SESAR
JOINT UNDERTAKING

Addressing airport cyber-security

Executive summary report

founding members

EUROPEAN UNION

EUROCONTROL

Executive summary

The APOC is critically important…	If the availability and/or integrity of information systems is compromised then this 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. 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-situation 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 – see Annex B for how to do this. Cyber-exercises can be run to test the practical readiness of existing arrangements and learn lessons.

Contents

1 Airport cyber-security in the Single European Sky

Airports are increasingly data driven and rely upon accurate and timely information for efficient operations. Seamless exchange of information across integrated systems supports real-time decision-making for the benefit of all aviation stakeholders. Increased connectivity has enabled resources to be used more efficiently, irregular operations to be overcome quicker and disruption has often been avoided altogether. However, increased reliance on data and increased integration also increases the risk of malicious cyberattack that disrupts airport operations.

The SESAR airport operations centre (APOC) is the heart of the airport information network and 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. As a data integrator it creates a more complete picture of operations at the airport, and therefore it is essential that both the input and output data are reliable and resistant to manipulation. It's also vital that different partners are aware of cyber-threats and able to mitigate them together.

The costs of a cyber-security breach can be high:

€1m/hour cost to economy of disruption at a major European airport[1]

€2m+ direct cost of a serious cyber-compromise[5]

€250m in lost European airport revenue alone for a six-day closure[2]

It is therefore important to take cyber-security seriously, especially as:

170 days is the average time to detect a malicious or criminal attack[3]

90% of large organisations reported suffering a security breach[4]

75% of board directors are not involved in the review of cyber-security risks[5].

A study undertaken within the context of SESAR Project 06.03.01[6] and led by SESAR member, Eurocontrol, in collaboration with Helios, Groupe ADP and Professor Chris Johnson from the University of Glasgow has explored how cyber-security should be addressed in the APOC. This report summarises key findings as well as providing:

- Airport cyber-attack scenarios (eg blackmail against a DDoS attack) – see Annex A
- A cyber-security maturity checklist – see Annex B
- Recommended guidance and standards – see Annex C

[1] Research for ACI Europe from 2015
[2] ACI Europe estimate for lost revenue due to the eruption of Eyjafjallajokull in Iceland in April 2010
[3] HP / Ponemon Institute research 2014
[4] UK BIS 2015 Information Security Breaches Survey covering companies
[5] PwC 2015 Global State of Information Security Survey
[6] 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".

2 Potential cyber-weaknesses and future trends

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. Unsurprisingly the APOC is therefore a potential target for cyber-attackers and may be vulnerable to different types of cyber-attacks.

Airports utopian and dystopian shared futures

The fact that an increasing number of systems will be interconnected is beyond doubt. For instance, each Airport Operation Plan (AOP) will be connected to the European Network Operation Plan (NOP).

Today many existing systems such those monitoring and controlling industrial processes are isolated (i.e. still standalone/air gapped, a good example are SCADA[7] systems). In order to optimise future airport performance, this data must be integrated into real-time dashboards: Standalone systems will not exist in an interconnected future. It is also obvious that airports will rely more on integrated IT systems than today.

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 polices of foreign countries heighten the probability that state-backed attackers will target European airports and the ATM network.

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

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. 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 are used. Audit and penetration tests are performed regularly.

In an airport 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.

[7] Supervisory Control And Data Acquisition (SCADA) devices are a type of Industrial Control System (ICS). SCADA devices are used for remote monitoring and control of industrial processes.

3 Human aspects: trust between stakeholders

The APOC will be the 'nerve centre' for decision-making. The Airport Operator needs to be willing to rely on actions of itself, and its partners and suppliers and be confident 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 operators as well)
- APOC functions behave as intended to deliver its intended benefits

Such trust is enabled by security assurance, namely the planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given security requirements. Assurance 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 as APOC has high business criticality - and so process, system and environment aspects need to be addressed.

Top assurance principles identified by the study:

Trust comes from assurance, and assurance should be:

1) **Proportionate to risk**; the higher the risk the more assurance is needed

2) **Built progressively** through the lifecycle; secure by design is best

3) **Maintained**; assurance degrades with time, and with new systems and data; what is secure one day can be totally insecure by the following morning

4) **Enforced by audit**; external scrutiny is essential

Whilst current and envisaged legal and regulatory requirements do not tightly define assurance methods nor a level of assurance for APOCs, changes to ECAC Doc 30[8] should introduce a set of auditable requirements for cyber-security that should eventually provide a strong mandate for 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.

