指导性文件
GUIDANCE NOTES
GD26-2019

中国船级社

CHINA CLASSIFICATION SOCIETY

海事网络风险评估与管理体系指南

Guidelines on Maritime Cyber Risk Assessment and Cyber Safety Management System

（2019）

2020年2月1日生效

北京

目　　录

前言

注意到网络风险对船舶安全和防污染的危害，IMO 海上安全委员会先在其第 96 届大会通过了《海事网络风险管理暂行指南》（MSC.1/Circ.1526），后在其第 98 届大会批准了《海事网络风险管理指南》（MSC-FAL.1/Circ.3）以替代暂行指南（MSC.1/Circ.1526）。

根据第 98 届大会通过的决议《安全管理体系中的海事网络风险管理》（MSC.428(98)），安全管理体系需考虑网络风险管理。同时，IMO 鼓励各国政府不迟于 2021 年 1 月 1 日之后的首次 DOC 年度审核时，核查安全管理体系是否包括了网络风险管理的相关内容。

本指南提供了海事网络风险评估的方法以及制定、实施和改进管理体系的建议，以便业界对海事网络风险具备必要的认知，并引起足够的重视，为早日将网络风险管理纳入安全管理体系做好准备。

一、 通则

1.1 背景

随着计算机技术的飞速发展，网络已经成为社会发展和经济发展的重要保证及必备工具。在航运业，数字化、集成化、自动化和网络化的发展，极大促进了船舶各系统通过网络互联互通。而卫星通讯的日益普及，更使船舶网络与公司网络和其他相关方的网络的连接更加频繁。

网络给航运业带来便利和效率的同时，也带来了网络威胁。网络威胁会使船舶遭受到恶意的或无意的访问或攻击，因此，航运业需采取必要的措施，努力保护各项资产，减少和避免由此造成的安全、环境以及商务方面的不利影响。

从发展趋势来讲，自动化码头、智能船舶和无人船舶的发展，都需要安全和高效的网络来保障船舶的正常营运和航运业的持续发展。

网络威胁伴随着网络技术的升级换代在不断变化和发展，同时，广泛使用的个人移动终端和移动介质会带来难以预期的安全隐患，所以，对于网络风险的管理不仅要基于已知的威胁，还需尽力考虑未知的威胁。

据报道：

- 2011 年，某油船从阿拉伯湾启程前往地中海。该轮的行程、货物、船员、地点以及有无武装警卫等各项信息被海盗雇佣的技术人员提前获悉，从而被海盗锁定并劫持。
- 2011 年和 2013 年，欧洲某港口的信息系统遭到网络攻击，货物数据被篡改，使得毒品走私计划得逞。
- 2014 年，某燃料供应商因被保险公司指控卷入一起网络攻击事件，付出了缴纳罚款约 1800 万美元的代价。
- 2015 年，伦敦船东保赔协会发布消息称，船舶网络诈骗数量正日益增加，其中包括拦截船舶代理商的邮件，入侵其电子邮箱账号，以实施将原支付账户换成新的银行账户等计划。

- 2016 年，有关机构统计，无人驾驶船舶的前三大风险为：航行风险，网络安全和失联。
- 2017 年，Petya 的网络病毒袭击全球，著名航运企业在全球多处办事机构及部分业务单元的 IT 系统因此出现故障，所遭受的损失据称达数亿美元。
- 2018 年，MARAD 发出航行警告，指出在黑海海域大约 20 艘的船舶的 GPS 遭遇了一起奇怪的恶作剧式的“干扰”，导致船位显示不准，船位丢失等情况。
- 同年，全球集装箱航运巨头中远海运集装箱运输有限公司美国地区网站遭到网络攻击。根据相关报道，航运公司发言人确认其美国地区网络遭遇了勒索软件的攻击。

网络安全问题已开始损害航运业的正常运行，并逐渐成为业界的焦点。为规避和降低风险，并满足 IMO 海上安全委员会的建议，各方需要尽快开展海事网络风险的评估和管理，确保海事网络安全管理体系得以正常运行。

1.2 目的

本指南依据 IMO 海上安全委员会在其第 98 届大会批准的《海事网络风险管理指南》（MSC-FAL.1/Circ.3）进行编写，为业界执行第 98 届大会通过的决议《安全管理体系中的海事网络风险管理》（MSC.428(98)）提供指南。

本指南通过介绍海事网络的基础知识，提出进行海事网络风险评估的方法，给出海事网络管理体系的制定、执行和改进的建议，为业界提供尽可能全面的、有效的、可操作的指南，以便业界根据实际情况在决策前参考，帮助业界保护船舶免于或减少受到当前以及未来的网络威胁。

海事网络风险管理是船东、管理公司和船舶通过制定和执行各种措施和计划，采用规避、转移、降低或容忍的方式，将网络风险控制到合理水平的活动过程。当网络范围有限时，可采用较为简洁的方式；当网络范围较广且系统复杂时，应采用更综合的方案，并尽力寻求业界、主管机关及合作方的支持。

海事网络风险管理是为了最大限度地保证航运的正常操作和安全运行，因此，海事网络风险管理的措施和计划应有尽可能多的缓冲空间和富裕度，以避免网络安全事件的发生。同时，全力确保即使网络安全事件发生后，也能够保证资产和人员的安全以及海洋防污染不受到影响。

1.3 适用范围

本指南适用范围与《国际安全管理（ISM）规则》一致。从海事网络的角度来讲，本指南适用船舶网络及公司网络中涉及船舶安全管理的部分。

如果船舶（尤其是网络程度化高的船舶）的网络受到攻击后会出现船舶被远程挟持的情况，在执行网络风险管理时，还需符合《国际船舶和港口设施保安（ISPS）规则》的要求。

根据第 98 届大会通过的决议《安全管理体系中的海事网络风险管理》（MSC.428(98)），IMO 鼓励不迟于 2021 年 1 月 1 日之后的首次 DOC 年度审核时，完成海事网络风险管理的实施。

从操作实践的角度讲，本指南建议公司不迟于 2021 年 1 月 1 日之后的首次 DOC 临时审核、初次审核、年度审核和换证审核时，完成海事网络风险管理的实施。

本指南的相关规定对于不适用《国际安全管理（ISM）规则》的情况，可参照执行。同时，希望航运业的各个组织，根据本指南开展网络风险管理。

本指南为建议性指南。

1.4 基本原则

为了确保措施和计划得到有效的执行，海事网络风险管理应覆盖从高级管理层到每一位船员或员工。高级管理层应注重采取各种措施将网络风险意识宣贯到公司的每个层面，并通过有效的反馈机制，确保网络风险管理能得到持续的运行并被定期评估，从而建立起全面的、有效的、灵活的、可操作的管理体系。同时，高级管理层应注意到需指派足够的人力和划拨必要的经费，用于海事网络风险管理体系的制定和实施。

为确保有效实施，海事网络风险管理体系的建立，需与公司和船舶的网络实际情况相一致。所以在制定海事网络风险管理体系文件前，应先调研网络现状；再基于调研的结果开展网络风险的评估；然后，根据评估中发现的风险拟定恰当的措施，采用有效的方式合理利用资源解决问题；最后，将网络风险管理的各种措施纳入安全管理体系。

为确保效果，在具体实践中，各相关方应充分考虑船旗国政府的要求，以及相关的国际标准、行业标准和最佳实践。

海事网络风险管理是安全管理体系的组成部分，并与之协调一致。对于网络风险管理中涉及的商业敏感信息或保密的数据，公司应当注意保护，尤其是避免在体系文件中述及。同时，还应注意 ISPS 规则 A 部分第 8 章关于“船舶保安评估”的强制性要求，和 ISPS 规则 B 部分第 8.4.11 条关于“无线电和无线通信系统，包括计算机系统和网络”的非强制性要求。

1.5 体系建立的三个阶段

本指南建议按照如下三个阶段进行体系的建立，详如下表：

阶段 1 **风险评估**	**阶段 2** **体系建立**	**阶段 3** **体系运行**
（1）海事网络调研	**（1）制定措施**	**（1）制定体系**
识别和熟悉海事网络连接范围和特性	避免和降低风险的发生和危害	将措施、计划、响应及恢复纳入体系
（2）风险识别	**（2）应急计划**	**（2）实施体系**
寻找由于海事网络的使用而产生的风险	网络事件发生后，减少和降低产生的危害	发布后，开始实施，并保存相关记录
（3）风险评估	**（3）响应及恢复**	**（3）改进体系**
对识别出的风险，进行量化评估	网络事件发生后，有效响应和恢复的能力	根据业界信息、反馈和险情等，改进体系

