International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/270
28/9/18
English, Arabic, Chinese[1]**,**
French, Russian and Spanish only[2]

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

SYSTEM-OF-SYSTEMS NOTION OF CYBERSECURITY IN AVIATION

(Presented by Canada, Austria on behalf of the European Union and its Member States[3], and the other Member States of the European Civil Aviation Conference[4], EUROCONTROL, Singapore, and co-sponsored by Australia and New Zealand)

EXECUTIVE SUMMARY

This paper will briefly introduce the concept of a system-of-systems, and establishes why such an approach would be suitable in the context of addressing cybersecurity considerations in civil aviation. This paper will also introduce the notion of security-by-design, and how the integration of this concept within the aviation system will improve its resilience.

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 system as the sector encounters further digitalization. The aviation system is highly integrated and information travels globally. Therefore, cybersecurity initiatives in the aviation sector must take a holistic and end-to-end approach.

[1] Chinese version provided by Singapore.

[2] English, Arabic, French, Russian and Spanish versions provided by Canada.

[3] 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.

[4] 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.

1.2 A holistic, end-to-end approach can only be successful if aviation is understood as a "system-of-systems", for which all members of the aviation community share responsibility. The aviation system is made up of a variety of networks and devices that are becoming increasingly connected and mutually dependent for the exchange of digital data and information, while aviation stakeholders such as States, aircraft and aerodrome operators, air navigation service providers (ANSPs) and others have come to rely on interconnected and interoperating information and communications technology (ICT) systems for their day-to-day operations.

1.3 Developments such as system-wide information management (SWIM), the introduction of remotely piloted aircraft systems (RPAS) and the emergence of future airspace users and stakeholders that are not yet operational further reinforce this interdependency. The aviation system of the future thus requires more concerted design and less individual evolution to maintain its resilience against cyber interference.

1.4 The evolution towards interconnected and interoperating information systems mentioned above also brings new vulnerabilities. Cyber-related events can impact aviation on many levels and can jeopardize the performance of the air navigation system and endanger the overall safety of the sector. These events can influence information exchanges between stakeholders, directly affecting safety, security, capacity and efficiency with potentially severe repercussions.

2. DISCUSSION

2.1 **Aviation as a system-of-systems (SoS)** – in the aviation sector, many stakeholders, both direct and indirect, play a role in the functioning and maintenance of individual sub-systems and the system as a whole – with the understanding that a system can be comprised of products, people and processes. Each of these sub-systems draw directly from other sub-systems in order for them to function smoothly and efficiently; conversely, each of these sub-systems also has a significant impact on the others when it is unable to function correctly.

2.2 These sub-systems today are designed, integrated, operated and managed independently of each other, and evolve at their individual paces, leading to an overall evolutionary process that is challenging to predict and pin down deterministically. Since aviation stakeholders have a total system responsibility for the overall product, the consideration of aviation as a SoS is all the more important. Responsibility for the functioning of the aviation system therefore includes both direct stakeholders, such as aircraft and aerodrome owners/operators and ANSPs, as well as indirect stakeholders, such as States and equipment manufacturers / designers.

2.3 Given that these sub-systems serve individual functions that are chained together to achieve common objectives (e.g. communications between air traffic control and pilots, or location tracking data between aircraft operation control centres and aircraft), compromising any of these sub-systems would adversely affect the overall functionality of the entire chain of sub-systems. As such, cybersecurity risk management will need to be addressed using a holistic approach in order to reduce the reachability of threat actors to core functionality.

2.4 **Cybersecurity: an ongoing, evolutionary consideration -** given the evolutionary nature of SoS described above, cybersecurity must similarly be an ongoing consideration among the many stakeholders in the aviation SoS. It is also imperative that the aviation SoS maintains its required cybersecurity conditions by means of sufficient flexibility and adaptability when its components permanently interact in a variety of manners with each other (e.g. aircraft interacting with different air navigation service providers as they transit through different flight information regions).

2.5 Therefore, the development and maintenance of such cyber resilience across the SoS require continued coordination among all stakeholders (see paragraph 2.2), in order to maintain the desired flexibility and adaptability needed for the aviation SoS to function correctly.

