

安全、风险和合规管理

IMO网络风险管理指南 初级读本

知道什么以及如何遵守





目录

安全和风险管理的重要性.....	3
IMO的CRM模型	4
专注于CRM概念.....	5
建立网络安全深度和广度防御	5
建立或增强网络安全计划的关键程序.....	7
识别易受攻击的船载网络技术	8
关于美国保赔协会	9
保赔险	9
关于ABS集团	9

鼓励组织在2021年1月1日之后对公司的合规文件进行首次年度验证之前,在安全管理系统中应对网络风险管理。

过去20年来,海上网络安全一直是困扰并引起人们争论的焦点问题之一。过去5年中,各国政府、船旗国、船舶所有人和经营人等一直将海上网络安全视为主要的安全问题和操作风险,并致力于就海洋产业如何有效控制不断进化的网络威胁提供建议和指引。

对许多于航运安全和海洋环境保护非常重要的系统的操作、控制而言,网络技术已经变得至关重要。-IMO

国际海事组织(IMO)提升了海上人命安全和环境。2017年,IMO发布了通函《海事网络风险管理指南》(《网络风险管理指南》),并在2018年通过了一项旨在对航运业抵御潜在网络攻击或者事故的安全措施提供帮助的决议。

IMO的《网络风险管理指南》建议海事组织开始实施网络风险控制并建立网络弹性。IMO决议建议组织在2021年1月1日之后对公司的合规文件进行首次年度验证之前,在安全管理系统中应对网络风险管理。

安全和风险管理的重要性

尽管IMO2017年的决议仅是“鼓励”网络风险管理(CRM)合规,重要的是大家应当认识到,网络安全对您的业务,对海上财产和操作的安全性、完整性、可靠性都至关重要且起到决定作用。

在采用IMO的前瞻性指南支持有效的网络风险管理实践的同时,我们建议各个组织建立一套全面的网络安全功能,以促进与国际标准和/或船旗国和港口管理要求的适当程度的合规。





IMO的网络风险管理模型源于被普遍采用的国家标准与技术研究所(NIST)网络安全框架

IMO的CRM模型

根据从IMO获取的信息,CRM是“识别、分析、评估并传达与网络相关的风险,并接受、避免、转化或者减轻这种风险至一个可接受的水平,考虑对利益相关者采取行动的成本和收益的程序。”

除了IMO指南,一个联合行业集团,包括波罗的海国际航运公会(BIMCO)、国际邮轮协会(CLIA)、国际航运商会(ICS)、国际干散货船东协会(INTERCARGO)、国际船舶管理人协会(IMTERMANAGER)、国际独立油轮船东协会(INTERTANKO)、国际海上保险联盟(IUMI)、石油公司国际海事论坛(OCIMF)和世界航运理事会(WORLD SHIPPING COUNCIL),发布了深入的《船上网络安全指南》。该《指南》在众多的合规要素中,对IMO的网络指南、风险评估和深度和广度风险防御进行了增补。

升级您的SMS,意味着理解并采纳CRM原理,实施适当水平的网络风险管理,建立网络安全能力和对整体网络弹性的持续监管,以预防、应对网络事故并在发生网络事故后恢复。



图1 – NIST网络安全框架

专注于CRM概念

IMO首先将海上网络风险定义为一种衡量技术资产（例如，海上船舶上的系统）受到潜在情况或事件威胁，导致与航运相关的操作失灵或者出现安全故障的程度的度量。其中包括由于网络事件而被破坏、丢失或破坏的信息或系统。

网络风险管理表示识别、分析、评估并传达与网络相关的风险，并避免、转化或者减轻这种风险至一个可接受的水平的程序。

IMO表明，有效的CRM应当考虑暴露或者利用网络漏洞对信息技术（IT）系统和操作技术（OT）系统的安全影响。

健康、环保、安全和质量系统，包括SMS，是经过深思熟虑得出的成果，并且包含了恰当控制这些风险的政策和程序。控制与安全相关的网络风险要求对现有的SMS有深刻的理解，并且网络相关元素要融入安全系统并与之成为一个整体。