二、 海事网络及其风险

2.1 海事网络

随着计算机技术在航运界的广泛应用，现代船舶的信息化程度和自动化程度越来越高。为了更好的实现船舶数据共享、存储及使用，越来越多的船舶电子/信息化系统通过网络连接起来，这其中许多模块或系统通过卫星、WIFI 或 4G 技术连接到了互联网。

通常，船用网络可分为两类，第一类是用于信息收集和信息管理服务的网络，如，用于报告，调度，库存管理，运营和维护管理，电子邮件，电话，打印服务及船岸通信系统，这类网络通常称为信息网络（IT 网络），其组成包括船员使用的计算机、网关、路由器、文件服务器、数据库服务器、应用服务器等设备；第二类是负责采集、监视和控制全船设备的运行状态，服务于船舶操控系统的网络，称为控制网络（OT 网络），例如，分布于机舱的主推进监控系统、辅机监控系统、电站监控系统、火灾报警系统等以及驾驶台上的导航系统、综合船桥系统等。船舶网络系统示意如下图：

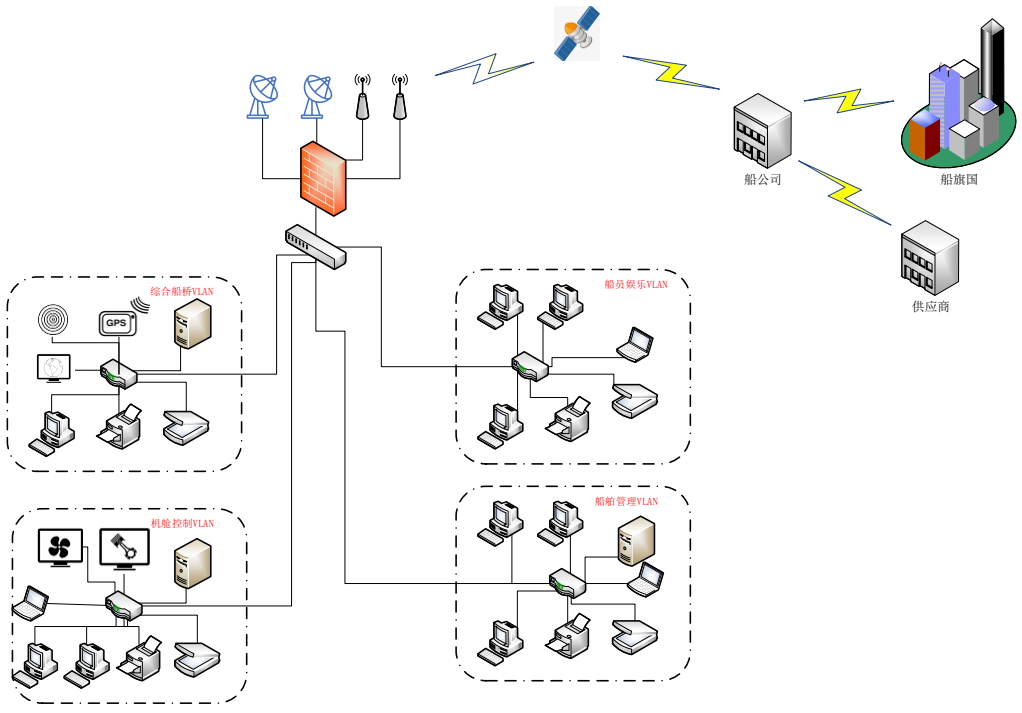

图 2.1 船舶网络系统示意

2.2 网络风险

随着网络技术在航运业的广泛应用，船舶网络在许多涉及船舶安全和防污染的关键系统中发挥越来越重要的作用，但伴随着网络的运用，网络风险随之而来。网络风险来自多方面，如程序中的操作错误、软件缺陷、未经授权访问的系统入侵、管理公司对船舶网络未能采用有效的风险控制程序等。通过调查发现，智能船舶易受网络风险攻击的系统包括船桥系统、货物操作和管理系统、推进和机械设备管理以及动力控制系统、访问控制系统、乘客服务和管理系统、乘客公共网络管理及船员保障系统、通信系统等。

在过去，船载系统虽然存在难以及时更新的问题，但由于其通常处于孤立状态，而且由于船舶长期离岸，船舶网络时常处于离线状态，使其减少暴露及遭受远程攻击。另外，当前船舶使用的一些嵌入式系统甚至在使用过时的和不支持的组件，虽然更高的网络速度使得系统更新变得容易起来，但由于其自身特殊性，仍然存在此类风险。

船员的安全意识对船舶网络安全的有决定性影响。船员可能一直使用着感染病毒的 USB 设备，一旦将其插入船载 PC，这会感染 PC 和船舶网络。另外，船载系统修复中遇到的最大挑战是互联网访问，最大的问题则是操作系统和应用更新。如果用户不用自己的账户连接到互联网则没有一台计算机能保持连续的互联网访问。

另外，随着卫星宽带数据速率的提高和收费在船上网络的竞争力的增强，船舶网络自然会更加类似于岸边的“分支机构”。同样，廉价的网络接入几乎改变了日常生活的各个方面，并将改变海运船舶的运营操作。这个关键系统的相对安全性因此会受到负面影响。虽然 USB 传播的恶意软件的威胁目前是主要关注的问题，但扩展对网络数据系统的访问将带来新的威胁，并需要成熟的业务流程来管理它们。漏洞管理流程，特别是扫描确定网络计算机状态的系统，可能是船载网络安全事件风险的有效方法。这可以也应该在增加船载系统接入公共互联网和其他岸基网络之前完成。

在某些情况下，船载系统需要运行旧版和具有脆弱性的 Web 浏览器和 Java 客户端才能使旧系统的功能正常运行。这种情况在基于岸上的基础设施上发生的

频率较低，并且随着互联网在船上的广泛应用而不得不改变。当有必要使用过时的或不受支持的软件组件时，应设计和部署补偿控制措施以抵消风险。例如，如果绝对有必要使用浏览器的旧版本，则可以通过基于主机的防火墙来限制通信，以便它只能与托管所需应用程序的端点进行通信。一个最新的浏览器然后可以用于一般的互联网浏览。虽然补偿这样的控制并不理想，但重要的是理解安全措施往往会对可用性产生负面影响。在保持可用性的同时寻找风险管理的适当平衡需要仔细考虑，并且在某些情况下需要一些试验和错误。

三、 海事网络风险评估

3.1 基本原则

海事网络风险评估的过程和结果是建立海事网络风险管理体系的重要基础。其评估的过程至少应包括：海事网络调研、风险识别和风险评估。

海事网络风险评估的过程，不仅会促进参与人员的网络风险意识，更有利于发现更深入和更广泛的风险。

海事网络风险评估的结果是制定安全管理措施的依据。因此，风险评估的工作应得到公司各个层面和各个部门的支持。

注意到网络技术的专业性和快速发展，本指南建议，评估的参与人员至少有一名具备足够的计算机知识和网络知识。

海事网络风险评估时，邀请第三方参与是公司自评的有效补充方式。第三方可以帮助进行更深入的风险识别，发现更多的潜在风险。

3.2 海事网络调研

对海事网络的连接范围和特性进行调研是寻找风险的起点，也是认知和熟悉海事网络的过程。调研时，应注意到所有涉及网络连接的因素，包括：系统、资产、数据、功能、端口、权限、人员等。同时，为方便后续工作及实施后的改进，调研过程应进行必要的记录。

为调研海事网络，可以采用的方法包括：图纸核查、船员自查、现场查验和服务商检查等。公司可根据网络的复杂程度和不同网络之间的相似程度，采用一种方式或多种方式组合进行海事网络的调研。

3.2.1 海事网络调研举例

海事网络的调研应充分并尽量保证调研结果完整和准确。为方便理解并供各方参考，关于海事网络调研，针对网络情况较为简单的船舶，本指南建议从如下

六个方面开始调研：

1. 无需上网，无工作计算机；
2. 无需上网，有工作计算机；
3. 船舶设备需上网；
4. 工作计算机需上网；
5. 船员娱乐需上网；
6. 乘客娱乐需上网。

针对网络情况较为复杂的船舶，本指南建议从网络建设和需求开始调研，并注意如下环节：

1. 公司决策网络需求；
2. 公司与网络服务商签订供应合同以及明确使用网络的设备（例如：航行设备、CCTV、邮箱服务、船员娱乐等）。网络服务商通常为无线电检测服务公司；
3. 网络服务商采购网络供应商的服务以及网络供应商的配套设备（天线、调制解调器、路由器）；
4. 网络服务商采购交换机和防火墙，并根据供应合同，进行网络配置和安全配置，在网络需求得以实现的同时，限定上网需求在合同范围内；
5. 需上网的终端接入网络。一般需接入位于防火墙后的交换机。但对于只需读出数据，无需写入的终端（例如：CCTV），可直接接入路由器；
6. 船舶使用网络服务进行防病毒软件的安装。

