International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/160
28/9/18
(Information Paper)
English only

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

CONSIDERATIONS ABOUT CYBERSECURITY IN AVIATION

(Presented by Austria on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2]; and by EUROCONTROL)

EXECUTIVE SUMMARY

This paper supports the AN-Conf/13-WP/42 on cybersecurity by expanding on concepts intended to be used to improve the situation of cybersecurity in aviation. It will touch on notions like aviation being a System-of-Systems, which should be designed with Security-by-Design in mind. It will also touch on rationales why any organisation should manage not only their individual cybersecurity risks, products and services by means of an Information Security Management System (ISMS), but also why this should be done in a concerted way.

The paper also addresses the notions of dependability, confidence and trust, from which it derives concepts for digital or technical trust, trustworthiness and operating conditions for cybersecurity, why they are needed and which benefits they provide.

The paper further touches on the differences between information sharing and the notion of reporting and notification.

1. INTRODUCTION

1.1 The availability of correct information and the correct functioning of safety-critical information systems are pre-requisites for a safe and secure civil aviation as the sector encounters further digitalization. The aviation system is highly interconnected and information travels globally. Therefore, a holistic and end-to-end approach must be taken to cyber security initiatives in the aviation sector. These will only be successful if aviation is understood as a "System-of-Systems", for which all members of the aviation community are accountable and share responsibilities. The aviation system in the future thus

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

requires more concerted design and less individual evolution to maintain its resilience against cyber interference.

1.2 To avoid confusion with other terminology, this paper will use the term "cyber security" interchangeably with "information security". The latter is also perceived as the more accurate term, as the ultimate objective of protection is information and those systems and interfaces processing, exchanging, or storing information.

1.3 This paper supports the European working paper AN-Conf/13-WP/42 and introduces into the different concepts in a more detailed manner. It starts with a discussion about the "System-of-Systems" notion, including fundamental design principles like "Secure-by-Design".

1.4 It further addresses some objectives and characteristics of Information Security Management Systems in general as well as its extensions with respect to the "System-of-System" approach, as required for the aviation sector.

1.5 This paper also elaborates on the notion of Dependability, Trust, and Confidence. Trust generally reflects the level of anticipation that another party behaves as legitimately expected, while confidence is about the level of control and scrutiny, of facts and evidences, which can be considered in the assessment of expected behaviour of another party (or system). In the aviation sector, trust - in addition to confidence - in each partner is paramount. *Digital* or *Technical Trust* and *Trustworthiness* are two related concepts which will be addressed in this context. Further, the information security environment is constantly changing, a concept allowing implementation of cybersecurity measures at different times and adaptation of diverging trustworthiness levels will thus be required. One reason: it will be highly unlikely that all aviation will be able to establish to the same level of trustworthiness at the same point in time. This paper will describe an adaptation of the existing concept of Operating Conditions, as it can be applied to cyber security.

1.6 Sharing information for long term trend and systemic weakness analyses purposes differs from Information Sharing for operational purposes. However, they are linked to the extent that lessons learnt from operational occurrences should be used to initiate changes targeted to reduce risks. Regulatory update processes are one vehicle to achieve improvements. Within organisations Computer Security Incident Response Teams (CSIRT) or Cyber Security Centres (CSC) are usually tasked to support operational Information and Communication Technology (ICT) entities in securing their services and systems.

2. DISCUSSION

2.1 **System-of-Systems –** Before entering into the discussion of *Systems-of-Systems* it should be emphasised that in the context of this paper a *System* consists of Products, People and Processes. This means that the term *System* should be broadly interpreted and is not limited to technical equipment!

2.1.1 A description of a System-of-System (SoS) reads like this: "A system of systems (SoS) brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals."[3].

[3] ISO/IEC/IEEE 15288 Annex G (ISO, 2015), Systems and software engineering -- System life cycle processes

2.1.2 That's not much different from the description of a system itself. This is quite natural, as a SoS is a System in itself. So, in the context of ICAO, what distinguishes a SoS from a "*System*"? There are a few characteristics, which allow for a distinction (Maier, 1998[4]):

- **Operational independence of elements:** The elements that make up a system of systems are in turn fully self-sufficient systems. These systems can also be independently operated and used. You can also leave a system-of-systems network to join another System of Systems.

- **Managerial independence of elements:** The subsystems of a SoS can not only work independently of each other, they are usually also developed and procured separately. Their lifecycle is independent of the system-of-system lifecycle model. However, from the security perspective a SoS can only be protected by shared management of risks by all SoS elements.

- **Evolutionary Development:** A completely developed System of Systems does not exist! Its development and existence is evolutionary. Over the entire lifecycle, functions - and thus subsystems - are added, removed or changed on the basis of operational experience. From an information security perspective this creates the challenge of composability: Under which conditions can changes to the SoS composition avoid degradations in the effectiveness of protection of the SoS?

- **Emergent behaviour:** Emergence is the more or less spontaneous formation of new qualities or functions of a system as a result of the interaction of its elements. Emergence can be observed well in nature, for example in the swarm behaviour. A large bird or fish swarm are good examples of this. The individual individuals of such a swarm know only the position and direction of movement of their immediate neighbours. By emergence, however, the movement of the entire swarm appears to an outside observer as if it were centrally controlled. Transferred to a system of systems, this means that the composition of the subsystems creates certain properties and services for the user that can no longer be uniquely assigned to subsystems.

