指导性文件
GUIDANCE NOTES
GD25-2019

中 国 船 级 社

CHINA CLASSIFICATION SOCIETY

船舶网络系统要求及安全评估指南

Guidelines for Requirement and Security Assessment of Ship Cyber System

2020

生效日期：**2020** 年 **3** 月 **1** 日

目　录

前　言

近年来，随着船舶数字化、智能化、网络化发展水平的提升，越来越多的控制系统、通讯导航系统、信息管理系统及设备不断接入船舶网络，实现对外信息交互。船舶越来越多的“在线”，使船舶遭受网络威胁的隐患不断加剧，在这样的背景下，船舶的网络安全显得尤为重要。

基于提升应对网络风险威胁意识的迫切需求，IMO 在 98 届海上安全委员会通过并发布了《海事网络风险管理指南》（MSC-FAL.1/Circ3）通函，提出了对网络风险的应对措施。IACS 于 2018 年发布针对船舶网络安全的 12 项建议案，国际海事界对船舶网络风险问题的认识正不断提升。

为此，中国船级社组织编制了本指南，旨在规范船舶网络的建设、运维、评估和检验工作，使有关的管理人员和技术人员理解船舶网络安全的重要性，形成综合提升船舶网络系统建设水平、威胁防御能力的新观念，保障船舶网络环境的稳定性，并为船舶的智能化、数字化、网络化提供基本的条件与保障。

指南面向船舶网络系统的设计、实施、运行、退役等环节，针对操作、集成、维护、设计、安全意识、管理水平等方面的风险点，为船东/船舶管理公司、系统开发方等提供网络系统建设指导，并提供安全评估方法、检验和试验要求。

第1章 通则

第1节 一般规定

1.1.1. 适用范围

1.1.1.1. 本指南适用于基于数字通信方式的船舶网络系统和设备。

1.1.1.2. 本指南为船舶（包括船舶及海上设施）网络及系统的建设、运维、评估和检验提供指导，以保障船舶网络及系统具备安全性及必要的威胁防御能力，并为实施船舶网络安全风险管理提供参考和操作指导。

1.1.1.3. 本指南主要包含以下内容：

（1） 从技术和管理两个方面指导船舶网络系统建设和运维；

（2） 产品安全评估要求；

（3） 船舶检验要求。

1.1.2. 一般要求

1.1.2.1. 应采取有效的技术措施，并建立和实施有效的船舶网络安全风险管理制度，以提高对网络安全威胁的抵御能力，确保网络安全风险处于可接受水平，满足相关方（运营方、使用方、监管方等）对网络安全的期望。可接受水平系指安全风险（安全事件出现的可能性和后果）的最大可承受限度。

1.1.2.2. 船舶网络设计方，应进行船舶网络安全规划，明确船舶网络安全工作的总体方针和安全策略，形成船舶网络安全规划说明书，说明安全工作的目标、范围、原则等，阐明管理措施如何与技术措施共同构成完整的安全体系。

1.1.2.3. 船舶网络设计方，应开展设计阶段网络安全风险评估，分析评估设计方案与网络安全规划（目标和需求等）和相关标准的符合性，以完善设计方案，并作为网络系统建设过程的风险控制依据。

1.1.2.4. 船舶制造方和/或船舶网络集成方等建设方，应在网络系统开工建设前制定/完善网络安全建设管理制度，完善相关设备设施和技术措施，以确保建设期间的网络安全风险处于可接受水平。

1.1.2.5. 船舶运营方和/或船舶网络使用方等运维方，应在船舶试航/网络系统运行前，开展运维阶段网络安全风险评估，并基于评估结果制定/完善船舶网络安全运维管理制度，完善相关设备设施和技术措施，以确保运维期间的网络安全风险处于可接受水平。

第2节 附加标志

1.2.1. 附加标志及评估报告

1.2.1.1. 对于网络系统产品，经申请，并经本社审图和评估合格，向其签发评估报告。

1.2.1.2. 对于船舶网络系统，经申请，并经本社审图和评估合格，向船舶授予如下附加标志：

Cyber Security (P，S)

其中，P表示满足基本要求，S表示满足高级要求。

（1） P 级应满足本指南第 2 章管理要求，以及表 1.1.3.2 所列技术要求；

P 级技术要求 **表 1.1.3.2**

	条目	条目名称	P 级
物理安全	3.2.1	物理处所要求	√
	3.2.2	物理访问控制	√
	3.2.3	设备安装部署	√
网络架构	3.3.1	网络冗余	-
	3.3.2	网络隔离与分段	√
	3.3.3	通信安全	√
	3.3.4	无线网络	√
	3.3.5	资产清单	√
	3.3.6	网络测试	√
区域边界	3.4.1	边界防护	√
	3.4.2	恶意代码防范	√
	3.4.3	入侵防范	-
	3.4.4	监测与报警	-
	3.4.5	远程运维（如适用）	√
	3.4.6	访问控制	√
计算环境	3.5.1	身份鉴别	√
	3.5.2	数据安全	√
	3.5.3	系统安装与更新	√
	3.5.4	应急响应与事故恢复	√
	3.5.5	备份	√
安全审计	3.6.1	配置要求	√
	3.6.2	安全审计（日志）	-

（2） S 级应满足本指南第 2 章管理要求和第 3 章技术要求。

1.2.1.3. 船舶网络安全附加标志的授予、保持、暂停、取消和恢复应符合本社《钢质海船入级规范》第 1 篇第 2 章第 9 节的规定。

1.2.2. 申请

1.2.2.1. 申请本社进行船舶网络安全评估的系统和/或船舶，应向本社或本社指定单位或本社的当地分支机构提出书面申请，必要时可签订评估服务合同和/或协议。

1.2.2.2. 如果申请船舶网络安全附加标志的系统和/或船舶没有进行过相应评估，本社在接受其申请之前，应按照附录 2 进行预评估。

第3节 术语及规范引用

1.3.1. 术语

1.3.1.1. 访问控制：对系统交互能力和方式的选择性限制，包括使用系统资源处理信息、获得系统信息和知识，或控制系统部件和功能。

1.3.1.2. 资产管理：对任意数据，计算机或设备的控制。

1.3.1.3. 授权：防止未授权用户访问或使用系统，即规定了用户对数据的访问权限。

1.3.1.4. 主干网：是通过桥接器与路由器把不同的子网或 LAN 连接起来形成单个总线或环型拓扑结构。

1.3.1.5. 配置管理：系统性地处理硬件、软件变化的操作和程序，以保持系统或设备的完整性。

1.3.1.6. 控制系统：由控制主体、控制客体和控制媒体组成的具有自身目标和功能的管理系统，可以按照所希望的方式保持和改变机器、机构或其他设备内任何感兴趣或可变的量。

1.3.1.7. 网络安全：网络环境下存储、传输和处理的信息的保密性、完整性和可用性的表征。

1.3.1.8. 数据泄露防护系统：通过身份认证和加密控制以及使用日志的统计对内部文件进行控制的系统。

1.3.1.9. 网络攻击：以访问、危及、损毁公司和/或船舶的系统和数据为目的，针对 IT 和 OT 系统、计算机网络、个人计算机设备的任何型式的攻击性操作。

1.3.1.10. 网络事件：对船上系统，网络和计算机或其处理、储存、传输的信息造成实际或潜在负面影响的事件，且需要通过响应措施来消除其后果。

1.3.1.11. 网络系统：集设施，人员，流程和通讯一体化，并集成网络服务的系统，如信息管理系统、控制系统和访问控制系统。

1.3.1.12. 缺陷：非预期的软件功能。

1.3.1.13. 拒绝服务攻击：网络攻击的一种类型，阻止合法和授权用户访问信息，通常通过服务器缓冲区满溢的方式实现。分布式拒绝服务攻击是由网络攻击者掌控多台计算机和/或服务器来实现拒绝服务攻击的。

1.3.1.14. 防火墙：防止对网络系统设施和信息未授权访问的逻辑或物理阻断。

1.3.1.15. 信息安全：针对信息的安保措施，防止对其未经授权的访问，关闭，修改或销毁。

1.3.1.16. 入侵检测系统：用以监测网络或系统活动，探测恶意或违规操作，并进行报告的设备或软件应用。

1.3.1.17. 入侵防御系统：也称为入侵检测和防御系统，是监测网络和系统恶意活动的网络安全装置。

1.3.1.18. 局域网：在使用网络媒体的有限区域内，使计算机间互相连接的计算机网络。

1.3.1.19. 恶意软件：泛指能传染计算机系统并影响其性能的软件。

1.3.1.20. 网络拓扑结构：用传输媒体互连各种设备的物理布局。

1.3.1.21. 网络传输介质：是网络中发送方与接收方之间的物理通路，如同轴电缆、光纤、无线传输等。

1.3.1.22. 信息技术：用于管理和处理信息所采用的各种技术及系统。

1.3.1.23. 工控系统：即工业自动化控制系统，主要指使用计算机技术，微电子技术，电气手段，使工业制造和运行过程更加自动化、效率化、精确化，并具有可控性及可视性。

1.3.1.24. 操作技术：对船上软件，硬件和相关网络的监测和控制技术及系统。

1.3.1.25. 恢复：在事件之后，短时间内对系统重要的服务和操作，以及长时间内对全部能力的复原活动。

1.3.1.26. 风险评估：为告知优先事项，建立行动方案，并告知决策风险的数据收集和数值分配过程。

1.3.1.27. 风险管理：是一个识别、分析、评估和沟通风险并且接受、避免、转移或控制风险到一个可接受的水平，考虑有关成本和效益举措的过程。

1.3.1.28. 路由器：从一个网络向另一网络转发数据的装置，例如从卫星通信网络将数据转至船用计算机网络。

1.3.1.29. 虚拟局域网：可使地理上分散的网络节点像在同一物理网络里进行通讯。

1.3.1.30. 虚拟专用网络：如同计算机设备直接连接到专用网络那样，可以使得用户通过共享的或公共网络传送和接受数据，从而受益于专用网络的功能性、安全性和管理策略。

1.3.1.31. 病毒：一种隐匿、可自我复制的计算机软件，会恶意感染并操纵计算机程序和系统的运行。

1.3.1.32. Wi-Fi：一种允许电子设备连接到一个无线局域网的技术。

1.3.1.33. I 类、II 类、III 类系统的定义见本社《钢质海船入级规范》第 7 篇第 2 章 2.6.3。

1.3.2. 规范性引用文件

指南引用下列参考文件。凡是注日期的引用文件，仅引用版本适用。凡是不注日期的引用文件，其最新版本适用于本指南。

（1） 中国船级社《钢质海船入级规范》及其修改通报

（2） UR E22

（3） 《工控网络与系统信息安全标准综述 2-1:工业自动化和控制安全管理系统》（IEC 62443-2-1）

（4） 《工控网络与系统信息安全标准综述 3-3：系统安全要求与安全保障等级》（IEC 62443-3-3）

第2章 管理要求

第1节 一般规定

2.1.1. 一般要求

2.1.1.1. 应建立和实施有效的船舶网络安全风险管理制度，以提高对网络安全威胁的抵御能力，确保网络安全风险处于可接受水平，满足相关方（运营方、使用方、监管方等）对网络安全的期望。

2.1.1.2. 有效的安全风险管理制度体系指基于风险的可持续改进的管理制度，涵盖规划与设计、实施与运行、检查和评审、保持和改进，如图 2.1.1.2 所示。

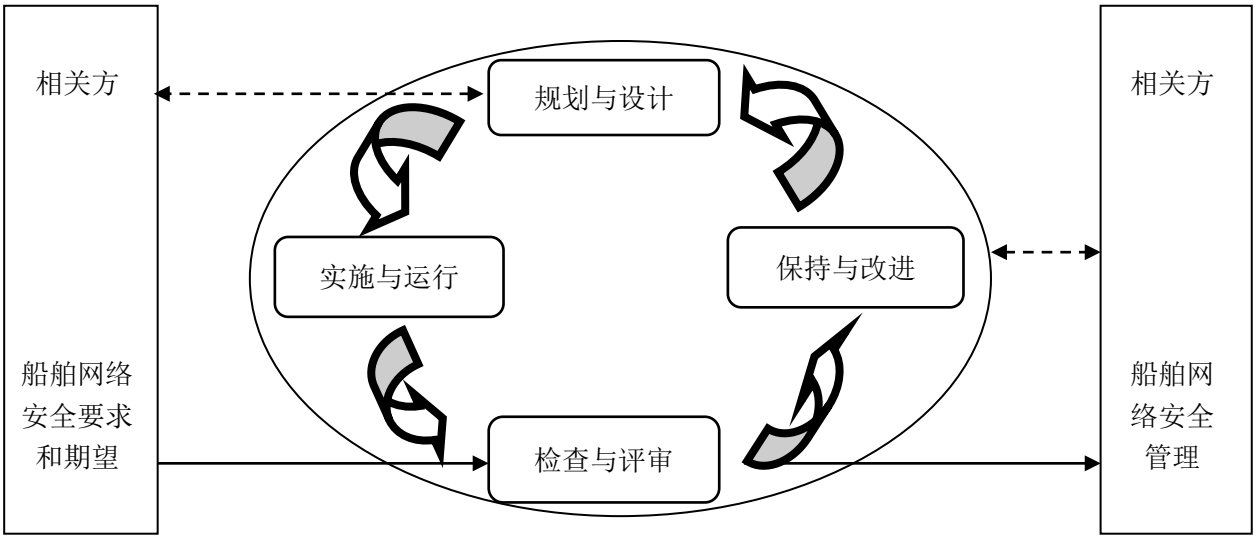

图 2.1.1.2

2.1.1.3. 本章第 2 节~第 6 节为建议性要求，旨在规定船舶网络安全风险管理需考虑的安全要点，为相关方建立和实施船舶网络安全风险管理制度提供指导，可以考虑采用其他有行之有效的管理方式或技术措施予以替代。

2.1.2. 建设管理

2.1.2.1. 应建立建设管理制度，设立安全管理机构与岗位，将管理职责落实到具体机构和人员，并以书面形式通知相关方（包括组织和人员）。

2.1.2.2. 船舶网络系统建设期间，应按制定的建设管理制度开展管理工作，对重要事项形成管理记录，包括但不限于下列内容：

（1） 相关人员的网络安全意识和技能培训/教育；
（2） 网络产品（软、硬件等）采购；
（3） 软件开发；
（4） 重要工程节点，如集成测试、安全测试、上船安装、试航试验、验收交付等；
（5） 网络交付后运营服务商的选择。