3.3 风险识别

通常认为，海事网络风险系指对人员、防污染和资产造成潜在危害的行为或数据。这些风险可能是由于不恰当的操作、不合适的集成、不及时的维护、不规范的操作以及不合理的网络设计导致，也可能是由于有意的或无意的网络攻击导致。

风险的出现会暴露出各种漏洞及不足之处，所以，需要通过识别风险去寻找薄弱环节，并予以改进，将风险至少降低至可接受的水平。

对于船舶的网络风险识别时，除进行通用的项目外，还应注意船舶是否具有

特殊的设备或系统需要进行风险识别。

为了方别识别海事网络风险，建议将风险进行分类。

按所在的系统分类，可以分为：信息系统、操作系统、数据及其传输。信息系统对数据的使用以信息为目的。操作系统对数据的使用以控制或监测物理活动为目的。在计算机科学中，数据泛指所有能输入到计算机并可以被程序处理的各种介质。就本指南而言，数据传输的方式应包括：网络传递、移动介质传递和特殊接口。

按需采取的措施分类，可以分为：对外防护和内部保护。对外防护关注于防止未授权访问、被控制、被毁坏。内部保护关注于关键数据和操作系统的可用性和完整性出现问题时如何补救。较为形象的理解方式为：对外防护主动地将危险源防御在外部；内部保护被动地为需保护的对象提供恢复原有能力的措施。内部保护事件可能由下述原因导致：对外防护事件、软件维护和升级时的错误、运行必需的外部数据丢失或被控制或造假。

3.3.1 威胁

通过网络的互联互通，一些未经授权接入网络的组织或个人，会有意或无意地从网络的外部影响网络的正常使用，进而造成可预见的或不可预见的危害。

这些潜在的危害举例如下：

- 危险分子（包括心有不满的员工），以相关方名誉受损或日常运行中断为目的，损坏数据、公开敏感数据、引起媒体关注、阻碍服务和系统的正常使用；
- 犯罪分子，以经济利益或商业竞争或行业竞争为目的，出售盗取的数据、勒索赎回盗取的数据或系统的可用性、编造虚假的货物运输、收集信息用于犯罪；
- 投机分子，以证明个人能力或勒索为目的，突破网络防护、经济利益
- 别有居心的政府、政府资助的机构、恐怖分子，以政治利益或间谍行为为目的，获取信息、破坏经济、破坏重要设施。

上述这些情况在网络上一直存在，且这些人员具备足够的技能和资源。他们切实地威胁到各项资产的安全以及公司进行日常运行的能力。

不论是岸基还是船上的从业人员，都可能会危害网络系统和数据。公司应当做好准备，因为在操作和管理 IT 和 OT 系统时，人们会出现操作失误或不遵守安全措施的情况。当然，这种情况也可能是不满的员工蓄意为之。

就本指南而言，危害网络正常使用的行为，即为网络攻击，并可分为：

- 随机性攻击，公司或船舶的系统和数据是许多潜在目标中的一个；
- 特定性攻击，公司或船舶的系统和数据是选定的目标。

随机性攻击中，攻击方使用互联网上存在的工具和技术手段进行。他们定位、发现和利用普遍存在的薄弱环节。如果公司和船舶的薄弱环节正好与其一致，则被攻击。此类攻击举例如下：

- 恶意软件；
- 社会工程；
- 网络钓鱼；
- 虚假网站；
- 随机扫描。

特定性攻击中，攻击方拥有娴熟的技能，并使用针对公司和船舶的专用工具和技术手段。此类攻击举例如下：

- 暴风算法（穷举法）；
- 拒绝服务；
- 鱼叉式网络钓鱼；
- 破坏供应链。

海事网络的使用者和管理者应意识到上述攻击是活跃的，需通过有效的管理，尽早识别网络攻击、缓和网络攻击和降低攻击导致的危害。

3.3.2 脆弱性

网络的脆弱性系指网络的各个组件及信息系统、操作系统、数据及其传输的薄弱环节和不当操作导致。对于非联网的孤立系统，其风险更少，但会因组件的可靠性、软件升级、使用移动介质和不当的操作出现风险。

船舶使用的网络系统，举例如下：

- 桥楼系统；
- 推进、电力和设备管理；
- 货物管理系统；
- 门禁系统；
- 乘客服务和管理系统；
- 乘客娱乐系统；
- 船舶和船员管理系统；
- 互联网服务。

用于船岸连接的网络系统，举例如下：

- 柴油机性能监测；
- 航行性能监测；
- 航行数据上报；
- 维护和备件管理；
- 货物、起货机、货泵管理；
- 闭路电视监控系统。

由于网络系统构成的多样性，上述两方面的举例，仅供参考。相关方应通过审查船舶网络系统的结构和辨识船岸联系接口，全面识别组件及系统。此时，应对新技术和新设备予以更多关注，因为，新技术和新设备缺少使用经验，这意味

着更多未知的风险。

网络系统的脆弱性通常是由下述原因造成：

- 废弃的和没有技术支持的操作系统
- 杀毒软件和防恶意攻击软件，过期或未安装
- 安全措施不全面及未按规定执行；
- 网络缺少边界保护措施及缺少分隔；
- 关键设备或系统与岸基时时连接；
- 对合作方的访问权限控制措施缺乏。

应考虑服务供方的网络安全情况，并建议服务供方确认其网络安全意识和管理的现状，并根据其提供的服务予以评估，尤其是服务供方能通过网络与船舶或公司的网络直连时。

3.4 风险评估

3.4.1 风险评估的量化

就本指南而言，风险评估是指，对识别出的风险，围绕可能造成的负面影响和损失的可能性及危害程度进行量化评估的工作。

由于风险发生的可能性和危害程度共同决定了该风险的高低程度，所以，应先对风险发生的可能性和危害程度进行分级或评分，再根据二者的分级或评分，给出风险的级别和得分。风险发生可能性高且危害程度较大，则为高等级风险。风险发生可能性低且危害程度不高，则为中等级或低等级风险。详情可参考图 3.4.1-1 风险数量较少时和图 3.4.1-2 风险数量较多时。

