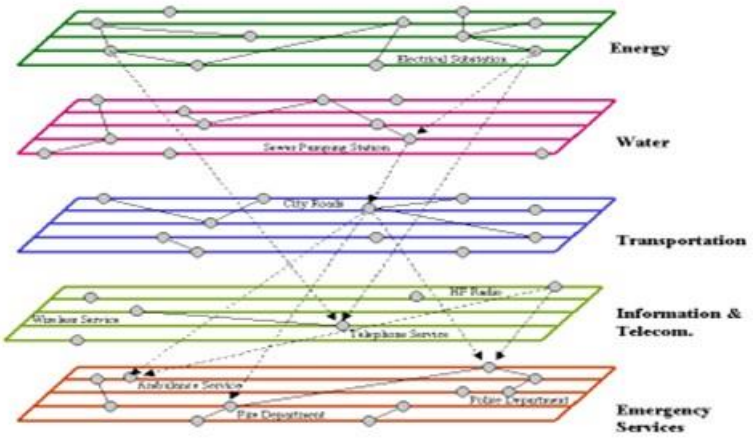


Figure 8: FP7 GAMMA European Infrastructure Interdependencies

In Figure 7, we see an important distinction between periodic and 'ad hoc' reporting. Periodic reports describe statistical information or lower priority summarises of cyber-security lessons. In the context of the present project, these might be exchanged between APOC partners every month. Summaries of these meetings may be exchanged at a national and European level – often with a degree of anonymity that might otherwise expose vulnerabilities. In contrast, ad hoc reports are time critical, normally in the immediate aftermath of an attack. They are intended to stimulate immediate action.

It is important to stress that the use cases that are embodied within existing European cyber-incident reporting tools cannot be directly applied to this project. For instance, it is assumed that individual companies report to Europe only through their regulatory agency. Hence they never directly interact with the pan-European system – all information is submitted and distributed through the NRA. This helps to retain access control and preserve the security of the incident reporting system. In contrast, subsequent pages assume that APOC stakeholders will be responsible for gathering reports within their airport and then directly interacting both with national bodies (security, regulatory etc.) and with a European coordinating agency.

As mentioned, it is possible to develop taxonomies of information that should be shared about any incident. For example, the following table adapts existing European incident reporting requirements for cyber-incidents under the Telecoms Directive for the APOC context. It is not definitive and represents a starting point for further discussion.

Data Identifier	Type	Description and Comments
Causes	Causal enumeration	Human Error/Hardware Failure/Software Failure/ Natural disaster/Malicious Attack/Third party failure, recommended by ENISA, (ENISA, 2011) Note there could be several root causes per incident. More detailed causes could be included in the taxonomy or additional details could be included in the free text description. A US list of cyber causal factors is available and can be accessed online (FCC, 2013).
Started	Date and Time	"The duration of the incident is the time span between when the service starts to degrade and when the service is available again to the end-user, or simply the length of time the end-user was unable to use the service" (ENISA, 2011, p11).

Data Identifier	Type	Description and Comments
Ended	Date and Time	"The duration of the incident is the time span between when the service starts to degrade and when the service is available again to the end-user, or simply the length of time the end-user was unable to use the service" (ENISA, 2011) p11.
APOC Services affected	Enumeration	This could vary from APOC to APOC depending on the nature of the implementation and the size of the airport but some agreement at a European level would be needed to compare incidents across different member states.
APOC service minutes lost	Natural	This is different from the duration of the incident because different services may be interrupted for different intervals within the overall attack but ENISA use this as a crude measure of impact.
Severity	Severity enumeration	See table 1 from ENISA 2011, p. 14. This provides a risk matrix that can be used to distinguish different levels of severity for different cyber-incidents.
Infrastructures affected	Service enumeration	Telephony/ Internet/ SMS/ Email/Others – note it could affect several of these (ENISA, 2011) p. 9. The FCC extend the ENISA list in NORS with satellite services. This is different from the APOC end-user services that are affected.
Actions taken	Recommendation enumeration	A range of actions might be taken in the aftermath of an incident. The Network Reliability and Interoperability Council have developed a list of Best Practices; which are also recommended by the FCC. These can be accessed via www.nric.org or online (FCC, 2016).
Shared?	Boolean	This field is set to true if the national regulator who created the incident report agrees that it should be visible to other APOCs/States. At present, this is a Boolean for simplicity but they may want to give more detailed permissions – e.g. only visible to other regulators in member states but not to other APOCs.
Created by	NR_user_id	It is important to have traceability back to the individual who created the incident report in the first place. Some incidents may cross multiple borders (two or more APOCs) hence it may be necessary to merge reports to avoid duplication.
NRA Comments	Append Only String	This field enables other regulators to add comments about similar experiences etc. – this is append only so that one member state cannot directly edit the contributions from other NRAs.
Description	String	This field provides a description of the incident and anything else that is not captured in the form. It is important to monitor these fields to see if data can be codified in the model. Also, it is important to implement free text search facilities over this data.

Table 12: Example of the types of data to be shared following a cyber-security incident

It is possible to identify a number of high-level architectures for information sharing. Figure 9 illustrates a relatively simple approach. As can be seen, a suspected incident is reported either through manual recognition or by an automated alert – for instance from an intrusion detection system. Inside the APOC, it will be necessary to safeguard the system and gather evidence. In an ideal situation, there should be sufficient forensic capability to reconstruct the attack vector. At present, ENISA is developing AV-CERT capability and individual member states also provide similar support – although in all cases these national bodies lack specific aviation expertise. The role of such external agencies is

considered in the following paragraphs. In contrast, the simple approach in Figure 9 assumes that the APOC stakeholders handle the forensic response internally. Causal analysis is complex here – in safety-related incidents, a root cause is defined to be a contributory factor that if it were prevented then the accident would not have occurred. However, in security if a vulnerability is patched then an attacker may look for other weaknesses. Hence, specialist support may be required to ensure that the response to an incident triggers a thorough review of other attack vectors that might be used in a second wave of attacks.

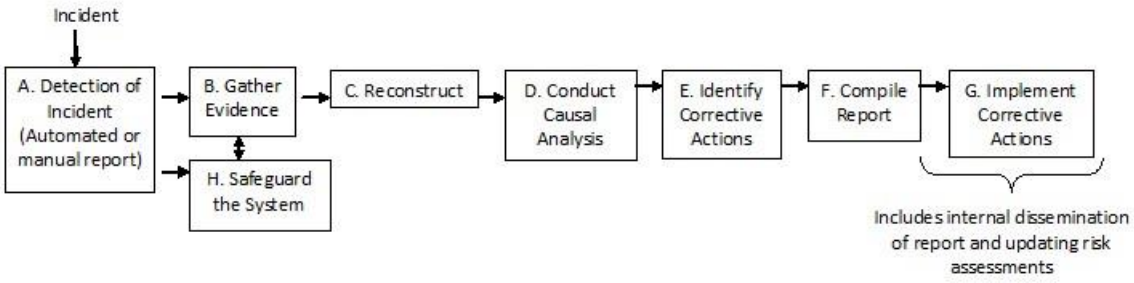


Figure 9: Simple Process for the Exchange of Cyber-Information

Figure 10 provides a more complex view of cyber-information exchange. As there are many stakeholders within an APOC and any one of these may suffer numerous low-risk attacks every day, a 'gatekeeper' or CISO is appointed with responsibility to monitor the threat level across all participants. Their role is to determine when to escalate a response and coordinate information sharing with higher levels of management in the APOC. This management cell is only convened in response to a major incident and every six months to review cyber-incident data. In Figure 10, these major incidents and periodic reviews are also shared with an external national body – and in the context of this project with European agencies. The internal management group would then also be responsible for the periodic review of cyber-threat surveys issues by the centralised European information exchange body.

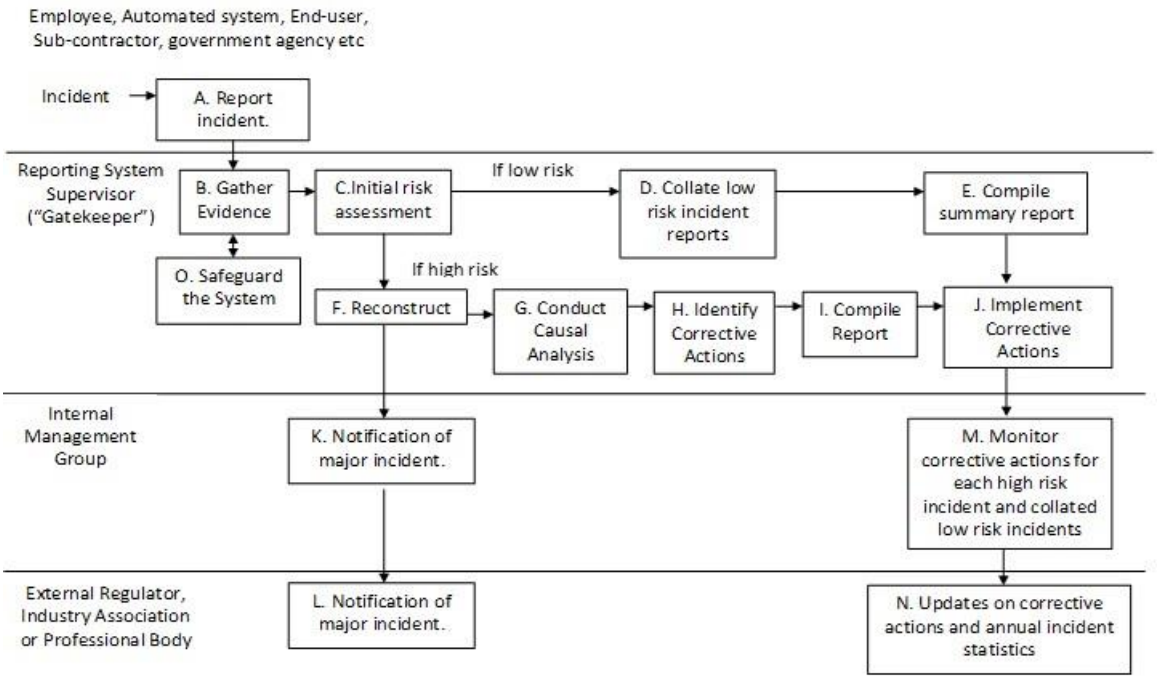


Figure 10: External Agencies in Cyber-Information Exchange

The previous two figures are not intended to explore every possible alternative for managing information exchange across Europe's airports. However, they begin to provide a structure for incident reporting and threat exchange. As mentioned, it is possible to identify alternative allocations of responsibility – especially for smaller airports where it is unrealistic to expect internal resources to support all of the tasks listed above. However, the key stages illustrated in these diagrams are the minimum expectations for the forensic response to cyber-incidents identified by both NIST is the United States and ENISA in Europe. Figure 11 provides a more elaborate overview – in this case, the Joint Industry Monitoring Group could be at the APOC level in larger airports, or across all national airports. The Security Agency/CERT function could be performed by EUROCONTROL coordinating support from ENISA and EASA.