2.1.2.3. 船舶网络系统开工建设前，应将最新有效的船舶网络安全建设管理文件提交给验船师检查，以确认管理制度的完整性。

2.1.2.4. 建造检验中，应将船舶网络安全管理机构和人员资料、管理记录文件（包括报告、日志、

记录表单等）提交给验船师检查，以确认安全管理工作符合管理制度运行和安全策略的要求。

2.1.2.5. 重要工程节点，如船舶网络集成测试、网络安全测试、上船安装、试航试验、验收交付等，应有验船师见证。

2.1.3. 运维管理

2.1.3.1. 应建立运维管理制度，设立安全管理机构与岗位，将管理职责落实到具体机构和人员，并以书面形式通知相关方（包括组织和人员）。

2.1.3.2. 船舶网络系统运维期间，应按制定的运维管理制度开展管理工作，对重要事项形成管理记录，包括但不限于：

（1） 相关人员的网络安全意识和技能培训/教育；
（2） 船舶网络与信息资产的安全管理，包括资产登记、变更等；
（3） 运维管理，包括日常运维、应急准备、应急响应、定期检查/检测等；
（4） 运营服务商的安全管理；
（5） 船舶网络系统的风险评估；
（6） 船舶网络安全管理方面的审核和评审（内审和/或外审）。

2.1.3.3. 最新有效的船舶网络安全运维管理文件应在船上随时可用。初次检验时，应将船舶网络安全运维管理文件提交给验船师检查，确认管理制度的完整性。

2.1.3.4. 年度检验时，应将船舶网络安全运维管理机构和人员资料、管理记录文件（包括报告、日志、记录表单等）提交给验船师检查，以确认安全管理工作符合管理制度的要求。

2.1.3.5. 发生重大变化时，应将相关文件资料提交给本社，然后由指定的验船师检查，以确认安全管理工作符合管理制度的要求；发生重大安全事件时，应及时通知本社，并提交事故信息和事故处理措施及解决方案。

第2节 管理制度

2.2.1. 制度与文件

2.2.1.1. 建设方应建立安全建设管理制度，包含但不限于本章第 4 节和第 5 节所列各适用的管理活动。运营方应建立安全运维管理制度，包含但不限于本章第 4 节和第 6 节所列各适用的管理活动。

2.2.1.2. 管理制度应以文件化的形式体现，一般包括管理手册、管理规定/程序、操作规程/须知和记录表单/报告等四个层级。

2.2.1.3. 管理手册为纲领性文件，说明安全管理工作的目标、方针、范围、原则、组织机构、管理活动运作框架和安全策略等。

2.2.1.4. 管理规定/程序为程序性、规定性的文件，描述各管理过程、涉及的管理活动及管理标准，明确管理过程的输入、输出、相互作用。

2.2.1.5. 操作规程/须知为指南和操作性文件，用于具体指导管理工作执行，包括各种操作须知、使用手册和技术规程等。

2.2.1.6. 记录表单/报告为记录性文件，用于进一步规范管理工作的输入和输出。

2.2.2. 制定与发布

2.2.2.1. 应指定或授权专门的部门或人员负责管理制度的制定。

2.2.2.2. 管理制度应经批准后通过正式、有效的方式发布实施，并进行文件版本控制。

2.2.3. 审核与改进

2.2.3.1. 应定期或在发生重大变化时进行内部审核，以确定安全管理制度的实施情况是否符合预期，是否符合相关组织和相关法律法规的要求。

2.2.3.2. 应定期或在发生重大变化时进行管理评审，对安全管理制度的适宜性、符合性、持续性、稳定性、充分性和有效性进行论证，并评价和确定改进的机会、变更的需要。

2.2.3.3. 对检查、审核、评审、安全事件调查等活动中发现的不符合情况，应采取纠正与预防等管控措施，必要时对存在不足或需要改进的安全管理制度进行修订。

第3节 管理机构

2.3.1. 机构与岗位

2.3.1.1. 建设方和使用方宜设立由决策层、管理层和执行层构成的三级管理机构和相关岗位，定义岗位职责，并配备岗位人员或将岗位职责落实到具体人员。有冲突的职责和责任范围应分离，以减少未经授权或无意修改或误用的机会。

2.3.1.2. 决策层一般为指导和管理网络安全管理工作的委员会或领导小组，其最高领导由单位主管/分管领导担任或授权，负责船舶网络安全方针、策略、重大事项等方面的决策。

2.3.1.3. 管理层一般为网络安全管理的职能部门或工作小组，负责船舶网络安全日常管理工作的具体组织和协调。

2.3.1.4. 建设方的执行层一般由安全管理员、系统管理员等岗位构成，负责落实具体管理工作。安全管理员是网络安全的负责人。系统管理员负责网络系统及相关设施的部署、安装、配置、技术支持和日常运维管理。

2.3.1.5. 使用方的执行层一般由船端安全管理员、船端系统管理员、岸端系统管理员等岗位构成。船端安全管理员是船舶网络安全的负责人，一般为船长或其指定人员。岸端系统管理员负责船舶网络系统及相关设施的部署、安装、配置和技术支持。船端系统管理员负责船舶网络系统及相关设施的日常运维管理。

2.3.2. 授权与审批

2.3.2.1. 应根据各职能部门和岗位的职责明确授权审批事项、审批部门和审批人等。

2.3.2.2. 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程。

2.3.2.3. 应定期（间隔不长于 1 年）审查审批事项，及时更新需授权和审批的事项、审批部门和审批人等。

2.3.3. 沟通与合作

2.3.3.1. 应加强各类管理人员、内部机构以及外部机构（监管、检查等）之间的合作与沟通，有条件时组织召开协调会议，共同协作处理网络安全问题。

2.3.3.2. 应加强与网络安全相关的外部机构、各类供应商、业界专家及安全组织的合作与沟通。

2.3.3.3. 应建立网络安全相关的外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

2.3.3.4. 密切关注主管机关、船级社及行业协会的有关网络安全事件的通函、通告，了解网络安全事件的动机和攻击方式，以便识别威胁采取行动。

第4节 基本管理要求

2.4.1. 人员管理

2.4.1.1. 录用与离岗

（1） 应指定或授权专门的部门或人员负责人员录用；

（2） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术能力进行考核；

（3） 应与被录用人员签署保密协议，与关键岗位人员（岸端系统管理员、船端安全管理员等）签署岗位责任协议；

（4） 应及时终止离岗人员的所有访问权限，收回各种身份证件、钥匙、徽章等以及单位提供的软硬件设备、用户账号和其他相关资产；

（5） 应办理严格的调离手续，关键岗位人员尚应承诺调离后的保密义务后方可离开。

2.4.1.2. 培训与考核

（1） 应对各类人员（包括操作人员）进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

（2） 应制定有针对性的培训计划，对安全基础知识、岗位操作规程等进行培训；

（3） 应定期对不同岗位的人员进行船舶网络安全管理和/或操作技能考核。

2.4.1.3. 第三方人员

（1） 在第三方人员物理访问受控区域前，应先提出书面申请，批准后由专人全程陪同，并登记备案；

（2） 在第三方人员接入受控网络访问系统前，应先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

（3） 第三方人员远程接入时，远程接入点不能为公众场合，且应在接入前、接入过程中及接入完成时相互确认；

（4） 第三方人员使用网络系统前（包括设备和应用系统），应接受必要的安全培训/教育；

（5） 第三方人员离场后应及时清除或禁用其所有的访问权限；

（6） 获得系统访问授权的第三方人员应签署保密协议，并接受适当的安全培训/教育，不得进行非授权操作，不得复制和泄露任何敏感和重要信息。

2.4.2. 风险管理

2.4.2.1. 应采取必要的措施识别建设和运维中的安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

2.4.2.2. 应定期或在下列情况下开展网络安全风险评估，形成风险评估报告：
（1） 当发生重大船舶网络与信息安全事件时；
（2） 当重大改变发生或提出时；
（3） 组织内部确定有必要时，或外部组织要求时。

2.4.2.3. 网络安全风险评估应考虑但不限于如下内容：
（1） 威胁，如恶意软件、网络钓鱼攻击等；
（2） 脆弱系统的识别和保护，如 ECDIS（电子海图）、ENPs（电子航海出版物系统）等；
（3） 缓解措施，如 USB 控制等；
（4） 内部关键人员的识别，如管理员、报告可疑事件的人等；
（5） 关键联系人的硬拷贝，如 DPA（指定人员）、CSO（安全员）等；
（6） 密码的管理；
（7） 供应商/承包商的承诺。

2.4.2.4. 运维期间的网络安全风险评估应包含技术检测。

2.4.2.5. 对风险评估中发现的安全风险，应进行风险处置和再评估（残余风险评估）。

2.4.3. 安全检查

2.4.3.1. 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

2.4.3.2. 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的有效性等。

2.4.3.3. 应制定安全检查表格来实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

2.4.4. 变更管理

2.4.4.1. 变更前应明确变更需求，并制定变更方案，变更方案经审批后方可实施。

2.4.4.2. 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

2.4.4.3. 对于重大变更，应进行变更失败的风险评估，并建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

2.4.5. 事件与应急管理

2.4.5.1. 应及时向管理员和其他相关人员报告所发现的安全弱点和可疑事件。

2.4.5.2. 应制定安全事件报告和处置管理规定，明确不同安全事件的报告、处置和响应流程，包括

现场处理、事件报告和后期恢复的职责等。

2.4.5.3. 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

2.4.5.4. 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

2.4.5.5. 对重大安全事件，现场应急响应结束后，还应进行事件调查，并形成事件调查报告，必要时启动风险评估，并对存在不足的管理制度文件进行修订。

2.4.5.6. 应制定应急计划，以便指明如何及时发现并采取措施限制网络安全事件的后果，以及通过适当的响应行动确保安全和恢复受影响的系统。至少包括要寻找的症状、要立即采取的控制措施、系统恢复措施、人员沟通方式等内容。所有应急措施应易于船员理解，如需要岸上支持，则应说明如何获得外部援助。

2.4.5.7. 应定期对相关的人员进行应急计划培训，并进行应急计划的演练。

2.4.5.8. 应定期或在应急响应结束后对原有的应急计划重新评估，修订完善。

2.4.5.9. 应急计划应保存在负责人员易于获取的位置，其有效性不应因发生网络安全事件而失效，可以是独立于船舶网络的硬拷贝（纸质文本）或电子设备。

2.4.6. 备份与恢复管理

2.4.6.1. 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

2.4.6.2. 应识别需要定期备份的重要业务信息、系统数据及软件系统等，制定备份计划，备份计划应规定备份信息的备份范围、备份方式、备份频度、存储介质、保存期等。

2.4.6.3. 定期对备份数据和恢复程序进行测试，确保备份数据能够正常工作。检查和测试备份介质的有效性，确保在恢复程序规定的时间内完成备份的恢复。

2.4.7. 服务供应商管理

2.4.7.1. 应确保服务供应商的选择符合相关组织的规定，包括产品供应商、通信服务供应商和外包运维服务商等。

2.4.7.2. 应与选定的服务供应商签订相关协议，明确整个服务供应链各方应履行的网络安全相关义务。

2.4.7.3. 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

2.4.7.4. 应识别所有网络服务的安全机制、服务等级和管理要求，并包括在网络服务协议中。

2.4.7.5. 对外包运维服务商，尚应符合下述要求：

（1） 选择外包运维服务商时，应保证其在技术和管理方面均应具有按要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

（2） 应签订协议明确约定外包运维的范围、工作内容和安全要求等，例如对敏感/重要信息的访问、处理、存储的要求，对 IT/OT 设施和网络及应用系统中断服务的应急保障要求等。

2.4.8. 密码管理

2.4.8.1. 应遵循密码相关标准。

2.4.8.2. 应使用密码管理监管机构认证核准的密码技术和产品。

2.4.9. 保密管理

2.4.9.1. 应符合相关组织对国家秘密、商业秘密、隐私等保密相关要求。

2.4.9.2. 应对列入保密范围的信息、不良信息等信息发布进行管控。

2.4.9.3. 应对信息传输进行管控，以保护通过通信设施传输的所有类型信息的安全，并有相应的保密协议或不扩散协议来防止所传输的信息被泄露。

第5节 建设管理补充要求

2.5.1. 确定需求

2.5.1.1. 应以书面形式说明船舶网络安全需求、目标和船舶网络范围。

2.5.1.2. 应组织相关方和有关安全技术专家对安全需求和目标的合理性和正确性进行论证。

2.5.1.3. 所确定的安全需求和目标应经过船东同意。

2.5.2. 规划设计

2.5.2.1. 应根据安全目标进行安全整体规划和方案设计，并形成配套文件。

2.5.2.2. 应根据安全目标选择基本安全措施，并依据风险分析的结果补充和调整安全措施。

2.5.2.3. 应组织相关方和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，并经船东同意后才能正式实施。

2.5.3. 工程实施

2.5.3.1. 应指定或授权专门的部门或人员，负责工程实施过程的管理。

2.5.3.2. 应制定安全工程实施方案，控制工程实施过程，妥善保障开发环境的安全，监控外包开发活动。

2.5.3.3. 应通过第三方工程监理控制项目的实施过程。

2.5.4. 产品采购和使用

2.5.4.1. 应确保网络安全产品采购和使用符合有关规定。

2.5.4.2. 应确保密码产品与服务的采购和使用符合密码管理的要求。

2.5.4.3. 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

2.5.5. 软件开发

2.5.5.1. 应将开发环境与实际运行环境分开，测试数据和测试结果受到控制。

2.5.5.2. 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

2.5.5.3. 应制定代码编写安全规范，要求开发人员参照规范编写代码。

2.5.5.4. 应具备软件设计的相关文档和使用指南，并对文档使用进行控制。

2.5.5.5. 应保证在软件开发过程中对安全性进行测试。外包开发的，在软件交付前，对可能存在的恶意代码进行检测；自行开发的，在软件安装前，对可能存在的恶意代码进行检测。