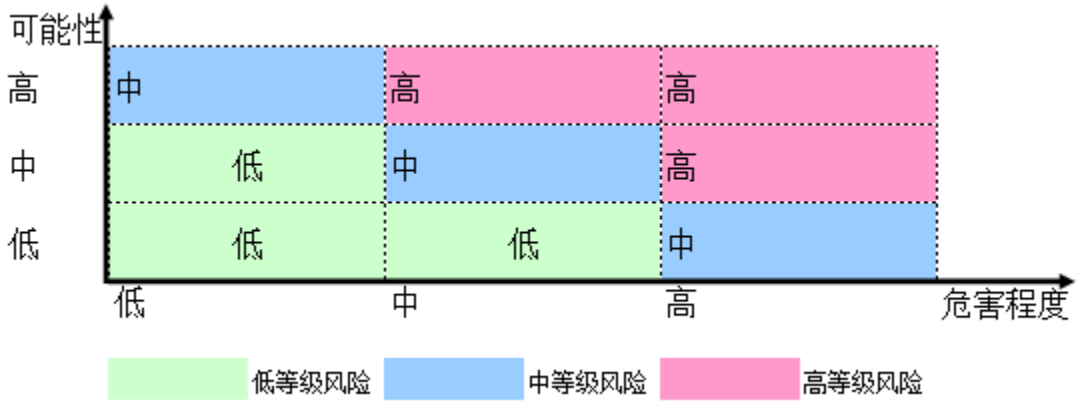

图 3.4.1-1 风险数量较少时的风险等级

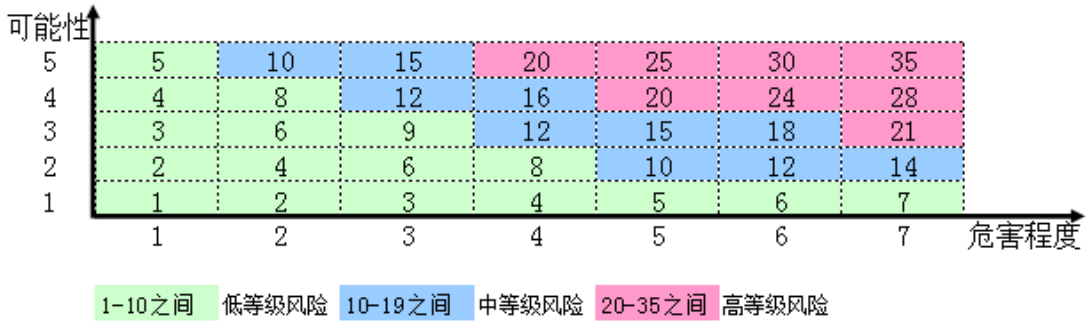

图 3.4.1-2 风险数量较多时的风险等级

需注意，对于高等级风险应立即采取措施降级至中等级或低等级风险；对于中等级风险，安全措施及投入资本应尽可能完善；对于低等级的风险，需制定必要的安全措施。

3.4.1.1 风险发生的可能性

对风险发生的可能性进行评估时，应注意借鉴现有经验，并考虑风险的发展趋势。同时，应尽量采用偏向安全的判定结果。

对于网络系统的维护和管理由合作方承担部分或全部的职能的情况，由于船公司无法评估合作方承担的职能，因此，合作方应向公司递交评估报告以便公司审查。此时，公司网络风险管理体系应适当地指向合作方的网络风险管理。

网络风险发生的可能性受到网络现状和所处的环境及使用者所影响，对风险发生的可能性进行分析需注意网络现状及网络所处的环境因素，例如：

- 已使用的网络控制手段；
- 网络连接的数据交换，存在双向（上行和下行）及单向（上行或下行）两种情况；
- 利益相关方参与船舶操作，可能导致的责任不清和硬件投入不足；
- 全球供应链中，船舶与相关方的网络界面；
- 设备远程监控界面；
- 与岸基合作方共享的敏感信息；
- 用于控制船舶安全和防污染的关键设备的计算机系统；
- 技术人员、供方、港口官员、岸站代表、代理、引水员等的移动介质；
- 允许个人设备接入船舶系统或网络；
- 第三方软件（船舶管理、稳性、船体应力、海图更新、闭路电视等）。

3.4.1.2 风险的危害程度

海事网络风险危害程度评估时，至少应从保密性、完整性和有效性（CIA 模型）三个方面，考虑船舶操作、资产安全、人身安全、防止污染受到危害的程度。

- 保密性：非法连接和非法泄露船舶、船员、货物和乘客等信息和数据；
- 完整性：修改或破坏涉及管理和操作的安全性、有效性的信息和数据；
- 可用性：信息和数据的无法修复或系统服务和操作的无法使用。

以上三项的重要程度与信息或数据的用途相关。例如：对于涉及商务操作的 IT 系统，重点是保密性和完整性。而对于 OT 系统，则主要是完整性和可用性。

3.4.4 风险评估举例

为方便理解并供各方参考，关于风险评估，针对网络情况较为简单的船舶，本指南举例如下表：

序	风险来源	危害的方式	原因	可能性	危害程度	风险程度
1.	无需上网的工作计算机	电脑无法使用或数据丢失，导致无法正常工作	病毒	中	中	中
2.	船舶设备上网	船舶信息、商业信息和个人信息的泄露	木马、后门程序	高	中	高
3.	船舶设备上网	设备参数被修改，导致设备故障或航路偏移等	恶意攻击、木马、后门软件	中	高	高
4.	工作电脑上网	船舶信息、商业信息和个人信息的泄露	木马、后门程序	高	中	高
5.	工作电脑上网	电脑无法使用或数据丢失，导致无法正常工作	病毒、木马、后门程序	中	中	中
6.	船员娱乐上网	个人信息、船舶照片、工作文件的泄露	木马、后门程序	中	中	中
7.	船员娱乐上网	散播病毒在船舶局域网内，导致其他终端中毒	病毒、木马、后门程序	中	中	中
8.	乘客娱乐上网	散播病毒在船舶局域网内，导致其他终端中毒	病毒、木马、后门程序	高	中	高

对于船舶设备上网，应注意到在面临网络风险时，IT 系统和 OT 系统的危害程度不同，并应分开进行评估，本指南举例如下表：

序	风险来源	危害的方式	原因	可能性	危害程度	风险程度
1.	AIS（OT）上网	AIS 数据故障增加船舶搁浅或碰撞风险	病毒、木马、后门程序	中	高	高
2.	GPS（OT）上网	GPS 数据错误增加船舶搁浅	病毒、木马、后门程序	中	高	高

序	风险来源	危害的方式	原因	可能性	危害程度	风险程度
		或偏航风险				
3.	维护保养体系（IT）上网	维护保养不及时，增加设备故障的风险	病毒、木马、后门程序、兼容性	中	中	中

3.5 注意事项

3.5.1 信息（IT）系统和操作（OT）系统

在对船舶的 IT 和 OT 系统进行海事网络风险识别和评估时，应注意：

- ✓ 识别现有保护手段；
- ✓ 识别薄弱环节。人员因素、使用的规定、软件补丁、防火墙版本；
- ✓ 船舶关键操作的薄弱环节识别和评估；
- ✓ 潜在的网络攻击及其影响和概率，以便进行措施的制定；
- ✓ 咨询制造商和供方，以获悉他们在网络安全方面的技术和管理措施；
- ✓ 对于制造阶段的设计不佳或配置不合理导致的网络隐患，应尽快解决。

针对 IT 和 OT 系统基础设施的渗透试验有助于识别防御等级能否满足需求。此类试验通过模拟网络攻击进行，具备很强的完整性，但建议此类试验仅对 IT 系统进行，不建议对 OT 系统进行试验。对 OT 系统可采用被动试验的方法，例如：扫描传输数据，但不应当尝试主动访问 OT 系统或植入软件。

3.5.2 海事网络调研

在海事网络调研阶段，应注意：

- ➢ 列明船舶的关键功能和系统以及他们对安全的危害程度；
- ➢ 列明船舶 IT 和 OT 系统中关键设备的主要厂家；

- 查阅船舶 IT 和 OT 系统关于网络架构、界面和连接的说明；
- 列明涉及网络安全的制造商的联系方式，并建立联系；
- 查阅船舶 IT 和 OT 系统的维护保养文件；
- 船东和管理公司明确在网络和设备维护和技术支持方面的合同要求和责任；
- 评估是否需外部专家、制造商、服务商的支持。

3.5.3 风险评估

在进行风险评估时，风险的来源需注意：

- 技术方面，例如：软件缺陷、软件过期、软件未补丁；
- 设计方面，例如：接入管理、未管理的网络连接；
- 执行方面，例如：电脑、服务器、路由器和其他网络设备的配置；
- 措施不当或其他的人为错误。

3.5.4 记录和报告

风险的量化评估以及制定的安全措施，应予以记录，并形成报告。报告应包括如下几个方面：

- 管理摘要。高度总结评估结果、相关建议和网络安全情况；
- 技术发现。详细报告，包括：风险的来源、可能性、危害程度、风险等级及对应的安全措施；
- 措施的优先级。综合考虑效果、费用和适用性等因素，列明拟采用的安全措施的优先级。同时，措施中不应包括进行第三方评估的公司出售的服务和产品；
- 过程的记录。应注意详细记录各环节的情况、发现的技术细节和薄弱环节、使用的工具和软件名称以及渗透试验恢复后的样本数据等；

- 归档。为便于查询，必要的文字资料应予以归档。

3.5.5 制造商

需要制造商协助时，应当寻求制造商的帮助并协作完成，促进共同改进。

3.5.6 合作方

注意识别合作方的网络是否与公司或船舶的网络有连接。如有连接时，应协作完成风险评估的工作；

注意识别合作方的工作人员是否需使用网络或计算机。如需使用，需至少调研合作方是否有措施保证其工作人员的网络安全意识。

四、 海事网络管理体系

4.1 基本原则

海事网络管理体系是船舶和公司的管理体系的重要组成部分，应作为管理体系的一部分予以运行和改进。

海事网络管理体系需包含标识、保护、发现、响应和恢复的功能。因此，为了确保网络的合理设计、规范建设和正常使用，需根据设定的安全水平和风险评估的结果，在管理体系中包括：

- 制定和执行日常使用的安全措施；
- 制定应急计划，减少和降低网络事件发生后的危害；
- 制定措施确保响应能力，保证应急计划的正常进行；
- 制定恢复计划；
- 调查发生的网络事件。

安全措施能预防网络事件和保证操作。而在网络事件发生后，即使网络事件造成实际危害，管理体系可以帮助各方通过合理应对和积极响应，执行应急计划和恢复计划，尽最大可能使网络恢复到可用状态。