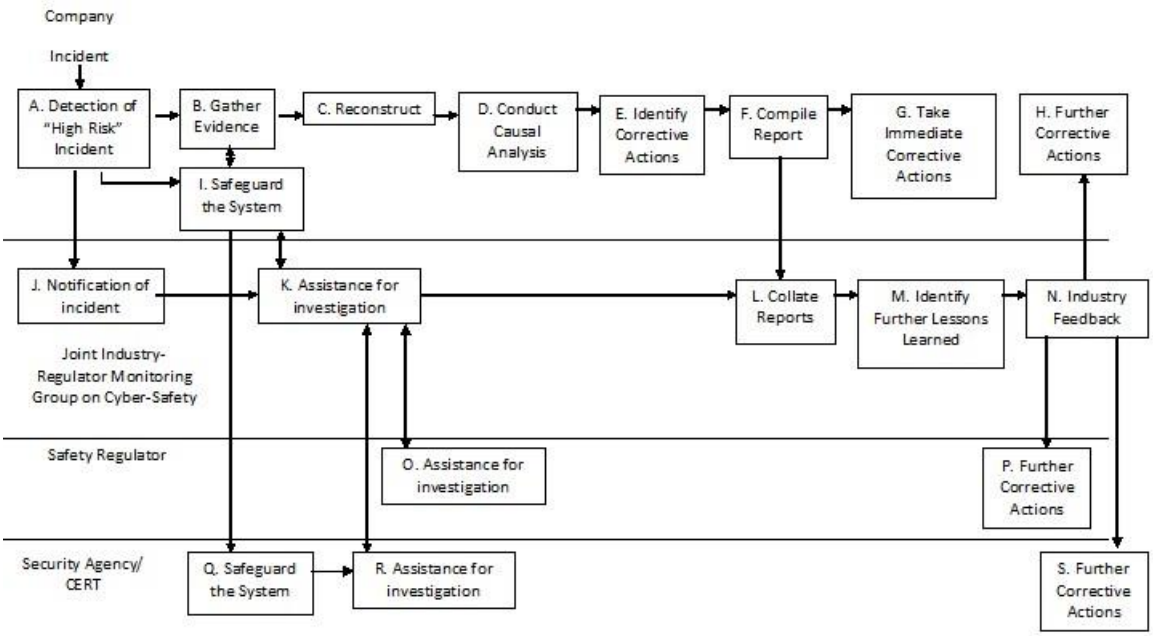


Figure 11: European Architecture for APOC Cyber-Information Exchange

Figure 12 uses the previous cyber-incident reporting architectures to derive a simplified data model for information exchange between APOCs and their associated stakeholders. This improves on the earlier generic use case that was derived from the existing European cyber-incident exchange systems because it explicitly acknowledges the role that APOC stakeholders play in contributing information both to national and to European agencies. It is important to note that APOCs might interact directly with the European coordinating agency but as mentioned previously this creates significant legal and political concerns over national sovereignty, hence we retain the NRA role used by ENISA.

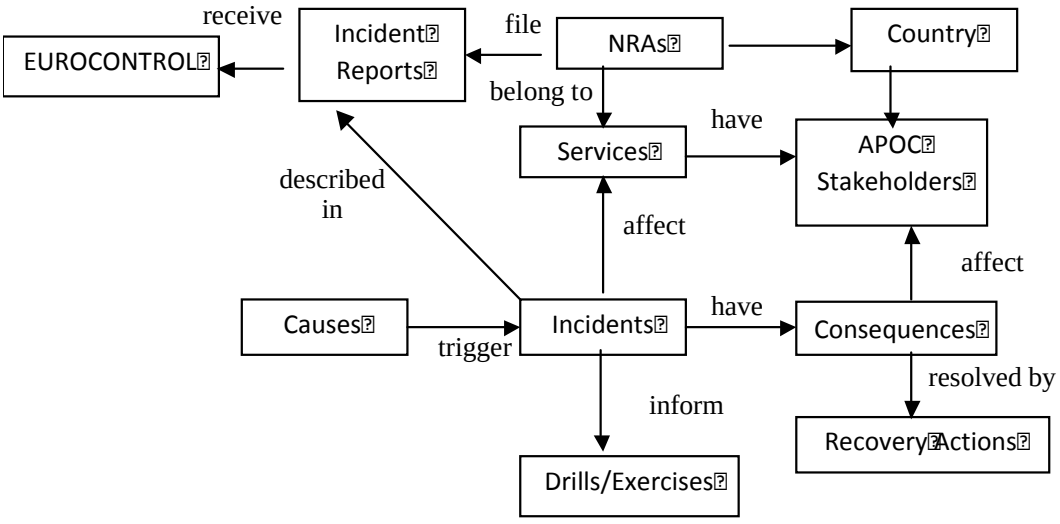


Figure 12: APOC Incident Reporting Data Model

5.3.1 Summary

This section has identified key roles in the exchange of cyber-security information between APOC stakeholders and the appropriate national/European coordinators. We have distinguished between the need for periodic (statistical) and ad hoc (responsive) mechanisms. We have also sketched some of the key information requirements for

incident exchange. The architectures presented here outline the forensic and incident response requirements for APOCs that are recommended best practice across the US (NIST) and Europe (ENISA).

5.4 Relevant ATM cyber-incident reporting mechanisms

The European Commission has recently funded a number of research projects, which are specifically developing architectures for cyber-incident reporting across Europe. The two most notable are FP7 Security Project ECOSSIAN – (European COntrol System Security Incident Analysis Network, (ECOSSIAN, 2016)) and FP7 GAMMA (Global ATM Security Management Project, (GAMMA, 2016)). The following section reviews our previous proposed use cases derived from the existing ENISA systems and architecture for APOC cyber-security information sharing against the proposals that are emerging from these two initiatives.

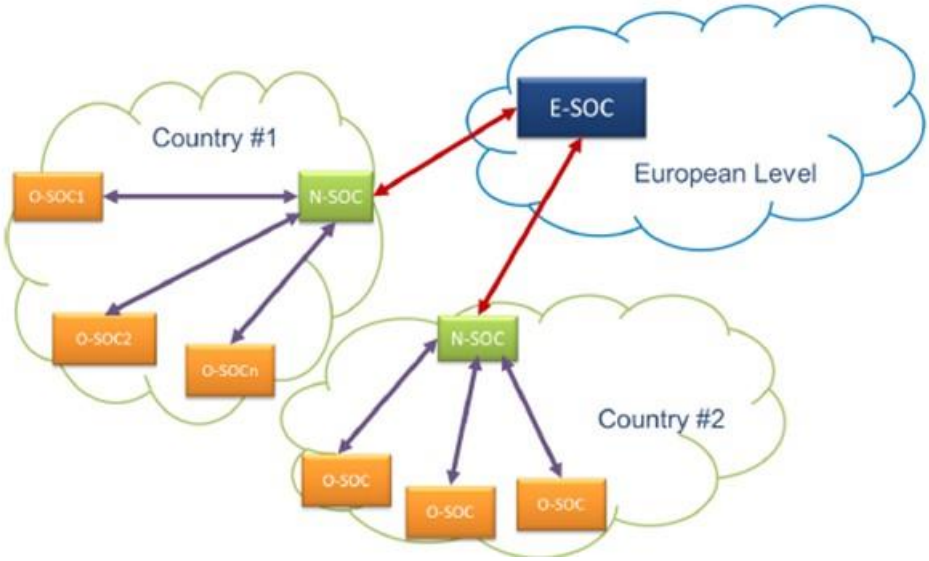


Figure 13: The ECOSSIAN SOC Hierarchy (1)

Figure 13 provides an overview of the ECOSSIAN incident reporting architectures. It is more general in the sense that they advocate the development of SOCs at an Organizational, National and European level. SOCs extend the focus of previous sections on information sharing – an SOC may also conduct audits and promote wider security measures. We view this as entirely consistent with the proposals in the previous section; recognising the problems if an APOC was to report direct to a European agency. Previous sections have avoided using the SOC concept because for many smaller/regional airports this may simply be an individual with direct responsibility for maintaining cyber-situational awareness within that organisation. Figure 14 provides a more focussed technical overview of the reporting system architecture that is being developed to support the SOC hierarchy. The term X-SOC stands for different levels of Organisational, National and European Security Operations Centres where the underlying support architecture is the same in each case.

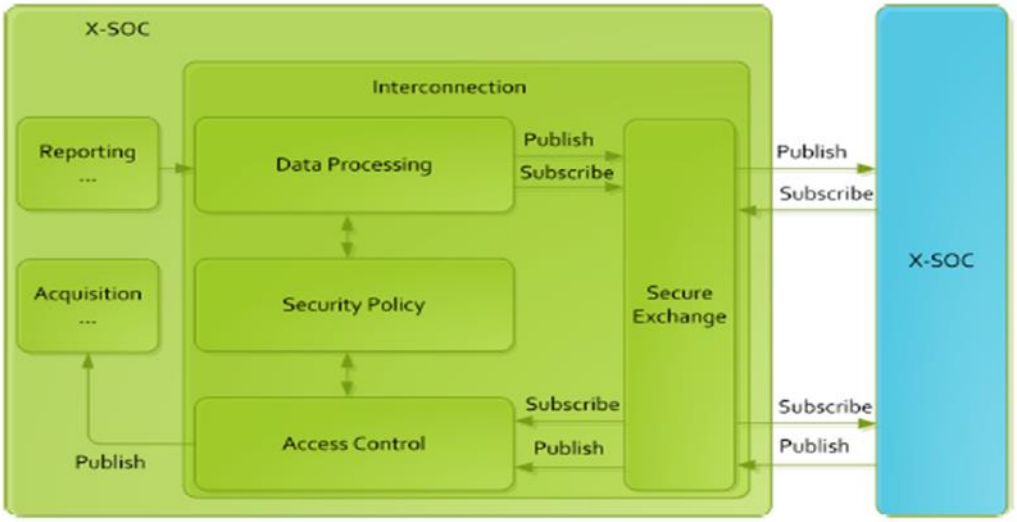


Figure 14: The ECOSSIAN SOC Hierarchy (2)

A key feature of this system is that users can exploit the publish/subscribe model – in many cyber-incident reporting systems stakeholders are overwhelmed with a mass of detailed reports about attacks on systems that they do not have installed in their organisation. In contrast, the ECOSSIAN reporting infrastructure enables users to explicitly subscribe only to those types of incident that are relevant to them – these preferences can be expressed in terms of the taxonomy introduced at the start of this section. Of course, the down side is that users may miss critical information if they only subscribe to a narrow range of incident parameters.

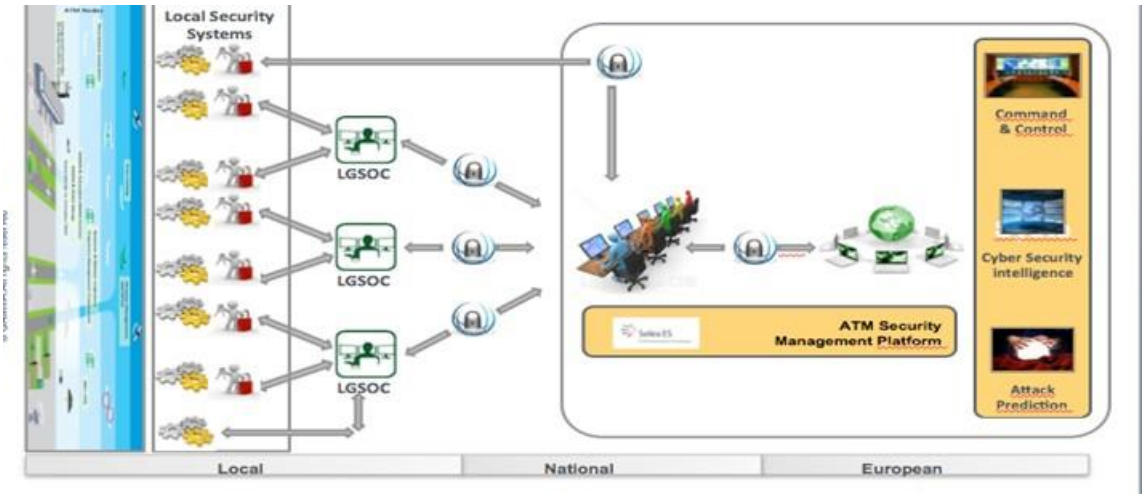


Figure 15: The GAMMA SOC Hierarchy

ECOSSIAN provides broad support for incident reporting across all critical infrastructures. In contrast, the GAMMA project focuses more narrowly on ATM. However, GAMMA shares the same high-level vision of local, national and European reporting mechanisms, illustrated in Figure 15. They have an ambitious agenda in which software support is developed to actively detect but also predict future incidents. Figure 16 provides an overview of the proposed Security Management Platform (SMP). Again, there are strong common themes between the aims of this research project and our work. The output of the GAMMA include visualisations that are intended to support cyber-situational awareness. These can be directly linked to the dashboards and other visualisations to be

presented in the following sections; similarly the work on maintaining and measuring the cyber-situational awareness needed to support SPOC cyber-CDM can all be applied to the GAMMA proposals.

