



国际民用航空组织

工 作 文 件

AN-Conf/13-WP/270

28/9/18

仅有中文¹、阿拉伯文、英文、
法文、俄文和西班牙文²

(Chinese, Arabic, English,
French, Russian and Spanish
only)

第十三次空中航行会议

2018年10月9日至19日，加拿大，蒙特利尔

委员会 A

议程项目 5： 正在出现的问题

5.4： 网络抵御能力

航空网络安全中的“各系统组成的系统”的概念

（提交方：加拿大、奥地利代表欧盟及其成员国³、欧洲民用航空会议⁴其他成员
国、欧洲空中航行安全组织以及新加坡。

联署方：澳大利亚和新西兰）

执行摘要

本文件将简要介绍“各系统组成的系统”的概念，并阐明为什么这种方法适用于处理民用航空中的网络安全考虑因素。本文件还将介绍设计安保特性的概念，以及将这一概念整合到航空系统中将如何提高其抵御能力。

行动：请会议同意第3段中的建议。

¹ 中文版本由新加坡提供。

² 阿拉伯文、英文、法文、俄文和西班牙文版本由加拿大提供。

³ 奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典和联合王国。

⁴ 阿尔巴尼亚、亚美尼亚、阿塞拜疆、波斯尼亚和黑塞哥维那、格鲁吉亚、冰岛、摩尔多瓦共和国、摩纳哥、黑山、挪威、圣马力诺、塞尔维亚、瑞士、前南斯拉夫的马其顿共和国、土耳其和乌克兰。

1. 引言

1.1 随着航空部门进一步实现数字化，随时提供准确信息以及对安全极其关键的系统的正常运行，是安全可靠的民用航空系统的先决条件。航空系统高度集成，信息在全球范围内传输。因此，航空部门的网络安全举措必须采取整体和端到端的方法。

1.2 只有航空被理解为“各系统组成的系统”，航空界的所有成员都对此系统共担责任，整体的端到端的方法才能取得成功。航空系统由各种网络和设备组成，这些网络和设备日益互联互通并相互依赖，以便交换数字数据和信息，而航空利害攸关方，如国家、航空器和机场运营人、空中航行服务提供者（ANSP）和其他方已经开始依赖互联和互操作的信息和通信技术（ICT）系统来进行日常运营。

1.3 各方面的发展，如全系统信息管理（SWIM）、遥控驾驶航空器系统（RPAS）的引入以及尚未投入运营的未来空域用户和利害攸关方的出现，进一步加强了这种相互依赖性。因此，未来的航空系统需要更加协调一致的设计和更少的各自为阵的演变，以保持其抵御网络干扰的能力。

1.4 朝着上述互联和互操作的信息系统的演变，也带来了新的脆弱性。与网络有关的活动可能在很多层面上影响航空，并可能破坏空中航行系统的性能并危及该部门的整体安全。这些事件可能影响到利害攸关方之间的信息交换，直接影响安全、安保、容量和效率，并可能产生严重后果。

2. 讨论

2.1 航空作为“各系统组成的系统”（SoS）— 在航空领域，许多利害攸关方，无论是直接还是间接地，都在各单独子系统和整个系统的运行和维护中发挥作用 — 基于的理解是，系统可以由产品、人员和流程组成。这些子系统中的一个都直接从其他子系统中获取信息，以使它们平稳高效地运行；反过来，当这些子系统无法正常运行时，每个子系统对其他子系统也会产生重大影响。

2.2 如今，这些子系统的设计、集成、运行和管理彼此独立，并以各自的速度演化，导致整体演化过程难以精准地预测和确定。由于航空利害攸关方对整个产品负有全部系统责任，因此将航空视为“各系统组成的系统”更为重要。因此，航空系统运作的责任包括直接利害攸关方，如航空器和机场所有人/运营人和空中航行服务提供者，以及间接利害攸关方，如国家和设备制造商/设计者。

2.3 鉴于这些子系统提供单独的功能，而这些功能又链接在一起以实现共同的目标（例如空中交通管制和飞行员之间的通信，或航空器运行控制中心与航空器之间的位置跟踪数据），这些子系统中的一个受到损害，都会对整个子系统链的整体功能产生不利影响。因此，需要使用整体方法来解决网络安全风险管理问题，以降低威胁的实施者进入核心功能的可能性。

2.4 **网络安全：一种持续和演变的考量** — 鉴于上述“各系统组成的系统”的演变性质，网络安全必须同样是航空“各系统组成的系统”中许多利害攸关方持续考虑的问题。当航空“各系统组成的系统”的组件以各种方式永久地互动时，航空“各系统组成的系统”还必须通过足够的灵活性和适应性来维持其所需的网络安全条件（例如，航空器在通过不同的飞行情报区时与不同的空中航行服务提供者进行互动）。