安全措施的制定和风险评估以及公司为了网络安全所做的各种努力，是通过避免和降低风险的发生及其导致的危害，努力使网络达到大家认可和接受的安全水平。因此，在制定安全措施时，应重点考虑安全性。

4.2 海事网络管理体系与安全管理体系

IMO 决议 MSC.428（98）将网络风险识别为特定威胁，公司应尽可能尝试以与可能影响船舶安全运行和环境保护的任何其他风险相同的方式解决这些风险。有关如何将网络风险管理纳入公司 SMS 的更多指导，请参见本指南的附录 1。

网络风险管理应成为有利于船舶安全和有效运行的安全和保障文化的固有

组成部分，并在公司的各个层面进行考虑，包括岸上高级管理人员和船上人员。在船舶运营的背景下，网络事件预计会导致物理效应和潜在的安全和/或污染事故。这意味着公司需要评估船上使用 IT 和 OT 所产生的风险，并建立适当的网络事故保障措施。

在将网络风险管理纳入公司的 SMS 时，应考虑除了对其运营的船舶进行通用风险评估外，特定船舶是否需要进行特定的风险评估。公司应根据特定船舶在其车队中是否具有独特性，考虑是否需要进行特定的风险评估。要考虑的因素包括但不限于 IT 和 OT 在船上的使用程度，系统集成的复杂性以及操作的性质。

4.3 安全措施的深度和范围

由于网络风险的复杂性、隐蔽性和潜伏性，为了提高海事网络中各系统和相关数据的生存能力和恢复能力，对于关键系统和数据，应在探测风险和防范风险方面，注重提高安全措施的范围和深度。

为提高深度，应制定和执行多层措施探测和防范网络事件，例如：

- 船舶保安计划中的保安措施；
- 网络架构的优化，尤其是有效的分隔；
- 网络防火墙和防病毒软件；
- 网络入侵监测工具；
- 软件白名单；
- 访问控制和账户控制
- 密码保护；
- 控制移动介质的使用；
- 人员风险意识和熟练度的培训。

为扩大范围，应注重措施的全面性，确保措施能覆盖到每个可能遭受攻击的系统，避免出现管理真空区域。

对于网络系统高度集成的船舶，为了提高措施的深度，需要将技术手段和程序措施分层运用在各个易受攻击的系统，进而避免某一系统中的薄弱环节被用来绕开其他系统的保护措施。这样，就满足了安全措施在范围方面的要求，即不同系统的薄弱环节不会互相影响。

安全措施的深度和范围互为补充，是海事网络风险管理体系的重要保障。

4.4 安全措施

海事网络安全措施的制定和执行，应注意如下方面：

- 与网络的实际情况相符，具备针对性、操作性和实用性；
- 清晰并易于理解和执行；
- 责任人具备足够的技能和意识履行职责；
- 明确指出船长、责任船员和公司责任人的职责；
- 责任人是否具备足够的知识和技能；
- 船舶网络的维护是否需要由服务商完成；
- 程序化，并是公司方针、体系文件和访问控制的组成部分；
- 关注能提供最大收益的方式或方式的组合；
- 按优先级分类；
- 新船与现有船相比，采用更方便和有效的技术型措施；
- 网络系统设计和配置时的安全措施，会有效提升安全性和系统弹性；
- 特别注意船舶系统的接入无法得到有效控制的情况，例如：进坞、搁置、新船交付、现有船交接等。由于，这些情况下难以发现是否有恶意软件被植入系统中，所以，建议，（1）先移出敏感数据，再重装系统；（2）可能时，在使用前，还需进行恶意软件扫描；（3）OT 系统进行功能试验确保完整性。

为便于将安全措施纳入管理体系，可以将安全措施分类为：技术型安全措施

和程序性安全措施。

安全措施的制定需依据风险评估的结果，为了方便理解二者之间的关系，本指南附录 2 中提供了一些实例供各方参考。

4.4.1 技术型安全措施

技术型安全措施关注通过增加硬件、安装软件、管理权限、设定要求等方式，使网络系统及其管理，在技术方面受到保护，且能在损坏后恢复。

技术型安全措施包括但不限于如下措施：

4.4.1.1 限制及控制网络接口、协议和服务

以清单的形式明确可以访问网络的设备、软件、进程等，在对网络访问进行控制的同时，识别未经授权的网络访问。

路由器应当被锁定以防止被攻击，且关闭不使用的端口以防止非法连接。

4.4.1.2 配置网络设施

为了配置网络设施，例如：防火墙、路由器和开关，应识别网络中的各系统是否需进行控制。通常，船舶的 IT 和 OT 系统都应予以控制。

对需控制的网络应根据情况配备防火墙、安全网关、路由器和开关。

非控制的网络由于是在缺少保护的情况下和网络直接连接，所以，风险较大，因此，非控制的网络应与需控制的网络隔离。

举例如下：

- 对于船舶航行起到关键作用的网络，应当高度保护；
- 对于合作方用于访问 OT 系统的网络（系统更新或在线服务）需控制。且可连接该网络的岸基设备应防止非法登陆；
- 非控制的网络通常为乘客网络、船员娱乐网络、无线网络等；
- 岸基仅能监视的船舶闭路电视可为非控制的网络。

船上网络应通过防火墙建立安全区。安全区内连接越少，越安全。保密系统和关键安全系统应在保护程度最高的分区。

4.4.1.3 限制场所（物理安全）

与 ISPS 一致，同时作为网络安全的一个核心环节，对于设有船舶保安和安全关键设备及其电缆的处所，应对进入进行限制。

4.4.1.4 监测、阻止和报警

识别侵入和感染是控制的关键。

可通过明确网络操作和数据流的基准，设定并管理网络警报的临界点。为此，应当明确监测的责任人和职责。

可选择使用“入侵监测系统”或“入侵防护系统”或防火墙自带功能，识别威胁、恶意软件及代码，并记录、报告并尝试阻止。船上的责任人应能识别报警并了解其含义。发现的事件应当告知相应的负责人员或服务商。

4.4.1.5 卫星和无线电通信

卫星和无线电通信的措施应当和服务商合作。

航行和控制系统需上行连接到岸基合作方时，需考虑如何防止其非法连接到船上的系统。

接入连接是通信分销商的责任。用户末端通过路由到各终端的连接是船东的责任。在终端，应当确保数据安全，防火墙和专用连接的功能。

当使用 VPN 时，应当加密。此外，还需在服务器和计算机接入网络前设置防火墙。应寻求通信分销商的建议，选择适合此类连接的路由和连接方式。同时，船东和通信分销商应考虑 VPN 连接的岸基过滤。

卫星通讯终端和其他通讯设备已安装厂家的管理软件，且该软件能够通过网页的形式访问和管理。建议公司在保安评估时予以考虑。

4.4.1.6 无线接入控制

无线接入控制应限定在合适的、授权的设备，并使用定期更新的强密码保护。

4.4.1.7 恶意软件检测

用于自动检测和识别恶意软件的查杀软件，应定期更新。

通常，船上计算机与岸上计算机的保护等级应一致。对于所有工作相关的计算机，防病毒和防恶意软件的软件应安装、维护和更新。

4.4.1.8 软硬件的安全设置

仅高级官员可以进行管理员配置，以便管理和安装及变更用户权限。用户权限需限定在仅供所需使用的范围，且不允许其变更系统或安装和运行新程序。

4.4.1.9 邮件和浏览器保护

邮件联系是船岸联络的关键活动。邮件和浏览器保护包括：

- 防止岸基人员和船上人员受到社会工程学危害；
- 防止邮件被用于泄露敏感信息；
- 确保通过邮件或语音交流的敏感信息，在保密性和完整性方面受到保护；
- 防止浏览器和邮件客户端运行恶意软件脚本。

推荐方法包括：

- 邮件压缩或加密；
- 禁止邮件系统含有链接；
- 避免使用通用邮件地址；
- 系统的用户权限设置。

4.4.1.10 数据修复能力

数据修复能力指修复系统或从安全备份或影像文件中恢复数据，从而获取一个安全的系统。因此，必要的信息和足够的软件备份设施应当安全保存，以便能在网络事件后使用。

保留间隔期和备份方案需明确，以便优先对应当快速回复的关键系统进行操作，进而减少危害。对数据依赖较多的系统，应予以更多关注。对于安全航行和船舶操作至关重要的 OT 系统，应设有备用系统，以便提供快速修复的能力。

