Protecting aviation safety against cybersecurity threats

Peter Stastny\(^1\) and Adrian-Mihail Stoica\(^1\)

\(^1\) University Politehnica of Bucharest, Splaiul Independentei 313,
Sector 6, Bucharest, Romania

Corresponding author: peter.stastny@btinternet.com

Abstract: In Air Traffic Management (ATM), Safety Management Systems (SMS) form the principal vehicle for implementing safety policies, practices and procedures in accordance with internationally agreed Standards. In a constantly changing operating environment, it is essential to maintain SMS effectiveness to maintain and enhance levels of ATM safety. Research at the University Politehnica of Bucharest (UPB) has analysed the major, fast-rising threats to ATM safety emerging in the cybersecurity field, and the related synergies between formal management systems in the fields of security and safety. Its ultimate objective is to assess the feasibility of equipping SMS with protection against security risks, especially cybersecurity. It further explores the potential effects of cybersecurity threats to aviation safety and the available protection mechanisms. In considering the synergies between Security Management Systems and Safety Management Systems in ATM, the possibility of full integration of the two into a single protection system is explored. Whilst, despite similarities, such a combination is not found to be an optimal arrangement, the examination nevertheless enables the derivation of the security measures required in order to enhance the effectiveness of SMS.

Keywords: ATM, Safety, SMS, Cybersecurity.

1. Introduction

In Air Traffic Management (ATM), Safety Management Systems (SMS) are the principal vehicle for implementing safety policies, practices and procedures in accordance with internationally agreed Standards [1]. In a constantly changing operating environment, it is essential to maintain SMS effectiveness to maintain and enhance levels of ATM safety. Research at the University Politehnica of Bucharest (UPB) into the future development directions of SMS has identified a range of new safety approaches and methods designed to ensure that safety performance keeps pace with increasing industry challenges and pressures and thus avoids a progressive decline in aviation safety.

Six development paths for enhancing the effectiveness of SMS have been identified, including three in the category of ‘Opportunities’ - self-initiated proactive measures as part of SMS management and development - and three in the category of ‘Threats’ - protective measures required to respond to external factors which have the potential to degrade ATM safety levels. In the ‘Threats’ category, Cybersecurity is targeted as a major area for action. For each development path, enhancement measures are proposed, designed to contribute to an overall increase in levels of SMS effectiveness over the next decade, thus enhancing overall SMS performance and countering the effects of increased pressures and threats in the ATM system over that time.

2. Cybersecurity threats

Globally, the demands of society have resulted in the development of ever-more complex technological systems which operate in, and support, almost all aspects of modern life. Such systems rely on the use of information technology and can therefore be vulnerable to attacks based on malicious use of software-based techniques.

Recent experience has illustrated a wide range of targets for such attacks, including central state-operated administrative functions such as financial and healthcare services, as well as critical national infrastructure such as energy, water, and transportation networks. In aviation, certain airport IT systems have been attacked, including in the UK (Heathrow, Gatwick), Ukraine (Kiev and Odessa) and the US (Atlanta), among others. Not all the attacks on aviation targets have impacted
safety. However, the scale and potential of the attacks has served to place ANSP’s on a defensive footing, both at the time and since.

3. Effects on aviation safety

In its report “Dealing with Airport Cyber-Security”, the EU/EUROCONTROL Single European Sky ATM Research (SESAR) Programme has acknowledged airport cybersecurity as a major challenge and has further identified potential cyber-attackers, as well as a range of attack scenarios and vulnerabilities [2]. In addition, the report references current best practice in assessing and mitigating cybersecurity threats (dealt with in more detail in paragraph 4 below).

Many airport threat areas are not restricted or limited to airports alone. Airports exist as nodes within both national and international airspace and air-route networks. Their operations are critically connected to, and dependent on, other non-airport parts of the airspace network.