- **Geographical distribution of elements:** The geographical extent and distribution of subsystems of a SoS is often very large. "Size" is certainly a fuzzy and relative concept, but in terms of a SoS, it means that its subsystems, due to their spatial distance from one another, can essentially exchange only information, and not significant amounts of mass, matter or energy.

Systems-of-Systems can be classified into the following categories (Maier 1998; Dahmann and Baldwin 2008[5]; DUS(AT) 2008[6]; Dahmann, Lane, and Rebovich 2008[7]):

- **Virtual:** Virtual SoS lack a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behaviour emerges—and may

[4] Maier, M.W. 1998. "Architecting Principles for Systems-of-Systems". Systems Engineering.
[5] Dahmann, J., and K. Baldwin. 2008. "Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering." Paper presented at IEEE Systems Conference, 7-10 April, Montreal, Canada.
[6] DUS(AT). 2008. Systems Engineering Guide for Systems of Systems," version 1.0. Washington, DC, USA: Deputy Under Secretary of Defense for Acquisition and Technology (DUS(AT))/U.S. Department of Defense (DoD).
[7] Dahmann, J.S., J.A. Lane, and G. Rebovich. 2008. "Systems Engineering for Capabilities." CROSSTALK: The Journal of Defense Software Engineering. (November 2008): 4-9.

be desirable—but this type of SoS must rely upon relatively invisible mechanisms to maintain it.

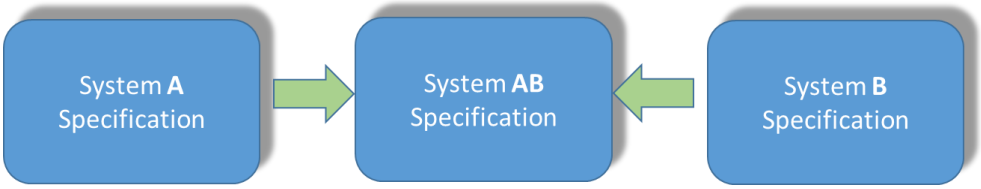
- **Collaborative:** In collaborative SoS the constituent systems interact more or less voluntarily to fulfil agreed upon central purposes. The Internet is a collaborative system. The Internet Engineering Task Force works out standards but has no power to enforce them. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.

- **Acknowledged:** Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.

- **Directed:** Directed SoS are those in which the integrated system-of-systems is built and managed to fulfil specific purposes. It is centrally managed during long-term operation to continue to fulfil those purposes, as well as any new ones the system owners might wish to address. The constituent systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

2.1.3 In the context of ICAO the aviation community will establish multiple types of sub-SoS. However, on the ICAO level aviation can be considered to be at best a SoS of the ***Acknowledged*** category.

2.1.4 In the context of information security of a System-of-System, a consideration mentioned above needs to be highlighted: ***Composability***. It describes the challenges of integrating multiple elements (components for systems, or subsystems for SoS) into bigger entities. Systems integration based upon the functionality of its individual elements is focused upon the individual properties of these elements. Interface definitions and functional specifications determine the conditions under which such integration can take place (e.g. compatible definitions for network interfaces or information formatting; frequency of exchange; physical layout; etc.). Physical or logical performance properties may create further conditions for integration (e.g. heat dissipation; duty-cycle; Gflops; MTTF; Severity of safety effects; etc.). In essence, if determined that integration is possible, the individual properties of each element are maintained. An example: In the figure below System A and System B are integrated and form the resulting System AB. Interfaces and functional properties expose their combined characteristics to their environment, unless they are now internal to the new system (e.g. individual external interfaces may



become combined internal interfaces).

2.1.5 However, when it comes to the integration in the information security context, as shown in the next figure, the limitation to specified functionality and performance is no longer adequate. The integration under consideration of the information security context includes additionally the integration of

the Security Environment (SE) of each element. Not only is each individual SE largely unknown (its space is simply too vast, we only know about individual spots that have been investigated), the resulting SE is almost totally unknown – including the consequences of their integration. To be able to make any assessment of the SE, an extra step of assurance actions is required, which are dedicated to the resulting combined environment called Refutation.