4.4.1.11 应用软件升级

应用软件的关键安全补丁和升级需及时和正确地完成，以早日修复系统中的安全漏洞。

4.4.2 程序型安全措施

程序型安全措施关注人员如何使用船上的系统。对于包含敏感信息的措施应保密，且根据公司策略操作。

程序型安全措施包括但不限于如下措施：

4.4.2.1 培训和意识

培训和意识是网络安全有效防护的关键支持因素。

来自内部的网络攻击需予以注意并重视。

可根据职责不同，对船上人员和岸基人员的培训和意识培养适当分类。并注意到即使是 IT 和 OT 系统中的关键角色，也会由于疏忽而引起风险。

合作方应进行网络安全保护和培训。必要时，船东和管理公司应向合作方确认其网络保护情况。

网络安全宣传材料应方便所有人员使用，建议其内容包括：

- 邮件风险及如何安全操作；

- 上网的风险；
- 使用自有设备的风险；
- 避免使用被感染的硬件或软件在公司硬件上安装和维护软件；
- 保护信息、密码和数字证书；
- 非公司人员导致的网络风险；
- 检测可疑行为或设备及可疑网络事件正在发生时如何报告；
- 网络事件对船舶安全和操作的后果或影响的意识；
- 熟悉日常安全措施的操作；
- 用于合作方移动介质在连接船舶系统前的保护措施；
- 不能因杀毒软件和防恶意攻击软件的使用而降低其他要求。

网络风险管理中承担职责的人员，应能识别计算机受损后的迹象，例如：

- 没有响应或响应慢；
- 意料之外的密码变更或合法用户被系统阻挡；
- 程序中的意外错误；
- 磁盘空间或内存空间的意外或突然变化；
- 意外退回的邮件；
- 意外的网络连接困难；
- 系统崩溃频发；
- 不正常活动的硬件或进程；
- 浏览器、软件、设置、权限的异常变化。

如使用“入侵监测系统”，责任人应能正确阅读该系统的报告，以便早日发现潜在的威胁。

4.4.2.2 访客权限

需适当限制政府官员、技术人员、代理、港口官员和船东代表使用船上电脑。

关键性的 OT 系统，需通过明显的物理措施予以保护，以防止非法使用。

对于访客使用船舶网络的情况，应尽量避免。确需使用时，应设定权限。

服务商由于维护而需连接网络时，应得到认可，且遵守安全规定。

访客使用的电脑和打印机，应当与所有受到保护的网络及设备隔离。

为防止移动设施的接入，对于所在处所未予以防护的计算机和网络端口，应在可用端口上加锁或安装隔离设施。

4.4.2.3 升级和软件维护

软件和硬件需通过技术支持和更新以应对潜在的漏洞。因此，对于技术支持或更新无法获取的软件和硬件，应当在网络风险评估中仔细确认可用性。

软件和硬件的更新情况，需确保在适当的安全水平。更新的时间间隔可依据船型、网络速度、海上时间等因素判定。操作系统的软件应尽快更新。

路由器、开关、防火墙、各种 OT 设施使用自有固件运行。如这些固件需要定期更新，则应当通过程序要求予以明确。

应注意软件的有效维护取决于生命周期中维护措施的制定和执行。

4.4.2.4 防毒软件和防恶意软件工具的更新

通过程序要求确保不仅船舶能及时获得更新，而且船上电脑会及时安装更新。

4.4.2.5 远程访问

通过程序要求对 IT 和 OT 系统的远程访问予以控制。

建立指南以明确有权访问的人员，访问的时间，访问的内容。

涉及远程访问的各项要求，应明确船长和其他关键船员的协调合作。

当远程访问导致 IT 或 OT 系统损坏时，应当记录备查。

需要远程访问的系统需清晰地识别、监测和定期查验。

4.4.2.6 管理员权限的使用

信息的访问权限应当限定在相关授权的人员。

管理员权限能够对系统设置和数据进行完全的访问。管理员账户登录后，会使得现有的薄弱环节更容易被攻击。管理员权限只能由因公司或船舶工作需要，且经过适当培训的人员使用。无论如何，管理员权限应当被限定在需要时才使用。

用户权限的管理应注意及时删除不再使用的账号。用户账号不能从一个用户传递到下一个用户。对于岸基远程访问船舶系统的人员，同样适用本条类似的要求。

需注意到相关方会被授予访问船舶系统的权限。而一些服务供方往往既具备船舶的丰富知识还拥有较高的权限，所以，应当予以关注。

为了保护保密数据和关键系统，应制定强密码策略。密码应为强密码且定期变更。公司应注意到过于复杂的密码，如果需要定期更换，会被记录在纸上且放在电脑旁边的风险。

4.4.2.7 物理介质和移动介质

从非控制系统向控制系统转移数据，意味着恶意软件风险的转移。移动介质可以绕开防御的多个层面，并能用来攻击未连入网络的系统。因此需指定清晰明确的使用规定，从而确保正常情况下，这类设备不用于在非控制系统与控制系统间传递信息。

对于不可避免的使用移动介质的情况，应当按照规定进行恶意软件的检查以及通过数字签名和水印验证合法性

移动介质的使用规定，应包括未连网的电脑。如果无法在船上进行扫描，例如：维护工程师的笔记本，则应该在登轮前进行，并记录结果和时间。必要时，

公司应当告知港口和岸站，移动介质需扫描检查后，船舶采会允许使用。这些文件包括但不限于：

- 货物文件、装载计划；
- 国家的、客户的和港口当局的表格；
- 加油单；
- 船舶仓库和冷库清单；
- 轮机员维护记录。

4.4.2.8 设备报废及数据销毁

老旧的设备会存储敏感数据或保密信息。为防止外泄，应当制定程序确保老旧的设备在报废前，其存储的数据和信息被销毁。

4.4.2.9 获取岸基支持和应急计划

船舶受到网络攻击时，应能从岸基获得技术支持。技术支持的细节和相关程序应在船上随时可用，并是应急计划的一部分。

4.5 应急计划

制定应急计划时，应注重网络事件的及时发现和安全措施的优先顺序。

制定应急计划和程序时需注意，不应由于网络事件的影响而无法执行。

需特别注意应急计划和相关信息不能为电子版，因为网络事件会出现数据删除和通讯关闭的情况。

应按照 CIA 模型评估网络事件对操作和资产等的影响。通常，IT 系统受损会导致日常工作的连续性，并不影响船舶的安全操作。如网络事件仅涉及 IT 系统，需优先考虑执行事件的调查和系统恢复。

船舶 OT 系统受损，会对船舶安全操作即刻带来明显的影响，因此，应当立即采取有效的手段确保船员安全、船舶安全和防止污染。通常，此类的应急计划

需包括关键系统受损后使用其他模式进行操作。由于涉及船舶安全，相关的操作和应急程序应构成 SMS 的一部分或引用 SMS 中既有的内容。

SMS 中与网络事件相关的不合格报告程序，应明确报告的对象和授权的程度以便船上及时执行应急计划。

船上人员应意识到，因网络事件导致 OT 系统受损需按设备故障对待。

网络事件包括但不限于下列情况：

- 电子航行设备有效性受损或航行相关数据失真；
- 外部数据源的有效性和完整性受损，包括但不限于全球卫星系统；
- 必需的岸基联系失效，包括但不限于 GMDSS 通信；
- 工业控制系统的有效性受损，包括，推进、辅助和其他关键系统，还包括，数据管理和控制的完整性；
- 勒索软件或拒绝服务。

明确责任人，船舶能采取的措施（杀毒、隔离、恢复系统），联系方式，当船舶搞不定时，寻求岸基支持，远程操作（高级工具、管理员设置、关闭服务），操作建议（高级工具、管理员设置、关闭部分服务），锁闭设备后尽快解决。恢复备份计划。

4.6 有效响应

应成立一个包括船上人员、公司人员和/或外部专家的响应团队，承担恢复 IT 和/或 OT 系统的职责，以便船舶能重新正常操作。该团队需具备执行各项安全措施和响应可预见的网络事件的能力。

有效的响应至少包括如下内容：

- 初始评估。团队需识别网络事件的现象、IT 和/或 OT 系统受损的范围和现状、受控数据受损的范围、后续危害；
- 系统和数据的恢复。初始评估后，IT 和 OT 系统及数据应当消除感染、恢复和复原，尽量达到可用的状态；

