国 际 民 用 航 空 组 织

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

工 作 文 件

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

强化航空领域的网络安保观念

（由奥地利代表欧盟及其成员国[1]和欧洲民航会议[2]其他成员国；
和欧洲航空安全组织提交）

执行摘要

本文重点强调可信赖性，为什么在使用信息安保管理系统时需要信赖，它会给机构带来什么好处。此外，本文还阐述为什么同等水平的网络安保性能，无论时间、地点和所连接的系统如何，是一个至关重要的前提条件，如何在地对地或空对地运行中得以实现。

本文通过分析机构与机构之间或与其运行的系统之间的互动产生的风险，简要介绍为什么机构要借助信息安保管理系统（ISMS）管理各自的网络安保风险、产品和服务。

本文进一步介绍有关航空临界点和信息共享裨益的普遍观点。

行动：请会议批准第3段中的建议。

[1] 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、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、瑞典和英国。

[2] 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、前南斯拉夫马其顿共和国、土耳其和乌克兰。

1. 序言

1.1 随着民航业数字化的进一步发展，具备信息精准、运行顺畅的安全临界系统是保障民航安全和安保的前提条件。航空系统高度集成，信息传播遍及全球。因此，航空业的网络安保举措必须采取整体性和端到端的方法。

1.2 本文突出介绍了在航空业引入信息安保管理系统（ISMS）的裨益。这种管理系统最好与现有航空风险管理系统进行调整或集成在一起，从而个别机构乃至全行业为更好地应对信息安保威胁做好准备。

1.3 考虑到信息可以共享，业内许多机构的系统是通用的，面临的风险是相同，采用通用管理系统方法有利于全行业协调行动。

1.4 除了 ISMS 方法之外，本文还阐述了信任理念。在航空业内，伙伴之间的信任和信心至关重要。就每次飞行而言，一个完善的培训、认证、监督和复查系统可以确保所有伙伴都相信对方能够认真和正确地履行各自在航空链条中的作用。

2. 讨论

2.1 **如何利用ISMS** — 目前的ISMS概念本质上仅限于单个机构。但是，民用航空是一个紧密融合的系统的系统，是由相互联系的产品、人员和流程构成的，甚至还与军用系统[3]连接，因此，单个机构自行其是是不行的。因此，民用航空在引入ISMS系统时首先要有跨机构网络安保管理的理念。

2.2 因此，一个全球协调 ISMS 的方法是民航业的一个关键条件。这样一个全球体系将有利于统一实施一些辅助概念，如全球互联互通的、安全的通信基础设施、信任体系等，从而有利于建设未来的基于可信赖的信息交换系统。这种未来系统不是组织机构经过一次变革就可以一蹴而就的，因此需要各国或各地区为其创造有利条件。这些概念变为现实的前提，是所有机构都建立起 ISMS。建立 ISMS 系统应以现有安全管理（如附件 19 —《安全管理》）和航空安保风险管理系统为准，遵守国际民航组织的规定和行业标准，并建立有效的监督机制。

2.3 **可信赖性的概念** — 民用航空界经过数十年的努力已经建立起了一个坚实的信心体系。可信赖性现已正式成为一种理念，即一个机构或其运行的系统可以倚赖另一机构或其运行的系统的网络安保特性[4]。信任从来都不是绝对的，这一概念根据对依赖方产生的影响（安全或业务的连续性，比如一个地区的高质高效的交通流量）把可信赖程度分为多个层次。

2.4 例如，在航空器审定中，对适航性的信心主要源于适当的行动能够产生可接受的结果的保证。这些行动是按照安全风险影响的严重程度而设计的。在开发过程中，影响越严重，审查就越严格。因此，针对网络安保特性提出了相似的概念，其初衷是要反映出为阻止网络威胁所采取的措施的有效性。实质

[3] AN-Conf/13-WP/39提及

[4] 信息文件（AN-Conf/13-WP/160）将对信息安全管理系统的概念和原理、可信赖性和网络安全运行条件概念以及信息共享的好处进行解释

上，相信在开发过程中没有错误和漏洞，相信一个组织有能力足以保护民用航空，这种信心是未来安全飞行的保障。可信赖性的概念应融入 ISMS 系统，而 ISMS 系统则应与现有管理系统进行统一和整合。

