MSC-FAL.1/Circ.3/Rev.1 通函
（2021 年 6 月 14 日）

海事网络风险管理指南

1　便利委员会在其第 41 届会议（2017 年 4 月 4 日至 7 日）和海上安全委员会在其第 98 届会议（2017 年 6 月 7 日至 16 日）上，审议了增强网络风险威胁和安全隐患意识的迫切需求，批准了海事网络风险管理指南，其文本载于附件。

2　本指南提供关于海事网络风险管理的高级建议，以保护航运免于当前和新出现的网络威胁和安全隐患的危害。本指南也包括支持有效网络风险管理的功能要素。

3　海上安全委员会在其第 103 届会议（2021 年 5 月 5 日至 14 日）和便利委员会在其第 45 届会议（2021 年 6 月 1 日至 7 日）上，批准了对本指南第 4.2 段中附加导则和标准的更新。

4　提请各成员国使所有相关利益方注意到本通函的内容。

5　本通函和任何修订取代 MSC.1/Circ.1526 通函中包含的暂行指南。

附件

海事网络风险管理指南

1 引言

1.1 本指南为海事网络风险管理提供高级建议。就本指南而言，海事网络风险系指技术资产受到潜在环境或事件威胁的一种量度，其可能由于信息或系统损坏、丢失或破坏而造成航运相关操作、安全或保安故障。

1.2 利益相关方应采取必要措施，保护航运免于当前和新出现的与航运进程和系统的数字化、整合和自动化相关的威胁和安全隐患。

1.3 对于与特定风险管理进程的发展和执行相关的细节和指导，本指南的使用者应参照特定成员国政府和船旗国主管机关的要求以及相关国际和行业标准和最佳操作方式。

1.4 风险管理对于安全航运操作很重要。风险管理习惯上注重实际领域的操作，但由于对数字化、整合、自动化和基于网络系统的依赖性的增加，对航运业网络风险管理的需求已日益增多。

1.5 基于支持安全航运的目标，其在操作上可适应网络风险，本指南提供的建议可纳入现有风险管理进程。就这一点而言，本指南与本组织建立的安全管理操作方式互补。

2 一般规定

2.1 背景

2.1.1 对航运安全和海洋环境保护至关重要的许多系统的操作和管理而言，网络技术已必不可少。在某些情况下，这些系统应符合国际标准和船旗国主管机关的要求。然而，进入、互相连接或网络连接这些系统造成的安全隐患会导致应处理的网络风险。具有脆弱性的系统包括但不限于：

.1 驾驶室系统；

.2 货物装卸和管理系统；

.3 推进和机器管理和动力控制系统；

.4 进入控制系统；

.5 乘客服务和管理系统；

.6 乘客界面公共网络；

.7 行政和船员福利系统；和

.8 通信系统。

2.1.2 信息技术和操作技术系统之间的差别应予以考虑。可认为信息技术系统集中于将数据用作信息。可认为操作技术系统集中于使用数据控制或监控实际过程。此外，也应考虑保护这些系统内的信息和数据交换。

2.1.3 虽然这些技术和系统使航运业效益大幅提升，其也对与航运基本系统的操作相关的关键系统和进程构成风险。这些风险可能起因于网络相关系统的不当操作、整合、维护和设计以及有意或无意的网络威胁引起的安全隐患。

2.1.4 威胁以恶意行为（例如，黑客入侵或引入恶意软件）或良性行为（例如，软件维护或用户权限）的非预期后果呈现。一般来说，这些行为暴露安全隐患（例如，软件过期或防火墙无效）或利用操作或信息技术中的安全隐患。有效的网络风险管理应考虑这两种风险威胁。

2.1.5 安全隐患可起因于不足的系统设计、整合和/或维护以及网络纪律的疏忽。一般来说，如果操作和/或信息技术中的安全隐患直接（例如，导致非法进入的弱密码）或间接

（例如，无网络隔离）地暴露或被利用，可能会影响安全以及信息的机密，完整性和有效性。此外，当操作和/或信息技术的安全隐患暴露或被利用时，对安全会有威胁，特别是涉及关键系统（例如驾驶室航行或主推进系统）时。