2.6 An important challenge to address in pursuit of this objective is the concept of "composability" – the ability to integrate multiple elements (components for systems, or subsystems for SoS) into bigger entities securely. The key challenge here is the departure from the safety paradigm, in which the integration of elements focused primarily upon their functionality and interactions across common interfaces. From the cybersecurity perspective, the integration of individual elements also requires careful consideration of how cybersecurity postures of each element contributes to the overall cybersecurity state. A key question that will arise in this pursuit includes how to support States and regions (and other individual stakeholders) in their development journeys such that the SoS can be effectively protected from cybersecurity attacks, despite the inevitable variance that will exist between sub-systems.

2.7 In achieving the above goal, the integration of individual sub-systems will require careful consideration and integration of native security environments for each sub-system, to the extent that a holistic and cyber resilient environment emerges. Uncoordinated approaches to cybersecurity could either lead to undetected vulnerabilities in protection; overlaps in perceived system defences are just as dangerous, since that scenario would still potentially result in a viable attack surface for the aviation SoS.

2.8 Therefore, a globally coordinated approach to managing system interactions is essential, and core to that objective is a common view of how these systems and sub-systems interact.

2.9 **Integrating security-by-design for aviation systems –** in order for the aviation SoS to achieve its desired level of cyber resilience, it is important for cybersecurity considerations to be incorporated from the beginning of system development, as opposed to being considered retroactively. This would also allow for interfacing considerations between sub-systems to be taken into account, such that these interactions would also take place in a secure and efficient manner.

2.10 Most current security standards focus on mitigating measures taken and implemented *within* the organisational context – there is a pressing need to adjust the focus of such measures to include and account for measures that must be taken from the inter-organisational perspective as well. This allows for the assurance of overall SoS security, over and above security arising from an amalgamation of sub-systems which are individually secured.

2.11 Without appropriate management, uncoordinated cybersecurity approaches of aviation sub-systems can pose a risk to the system as a whole. This lack of coordination also potentially stems from insufficient communication between sub-system managers and other relevant stakeholders during the development and design of cybersecurity approaches.

2.12 Through multiple layers of coordination (e.g. between States as managers of domestic aviation systems, managers of sub-systems within domestic aviation systems, etc.) across different levels of sub-systems, as well as ensuring that individual sub-systems are effectively protected in their own right, States would be contributing to an aviation SoS that maintains defence-in-depth as a natural outcome of such work.

2.13 **Future work** – Such work in incorporating security-by-design as part of initial system design should not replace the best practices honed by the aviation community through many decades of experience in developing aviation systems and working on cybersecurity challenges. By incorporating such principles alongside and complementary to the traditional focus on system redundancy as well as the emphasis on maximising ease of access to operational data and systems, stakeholders will further strengthen the aviation SoS in its cyber resilience policies, while maintaining operational effectiveness.

2.14 As part of the variety of operational concepts and solutions being discussed at various aviation fora today, it is important for States and industry to take the above considerations into account through the development and design process. By extension, the community may also evolve its collective work to further identify representative sub-systems and research to which extent its results – based upon the measures taken and the practices used – can be transferred to other sub-systems to improve cyber resilience across the board.

2.15 Similarly, following success in this arena, the aviation community may consider working to initiate the further development of increasingly larger sub-systems, which take information security into consideration during their initial design phase. As such work progresses and matures, stakeholders may begin to collectively explore whether there exist suitable and trusted candidates to be tasked with responsibility in developing and maintaining such systems which are secure-by-design, and the feasibility of such processes in the aviation system of the future.

2.16 Through continued investment and dedication of efforts in the area of system cyber resilience, the aviation community will contribute effectively to the safe and efficient operation of the aviation ecosystem ("SoS") well into the future.

3. CONCLUSION

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

That the Conference:

a) urge ICAO and States to acknowledge that the cyber resilience of the aviation system depends on continued coordination among all relevant stakeholders;

b) request ICAO to acknowledge the concept of SoS, requiring the necessity of collaboration and coordination among managers of sub-systems, in particular when developing, integrating, operating and maintaining subsystems that are "secure by design";

c) urge ICAO to develop a framework that requires and guides States to implement measures to mitigate the cyber threat and risk to civil aviation systems. This may result in the development of SARPs for several affected ICAO Annexes; and

d) recognize the concepts contained in Information Paper: "*Considerations about Cybersecurity in Aviation*".

— END —