Major inter-connections involve the exchange of safety-critical data via software-based systems. In this context, airports may be regarded as potential entry points for threats aimed at the entire aviation system. The SESAR report assesses ATM as being one of several elements of airport operations subject to potential cybersecurity threats where safety can be impacted.

The report concludes that the effects of cyber-based attacks may be realised in a number of areas having commercial consequences, including business continuity and related disruption. As one example, the introduction of corrupted or false data can have dramatic negative effects beyond the airport itself and can lead to more major problems within the en-route network, including in the planning of flow control. Such problems inevitably impact on the safety of the ATM system.

Safety reports have highlighted the ability of attackers to gain access to aircraft systems. Airlines offering on-board internet connectivity present an entry point to on-board software-based systems – not only those controlling internet access but also those involved in flight control and navigation.

4. Cybersecurity protection mechanisms

In view of these factors, it is necessary to consider the protection mechanisms that currently exists to counter such cybersecurity threats.

In terms of global requirements, ICAO Annex 17 sets high-level Standards for aviation security, including Cybersecurity, by which “each State shall establish and implement a written national civil aviation security program” and, in respect of ANSPs, “air traffic service providers operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security program of that State.”

As a practical means to comply with the ICAO Standards, the US National Institute of Standards and Technology (NIST) has produced a ‘Framework for National Infrastructure Cybersecurity’ which sets out current industry best-practice in this field [4], as summarised in table 1.

| Core Function | Objective |
|---------------|-----------|
| Identify      | To understand the cybersecurity environment. |
| Protect       | To develop and implement appropriate safeguards. |
| Detect        | To implement measures to quickly identify cybersecurity events. |
| Respond       | To develop the ability to contain the impact of cybersecurity incidents. |
| Recover       | To develop the capability to restore impaired capabilities and services. |

The Framework defines an approach to implementation consisting of Tiers which represent progressively increasing levels of protection and defence capability. These have been assessed in the context of ATM by EUROCONTROL and its stakeholders, and table 2 presents the five levels of increasing maturity of cybersecurity protection offered [5]: -
Table 2. Levels of Cybersecurity Maturity in an ATM Context (source – EUROCONTROL).

| 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, but results are not formally recorded. |
| 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. Processes and systems are monitored and there is a framework for continuous monitoring. Metrics can be structured and prioritised. |
| 4     | Optimised | Feedback is used to make improvements. There is a focus on a continuity improving process and performance. Functions are fully integrated as an aspect of normal operations and business. |

A further development has been the introduction of Security Management Systems (SeMS) used by organisations open to cybersecurity vulnerability as a structured and formalised way of embedding the above Framework principles and processes into the overall management of their operations [6].

5. Synergies with SMS

Providers of ATM services (ANSPs) are inextricably exposed to potential cybersecurity threats through their involvement in the international aviation network. Many ANSPs provide ATM at airports and, even those that do not, have complex data-exchange connections to many that do. Thus, ANSPs in Europe have an obligation to have in place appropriate cybersecurity protection measures.

At the same time, all ANSPs bear obligations under ICAO Standards and EU legislation to have Safety Management Systems in place [1][7]. In addition, under the EU Single European Sky Performance Scheme, ANSPs are required to achieve progress in increasing SMS maturity in accordance with legally-binding Key Performance Targets, including those based on the CANSO/EUROCONTROL Standard of Excellence (SoE) (outlined in figure 1 below) [8]: -

![Figure 1. CANSO/EUROCONTROL SoE Levels of SMS Maturity (source CANSO).](image_url)

This raises the inevitable question – is it possible to combine the management systems for safety and security? Initial examination reveals a number of synergies between SMS and SeMS. Both systems: -

- …exist as formal management systems aimed at achieving specified objectives while operating within the overall management structure of the operating organisation;
- …are implemented through a similar range of policy, processes and procedural steps, and use monitoring and feedback systems to ensure correct performance;
- …require a progressive and measured approach to increasing maturity;
• …utilise a system of maturity measurement – five steps in each case – in which progression can be resolved into additional actions and methods being implemented on the part of the operating organisation.