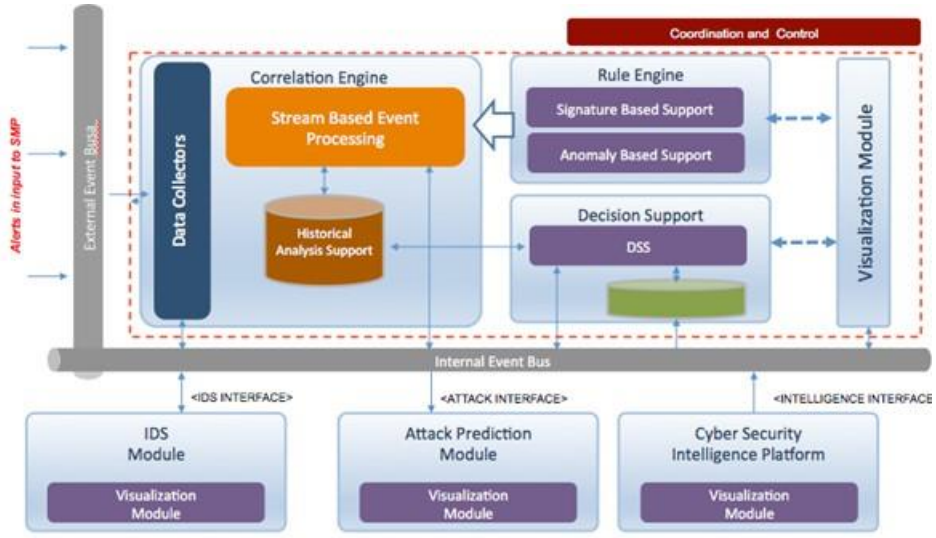


Figure 16: The GAMMA Security Management Platform Architecture

The previous section presented use cases and cyber-incident reporting techniques that can support CDM within APOCs and are consistent with the existing techniques used by ENISA's existing reporting infrastructures. In this section, we extended this analysis to demonstrate links between the proposals and more recent European research initiatives. The key point is that the options discussed for APOC sharing are consistent with both GAMMA and ECOSSIAN hence we are well placed to exploit the products of their research when they reach an appropriate level of maturity.

5.5 Dashboard design for APOC

The previous section indicated that the GAMMA project is proposing a number of different visualisations to support decision making through their Security Management Platform for Air Traffic Management. These are not publicly available – however, they will be incorporated if more details are available before the end of this project. In the meantime, it is important to summarise how APOCs might exploit existing cyber-security dashboards to support CDM and mutual cyber-situational awareness. There are two key concerns in developing such interfaces:

1) **False positives** undermine situational awareness if users continually have to dismiss irrelevant, false warnings.

2) **Missed positives** threaten security if the system fails to alert the user to a genuine threat. This is important because a system is not necessarily clean simply because a dashboard fails to warn the user of a potential compromise.

Crucially, there is often a trade-off to be made; reducing the number of false positives often implies an increased likelihood of missed positives. It is also important to stress that some recent attack methods deliberately infect anti-viral products so that running the dashboard may install the malware.

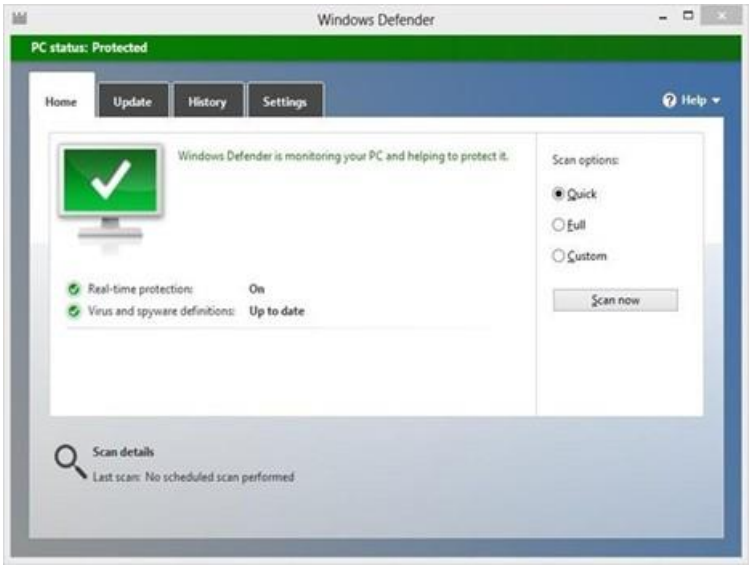


Figure 17: Microsoft Defender User Interface

Figure 17 illustrates the mass-market Microsoft Defender interface. It has a number of key features that are common to cyber-security dashboards. It hides the details of the algorithms and techniques that are used to monitor the underlying system. This is important because the intention is to provide a 'health check' that will trigger further actions if a problem is identified. The person or team using the dashboard need not be the same as the individual/team responsible for acting once an issue has been identified. Defender uses a black-list approach to intrusion detection – it relies on signatures (file characteristics, process structures) to look for potential malware. These signatures are, in turn, identified and shared by security companies and national intelligence agencies. No such signature exchange mechanisms exist within aviation hence the approach would have to build on more general sources – for example, the US Industrial Control System CERT provides updates that are applicable for some aspects of APOC operations. We cannot, however, expect these to identify attacks that are specifically focussed on aviation infrastructures or which have not been identified in other industries.

We can contrast Figure 17 with Figure 18 which provides a flavour of the lower level monitoring that is hidden by an appropriate dashboard. The key here is that following the indication of a problem it must be possible for investigators to gather the forensic data within the system logs indicated in Figure 18. This is a non-trivial requirement. Most aviation organisations do not retain forensic data, system logs are only held for debugging and performance monitoring. EASA is concerned that if a serious attack did occur today, we would not have the lower level information necessary to identify the attack vector. Hence, before we can implement the dashboard concept, APOCs would need to conduct an audit to identify high-value systems and the level of detail that would be needed – for instance, to trace back and identify previous attacks. The decision to focus on core or high value systems is justified by the associated costs with maintaining and preserving the mass of lower level details that might be required in the aftermath of a cyber-attack.

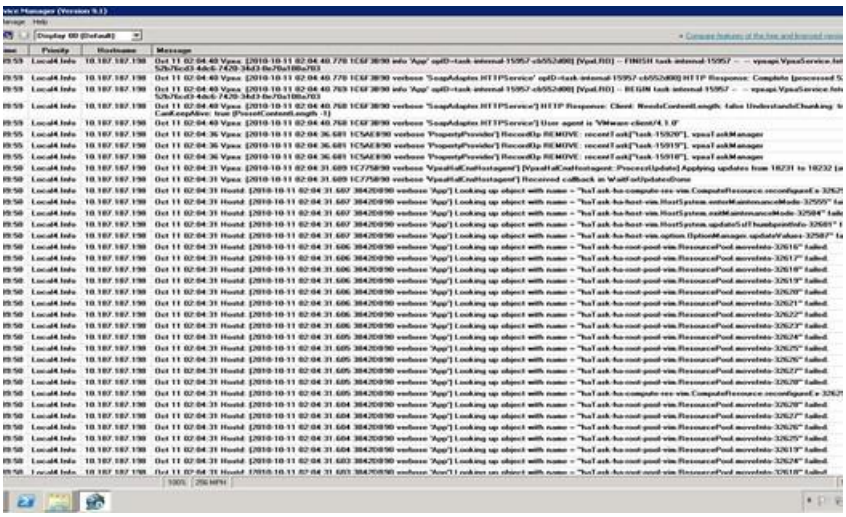


Figure 18: System Logs Underpinning Cyber-Dashboards

Figure 19 illustrates a white-list approach to intrusion detection. This shows the network traffic within a European ACC with each peak corresponding to increases in traffic over a 24-hour period. We can use this to form a picture of what a 'normal' day might look like. In contrast to the black-lists used by Defender in Figure 17 a white list does not try to identify malware signatures, instead it tries to ensure that only approved software is running. Here we attempt to characterise normal behaviour and issue an alarm when we detect anomalies. One of the major problems here is that we do not have sufficient evidence of normal network traffic in APOCs to refine our white list – however, it is far easier to compile a whitelist early in the development of the APOC concept updating each time new services are integrated into a software architecture. There are further concerns. If sub-contractors install updates that are unknown to the whitelist then the Intrusion Detection System will generate security warnings.

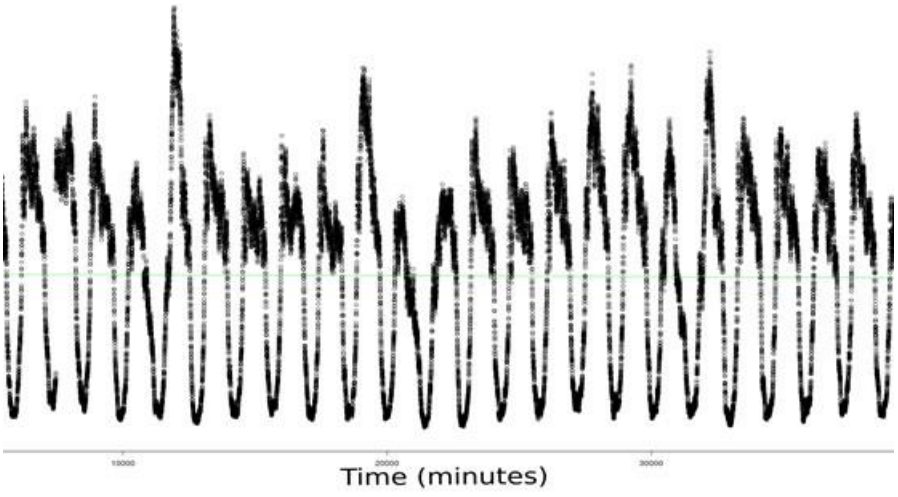


Figure 19: Linking Network Data to APOC Significant Events

We would recommend that APOCs exploit a hybrid approach of white list and black list technologies. The NIS Directive should improve the exchange of malware signatures for black lists through the incident reporting/information exchange that is summarised in previous sections of this report. At the same time, whitelisting helps review the processing and networking resources used by APOC components. The discipline and cost of

compiling and maintaining a whitelist is justified by the significant benefits it provides to long-term cyber-situational awareness. The application of these approaches must be tempered by a degree of pragmatism – given that it can be hard to characterise the requirements of legacy systems. It follows that the dashboard might focus on specific high-value systems and not cover other areas of an APOC. However, if some action is not taken to support these techniques then there is little prospect that a dashboard can be developed to support cyber-CDM.

Figure 20: The Alien Vault Dashboard

Figure 20 illustrates the user interface to the Alien Vault dashboard. This is a general-purpose visualisation tool for Security Information and Event Management (SIEM). In the screenshot on the left, the top right graph shows the number of security related events over the last 24 hours. The top right provides a colour coded high-level assessment of the threat level in terms of the number of identified threats over time. The bottom left visualisation shows the number of security events being recorded per system – recall that it may not be appropriate to monitor all applications within an APOC. The image on the bottom right has been configured to show the distribution of security events over a longer period of time – weeks rather than hours In particular, it focuses on unresolved alarms and open tickets. These are security concerns reported by staff awaiting a response.

