International Civil Aviation Organization

AN-Conf/13-WP/42
28/8/18

WORKING PAPER

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

STRENGTHENING CONCEPTS FOR CYBER SECURITY 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 will briefly introduce the rationales why organisations should manage their individual cyber security risks, products and services by means of an Information Security Management System (ISMS), which takes into account the risks related to the organisation's interactions with other organisations or systems they operate.

The paper also focuses on trustworthiness, why it is needed and which benefits it provides to organisations to use an ISMS. In addition, the paper will also address why an equivalent level of cyber security performance, independent of time and location, of connecting systems is a crucial pre-requisite and how this can be achieved for ground/ground or air/ground operations.

The paper further introduces into a common perspective of criticality for aviation and the benefits of information sharing.

Action:
The Conference is invited to agree to the recommendations in paragraph 3.

1. INTRODUCTION

1.1 The availability of accurate information and the correct functioning of safety-critical systems are pre-requisites for a safe and secure civil aviation as the sector encounters further

[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.

digitalization. The aviation system is highly integrated and information travels globally. Therefore, a holistic and end-to-end approach must be taken to cyber security initiatives in the aviation sector.

1.2 This paper highlights the advantages of the introduction of Information Security Management Systems (ISMS) in the aviation sector. 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.

1.3 A common management system approach allows the coordination of measures throughout the sector, taking into account the fact that information is shared, that the same systems are common to many actors in the sector and that risks are shared.

1.4 In addition to an ISMS approach, this paper also elaborates on the notion of trust. In the aviation sector, trust - in addition to confidence - in each partner is paramount. A robust system of training, certification, oversight and double-checks ensures that for each flight, all partners traditionally had confidence in each other to fulfil their part of the aviation chain conscientiously and correctly.

2. DISCUSSION

2.1 **How to take advantage of an ISMS** - Existing concepts of ISMS are inherently limited to individual organisations. Civil aviation, however, is such a tightly interwoven system-of-systems, comprising of interconnected products, people, and processes, including even connections with military systems[3], that an individual organization perspective is insufficient. As such, civil aviation will have to introduce ISMS with the notion of trans-organisational management of cyber security.

2.2 A globally coordinated ISMS approach is thus a key enabler for the civil aviation sector. Such a global framework would facilitate the coherent implementation of a number of supporting concepts, such as a globally interoperable and secure communication infrastructure, as well as a trust framework or other concepts to allow a future system based on the trustworthy exchange of information. As such future will not be built at one single time, individual evolution of organisations, States or regions will need to be facilitated. The existence of ISMS in all organisations will be pre-requisite to make those concepts a reality. Implementations of ISMS should be aligned with the existing management systems for safety (e.g. Annex 19 — *Safety Management*) and aviation security risk management and ICAO provisions and industry standards as well as effective oversight mechanisms.

2.3 **The trustworthiness concept** - In civil aviation, a strong framework of confidence has been built over decades. Trustworthiness is now 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[4]. As trust is never absolute, the concept proposes multiple levels of trustworthiness, which should depend upon the impact (safety or service continuity, e.g. expeditious flow of traffic in a region) it will have upon the relying party.

2.4 For example, in aircraft certification most confidence about the airworthiness is derived from the assurance that the appropriate actions have been performed yielding acceptable results. Those actions have been designed to address the severity of impact of safety risks. Higher levels of severity of impact will need higher levels of scrutiny in the development process. For cyber security properties a similar concept is proposed. It is designed to reflect the effectiveness of protection against cyber threats. In essence, confidence in the absence of development errors and vulnerabilities and in organisations adequately protecting civil aviation is what will prepare the future of safe flight. The trustworthiness

[3] AN-Conf/13-WP/39 refers

[4] Information Paper (AN-Conf/13-WP/160) will explain the concepts, and principles of ISMS, the Trustworthiness and Cyber Security Operating Conditions concepts, as well as the benefits of Information Sharing

concept should be integrated into ISMS, which in turn should be aligned or integrated with existing management systems.

