International Civil Aviation Organization

AN-Conf/14-WP/113[1]
28/6/24

WORKING PAPER

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 4: Hyper-connectivity of air navigation system
4.2: Cybersecurity and information system resilience

CYBERSECURITY – RISK MANAGEMENT AND INVENTORY OF CYBER INFORMATION ASSETS IN AIR NAVIGATION SERVICES (ANS)

(Presented by Chile and co-sponsored by 20 Member States of the Latin American Civil Aviation Commission (LACAC)[2])

EXECUTIVE SUMMARY

This paper presents general cybersecurity guidelines to be considered by air navigation services (ANS) in order to address the current threats to the technological systems used in this area. The constant exchange of information renders such systems potential targets for a cyberattack.

The circumstances result from the functional structure of the aviation system, including the civil aviation authorities, air navigation services providers (ANSPs), airport operators, and any other relevant organizations.

Action: The Conference is invited to:

a) promote the development of a risk management plan for the ANS that enables any cybersecurity threats to be identified and mitigated during the design, installation and operation of the required networks and systems;
b) promote features which facilitate risk management, such as the implementation of a single, integrated registry for each cyber asset identified in the ANS, and which enable threats to be identified, with priority levels for action, maintenance and rapid recovery of the system, if necessary; and
c) renew the commitment to continuous improvement of the various processes, including those designated as critical, in order to achieve optimal cybersecurity levels in the ANS.

1. INTRODUCTION

1.1 The technological change implemented within the various organizations throughout society results in the increasing exposure of these organizations to cyber delinquency. The provision of air navigation services (ANS) is not immune to this problem either, and therefore there is impetus to develop

[1] Spanish version provided by Chile.
[2] Argentina, Aruba, Belize, Brazil, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay and Venezuela (Bolivarian Republic of)

strategies and establish protective barriers against this latent, growing threat, which could potentially affect optimum levels of operational security.

1.2 The need to develop risk management methods for the identification and mitigation of any cybersecurity threat to the ANS system necessitates a renewed commitment to ensuring continuous improvements to the various processes, including those designated by the organization as critical.

1.3 A cybersecurity policy developed by the ANS should consider the complete aviation system life cycle and include elements such as cybersecurity culture, the promotion of security by design, supply chain security for IT programmes and equipment, data integrity, appropriate access control, proactive vulnerability management, improved system update times, and the incorporation of data monitoring systems and processes.

2. DISCUSSION

2.1 The aim of achieving a globally interoperable navigation system presupposes shared networks and IT infrastructures, architectures and network-centric operations. The information exchange of the future will not be limited to point-to-point communications, but will also use the architecture of open systems and Internet-based information flow. All of this increases system vulnerability to a cyberattack.

2.2 Cybersecurity implementation in ANS must consider the protection and resilience of the networks, systems and their operational continuity, confidentiality, integrity and the availability of information. The latter requires analysis of operational impacts and of the system life cycle.

2.3 A cyber incident is defined as any event compromising the availability, authenticity, integrity or confidentiality of the systems, or of the stored, transmitted or processed data, or of the corresponding services offered by the information systems and their infrastructure, which may affect their normal operation.

2.4 The ANS are exposed to a range of cyberthreats such as information inundation, passive interception of information, active interception of information, modification of system configurations or data, destruction of system configurations, interruption attacks or denial-of-service attacks, and others.

2.5 The ANSPs should identify the logical and physical supports of the critical information systems used in their operations and consider the degree of impact thereon in the event they are damaged or interrupted.

2.6 Measures to protect critical information systems should be implemented as early as possible in the design phase to ensure that they are as resilient as possible to cyberattacks.

2.7 Infrastructure security measures should consider security by design, network separation and remote access.

2.8 Security measures in the supply chain for physical and logical supports should consider the periodic updating of aviation Information and Communication Technology (ICT) systems required because of changes in operational requirements and the modernization of logical supports.

2.9 The implementation of a risk management plan for ANS requires, at a minimum, the identification of the air traffic management (ATM) cyber assets and the definition of classification levels for incidents, hazards and system impacts.

	DESCRIPTION OF PROCESSES							
Strategic product	Process	Sub-process	Asset name	Identifier or Code	Type	Location	Person responsible / Owner	Support

				CRITICALITY ANALYSIS			
Storage medium	Retention time	Disposal	Search criterion	Confidentiality	Integrity	Availability	Criticality