In contrast, the screen on the right shows how a user of Alien Vault can drill down to look at specific system logs that drive the higher-level visualisation tools. It is open source and hence some of the concerns about malware insertion within the dashboard can be mitigated. This tool supports automated asset discovery – this is important because we cannot detect or mitigate an attack if we are unsure what is connecting to an APOC. This is a significant concern given the ad hoc way that some of these infrastructures have developed – with multiple stakeholders bridging their systems across shared network infrastructures. It will also conduct a vulnerability assessment by identifying common network and server configuration problems. It will also look for necessary patches and updates.

The key point here is not to advocate this tool as the ideal solution for APOCs but to illustrate what is possible. The following section focuses on metrics for CDM and cyber-situational awareness that must be identified in order to determine the degree of support that such desktops might provide within the APOC concept of operations.

5.6 Summary

This section started with a summary of the information that might be exchanged both within and between APOCs about potential cyber-incidents. We then built upon ENISA's existing reporting systems to identify an architecture that supports sharing across Europe, which is also consistent with the Network and Information Security Directive. We distinguished between ad hoc and periodic reports and stressed the role of national regulators as an interface between APOC stakeholders and European agencies for international information sharing, given concerns over national sovereignty.

In existing European reporting systems, the regulator in each member state coordinates the provision of data and reports through a web interface to ENISA who then distribute the reports to other member states. This avoids the situation where ENISA might be seen to side-step national regulatory provision. We would recommend a similar scheme across Europe's airports – given that in many member states there is a legal requirement on operators to report safety (and security) concerns to the national regulator before any European agencies. This creates a framework for cooperation between each state and Europe. It is important to note that APOCs might interact directly with the European coordinating agency but as mentioned previously this creates significant legal and political concerns over national sovereignty, hence we retain the NRA role used by ENISA.

It is premature to build an APOC specific taxonomy for the exchange of cyber-incident data given that the NIS Directive is moving towards implementation. This will enter into force in August 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services. This places a requirement on airport operators to report cyber-incidents; it is highly likely (certain) that ENISA will coordinate the information requirements for the implementation of this directive and any APOC specific taxonomy should be consistent with this. Subsequent sections demonstrated that this approach was consistent with the interim results from the GAMMA and ECOSSIAN EC research projects.

Finally, we showed how cyber-incident information might be visualised and communicated using existing dashboard architectures. However, the use of these systems relies upon the acquisition and monitoring of system logs that are not routinely available within some airport networks. Before we can implement the dashboard concept, APOCs would need to conduct an audit to identify high-value systems and the level of detail that would be needed – for instance, to trace back and identify previous attacks. The decision to focus on core or high value systems is justified by the associated costs with maintaining and preserving the mass of lower level details that might be required in the aftermath of a cyber-attack. The following section identifies ways of assessing the contribution that such tools can make to cooperating decision making in response to potential cyber-incidents.

6 Common cyber-situational awareness

6.1 Introduction

This section sets out to ensure that any increase in cyber-incident information sharing supports rather than undermines the mutual situational awareness of key APOC stakeholders; it is critical not to swamp decision makers with a mass of irrelevant detail and false alarms while at the same time ensuring that they have the information they need to respond to potential attacks. There is also a concern to provide an appropriate level of detail with higher risk attacks – on the one hand, if insufficient information is provided then stakeholders may find it hard to mitigate any future attack – and at the same time if too much detail is provided about a specific attack then it can be hard for recipients to translate those details into lessons that can be applied in their own, different operating environments. There are also related concerns over the inadvertent disclosure of IPR or of other confidential data during the exchange of information on cyber-incidents.

The approach used here is to propose appropriate metrics that can assess the level of cyber-maturity within an organisation and Cyber-Situational Awareness (CyberSA) for particular end users of a dashboard/SIEM system.

Key concepts/ideas in this section include the distinction between the cyber-security maturity of an organisation, which provides an overall measure of the general awareness of cyber-threats and mitigations, and the concept of situational awareness applied to key individuals making critical decisions in response to specific threats. We provide proposals for measuring both organisational cyber-maturity and for the measurement of CyberSA, for instance within an APOC integrating dashboards with other information displays. This organisational work builds on the previous work of Helios and Thales on the cyber-maturity of SESAR and also on EUROCONTROL studies led by Barry Kirwan (Reader, et al., 2015) in safety culture. Subsequent sections identify metrics for assessing individual and group cyber-Situation Awareness. These stem from Endsley's (Endsley, 1995) three-level model that dominates the literature in this area and is widely applied by the FAA and by SESAR itself.

The objectives for this section are to:

1) Develop the cyber-security KPIs in line with the other APOC KPAs identified in the SESAR role definition.
2) Build on previous work into CyberSA, especially across multi-stakeholders, avoiding false positives that might delay operations and false negatives that raise security concerns.
3) Develop principles for cyber-security CDM/SA across national borders, when information about vulnerabilities and threats relate to both national security and sovereignty.

6.2 More Detailed Approach

A principle within this study is to build on previous work rather than invent one-off solutions that while customised, are likely to be prohibitively expensive for APOCs to develop and maintain. For example, the previous section focused on the open source Alien Vault security information and event management (SIEM) tool. It is important to ensure that such representations can be integrated into the wider aspects of APOC CDM.

One possible way forward would have been to deploy this or a similar tool into an APOC.

CyberSA is a dynamic area; previous sections have described how GAMMA and ECOSSIAN are developing new techniques in addition to those already available. There are dozens of potential visualisations and it is hard to know which might offer the greatest support to the cyber-security of future generations of airport operations. Before deploying any particular system, it is essential that we understand how to measure the success/failure of a dashboard and related tools. This section, therefore, focuses on metrics to assess enhanced situational awareness and cooperative decision-making that are the result of appropriate visualisation techniques. We build on the following three stages for CyberSA:

1) **Enumerate Suitable APOC CyberSA KPIs**: Existing KPI's for cyber-security within SESAR tend to focus on the duration of interruptions to service. Such metrics ignore situations where a system is known to be insecure but where we lack the financial or technical resources to protect it in the short term. Interruption-based metrics create a false sense of confidence. Zero minutes of interruption might not indicate a high degree of protection but instead arise because we were lucky not to suffer an attack. In contrast, KPIs for CyberSA consider a broad range of vulnerabilities and provide a fair measure of the confidence that we might place in APOC infrastructures – identifying areas of strength and of weakness. CyberSA metrics can distinguish between situations where we know there are vulnerabilities and are acting to address them from situations where we do not even understand our vulnerabilities.

2) **Analyse Interactions between CDM and APOC CyberSA**: Cyber-Situation Awareness is not an end in itself – the key output of improved information and communication is to focus and inform collaborative decision-making. Key decisions have been documented in the use cases later. We argue that the resulting information requirements for CDM can provide the foundations for subsequent cyber-exercises as more APOCs reach full deployment.

3) **Document Cross-Border, Cross-Industry Concerns in APOC CyberSA**: Cyber-SA requires international cooperation. Cyber-incidents may be detected in one member state and be launched using proxies in another country stemming from attackers in a third state. This builds on the cross-border concerns identified in the use cases; where for example, the identification of an incident should automatically result in the ad hoc notification of APOC partners but also national and international police and regulatory agencies. In some ECAC states, there are recognised single points of contact (typically national CERTS) in other countries things are more complex – for instance, reflected in distinctions between the UK CAA, CPNI, UK CERT and GCHQ/CESG.

6.2.1 Key Issues

The following key issues are at the heart of this section:

1) Conventionally CyberSA has focussed on individuals and small teams, how can we scale these concepts up to the distributed networks of stakeholders intended within the APOC role document across technical, organisational and cultural boundaries?

2) How do we ensure cooperation and agreement in decision making when everyone involved in an APOC will have to work together to secure their systems?

3) How do we sustain the self-confidence in APOCs to respond effectively and in a timely fashion with their own resources and at the same time rapidly identify situations where airports need external support?

6.3 Cyber-security Maturity Assessments

The previous section described techniques that can be used to share information about cyber-threats. The intention is to support CDM in response to a growing range of possible attacks. However, these techniques will not be successful unless we improve the underlying cyber-security maturity level among APOC stakeholders. Previous work within the SESAR programme has established techniques for measuring cyber-security maturity at European, National and organisational levels (Helios/Thales, 2015). The following sections focus on organisational metrics appropriate for APOC operations. The subjective assessment can be replicated for individual service providers, where appropriate drawing on evidence of policies and processes deployed within a particular company. The following sections build on this to identify more detailed KPIs for cyber-security within the context of airport operations.

Leadership and governance

Objective: Leadership should establish clear roles, responsibilities, appropriate investment and budgets. Cyber-security awareness should be championed with a corresponding management system. Cyber-security performance indicators should be established and reported.

There is a lot of divergence in the approach of different airport operators with respect to cyber-security. Some have a defined strategy, whilst others adopt a more reactive approach and only develop actions and implement fixes as a result of incidents. Some are taking a strong lead, having established a CISO, but others are not engaging with the topic as a whole.

The level of maturity of cyber-security governance depends on the competence and experience of those being appointed as CISO. Many have experience in physical rather than cyber-security. Also their lack of ATM background can make explaining how to implement the cyber-security process to those in operations difficult. Other CISOs have extensive aviation experience, which can make implementing a SecMS/ISMS within their organisations easier although it may also limit their exposure to cyber-security techniques from other industries. As cyber-security is a relatively new specialism within ATM, it is recognised that there are only a few security experts and it will take time to develop individuals with experience in both ATM and cyber-security. The following legend was introduced in the previous SESAR project to reflect individual assessments of cyber-security maturity; across Europe as a whole we might argue that leadership and governance within cyber-security is ad hoc and not harmonised.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Cyber-security Risk Management

Objective: Regular (re)assessment of cyber-security obligations, context, assets, risks, issues and maturity occurs. Risk management should be the basis of all cyber-security activities.

There is a large variance in the management of cyber-risk across APOC stakeholders and between different airports. Some companies are well advanced in establishing SecMS/ISMSs, but there are also many, which are not close to establishing SecMSs/ISMSs and some are not even aware of the need for a SecMS/ISMS. There is sometimes still significant uncertainty over residual risks. Until each organisation has completed a risk assessment in all areas of business (e.g. both operational and IT systems) understanding the main risks will continue to be difficult. A host of complex, technical issues remain to be solved – these include the need to secure both new commissions as well as a vast array of legacy infrastructure.

Different organisations use different methodologies for risk assessments and express risk in different ways. This makes information sharing difficult as it needs to be exchanged in a standardised way in order to compare and combine the results of risk assessments to get a harmonised system. There is also limited coordination with national security risk assessments in some member states.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Compliance and assurance

Objective: A compliance and assurance regime should be implemented across the organisation, partners and suppliers. Technical level assurance should be implemented through accreditation, audit, evaluation and/or certification of systems and services. Periodic internal and external reviews provide independent assurance.

There are defined compliance and assurance mechanisms, but in some member states each airport operator currently works in isolation in the absence of mechanisms to share best practice. In other countries, there are coordination mechanisms – for instance, in France airports share information in an ANSSI working group. ISO27001 (ISO/IEC, 2013a) is generally accepted as a basis for assuring cyber-security, and is often used as a means of compliance with 1035/2011 for SecMSs. There are standards available (CEN, 2014), (ISO/IEC, 2013a), (NIST, 2013) for operational stakeholders and supply chain to use and considerable material available from other sectors that is applicable to civil aviation. However, it is not considered to just be a matter of stakeholders applying the existing standards, as the information is not necessarily deemed to be complete and there is disagreement about the best standards to apply. There are not yet mature and accepted standards/best practice, but instead pockets of progress. This can be considered comparable to when the industry first began to formally implement safety.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Security architecture

Objective: An enterprise wide, architectural approach to cyber-security should be taken, which is clearly aligned to operational and business drivers. Security principles underpin this architecture.

