国 际 民 用 航 空 组 织

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

工 作 文 件

第十四次空中航行会议

2024 年 8 月 26 日至 9 月 6 日，加拿大蒙特利尔

议程项目 **4：** 空中航行系统的超联通

4.2： 网络安全和信息系统的韧性

网络安全 — 空中航行服务（ANS）中网络信息资产的风险管理和盘点

（由智利提交，并由拉丁美洲民航委员会（LACAC）20 个成员国[2]共提）

执行摘要

本文介绍了空中航行服务（ANS）应考虑的一般网络安全准则，以应对该领域使用的技术系统当前面临的威胁。连续不断的信息交换使此类系统易成为网络攻击的潜在目标。

这些情况是由航空系统的职能结构造成的，包括民航当局、空中航行服务提供者（ANSP）、机场运营人和任何其他相关组织。

行动：请会议：

a) 推动制定空中航行服务风险管理计划，使得在设计、安装和运行所需网络和系统期间能够识别和减轻任何网络安全威胁；

b) 推动有助于风险管理的做法，例如对于空中航行服务查明的每项网络资产实施单一的综合登记，并有助于识别威胁，附带行动的优先级别，维护并在必要时快速恢复系统；和

c) 重申对持续改进各流程的承诺，包括那些被指定为关键的流程，以便实现空中航行服务的最佳网络安全水平。

[1] 西班牙文版本由智利提供。

[2] 阿根廷、阿鲁巴、伯利兹、巴西、哥伦比亚、哥斯达黎加、古巴、多米尼加共和国、厄瓜多尔、萨尔瓦多、危地马拉、洪都拉斯、牙买加、墨西哥、尼加拉瓜、巴拿马、巴拉圭、秘鲁、乌拉圭和委内瑞拉玻利瓦尔共和国

1. 引言

1.1 在全社会的各不同组织内实施的技术变革导致这些组织越来越暴露于网络不法行为之下。提供空中航行服务（ANS）也不能幸免于此，因此，有必要制定战略并建立保护屏障，以抵御这种日益增长的潜在威胁，这种威胁可能会影响最佳的运营安全水平。

1.2 需要开发风险管理方法，以识别和减轻对 ANS 系统的任何网络安全威胁，因此需要重申对确保持续改进各项流程的承诺，包括组织指定为关键的流程。

1.3 ANS 制定的网络安全政策应考虑整个航空系统生命周期，并包括以下要素：网络安全文化、通过设计促进安全、IT 方案和设备的供应链安全、数据完整性、适当的访问控制、积极主动的漏洞管理、改进系统更新时间以及纳入数据监控系统和流程。

2. 讨论

2.1 实现全球可互操作的导航系统这一目标的前提假设是共享网络和 IT 基础设施、架构和以网络为中心的运行。未来的信息交换将不仅限于点对点通信，还将使用开放系统的架构和基于互联网的信息流。所有这些都增加了系统对网络攻击的脆弱性。

2.2 在 ANS 中实施网络安全必须考虑网络、系统的保护和韧性及其运行的连续性、信息的保密性、完整性和可供性。后者要求对运营影响和系统生命周期进行分析。

2.3 网络事件被界定为任何可能有损系统、或所存储、传输或处理的数据、或信息系统及其基础设施提供的相应服务的可供性、真实性、完整性或保密性，从而可能影响其正常运行的事件。