Whilst full harmonisation across Europe is desirable, it is unlikely due to national sovereignty concerns and differences in threat levels. Common rules are needed, but 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.

[8] European Civil Aviation Conference (ECAC) Doc 30 (formally the 'ECAC policy statement in the field of civil aviation facilitation') contains requirements relating to security within the airport. These are currently being revised to better address cyber-security.

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. More assurance can be taken, if assessed by a well-resourced national security agency, with both offensive and defensive capabilities, 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. 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. Knowing that certain controls are still under development or are not as strong as they need to be gives 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.

Where legal and regulatory needs fall short of providing sufficient assurance, a voluntary, standards-based approach would be helpful. The UK banking system's CBEST[9] scheme is a useful model, though sharing of cyber-threat and incident reporting may be difficult to achieve in a pan-European context.

A multi-lateral External Agreement (an auditable set of mutual agreements, as per EUROCAE Standard ED-201[10]) 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 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.[11] Ultimately this is what is required to present to, and convince others, to get the trust required.

[9] CBEST is a cyber-vulnerability testing framework in the UK banking sector.
See http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
[10] EUROCAE ED-201 Aeronautical Information System Security (AISS) Framework Guidance identifies security topics which have to be addressed by civil aviation stakeholders – thereby setting out the foundations for other EUROCAE standards on air, air-ground and ground security.
[11] See ISO 15443, for example, for more on assurance cases.

4 Information sharing and situational awareness

It is crucial that information is shared so that high cyber-security levels and situational awareness can be maintained. Sharing of vulnerabilities, threats and good practices, and using dashboards for cyber-situational awareness, must be tailored to support the exchange of information between APOC stakeholders. It is critical to present cyber-security information in a way to retain interest in periodic reports and ensure a fast and effective response when incidents are detected.

Information sharing between stakeholders

A low-cost infrastructure is needed to ensure the exchange of cyber-information between member states but working in close partnership with each nation's aviation regulator.

In the existing European cyber-incident reporting system, the telecommunications regulator in each member state coordinates the provision of data and reports relating through a web interface. ENISA then distribute the reports to other member states. This avoids a situation where a European agency might be seen to by-pass national regulatory provision.

A number of research projects have developed architectures for cyber-incident reporting across Europe, including FP7 Security Project ECOSSIAN – (European COntrol System Security Incident Analysis Network, (ECOSSIAN, 2016)) and GAMMA (Global ATM Security Management Project, (GAMMA, 2016)).

Common cyber-situational awareness

Cyber-situational awareness ensures:

- Distributed networks of stakeholders within the APOC can monitor and respond to a changing landscape of threats;
- Cooperation and agreement in decision making across the APOC even though multiple stakeholders will be present;
- Confidence is maintained within the APOC yet external support is requested when appropriate.

APOC KPI's relating to slot adherence, punctuality, throughput, efficiency, connectivity and environmental impact provide little information about the likelihood of future security incidents.

New KPIs are needed to address cyber-situational awareness for both the organization as and the individual, as individuals with different experience will often have different perceptions of the risks summarised in cyber-dashboards.

Cyber-resilience is supported by a combination of organisational cyber-maturity assessments and detailed metrics - at the individual and team level - for the cyber-situation awareness of key APOC stakeholders. Example metrics which can be used to assess awareness at individual level are SART[12] and SAGAT[13]. These could form the basis of future KPIs.

[12] Situational Awareness Rating Technique. See: http://www.skybrary.aero/index.php/Situation_Awareness_Rating_Technique_(SART)
[13] Situation Awareness Global Assessment Technique. See: http://www.skybrary.aero/index.php/Situation_Awareness_Global_Assessment_Technique_(SAGAT)

We have made tools available for assessing organisational cyber-maturity, through previous work in SESAR. These can be found in Annex B of this summary.

Dashboard design for APOC

Security dashboards can show the distribution of recent security related events (i.e. last day, week, month etc.), the threat level in terms of the number of identified threats over time and systems targeted, the number of security events being recorded per system, unresolved alarms and open tickets, and the specific system logs that drive the higher-level visualisation tools.