- 事件调查。为全面了解网络事件的原因和结果，公司应开展事件调查，，以有效防止再次发生；
- 防止再犯。作为纠正的一部分，应基于调查结果改进既有规定。

如网络事件复杂，导致 IT 或 OT 系统无法恢复到正常工作状态，则需进行船舶应急计划中的恢复计划。此时，响应团队应给船舶必要的建议，包括但不限于：

- IT 或 OT 系统是否应关闭或为了保护数据而继续运行；
- 船岸联系的特定连接是否应关闭；
- 使用已安装的防护软件中的高级功能；
- IT 或 OT 系统的损坏超出现有恢复计划的范围。

4.7 恢复计划

由于网络事件并不会自行消失和解决。例如，当 ECDIS 被恶意软件感染后，启动备用 ECDIS 后，会产生下一个网络事件。因此，应当明确如何清理和修复被感染的系统。

恢复计划用于将 IT 和 OT 系统及其数据恢复到能使用的状态，并在船上和岸基有纸质副本。

网络安全责任人应熟悉本计划。

计划的详尽程度取决于船舶的船型和船舶系统。

数据修复能力是有效的技术保护手段，通常采用软件备份数据的方式。软件备份的可用性，不论是船舶还是岸基，都应当能够在网络事件后将数据恢复到可用状态。

当 OT 系统未设有备份系统时，恢复将较为困难。如需岸基支持时，相关信息及负责人应当构成恢复计划的一部分。

如船上人员不具备足够的专业知识和技能，恢复计划可仅限于获取快速的技术支持。如船上人员专业知识和技能较强，可进行更广泛的调查和恢复。

4.8 网络事件的调查

既往案例的经验和教训将有效提升响应能力，所以，应制定信息收集的措施。

为了全面了解发生的网络事件，获取更多的信息，公司按照程序，调查网络事件。必要时，还需寻求外部专家的支持。调查得到的信息，既能提高船舶和岸基的安全管理水平，还能广泛帮助业界应对网络风险。调查时，应做到：

- 帮助船舶和岸基更好的理解潜在的网络风险；
- 总结经验和教训；
- 改进安全措施，防止再犯。

4.9 管理评估和改进

认识到海事网络风险管理是一个持续改进和不断完善的过程，以及，注意到 ISM 规则中定期评估 SMS 有效性的要求，公司应当定期及在网络事件发生后，评估网络风险管理的有效性，并基于评估结果进行相应的改进。

附录 1 海事网络管理体系与安全管理体系

海事组织第 MSC.428（98）号决议明确指出，为了满足 ISM 规范的目标和功能要求，应将网络风险管理纳入到经批准的安全管理体系。该决议引用的海上网络风险管理指南(MSC-FAL.1/Circ.3)提供了包含标识、保护、发现、响应和恢复要素进行网络风险管理的总体性建议。参照海上网络风险管理指南(MSC-FAL.1/Circ.3)，本附录给出如下旨在提供所有公司应考虑实施的建议措施，以便在批准的安全管理体系中纳入网络风险管理。

A.标识

标识角色和职责	
动作	备注
ISM 规则：3.2 更新安全和环境保护方针，以纳入网络风险的内容。	更新的安全和环境保护方针应说明： ➢ 承诺网络风险管理是安全与环境保护方针的一部分； ➢ 理解网络风险管理既有安全又有防护方面，但重点是管理因操作系统、信息系统和网络的使用而产生的风险 ➢ 理解如果没有适当的技术型和程序型预防风险和控制措施，操作系统容易崩溃，并将影响船舶安全运行和环境保护。 更新后的方针不应提及网络风险管理的重视程度比公司面临的其他风险更多或更少。
ISM 规则：3.3 更新安全管理体系中的责任和权限信息，以纳入涉及网络风险管理的责任和权限。	通常，IT 人员应知道计算机系统中的潜在漏洞，并知道适当的技术和程序保护措施，以帮助确保系统和数据的可用性和完整性。 操作和技术人员通常应该了解船上关键系统中断对安全管理系统的安全和环境的影响。 需要更新责任和权限信息的内容包括： ➢ 鼓励 IT 人员（可能由第三方提供）与公司的业务和技术人员合作的职责和权限的分配； ➢ 包含将遵守网络风险管理方针和程序纳入船长的现有责任和权限。
ISM 规则：6.5 运用现有的体系，找出用于网络管理体系的培训项目。	培训是一种构成网络风险管理的基础保护和控制措施。 它有助于帮助了解个人行为将如何影响公司网络的安全运行。应使用现有的程序，识别培训需求，并评估如下方面的益处和需求： ➢ 公司全体人员接受基本的网络安全培训，以支撑公司的网络风险管理方针和程序；

	➢ 承担网络风险管理职责的人员，接受与其职责和权限相匹配的培训。

标识遭到破坏时危及船舶操作的系统、资产、数据和能力	
动作	备注
ISM 规则：10.3 运用现有的体系，识别会导致危险情况的设备和技术系统（OT 和 IT）的突发故障。	对于出现故障会导致险情的设备和技术系统（包括 OT 和 IT）以及相关功能，经批准的安全管理体系已进行了标识，并将可能产生的危害予以记录。 应注意，含有网络风险管理的安全管理体系应标识针对数据丢失导致危险的情况。因为，数据的有效性和完整性对关键系统的影响，在一定程度上，与关键系统变得不可用和不稳定具备同等的危害。所以，在设备和技术系统的清单后，还需附有使用的数据及数据源的清单。

B.保护

风险控制措施	
动作	备注
ISM 规则：1.2.2.2 评估所有已识别的船舶、人员和环境风险，建立适当的保护措施。	公司实施的全部风险控制措施应通过风险评估确定，并考虑本指南中提供的信息。 作为基础，在进行风险评估之前应考虑以下措施。这些技术型和程序型措施，应合适的范围，在各家公司得到实施。 ➢ 硬件清单。制定和维护船上所有关键系统硬件记录，包括公司控制网络上的授权和未授权设备。安全管理体系制定在整个船舶使用寿命期间维护此清单的程序； ➢ 软件清单。制定和维护在公司控制的硬件上运行的所有授权和未授权软件的记录，包括版本和更新状态。应更新安全管理体系以包括以下程序： ✓ 受控硬件更换时的记录要求； ✓ 受控软件更新或更换时的记录要求； ✓ 受控硬件上进行新软件或软件更新时的授权要求； ✓ 防止安装未经授权的软件及在发现后删除； ✓ 软件维护。 ➢ 数据流程图。关键系统与船上和岸上其他设备/技术系统之间的数据流程图，包括第三方提供的数据。在此过程中发现的漏洞应由公司记录并安全保存。应更新安全管理体系包括以下程

	序： ✓ 维护数据流图以反映硬件，软件和/或连接的变化； ✓ 标识并响应新硬件安装后创建的新数据流引起的漏洞； ✓ 审查关键系统与其他 OT 和 IT 系统之间的连接需求。此类审查应基于以下原则：系统应仅在需要船舶安全和有效运行或实现计划维护的端口进行连接； ✓ 控制可移动介质、接入点的使用和点对点或非受控数据流的创建。可通过限制使用可移动介质和禁用关键系统上的 USB 和类似端口来实现。 ➢ 为受控的所有硬件实施安全配置。包括为所有受控的硬件和软件记录和维护普遍接受的安全配置标准。安全管理体系应包括船舶和岸上人员以及第三方分配和使用管理员权限的要求。但是，不建议安全管理体系中包含安全配置的详细信息。该信息应由公司单独和安全地保存。 ➢ 日志核查。应维护并定期核查安全日志，应使用此功能在所有关键系统上启用安全日志记录。 安全管理体系应更新包括以下的程序： ✓ 维护安全日志的方针和程序以及将适任人员的定期核查纳入运行维护程序； ✓ 如适用，应有公司核对和保留安全日志的程序。 ➢ 意识和培训。 ➢ 物理保安措施。通过遵守 ISPS 规则要求的船舶安全计划（SSP）中规定的安全措施，增强了船舶的物理安全。应采取措施限制访问并防止对船上关键系统网络基础设施的未授权访问。

制定应急计划	
动作	备注
ISM 规则：7 更新依赖于 OT 系统的，涉及人员和船舶安全以及环境保护的关键操作的程序、计划和须知	经批准的安全管理体系应该已经包括了涉及人员和船舶安全以及环境保护的关键操作的程序、计划和须知。 通常，这些要求应不受将网络风险管理纳入安全管理体系的影响。这是因为 OT 系统可用性受损导致的危害，或这些系统提供的或使用的数据的完整性受损导致的危害，与 OT 系统不可用或不稳定导致的危害，在一定程度上，是相同的。 尽管如此，如果怀疑网络风险会导致关键系统不可用，则应制定操作须知。须知应恢复备份，以及在