IMO的CRM模型源于被普遍采用的国家标准与技术研究所（NIST）的网络安全框架。NIST框架为构建网络安全计划提供了清晰的过程模型，该模型参考了许多国际网络最佳实践，从确定您组织的关键技术一直到安全地从网络事件中恢复过来，都可以参考。

IMO指南汇聚了支持有效海上安全的功能要素，或者仅是以最优实践对CRM进行了补充：

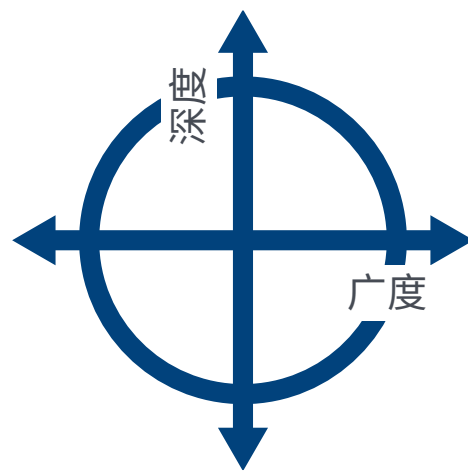
- **识别**——定义人员在CRM中的角色/责任，识别混乱时对船舶运营构成危险的系统、财产、数据和能力。
- **保护**——实施风险控制流程和措施，制定应急计划以防范网络事件并确保船舶运营的连续性。

- **探测**——制定并实施必要的活动以及及时发现网络事件。
- **应对**——制定并实施活动和计划，以提供因网络事件而受损的运输操作或服务所必需的弹性和恢复系统。
- **修复**——确定措施来备份和恢复受网络事件影响的航运运营所必需的网络系统。

因此，IMO建议对网络风险采取一种具有弹性的风险管理方法，这种管理方法作为现有安全的自然延伸可以不断进化。

建立网络安全深度和广度防御

联合企业集团在其网络安全指南中强调的一个重要概念是“在深度和广度上进行防御”。在技术层面这个概念的含义分三个部分：知道必须实施的建立和保持约定水平的网络安全的必要行动，知道在组织中谁对网络安全管理负责，以及发展多层次的保护和探测手段。深度防御是一种强有力的、一体的并且分层次的方法，包括程序、政策和技术等；广度防御意味着要覆盖所有的脆弱的网络技术，基本上是系统的系统方法。



联合企业集团指出,用多层保护措施来保护关键系统和数据是非常重要的,这些措施考虑了人员、程序和技术在以下方面的作用:

- 增加检测到网络事件的可能性
- 增加IT系统和OT系统的保护信息、数据或可用性所需的精力和资源

风险控制	企业	船舶	风险控制	企业	船舶
风险评估	✓	✓	事件响应能力	✓	✓
培训与了解	✓	✓	风险管理程序	✓	
供应商风险管理	✓	✓	数据修复	✓	✓
应变管理	✓	✓	访问控制(IDAM)	✓	✓
事件应对计划	✓		邮件/网络管理	✓	✓
发展策略	✓		漏洞管理		✓
网络体系结构审核		✓	补丁管理		✓
漏洞扫描		✓	入侵检测		✓
登录监管		✓	白名单		✓
资产清单		✓	恶意软件管理		✓
			实体安全		✓
			可移动媒体		✓
			资产管理		✓