At the same time, however, there are some fundamental differences between the two systems which negatively affect the degree to which they may be integrated in the ATM context: -

• While their common over-arching objective is to safeguard the ATM system, their specific management-system objectives, although operating in parallel, may be quite different. In safety, the focus is primarily on correcting failures (of all types) in the ATM system whereas, in security, the emphasis is on protective defence against aggressive action;
• To be increasingly effective, both systems require the operating organisation to achieve increasing levels of maturity. However, the steps towards full maturity in each case are not comparable. Furthermore, increased maturity in one system does not translate in any way to similar progress in the other;
• Within an operating organisation, both safety and security activities require involvement by the entire workforce. However, in both cases, the relevant management systems require to be overseen by specific expertise (e.g. in SMS, a safety department). The professional expertise required in the two fields is markedly different.

Despite these important differences, and while not achieving full integration of the two systems, it is nevertheless beneficial to explore the extent to which the effectiveness of SMS may be “reinforced” by means of certain measures to improve resistance to cyber-attacks, and to support the parallel operation of SMS and SeMS. Figure 2 below presents a view of the parallel nature of the two management systems, in which their similarities and differences are well illustrated: -

Figure 2. The Interface between SMS and SeMS (source EUROCONTROL).

The (previously-referenced) SESAR Report points out that not all effects of cyber-attacks are safety-related. However, the variety of potential types of attack is large and, in any given attack scenario, it is impossible to know a priori whether there is an impact on safety and, if so, what the nature and magnitude of that impact may be.

So how can the effectiveness of an SMS be enhanced to counter cybersecurity threats? What would be the specific objectives in doing so, and what would be the specific enhancement measures?

6. Safety and security in parallel

6.1. Independent co-assurance

Before any safety-related service can be provided, it is undoubtedly necessary to reach a satisfactory conclusion on both the safety and security of the service in question. If this cannot be through the use of a single management system, then independent but coordinated action in the two fields is possible to a certain extent.
Johnson and Kelly [9] examined the processes for Risk Assessment in both the safety and security fields concluding that:

“safety and security can be co-assured independently, as opposed to unified co-assurance which has been shown to have significant drawbacks. This also allows for separate processes and expertise from practitioners in each domain. The focus is shifted from simplified unification to integration through exchanging the correct information at the right time using synchronisation activities.”

These principles are embedded in a proposed Safety-Security Assurance Framework by which the necessary inter-domain coordination can take place. This approach relies upon the construction of parallel arguments with phased interventions where the system architecture is updated accordingly – see figure 3 below:

This approach is entirely consistent with current SMS practises in ATM, where the Safety Case methodology has become the standard basis on which to document the safety argument outcomes of the risk assessment process.

6.2. Security-informed safety.
Along similar lines, Bloomfield et al [10] introduced the concept of “Security-Informed Safety”. This concept is based on the use of structured safety cases, used within SMS processes, and analyses the impact of security on the safety arguments constructed and presented within the safety case process.

The usual top-level claim to be proven within a safety case is that “the system is safe”. In considering the impact of security, this top-level claim is modified to become “the system is safe and secure”. This captures the key point that, if the impact on safety of an unquantified security threat cannot be defined, then a system that cannot be assessed as secure cannot be considered to be safe.

Within this concept, the arguments are therefore resolved in parallel, as follows:

(security only issues) + (safety and security issues) + (safety only issues)

allowing a clear definition of the issues that are in each category. The respective parallel cases for safety and security can then be assessed accordingly.

6.3. Limitations
It is clear that both the above approaches can offer significant clarity and assistance in reaching the required levels of acceptability for system safety and security. However, from a safety viewpoint, it is evident that both methodologies focus exclusively on the risk assessment and mitigation area of safety management, to the exclusion of other areas.
Thus, the other elements of SMS that are required to deal with the safety effects of cybersecurity threats, such as enhancement of safety policy, allocation of responsibilities, reporting of occurrences and training (inter alia), are not considered.