2.5.5.6. 应对软件系统的更新和发布进行授权和批准，并对程序资源库的修改进行版本控制。

2.5.5.7. 自行开发应保证开发人员为专职人员，开发人员的开发活动受到监控。

2.5.5.8. 外包开发应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

2.5.6. 测试验收

2.5.6.1. 上船实施前，应制定测试方案，明确测试内容（至少包含密码应用安全），并依据测试方案实施测试，形成测试报告。

2.5.6.2. 上船实施后，应制定验收测试方案，明确验收测试内容，并依据验收测试方案实施验收测试，形成验收报告。

2.5.6.3. 应谨慎选择测试数据，并加以保护和控制。

2.5.7. 系统交付

2.5.7.1. 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。该清单应留存在船上。

2.5.7.2. 应对负责运行维护的技术人员进行相应的技能培训。

2.5.7.3. 应提供建设过程文档和运行维护文档。

2.5.8. 云服务商管理

2.5.8.1. 应选择安全合规的船舶网络系统的云服务供应商，其所提供的云计算平台应为其所承载的业务应用系统提供相应的安全保护能力。

2.5.8.2. 应在云服务供应商的服务协议中规定云服务的各项服务内容和具体技术指标。

2.5.8.3. 应在云服务供应商的服务协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

2.5.8.4. 应在云服务供应商的服务协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

2.5.8.5. 应与云服务供应商签署保密协议，要求其不得泄露云服务客户数据。

2.5.8.6. 应及时将供应链安全事件信息或安全威胁信息传达到云服务客户。

2.5.8.7. 应及时将供应商的重要变更传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

2.5.9. 移动互联管理

2.5.9.1. 移动应用软件采购中，应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

2.5.9.2. 移动应用软件采购中，应保证移动终端安装、运行的应用软件由指定的开发者开发。

2.5.9.3. 移动应用软件开发中，应对移动业务应用软件开发者进行资格审查。

2.5.9.4. 移动应用软件开发中，应保证开发移动业务应用软件的签名证书合法性。

2.5.10. 工控系统管理

2.5.10.1. 重要设备应经本社认可的专业机构进行安全性检测后方可采购使用。

2.5.10.2. 外包软件开发时，应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

2.5.11. 大数据管理

2.5.11.1. 宜选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应的安全保护能力。

2.5.11.2. 宜以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

2.5.11.3. 宜明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

第6节 运维管理补充要求

2.6.1. 环境管理

2.6.1.1. 应对物理访问、物品带进出等方面制定管理规定。登船访问应经批准，且有指定人员陪同，并做好登记。

2.6.1.2. 应定义安全区域，用来保护包含敏感或关键信息和信息处理设施的区域。安全区域应有适当的进入控制保护，以确保只有授权人员可以进入。

2.6.1.3. 应不在安全区域接待来访人员，不随意放置含有敏感/重要信息的纸档文件和移动介质等。

2.6.1.4. 应指定专门的人员定期对机房等处所的供配电、空调、温湿度控制、消防等设施进行维护管理。

2.6.1.5. 应妥善安置及保护设备，以减少来自环境的威胁与危害，并减少未授权访问的机会。

2.6.1.6. 应保护设备免于电力或通信中断及其它因支持设施失效导致的中断。

2.6.1.7. 应确保无人值守的设备有适当的保护，如锁屏或置于视频监控之下，以防未经授权的使用。

2.6.1.8. 应采用清除桌面纸质和可移动存储介质的策略，以及清除信息处理设施屏幕的策略（如锁屏、屏保等）。

2.6.2. 资产管理

2.6.2.1. 应编制并保存与保护对象（主机设备、网络/安全设备等）相关的资产清单，清单中列明资产使用人、维护人、所处位置、重要性、备份方式与周期（如有时）等。

2.6.2.2. 应根据资产的重要程度对资产进行标识和登记管理，选择相应的管理措施，管控其新增、变更、维护/维修、出场/回场、报废等基本情况。

2.6.2.3. 应监控、调整资产的使用，并反映将来容量的需求以确保系统性能。

2.6.3. 介质管理

2.6.3.1. 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行专人管理，并定期盘点；用于船舶系统软件更新维护的介质应专人专用。

2.6.3.2. 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，防止未经授权的访问、滥用或在运输过程中的损坏，并对介质的归档和查询等进行登记记录。

2.6.3.3. 应禁止接入私人移动介质（船员娱乐网络除外），ECDIS 等关键设备应只允许接入专用移动介质。

2.6.3.4. 介质报废时，应按照正式程序进行可靠的、安全的处置。

2.6.4. 设备管理

2.6.4.1. 应对各种设备（包括备份和冗余设备）、线路等指定人员定期进行维护管理，以确保其持续的可用性及完整性。

2.6.4.2. 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。

2.6.4.3. 信息处理设备应经过审批才能带离船舶，并记录出场和归还的时间，含有存储介质的设备带出时其中重要数据应加密或清除。设备在场外（如离船出差等）应做好安全防护，以防未经授权的使用和信息泄露（如设备被盗、丢失等），在出入境时应对相关国家/地区主管机关的网络与信息安全相关规定予以特别考虑。

2.6.4.4. 未经事先授权，不得将设备带离现场。船东应指定责任人现场有权允许拆除设备（包括设备部件）。拆除设备应限制带离现场的时间，并记录归还时间。

2.6.4.5. 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏

感/重要数据和授权软件无法被恢复重用。

2.6.4.6. 各设备的 USB 接口和网线接口等对外通信接口，应通过物理锁闭和/或技术加密等方式进行有效的访问控制管理，以防范未经授权的使用。

2.6.4.7. 便携式电脑、掌上电脑等移动设备（包括船员和第三方人员携带的外来设备），在船上的使用应进行有效控制，以防未经授权的接入和使用。除船员娱乐网络外，应禁止私人设备接入。

2.6.5. 网络和应用系统安全管理

2.6.5.1. 应建立网络和应用系统安全管理制度，对账户管理、安装升级、运维操作与日志、访问控制、恶意代码防范、配置管理等方面作出规定。

2.6.5.2. 账户管理

（1） 应划分不同的角色进行网络和应用系统的管理和使用，明确各个角色的责任和权限；

（2） 应对申请账户、建立账户、删除账户等进行控制，并定期审查账户及访问权限，只允许用户访问被明确授权使用的网络和网络服务，限制及控制特权的分配及使用。

2.6.5.3. 安装和升级

（1） 应由受过培训、具有合适权限的人员进行设备和软件的安装、配置、更新、升级、打补丁。所安装的设备和软件应经批准，操作成功后应形成相关日志。应制定安装、配置和操作手册，依据手册进行安全配置和优化配置等；

（2） 应密切关注漏洞和补丁发布，严格软件安装、升级、补丁管理，关键 OT 系统的软件升级、补丁安装前要请专业技术机构进行安全评估和测试验证；

（3） 安装、配置、更新、升级、打补丁前应制定预案，以便在必要时还原。

2.6.5.4. 运维操作与日志

（1） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

（2） 应严格控制变更性运维，经审批后才可改变连接、安装软件/组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置文件/信息库；

（3） 应严格控制运维工具的使用，特别是可以覆盖软件系统和应用权限控制的工具，经审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

（4） 应严格控制远程运维的开通，经审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。远程接入点不能为公众场合，且应在接入前、接入过程中及接入完成时相互确认。远程维护期间的所有活动都应由经过培训的内部人员进行监控；

（5） 宜对网络及应用系统的运行状态进行监测，对报警及时响应；

（6） 宜定期对日志、监测和报警数据进行分析、统计，以及时发现可疑行为。

2.6.5.5. 访问控制

（1） 应保证所有与外部的连接均得到授权和批准，定期检查违反无线上网及其他网络安全策略的行为，必要时加强网络安全意识教育培训；

（2） 在需要进行访问控制时，应通过安全的登录程序，控制对网络和应用系统的访问。

2.6.5.6. 恶意代码防范

（1） 应提高所有用户的防恶意代码意识，对外来计算机、存储设备等接入前进行恶意代码检查，对外来的文件（email 附件、网络下载文件等）在使用前（读取或执行等）进行恶意代码检查；

（2） 应实施检测、预防和恢复措施以应对恶意代码/软件，并定期验证防恶意代码攻击的技术措施

（如防病毒软件和病毒库）的有效性。

2.6.5.7. 配置管理

（1） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件/组件、软件/组件的版本和补丁信息、各个设备或软件/组件的配置参数等；

（2） 应将基本配置信息的改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

2.6.6. 云服务供应商管理

2.6.6.1. 应与云服务供应商签署保密协议，要求其不得泄露云服务客户数据。

2.6.6.2. 应及时将供应链安全事件信息或安全威胁信息传达到云服务客户。

2.6.6.3. 应及时将供应商的重要变更传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

2.6.6.4. 云计算平台的运维地点的选择和运维操作的实施应考虑监管机构和相关组织的规定。

2.6.7. 移动互联管理

2.6.7.1. 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

2.6.8. 物联网管理

2.6.8.1. 应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

2.6.8.2. 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。

2.6.8.3. 应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

2.6.9. 大数据管理

2.6.9.1. 宜建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。

2.6.9.2. 宜制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。

2.6.9.3. 宜在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。

2.6.9.4. 宜定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

第3章 技术要求

第1节 一般规定

3.1.1. 一般要求

3.1.1.1. 应从物理安全、网络架构、区域边界、计算环境、安全审计等方面采取适当的技术措施提高网络系统的威胁防御能力。

3.1.1.2. 如因条件受限，技术措施确实无法达到时，可采取适当的管理措施予以替代。

3.1.2. 物理安全

3.1.2.1. 船载计算机存放应满足船用条件及备用电源要求。

3.1.2.2. 船舶网络系统应满足物理访问控制要求。

3.1.2.3. 船舶网络系统设备应满足相关的安装及实施要求。

3.1.3. 网络架构

3.1.3.1. 对网络架构的设计应基于风险评估。

3.1.3.2. 网络设计应保证船舶在维持安全所需数据的机密性、完整性和可用性的同时，仍能继续其关键任务的操作。

3.1.3.3. 设备标准，船舶网络中涉及到设备、线缆及无线设备及相关试验都应遵守本指南第 4 章相关要求。

3.1.3.4. 网络冗余，主干网络要求进行冗余设计，包括网络通信设备和网络处理、存储设备等。

3.1.3.5. 网络隔离，应通过物理隔离或逻辑隔离（如虚拟专用网）的方式将网络进行隔离，并对每个网络区域边界进行界定。当允许在不同网络区域之间相连接时，应通过适当的边界保护设备（如代理、网关、路由器、防火墙、单向网关、保护和加密隧道等）对边界进行控制。

3.1.3.6. 网络分段，应根据系统 I、II、III 类型、资产重要性、系统功能等因素对网络进行分段。可参考 IEC 62443-2-1 相关要求进行网络分段。

3.1.3.7. 网络边界防御，应在网络边界安装适当的网络防护设备，船舶网络与外部网络边界之间应安装合适的网络安全防御装置。

3.1.3.8. 网络事件监测及报警，为确保网络的预期性能和可靠性，应部署适当的网络监测和报警系统。网络监控系统应提供足够的信息来描述网络事件，供预期用户使用。当船舶提供远程连接时，应能够识别源自船舶外部的网络事件。

3.1.3.9. 网络防护，船舶网络中应配备相应防护设备，如恶意代码防范、入侵防御等措施。

3.1.3.10. 网络集成，在船舶网络的集成过程中应考虑不同网络的集成、接口、安全措施、设备冗余及故障报警等内容。

3.1.3.11. 应急响应计划，应制定适当的网络事件响应机制，以应对检测到的网络安全事件。

3.1.3.12. 备份恢复计划，应明确船舶网络备份范围，备份方式、频度、存储介质和保存期等内容。

3.1.3.13. 基于 II 类和 III 类系统以及集成系统设计的网络应具有弹性，即由于网络设备故障或网络事故而导致的某一部分发生故障，不应影响连接到未受影响网络上的其他系统。

3.1.3.14. 应将 II 类和 III 类系统及其数据与非关键数据和进程分离，以尽量减少受攻击危害。

3.1.4. 区域边界

3.1.4.1. 应基于网络的隔离与分段，确定边界并进行控制。

3.1.4.2. 应通过一定的技术手段建立恶意代码防范机制。

3.1.4.3. 应对从外部或内部发起的网络攻击行为进行检测、防止或限制。

3.1.4.4. 应对船舶外部及内部通信进行监视和控制。

3.1.4.5. 应对船舶网络系统的远程运维进行相应的监测和限制。

3.1.4.6. 应对网络系统进行访问控制。

3.1.5. 计算环境

3.1.5.1. 应对网络系统中的用户（人员、软件、设备）及账号进行认证。

3.1.5.2. 应基于风险分析，对网络系统中数据进行安全管理。

3.1.5.3. 应建立应急响应与事故恢复机制，并保证其有效性。

3.1.5.4. 应基于风险分析，对重要业务信息、系统数据及软件系统制定备份计划，并保证其有效性。

3.1.6. 安全审计

3.1.6.1. 网络设备应满足一定的安全配置。

3.1.6.2. 应定期在网络边界、重要网络节点，对重要的用户行为和重要安全事件进行审计。

第2节 物理安全

3.2.1. 物理处所要求

3.2.1.1. 船载计算机相关设备存放应满足船用条件。

3.2.1.2. 正常失电时仍有必要使用的网络系统，应能在正常供电失电时自动转接到备用电源。该备用电源可以采用 UPS，其容量应至少能维持 30min 供电的需要。

3.2.2. 物理访问控制

3.2.2.1. 服务器型设备应该位于可正常锁闭的房间内，以防止未经授权的访问。如果有困难，设备应位于可锁闭的柜子或控制台内。

3.2.2.2. 船舶网络主干网中的网络设备（路由器、交换机、防火墙、网关、协议转换器等）应安装在被保护的设施内。

3.2.2.3. 当使用移动设备或便携式存储设备时，应特别注意下述事项，以确保设备受到保护：
（1） 除非经过特别授权，移动设备（例如笔记本电脑、平板电脑、智能手机等），包括便携式存储设备（例如 USB 驱动器、HDD、CD、DVD 等），不得被允许连接到任何设备；
（2） 当便携式存储设备用于软件维护时，应在使用前通过负责人授权；
（3） 除非连接外部设备进行维护或类似操作，到网络的连接应物理阻断；
（4） 应通过策略和物理或逻辑手段防止不适当和未经授权的便携式设备连接到 OT 系统的行为。

3.2.2.4. 应通过以下入口控制手段对安全区域进行保护，如专人值守、安装屏障或配置电子门禁系统，以允许被授权人进入：
（1） 应配备访问记录表，记录访问者进入和离开区域的日期和时间。尤其是系统集成商或供应商的服务工程师等访问者，应该通过身份证等进行认证，并且只允许授权的访问；
（2） 所有访问记录均应进行安全维护和监控。

3.2.2.5. 支持网络的物理安全设备：
（1） 物理安全设备（例如监视摄像机、入侵检测器、电子锁等），应具有强登录认证方法，如密码、智能卡、令牌等。如果采用密码，则应为非默认值，保持密码的复杂性，并定期更新；
（2） 物理安全设备应定期进行测试，确保其工作在正常作业状态；
（3） 物理安全设备的记录数据，应经授权才可进行维护和访问。

3.2.2.6. 建立系统资产（包括设备、系统、工作站、服务器、可编程逻辑控制器、网络协议转换器、网络连接等）访问控制列表（ACL），并保持最新。

3.2.2.7. 通过 USB 端口访问 OT 系统前，应对该端口传输的设备和/或数据进行检测。

3.2.3. 设备安装部署

3.2.3.1. 网络系统相关设备的安装除需满足本社《钢质海船入级规范》第 4 篇第 1 章第 2、3 节相关要求以外，还需满足本节其它要求。

3.2.3.2. 为保障船舶网络及相关系统稳定运行的冗余设备应尽量安装在两个不同位置。

3.2.3.3. 布线，线缆的要求应满足本社《钢质海船入级规范》第 4 篇第 2 章第 12 节相关要求，当船舶主干网布线采取冗余形式时，冗余线缆应尽可能远离，例如从左右两舷分开敷设。