2.1.6　有效的网络风险管理也应考虑暴露或利用信息技术系统的安全隐患所造成的对安全的影响。这起因于与操作技术系统的不当连接或操作人员或第三方程序上的失误，可能会危及这些系统（例如，诸如记忆棒的可移动介质使用不当）。

2.1.7　关于安全隐患和威胁的更多信息，见第 4 节中的附加导则和标准。

2.1.8　这些快速变化的技术和威胁使只通过技术标准处理这些风险变得困难。因此，本指南推荐针对网络风险的适应性强的风险管理方法，可作为现有安全管理操作方式的自然延伸。

2.1.9　考虑潜在的威胁源、安全隐患和相关风险减轻策略时，也应虑及网络风险管理的潜在控制选项，包括管理、操作或程序以及技术控制。

2.2　应用

2.2.1　本指南拟供航运业的所有组织使用，并设计成鼓励网络领域的安全管理操作方式。

2.2.2　认识到航运业中没有两个个组织是一样的，本指南以广义的术语进行表述以广泛应用。对于网络相关系统有限的船舶，简单应用本指南已足够；然而，具有复杂网络相关系统的船舶可能会要求更大程度的关注，并应通过声誉良好的行业和政府合作伙伴寻找附加资源。

2.2.3　本指南是建议性的。

3　网络风险管理要素

3.1　就本指南而言，网络风险管理系指标识、分析、评定和传达网络相关风险并接受、避开、转移或减轻风险至可接受程度的过程，并虑及对利益相关方采取行动的成本和效益。

3.2　海事网络风险管理的目标是支持安全航运，其在操作上可适应网络风险。

3.3　有效的网络风险管理应从高级管理层开始。高级管理应将网络风险意识文化深入各级组织，并确保整体灵活的网络风险管理制度，其连续操作并通过有效的反馈机制不断评估。

3.4　实现上述目标的一个可接受的方法是全面评定和比较一个组织的当前和期望的网络风险管理立场。这种比较会显示应处理的差距，以通过优先的网络风险管理计划实现风险管理目标。该基于风险的方法将使一个组织能以最有效的方式最好地应用其资源。

3.5　本指南提出支持有效网络风险管理的功能要素。这些功能要素不是有顺序的—所有实际上应同时发生并连续，并应适当纳入风险管理框架：

.1　标识：明确网络风险管理的人员角色和职责，标识遭到破坏时危及船舶操作的系统、资产、数据和能力；

.2　保护：实施风险控制过程和措施以及应急计划以抵御网络事件并确保船舶操作的连续性；

.3　发现：制定和实施及时发现网络事件所必需的各项行动；

.4　响应：制定和实施行动和计划以提供适应性，并恢复由于网络事件而受损的船舶操作或服务所必需的系统；

.5　恢复：确定备份和恢复受到网络事件影响的船舶操作必需的网络系统的措施。

3.6　这些功能要素包含涉及影响海上营运和信息交换的各关键系统的有效风险管理的各项行动和期望结果，并构成具有有效反馈机制的持续过程。

3.7　有效网络风险管理应确保组织的各级适当意识到网络风险。意识程度和准备状态应适于网络风险管理系统中的角色和职责。

4 实施网络风险管理的最佳操作方式

4.1 所述的网络风险管理方式为更好理解和管理网络风险提供基础，从而使风险管理方式能解决网络威胁和安全隐患。对于网络风险管理的具体导则，本导则的使用者也应参见成员国政府和船旗国主管机关的要求，以及相关国际和行业标准以及最佳操作方式。

4.2 附加导则和标准可包括但不限于：[1]

.1 由 ICS、IUMI、BIMCO、OCIMF、INTERTANKO、INTERCARGO、InterManager、WSC 和 SYBAS 制定和支持的《船舶网络安全指南》；

.2 IACS 网络弹性建议综合文本（Rec.166）；

.3 ISO/IEC 27001 标准：信息技术—安全技术—信息安全管理系统—要求。国际标准组织（ISO）和国际电工委员会（IEC）共同发布；

.4 美国提高关键基础设施网络安全的国家标准和技术框架学会（NIST 框架）。

4.3 应参见使用的任何导则或标准的最新版本。

[1] 附加导则和标准列为本指南使用者获得更详细信息的非全面参照。参考的导则和标准未经本组织发布，其使用仍由本指南的个人用户决定。