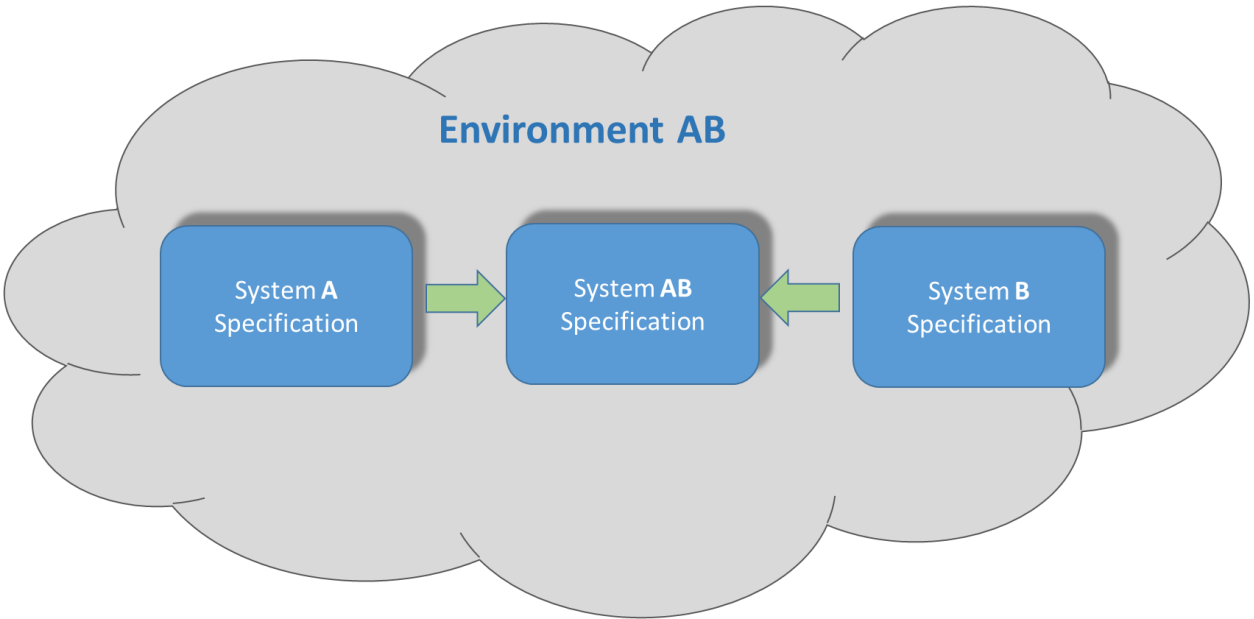
2.1.6 Refutation is introduced by Eurocae/RTCA ED-203A / DO-356A and used in the sense of demonstrating the absence of problematic behaviours, as in refuting the allegation of vulnerabilities. Hence, information security refutation is demonstrating the absence of information security problems.

2.1.7 An example: In the figure below System A, including its (information security) environment, and System B, also including its (information security) environment are integrated and form the resulting System AB, including its combined (information security) environment. Like in the example before, Interfaces and functional properties expose their combined characteristics to their environment, unless they are now internal to the new system (e.g. individual external interfaces may become combined internal interfaces). However, no statement can be made about the combined environment, until Refutation actions have been performed.

2.1.8 Examples for refutation actions are security penetration testing and may include fuzzing tests. As a generalization, when a set of requirements are generated in response to a negative requirement/objective – specifying the absence of specific behaviours – then even though a set of requirements are correct and complete and are properly developed, this does not mean that the resulting assurance actions necessarily provides confidence in the absence of specific undesired behaviours beyond what is called process assurance.

2.1.9 ED-203A / DO-356A continue in stating, "Refutation activities act as an independent set of assurance activities beyond those assurance activities driven from the formalized analysis and requirements. Any time system complexity precludes exhaustive testing that an unwanted behaviour never occurs, refutation can be used to formally demonstrate that an unwanted behaviour has been precluded to an acceptable level of confidence".

2.1.10 For integrations like the one in the figure below applying refutation for key areas seems to be straightforward. However, the above mentioned exhaustive refutation effort may increase overwhelmingly, as the complexity of the SoS – ultimately like the global aviation system - increases. The task of the community is thus to identify representative subsystems and research to which extent and by which margin of error its results – based upon the measures taken and the practices used – can be