3.2.3.4. 连接到 II 和 III 类系统的关键计算机和网络设备应安装在安全区域，以避免外来者访问。

第3节 网络架构

3.3.1. 网络冗余

3.3.1.1. 应对网络系统的业务需求进行评估，为了保证可用性，可考虑冗余组件或架构。一般应提

供通信线路、关键网络设备、关键计算机设备和安全设备的硬件冗余，以保证系统的可用性。

3.3.1.2. 冗余系统应具备故障自诊断功能，以保证系统故障时能够有效转移到备用单元。

3.3.2. 网络隔离与分段

3.3.2.1. 一般要求

（1） 网络隔离应依据设计文件和风险分析进行。隔离可以使用物理隔离和逻辑隔离（例如虚拟专用网络）来实现。每个隔离区域的边界应明确界定；

（2） 应将关键系统分成具有共同网络安全要求的区域，以便实现网络安全管理；

（3） 需要实时控制和数据传输的 OT 系统（如推进系统、货控系统），应使用独立的网络设备组网，在物理上实现与其它数据网及外部公共信息网的安全隔离。

3.3.2.2. 网络采用物理隔离，则需至少满足以下要求：

（1） 网络边界处不应安装通向其他区域的永久网关；

（2） 永久性无线接入不应连接到网络边界；

（3） 供移动设备使用的端口，应在逻辑上不可用。如果网络中包含敏感数据，则应提供物理锁定，以防止对这些端口未授权访问。

3.3.2.3. 网络采用逻辑隔离，则需至少满足以下要求：

（1） 若有合适的边界防护设备，则允许不同的网络区域之间通信；

（2） 供移动设备使用的端口，应采用与 3.3.2.2（3）条相同的措施。

3.3.2.4. 应根据系统类型（I、II、III 类）、资产重要性、系统功能等因素对网络进行分段。可参考 IEC 62443-2-1 相关要求进行网络分段。

（1） 对于包含 III 类系统的网络，应提供物理分段，并使用独立的交换机；

（2） 对于包含 II 类系统的网络，可以采用 VLAN（虚拟局域网）上的逻辑分段；

（3） 每个分段应具有自己的地址范围。

3.3.2.5. 非受控网络，如船员或乘客娱乐网络，不应连接到受控网络（禁止在非受控网络和受控网络之间进行通信），不受控制的网络被认为是不安全的。

3.3.2.6. 不同安全要求的网络相连接时，应全部满足安全要求高的网络的相关要求。

3.3.2.7. 隔离区（DMZ“非军事化区”，也称隔离区）

（1） 当船舶与外界存在数据交换或业务访问时，可设置 DMZ；

（2） 对 DMZ 的访问应被授权；

（3） DMZ 网络应独立于船舶内部网络。

3.3.3. 通信安全

3.3.3.1. 通信传输与接口的设计应考虑一个系统或设备故障扩展到另一个系统的可能性和后果，并制定适当的技术保障措施。

3.3.3.2. 应基于网络的通信需要，在网络设计及改变网络结构时进行网络通信量估算，确保网络各个部分的带宽满足业务高峰期需要。应提供满足 3.3.3.3 条要求的通信量估算书以供审查。

3.3.3.3. 在进行船舶网络系统的通信量估算时，应该考虑以下因素以确定合适的网络数据吞吐量：

（1） 特定应用的数据速度要求；

（2） 数据格式。

3.3.3.4. 不同网络之间的数据交换应采用标准接口。每个网络的设计应符合公认的标准，如 IEC 标准-IEC 61158 或 IEC 61784 等。

3.3.3.5. 数据分类、数据分级、数据格式和数据内容应符合 IEC61162 等可接受的国际标准或其他等效标准。

3.3.3.6. 关键系统应具备一定的容错能力。对于 II 和 III 类系统，各子系统及其网络之间的接口设备应具备一定的校验能力，以确保数据的正常传输。本地控制和指示器应作为容错体系结构的一部分。

3.3.3.7. 在设计文件中应说明通信路径和协议。

3.3.3.8. 若船舶网络支持远程访问，则船岸接口设备应具备终止连接并恢复到未损坏状态的能力。如果设备本身不具备这种功能，则应通过安装其他附加网络设备来满足该功能要求。

3.3.3.9. 应对为船舶提供网络服务的接口进行管理：

（1） 为每个接口建立流量策略；

（2） 确保通过每个接口传输的信息的机密性和完整性；

（3） 对通信接口进行监控，阻止与安全配置策略不一致的流量；

（4） 流量策略应记录支持的任务/业务需求和持续时间，定期删除不再支持的策略；

（5） 限制系统连接外部网络的数量；

（6） 在会话结束时或在一段不活动时间之后，终止与通信会话相关联的网络连接。

3.3.3.10. 根据需要提供安全的带外通信通道，以支持事件响应。

3.3.3.11. 未经明确许可，任何系统、模块、组件、设备或应用程序不得通过网络或带外进行通信。

3.3.3.12. IT-OT 网关或接口系统仅限于严格规范的端口、协议和服务。

3.3.3.13. IT-OT 网关或接口系统需在严格的文件传输控制和筛选下进行维护。

3.3.3.14. 可安装内容过滤模块，在消息(如电子邮件、社交信息)进入专有网络之前，为其筛选通信路径，以便检测和消除潜在的破坏文件、附件和链接。

3.3.3.15. 通信安全

（1） 通信加密，在进行外部通讯时，应进行加密；

（2） 防火墙过滤

① 通过防火墙的通讯需求应被定义，授权源（MAC 和 IP 地址）、协议和端口号应被控制并通过防火墙过滤；

② 为了确保对安全性的控制，通信在默认状态下是被阻止的；

③ 实施安全策略（规则）允许对该网络的预期运行重要的数据流量通过；

④ 应用程序防火墙应能拦截检测到的入侵和异常通信；

⑤ 下一代防火墙应包含应用防火墙和身份识别功能模块；

（3） 入侵防御系统（IPS），可使用威胁特征码、已知漏洞攻击、异常活动和流量行为分析等多种不同技术来检测网络攻击，并将检测到的可疑的数据包丢弃。

3.3.4. 无线网络

3.3.4.1. 无线设备的设计和测试应满足 IACS UR E22 的要求。

3.3.4.2. 无线网络架构

（1） 通过无线网络传输的需求应被定义和确认；

（2） 接入无线网络的系统应有相同的安全要求；

（3） OT 系统之间的无线通讯应经授权，IT、OT 系统禁止接入同一无线网络；

（4） 关键系统或控制系统不能同时接入无线和有线网络；

（5） 使用实体和加密认证来保护无线接入的机制。

3.3.4.3. 无线访问控制

（1） 应提供唯一识别和认证所有参与无线通信的用户（人、软件过程或设备）的能力；

（2） 应按工业界普遍接受的最佳实践，对与控制系统相连接的无线接入点的授权、监控和使用进行控制；

3.3.4.4. 选择无线电天线并校准传输功率电平，以降低在受控边界之外接收可用信号的可能性。

3.3.5. 资产清单

3.3.5.1. 船东/船厂应在船舶交付前向本社提供一份船舶网络系统的资产清单。该清单应至少包含以下内容：

（1） 硬件设备

① 可编程逻辑控制器（PLC）及其相关设备；

② 分布式控制系统（DCS）及其相关设备；

③ 监控和数据采集（SCADA）系统及相关设备；

④ 通信设备（如路由器、交换机等）；

⑤ 网络设备（如防火墙、网关等）；

⑥ 人机界面（HMI）；

⑦ 与 OT 系统和 IT 系统相连接的相关设备（如：计算机、服务器、存储设备、打印机等）；

⑧ 与船舶重要系统（如航行系统、推进系统、货控系统等）相连接的设备等；

以上每一设备应注明以下内容：

a）名称；

b）品牌/制造商（供应商）；

c）型号；

d）嵌入式固件版本；

e）物理特性（如适用）；

f）实际物理位置（机舱、起居处所等）；

g）连接的交换机（对于以太网交换机，应指定每个端口的 VLAN 号）；

h）功能描述；

（2） 软件清单

① 软件列表（包括系统软件和应用软件），软件列表应至少包括以下内容：

a）软件名称和发布者；

b）安装日期、版本号和功能描述；

c）维护方式（本地/远程）；

d）账户类型（通用/专用）；

e）访问控制清单；

f）IP/端口目的地址（如果未知，则应将信息标识为“丢失”）；

g）许可号；

② 网络服务列表

a) 基于 IP 的服务

- 协议名称和版本;
- 监听端口和目的；

b)基于非 IP 的服务

- 监听接口和目的；

③ 集成文档。

3.3.5.2. 在船舶整个生命期间，应对资产清单应进行跟踪，并在硬件或软件设备发生更改时，及时对清单进行更新。

3.3.6. 网络测试

3.3.6.1. 完成网络线缆和设备的安装后，应进行网络测试以验证网络的预期运行。网络系统的测试至少应包含以下内容：

（1） 构成网络系统的所有布线（线缆敷设）和网络设备；

（2） 所有的外部和内部通信；

（3） 监测和报警系统；（如适用）

（4） 备份程序的有效性；

（5） 网络事件响应机制（关键计算机系统失效后的响应和恢复能力）；

（6） 网络事件的就地控制能力；

（7） 网络负载；

（8） 网络风暴测试；

（9） 冗余测试（如适用）。

3.3.6.2. 新设备、网络系统在安装到船舶之前应进行性能测试、潜在系统影响测试以及和安全访问方法测试。

第4节 区域边界

3.4.1. 边界防护

3.4.1.1. 边界控制

（1） 根据计算机系统的分类对安全边界进行定义；

（2） 当允许不同网络区域之间可相互连接时，应该通过使用适当的边界保护设备（例如代理、网关、路由器、防火墙、单向网关、保护和加密通道）对边界进行控制。

3.4.1.2. 船舶内部网络与外部网络通信的接口需进行通信控制，并应加装边界防火墙。

3.4.1.3. 应在每个网段之间设置内部防火墙。

3.4.1.4. 若通过防火墙与影响人身安全或船舶安全的系统进行通信，则应提供两个不同的防火墙，两个防火墙都应实时运行，并设置为心跳模式。

3.4.1.5. 边界保护装置发生运行故障时，应发出安全报警。

3.4.1.6. 应在 IT 网络和 OT 网络之间安装保护装置，以便跟踪和记录所有流量，限制流量类型、流量协议和流量来源。

3.4.1.7. 任何系统、工作站或设备应默认激活任何固有的保护系统。

3.4.1.8. 服务器、系统、模块、组件、设备或应用都应启用密码访问，特殊情况需经本社同意。

3.4.1.9. 任何 OT 系统或过程控制系统不能直接连接到互联网上。

3.4.2. 恶意代码防范

3.4.2.1. 应在每台船载计算机或具有标准操作系统的任何可编程设备上安装防病毒软件。对于没有标准操作系统的 PLC 或其他设备，应根据制造商的建议采取安全措施。

3.4.2.2. 应定期执行防病毒软件程序的更新、安全审计。

3.4.2.3. 应在每台船载计算机上提供识别防病毒数据库状态的方法。

3.4.2.4. 恶意代码保护系统，应至少配置：
（1） 以定义的频率定期扫描系统；
（2） 在下载、打开或执行外部来源的文件时实时扫描；
（3） 在检测到恶意代码时，能阻止、隔离恶意代码，并发出警报。

3.4.2.5. 应关注恶意代码检测和处置期间产生的误报及其对系统可用性的潜在影响。

3.4.2.6. 启用垃圾邮件保护机制，根据策略和程序及时更新垃圾邮件保护机制。

3.4.2.7. 经授权的移动计算机系统或移动介质连接到 OT 系统之前，应扫描其是否存在恶意代码。

3.4.2.8. 定期使用检测系统对恶意代码、未经授权的软件进行扫描。

3.4.3. 入侵防范

3.4.3.1. 在关键网络节点处检测、防止或限制从外部或内部发起的网络攻击行为，检测到网络攻击行为、异常流量情况时发出警报。

3.4.3.2. 定期对网络中系统及设备的端口、服务等进行检查，停用无用的后台程序和进程，关闭不需要的系统服务、默认共享和高危端口，如端口 135、137、138、139、445 等。

3.4.3.3. 定期执行漏洞扫描和安全审计，发现可能存在的漏洞，并在经过充分测试评估后，应及时修补漏洞。

3.4.3.4. 网络系统应具备数据有效性校验功能，保证通过人机接口或通信接口输入的内容符合系统设定要求。

3.4.3.5. 应通过限制终端接入方式或网络地址范围对网络中的终端进行限制，并应能够检测到非授权无线接入设备和移动终端的接入。

3.4.3.6. 应能对针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。

3.4.3.7. 可在船舶网络中部署入侵检测系统（IDS）和入侵防护系统（IPS），应阻止异常流量，如果检测到可能影响安全性的事件，IPS 应向有人值守的站点发出警报。

3.4.3.8. 应采用建立机制防止或缩小拒绝服务攻击的影响。

3.4.3.9. 应关闭不使用的机器，以防止潜在的入侵。

3.4.3.10. 服务器、工作站、台式机、笔记本电脑或其它移动设备，应禁止未授权的软件自动运行。

3.4.4. 监测与报警

3.4.4.1. 对无线网络进行监测，防止未经授权的接入点访问网络系统或基础设施。

3.4.4.2. 对工作站、服务器和移动设备进行连续自动监测，并对监测事件进行日志记录，对异常行为进行报警。

3.4.4.3. 对 VPN 流量进行保护性审查和过滤，并监测所访问节点。

3.4.4.4. 对监测到的影响船舶安全的异常或事件，允许从网络中隔离相应设备。

3.4.4.5. Ⅱ类和Ⅲ类系统的网络设备，应能够通过执行自诊断来监测以下状态：
（1） 网络设备上的每个端口上行链路；
（2） 网络设备上的每个端口下行链路；
（3） 通电或硬件复位；
（4） 网络风暴监测；
（5） 风扇停止（仅当网络设备带有风扇和具有风扇停止监测功能时）；
（6） 温度异常（仅当网络设备具有异常温度监测功能时）。

3.4.4.6. 网络监测设备应具有监测异常状态变化的功能，并将以下异常状态通知用户：
（1） 当网络设备或网络终端断开链路或关闭电源时；
（2） 当不属于网络的网络设备或终端连接到网络时；
（3） 网络拥塞达到阈值时。

3.4.4.7. 任何异常或故障报警都应显示并保持所有功能，以保障集成网络中基本系统的正常运行。

3.4.4.8. 记录所有远程登录尝试、远程访问事件的时间、日期、持续时间和源头，同时记录远程访问失败的尝试。

3.4.4.9. 监控网络日志分析设备的攻击参数，包括但不限于：
（1） OT 系统边界上的异常通信 IP 流量；
（2） 恶意网络连接的 IP 流量；
（3） 检测到的恶意软件和攻击的网络主机的行为；
（4） 用户登录时间/地点，以检测被盗凭证或不当访问；
（5） 用户账号或者用户管理行为偏离正常行为。

3.4.4.10. 由自动安全响应协议捕获、记录、管理自动警报响应系统触发的警报，并报告给授权人员以供进一步审查。

3.4.4.11. 在检测到针对 OT 系统的入侵企图时执行以下操作：
（1） 按事件、严重性和类型记录和报告所有 OT 系统安全事件；
（2） 记录和报告事故恢复措施和事故后补救影响（如有）；