2.5 因此，在“各系统组成的系统”中开发和维护此种网络抵御能力，需要所有利害攸关方之间的持续协调（见第 2.2 段），以保持航空“各系统组成的系统”正常运行所需的灵活性和适应性。

2.6 为实现这一目标而要解决的一个重要挑战是“可组合性”的概念 — 将多个元素（系统组件或 SoS 子系统）安全地集成到更大的实体中的能力。这里的关键挑战是偏离安全范例，其中各元素的集成主要侧重于它们的功能和共同接口的互动。从网络安保的角度来看，个别元素的整合还需要仔细考虑每个元素的网络安保状态如何有助于整体网络安保状态。在这一探索中将出现的一个关键问题包括如何在其发展历程中支持国家和地区（以及其他个体利害攸关方），以便尽管子系统之间存在不可避免的差异，但仍可以有效地保护“各系统组成的系统”免受网络安保攻击。

2.7 为实现上述目标，各个子系统的整合需要仔细考虑，并整合每个子系统的本地安保环境，以塑造出整体的和具有网络抵御能力的环境。未经协调的网络安保方法可能导致保护漏洞不能被发现；设想的系统防御手段的重叠同样危险，因为这种情况仍然可能导致航空“各系统组成的系统”成为可行的攻击面。

2.8 因此，在管理系统互动方面采取全球协调一致的方法至关重要，而实现该目标的核心是就这些系统和子系统如何互动形成共同观点。

2.9 为航空系统纳入设计安保特性 — 为了使航空“各系统组成的系统”达到所期望的网络抵御水平，从系统开发开始就纳入网络安保考虑，而不是事后追溯考虑，这是至关重要的。这还将得以考虑子系统之间的接口考虑因素，使得这些互动也将以安全高效的方式进行。

2.10 目前大多数安保标准都侧重于在组织范围以内采取和实施缓解措施 — 迫切需要调整此类措施的重点，以包括并考虑也必须在组织之间采取的措施。这将得以保证“各系统组成的系统”整体的安保，高于把单独保护的各子系统合并之后达到的安保水平。

2.11 如果没有适当的管理，航空子系统未经协调的网络安保方法可能对整个系统构成风险。缺乏协调也可能源于子系统管理者与其他相关的利害攸关方之间在网络安保方法的开发和设计过程中沟通不足。

2.12 通过在不同层次的子系统之间进行多层协调（例如在作为国内航空系统的管理者的国家之间，以及在国内航空系统内的子系统管理者之间等），并确保各个子系统本身得到应有的有效保护，各国将为航空“各系统组成的系统”做出贡献，该系统作为此类工作的自然结果，将保持深度的防御水平。

2.13 未来的工作 — 将设计安保特性作为初始系统设计的一部分纳入其中的这项工作，不应取代航空界在开发航空系统和应对网络安保挑战方面数十年的经验所汲取的最佳做法。通过将这些原则与传统的侧重于系统冗余的做法相结合和予以补充，并强调最大限度地提高运营数据和系统的进入便利，利害攸关方将进一步加强航空“各系统组成的系统”的网络抵御力方面的政策，同时保持有效的运行。

2.14 作为当今各种航空论坛上讨论的各种运行概念和解决方案的一部分，各国和业界通过开发和设计过程考虑上述因素是极为重要的。推而广之，业界也可以进一步推进其集体工作，以进一步确定代

表性的子系统和研究工作，根据所采取的措施和使用的做法，其工作成果可以转移到其他子系统，以提高整个网络的抵御能力。

2.15 同样，在这一领域取得成功之后，航空界可以考虑努力开始进一步发展越来越大的子系统，这些子系统在初始设计阶段就要考虑到信息安保。随着这些工作的进展和成熟，利害攸关方可以开始集体探讨是否存在合适且值得信赖的候选人，负责开发和维护这些具备设计安保特性的系统，以及此类流程在未来航空系统中的可行性。

2.16 通过持续投资和致力于系统网络抵御能力的努力，航空界将在未来有效地促进航空生态系统（“各系统组成的系统”）的安全和有效的运行。

3. 结论

3.1 请会议就以下建议达成协议：

会议

- a) 敦促国际民航组织和各国承认，航空系统的网络抵御能力取决于所有相关的利害攸关方之间的持续协调。
- b) 要求国际民航组织承认 SoS（“各系统组成的系统”）的概念，需要子系统管理者之间进行协作和协调的必要性，特别是在开发、集成、操作和维护具备“设计安保特性”的子系统时。
- c) 敦促国际民航组织制定一个框架，要求并指导各国实施减轻网络威胁和对民用航空系统的风险的措施。这可能导致为几个受影响的国际民航组织附件制定标准和建议措施。
- d) 认识到信息文件“关于航空网络安保的考虑”中所载的概念。