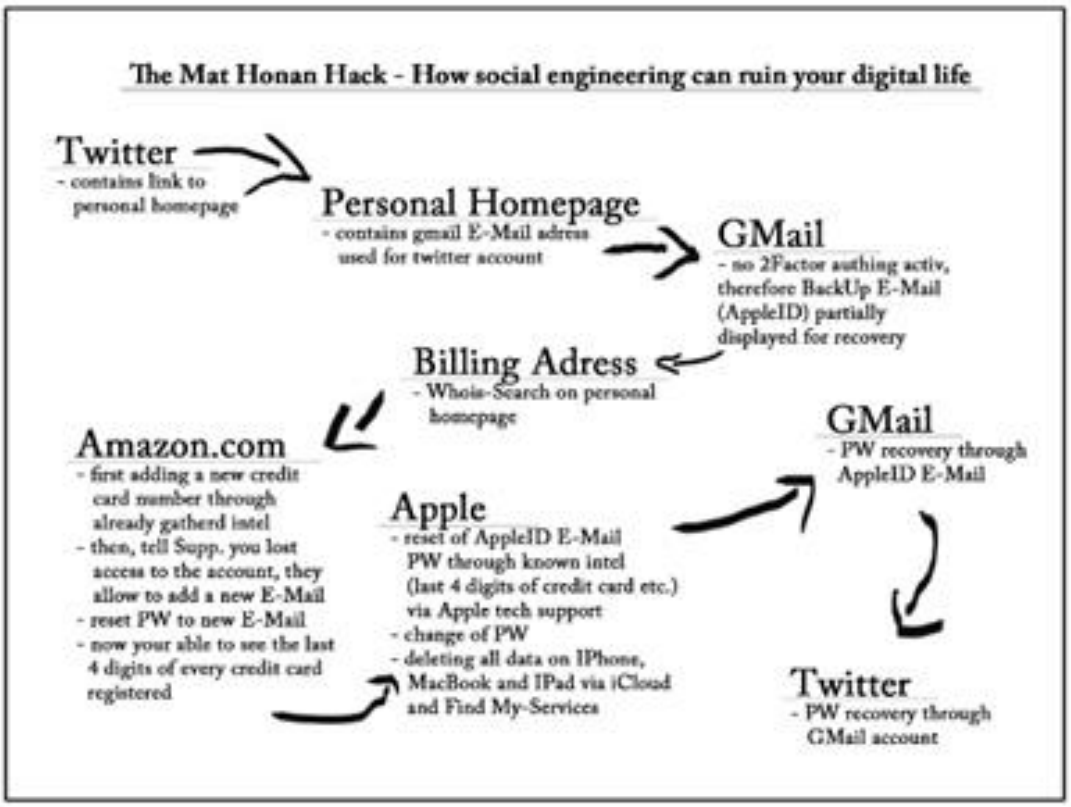


transferred to other subsystems. An example: SESAR is developing coherent approaches for its constituents, resulting in a significant degree of compatibility among them. It may be conceivable that refutation results of one constituent system will also be applicable to other constituent systems, and thus do not require a full repetition there. Another task is to initiate the development of larger subsystems, which consider information security during their initial design phase (see "Secure-by-Design"). This will allow for the evolution of the aviation system to higher levels of resilience and maturity against unauthorised or unlawful electronic interference by adverse (intentional) or negligent (unintentional) actors.

2.1.11 An example for such global, collaborative SoS is The Internet. Organisations are individually trying to protect themselves against information security threats. Unfortunately, their approach is not sufficient, as one prominent case demonstrated in 2012: an editor of the Wired Magazine, Mat Honan, explains in the "HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING" article[8], how "*IN THE SPACE of one hour, my entire digital life was destroyed*". A malicious hacker, interested in his Twitter account, took advantage of the uncoordinated information security approaches taken by Internet Giants like Google, Apple, or Amazon, and eventually gained access to his Twitter account.

The lessons learnt from this case are that not only gaps in the approaches will create dangerous loopholes, uncoordinated overlaps may be equally dangerous for the effectiveness of protection or a larger System-of-Systems.

[8] https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/



2.2 **Secure-by-Design –** In engineering, this means that systems – in the broad sense as mentioned above – when they are designed and integrated into SoS, are securable, secure and remain secure during their whole life-cycle. Adverse practices are taken for granted and care is taken to minimize their impacts. However, in the past, and unfortunately probably for many years to come, information security has been and will be considered by some as an add-on to systems.

2.2.1 The aviation system that we use today has been designed during many decades, using a threat model relying upon presumptions such as attackers having inferior technological, or financial capabilities and little or no knowledge of the system. An insider threat was not included in the model for a very long time and only less than a decade ago information security threats have been internationally recognised by the aviation community as part of the ICAO Beijing Convention of 2010 (though only indirectly). However in the meantime the world has evolved, developing new information system technologies that aviation is heavily relying upon, however without reconsidering its threat model. A new model should now include the fact that technological capabilities have increased with the development of e.g. Software Defined Radios which allow interception and generation of messages on analogue channels at no extra cost for bespoke components. At the same time, the benefits of using commercial technologies in aviation helped also reducing the effort for potential adversaries to interfere with the system.

2.2.2 A *common* understanding of the term "secure" is that no interference with a system could change its intended or expected behaviour or performance. While this seems simple from a concept perspective, it is more difficult in its application as it can encompass many complex interactions, in particular in a SoS environment.

2.2.3 Many of the core functions of the aviation system are shared among multiple stakeholders. Knowing about those functions and their security needs is essential to the functional and architectural design of the system. As a general rule, the Secure-by-design principles will rely upon three pillars which are reflecting the most common risk assessment and management methodologies.

- 1st pillar - reflects the fundamental principles of the architecture: how components relate to each other and the nature of their interfaces. It deals with dependencies and reduction of complexity, with composition of systems and with trust. But it will also consider the evolution of the system without jeopardising its security capabilities.

- 2nd pillar - deals with the information security needs of functions across federated aviation systems, and the design and effectiveness of information security measures applied. Ensuring to meet those needs continually, requires trans-organisational risk management. Sharing the results of risk assessments among providers of functions are giving the key elements to the definition and application of mitigations. However, the design of information security measures should consider an approach which prevents to oppose security principles (e.g. “secure fail”) with safety principles (e.g. “safe fail”).

- 3rd pillar - contributes to the initial and continuing security of a system. A system and in particular a SoS will evolve throughout its lifetime. For example, an aircraft will be operating for approximately 30 years without any fundamental change in its information system architecture. One retrofit during lifetime is the maximum to be expected, implying that the maintenance of the security status of the aircraft would require an agility which has to be integrated into the design. But retrofitting has also its challenge to avoid transforming a system able to sustain the security objectives, into a system which is not. The reliability of processes to maintain the level of security of a system at its best, is also an essential element of the third pillar.