There are defined mechanisms for dealing with security architectures of new and legacy systems, but these approaches vary across airport operators. Some have put in place perimeter protection of their legacy systems in the interim and then plan to migrate to an APOC SOC for the new systems. Approaches vary but plans do exist, although the results of some risk assessments show that there are some systems with no real protection.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Security requirements

Objective: Cyber-security engineering requirements should be established for the systems and organisation. Cyber-resilience is considered as a key requirement during feasibility and requirements definition stages of projects.

There are defined processes for developing security requirements, but more experience is needed in using them for systems especially audit within the context of APOC operations. It is recognised that a holistic approach needs to be taken to cyber-security requirements so as not to neglect other aspects of security, such as training and the organisation. For example rather than demanding complex technical controls, it may be easier to establish procedural rule (e.g. compare a bespoke system without USB ports to a policy of not using USB ports). APOC stakeholders are beginning to develop their own security requirements, but they could benefit from assistance in interpreting the standards into requirements. The acceptable level of risk for aviation systems also needs to be established in order to develop requirements.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Security engineering

Objective: Cyber-resilience should be built into systems through engineering processes. This includes, for example, secure coding practices, test and vulnerability management, developer/engineer security, and penetration testing.

Various frameworks and methods exist to achieve security engineering, but it seems that many APOC stakeholders still regard security as little more than an additional burden and there is limited demand for security solutions, but some operators have more defined processes. For the supply chain, security can still be seen as an additional burden with a temptation to do the minimum. Some suppliers and operators are beginning to improve processes to make them more secure. There are stakeholders who enquire about the processes being applied in order to ensure the security of the system, especially military customers, but this is a costly process.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Security in Acquisition

Objective: Cyber-resilience should be built into systems and service procurement processes through the inclusion of requirements, descriptions and criteria in the acquisition contract for the system or service in accordance with the applicable legislation and regulations, policies and security architecture.

Unlike a lot of areas where there are standards, secure acquisition and procurement is an underdeveloped aspect, even in other industries. Currently this area focuses on how requirements are specified in the contract and shifting responsibility to suppliers, rather than using cyber-liability insurance or jointly managing risk in an effective way. The supply chain has a similarly patchy approach. For safety there is an established safety acquisition process to ensure that newly purchased systems are safe, and culture change is required to deal with security requirements in a similar way. This is critical given that many airport operators are in the process of integrating services to realise the benefits implicit within the APOC concept of operations. The supply chain view is that airport operators are not mature in expressing their cyber-security requirements. They are sometimes very high level and it is unclear if the requirements need to be fulfilled via technical control or the equipment. There needs to be flexibility for APOC stakeholder to decide between safety and security without defining all actions as requirements on the equipment. Airport operators vary in maturity, but are currently coordinating to establish best practice on how the security requirements are dealt with, and whether this is through adaptions to the equipment or to operational procedures.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Operational Planning

Objective: Alongside the development and procurement of secure and resilient systems, the accompanying procedures should be planned.

Alongside the development and procurement of secure, resilient systems, is the need for planning the accompanying procedures. This includes procedures for use and maintenance, and contingency planning for cyber-attacks. APOC stakeholders are at varying stages of maturity, but are currently coordinating to establish best practice on how the security requirements are dealt with, and whether this is through adaptions to the equipment or to operational procedures.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Situational Awareness (Discussed in more detail in section 6.5)

Objective: Activities should be established and maintained to collect, analyse, alarm, present, and use operational and cyber-security information. CDM is facilitated through engineers and management being involved across organisational boundaries. This involves threat intelligence and awareness; continuous scanning, logging and monitoring; vulnerability auditing; promotion of results through regular briefings.

Situational awareness varies but is mostly unaddressed/ad hoc and is not coordinated. More needs to be done to develop and share threat intelligence data, between APOC stakeholders, with other industries and national security agencies. Airport operators are taking different approaches to security, with some implementing a perimeter approach and others an SOC approach, but all are certified.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Protection and detection

Objective: System controls should exist to protect systems from attack, and detect attacks when they do occur. These include technical controls, such as access controls, network defence, intrusion detection, communications security, etc.; physical and environmental protection; media protection; associated asset, change and configuration management.

Protection and detection depends on the high level objectives of the organisation. Many companies adopt the minimum level of protection. They may accept not protecting the old system, but this is driven by the risk and threat level of the individual operator and their State, and is also linked to the level of maturity of the organisation. Operators also do not currently possess the capabilities to implement a fully secure cyber-defence, as this takes time and the risks are not fully understood. Once the probability of a potential security

incident is understood, it becomes possible to prioritise the necessary mitigating actions and develop risk-based proportional security safeguards. It is important to stress, however, that these activities must not sacrifice core objectives – when for instance monitoring delays the exchange of necessary information or where faults in anti-viral products bring down otherwise correct operational systems.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Incident response and recovery

Objective: As well as a localised implementation of the EATMS contingency measures, with sufficient integration between these two levels of activity, there should be: reporting, prosecution and legal response, lesson learning, and post-incident adaption.

This has been discussed extensively in the previous section, but it is important to honestly assess available cyber-information sharing mechanisms when considering the cyber-security maturity level of existing airport operations. Many airport operators have defined processes for response and recovery, but these measures are not harmonised or coordinated across the industry and borders. There are national laws that govern the transfer of information across Europe and some information is classified, especially linked to certain events. It is necessary to develop means to share information on incident response and recovery, especially to avoid propagation of attacks across the network to neighbours without exposing sensitive information about existing vulnerabilities. Here transverse activities including common EATMs cyber-security services and contingency measures are important. Coordination on safety is easier in civil aviation as there is a history of sharing safety information. The problem is that cyber-security is a new topic for airport operation and comes with sovereignty issues surrounding information sharing and it needs to be established how to increase cooperation between pan-EU and national level.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

Awareness and training

Objective: The capability needed by the staff, contractors and suppliers should be developed through awareness raising, education and training, embedding a security culture within the organisation, and running cyber-exercises to build readiness and learn lessons.

There are varying levels of awareness in different organisations. This is an extremely important action at every level – CEO, Director, operational, and technical - but APOC stakeholders are mostly still at a very early stage of awareness training, so this is an important action to progress. In order for this to be achieved, it is important to measure

returns from investment in cyber-security training – to ensure that any investments are not ignored.

Maturity	Unaddressed	Ad-hoc	Defined	Managed	Optimised
Harmonisation	Isolated	Coordinated	Collaborative	Harmonised	

6.4 Cyber-KPIs for APOC

The previous section presented a number of attributes that can be used to assess the cyber-security maturity of APOC stakeholders. Improving this maturity takes a considerable amount of time and effort – for instance, through changes in training and in management structure. In contrast, the APOC concept of operations is specifically intended to improve a broad range of more dynamic Key Performance Indicators (KPIs). EC 691/201013 describes the requirements for KPIs as follows:

Key performance indicators should be selected for being specific and measurable and allowing the allocation of responsibility for achieving the performance targets. The associated targets should be achievable, realistic and timely and aim at effectively steering the sustainable performance of air navigation services.

At a more detailed level, EUROCONTROL have proposed criteria for the identification of appropriate KPIs, as shown in Table 13 (Kosanke & Schultz, 2015). These in turn have motivated the proposed APOC KPI's illustrated in Table 14. These metrics relate to slot adherence, punctuality, throughput, efficiency, connectivity and environmental impact.

Criteria	Description
Significance	• KPI has the ability to monitor respective airport activity • Changes in performance should be clearly recognizable in KPI value changes
Number of covered objectives	• Each objective defined in step 1 needs to be covered by at least one KPI • KPIs covering several objectives are preferred
Measurability	• General ability to be measured is prerequisite • Direct measurement of KPI is possible or need of expressing the KPI in terms of supporting metrics • Performance is quantitatively expressed • Abidance to privacy regulations
Data availability	• Necessary investments to provide required data • Sufficient data quality is a prerequisite • Necessary data granularity
Real-time availability	• Calculation of KPIs has to be possible in real-time • KPIs should be able to be forecasted for a time-frame of 24 hours

Table 13: KPI Attributes

One approach to measuring the success of cyber-security measures would be to assess the impact of all previous cyber-incidents on a subset of these higher-level KPIs. In other words, the impact of a cyber-incident could be measured in terms of the reduction in runway utilization or equipment resources per interval. This approach would be well aligned with the overall APOC and TAM concepts, illustrated by the DLR KPI prototypes shown in Figure 21. APOC stakeholders could visualise the impact of an incident in real time through the reduction in efficiency, punctuality, throughput shown in the APOC shared displays.

Performance Indicator	Measurement Variable
De-icing resources per interval	$\frac{\#\text{ used de-icing equipment}}{\#\text{ available de-icing equipment}}$
De-icing queue per interval	$\#\ \mathrm{A/C\ in\ de-icing\ queue}$
Keeping the de-icing duration per interval	$\frac{ADIT}{EDIT} = \frac{AEZT-ACZT}{EDIT}$
Snow removal resources per interval	$\frac{\#\text{ used snow removal equipment}}{\#\text{ available snow removal equipment}}$
Limitation of A/C stands per interval	$\#\ \mathrm{snow\ covered\ A/C\ stands\ (Terminal/Apron)}$
Limitation of taxiways per interval	$\#\ \mathrm{snow\ covered\ taxiways}$
Keeping of the snow removal duration of the runway per interval	$\frac{ADORC}{EDORC}$
Runway queue per interval	$\#\ \mathrm{A/C\ in\ runway\ queue}$
Taxiway resources per interval	$\frac{\#\text{ open taxiways}}{\#\text{available taxiways}}$
A/C stand resources per interval	$\frac{\#\text{ occupied stands (Terminal/Apron)}}{\#\text{available stands (Terminal/Apron)}}$
Keeping the planned A/C stands per interval	$\#\ \mathrm{changed\ A/C\ stand\ positions}$
Runway occupancy time per interval	$\sum(ATLR-ATFT)+(ATDR-ATOT) = \sum AROT$
Runway utilization rate per interval	$\frac{\#\text{ flight movements}}{\text{capacity}}$
Utilization rate per interval (departure)	$\frac{\text{handled traffic (departure)}}{\text{capacity (departure)}}$
Utilization rate per interval (arrival)	$\frac{\text{handled traffic (arrival)}}{\text{capacity (arrival)}}$
Equipment resources per interval	$\frac{\#\text{ used equipment}}{\#\text{ available equipment}}$
Waiting queue for GH-service per interval	$\#\ \mathrm{declared\ A/C\ for\ GH} - \#\ \mathrm{handled\ A/C\ by\ GH}$
Keeping the estimated duration of turn-round per interval	$\frac{ATTT}{ETTP} = \frac{AOBT-AIBT}{ETTP}$

Table 14: Examples of APOC KPIs (Kosanke & Schultz, 2015)

Figure 21: DLR KPI APOC Visualisations (Guenther, 2013)

There are numerous problems with this approach. It only provides information to stakeholders during or after an attack. It is entirely backwards looking and provides little information about the likelihood of future incidents. In a vulnerable system, the fact that there are no previous incidents affecting other KPIs should not inspire confidence. Simply because there has not been any previous attack does not mean that there will be no attacks in the future. The use of existing performance based KPIs cannot be used to measure changes in the threat level – for instance from the publication of zero day exploits in APOC sub-systems or changes in the socio-political environment, for example when environmental protest groups advocate direct action to resist airport expansion. Hence we need metrics that reflect our ability to detect and resist future incidents rather than a retrospective measure of the previous impact of cyber-attacks on our

infrastructures. It is for this reason that we have advocated the combination of organisational cyber-maturity assessments, presented in the previous section, together with more detailed metrics for the CyberSA of key APOC stakeholders – at the individual and team level. These are presented in the following section.