However, dashboards are closely integrated with Intrusion Detection Systems (IDS) and two key concerns affect the utility of APOC dashboards:

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

   White list IDS try to ensure that only approved software is running. The white list approach characterises normal behaviour and issues an alarm when anomalies are detected. It can be hard to characterise 'normal' behaviour in an evolving APOC where new stakeholders and services continue to be introduced. Such changes might otherwise trigger an alarm. Some of these concerns can be reduced by compiling a white list early in the APOC development and updating it each time new services are integrated into the software architecture.

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.

   Black lists IDS rely on signatures (file characteristics, process structures) to look for potential malware. We cannot, however, expect these to identify attacks which have not been identified previously.

There is a trade-off; reducing the number of false positives often implies an increased likelihood of missed positives.

Important points regarding information sharing and dashboard design

- We recommend that any security concerns are first reported to the national regulator before any European agencies.
- The key to measuring cyber-situational awareness is the use of self-assessment at the individual and team level.
- APOC dashboards should exploit a hybrid approach of white list and black list technologies for detecting illicit activity.
- The Network and Information Systems (NIS) Directive[14] will improve the exchange of malware signatures for black lists through the incident reporting/information exchange architectures.
- The discipline and cost of compiling and maintaining a white list is justified by the significant benefits it provides to long-term cyber-situation awareness by explicitly enumerating the software that is expected to be running inside the system.

[14] See: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

5 Recommendations

A detailed set of conclusions and recommendations can be found in the full study report.

Key recommendations for **airports**:

1	Undertake a cyber-security maturity assessment
2	Review readiness against cyber-attack scenarios, especially the vulnerabilities list
3	Undertake / rehearse cyber-exercise without and with stakeholders
4	Include cyber-security requirements in the procurement of A-CDM, APOC and TAM solutions

Key recommendations for **SJU and SESAR work programme**:

1	Ensure coordinated approach to cyber-security in NMOC/NOP and APOC SecRAM
2	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
3	Support project-level SecRAMs and Security Cases with templates and examples

Key recommendations for the **EC**:

1	Provide guidance on establishing a clear and consistent interface between European institutions and state agencies for airport cyber-security
2	Work with ECAC (and other relevant bodies) to assess the feasibility of cyber-security accreditation standards for airports
3	Develop guidance and case studies on supply chain cyber-security risk
4	Organise annual confidential workshop for airports to share cyber-security progress, guidance and challenges
5	Ensure Acceptable Means of Compliance (MoC) exist for all cyber-security regulatory requirements to help reduce costs for all member states and encourage consistency
6	Complete a feasibility study for a voluntary, standards-based cyber-testing scheme (akin to CBEST)

The full report also provides guidance to SESAR 2020 projects, including PJ04, among other on conducting security risk assessments and priority research areas.

A APOC cyber-attack scenarios and APOC weakness

We illustrate potential APOC vulnerabilities – and more generally airport vulnerabilities - 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. Further, the APOC could even help resolve such an incident by helping all relevant stakeholders focus on recovery.

A.1 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
- Organised crime, who are interested in obtaining financial reward or ransom in exchange of not provoking cancellations or flight disruptions
- State Cyber-Forces, who have large amounts 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).

A.2 Scenario 1: Distributed denial of service attack on the Airport's internet connection

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 IP addresses owned by the airport authority. These are not difficult to determine: they can be found by checking the main website 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. These services can be hired. 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?	Impacts on APOC, Airport and Network
More and more companies are being targeted by DDoS attacks since such attacks have become a way for cyber-criminals to obtain income. 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 determined to oppose airport operations/expansion.	Stakeholder representatives will be cut off from their headquarters since they use VPN networks and voice over IP technology via the airport's internet connection. Stakeholder representatives could still make decisions but these will be hard to communicate within their organisation or across the airport: The APOC will be isolated from airport operations. If the internet is used to exchange data with the NOP, the Network will no longer be updated. The airport will not have up-to-date weather forecasts which could be very critical in case of low visibility or snowy conditions. Dedicated networks could be disturbed as they may share some physical hardware resources that will be busy or become unavailable.

A.3 Scenario 2: Deep and slow infiltration to steal data

A group of highly motivated and skilled cyber-criminals wants to infiltrate an airport network 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 compromised 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 and 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?	Impacts on APOC, airport and network
This scenario is an extension of an attack carried out on TV5Monde 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.	Extracted data may be related to flights and contain critical information (delays, flight load factors, 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 provides for severe penalties of up to 5% of worldwide turnover if data related to EU residents are leaked. Leaked data could be used against APOC stakeholders, and hence help conduct further attacks on the aviation industry.The airport website could also be defaced to promote an ideology or to publicise compromising information. Finally, the hackers can remotely damage the IT infrastructure, which will result in long-term disruption to the APOC and the AOP and ultimately the airport. This would result in loss of confidence and major revenue loss for the airport operator and airlines.