From a holistic perspective, therefore, the ways in which SMS can manage and counter such threats need to be analysed.

7. Coping with and countering cybersecurity threats in SMS

7.1 Objectives.

Regarding any enhancement of SMS in the context of cybersecurity, it should be clear that: -

• With reference to the analysis in paragraph 5 above, an enhanced SMS is not intended to be a replacement or substitute for a SeMS. The organisation will still require a security management system as part of the overall management of its operations;

• the objective of any enhancement is to reduce, to the maximum extent possible, the effects of cyber-attacks on the functioning of safety management. Thus, any cyber-attack should have a minimal (if not zero) effect on safety, though other (non-safety) consequences may be experienced;

• Any enhancement should be in alignment with, and in support of, the parallel operation of the SeMS.

7.2 Enhancement measures.

A start-point for assessing the enhancement measures required, and also to consider the ability of SMS to support the organisation’s overall cybersecurity protection, is to examine the key components of a SeMS. Consistent with other industry sources, UK CAA CAP 1223 summarises these as follows [6]: -

• Management Commitment
• Threat and Risk Management
• Accountability and responsibilities
• Resources
• Performance monitoring, assessment and reporting
• Incident response
• Management of change
• Continuous improvement
• Education and security culture
• Communication

At the same time, the SMS arrangements in use by European ANSPs are summarised in figure 4 below:

![Figure 4. Current CANSO/EUROCONTROL SMS Arrangements. (source CANSO/EUROCONTROL).](image)

The similarity between the key constituents of both systems is evident, and points towards the ways in which the design and operation of SMS may be reinforced in support of SeMS.
In addition, a 2013 study conducted by Chivers and Hird [11] examined deficiencies in the security arrangements in ATM service-provision in Europe and also compared the results with similar findings by the Department of Transportation in the US. A high level of correspondence was found, with a significant number of deficiencies or ‘blind spots’ occurring in many of the SMS and SeMS management elements examined above, including the processes relating to:

- Senior management responsibility
- Policy review
- Policy communication
- Independent review
- Accreditation process
- Incident response
- Business continuity planning

Clearly, cybersecurity protection and detection of threats have the potential to impact the vast majority of SMS functions – not just Risk Management. Deriving from the above analysis, a number of essential areas are therefore immediately identified, falling in to two main categories:

- Proactive – those SMS functions where preparatory measures can be deployed in advance of threats being realised, and
- Reactive – those SMS functions whose role is to respond to attacks both in real-time and through historical analysis.

With respect to the SMS Framework in figure 4, table 3 below proposes measures to be applied to current arrangements to enhance SMS effectiveness by providing an initial capability to support security management in detecting and counter-acting cybersecurity threats:

**Table 3. Proposed Measures to Enhance ATM SMS Effectiveness in Cybersecurity.**

| SMS Elements                          | Potential Organisational Vulnerability/Need                                                                 | Proposed Counter-Measures for SMS Enhancement                                                                 |
|---------------------------------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Safety Policy                         | Organisation insufficiently aware of need for defence against cybersecurity threats.                      | Incorporate the need to reinforce the SMS and support the SeMS within the organisation’s safety policy.        |
| Organisational Safety Responsibilities| Key personnel are unaware of their roles and responsibilities in respect of cybersecurity threats.         | Define roles and responsibilities for key safety personnel in respect of cybersecurity threats, and the need to liaise with and support organisational security management personnel. |
| Coordination of Emergency Response Plan (ERP) | Emergency Response Plan unprepared to cope with cyber-attacks [12].                                        | Include cyber-attacks as a source of actual or potential disruption to be managed within the scope of the ERP. |
| Risk Management Process               | Need to consider cybersecurity threats to safety alongside all other risks.                                | Include cybersecurity threats within the safety risk assessment and mitigation process, including a means of risk categorisation. Co-assurance methodologies (ref. para 6 above) may be used if consistent with the means of documenting safety arguments (e.g. use of safety cases). |
| Safety Interfaces                     | Need to ensure that SMS actions taken in respect of countering cybersecurity effects on safety are fully coordinated within the organisation. | Implement procedures to ensure full coordination between SMS responses to cybersecurity threats and wider organisational functions, including security management. |
| Safety Performance Monitoring         | All threats to ATM safety need to be monitored to establish the scale and nature of the threats, as well as longer term trends. | Update performance monitoring procedures to include the effects of cybersecurity threats on ATM safety performance. |
| Continual SMS Improvement             | SMS must be kept current in terms of known or anticipated threats to safety.                             | Updated assessments of cybersecurity threats to be taken into account as part of regular SMS effectiveness reviews. |
Safety Reporting