6.5 Cyber-situational awareness

The following sections build on the pioneering work of Endsley on assessing situational awareness in safety-critical systems. This is justified because Endsley's work has been widely applied in Air Traffic Management, including within the SESAR programme. It is arguably easiest to identify attributes of situational awareness after it has been lost. The concept can be defined as follows:

"Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988)

Projection is a key issue in this definition. In other words, the aim of promoting situational awareness is for the decision maker to be able to anticipate the effect of future actions on complex systems. Such predictions are supported when decision makers have a clear understanding of the existing state of their system. Initially, work on situational awareness was narrowly focussed on safety-critical systems. Metrics were developed to measure the users' ability to predict the future safety of complex application processes. However, there has been a growing focus on CyberSA (Tadda, 2008). Much of the previous work on cyber-incident reporting, including the new Network and Information Systems Directive, is specifically intended to improve situational awareness. For instance, Table 15 provides an overview of the ECOSSIAN work in this area.

	Fusion Level 0/1 Signal/Object Assessment	**Fusion Level 2** Situation Assessment	**Fusion Level 3** Impact Assessment	**Fusion Level 4** Process Refinement
Perception	Data Measurement	Situational Element Processing	Threshold / Alarm Function	
Comprehension	Analysis & Object / Element Identification	Situation Recognition / Classification	Goal / Performance Analysis	Action Planning and Selection
Prediction		Future State Estimation / Trend	Future State & Impact Evaluation	Effect Estimation

Table 15: The Impact of Data Fusion on Situation Awareness in the ECOSSIAN project (Kolev, et al., 2013)

The fusion level in Table 15 refers to the integration of data through the range of cyber-security monitoring tools being developed within the GAMMA project. The levels are core concepts within the Endsley view of situational awareness.

- **Perception** by a user of their environment: This is important because users have finite perceptual capabilities. There are limits to the amount of information they can attend to. If data is poorly presented or missing then users cannot correctly perceive the state of their system and are unlikely to make accurate future predictions. In terms of cyber-security, APOC stakeholders cannot respond to an attack if they lack the data that is necessary to detect that it has occurred.

- **Comprehension** of a situation and its significance determined by the user's goals: In other words, even if a user is presented with data they cannot make accurate predictions if they do not understand what that data means. For cyber-security, APOC stakeholders must understand whether or not particular logs or dashboard indications suggest that an attack is occurring.
- **Prediction** of future behaviour: In complex systems, predictions may only be possible in the short term because this behaviour will itself be influenced by a host of other internal and external factors. Prediction in the Endsley model enables strategy not just reaction. For CyberSA, prediction may refer to the users ability to anticipate the impact of an attack or the effectiveness of potential counter measures.

It is important to understand the interactions between these levels of situational awareness and expertise. A novice may perceive everything; but lack the experience to understand what they see, hence they will fail at comprehension and prediction.

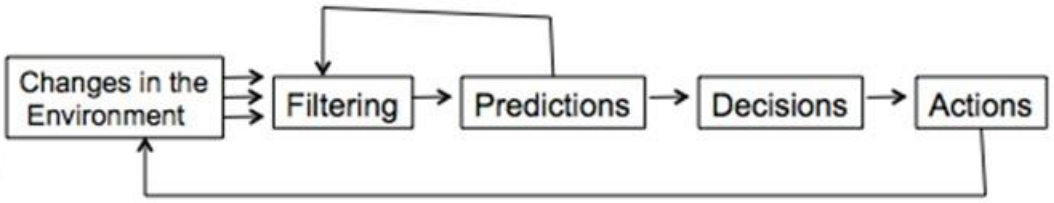


Figure 22: Modelling Cyber-Situation Awareness and CDM

Figure 22 provides a high-level overview of decision making within the Endsley model of Situation Awareness. Changes in the environment – such as one of the attacks scenarios from previous sections of this final report – can be perceived by APOC stakeholders, for instance through changes in a dashboard. Because people cannot monitor every variable or log that might be influenced by these changes, they adopt monitoring strategies to optimise finite perceptual resources. This introduces a form of filtering that is influenced by their predictions about possible future events. For example, if a system never suffers an attack and there is insufficient training in responding to cyber-attacks then users are unlikely to monitor the information presented by a cyber-dashboard. The filtering will direct their attention to more frequently used systems and they will exhibit poor levels of situational awareness when an attack does occur. Any subsequent decisions rely on the users' ability to detect changes in their environment and then make accurate predictions about the consequences both of those changes and their interaction with the system.

Figure 23 provides an overview of the FAA's application of Endsley's model to understand contributory factors in ATM related accidents. The values show the percentage of incidents where particular levels of poor situational awareness were identified as a potential cause.

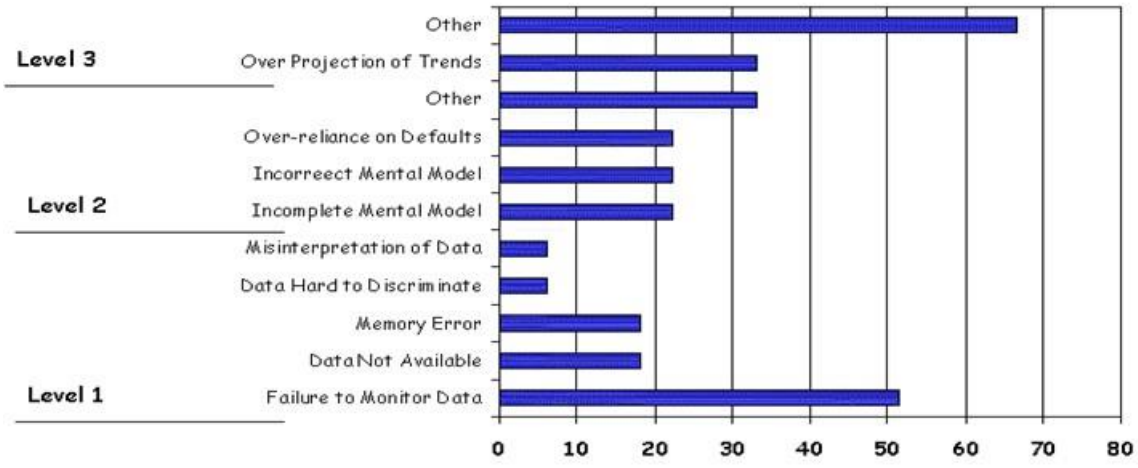


Figure 23: Situation Awareness as a Contributory Factor in ATM Related Accidents

Previous sections have proposed cyber-maturity metrics that can be applied to assess the readiness of APOC stakeholders to respond to a growing range of potential threats. In contrast, this section proposes Cyber-Situation Awareness metrics that can be applied to individuals and groups rather than to particular companies. The SESAR programme has already made extensive use of two existing metrics for situational awareness. Situation Awareness Rating Technique (SART)[11] and Situation Awareness Global Assessment Technique (SAGAT)[12] both have detailed entries within the SESAR Human Performance Repository (see Figure 24).

Figure 24: SART and SAGAT entries in the Human Performance Repository

SART is a simple subjective rating technique that is used after interacting with a system. Endsley argues that subjective ratings often provide the best measure of how an individual feels when interacting with an application. From the point of view of this project, SART assessments might be used after operating an APOC cyber-dashboard. Individuals are asked to rate their experience from 1=Low to 7=High along a number of dimensions that are intended to measure their degree of situational awareness. These include: Familiarity of the situation, focussing of attention, information quantity, information quality, instability of the situation, concentration of attention, complexity of the situation, variability of the situation, arousal, and spare mental capacity. The ratings are then combined in order to

[11] Situational Awareness Rating Technique, for further information please see: http://www.skybrary.aero/index.php/Situation_Awareness_Rating_Technique_(SART)

[12] Situation Awareness Global Assessment Technique, for further information please see: http://www.skybrary.aero/index.php/Situation_Awareness_Global_Assessment_Technique_(SAGAT)

calculate a measure of overall Situation Awareness. 3D SART simplifies these 10 dimensions into three areas:

1) Demands on attentional resources,

2) Supply of attentional resources, and

3) Understanding of the situation.

The main advantage of SART as the basis for a cyberSA KPI is that it is cheap and simple to administer. However, self-assessments can be very misleading. Individuals and teams might express high confidence in their situational awareness and yet totally overlook a potential threat. In other words, people do not know what they do not know and this would not be accounted for under a SART assessment. A further problem is that SART lacks explanatory power – we cannot easily use it to identify those attributes of a cyber-dashboard that experts find most useful in monitoring for potential threats.

The SAGAT provides alternate means of measuring CyberSA within the SESAR program. SAGAT was developed by Endsley from information processing theory; it assumes that SA is influenced by an individuals internal mental model of a situation/system. The more accurate and complete the model then the more accurate will be the users predictions about future operation. In contrast to SART, SAGAT does not rely on post hoc subjective assessments. Instead, the user interacts with a system which is then paused at randomly selected times. They must then answer a series of questions about their perception of the situation through queries on specific data. In ATM applications, ATCOs are typically asked about the position and routing of aircraft in their sector. In an APOC, they might be asked about recent alerts summarised in a cyber-dashboard based on the visualisations shown in the previous section. These direct interventions limit the problems that can arise when individuals rationalise their experiences after having used a system. By selecting random intervals, users cannot mentally prepare for the queries by attending to more information or memorising variables. However, these temporary halts represent the main disadvantage of this technique. The pauses can be difficult to implement in a live system and they can also interrupt/disturb the users interaction with an application.

Both SART and SAGAT can be used to measure the utility of proposed cyber-dashboards. SAGAT in particular, can be adapted to meet the requirements for a cyber-KPI, within the KPI requirements posed by EUROCONTROL and by regulations such as EC 691/2010; for instance by posing questions of stakeholders about their understanding of the existing threat level based on intelligence provided through both the information sharing systems and the dashboards that have been presented in previous sections of this report. The following sections provide sample questions that might be used in this way.

6.6 Collaborative decision-making

SART and SAGAT were both intended as metrics for assessing individual situational awareness; hence they complement the SESAR organisational maturity metrics of earlier sections. However, the main benefits justifying the implementation of APOCs are focussed on supporting Cooperative Decision Making. It is possible to modify these existing metrics to take into account a team-based perspective on Situation Awareness. For example, the SART and SAGAT assessment tools can be simultaneously administered across the APOC stakeholders with the expectation that different team members will exhibit different levels of awareness for any particular cyber-incident. Paul and Whitely have proposed a number of questions that might be used as probes within the SAGAT approach to assess Cyber-Situation Awareness (Paul & Whitley, 2013). These are summarised in Figure 25.