A.4 Scenario 3: Major integrity loss

A highly motivated group wants to disrupt operations at the airport and, if possible, operations at other European airports. In order to do this, they send incorrect flight information to the targeted airport using a messaging service deployed around the world and 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 by knowing its address which could easily be found on a proprietary search engine by searching the target name and the messaging service name.

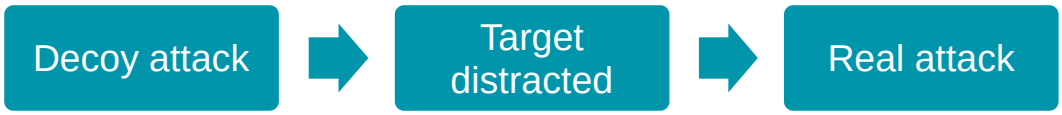
Flight information sent to an airport are formatted following the IATA message specifications. Attackers have to know how to write the false messages they intend to send: This could be easily done since all relevant information are illegally stored on several public servers around the globe. These documents 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?	Impacts on APOC, airport and network
A similar scenario happened to a major European airport when a software company based in the USA sent false information on real flights and used a wrong address in the signature field of the messages. As a result the airport became more cautious when 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.	The updates invoked by the messages will trigger alerts in the APOC. At worst, it will be impossible to distinguish legitimate alerts from false ones. Flights will be delayed since resources schedules will be disturbed as well as the sequence for departing flights. Good data sent by the stakeholders is interspersed by incorrect data sent by the attackers: The AOP is significantly slowed down by the amount of information that need to be processed. False information is sent to the NOP, which will share it with other AOPs, spreading false information across Europe: The NOP becomes too busy updating data from the targeted airport.

A.5 Scenario 4: Blended attack



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

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 the first scenario 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 target 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.

Why this scenario?	Impacts on APOC, airport and network
This kind of attack has already been carried out on the Ukrainian power grid in 2015 and should be addressed because such hybrid techniques may become more prominent in the future. Blended attacks illustrate that APOC stakeholders should be aware of cyber-security issues, especially the possibility of diversionary attacks, in order to react in an appropriate way when such situations occur.	Minor changes will be sent to disturb handling teams and thus create small delays that little by little will impact outgoing flights to other European airports. The stakeholders will have difficulties understanding that an attack is behind another one and will not necessarily focus on the delays that are created: The decision making process will concern the first and obvious attack instead of the second.

A.6 Scenario 5: Low level attack on APOC ICS/SCADA infrastructure

Programmable Logic Controllers (PLCs) are simple devices that can be used to control physical processes. They run bespoke firmware and do not use conventional operating systems. No logging or forensic capability typically exists for these devices nor do they have any intrusion detection facility. PLCs are an integral part of Supervisory Control And Data Acquisition (SCADA) devices. There are hundreds of thousands of them at every airport, but they are often 'invisible' because they are stand-alone components controlling everything from power distribution through air-conditioning and baggage handling. APOCs increase the integration of these devices through IP interfaces that enable stakeholders to monitor their behaviour.

In the past, PLCs were 'air gapped' but now with increasing interconnectivity, existing SCADA components are very vulnerable – for instance some PLCs have firmware updates distributed from web servers whose URL is in plain text on the installation packages – hence they can be spoofed.

There is also 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.

Previous attacks have shown that malware can change its behaviour over time in order to remain concealed: This prevents diagnosis, especially when airports have no Industrial Control Systems (ICS) forensic capability. In the air gapped case, there is no need to synchronise the state machine stages but this could be done over APOC cyber-physical networks.

Why this scenario?	Impacts on APOC, Airport and Network
CDM depends 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 have been exposed to a growing number of attacks like in Ukraine or Stuxnet in Iran. This scenario reminds us that Collaborative Decision Making (CDM) can be attacked with significant effects. The likelihood of such a scenario might be relatively low now but the intelligence communities across member states have stressed that the threat of such attacks will be increasing, especially in the next 3-5 years.	The attackers might reprogram upper permissible voltage levels so that the APOC networks are continually starved of power. They might alter the temperature settings on building management which could easily impact both the quality of service to end users and APOC stakeholders. Such attacks would undermine confidence in the supply chain. Mutual situational awareness would also be undermined as engineers struggle to resolve the source of the problem. These effects might be exacerbated if information about the attack is leaked to the media or components which do have safety related functions (runway lighting systems, security screening applications, etc.) are impacted.