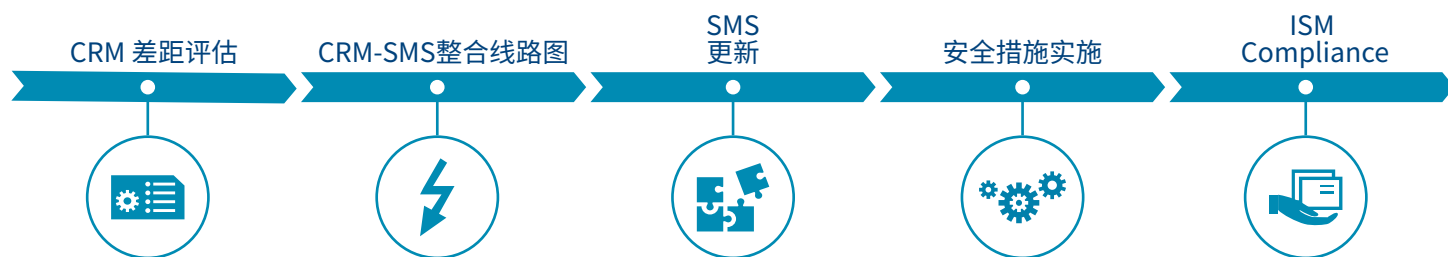
图 2 – ABS集团建议采用上述网络安全控制措施以符合IMO要求

联合企业集团强调, 船载OT系统应该要求一项以上的技术和/或程序保护措施。通过深度和广度的防御方法, 船舶所有人将考虑保护和检测的组合, 从根据船舶安全计划的船舶物理安全到网络保护和入侵检测, 再到定期与网络安全控制有关的扫描/测试和程序性活动。

深度和广度防御指南要求您制定一套全面的安全措施, 也称为控制措施。



建立或增强网络安全计划的关键程序



开发CRM程序不仅仅涉及程序和政策,还在于技术的实施和管理。CRM主题和功能与多个SMS (ISM代码) 保持一致。每个组织的正确解决方案将有所不同。这会有共同的元素,但这取决于风险环境。联合企业集团建议先进行风险评估,然后再制定攻略以开发适合其情况的能力。

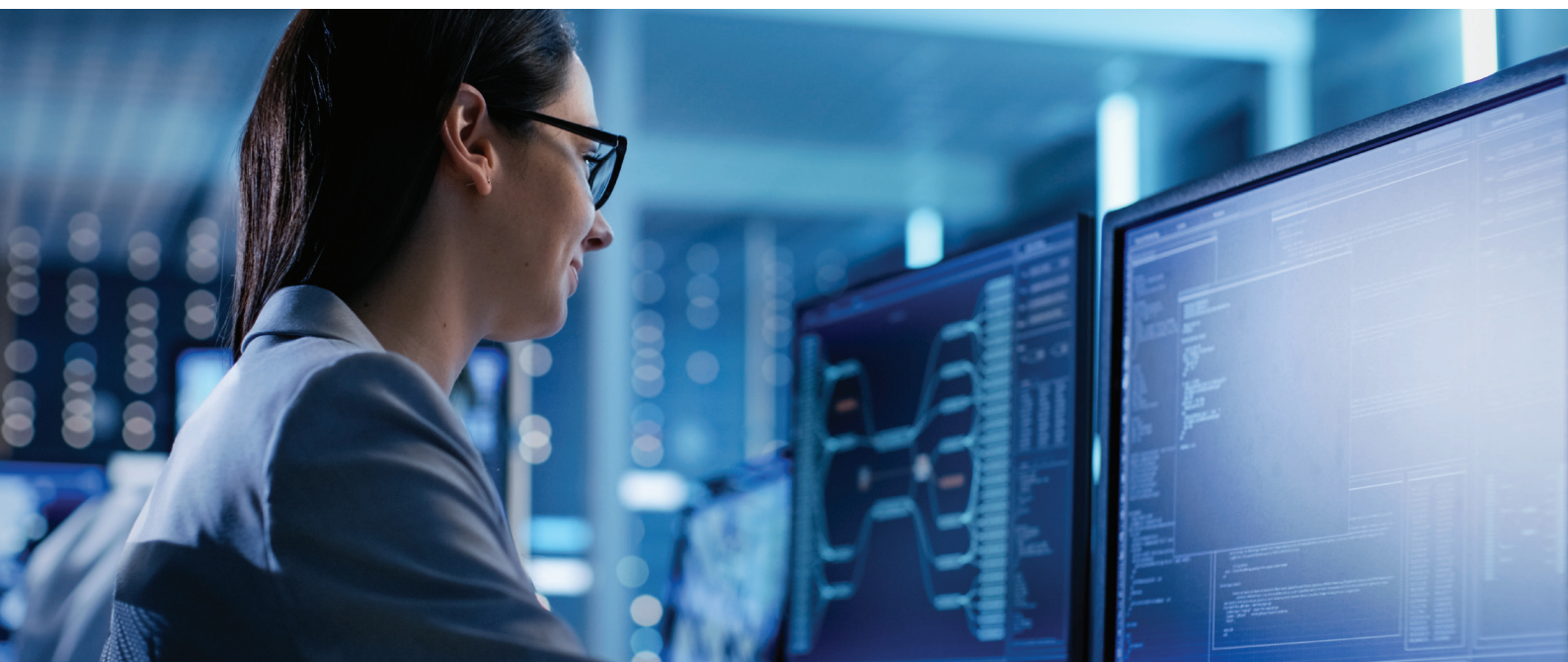
CRM 差距评估:针对IMO2021的要求,实施自我评估或第三方差距分析,此类评估或分析应专注于IMO和联合企业集团对五个关键CRM基本原理的关注:识别、保护、探测、应对及修复