1. Are there more or less bad guys attacking my network than normal?
2. Can I see the attack I know is happening?
3. Does the attack have a negative effect on other business operations?
4. Does this attack matter?
5. Have I seen an attack like this before?
6. How did the bad guys get into my network?
7. How is my network being attacked?
8. How is my network different from last week?
9. How serious is the attack?
10. How successful was the attack?
11. Is anything different happening on my network than normal?
12. Is anything interesting happening on my network?
13. Is it a good day on the network?
14. Is my network configured correctly?
15. Is my network healthy?
16. Is something bad happening on the network?
17. Is something happening on the network?
18. Is the event on my network good, bad, or just different?
19. Is there more or less traffic on my network than normal?
20. Is this a new attack I have not seen before?
21. What are the bad guys doing on my network?
22. What did the bad guys do?
23. What did the bad guys take?
24. What do I do about the attack?
25. What do I not see happening on my network?
26. What does my network look like to the bad guys?
27. What does my network look like?
28. What does the attack look like?
29. What does the event on my network mean?
30. What happened on the network last night?
31. What is different on my network from last week?
32. What is happening on my network now?
33. What is happening with my network?
34. What is normal for my network?
35. What is not normal for my network?
36. What is the most important event happening on my network?
37. What is the status of my network?
38. What malware have been detected on my network?
39. What systems are up or down on my network?
40. Where are the bad guys attacking from?
41. Where on my network am I being attacked?
42. Who is attacking my network?
43. Why is my network being attacked?
44. Why are computers on my network not available?

Figure 25: Situation Awareness Probes for APOC CDM

We would propose that a subset of these questions is used during the operation of any proposed cyber-dashboard across stakeholders within the APOC using simulated scenarios. This would provide an indication as to whether or not key individuals were able to use their systems to perceive and understand the symptoms of various attack scenarios presented in this report. In particular, we would compare their responses to determine whether dashboards combined with other forms of cyber-incident information exchange supported a coordinated response to emerging threats.

6.7 Summary

This section has focussed on techniques that can be used to assess the ability of an APOC to detect and mitigate a growing range of cyber-threats. The opening pages built on previous work within the SESAR programme. We presented high-level questions that can be used to assess the cyber-maturity of stakeholder organisations. Key topics included the introduction of cyber-security requirements within procurement documents, the provision of training on the importance of cyber-security and also the degree of planning on how to recover when an incident does occur. These cyber-maturity metrics provide a valuable snapshot for participants within an APOC. However, they cannot support the more detailed feedback loops that are envisaged. For this, there is a need to identify more detailed and dynamic KPIs that help to measure CyberSA at an individual and group level. The use of existing performance based KPIs cannot be used to measure changes in the threat level – for instance caused by the publication of zero day exploits in APOC sub-systems or changes in the socio-political environment when environmental protest group advocates direct action to resist airport expansion. Hence we need metrics that reflect our ability to detect and resist future incidents rather than a retrospective measure of the previous impact of cyber-attacks on our infrastructures. It is for this reason that we have

advocated the combination of organisational cyber-maturity assessments, together with more detailed metrics for the CyberSA of key APOC stakeholders – at the individual and team level. For these metrics, we have again built on previous work with the SESAR programme – focussing on the role of SART and SAGAT within the human performance area.

Both SART and SAGAT can be used to measure the utility of proposed cyber-dashboards. SAGAT in particular, can be adapted to meet the requirements for a cyber-KPI, within the requirements posed by EUROCONTROL and by regulations such as EC 691/2010; for instance by posing questions of stakeholders about their understanding of the existing threat level based on intelligence provided through both the information sharing systems and the dashboards that have been presented in previous sections of this report. SART is a subjective technique that is susceptible to post hoc rationalisation. In contrast, we would advocate the random assessment tools within the SAGAT method.

We have identified questions that can be posed during interaction with potential Cyber-dashboards, informed by the output from cyber-incident reporting and information exchange tools, to assess APOC participants' ability to detect and then respond to potential threats.

7 Conclusions and recommendations

This section summarises the results of this study, and makes recommendations, including to policy-makers and programme managers, the SESAR 2020 partners undertaking subsequent work, and airports themselves.

7.1 Conclusions

The Airport Operations Centre (APOC) is critically important. Even with a downtime of two hours of the APOC, flights will be delayed or even cancelled and the impact of such disruptions can, of course, be huge. At the heart of APOC is Collaborative Decision Making (CDM) and the Airport Operations Plan (AOP) and so anything that affects CDM and AOP is in scope of the guidance and recommendations in this report. The APOC is easily disruptable if availability and integrity of data and/or systems can be compromised. Particular cyber-problems for the APOC include:

- Given current legacy systems and services, airports may well build APOC and CDM on top of untrustworthy, unauthenticated data sources and insecure networks. With such a foundation, establishing trust in the APOC will be impossible. In the short term, it is therefore important to explain how the vulnerabilities associated with these legacy systems will be mitigated. In the medium term, it is necessary to create a road map explaining how insecure legacy systems will be replaced.
- System integration increasingly results in extended supply chains where each stakeholder relies on services provided by their partners, but which might be delivered by third party companies. An extended supply chain means more people having access to core infrastructures, which poses security risks. In essence, whilst services can be outsourced, cyber-risk cannot be.
- Even if systems within airport control can be adequately secured, assurance needs to extend to all sources of data. The end-points of connections need to be trusted; if these are untrustworthy problems will occur. The most dangerous scenario identified is where a communication service is used to inject false data affecting the whole of the aviation community. Even though it is possible to 'unplug' the affected service, this will still be a solution which will degrade stakeholder capability to exchange data with the airport APOC and other APOCs across Europe (since the Network Operations Plan (NOP) will not be updated from the airport AOP).

If today's problems remain unaddressed we will face a 'dystopian future' with high cyber-risk and failure to exploit the modernisation and benefits that SESAR promises. This will adversely impact European aviation as a whole. The worst case is that with increasingly skilled attackers, airports are frequently disrupted with the consequent impact on the travelling public.

The opportunity exists to fix these problems and achieve a more utopian future in which technology and data drives performance improvements for all. As is more generally the case with SESAR R&D, there is an opportunity to address cyber-security in a systematic and joined-up manner that enables (but not guarantees) the security functionality, assurance and operating environment. Most directly this means building-in the right security requirements from the very start of SESAR solutions. Furthermore work and coordination on common and harmonised security architectures will improve industrialisation and deployment.

Key technical controls required for an APOC include intrusion prevention/detection, data diodes (to protect read-only data, such as relating to passengers), logging and audit capabilities, device and service authentication and data validation tools (which will also support general robustness for airports too). Zoning and network separation will be limited, due to the APOC's 'nerve centre' position and single logical platform/data repository, but should be applied where possible.

The combination of organisational cyber-maturity assessments, together with more detailed metrics for the CyberSA of key APOC stakeholders – at the individual and team level – is one promising approach. Detailed and dynamic Key Performance Indicators (KPIs) are needed to measure CyberSA at an individual and group level.

Ultimately, trust is enabled by security assurance, which comes from the actions of developers, implementers and assessors of security functionality, and in particular through structured design processes, documentation and testing. For APOCs, a high level of assurance is required due to high business criticality - and so process, system and environment aspects need to be addressed. Practical-level characteristics that engender trust are technical competence, openness and transparency to external assessment and criticism, self-awareness and honesty.

Current and envisaged legal and regulatory requirements do not tightly define security assurance methods nor a level of assurance for APOCs. However, impending changes to ECAC Doc 30 should introduce a set of auditable requirements (including an audit scheme) for cyber-security that should eventually provide a strong mandate for airports, including APOCs, to adequately address the majority of cyber-risks. Addressing nation state threats (i.e. very capable and persistent attackers) would require additional support from national authorities. The Network and Information Security Directive (EU, 2016) makes this more likely.

A key question is the extent to which pan-European harmonisation can occur. Specific assurance requirements will be subject to negotiation and agreement with regulators (and other national authorities), partners/suppliers, customers, etc, and therefore vary across APOCs – but harmonisation would be beneficial to encourage mutual trust and to facilitate efficiency. Common rules are needed, but must be implemented in ways that are dictated by national circumstances. Ultimately, full harmonisation across Europe is very unlikely due to national sovereignty concerns and differences in threat levels.

7.2 Guidance for SESAR 2020 PJ04 Total Airport Management

Under SESAR 2020 PJ04 will develop the TAM approach further through a closer integration of both landside and airside performance monitoring, as well as the development and validation of monitoring and decision support tools for collaborative management between stakeholders. This work already recognises that APOC and TAM are based on system integration and large exchange of data, both locally and with the Network via SWIM, and therefore the importance of considering both how SESAR developments could be impacted by potential cyber-threats and the resulting required mitigations.

Guidance for PJ04 Security Risk Assessment

All SESAR projects must undertake a Security Risk Assessment using the SESAR Security Risk Assessment Methodology (SecRAM), as outlined in the SESAR 2020 Project Handbook, and as detailed in lower level guidance. This study sees this activity as a crucial early step in PJ04. Specific advice for that assessment, from the experience of this study is:

- Ensure technical and operational staff involvement in the risk assessment – good judgement of both the likelihood of compromise and impact of compromise is only available if technical and operational staff are consulted and review the assessment.
- Define the 'Primary Assets' in the assessment as the APOC services (as defined themselves in the APOC OSED) – this is in line with emerging SecRAM and EATMA good practice.
- Validate this study's initial assessment of APOC criticality, as set out in sub-section 2.2.
- Coordinate/normalise the risk assessments between the APOC and NMOC (AOP-NOP) so that the parameters are coherent – for example, the values for severity of impact, and likelihood of threat, should be consistent.

Guidance for PJ04 proposed cyber-security activities

This study has also reviewed PJ04's original proposal for addressing cyber-security. As part of producing the OSED/SPR/INTEROP, a security assessment is expected on the tool/prototypes and to ensure security compliance when concepts will be fully mature for deployment in operational environments.

We believe that the PJ04 proposal addresses many of the right areas of cyber-security. However, there are some gaps and therefore we recommend that PJ04:

1) Identify early on what cyber-standards are going to be used, as references in the proposal (to Commission strategy and decisions) are too high-level;
2) Identify cyber-logging and auditing requirements to support post-event forensics and analysis (thereby building on the mention of Security Information and Event Management (SIEM));
3) Aim to publish the results of the 'ethical hacking penetration test activity', and if this is not possible due to national legislative boundaries, then ensure these lessons are documented as a practical case study into the difficulties of information sharing in cyber-security;

4) Undertake field trial of network security monitoring tool (as a further practical activity) and similarly publish a summary;

5) Consider blended attacks (see scenario in sub-section 3.4.4) as the current proposal lacks an integrated approach to attacks on digital and physical assets;

6) Explore interaction between cyber and safety critical aspects, especially where safety requirements undermine security;

7) Link security activities to the business case aspects of the solution, to ensure that cost control and cost-effectiveness aspects of security are addressed;

8) Ensure any civil-military cyber-aspects of, and requirements for, APOC/TAM are addressed;

9) Build an initial APOC Security Case that contains the results of all security analysis and starts to make the case that the concept can be industrialised and deployed in a securable manner;

10) Create a template recovery plan showing airport stakeholders the steps involved in detecting, containing and recovering from a breach of information security – including the rebuilding of trust across the APOC and with external agencies.

Most importantly, the outputs from PJ04 cyber-security activity should be packaged in a way that is understood and usable by the rest of the project and programme. The keystone for this is to publish a simplified and sanitised version of the SecRAM results, as a case study to support real-world APOC risk assessments.