2.5 **网络安保的运行条件** — 为了充分利用可信赖性的概念，需要考虑作为全球互通和安全的基础设施组成部分的个别机构及其系统的动态演进。预设网络安保运行条件是应对这一挑战的一种方式。同伴之间进行任何连接都需要他们之间具有同等的可信赖程度，这一点十分重要，因此，这就需要确定同伴的匹配性。有些同伴组合符合网络安保要求，风险程度可以接受，因此，他们之间的可信赖程度允许他们进行互联。而另一些组合可能不符合这些要求。这样就需要鼓励同伴就匹配但可信赖程度不同的条件取得一致，从而最终找到一个平衡的方法。需要区分同伴之间两种不同连接的转换：一个是系统相连的机构之间的连接的转换，另一种是机载或天基设备与地面系统之间的转换，它们之间的转换速度非常快。两者的主要区分标志是他们网络安保环境演变的速度。

2.6 缓慢演变：一方面，地面系统，主要是空中交通管理（ATM）和空中航行服务（ANS）系统，发展速度相对缓慢。其运行条件的变化主要取决于各自的网络安保状态或其所连接的一个系统。这就需要考虑对网络安保特性进行同步协调，使所有联网各方能够满足网络安保的总体要求。所谓运行条件的概念就是要正确匹配联网机构之间的可信赖的程度。

2.7 快速演进：另一方面，航空器从一地点向另一地点移动速度相对较快，同时还要与大量的同伴系统在短时间内保持动态连接。一般而言，一架航空器或 ATM/ANS 系统在某一天中所处的网络安保状态是不同的。因此要使他们保持运行，双方都需要进行转换。对网络安保而言，调整运行条件概念也许可以提供一个应对策略。例如，按照现有运行条件概念，一个空域中适用的横向分隔要求需要配备一定的地面设备和航空器系统才能满足这些要求。因此，运行条件概念可以作为网络安保的蓝图，以满足由可信赖程度引入的网络安保特性的要求。ATM/ANS 与航空器系统之间可信赖程度充分匹配才能确保空域使用中的安全和安保。

2.8 **关于网络问题的信息共享** – 关于 ISMS，另一个需要考虑的问题是信息共享。一个 ISMS 全球体系还有助于建立一个更加统一的网络安保风险信息共享机制。信息技术（IT）世界已经提出一个网络安保中心的概念，用以“处理”网络安保事件信息，包括收集和建立事件、威胁和薄弱环节的数据库，对行之有效的方法进行分析，就应对各辖区内发生的事件提出指导。这些工作都与信息共享密不可分。

2.9 国际上，计算机应急响应小组（CERTs）和计算机安保事件响应小组（CSIRTs）创立了一个名为事件响应和安保小组论坛（FIRST）的社区。该论坛为航空界绘制了一个协同开展全球信息共享的蓝图，目的不仅是对事件进行响应，还要阻止未来的袭击。对于已发现的新漏洞，CSIRTs 收集的信息在一定程度上有助于预测正在出现的风险，从而采取预防措施，以限制对民航造成的破坏性影响。总而言之，目标是提高人们对网络威胁和航空系统薄弱性的认识。只有航空界的 CSIRTs 之间及其成员间加强协调，才有可能在全球范围内针对网络威胁采取统一的缓解和防御性措施。

2.10 网络安保威胁已经超出民航领域，侵入到其他交通和非交通系统（例如银行系统和核工业）。这些行业使用的技术相同，实施方法类似，受到的威胁和存在的薄弱性也不尽相同。因此，这些行业的机构就策略、情报信息和最佳做法开展分享和交流十分重要。民航网络安保解决方案应该借鉴其他国家或地区的跨行业的解决方案和经验。另外，与从事其他行业网络安保工作的政府部门保持密切沟通将会使各国民用航空管理机构受益匪浅。

3. 结论

3.1 请会议批准下列建议：

会议：

a) 敦促国际民航组织支持各国要求各机构根据国际行业标准并通过与现有管理系统进行协调和集成，利用信息安保管理系统管控与其运行、产品和服务相关的网络风险；

b) 要求国际民航组织鼓励各国采取适当措施，建立全球互通的基础设施，抵御网络攻击。该基础设施应符合互操作性和网络安保要求，以实现安全和高效空中交通的更高的整体目标；

c) 敦促国际民航组织以多学科方法制定机构间信任规定，建立更广泛的信任体系，并鼓励其实施；

d) 要求国际民航组织鼓励各国采取措施，推动航空运营人通过全球“可信赖的组织”网络等酌情指定的渠道建立和促进运营网络安保相关信息共享；

e) 敦促国际民航组织促进制定有关可信赖性和网络安保运行条件的规定，保证此种全球可互用的基础设施的运行得到安保保障；

f) 要求国际民航组织鼓励各国扩大现有的或建立新的网络安保相关事实的报告渠道，更好地处理新的航空安全和安保风险，确保交通的快捷流动；和

g) 要求国际民航组织呼吁各国促进政府和非政府部门就航空和其他领域之间的网络安保开展跨行业合作。

— 完 —