2.2.4 Experience has shown that when these principles were applied to the design of a system, development time and effort often rose in comparison to typical "time to market"-driven commercial development practices. This economic discrepancy has resulted in various proposals for using untrustworthy components to create trustworthy systems, with unsatisfactory results. However, regulation has been influencing positively the safety level of flights so far, and the future will prove to be even safer with a novel engineering approach integrating information security across the aviation system, embracing the "Secure by Design" paradigm relying upon the 3 pillars above.

2.3 **Information Security Management Systems –** Existing concepts of Information Security Management Systems (ISMS) are inherently limited to individual organisations. Two of the most prominent standards for ISMS are ISO 27001, or NIST Special Publication 800-39, but other standards also exist. Their scope is to: "*…specify the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization*". In addition they also include requirements related to the assessment and treatment of risks, as they pertain to an individual organisation.

2.3.1 The risk management process itself is very well established in aviation. However, there are a number of reasons, why the introduction of an ISMS is a fundamental deviation from the way the aviation community is used to conducting business. One key reason is the difference between the treatment of so-called "*software bugs*" in the traditional risk management process and the one of "*vulnerabilities*" in the ISMS.

2.3.2 For the former, safety and quality assurance requirements require measures for the identification and remediation of software design and implementation errors, commensurate with the level of safety risk they may create or contribute to. As soon as all those measures have been taken, all tests completed and passed without deficiencies, the software will only be modified again if unexpected behaviour can be traced down to software deficiencies.

2.3.3 For vulnerabilities this will be quite different. Just like software bugs, all known vulnerabilities will have to be eliminated with scrutiny commensurate with the level of safety risk they may create or contribute to. The security environment, which is defined as "… *the external security context in which an asset performs its function*" changes constantly, independently and outside of the influence of the aviation community: new threats emerge, new ways to interfere with existing functionalities are discovered, and new vulnerabilities are either reported to manufacturers and/or recorded with public vulnerability databases (https://cve.mitre.org/) and scored. This means new vulnerabilities will become known in multiple ways:

- Unexpected behaviour
- Reporting/Publication by third parties, e.g. of standards or commercial implementations
- Research of own implementations, e.g. in response to new publications

2.3.4 Although the majority of vulnerabilities do not apply to the safety critical or airspace operational systems, the aviation community will have to observe very closely these types of information,

regardless where they are published. Vulnerability management includes, inter alia, the identification of vulnerabilities and resulting risks, and the definition of actions to be taken to remedy the effects commensurate with those risks until a fix has been developed and deployed. This type of activity is well established for "IT" (Information Technology) systems but has not been widely introduced into the "OT" (Operational Technology) systems management environment.

2.3.5 As civil aviation is such a tightly interwoven System-of-Systems, comprising of interconnected products, people, and processes, including connections with military systems, the limitation to the perspective of an individual organisation is insufficient. Thus civil aviation will have to introduce ISMSs with the notion of a shared, trans-organisational management of cyber security, allowing the coordination of measures throughout the sector, taking into account the fact that information is shared within the entire aviation system, and that the same systems are common to many actors in the sector. Some high-level ISMS subjects reaching beyond the boundaries of individual organisations are Information Security Policies, Asset Management, Communications Security, Cryptography, Supplier relationships, and Information Security incident management. Such management systems, preferably aligned or integrated with existing aviation risk management systems, assist both individual organisations and the sector as a whole to better prepare and respond to information security threats.

2.4 **Dependability, Trust, and Confidence –** In the paper "Basic Concepts and Taxonomy of Dependable and Secure Computing"[9], Avizienis et al. propose definitions relating to dependability as well as an associated taxonomy. These terms will be important in order to understand, what needs to be established by technical, organisational or operational means to enable recipients of information to place "trust" or "confidence" into it and the organisation submitting it.

2.4.1 The **Dependability** of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable. It can be said that the dependability of a system should suffice for the dependence being placed on that system. In other words, **dependence** of e.g. System A on System B represents the extent to which system A's dependability is affected by that of System B. An example is a flight crew of an airplane (= System A) depending on the information provided by an ATC Centre (= System B).

2.4.2 **Trust** is the anticipation of one entity in the evaluation of the expected behaviour of another entity. An example is that an originating system does not deliberately provide false information.

2.4.3 **Confidence** is about the level of control and scrutiny, which one entity can factor into the evaluation of the expected behaviour of another entity. An example is the process of initial aircraft certification, where assurance processes, inter alia, allow for a level of scrutiny of the development and integration process commensurate with the airworthiness requirements. It creates the level of confidence with the Certification Authority permitting it to issue the Type Certificate.