A.7 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
Business competitors					
Insiders			✓		✓
Hacktivists, Cyber-criminals and Terrorists	✓				
Hackers					✓
States and Organised crime	✓	✓	✓	✓	✓

Table 1: Entities likely to conduct the attacks described in the scenarios

A.8 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		✓		✓	
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)		✓			

Types	Vulnerabilities	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Organization	Lack of fault reports recorded in administrator and operator logs		✓			
Organization	Lack of records in administrator and operator logs		✓			

Table 2: Overview of the vulnerabilities identified for each of the attack scenarios

A.9 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 can 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.

B Cyber-security maturity assessment for airports

This **Cyber-security Maturity Assessment for Airports** allows you to quickly assess your readiness and that of your suppliers for a new era of data-driven airport operations. It is simple, reusable and helps identify priority areas to address. Whilst the study targeted airports deploying APOC/A-CDM/TAM, this Cyber-security Maturity Assessment is equally valid for any airport.

Key stages of cyber-security and resilience are captured in a lifecycle approach:

Foundation: prepare the groundwork for achieving an appropriate level of cyber-security and resilience. This is typically achieved through the application of security standards such as the ISO 27000 series, and then ongoing audit and independent assurance.

Design: ensure that new systems are designed with cyber-security in mind, and that they include enterprise-wide architectural issues, as well as specific requirements at service and system level.

Build: build systems and put them into service in-line with the established security requirements. This involves building trust with the supply chain that security measures have been appropriately applied.

Operate and maintain: since cyber-security is not absolute, operation and maintenance phase activities are ongoing to assess risk and adjust security controls appropriately. It is also necessary to detect and respond to risks and to ensure your staff are aware of the core issues.

There are **five levels of maturity** in this model:

Level	Maturity	Meaning
0	Unaddressed	There is no, or minimal, action. There are no responsibilities, processes or plans. Understanding is minimal.
1	Ad hoc	Sporadic actions are undertaken, often on a reactive basis. There are no formalised responsibilities, processes or plans in place. The function is only partly established.
2	Defined	There are defined responsibilities, processes and plans in place. Enforcement mechanisms may exist. Processes are followed some of the time.
3	Managed	Processes are followed, enforcement mechanisms are used and results are available. The function is fully established. It is well integrated with related functions. There is sufficient understanding such that activities can be structured and prioritised. Metrics are available to show effectiveness.
4	Optimised	Feedback is used to make improvements. There is a focus on a continually improving process and performance. Functions are fully integrated as an aspect of normal operations and business.

The maturity model has **12 key cyber-security functions** to assess:

Stage	Function	Target	Score
Foundation	Leadership and governance	The leadership within industry players establishes clear roles, responsibilities, appropriate investment and budgets. Cyber-security awareness is championed with a corresponding management system. Cyber-security performance indicators are established and reported.	
	Cyber-security risk Management	Regular (re)assessment of cyber-security obligations, context, assets, risks, issues and maturity occurs. Risk management is the basis of all cyber-security activities.	
	Compliance and assurance	A compliance and assurance regime is implemented across industry players, and their partners and suppliers. Technical level assurance is implemented through accreditation, audit, evaluation and/or certification of systems and services. Periodic internal and external reviews provide independent assurance.	
Design	Security architecture	An enterprise-wide, architectural approach to cyber-security is taken, which is clearly aligned to operational and business drivers. Security principles underpin this architecture.	
	Security requirements	Cyber-security engineering requirements are established for the systems and organisation. Cyber-resilience is considered as a key requirement during feasibility and requirements definition stages of projects.	
Build	Security engineering	Cyber-security and resilience is built into systems through engineering processes. This includes, for example, secure coding practices, test and vulnerability management, developer/engineer security, and penetration testing.	
	Security in acquisition	Cyber-security and resilience is 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.	
	Operational planning	Procedures covering operational use, maintenance, contingency plans, etc. are developed to support the deployment of secure and resilient systems.	
Operate and Maintain	Situation awareness	Ongoing activities collect, analyse, alarm, present and use operational and cyber-security information. Better decision-making is facilitated through operational staff, engineers and management being involved. This involves threat intelligence and awareness; continuous scanning, logging and monitoring; vulnerability auditing; and promotion of results through regular briefings.	
	Protection and detection	System controls exist to protect systems from attack, and detect attacks when they do occur. These include technical controls, physical and environmental protection; media protection; associated asset, and change and configuration management.	
	Incident response and recovery	Reporting, prosecution and legal response, lesson learning, and post-incident adaption are in place, alongside localised and regional contingency measures.	
	Awareness and Training	Staff, contractors and suppliers have the right understanding of their responsibilities towards cyber-security, appropriate to their role, and contribute to a security culture within the organisation. The organisation supports and maintains this, including through cyber-exercises to build readiness and learn lessons.	