7.3 Future research priorities

Finally, looking beyond the already planned work in SESAR 2020, this study identifies several areas for future research:

#	Research topic and rationale
1	Understand in detail how A-CDM, APOC and TAM actually support cyber-security (i.e. the positives of data validation and shared situational awareness)
2	Devise better cyber-security metrics for individual components (overall health being a function of constituents, but how are networks of ICS and SCADA best measured?)
3	Explore how to use the SESAR EATMA to identify cyber-security priorities, given gate-to-gate scenarios
4	APOC security architecture - to identify common architectures that exploit opportunities for segregation, multiple levels of assurance, reuse of common components, etc.
5	A sustained cyber-analysis of an airport including both the supply chain and the high-level down to SCADA infrastructures

Table 16: Future research priorities

7.4 Recommendations

Recommendations for the SJU and SESAR work programme

Immediate action	**REC01**	Ensure coordinated approach to cyber-security between Network-level (i.e. Network Monitoring Operations Centre (NMOC) / Network Operations Plan (NOP)) and Airport-level APOCs
Mid-term activity (one year +)	**REC02**	Organise a SESAR programme cyber-conference across all solution projects to share progress and assemble a gate-to-gate approach to cyber-security within SESAR
	REC03	Support project-level Security Risk Assessments and Security Cases with templates and examples

Recommendations for the EC

Immediate action	**REC04**	Provide guidance on establishing a clear and consistent interface between European institutions and state agencies for airport cyber-security
Mid-term activity (one year +)	**REC05**	Work with ECAC (and other relevant bodies) to assess the feasibility of cyber-security accreditation standards for airports
	REC06	Develop guidance and case studies on supply chain cyber-security risk
	REC07	Organise annual confidential workshop for airports to share cyber-security progress, guidance and challenges
	REC08	Ensure Acceptable Means of Compliance (MoC) exist for all cyber-security regulatory requirements to help reduce costs for all member states and encourage consistency
	REC09	Complete a feasibility study for a voluntary, standards-based cyber-testing scheme (akin to CBEST)

Recommendations for airports

Immediate action	**REC10**	Undertake a cyber-security maturity assessment
	REC11	Review readiness against cyber-attack scenarios, especially the vulnerabilities list
Mid-term activity (one year +)	**REC12**	Undertake / rehearse cyber-exercise without and with stakeholders
	REC13	Adopt an appropriate range of cyber-standards (ISO 27001 or EN 16495 for management system, ECAC Doc 30, ED-201 for multi-party agreements, etc.)
	REC14	Use CPNI guidance and good practice for securing ICS and SCADA (http://cpni.gov.uk/SCADA)
	REC15	Include cyber-security requirements in the procurement of A-CDM, APOC and TAM solutions

Recommendations for airport stakeholders (Airlines, Ground handlers, ANSP)

Immediate action	**REC16**	Review readiness against cyber-attack scenarios, especially the vulnerabilities list
Mid-term activity (one year +)	**REC17**	Undertake / rehearse cyber-exercise with the supply chain and with the airport

Recommendations for the Network Manager

Note that this study did not assess the security architecture or configuration of the Network Manager's external flows, but after determining the ability of a compromised AOP to 'pollute' the NOP, and after reviewing SESAR work on securing the future NOP, several general recommendations are made.

Immediate action	**REC18**	Review connection specifications for all NOP input feeds, against confidentiality, integrity, availability and non-repudiation requirements
Mid-term activity (one year +)	**REC19**	Ensure NOP input feeds are authenticated and have required data validation and message guarantees
	REC20	Encourage encryption and authentication by default for all strategic data exchange across the 'Network'

Recommendations for EUROCONTROL Airport Research

Immediate action	**REC21**	Encourage future research priorities to be adopted and recommendations to PJ04
Mid-term activity (one year +)	**REC22**	Publish practical examples and case studies of how good cyber-security practices have been applied at airports

A Abbreviations

ADP	Aéroports de Paris
AODB	Airport Operations Database
AOP	Airport Operations Plan
APOC	Airport Operations Centre
ASAT	Actual Start Up Approval Time
A-DCB	Airport Demand Capacity Balancing
ANSSI	L'Agence Nationale de la Sécurité des Systèmes d'Information
A-SMGCS	Advanced Surface Movement Guidance and Control System
ATM	Air Traffic Management
BIA	Business Impact Analysis
CDM	Collaborative Decision Making
CERT	Computer Emergency Readiness Team
CISO	Chief Information Security Officer
CNS	Communication, Navigation and Surveillance
CyberSA	Cyber-Situational Awareness
DCS	Departure Control Systems
DDoS attack	Distributed Denial of Service attack
EAL	Evaluation Assurance Level
EASA	European Aviation Safety Agency
ENISA	European Union Agency for Network and Information Security
GNSS	Global Navigation Satellite System
IATA	International Air Transport Association
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IED	In-line Explosive Detection system

IoC	Indicators of Compromise
IP	Intellectual Property
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISP	Internet Service Provider
MET	Meteorological Services
NIS	Network and Information Systems Directive
NMOC	Network Manager Operations Centre
NOC	Network Operations Centre
NOP	Network Operations Plan
OCC	Operations Control
OSED	Operational Services and Environment Description
PIDS	Perimeter Intrusion Detection Systems
PLC	Programmable Logic Controller
PNR	Passenger Name Record
RMADS	Risk Management and Accreditation Documentation Set
SAB	Security Accreditation Board
SART	Situational Awareness Rating Technique
SAGAT	Situation Awareness Global Assessment Technique
SCADA	Supervisory Control And Data Acquisition
SecMS	Security Management System
SecRA	SESAR ATM Security Risk Assessment
SecRAM	SESAR ATM Security Risk Assessment Methodology
SES	Single European Sky
SESAR	Single European Sky ATM Research

SIEM	Security Information and Event Management
SOC	Security Operations Centre
SWIM	System Wide Information Management
TAM	Total Airport Management
TOBT	Target Off Block Time
TSAT	Target Start Up Approval Time
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network

B References

Anon., 2016. *S,* s.l.: E.

ANSSI, 2002. [Online]
Available at: http://www.ssi.gouv.fr/en/certification/common-criteria-certification/

CEN, 2014. *European Committee for Standardization, EN 16495, Air Traffic Management - Information Security For Organisations Supporting Civil Aviation Operations.* s.l.:s.n.

Chang, S., Ericson, D. & Pearce, L., 2003. Airport Closures in Natural and Human-Induced Disasters: Business Vulnerability and Planning. *Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada.*

EC, 2004. *Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealin.* s.l.:s.n.

EC, 2008. *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security.* s.l.:s.n.

ECAC, 2009. *European Civil Aviation Conference (ECAC) Doc 30,* s.l.: s.n.

ECOSSIAN, 2016. *European COntrol System Security Incident Analysis Network.* [Online]
Available at: http://ecossian.eu

Endsley, M., 1988. Design and Evaluation for Situation Awareness Enhancement.. *Proceedings of the Human Factors Society 32nd Annual Meeting. Human Factors Society, Santa Monica, CA,* pp. 97-101.

Endsley, M., 1995. Measurement of situational awareness in dynamic systems.. *Human Factors: The Journal of the Human Factors and Ergonomics Society,* pp. 37(1), 65-84.

ENISA, 2011. *Technical Guideline on Reporting Incidents: Article13a Implementation, European Network and Information Security Agency, Version 1.0.* [Online]
Available at: http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporti

ENISA, 2016 (est.). *Securing Smart Airports,* s.l.: European Union Agency for Network and Information Security.

EU, 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* s.l.:s.n.

EU, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* s.l.:s.n.

EUROCAE, 2015. *ED-201, Aeronautical Information System Security (AISS) Framework Guidance,* s.l.: s.n.

FCC, 2013. *Network Outage Reporting System.* [Online]
Available at: http://transition.fcc.gov/pshs/outage/nors_manual.pdf

FCC, 2016. *Public Safety & Homeland Security Bureau, CSRIC Best Practices..* [Online]
Available at: https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm

GAMMA, 2016. *Global ATM Security Management Project.* [Online]
Available at: http://www.gamma-project.eu

Guenther, Y., 2013. *TAM – Total Airport Management an evolutionary approach to managing an airport.* [Online]
Available at: http://www.meta-cdm.org/workshops/workshop1/Guenther%20TAM%20presentation.pdf

Helios/Thales, 2015. *SESAR cyber-security Maturity Assessment: The third deliverable for the SESAR Strategy and Management Framework Study for Information cyber-security,* s.l.: s.n.

ICAO, 2014. *Security,* s.l.: s.n.

ICAO, 2015. *Aviation Security Manual (Doc 8973 – Restricted),* s.l.: s.n.

ISO/IEC, 2008. *ISO/IEC 21827:2008, Information technology -- Security techniques -- Systems Security Engineering.* s.l.:s.n.

ISO/IEC, 2011. ISO/IEC 15026:2011, Systems and Software Engineering.

ISO/IEC, 2012. ISO/IEC TR 15443:2012, Information technology -- Security techniques -- Security assurance framework.

ISO/IEC, 2013a. *ISO 27001:2013 Information and Data Security.* s.l.:s.n.

ISO/IEC, 2013b. ISO 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls.

ISO, 2015. *ISO 9000: 2015, Quality Management.* s.l.:s.n.

Johnson, C., 2014. Supporting the Exchange of Lessons Learned from cyber-security Incidents in Safety-Critical Systems.. In: *Proceedings of the 22nd International Systems Safety Society.* Louisville, USA: s.n.

Johnson, C., 2015. Contrasting Approaches to Incident Reporting in the Development of Security and Safety-Critical Software. In: *SAFECOMP.* Heidelberg, Germany: Springer Verlag, pp. 400-409.

Johnson, C., 2015. Cyber Security and the Future of Air Traffic Management: Identifying the Challenges for NextGen and SESAR.. In: *10th IET System Safety and Cyber Security Conference .* London: The IET, Savoy Place.

Kolev, D., Koelle, R., Casar Rodriguez, R. & Montefusco, P., 2013. *Security Situation Management – Developing A Concept of Operations And Threat Prediction Capability.* [Online]
Available at: http://www.gamma-project.eu/wp-content/uploads/2013/11/Paper_Security_situation_management.pdf

Kosanke, L. & Schultz, M., 2015. *Key Performance Indicators for Performance-Based Airport Management from the perspective of airport operations, Air Transport and Operations Symposium.* [Online]
Available at:
http://www.lr.tudelft.nl/fileadmin/Faculteit/LR/Organisatie/Afdelingen_en_Leerstoelen/Afdeling_C_O/Aerospace_Management_and_Operations/ATOS/Papers/2015/CATO2015_4_2_1.pdf

Langhe, K. d. et al., 2013. Economic Effects and Costs Of A Temporary Shutdown Of An Airport – Review And Case Study. *13th World Conference on Transport Research.*

Murphy, R., Sukkarieh, M., Haass, J. & Hriljac, P., 2015. *ACRP Report 140: Guidebook on Best Practices for Airport Cyber-security,* s.l.: Airport Cooperative Research Program; Transportation Research Board; National Academies of Sciences, Engineering, and Medicine .

NIST, 2011. *NIST 800-39 Managing Information Security Risk,* s.l.: U.S. Department of Commerce.

NIST, 2013. *NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations,* s.l.: U.S. Department of Commerce.

Paul, C. & Whitley, K., 2013. A taxonomy of cyber awareness questions for the user-centered design of cyber situational awareness. *In International Conference on Human Aspects of Information Security, Privacy, and Trust,* pp. 145-154.

Reader, T., Noort, M., Shorrock, S. & Kirwan, B., 2015. Safety sans Frontières: An International Safety Culture Model. *Risk Analysis,* p. 35(5).

SESAR, 2015a. 06.05.04 OFA 05.01.01 Consolidated OSED (D16, Edition 3).

SESAR, 2015b. *SESAR Strategy and Management Framework Study for Information cyber-security.* [Online]
Available at:
http://www.sesarju.eu/sites/default/files/documents/news/SESAR_Strategy_and_Management_Framework_Study_for_Information_cybesecurity_FINAL.pdf

SESAR, 2015c. 15.02.04 Future Communications Infrastructure SecRAR.

Snow, B., 2005. We Need Assurance!. *2005 Annual Computer Security Applications Conference.*

Tadda, G., 2008. Measuring performance of Cyber situational awareness systems. *Information Fusion, 2008 11th International Conference on. IEEE.*

This study, led by EUROCONTROL in the context of SESAR Project 06.03.01, explores how cyber-security should be addressed in the Airport Operations Centre concept.