2.4.4 There are three levels of confidence/trust when communicating information from one originating system to another receiving system:

a) The confidence that the information is from the alleged originator and that it has not be tampered with. This could be considered as "Digital Trust" or "Technical Trust", as it has to rely only on technical measures of the communication link to assure that confidence. Digital Trust is auditable, as it allows the verification that technical standards are complied with;

[9] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr - Basic Concepts and Taxonomy of Dependable and Secure Computing: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004.

b) The confidence that the infrastructure of a peer organisation (i.e. a "*system*") is resilient against unauthorised or unlawful electronic interference commensurate with the expected service delivery. This could be considered as "Organisational Trust", as it has to rely on organisational measures and technical measures put in place by that organisation. This results in the ability of one organisation to depend upon another organisation. Organisational Trust is auditable, as it allows the verification that process and technical standards are complied with;

c) The trust that the originator of information provides uncompromised information. This could be considered as "Societal Trust", as it relies on only on the anticipation of an expected behaviour. Societal Trust is not auditable.

2.4.5 Discussion of Case a): The common challenge for both areas of confidence (verification of alleged originator; verification of integrity of information) will be the system (organisation including its technical infrastructure) which guarantees the validity of the identity of the originator, expressed by an electronic identification (Digital Certificate) used for the electronic signature of the information exchanged. More information about this mechanism can be found in section 2.6.

2.4.6 Discussion of Case b): The challenge for this area of confidence is with the system (organisation) which approves and oversees (e.g. by audits and inspections) the operation of another system (organisation including its technical infrastructure). It guarantees that the system operates at a particular level of trustworthiness, with respect to the protection of the system against unauthorised or unlawful electronic interference, potentially creating or contributing to a risk of compromised information. More information about this mechanism can be found in section 2.7.

2.4.7 Discussion of Case c): In cases where no controls or scrutiny can be exercised by the aviation community, systems (organisations) may have to trust blindly. On the other hand, past experience in many areas may contribute to the evaluation of a significant level of trust, despite the lack of any hard evidence.

2.4.8 The next three paragraphs will address the two first cases, for which the international aviation community will have to establish standards and recommended practices.

2.5 **Digital or Technical Trust –** A study by Gartner, Inc, about Digital Trust states that it "…underpins every digital interaction by measuring and quantifying the expectation that an entity is who or what it claims to be and that it will behave in an expected manner." This has a few consequences which those, exchanging information of any kind by means of technical systems, will have to bear:

- Every party wishing to be part of a trusted information exchange will need to have a digital identity;

- The level of trust in that party is strongly dependent upon the level of scrutiny of its real identity, being a measure for the assurance of its validity;

- The level of trust in all parties is strongly dependent upon the technology used for the digital identity. Technologies, which are not Quantum-computing resistant, will undermine trust levels;

- Only exchanges between parties having such digital identity will be considered trustworthy;

- Setting-up an information exchange will require the verification of the validity of digital identities (authentication);

- Establishment of an information exchange requires consent by all participating parties (authorisation);

However, the benefits are:

- The integrity of each information exchange can be verified;

- The confidentiality of each information exchange can be assured, if required.

2.5.1 Digital or Technical Trust relies upon cryptographic methods to establish these benefits between parties of the aviation community. And it keeps adversaries out of the communication for the majority of risks. In all clarity it is to be stated that ***all*** Radio Frequency (RF) communication, such as the one by Satellite or VHF, is susceptible to electromagnetic interference, which may not impair the integrity or authenticity of the communication, but which will jeopardise its availability. Thus, Digital or technical Trust is not the Silver Bullet against all technical communication threats.

2.5.2 There are considerations which link Digital or technical Trust to Organisational and Societal Trust. They concern the first three bullets above and are related to the scrutiny of the verification of the real identity as well as to the organisations and systems operated issuing and maintaining the validity of the digital identities.

2.5.3 In all societies, identities of individuals are established and maintained by States, starting with birth certificates and ending with a death certificate. There are equivalents for organisations, which differ slightly between types of organisations and States. As long as communication takes place between individuals or organisations, the level of scrutiny of the validity of the real identity is largely in the hands of state authorities or delegated organisations, and as such subject to Societal Trust. As soon as communication takes place between technical systems, e.g. autonomous command and control communication or uploading of software into a system supplied by its manufacturer, concepts need to be established providing similar levels of validity of the digital identities used. For example, individuals could act as “device sponsors”, to act on behalf of a device whenever a digital identity is to be established or maintained.

2.5.4 Organisations establishing digital identities operate information systems to perform their duties. The level of trustworthiness (see next section) of these information systems is largely dependent upon how well they have been designed, developed, integrated, operated and maintained and how secure integration, operation and maintenance is. In particular for digital identities the process of their decommissioning is equally important. If these systems enjoy a high level of trustworthiness, their digital identities will benefit from it. However, if they fail to be highly trustworthy, the digital identities they established suffer from lower levels of trust, regardless of the level of scrutiny put into their establishment.

2.5.5 A global trust framework will thus be necessary to enable resilient and trustful information exchange between parties of the aviation community. It shall not only define elements of Digital or Technical Trust, but will also have to include those for Organisational Trust, considering the variability of the possibilities of Societal Trust from a global perspective.