（3） 记录并检查所有访问尝试；
（4） 在可行范围内，将多个来源和传感器检测到的事件数据进行聚合和关联，以便充分描述事件；
（5） 向事件响应团队提供所有事件数据，以进行事件控制，并从中获取经验教训；
（6） 评估对安全、环境、生产、损失时间和成本（实际或预期）的影响。

3.4.5. 访问控制

3.4.5.1. 对网络系统中的用户（人员、软件、设备）及账号进行标识，制定标识管理办法，如禁止使用公共符号进行标识。

3.4.5.2. 使用筛选机制、访问控制列表、复杂密码和/或多因素认证、带外通信等措施，保护敏感资源、资产免受未经授权的访问。

3.4.5.3. 用户管理
（1） 应对登录网络系统的用户分配账户和权限；
（2） 应重命名或删除默认账户，修改默认账户的默认口令；
（3） 不发放冗余用户账户；
（4） 应定期对账户进行管理及审查，及时删除或停用、过期的账户；
（5） 对所有访问网络系统的账户进行监控，如确定账户的使用期限，则可清理不必要的用户和管理员账户。禁用已过期的、与任何业务无关的账户。对超时注销、若干次尝试登录失败的账户进行锁定；
（6） 使用唯一的用户账户使用户能够并对其行为负责；应避免共享账户的存在，只有在出于业务或运营原因需要时才允许使用共享账户，并且应该批准和记录。

3.4.5.4. 口令管理
（1） 严格口令管理，及时更改系统安装时的预设口令，杜绝弱口令、空口令；
（2） 在提供新的，替换的或临时的访问认证信息之前，应建立程序以验证用户的身份；
（3） 应以安全的方式为用户提供临时访问认证信息，避免使用外部各方或未受保护的（明文）电子邮件，临时访问认证信息对于个人应该是唯一的，不应是可猜测的；
（4） 安装系统或软件后，应更改默认的供应商访问认证信息；
（5） 应该选择合适的认证技术来证实所声称的用户身份。如果需要强身份验证，则应将密码、智能卡、令牌设备或生物识别方法等身份验证方法结合使用；
（6） 登录程序的设计应尽量减少未经授权访问的机会。因此，登录程序应最小程度地披露有关系统或应用程序的信息，以避免向未经授权的用户提供任何不必要的帮助。

3.4.5.5. 基于密码的身份验证，应满足：
（1） 通过区分大小写、字符数、大小字母混合、数字和特殊字符等手段来强制实现密码的复杂性；
（2） 创建新密码时，至少强制执行更改字符的数量；
（3） 密码的存储和传输应加密；
（4） 应定期更换密码；
（5） 禁止密码重用若干代；
（6） 允许使用临时密码进行系统登录，并立即更改永久密码。

3.4.5.6. 权限管理

（1） 对网络中已识别的人员、组织、角色和设备授予相应的权限；
（2） 针对特定的工作需求、特殊系统的特权帐户，应采取网络访问限制；
（3） 建立和实施系统用户授权管理；
（4） 应授予管理用户所需的最小权限，实现管理用户的权限分离。

3.4.5.7. 第三方访问

（1） 授权第三方（设备供应商、系统开发方、系统维护方等，下同）访问网络系统时，需进行审核。定期对第三方的访问权限进行审核，确认其在可控范围内；
（2） 第三方的访问，需使用多因素认证，或采用强密码。第三方在网络系统中的行为日志应能被记录并保存；。
（3） 第三方接入网络系统时（必要时），需授权最小的访问权限，采用授权的存储介质。如非必要时，不允许第三方进行数据的收集与存储。

3.4.5.8. 访问规则

（1） 应配置访问控制策略，访问控制策略规定用户对网络的访问规则，包括访问网络和网络服务使用的方式（例如，VPN 或无线网络的使用）等；
（2） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外，受控接口拒绝所有通信；
① 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
② 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则；。
（3） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
（4） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
（5） 应保证当虚拟机迁移时，访问控制策略随其迁移；
（6） 应允许云服务客户设置不同虚拟机之间的访问控制策略；
（7） 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证。若使用口令，则长度不小于 8 位字符；
（8） 应在 OT 系统与其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
（9） 应在 OT 系统的边界防护机制失效时，发出报警信号；
（10） 限制连续无效登录尝试次数，当超过最大不成功尝试次数时，使用自动执行以下之一：
① 锁定帐户/节点一段时间；
② 锁定帐户/节点，直到管理员释放为止；
③ 根据延迟算法延迟下一次登录提示。

3.4.5.9. 在安装到网络环境之前，删除用户端系统、设备、应用程序和资产最初配置的所有默认设置，包括：

（1） 更改供应商默认密码；
（2） 默认情况下不授予普通用户帐户管理权限；
（3） 端点只能在其功能需求范围内进行横向网络访问或对其可见性，而不能默认访问网络上的其他系统或资产；
（4） 根据需要为应用程序配置单点登录(SSO)；
（5） 制造商的远程呼叫预配置软件将在标准用户配置文件中禁用，以防止未经授权的通信。

3.4.6. 远程运维

3.4.6.1. 远程运维的许可应当是有限的。

3.4.6.2. 网络系统正常运行时应能阻止远程维护。

3.4.6.3. 远程维护时，应满足以下要求：

（1） 应对远程运维的网络连接进行控制，此类连接的远端外部访问点应得到保护，以防止未经授权的访问；

（2） 应在开始会话时进行身份验证。密码不应以未加密的形式传输。如果系统不能提供加密，则应采用加密虚拟专用网络（VPN）进行通信；

（3） 应提供在尝试访问失败的情况下激活锁定期功能；

（4） 应能随时在本地取消远程运维；

（5） 如因某种原因远程维护连接中断，则应能自动终止对系统的访问；

（6） 应执行远程运维日志。日志信息应包含开始时间、结束时间、操作人员等。

3.4.6.4. OT 系统还应具备必要的能力，以减轻远程运维的风险：

（1） 应具备终止连接，并立即恢复到未损坏状态的能力；

（2） 在异常中断时，应具有不影响系统的完整性和可用性的能力。

第5节 计算环境

3.5.1. 身份鉴别

3.5.1.1. 对网络系统中的用户（人员、软件、设备）及账号进行认证，并对网络访问实现多因素认证，对接入设备实现动态地址分配等认证方式。

3.5.1.2. 建议采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

3.5.2. 数据安全

3.5.2.1. 应对数据进行风险分析，以评估数据安全的价值及其对系统性能的潜在影响。

3.5.2.2. 数据加密

（1） 应对系统中存储、传输和处理的数据采取有效措施，保证其可用性、保密性和完整性；

（2） 禁止在非专用通道或网络区域内传输 OT 系统的命令和控制信号；

（3） 如有第三方使用数据，则需制定相应的数据使用要求和控制规则；

（4） 如使用第三方提供的服务或数据，应保证服务安全和数据安全；

（5） 采用非安全网络进行通信时，需对通信路径和关键系统或功能的数据进行加密；

（6） 对公司及人员隐私数据进行管理，遵循国家或当地的法律法规要求；

（7） 对隐私数据的访问和分发进行严格控制；

（8） 船员和船东/船舶管理公司的隐私数据与其他数据的存储应相互隔离；

（9） 验证数据合法性，保证数据质量。

3.5.2.3. 通过将关键处理和数据与非关键数据和处理分离来减少对关键处理和数据的攻击。系统还应具备解耦能力，以防止由于单个网络事件造成的连锁反应。

3.5.2.4. 数据存储

（1） 数据存储设备的电源应保持稳定；

（2） 数据存储设备应具备防电磁干扰能力；
（3） 数据存储设备应符合预期用途，并适用于 UR E10 中规定的海事环境；
（4） 应采用数据泄露防护（DLP）软件以防止重要数据的“泄漏”；
（5） 若用于 II 或 III 类系统的数据存储在硬盘驱动器上时，则应存储在多个硬盘驱动器上，以便在驱动器发生故障时保护数据，例如： RAID 存储或等效装置。 备用兼容性的驱动器应可以在船上使用。

3.5.2.5. 作为网络风险管理的一部分，船东还应提供与数据安全相关的培训，该培训面向有权与船舶网络系统进行交互的人员。

3.5.2.6. 防止通过共享系统资源的方式进行未经授权和非预期的信息传输。

3.5.2.7. 提供对敏感数据存储、资产类型或数据位置的数据访问的日志记录功能。

3.5.2.8. 为数据处理提供安全的数据销毁方法。

3.5.3. 系统安装与更新

3.5.3.1. 系统安装及变更
（1） 软件历史版本应保留，连同所有需要的信息和参数、规程、配置细节以及支持软件，以作为应急还原措施；
（2） 建立和实施软件安装的用户管理规则；
（3） 遵循最小安装的原则，仅安装需要的组件和应用程序；
（4） 更新前确定回滚策略，在出现损坏的情况下，系统应该能够简单地恢复到早期版本；
（5） 更新成功后应形成相关信息日志，日志应包括时间、版本号和操作人。

3.5.3.2. 系统更新验证
（1） 确保更新的完整性和真实性，如加密或循环冗余校验-CRC；
（2） 更新前进行恶意代码扫描；
（3） 更新后验证系统运行正常。

3.5.4. 应急响应

3.5.4.1. 一般应考虑以下过程：
（1） 检测网络事件并识别故障系统；
（2） 确定有效的应对方案并采取适当的行动；
（3） 恢复故障系统；
（4） 调查并记录网络事件；
（5） 评估应急过程的有效性并更新事件与应急管理程序和应急计划。

3.5.4.2. 应备好实施事件应急响应所必需的软/硬件工具。

3.5.5. 备份

3.5.5.1. 已备份的数据至少是单冗余的，并保持有限的访问权限。

3.5.5.2. 若备份数据存储在硬盘驱动器上，则应提供备用兼容性的驱动器（如：RAID 存储或等效），以便在驱动器发生故障时保护数据。

第6节 安全审计

3.6.1. 配置要求

3.6.1.1. 根据设备的使用选择安全配置，当网络配置变更时，应及时更新资产清单中的基本配置信息列表。

3.6.1.2. 防火墙，至少应启用以下配置：

（1） 应在每个防火墙上设置安全策略（规则），应提供设置以仅允许在交换机之间传输基本或重要数据；

（2） 防火墙规则的设计应满足所在网络的预期操作所必需的数据流量；

（3） 设置 super 密码并加密存放；

（4） 配置 consol 口密码保护；

（5） 按用户分配账号，避免账号共享；

（6） 开启流量监控日志功能；

（7） 启用路由协议认证加密功能；

（8） 制定路由策略，禁止发布或接收不安全的路由信息；

（9） 配置 ACL 过滤常见的漏洞攻击及病毒报文；

（10） 关闭 AUX 口；

（11） 攻击防范配置；

（12） 关闭不必要的网络服务；

（13） 访问规则列表初始设置为拒绝一切流量。

3.6.1.3. 路由器及协议，至少应启用以下配置：

（1） 不同网络分段之间应该安装路由器；

（2） 每个分段都应有自己的 IP 地址范围；

（3） 通过 II 类和 III 类系统的数据应加密。

3.6.1.4. 交换机，至少应启用以下配置：

（1） 如应用于网络隔离、分段作用，应采用三层交换机；

（2） 交换机应启用口令加密；

（3） 配置 console 口密码保护；

（4） 避免共享账号；

（5） 启用账户锁定策略；

（6） 屏蔽用户端口上不必要的协议；

（7） 开启已知的典型攻击防护；

（8） 开启流量控制；

（9） 关闭不必要的服务；

（10） 检查是否基本安全防护；

（11） 开启生成树协议。

3.6.2. 安全审计（日志）

3.6.2.1. 执行日志管理，根据需要分配存储空间，以保持足够的日志时间来支持抵御攻击周期，至少保留 12 个月。

3.6.2.2. 应在网络边界、重要网络节点，对用户行为和安全事件进行审计。审计记录应包括：

（1） 用户(远程访问的用户、访问互联网的用户等）；

（2） 事件的日期和时间；

（3） 事件类型（异常情况、故障）；

（4） 事件是否成功（连接(成功/失败)，身份验证(成功/失败)），包括由如下设备生成的：

① 任何无线接入点(WAP)；

② 任何无线局域网(WLAN)；

③ 任何局域网(LAN)；

④ 任何防火墙；

⑤ 任何应用程序防火墙；

⑥ 任何状态全包检查(SPI)；

⑦ 任何入侵防护系统(IPS)；

⑧ 用于识别和认证网络访问的任何设备；

⑨ 用于实施或确保网络安全的任何设备。

3.6.2.3. 应对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略，对审计记录进行存储、管理和查询等。

3.6.2.4. 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

3.6.2.5. 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行记录将来可审计。

3.6.2.6. 应对审计记录进行保护，定期备份，避免受到防止篡改和未授权的访问等。

3.6.2.7. 应对审计进程进行保护，防止未经授权的中断。

3.6.2.8. 审计完成后应删除审计人员的访问权限和其采用的技术手段，包括设备、测试工具等。

第4章 产品评估

第1节 一般规定

4.1.1. 一般要求

4.1.1.1. 中国船级社规范和/或指南提出，需要对产品进行网络安全评估时，应按本章要求执行。

4.1.1.2. 网络系统系指本指南第 1 章第 3 节所定义的条目。

4.1.1.3. 网络设备系指连接到网络中的物理实体。基本的网络设备有：计算机、服务器、集线器、交换机、网桥、路由器、网关、网络接口卡（NIC）、无线接入点（WAP）、打印机和调制解调器等。

4.1.1.4. 技术评估系指按本指南的相关要求，对船舶网络系统类产品进行网络安全评估的相关工作。

4.1.2. 评估流程

4.1.2.1. 产品评估分为图纸审查、技术评估和现场试验。

4.1.2.2. 图纸审查：根据本章 4.1.3 相关要求对 4.2.1 中要求的图纸资料进行审核。

4.1.2.3. 技术评估：根据本章 4.1.3 及附录 4 的要求开展技术评估。

4.1.2.4. 现场试验：本社根据图纸审查和技术评估的情况，并按照本章 4.2.2 提出的测试方法，对网络系统进行必要的测试。

4.1.2.5. 图纸审查、技术评估和现场测试均合格后，由本社签署船舶网络安全评估报告（产品）。

4.1.3. 基本技术要求

4.1.3.1. 船舶网络系统（产品）的技术评估，应满足表 4.1.3.1 的全部要求。

船舶网络系统（产品）技术要求　　表 4.1.3.1

类别	条目名称	备注
网络架构	网络冗余	应满足第 3 章中的相关条款。
	通信安全	应满足第 3 章中的相关条款。
	无线网络	应满足第 3 章中的相关条款。
区域边界	边界防护	应满足第 3 章中的相关条款。
	访问控制	应满足第 3 章中的相关条款。
	远程运维	应满足第 3 章中的相关条款。
计算环境	身份鉴别	应满足第 3 章中的相关条款。
	数据安全	应满足第 3 章中的相关条款。
	备份	应满足第 3 章中的相关条款。