	对不可用进行调查时的防范型的替代措施。 定期检查 OT 系统向操作员提供的信息完整性的程序，应考虑包含在常规的操作维护程序中。
ISM 规则：8.1 更新应急计划，纳入网络事件的响应。	经批准的安全管理体系应该已经包括了船舶安全运行和环境保护所需的关键系统受损后的应急计划。通常，这些计划不应受网络风险管理纳入安全管理系统的影响。这是因为船上普遍的紧急情况的影响，应该与根本原因无关。例如，由于软件故障或设备的不适当维护或操作导致设备故障可能引起的火灾。 尽管如此，为应对 OT 的可用性或它们使用的数据的重大破坏，还应考虑在船舶应急计划的整体系统中制定一个网络事件的模块。该模块的目的是提供船舶安全运行和环境保护所需的多个 OT 系统同时中断的情况下应采取的行动的信息。以及在更复杂的情况下，需要采取适当的立即行动的补充信息。

C.发现

制定和实施及时发现网络事件的措施	
动作	备注
ISM 规则：9.1 更新不符合、事故和险情的报告程序，以纳入网络事件的报告程序。	经批准的安全管理体系已包括与不符合项相关的程序。将网络风险管理纳入安全管理体系时，需包括网络相关的不符合情况报告程序。不符合和网络事件，举例如下： ➢ 未经授权的网络访问； ➢ 未经授权或不当的使用管理员权限； ➢ 可疑的网络活动； ➢ 未经授权访问关键系统； ➢ 未经授权使用可移动介质； ➢ 未经授权连接个人设备； ➢ 不遵守软件维护程序； ➢ 未进行防范恶意软件和网络保护的更新； ➢ 关键系统可用性的丢失或受损； ➢ 关键系统所需数据可用性的丢失或受损。

D.响应

对于会受到网络事件影响的操作或服务，制定和实施措施和计划，以提高生命力，并进行恢复。	
动作	备注
ISM 规则：3.3 确保足够的资源和岸基支持来支持 DPA 应对关键	经批准的安全管理体系已确保提供足够的资源来支持 DPA。在将网络风险管理纳入安全管理体系时，应明确资源还需包括恰当的 IT 操作。这些资源可以

系统的异常	来自公司内部，也可以由第三方提供。在提供足够的资源时，应考虑以下因素： ➢ 公司或第三方技术支持人员应熟悉船上的 IT 和 OT 基础架构和系统； ➢ 任何内部响应团队或外部网络应急响应团队应为 DPA 提供及时的支持。 ➢ 提供船舶与 DPA 之间的替代通信方式，必要时，应能够独立于所有其他系统使用； ➢ 内部审核应注意确认足够的资源，适用时包括第三方，处于及时支持 DPA 的可用状态。
ISM 规则：9.2 更新纠正措施的执行程序，纳入防止网络事件再次发生的措施。	经批准的安全管理体系已包含应对不符合项的程序。通常，这些程序不会受到网络风险管理纳入安全管理体系的影响。但是，这些程序有助于确保： ➢ 考虑不符合项和纠正措施时，关注人员职责和权限； ➢ 纠正措施，包括防止再次发生的措施，是适当和有效的。
ISM 规则：10.3 更新用于提高 OT 系统可靠性的特定措施。	经批准的安全管理体系已经包括提高船上设备可靠性的操作维护程序。将网络风险管理纳入安全管理体系时应注意： ➢ 将软件维护作为操作维护程序的一部分。程序应确保适任人员及时安装和测试软件更新，包括安全补丁； ➢ 在必要和适当的情况下，允许远程访问关键系统以进行软件或其他维护任务。这包括一般性地授权访问（包括验证服务商自身采取的适当保护措施）以及每个特定的远程访问会话； ➢ 防止服务商使用不受控制或受感染的可移动介质进行软件更新； ➢ 定期检查关键系统向操作人员提供的信息，并在关键系统处于已知状态时确认此信息的准确性； ➢ 控制管理员权限的使用，确保软件维护任务由适任人员操作。

E.恢复

备份和恢复会受到网络事件危害的船舶系统	
动作	备注
ISM 规则：10.4 将备份的创建和维护，纳入船舶日常操作维护。	经批准的安全管理体系已包括维护和测试船上设备的备用设施的程序。尽管如此，它可能未包含维护和保存用于安全操作和环境保护所需的数据和系统的离线备份的程序。 将网络风险管理纳入安全管理体系应包括以下程

	序： ➢ 检查关键系统的备份程序； ➢ 检查关键系统的替代操作模式； ➢ 创建或获取备份，包括 OT 的清洁备份，以便从网络事件中恢复； ➢ 维护关键系统安全运行所需的数据备份； ➢ 如适用，备份和清洁备份的离线储存； ➢ 定期测试备份和备份程序。

附录 2 依据风险评估的结果制定安全措施

为方便各方依据风险评估的结果制定安全措施，举例如下表：

序	风险来源	危害的方式	原因	危害程度	可采取的安全措施
1.	无需上网的工作计算机	电脑无法使用或数据丢失，导致无法正常工作	病毒	中	网络安全教育、防病毒软件安装及更新、船舶设备接口管理
2.	船舶设备上网	船舶信息、商业信息和个人信息的泄露	木马、后门程序	中	网络安全教育、上网终端清单、防火墙、防病毒软件安装及更新、服务商管理、船舶设备接口管理
3.	船舶设备上网	设备参数被修改，导致设备故障或航路偏移等	恶意攻击、木马、后门软件	高	网络安全教育、上网终端清单、防火墙、防病毒软件安装及更新、服务商管理、船舶设备接口管理
4.	工作电脑上网	船舶信息、商业信息和个人信息的泄露	木马、后门程序	中	网络安全教育、上网终端清单、防火墙、防病毒软件安装及更新、工作电脑接口管理
5.	工作电脑上网	电脑无法使用或数据丢失，导致无法正常工作	病毒、木马、后门程序	中	网络安全教育、上网终端清单、防火墙、防病毒软件安装及更新、工作电脑接口管理、备份数据、备用计算机
6.	船员娱乐上网	个人信息、船舶照片、工作文件的泄露	木马、后门程序	中	网络安全教育、防火墙、限定上网软件
7.	船员娱乐上网	散播病毒在船舶局域网内，导致其他终端中毒	病毒、木马、后门程序	中	网络安全教育、防火墙、限定上网软件和/或端口
8.	乘客娱乐上网	散播病毒在船舶局域网内，导致其他终端中毒	病毒、木马、后门程序	中	网络安全教育、防火墙、限定上网软件和/或端口

表格中所述的常用安全措施包括：

1.网络安全教育；2.上网终端清单；3.防火墙；4.防病毒软件安装及更新；5.接口管理；6.限定上网软件和/或端口；7.人员管理。

同时，为了定期或必要时知悉船舶防火墙及防病毒软件的工作情况和为船舶提供必要的技术支持和维护，还需考虑：

8.指定船舶网络管理员；9.指定公司网络管理员；10.管理防火墙及防病毒软件的日志；11.采购网络服务商的安全服务。

简介上述方式如下：

1. 网络安全教育。根据船舶网络实际情况，采用培训或宣贯的方式，确保参加培训的人员具备必要的网络安全知识；
2. 上网终端清单。确定上网终端的明细，明确需管理的范围；
3. 防火墙。网络安全的关键设备。通过设置，可控制上网终端的权限，并抵御外来危害。禁止未授权的网络连接上网，对经授权的网络连接采用必要的策略控制性上网；
4. 防病毒软件安装及更新。网络安全的关键软件。防止电脑中毒；
5. 接口管理。减少因 U 盘、移动硬盘、手机等设施，通过接口与设备和电脑连接，导致设备和电脑中毒的情况；
6. 限定上网软件和/或端口。根据工作和娱乐需求，在限定上网终端的同时，限定上网终端可以上网的软件和/或端口，进一步确保安全；
7. 人员管理。识别登轮人员身份。对关键设备服务商、维修方的身份需加强管理。船舶关键处所需值班或无人时锁闭；
8. 指定船舶网络管理员。设定责任人，并需知识更新培训。具备在岸基支持的情况下，完成简单的网络安全维护及参数变更；
9. 指定公司网络管理员。设定责任人，为船舶提供岸基支持，并方便联系；
10. 管理防火墙及防病毒软件的日志。船舶网络管理员定期查阅日志，异常情况，及时向公司汇报。如可能，可由公司网络管理员远程管理；
11. 采购网络服务商的安全服务。注意到网络安全的专业性，公司可考虑采购网络服务商的安全服务，以便得到更专业的服务以及定期实船验证船舶网络安全。