2.6 **Trustworthiness –** In civil aviation, a strong framework of confidence has been built over decades. Trustworthiness is a formal concept by which one organisation - or a system it operates - can

rely on the cyber security properties of another organisation - or a system it operates. It can thus be considered as one possible instantiation of *Organisational Trust*. As trust is never absolute, the concept proposes multiple levels of Trustworthiness, which should depend upon the impact (e.g. safety or service continuity, such as expeditious flow of traffic in a region) it will have upon the relying party.

2.6.1 When discussing how trust can be established among organisation, NIST SP 800-39 states: "Organizations are becoming increasingly reliant on information system services and information provided by external organizations as well as partnerships to accomplish missions and business functions. This reliance results in the need for trust relationships among organizations. In many cases, trust relationships with external organizations, while generating greater productivity and cost efficiencies, can also bring greater risk to organizations. This risk is addressed by the risk management strategies established by organizations that take into account the strategic goals and objectives of organizations".

And it continues "*Two factors affecting the trustworthiness of information systems are:*

- *Security functionality (i.e., the security features/functions employed within the system); and*

- *Security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).*"

2.6.2 In aviation there is precedence for these concepts: Design Assurance is required for all aircraft development and integration and provides confidence about the airworthiness. ***Validation*** activities ensure that the *right functionality* has been put in place while ***Verification*** activities ensure that the *functionalities* have been put in place *correctly*. Confidence is based upon these assurance actions, and that they have been performed yielding acceptable results. Those actions have been designed to address – and be commensurate with – the severity of impact of safety risks. Higher levels of severity of impact will thus need higher levels of scrutiny in the development process.

2.6.3 Security assurance has to go yet one step further, as the right functionality being put in place correctly is only a necessary, but not a sufficient condition. Even after adequate scrutiny with respect to known vulnerabilities the potential for the existence of unknown vulnerabilities, or the misuse of intended functionality, still exist. Traditional airworthiness related assurance actions cannot make any statement about this potential. By extending those actions with ***Refutation*** actions, this potential can be evaluated and scored and remedial actions be derived.

2.6.4 Based upon those two factors, a similar concept is proposed for information security properties. It is designed to reflect the effectiveness of protection against cyber threats. Multiple levels of Trustworthiness, attributed to an organisation and the systems it operates, could be defined. Each level would be defined by combining

a) the implementation of security measures against identified information security risks with

b) the assurance that they have been architected and implemented commensurate with the risks they are intended to mitigate.

2.6.5 When two organisations connect their systems and operations thereof the trustworthiness level allows them to evaluate how much confidence each organisation can place into the peering organisation in contributing to its own protection – and then either take measures to compensate shortcomings or help the peering organisation to increase their level of trustworthiness. The latter may be the more cost-effective solution, in particular in complex interconnection arrangements.

2.6.6 In essence, confidence in (a) is primarily about the absence of development errors and vulnerabilities and (b) in organisations adequately protecting civil aviation is what will prepare the future of safe flight. The Trustworthiness concept should be integrated into ISMS, which in turn should be aligned or integrated with existing management systems.

2.7 **Operating Conditions for Cybersecurity** – Aviation is a global operation which constantly evolves. Changes are initiated permanently on organisational, local, national, regional and even global level. Further, transitioning globally to a safe and secure aviation sector will not happen overnight. Thus, special care has to be taken that all constituents of the aviation system migrate in a concerted way through increasing states of cyber security while maintaining seamless interoperability.

2.7.1 So, Trustworthiness Levels provide for one factor of the ability of a third party to evaluate the risk of a communication connection with an organisation and a system it operates. Another factor is about the residual risk that organisation exposes to the third party after applying its security measures. Trans-Organisational Risk Management standards complement these two factors for the final information security evaluation. There are a few limitations associated to this evaluation. First of all, this is a static snapshot in time. However, the dynamics of the evolution of individual organisations and systems they operate, belonging to the globally interoperable, secure infra-structure needs to be covered. Secondly, it requires criteria against which the acceptability of the connection between two organisations can be determined. For every connection between peers it will be essential that Trustworthiness Levels will be compatible among them, consequently requiring the definition of matching pairs. Certain pair combinations of Trustworthiness Levels will be permissible to connect, as they will meet cyber security objectives with acceptable risk levels. Other combinations may fail to meet the objectives.

2.7.2 Two levels of speed of evolution of connections between peers need to be distinguished: the one between organisations which connect their ground systems, and the one between air- or space-based vehicles and ground-based systems, between which the connections transition at a fast pace. Their key discriminator is the speed by which their cyber security condition evolves.

2.7.3 *Slow evolution*: On the one hand, ground systems in general – and ATM/ANS systems in particular - evolve on a comparatively slow pace. Changes in their operating conditions are largely determined by changes either of their own cyber security situation or the one of the systems they are connected to. This allows for a closely coordinated adaptation of cyber security properties – including associated roles and responsibilities – such that all connected parties meet the overall cyber security requirements. Thus, acceptable Operating Conditions could be established by proper pairing of Trustworthiness Levels between connecting organisations and systems. As a side effect, it will create incentives to reach agreements between interconnected organisations about the conditions for matching, yet differing Trustworthiness Levels, ultimately leading to economically balanced approaches. When functionalities change, leading to changed operating risks, Trustworthiness levels may have to be adapted. Also, changes in the notion of the acceptability of risks may be another factor requiring Trustworthiness levels to be adjusted. Previously acceptable pair combinations may no longer be acceptable, leading to modifications to security measure functionalities or assurance requirements by either or both peers.