4.1.3.2.　船舶网络系统（产品）的技术评估除满足表 4.1.3.1 的要求外，还应根据实际情况满足本指南第 3 章的其他相关要求。

第2节　图纸资料及测试项目

4.2.1.　图纸资料

4.2.1.1.　申请技术评估的网络系统，应按照《钢质海船入级规范》第 7 篇第 2 章表 2.1.6.3 的要求提供相关资料。

4.2.1.2.　除 4.2.1.1 要求的图纸资料外，还应将下列图纸资料提交本社批准：

（1）　系统说明书（产品技术条件），应明确规定产品的总体性能要求及总体设计要求，至少应包括下列内容的适用部分：

① 产品环境条件的要求应满足《钢规》中规定的工作条件（包括电磁兼容）的要求；

② 产品功能的详细描述应包括系统配备、产品的适用范围、产品可完成的控制和监测功能以及实现方法的详细说明、所实现的每一功能的安全状态的详细说明、系统在各种操作情况下的特性（包括，应急情况、故障情况）以及正常及异常状态下的操作指南；

③ 冗余设置及转换机制详细说明；

④ 故障监测和故障识别功能（自动和手动）的详细说明；

⑤ 数据的安全性、用户安全级别（功能进入限制）的详细说明；

⑥ 控制及监测项目清单：系统所有输入/输出信号列表（服务描述，仪器仪表，系统、信号的种类、量程及设定限值范围）

（2）　硬件说明书，至少应包括下列内容的适用部分：

① 硬件和外部设备技术规格明细表；

② 系统框图：描述所有系统主要部件（软硬件单元、模块）间的连接及与其他系统间的接口；

③ 产品主要硬件配置的详细说明；

④ 输入输出设备详细资料；

⑤ 供电设备详细资料；

⑥ 网络传输介质的规格及最大数据传输流量；

⑦ 网络传输介质采用的主要通信协议标准；

⑧ 接入网络设备的基本参数，如传输端口、子网掩码、网关地址、接受的通信协议等；
⑨ 存储介质规格参数

（3） 软件说明书，至少应包括下列内容的适用部分：
① 系统安装的软件列表和版本号；
② 对于每一硬件单元中安装的基本软件的描述；
③ 对于网络节点中安装的通信软件的描述；
④ 应用软件的描述：保持功能必须运行的系统模块的信息及其与其他系统依赖性的信息、保持每一功能必须运行的软件模块之间的关系、软件模块间的数据流和控制流；
⑤ 软件的配置，包括优先性方案；
⑥ 冗余系统间的切换机制

（4） 用户接口说明书，至少应包括下列内容的适用部分：
① 各工作站和操作站的功能分配及各站间控制转换的说明；
② 对于每一输入设备所指定的功能的描述；
③ 输入/输出设备的布置、尺寸规格及必要的实物图片；
④ 各用户输入界面说明、菜单说明

（5） 网络系统的拓扑结构图，至少包含网络系统的下列信息：
① 网络拓扑结构，能够清晰的显示网络传输介质与各接入系统、设备间的连接及访问关系；
② 路由器的布置，以及连接路由器的网络区域；
③ 系统防火墙的布置及接入方式，并划分其安全防护区域；
④ 船载工作站、服务器的布置及接入方式；
⑤ 接入网络的系统、设备，如通过路由器连接或直连接入网络的通信导航系统、机舱状态监控系统、显示控制单元等；
⑥ 入侵检测、入侵防御系统的布置及接入方式（适用时）；
⑦ 系统内外部及各单元的供电方式

（6） 系统配置文件，至少包含：
① 接入网络的设备、系统列表，包含版本号、安装维护日期、在网络系统中的标识名称等基本信息；
② 网络数据流量限定值；
③ 系统投入运行后，设备开放的端口；
④ 允许访问网络的用户及授予的权限；
⑤ 系统对限制访问地址的设定，如系统白名单；
⑥ 远程用户访问权限（适用时）；
⑦ 配置文件存储及备份的位置；
⑧ 为保护系统配置文件免受恶意读取或篡改所采取的必要措施

（7） 系统运行及试验程序，至少包含如下内容：
① 试验项目；
② 试验方法；
③ 结果评估衡准；
④ 参照标准。

4.2.1.3. 除 4.2.1.1 要求的图纸资料外，还应将下列图纸资料提交本社备查：

（1） 网络系统硬件安装说明，至少包含：

① 路由器、防火墙、工作站、服务器等的安装位置及安装方式；

② 为保护硬件设备免受物理损伤所采取的必要措施（适用时）；

③ 安装在特殊区域的设备对环境条件（温度、压力）的要求；

（2） 操作手册（包括故障处理说明书）

① 至少应包括系统启动、功能恢复、维护和定期试验、数据安全性及数据备份、用户权限限制、软件重装及系统恢复、故障定位和修理、系统更新、以及其他用户需注意的事项；

② 软件维护和使用说明（含软件和硬件变更管理的必要程序）；

（3） 软件验证的证据

① 根据软件编制标准，对软件模块的验证证据（软件错误的检测和修正）；

② 软件模块、子系统和系统层级的可编程设备功能的测试证据。

4.2.2. 测试手段

4.2.2.1. 网络系统的评估，一般应考虑采用如下技术手段进行：

（1） 安全漏洞扫描；

（2） 渗透测试；

（3） 压力测试；

（4） 负载测试；

（5） 网络风暴测试；

（6） 网络连接测试。

4.2.2.2. 网络系统测试应至少进行安全漏洞扫描、负载测试和网络连接测试。

4.2.2.1. 用于 II 类和 III 类系统的设备应按照 IACS UR E22 和 E10 的规定进行测试。

4.2.2.2. 相关测试项目可采用测试硬件和软件进行；也可通过核查配置文件，确认相关设备具有相应防护能力；或通过核查试验结果及报告进行。

4.2.2.3. 安全漏洞扫描

（1） 测试方通过技术手段，对网络系统产品进行全面的检测和漏洞扫描，定位漏洞分析原因，并将结果作为技术评估的结论之一；

（2） 漏洞扫描完成后，申请方应提供测试报告供本社验证。

4.2.2.4. 渗透测试

（1） 测试方通过技术手段，对网络系统产品进行全面的渗透测试，并将结果作为技术评估的结论之一；

（2） 测试通过测试方建立的渗透测试环境，对受试网络安全策略进行全面检查，对网络的脆弱性、技术缺陷进行主动分析，分析从安全攻击可能存在的位置进行；

（3） 渗透测试通过识别安全问题来帮助申请方理解当前的安全状况，并促进通过相关的操作规划来减少威胁、降低风险；

（4） 渗透测试对象为待接入船舶网络的网络系统产品，测试按如下分组进行：

① 系统及应用功能渗透；

② 数据库系统渗透；

③ 网络设备渗透。

（5） 渗透测试完成后，申请方应提供测试报告供本社验证。

4.2.2.5. 压力测试

（1） 测试方通过技术手段，对网络系统产品进行压力测试，并将结果作为技术评估的结论之一；

（2） 压力测试也称为强度测试，通过模拟实际应用的软硬件环境及用户使用过程的系统负荷，长时间或超大负荷地运行测试软件，来测试被测系统的性能、可靠性、稳定性等。压力测试需要确定一个系统的瓶颈或者不能接收的性能点，来获得系统能提供的最大的服务级别；

（3） 压力测试完成后，申请方应提供测试报告供本社验证。

4.2.2.6. 负载测试

（1） 测试方通过技术手段，对网络系统产品进行负载测试，并将结果作为技术评估的结论之一；

（2） 负载测试也会被称为“容量测试”或者“耐久性测试/持久性测试”，其目标是确定并确保系统在超出最大预期工作量的情况下仍能正常运行。负载测试通过测试系统在资源超负荷情况下的表现，以发现设计上的错误或验证系统的负载能力。在这种测试中，将使测试对象承担不同的工作量，以评测和评估测试对象在不同工作量条件下的性能行为，以及持续正常运行的能力；

（3） 负载测试完成后，申请方应提供测试报告供本社验证。

4.2.2.7. 网络风暴测试

（1） 测试方通过技术手段，对网络系统产品进行网络风暴测试，并将结果作为技术评估的结论之一；

（2） 网络风暴指由于网络拓扑的设计和连接问题，或其他原因导致广播在网段内大量复制，传播数据帧，导致网络性能下降，甚至网络瘫痪。网络风暴的产生通常由网络设备的不合理配置、网卡故障、网络环路设置错误、网络病毒、恶意攻击等原因造成；

（3） 网络风暴测试完成后，申请方应提供测试报告供本社验证。

4.2.2.8. 网络连接测试

（1） 网络连接测试的目的是验证网络设备连接的操作性和功能；

（2） 网络监控设备和监控功能应在网络系统中正常运行，具体如下：

① 显示物理架构图的功能；

② 报警功能；

③ 日志功能；

④ 流量显示；

⑤ 设置配置功能；

⑥ 故障恢复支持功能；

（3） 测试完成后，申请方应提供测试报告供本社验证。

第5章 船舶检验

第1节 一般规定

5.1.1. 一般要求

5.1.1.1. 本章适用于拟取得 Cyber Security（P， S）附加标志的船舶。

5.1.1.2. 本章规定的检验要求是对所有适用船舶检验要求的补充。其检验可与《钢质海船入级规范》第 1 篇第 5 章第 2 节规定的相同类型检验，也就是与年度、中间和特别检验同时进行，检验间隔期与之相同。

5.1.2. 图纸资料

5.1.2.1. 申请 P 级网络安全附加标志的船舶，应将下列图纸资料提交批准：

（1） 船舶网络安全规划说明书（设计送审时）；

（2） 网络安全建设管理文件（网络系统开工建设前）；

（3） 网络安全运维管理文件（船舶试航前/网络系统运行前）；

（4） 资产清单包括 3.3.5.1 所要求的内容；

（5） 网络系统架构说明书；

（6） 网络中各功能系统的设计方案；

（7） 设计阶段网络安全风险评估报告（设计送审时）；

（8） 运维阶段网络安全风险评估报告（船舶试航前/网络系统运行前）；

（9） 通信量估算书。

5.1.2.2. 申请 S 级网络安全附加标志的船舶，在申请 P 级网络安全附加标志的船舶的图纸资料的基础上，还应增加应将下列图纸资料提交批准：

（1） 网络安全技术措施详细说明书；

（2） 网络监控计划。

5.1.2.3. 网络安全规划说明书，应包含但不限于下列内容：

（1） 拟申请的附加标志;

（2） 网络安全需求、目标、范围、原则、功能描述等；

（3） 网络安全技术规划（为达到安全目标的技术设计思路和简要说明）；

（4） 网络安全管理规划（为达到安全目标而设置的管理机构、岗位及制定的管理制度简要说明）。

5.1.2.4. 网络安全管理文件，应包含不限于下列内容：

（1） 管理手册（包含安全目标、方针、范围、组织机构、管理活动运作框架、安全策略等）；

（2） 文件与记录控制；

（3） 人员管理；

（4） 风险管理（包含风险识别、风险分析、风险处置等）；

（5） 安全检查、审核与管理评审；

（6） 不符合情况的纠正与预防管理；

（7） 变更管理；

（8） 安全事件、应急、备份与恢复管理；

（9） 服务供应商管理；
（10） 密码管理；
（11） 建设管理（适用时），包括工程实施、采购、开发、测试验收、系统交付等；
（12） 运维管理（适用时），包括环境管理、资产管理、介质管理、设备维护管理、网络和系统安全管理、恶意代码防范管理、配置管理等。
（13） 风险评估报告（如有时）。

5.1.2.5. 网络系统架构说明书，应至少包含以下信息：
（1） 网络拓扑图，能够清晰的显示网络传输介质与各接入系统、设备间的连接及访问关系，包括与外部网络的连接，关键设备所在的物理处所；
（2） 传输介质型式（如双绞线、同轴电缆、光纤等）；
（3） 路由器的布置，以及连接路由器的网络区域；
（4） 交换机的布置，以及连接交换机的网络区域；
（5） 外部连接情况；
（6） 防火墙的布置及接入方式，；
（7） 船载工作站、服务器的布置及接入方式；
（8） 接入网络的系统、设备；
（9） 入侵检测、入侵防御系统的布置及接入方式（适用时）；
（10） 网络隔离（如 VLAN 划分）；
（11） IP 地址分配列表，至少包括如下信息：
① 有关的交换机清单；
② IP 范围的功能描述；
③ 与其他范围的互连;
（12） 非 IP 网络列表（如适用），包括：
① MAC 地址清单或网络上工业协议的特定地址清单;有关的交换机清单；
② 网络的功能描述；
③ 连接到其他网络（连接器）的设备；
（13） 非以太网访问点，包括：
① 访问端口列表；
② 如果有特殊协议；
③ 已连接设备的列表；
（14） 逻辑服务器和台式机列表，包括：
① IP 地址（网络，掩码，网关）；
② 操作系统版本；
③ 底层物理服务器；
④ 应用程序及其版本；
⑤ 服务和版本。

5.1.2.6. 网络安全技术措施详细说明书，包括但不限于：
（1） 区域边界（入侵防范、密码策略、监测与报警等）；
（2） 数据安全策略（数据加密、数据存储）；
（3） 日志审计策略。

5.1.2.7. 网络中各功能系统的设计方案，至少包含：系统目标，系统架构，系统组成，系统主要功

能、关键技术指标、技术参数、系统接口、备份计划等内容。

5.1.2.8. 风险分析评估报告，分为设计阶段和运维阶段。设计阶段，主要分析评估设计方案与网络安全规划（目标和需求等）和相关标准的符合性，以完善设计方案，并作为网络系统建设过程的风险控制依据。运维阶段，主要了解和分析网络系统运行中的安全风险，以完善网络系统运维的管理机制和技术措施，可参考附录 1 进行。

5.1.2.9. 网络监控计划是指为监控网络使用及设备故障、网络流量、网络异常报警等内容编制的方案。

第2节 初次检验

5.2.1. 一般要求

5.2.1.1. 初次检验中拟申请网络安全附加标志的船舶，验船师应按批准的图纸资料(含审图意见)进行检验，对船厂采取的措施进行落实确认；对船厂落实审批图纸及其审图意见的不同意见，及时向审图部门反馈。

5.2.2. 检验流程

5.2.2.1. 对船舶网络系统的主要检验过程为：

（1） 预评估：参考《附录 2 船舶网络安全预评估表》对船舶网络进行风险分析，掌握船舶网络系统的总体情况，按照《附录 3 对进行船舶网络系统（产品）/设备评定表》对需要相关系统、设备进行统计；