CRM-SMS线路图:制定基于风险的策略以更新SMS,并在您的组织中建立CRM性能

CRM-SMS集成:通过集合您的CRM政策、过程和策略来开发程序中的保护措施以便更新SMS

安全措施实施:实施全面的网络程序和性能,以满足IMO准则

建立和维护网络安全功能所需的大部分工作都集中在补救、缓解和管理关键技术中的漏洞。因此,首先要着重于确定网络技术和漏洞,以便更好地了解为CRM的投资计划和预算。



识别易受攻击的船载网络技术

据国际海事组织 (IMO) 表示, 网络技术 (关键技术) 已成为众多系统运行和管理必不可少的系统, 这些系统对于运输的安全和保障以及海洋环境的保护至关重要。这些系统中的漏洞可能是由于设计, 集成和维护实践不充分 (例如人为错误) 或缺乏与组织内保护网络系统相关的技术专业知识, 能力或管理所致。

暴露于网络风险中的易受攻击的OT资产, 包括但不限于:

- 桥梁导航系统
- 货物装卸和管理系统
- 推进和机械管理及动力控制系统
- 控制登陆系统
- 行政及船员的福利系统
- 交流系统

因为航运产业的科技在快速发展, 且数字化已经成为市场现实, 但网络威胁的发展速度快于能力建设的速度。这种变化和不确定性不仅鼓励网络威胁参与者利用虚拟漏洞和漏洞, 而且使船东和经营者仅通过技术标准来解决网络风险变得困难。