B.1 How to assess your cyber-security maturity

Using the model is a three-step process:

Internal cyber-security: For each of the 12 functions, score your current maturity on the 5- point scale against the target statement. This will require reflecting on your internal management, operational and technical arrangements, and consider policy, process, people and technology aspects.

Supply chain cyber-security: Your cyber-security is also dependent on that of your supply chain. If you share insecure systems and data that become compromised then you will suffer too. Therefore assessing or at least understanding supply chain cyber-security is crucial. Start by identifying partners, contractors and suppliers and then score them using the same functions and scoring scheme. You might first choose to do this for your key suppliers, before widening out to encompass your entire supply chain.

External validation: Whilst intended for easy self-assessment, the model could, of course, be used by third parties to validate or independently assess maturity.

B.2 Background to the maturity model

This maturity model is drawn from a 2015 SESAR Joint Undertaking study[15] on cyber-security that set out the elements needed to introduce a holistic approach to cyber-security within European air traffic management (ATM) and to develop a comprehensive response to cyber-threats.

This study included a comprehensive maturity model for both the ATM industry as a whole, and for SESAR research and innovation (R&I) programme. A 'light' version of the operational elements has been derived here to offer a quick and easy maturity assessment of airports.

[15] http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security

C Guidance on securing an airport and APOC

Several useful standards and sources of good practices to implementing cyber-security are already available, including some directly applicable to airports. Given that APOC cyber-security is reliant on more general airport cyber-security, a broad and holistic approach is needed. Leading sources of guidance are listed below; from each category one or more approaches should be adopted and systematically implemented:

Security Management System	**ISO 27001 Information Security Management System** is a certifiable global standard for an all-round management system, which whilst targeted for IT can be adapted for operational technology. **CPNI Security for Industrial Control Systems (SICS Framework)** (cpni.gov.uk/SCADA) is a multi-part guidance giving good practice. Detailed guidance is provided on multiple aspects of ICS security such as managing risk, establishing efficient governance mechanisms and configuring and managing access to ICS systems. Note that an Information Security Management System needs to be interfaced to a broader Security Management System.
Controls	**ISO 27002 Code of practice for information security controls** provides a control set and good practices to accompany ISO 27001. **EN 16495 Air Traffic Management. Information security for organisations supporting civil aviation operations** (once updated and aligned with the latest ISO 27002 standard) is tailored to civil aviation and contains some supporting guidance. **NIST SP 800-53 Security and privacy controls for Federal information systems and organisations** is a comprehensive catalogue of controls, with much supporting advice. It is mandatory for US Federal organisations and focused at business/information systems. **NIST 800-82 Guide to Industrial Control Systems (ICS) Security** provides guidance through typical system topologies, threats and vulnerabilities. It then provides recommended security countermeasures through an ICS-tailored security control overlay, based on NIST SP 800-53, corresponding to ISO 27002. **ISA/IEC-62443** is a set of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems.
Inter-organisational issues	**ED-201 Aeronautical Information Systems Security (AISS) Framework Guidance** is a EUROCAE standard that advises on the context of the shared responsibility for security. A central concept is that of a standardised External Agreement that 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. Though a recent standard, it has been 'road-tested' on an airport.
Other guidance and tools	**ACRP Report 140: Guidebook on Best Practices for Airport Cyber-security** contains detailed information on how cyber-security should be implemented within the context of the airport and how to mount an appropriate response and recover from attacks. **ACI** is providing a cyber-maturity benchmarking tool centred on the implementation of the ISO 27002 control families. **ENISA's Securing Smart Airports** report provides a series of good practices on how to secure airports.

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.