（2） 详细评估：根据网络系统要求，对船舶网络系统进行分类安全评估；

（3） 预评估和详细评估完成后，由本社向申请船舶授予船舶附加标志。

5.2.2.2. 预评估

（1） 预评估作为网络安全评估活动的初始工作，应由船东/船舶管理公司完成；

（2） 预评估旨在快速了解船舶网络安全状况，并为后续评估项目的制定提供依据。

（3） 预评估阶段通过如下几个方面掌握船舶网络的基本情况：

① 了解 ISPS Code 是否在船东/管理公司及船舶上有效应用；

② 掌握应用于船舶的，用以防范网络威胁的主要管理程序、技术手段；

③ 掌握易受网络攻击的关键设备、系统；

④ 掌握易受网络攻击的设备、系统的操作过程；

⑤ 掌握当网络安全事件发生时，船舶上用以应对的事件，并减轻事件所带来危害的主要措施；

⑥ 了解船舶网络系统的主要使用者，及其操作过程中可能面临的风险点；

⑦ 了解设备厂商对船舶网络及其设备的维护、升级等技术支持情况；

（4） 预评估应按照附录 2 船舶网络安全预评估表的内容开展。

5.2.2.3. 图纸审查

（1） 审核本章 5.1.2 要求相关图纸；

（2） 根据本指南第 2、3 章的相关要求进行审核。

5.2.2.4. 详细评估

（1） 详细评估通过全面分析船舶网络中的评估指标，识别船舶网络中存在的安全风险，并分析船

舶应对网络风险的能力；

（2） 本社对已完成预评估，且达到基线分值的船舶网络系统实施详细评估；

（3） 本社按照管理和技术两个方面开展评估；

（4） 详细评估的步骤如下：

① 船东/船舶管理公司提交申请；

② 本社根据网络系统在船舶的运行情况，根据附录 3 船舶网络系统/设备评定表评定纳入详细评估表的船舶系统/设备；

③ 本社根据附录 5 船舶网络安全详细评估表的要求进行核查，根据船舶状况确定是否开展船舶现场评估；

④ 如满足要求，本社为申请船舶授予附加标志。

5.2.2.5. 附加标志授予

（1） 评估完成后，由本社为船舶授予相应等级的附加标志；

5.2.3. 检验和试验项目

5.2.3.1. 网络系统开工建设/改建时，检查船舶网络安全建设管理文件，确认建设管理制度的完整性，并确认是否为最新有效文件。

5.2.3.2. 船舶网络系统建设/改建期间，检查船舶网络安全管理机构和人员资料、管理记录文件（包括报告、日志、记录表单等），确认安全管理工作符合管理制度运行和安全策略的要求。

5.2.3.3. 见证重要工程节点，如船舶网络集成测试、网络安全测试、上船安装、试航试验、验收交付等。

5.2.3.4. 船舶网络系统正式运行前，检查船舶网络安全运维管理文件，确认运维管理制度的完整性，并确认是否为最新有效文件。

5.2.3.5. 检查网络设备，诸如服务器、工作站、防火墙、电缆等的布置、安装和工艺等各方面，符合批准的图纸、图表、说明书、计算书和其他技术文件。

5.2.3.6. 核查资产清单与实船的一致性。

5.2.3.7. 根据 3.6.1 条配置要求对网络设备，如防火墙、交换机的配置进行核查。

5.2.3.8. 根据 3.3.6 条要求对网络系统进行测试。

5.2.3.9. 核查船舶网络安全管理文件，确认是否正式发布。

5.2.3.10. 如需对船舶网络系统产品进行网络安全评估，核查船舶网络系统（产品）评估情况。

5.2.3.11. 提交网络系统系泊试验大纲和航行试验大纲由现场验船师审核。

5.2.3.12. 视情况确定是否进行现场技术核查。

5.2.3.13. 根据附录 5，核查相关要求满足情况。

第3节 建造后检验

5.3.1. 年度检验

5.3.1.1. 年度检验

5.3.1.2. 船舶进行船级年度检验前，应向本社执行检验单位提交一份关于船舶网络系统的年度运行报告，报告应至少包括自上次年度检验以来的以下内容：

（1） 网络系统总体运行情况；

（2） 网络系统维护情况记录；

（3） 网络系统中接入系统/设备的故障/失效情况和原因分析；

（4） 船员的网络安全培训情况记录。

5.3.1.3. 年度检验时，本社应实船检查以下项目：

（1） 确认船舶网络安全运维管理文件在船上随时可用，并为最新有效文件；

（2） 核查《船舶网络安全评估报告（船舶）》；

（3） 检查船舶网络安全运维管理机构和人员资料、管理记录文件（包括报告、日志、记录表单等），确认安全管理工作符合管理制度的要求。

（4） 船舶网络运行日志，确认运行状况良好；

（5） 船舶网络安全的评估指标变化情况；

（6） 自上次检验以来，如已被认可的船舶网络发生拓扑结构变化，一般情况下，船东/船舶管理公司应向本社申请船舶网络安全临时检验，确认船舶网络符合本指南要求。

5.3.1.4. 如船舶网络安全的检验结果未达到本指南要求，由本社给出限期整改建议，或撤销船舶网络安全附加标志。

5.3.1.5. 如船舶超出限期仍未完成网络安全整改，由本社撤销船舶网络安全附加标志。

5.3.2. 临时检验

5.3.2.1. 当船舶网络结构或船舶网络系统发生重大变更后，一般情况下，船东/船舶管理公司应向本社申请船舶网络安全临时检验，确认船舶网络符合本指南要求。

5.3.2.2. 临时检验时，本社应检查以下项目：

（1） 检查船舶网络安全管理文件及相关资料，确认安全管理工作符合管理制度的要求；

（2） 变更涉及的网络设备，诸如服务器、工作站、防火墙、电缆等的布置、安装和工艺等各方面，符合批准的图纸、图表、说明书、计算书和其他技术文件；

（3） 资产清单变更情况；

（4） 如变更涉及网络主干网络调整，根据 3.6.1 条配置要求对网络设备，如防火墙、交换机的配置进行核查；

（5） 必要时，应根据 3.3.6 条要求对网络系统进行测试；

（6） 视情况确定是否进行现场技术核查。

5.3.2.3. 如船舶网络安全的检验结果未达到本指南要求，由本社给出限期整改建议，或撤销船舶网络安全附加标志。

5.3.2.4. 如船舶超出限期仍未完成网络安全整改，由本社撤销船舶网络安全附加标志。

附录 1 风险分析

第1节 风险分析

1.1 风险评估

依据有关网络安全技术和管理标准，船东/船舶管理公司应对网络系统及其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评估。需评估资产面临的威胁，以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对船舶造成的影响。

1.2 管理的要求

1.2.1 船东/船舶管理公司应确定用户、关键人员以及岸上和船上管理人员的角色和责任。

1.2.2 船东/船舶管理公司应确定船舶的系统、资产、数据和能力。如果这些系统、资产、数据和能力被破坏，可能对船舶的操作和安全构成风险。

1.2.3 船东/船舶管理公司应执行技术措施，以防止网络事故，并确保操作的连续性。这包括网络的配置、网络和系统的访问控制、通信和边界防御以及保护和检测软件的使用。

1.2.4 船东/船舶管理公司应执行程序性保护措施，以提供抵御网络安全事件的能力。

1.3 风险管理的流程

1.3.1 流程

1.3. 1.1 船舶系统安全风险管理过程可能循环进行风险评估或风险处置活动（图-1 风险管理流程图）。风险评估的循环方法能够使得每一次循环更加深入和具体。循环方法可以在确保高风险被准确识别和在识别控制措施上花费最小的时间和精力之间寻找平衡。

1.3. 1.2 首先确定范畴，然后进行风险评估。如果风险评估为进行有效决策的提供了充分的信息， 以确定将风险降低到可接受级别所需活动，则风险平复任务结束，开始进行风险处置。如果信息不够充分，则进行另外一个修订范畴和风险评估的循环，也可能是整个范围内的部分内容进行循环。

1.3. 1.3 有效的风险处置依赖于风险评估的结果。风险处置可能不会立即将残余风险降低到可以接受的级别，对于这种情形，可能需要变更风险范畴参数（如风险评估、风险接受或影响的准则）再次进行的风险评估循环，并可能需要进步的风险处置。

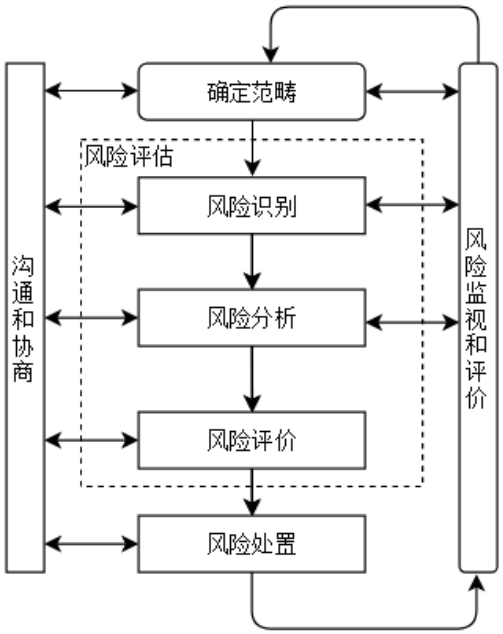

图-1 风险管理流程图

1.3.2 方法

具体船舶风险管理可参考《ISO/IEC27005：2018 信息技术-安全技术-信息安全风险管理》和《GB/T20984-2007 信息安全技术-信息安全风险评估规范》等执行。

第2节 风险评估流程

2.1 风险评估流程

风险评估流程如图 2 所示。

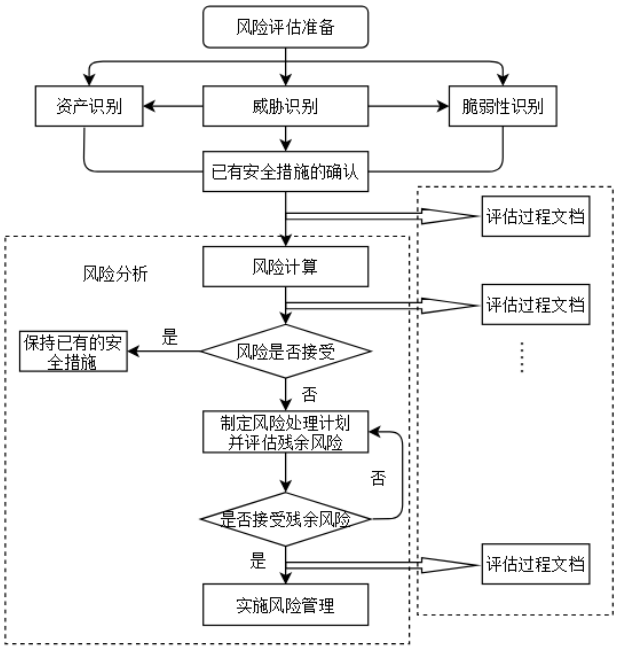

图 2 风险评估流程

2.2 风险分析

2.2.1 风险评估准备

风险评估准备是整个风险评估过程有效性的保证。船舶系统实施风险评估是一种战略性的考虑。其结果将受到船舶系统业务战略、业务流程、安全需求、系统规模和结构等方面的影响。

根据满足船舶系统业务持续发展在安全方面的需求、法律法规的规定内容，识别现有信息系统及管理上的不足，以及可能造成的风险大小。船舶系统风险评估范围应是船舶系统全部的信息及与信息处理相关的各类资产、管理机构。

2.2.1.1 资产识别

（1） 资产分类

船东/船舶管理公司提交图纸、资料、管理规程等，根据资产的表现形式，将具体的评估对象和要求进行合理分类，可将资产分为 IT 机房、网络资产、计算机、应用资产、管理资产等，详见表 1。

资产分类 **表 1**

资产分类	示例说明
IT 机房	集中存放卫通机柜、防火墙、交换机、机柜等 IT 设备设施的场所
网络资产	路由器、网关、交换机、防火墙、AC 控制器、AP 发射器、CCTV 摄像头、IP 电话机、卫通服务器等网络通信与安全设备
计算机	台式/便携工作计算机、CCTV 主机、配载仪、电子海图主机、液位遥测终端、机舱集中监控报警服务器、锅炉操控终端等船上配备的 IT 和 OT 计算机
应用资产	邮件系统、航标系统、CCTV 系统、配载系统、电子海图系统、液位遥测系统、机舱集中监控报警系统、锅炉操控系统等用于工作办公和船舶操控/监控/作业的应用系统
管理资产	各种管理文件、管理人员和使用人员

（2） 资产赋值

保密性、完整性和可用性是评价资产的三个安全属性。资产的赋值是由资产在这三个安全属性上的达成程度所决定的。船东/船舶管理公司根据确认的资产清单，根据三个安全属性进行如下的资产赋值。

a) 根据资产在保密性上的不同要求，可以将其分为不同的等级。如，1～3 个等级（分别对应：低、中、高），分别对应资产在保密性上应达到的不同程度或者保密缺失时对整个船舶系统的影响；
b) 根据资产在完整性上的不同要求，可以将其分为不同的等级。如， 1～3 个等级（分别对应：低、中、高），分别对应资产在完整性上缺失时对整个船舶系统的影响；
c) 根据资产在完整性上的不同要求，可以将其分为不同的等级。如，1～3 个等级（分别对应：低、中、高），分别对应资产在可用性上应达到的不同程度；
d) 资产重要性等级

资产价值依据资产在保密性、完整性和可用性上的赋值等级，经过评定得出。可根据船舶系统自身特点，选择资产保密性、完整性和可用性最为重要的一个属性作为资产的最终赋值，也可以根据资产保密性、完整性和可用性的不同等级及其赋值进行加权计算得到资产的最终赋值结果。最终资产赋值可以划分为不同级别。如，1～3 个等级（分别对应：低、中、高）。根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步风险评估。

2.2.1.2 威胁识别

（1） 威胁分类

造成威胁的因素可分为人为因素和环境因素。根据动机，可分为恶意和非恶意。环境因素包括自然界不可抗的因素和其他物理因素。威胁的作用形式可以是对信息系统直接或间接的攻击，在保密性、完整性和可用性等方面造成损害。也可能是偶发或蓄意的事件。对威胁的分类需充分考虑威胁的来源，并根据威胁的表现形式进行威胁分类。分类方法可参考《ISO/IEC27005：2018 信息技术-安全技术-信息安全风险管理》。

（2） 威胁赋值

判断威胁出现的频率是威胁赋值的重要内容，根据相关国家规范、近期信息安全威胁并结合行业经验以及有关统计数据进行判断并对威胁性赋值。在评估中，综合考虑以下三个方面：

a) 以往安全事件报告中出现过的威胁及其频率统计；

b) 实际环境中通过检测工具以及其各种日志发现的威胁及其频率统计；

c) 近年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警

对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率高低。等级数值越大，威胁出现的频率越高。如，1～3 个等级（分别对应：低、中、高）。

2.2.1.3 脆弱性识别

（1） 脆弱性识别的内容

船舶网络系统的脆弱性是资产本身存在的，如果没有被相应的威胁利用，单纯的脆弱性本身不会对资产造成损害，而且如果系统足够强健，严重的威胁也不会导致安全事件发生。即，威胁总是利用资产脆弱性才能造成危害。资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心，针对每一项协议保护的资产，设备可能被威胁利用的弱点，并对脆弱性的严重程度进行评估；也可以从物理、网络、系统、应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家标准，也可以是行业规范的安全要求。

a) 脆弱性识别是数据应来自于船东/船舶管理公司，以及相关业务领域和硬件方面的专业人员。脆弱性识别采取的方法主要有：问卷调查，工具检测，人工核查，文档查阅，渗透性测试等。

b) 脆弱性识别主要从技术和管理两个方面进行，技术脆弱性设计物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两个方面，前者与具体技术活动有关，后者与管理环境有关。