2.5 **Cyber security operating conditions** - To take full advantage of the trustworthiness concept, the dynamics of the evolution of individual organisations and systems they operate, belonging to the globally interoperable, secure, infra-structure, needs to be covered as well. Pre-specified cyber security operating conditions are one way to address the challenge. 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. This will create incentives to reach agreements between peers about the conditions for compatible, yet diverging trustworthiness levels, which will ultimately lead to balanced approaches. Two levels of migration of connections between peers need to be distinguished: the one between organisations which connect their systems, and the one between air or space based vehicles and ground-based systems, which transition between connections at a fast pace. Their key discriminator is the speed by which their cyber security condition evolves

2.6 Slow evolution: On the one hand, ground systems in general – and air traffic management (ATM)/air navigation services (ANS) in particular - evolve on a comparatively slow pace. Changes in their operating condition is largely determined by changes either of their own cyber security posture or the one of the systems they are connected to. This allows for a closely coordinated adaptation of cyber security properties such that all connected parties meet the overall cyber security requirements. The concept of operating conditions is addressing the proper pairing of trustworthiness levels between connecting organisations.

2.7 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. Generally speaking, aircraft or ATM/ANS systems will not be in a matching state of cyber security at one given day. To keep them operational, migration on either side will be required. For cyber security the adaptation of the concept of operating condition could provide a response. For example, in the existing concept of operating conditions, horizontal separation requirements applicable within one airspace mandate a certain equipage of ground and aircraft systems to meet these requirements. Thus the concept of operating conditions could serve as a blue print for cyber security, responding to the requirements with respect to cyber security properties introduced by trustworthiness levels. Adequately paired trustworthiness levels between ATM/ANS and aircraft systems would allow for safe and secure airspace use.

2.8 **Information sharing on cyber aspects** – Another aspect to be considered as part of an ISMS is the sharing of information. A global ISMS framework could also assist in creating a more coherent information sharing mechanism on 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, provide analyses and guidance on successful practices about how to counter the actual incident to its constituencies. These tasks are associated with information sharing.

2.9 Internationally, Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) have created a community, called the Forum for Incident Response and Security Teams (FIRST). This forum could serve the aviation community as a blueprint for a concerted approach towards global information sharing with the objective of not only reacting to incidents, but also preventing future attacks becoming successful. In dealing with the discovery of new vulnerabilities, the information collected by CSIRTs will allow for a certain anticipation of emerging risks and consequently take preventive measures to limit detrimental effects on civil aviation. In summary, this objective aims at improving the awareness about cyber-threats and vulnerabilities of aviation systems. Once aviation CSIRTs coordinate among each other and their respective members, internationally aligned mitigation and defensive measures against cyber threats will be possible.

2.10 Cyber security threats exist beyond civil aviation, e.g. in other transport sectors but also non-transport related sectors (e.g. banking system, nuclear industry). 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. Further, close communication with governmental entities engaged in cyber security of other sectors will enhance the benefits for the Civil Aviation Authorities of States.

3. CONCLUSION

3.1 The Conference is invited to agree on the following recommendations:

That the Conference:

a) urge ICAO to support States to require organisations to manage cybersecurity risks of their operations, products and services, including their interfaces to peers, by means of an Information Security Management System (ISMS), based upon international industry standards and preferably aligned or integrated with existing management systems;

b) request ICAO to encourage States to take appropriate measures such that globally interoperable infrastructure is in place, resilient against cyber-attacks. It shall meet interoperability and cyber security requirements to reinforce the holistic and higher-level goals with respect to safety and the expeditious flow of traffic;

c) urge ICAO to develop, following a multi-disciplinary approach, provisions for inter-organisational trust, as part of a wider broader trust framework, and to encourage their implementation;

d) request ICAO to encourage States to take measures, such that aviation operators establish and facilitate information sharing of operational cybersecurity related information through the appropriately designated channels, such as a global network of "trusted organisations";

e) urge ICAO to facilitate the development of provisions for trustworthiness and cyber security operating conditions to allow such globally interoperable infrastructure to be securely operated;

f) request ICAO to encourage States to expand existing or establish new reporting channels, for cybersecurity related facts, to better address new risks to aviation safety and security and to ensure the expeditious flow of traffic; and

g) request ICAO to call upon States to promote cross-sectoral governmental and non-governmental collaboration on cyber security between aviation domains and other domains.

— END —