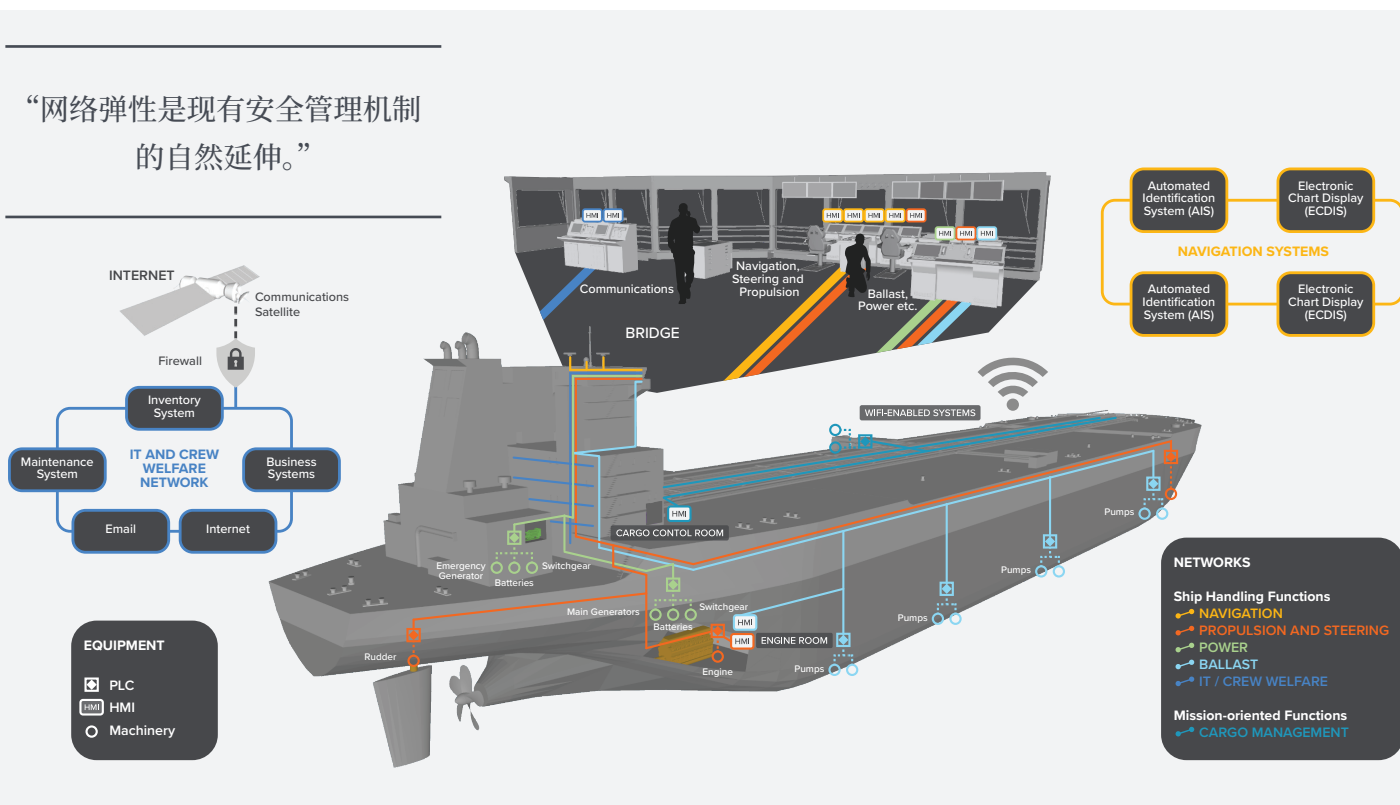


图 3 - 暴露于网络风险中的易受攻击的OT资产包括导航, 推进, 访问控制, 管理和通信系统。

关于网络风险管理的实践方法, 联合企业集团建议会员确定组织存在哪些威胁和漏洞, 评估风险, 制定保护和检测措施, 制定应急计划以及 (如果发生网络事件) 知道如何应对并从网络安全事件中恢复。联合企业集团表示, 这种实践方法是从深度和广度上对网络风险管理的防御。

关于 ABS Group

ABS集团公司 (www.abs-group.com) 通过其运营子公司, 提供数据驱动的风险和可靠性解决方案以及技术服务, 以帮助客户确认关键资产和运营的安全性、完整性、质量和环境效率。ABS集团总部位于得克萨斯州的Spring, 在20多个国家/地区拥有1,000多名专业人员, 为海洋和近海, 石油, 天然气和化工, 政府和工业部门提供服务。ABS集团是ABS (www.eagle.org) 的子公司, ABS是世界领先的海洋和海洋工程船级社之一。

cyber@abs-group.com | www.abs-group.com/cyber

关于美国船东互保协会

1917年, 美国船东互保协会 (美保) 于纽约成立, 其总部位于纽约, 是美国唯一一家互保协会。近年来, 美保以其美国传统, 成功打造了业内数一数二的国际保险公司。美保的日常管理由位于纽约总部的船东索赔局负责。美保能够为所有时区的会员提供当地服务, 并能够用多种语言与会员进行沟通。同时, 美保在伦敦, 比雷埃夫斯, 香港, 上海和休斯敦设有办公室, 此外, 美保还设有全球通代网络。美保是国际保赔协会集团的成员之一, 国际保赔协会集团由13个协会组成, 共同为世界90%的航运提供保赔险服务。关于美保的更多信息, 请见如下网址 www.american-club.com。

保赔险

保护和赔偿保险 (通常简称为“保赔险”) 为船东和租家在商业营运中提供第三方责任险; 其典型的承保风险范围包括货损、污染、乘客或船员的伤病亡以及码头和其他设施的损坏。基于互惠互利的非营利原则, 传统的保赔险与船舶险同时使用, 这与通常的海上保险形式不同, 因为协会会员既是保险人又是被保险人。

info@american-club.com | www.american-club.com