2.4 ANS 面临一系列网络威胁，例如信息泛滥、被动拦截信息、主动拦截信息、修改系统配置或数据、破坏系统配置、中断攻击或服务瘫痪攻击等。

2.5 ANSP 应确定其运行中使用的关键信息系统的逻辑和物理支持，并考虑如果这些系统遭到破坏或中断，对其的影响程度。

2.6 在设计阶段就应尽早实施保护关键信息系统的措施，以确保它们尽可能具有抵御网络攻击的韧性。

2.7 基础设施安全措施应从设计、网络隔离和远程访问等方面考虑安全性。

2.8 用于物理和逻辑支持的供应链安全措施应考虑到由于运行要求的变化和逻辑支持的现代化而需要定期更新航空信息和通信技术（ICT）系统。

2.9 实施 ANS 风险管理计划至少需要查明空中交通管理（ATM）网络资产，并界定征候事件、危害和系统影响的分类级别。

	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

图 **1.** 查明和盘点空中交通管理网络资产图表

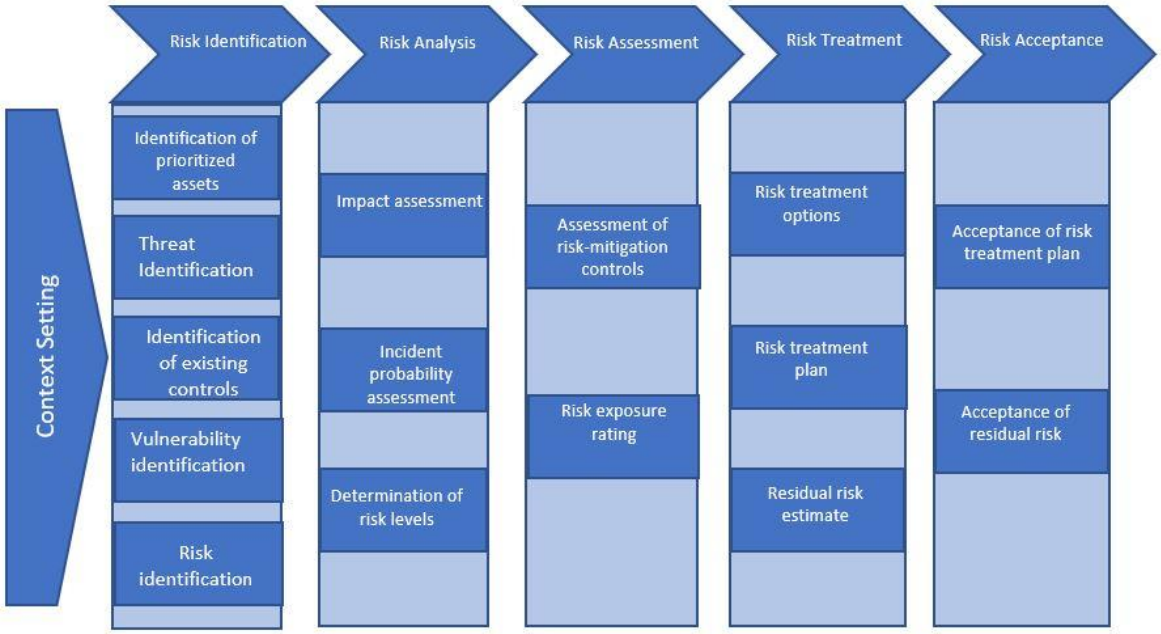

图 **2.** 风险管理图

		Susceptibilty						Risk																				
								Probability of occurrence									Impact											
								Threat agent factors				Vulnerability factors					Technical factors					Business fac						
ASSET ID	Vulnerability	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				

图 **3.** 已查明资产的风险分析和脆弱性图表

2.10 起草风险管理计划应使得可根据对网络和系统所面临风险的分析和评估，预见网络攻击和非敌对网络事件等威胁所产生的后果，以避免或减少此类事件的发生次数。通过规定即刻行动和逐步改进措施并附有各自的指标、控制措施和记录，可以减轻可能的影响。

2.11 为便于风险管理，应考虑的一个因素是为每个已查明的 ATM 网络资产进行单一的登记。这将能够：

a) 对相同类型和/或生命周期的网络资产进行分组；

b) 确保数据完好性；

c) 促进维持系统韧性的行动取得成功；

d) 防止要素重复或过时；和

e) 减少分析和决策所需的工作量。

3. 结论

3.1 需要实施网络安全战略以应对提供空中航行服务的数字威胁，这要求此类服务的提供者制定计划和工作规程，以保护系统和相关基础设施，并确保它们具有足够的韧性，以保持信息的保密性、完好性和可供性。

3.2 鉴于上述情况，并在国际民航组织网络安全行动计划的背景下，请会议同意：

空中航行服务提供者应：

a) 制定网络威胁风险管理计划，至少考虑查明ATM网络资产、征候事件分类、危害等级分类、对系统的影响程度和系统恢复规程；

b) 考虑在风险管理中的促进因素，例如为每个可互操作的ATM网络资产设计单一的登记；和

c) 重申对于持续改进各流程的承诺，包括被指定为关键的流程，以便实现空中导航服务（ANS）的最佳网络安全水平。

— 完 —