Figure 1. ATM cyber asset identification and inventory chart

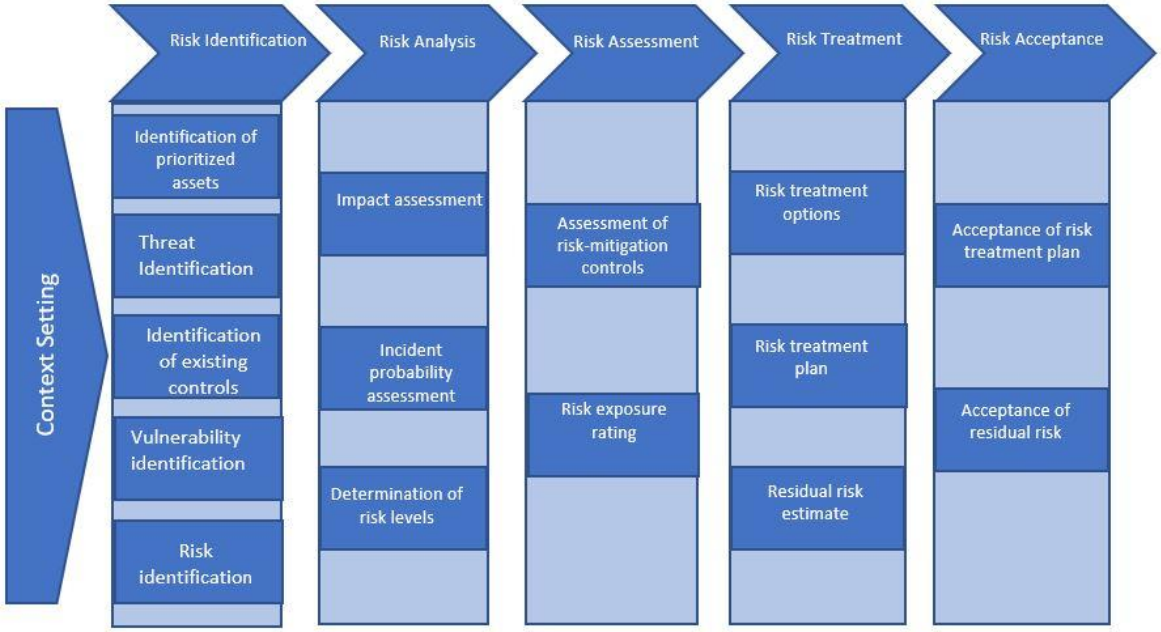

Figure 2. Risk management map

ASSET ID	Vulnerability	Susceptibilty						Risk																		
								Probability of occurrence									Impact									
								Threat agent factors				Vulnerability factors					Technical factors					Business fac				
		Identity fraud (Authenticity)	Manipulation (Integrity)	Rejection (No Rejection)	Information disclosure (Confidentiality)	Denial of service (Availability)	Privilege escalation (Authorization)	Skill level	Motivation	Opportunity	Size	Ease of discovery	Ease of exploitation	Awareness	Intrusion detection	**Total probability of occurrence**	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of responsibility	Overall technical impact	Financial loss	Reputational damage	Non-compliance	
ASST 17	Description of vulnerability	S	T	R	I		E	9	4	4	3	4	3	3	4	**4.25**	2	2	2	2	**2**	6	3	3	
ASST 17		S	T			I	D	E	4	4	7	4	4	4	7	4	**4.75**	4	4	3	3	**3.5**	3	4	4	
ASST 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	7	7	0	0	**3.5**	0	0	0	
ASST 16 & 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	**6.75**	2	2	2	2	**2**	2	2	2	
ASST 17		S	T			I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	
ASST 16 & 17		S	T			I	D	E	0	0	0	0	0	0	0	0	**0**	0	0	0	0	**0**	0	0	0	

Figure 3. Risk analysis and vulnerability chart for identified assets

2.10 The drafting of a risk management plan should make it possible to anticipate the consequences arising from threats such as cyber attacks and non-hostile cyber incidents based on an analysis and assessment of the risks to which the networks and systems are exposed, in order to avoid or reduce the number of such occurrences. Possible impacts can be mitigated by specifying immediate actions and progressive improvement measures with their respective indicators, controls and documentation.

2.11 One element that should be considered for the facilitation of risk management is a single registry for each ATM cyber asset identified. This will make it possible to:

a) group cyber assets of the same type and/or life cycle;

b) ensure data integrity;

c) promote the success of actions for maintaining system resilience;

d) prevent the duplication or obsolescence of the elements; and

e) reduce the effort required for analysis and decision-making.

3. CONCLUSION

3.1 The need to implement cybersecurity strategies to counter digital threats to the provision of ANS requires providers of such services to outline plans and work protocols in order to protect the systems and related infrastructure, and ensure that they are sufficiently resilient to maintain the *confidentiality, integrity and availability* of the information.

3.2 In light of the above, and in the context of the ICAO Cybersecurity Action Plan, the Conference is invited to agree:

that the ANSPs should:

a) develop a cyberthreat risk management plan considering, at a minimum, the identification of ATM cyber assets, incident classification, hazard level classification, the degree of impact on the system and system recovery protocols;

b) consider facilitating factors within risk management, such as the design of a single registry for each interoperable ATM cyber asset; and

c) renew the commitment to continuous improvement of the various processes, including those designated as critical, in order to achieve optimal cybersecurity levels in air navigation services (ANS).

— END —