2.7.4 *Fast evolution*: On the other hand, aircraft are migrating from one location to another at a comparatively high pace, while being connected dynamically to a large number of peers during a short period of time. The challenge here is, that aircraft or ground systems will not be in a one single or matching state of cyber security at any given day. There will be always individual differences due to the differences in the speed of evolution. Those connections could be established by proper pairing of Trustworthiness Levels between connecting systems. However, due to the comparatively high pace, matching Trustworthiness Levels need to be pre-coordinated and maintained a priori as part of

organisational approval and aircraft certification processes. To keep them acceptably secure for operation, the consideration of this evolution on either side will be required.

2.7.5 An example may shed some light of the concept: In the existing concept of Operating Conditions, horizontal separation requirements applicable within one airspace are mandated. A certain equipage of ground and aircraft systems with certain (functional and assurance) properties are needed to meet respective requirements. These properties create matching functional and safety levels, allowing for safe operation. Thus, the existing concept of Operating Conditions could serve as a blue print for cyber security. Adequately paired Trustworthiness Levels between ATM/ANS and aircraft systems would allow for safe and secure airspace use.

2.8 **Information Sharing** – A global ISMS framework could also assist in creating a more coherent information sharing mechanism for cyber security risks. The Information Technology (IT) world has created the concept of a *Cyber Security Centre*, which "handles" information about cyber security incidents, including collecting and maintaining databases of incidents, threats and vulnerabilities, and provides analyses and guidance on successful practices about how to counter the actual incident to its constituencies. These tasks are associated with Information Sharing.

2.8.1 Internationally, Computer Emergency Response Teams (CERTs) and CSIRTs have created a community, called Forum for Incident Response and Security Teams (FIRST). This forum could serve the civil aviation community as a template for a nucleus, for further expansion of its collaboration. While FIRST does not share operational information itself, it enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams. However, this approach will not suffice due to the inter-connectedness of the civil aviation community. It will need a concerted approach towards a global, operational information sharing mechanism with the objective of not only reacting to incidents, but also being increasingly resilient to future attacks. One example: In dealing with the discovery of new vulnerabilities, the information collected by CSIRTs will allow for a the anticipation of emerging risks, consequently allowing community members to take preventive measures to limit detrimental effects on civil aviation. In summary, this objective aims at improving the awareness about cyber-threats. Once aviation CSIRTs coordinate among each other and their respective members, internationally aligned defensive measures against cyber threats will be possible.

2.8.2 Further, cyber security threats exist beyond civil aviation, e.g. in other transport sectors but also non-transport related sectors. They often share technologies and implementations, hence threats and vulnerabilities. It is therefore fundamental to share policies, intelligence information, and best practices with organizations from these sectors. An approach to cyber security in civil aviation should thus benefit from other national or regional cross-sectorial approaches and experiences. Close communication with governmental entities engaged in cyber security of other sectors will enhance the benefits for Civil Aviation Authorities of Contracting States.

2.9 **Reporting and Notification** – While industry has developed models of voluntary information sharing, States often rely on mandatory reporting or notification. There are a number of differences between the two models, which sometimes create sharp discriminations. One example highlights a difference in information handling: Information Sharing uses the so called Traffic Light Protocol (TLP), which determines "*how widely originators want their information to be circulated beyond the immediate recipient.*" It is at the originators discretion to share or not to share – and when to share – information. States often combine principles of Information Classification to identify sharable information for a particular group of recipients with the need-to-know principle, to determine who will be the ultimate recipient.

2.9.1 ICAO Annex 13 requires Contracting States to establish mandatory and voluntary reporting systems. The objective of mandatory incident reporting systems is to "*facilitate collection of information on actual or potential safety deficiencies*". To capture also other deficiencies, which the mandatory reporting system does not capture, the voluntary reporting system "*shall be non-punitive and afford protection to the sources of the information*". The collected information is then analysed to determine patterns or systemic deficiencies. From this knowledge preventive actions can be derived. Obviously, this is a longer term process, which has no immediate operational impact. Further to that, ICAO requirements relating to the implementation of safety management systems (SMS) require that aviation service providers develop and maintain a formal process for effectively collecting, recording, acting on and generating feedback about hazards in operations, based on a combination of reactive, proactive and predictive methods of safety data collection.

2.9.2 A similar approach is taken by some regional or national regulations for other areas of commercial services. Taking European Union as an example, the Directive on security of network and information systems (NIS-Directive)[10] requires operators of essential services to notify their competent authority about "significant incidents". Similar objectives as for safety incident reporting schemes apply. However, the NIS-D also introduces a network of Computer Security Incident Response Teams (CSIRTs), which is established to "*contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation*". On the national level CSIRTs will collaborate with the Operators of Essential Services to detect cyber security events and to minimise the impact of cyber security incidents.

— END —

[10] 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 UnionOJ OJ L 194, 19.7.2016, p. 1–30