Need to achieve full visibility of cybersecurity occurrences and their effect on safety performance.

Introduce further categorisation within the safety reporting system to take account of cybersecurity events, including a means of severity classification (in terms of safety impact).

SMS Audits

To ensure that cybersecurity counter-measures are in place and functioning effectively.

To include SMS measures to counter cybersecurity threats in regular SMS audits.

Safety Communication

Cybersecurity issues and events need to form part of normal organisational communications (internal and external) on safety matters.

To improve organisational awareness by including cybersecurity information within normal communications methods on safety matters.

Training and Education

A key need is awareness of cybersecurity threats and defences at all levels of the organisation.

To formalise awareness of cybersecurity matters through their inclusion in organisational training programmes.

8. Conclusions

Cyber-attacks are a serious emerging threat to operating organisations and national critical infrastructure. Cybersecurity countermeasures are urgently needed across a wide range of industry sectors. In aviation, the formal management of security issues is now an ICAO Standard and the implementation of Security Management Systems (SeMS) represents best practice. In its field, SeMS needs to operate in parallel with SMS, and has comparable principles and processes.

Despite similarities, analysis has shown that SeMS cannot be directly integrated into SMS. Nevertheless, there are ways in which SMS can be reinforced to counter the effects of cyber-attacks on aviation safety and thereby also support SeMS.

A range of measures are proposed to enhance SMS effectiveness. Such measures are not intended to be a substitute for a SeMS but will facilitate cooperative parallel working of the two management systems, including the possibility for co-assurance activities.

REFERENCES

[1] ICAO 2016 Annex 19 to the Chicago Convention – Safety Management – Second Edition.
[2] European Union & EUROCONTROL 2016 Single European Sky ATM Research (SESAR) – Addressing Airport Cyber-Security - Final Report.
[3] ICAO 2017 Annex 17 to the Chicago Convention – Security.
[4] US National Institute of Standards and Technology (NIST) 2018 - Framework for Improving Critical Infrastructure Cybersecurity.
[5] EUROCONTROL 2018 - ATM Maturity Cybersecurity Model Workshop.
[6] UK Civil Aviation Authority 2018 – Civil Aviation Publication CAP 1223 – Framework for and Aviation Security Management System (SeMS).
[7] European Commission 2017 - Implementing Regulation (EU) 2017/373 Common Requirements for Providers of ATM/ANS and Other ATM Network Functions and their Oversight.
[8] CANSO 2015 – Standard of Excellence in Safety Management Systems.
[9] Johnson N. & Kelly T. 2018 University of York, UK – An Assurance Framework for Independent Co-assurance of Safety and Security.
[10] Bloomfield R. & Netkachova K 2013 City University London & Stroud R. Adelard LLP – Security-Informed Safety: If It’s Not Secure, It’s Not Safe.
[11] H. Chivers University of York & J.A. Hird EUROCONTROL 2013 - Security Blind Spots in the ATM Safety Culture – Paper to the 8th International Conference on Availability, Reliability and Security (ARES).
[12] CANSO 2015 - Emergency Response Planning Guide.