（2） 脆弱性赋值

可以根据脆弱性对资产的暴露程度、技术实现的难易程度等，采用等级方式对已识别的脆弱性的严重程度进行赋值。不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度一个。如 1～3 个等级（分别对应：低、中、高）。

2.2.1.4 已有安全措施确认

在识别脆弱性的同时，应对已采取安全措施的有效性进行确认。安全措施的确认将评估其有效性，即是否真正的降低了系统的脆弱性，抵御了威胁。对有效的安全措施继续保留，对确认为不适当的安全举措应核实是否取消、修正或替代。

安全措施可以分为预防性安全措施和保护性安全措施两种。

已有安全措施确认与脆弱性识别存在一定的联系。安全措施的使用将减少系统技术或管理上的脆

弱性。安全措施确认不需要和脆弱性识别过程那样具体到每个资产、组件的脆弱性，而是一类具体措施的集合，为风险处理计划的制定提供依据和参考。

2.2.1.5 风险计算

在完成资产识别、威胁识别、脆弱性识别，以及又有安全措施确认后，船东/船舶管理公司应采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对船舶信息系统的影响，即船舶网络系统安全风险。

船上网络安全风险分析可以是定性的，定量的，也可以是两者的组合：

（1） 识别资产并为资产分配价值；（2） 识别威胁，描述威胁的属性，并为威胁频率分配值；

（3） 根据特定资产识别漏洞并为漏洞严重性分配值；

（4） 根据威胁和脆弱性的严重程度计算安全事件的可能性；

（5） 根据安全事件的可能性和后果损失计算安全事件对系统的影响，即风险值。

风险计算原理范式如下：

风险值= R（A，T，V）= R（L（T，V），F（Ia，Va））（1）

其中，R 代表安全风险计算的功能；A 代表资产；T 代表威胁；V 代表漏洞；Ia 代表安全事件所起作用的资产的价值；Va 表示漏洞的严重程度；L 表示威胁利用漏洞的安全事件的可能性；F 代表安全事件的后果。风险计算可采用矩阵法和相乘法等进行计算。参考《GB/T20984-2007 信息安全技术-信息安全风险评估规范》附录 A。图 3 显示了船上网络安全风险分析计算的流程图。

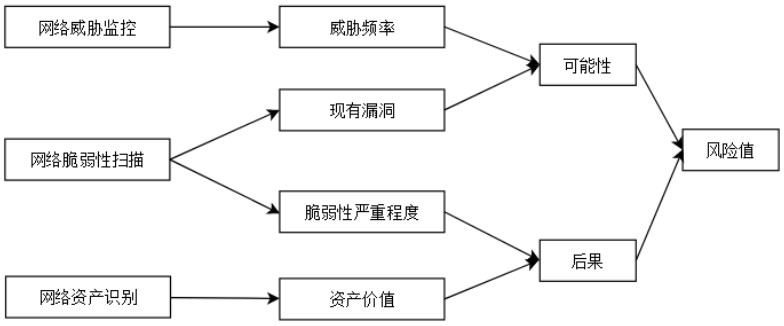

图 3 风险分析计算流程

2.2.1.6 风险结果判定

为实现对风险的控制与管理，应对风险评估的结果进行等级和处理。不同的等级分别代表资产风险严重程度的高低。等级数值越大，脆弱性严重程度一个。如，如，1～3 个等级（分别对应：低、中、高）。

应根据所采用的计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。详见表 2。

风险等级 表 2

等级	标识	描述
3	高	风险高，一旦发生将产生严重的经济或社会影响。
2	中	风险适中，一旦发生会造成一定的经济或生产经营影响，但影响面和影响程度不大，例如船舶设备不能正常工作。
1	低	风险低，一旦发生造成的影响几乎不存在，通过简单的措施就能弥补或有替代

等级	标识	描述
		措施，例如船上办公计算机不能正常工作。

2.3 风险处置措施

2.3.1.1 风险处置计划

对不可接受的风险应根据导致风险的脆弱性为船舶网络系统制定风险处置计划。风险处置计划中明确采取的弥补脆弱性的安全措施、预期效果、实施条件、季度安排、责任部门等。安全措施的选择将从管理与技术两个方面考虑。按措施的选择与事实应参照信息安全的相关标准进行。

2.3.1.2 残余风险评估

对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。对于采取了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步采取安全措施。

附录 2 船舶网络安全预评估表

Form

CYBER-P

评估申请方：　　评估系统：

评估方：　　评估日期：

分类	评估项目	说明	得分
技术措施 **（总分：100** **基线分值：60）**	是否对接入网络的主要系统实施了复杂密码（非默认、8 位以上）保护？（10 分）		
	船舶网络中，是否有支持远程维护的系统？（-）		
	网络安全拓扑结构可以覆盖所有的系统和接口吗？（10 分）	需通过网络拓扑结构文档了解。	
	是否已实施了船舶对外通信的加密？（10 分）	具备相应的加密措施，保护船岸、船船间通信的数据或报文信息。	
	当移动设备（笔记本电脑、U 盘等）接入网络时，是否具备文件传输及存储的加密措施？（5 分）		
	是否已关闭了网络中不必要的端口和服务？（5 分）		
	是否定期升级、安装补丁和修补程序？（10 分）		
	是否定期备份，并将备份文件存放在安全的地方？（10 分）	建议将备份文件存储在未连入互联网的设备中。	
	船舶网络中的系统管理员账户、用户账户是否得到了集中的存储、加密管理？（5 分）	接入网络的系统采用统一单点登录，且账户信息与系统数据的存储分离，并具备加密措施。	
	匿名账户或通用账户是否能够登录船舶网络？（10 分）		
	是否具有船舶网络的登录日志？（5 分）		
	系统配置文件是否已有效存储，并采取相应的文件保护措施？（20 分）	配置文件应对接入船舶网络的设备、系统进行记录，并记录基本的系统参数。	
	公司是否已实施 ISO 27001 信息安全的管理体系？（20 分）	船东/船舶管理公司已建立信息安全管理体系（ISMS），并通过 ISO 27001 认证。	
	公司是否参加过网络风险评估？（30 分）	已开展拓扑分析、安全隐患审计等工作，并能提供相关评估报告。	
	是否有网络安全事件处理程序？（15 分）	公司信息管理部门对网络安全事件有明确的行动规范，并具备职责清晰的程序文件。	
	是否对公司的网络安全水平定期评审？（10 分）	公司对网络安全水平定期评估，并相应的调整管理措施。	
	针对接入船舶网络中的系统，是否已由系统开发方签署保密方面的协议条款？（5 分）		
	公司是否强调了对设备密码的设置措施？（5 分）		

分类	评估项目	说明	得分
管理措施 **（总分：180** **基线分值：** **105）**	船员是否能意识到网络攻击的后果？（10 分）	通过公司的信息安全培训了解。	
	船员是否了解网络系统中用户及管理员的职责？（5 分）	同上。	
	船员是否意识到，使用未授权的移动数据存储设备存在风险？（5 分）	同上。	
	船员是否意识到，打开电子邮件附件和附件链接存在风险？（5 分）	同上。	
	公司是否为船员执行了网络安全的培训程序？（10 分）		
	通过网络收到，或邮件下载的文件是否设置了自动打开？（10 分）		
	接入船舶网络的主机已安装了入侵检测、病毒防御、流量分析软件？（15 分）		
	接入船舶网络的主机是否能够对日志和报警监控，并进行记录？（15 分）		
	网络系统已执行了渗透测试？（10 分）	通过专业的渗透测试系统实施。	
	网络系统已执行了漏洞扫描？（10 分）	通过专业的漏洞扫描系统实施。	

*上表中，基线分值代表申请CCS船舶网络安全附加标志的船舶，在预评估阶段应达到的基本分数。

附录 3 船舶网络系统（产品）/设备评定表

Form CYBER-K

评估申请方：　　评估船舶：

评估方：　　评估日期：

分类	系统/设备	是否与其他网络相连（Y/N）	是否纳入详细评估(Y/N)	备注
通信系统	卫星通信设备			
船桥系统	网络电话（VOIP）			
	无线网络（WLANs）			
	通用报警系统			
	定位系统（GPS 等）			
	电子海图系统（ECDIS）			
	动力定位（DP）系统			
	与电子导航系统和推进/操纵系统关联的系统			
	自动识别系统（AIS）			
	全球海上遇险和安全系统（GMDSS）			
	雷达设备			
	航行数据记录仪（VDR）			
	惯性导航系统（INS）			
	其他监测和数据采集系统			
推进、机械设备管理、电力控制系统	柴油机			
	锅炉控制系统			
	辅助安全系统			
	电站及电源管理系统			
	自动化监控系统			
	报警系统			
	应急系统			
	防污染系统			

分类	系统/设备	是否与其他网络相连（Y/N）	是否纳入详细评估(Y/N)	备注
	操舵控制系统			
访问控制系统	监控系统，如 CCTV 系统			
	航行值班报警系统（BNWAS）			
	船舶保安报警系统（SSAS）			
	人员登离船系统			
	公共广播和通用报警系统			
货物管理系统	货控室及系统设备			
	货物液位、压力和温度的监测和报警系统			
	液位指示系统			
	阀门遥控系统			
	气体液化系统			
	装载计算系统			
	惰性气体控制和监控系统			
	装卸货控制和监控系统			
	起重机控制和监控系统			
	货物调节，温度、通风系统			
	液化气体热氧化系统			
进水稳性	进水报警系统			
	压载水系统			
	水密门			
	水密舱口盖			
	舱底水系统			
	客船浸水探测系统			
锚	锚机控制与监控系统			
	系泊控制系统			
工程	吊装控制系统			
	钻孔控制和监控系统			
	石油和天然气监控、生产系统			

分类	系统/设备	是否与其他网络相连（Y/N）	是否纳入详细评估(Y/N)	备注
火灾及火源控制	火灾监测系统			
	探烟系统			
	防火门控制系统			
	消防泵控制和监测系统			
	灭火系统			
	危险气体探测系统			
	碳氢气体探测系统			
乘客服务管理系统	资产管理系统			
	医疗记录			
	乘客登船访问系统			
	基础设施支持系统（如域名系统、用户认证/授权系统）			
乘客网络	乘客的 Wi-Fi 或局域网登录			
	娱乐系统			
	通信系统			
核心基础设施系统	路由器			
	交换机			
	防火墙			
	虚拟专网（VPN）			
	虚拟局域网（VLAN）			
	入侵防御系统			
	安全事件日志系统			
信息管理系统	信息管理系统（备件物料管理、PMS 管理、人事管理、培训等系统）			
个人设备	船员的个人设备、局域网或 WiFi 接入互联网			
智能系统	智能航行			
	智能船体			
	智能机舱			
	智能能效管理			

分类	系统/设备	是否与 其他网络相连 (Y/N)	是否纳入详细 评估(Y/N)	备注
	智能货物管理			
	智能集成平台			
其他 系统	本表未涵盖，但接入船舶网络的其他系统			

附录 4 船舶网络系统（产品）技术评估表

Form CYBER-DD

评估申请方：　　评估系统：

评估方：　　评估日期：

类别	评估内容	详细说明	是否满足	备注
网络冗余	3.3.1.1.		□	
	3.3.1.2.		□	
通信安全	3.3.3.3.		□	
	3.3.3.7.		□	
	3.3.3.9.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
	3.3.3.15.	（1） （2） （3）	□ □ □	
无线网络	3.3.4.1.			

类别	评估内容	详细说明	是否满足	备注
	3.3.4.2.	（1） （2） （3） （4） （5）	□ □ □ □ □	
	3.3.4.3.	（1） （2） （3） （4）	□ □ □ □	
边界防护	3.4.1.5.		□	
	3.4.1.8.		□	
	3.4.1.9.		□	
访问控制	3.4.5.1.		□	
	3.4.5.2		□	
	3.4.5.3.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
	3.4.5.4.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	

类别	评估内容	详细说明	是否满足	备注
	3.4.5.5.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
	3.4.5.6.	（1） （2） （3） （4）	□ □ □ □	
	3.4.5.9.	（1） （2） （3） （4） （5） （6） （7） （8） （9） (10)	□ □ □ □ □ □ □ □ □ □	
远程运维	3.4.6.3.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	

类别	评估内容	详细说明	是否满足	备注
	3.4.6.4	（1） （2）	□ □	
身份鉴别	3.5.1.1.		□	
数据安全	3.5.2.2.	（1）	□	
	3.5.2.4.	（1） （2） （3） （4） （5）	□ □ □ □ □	
备份	3.5.5.1.		□	
	3.5.5.2.		□	

注：☒为“已满足”，—为“不适用”

附录 5 船舶网络安全技术评估表

Form CYBER-DS

评估申请方：　　评估系统：

评估方：　　评估日期：

*注：1.“适应级别”栏中“**P/S**”表示申请P级、S级附加标志的船舶均需满足。*

2.每项要求经评估后如满足则在“是否满足”栏“□”中打上“✓”。

类别	子类别	适应级别	评估条款	详细	是否满足	备注
物理安全	处所要求	P/S	3.2.1.1.		□	
		P/S	3.2.1.2.		□	
	访问控制	P/S	3.2.2.1.		□	
		P/S	3.2.2.2.		□	
		P/S	3.2.2.3.	（1） （2） （3） （4）	□ □ □ □	
		P/S	3.2.2.4.	（1） （2）	□ □	
		P/S	3.2.2.5.	（1） （2） （3）	□ □ □	
		P/S	3.2.2.6.		□	
		P/S	3.2.2.7.		□	
	安装	P/S	3.2.3.1.		□	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
	要求	P/S	3.2.3.3.		☐	
		P/S	3.2.3.4.		☐	
		P/S	3.2.3.4.		☐	
网络架构	网络冗余	S	3.3.1.1.		☐	
		S	3.3.1.2.		☐	
	网络隔离与分段	P/S	3.3.2.1.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.2.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.3.	（1） （2）	☐ ☐	
		P/S	3.3.2.4.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.3.2.5.		☐	
		P/S	3.3.2.6.		☐	
		P/S	3.3.2.7.	（1） （2） （3）	☐ ☐ ☐	
	通信安全	P/S	3.3.3.1.		☐	
		P/S	3.3.3.2.		☐	
		P/S	3.3.3.3.		☐	
		P/S	3.3.3.4.		☐	
		P/S	3.3.3.5.		☐	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
		P/S	3.3.3.6.		□	
		P/S	3.3.3.7.		□	
		P/S	3.3.3.8.		□	
		P/S	3.3.3.9.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
		P/S	3.3.3.10.		□	
		P/S	3.3.3.11.		□	
		P/S	3.3.3.12.		□	
		P/S	3.3.3.13.		□	
		P/S	3.3.3.14.		□	
		P/S	3.3.3.15.	（1） （2） （3）	□ □ □	
	无线网络	P/S	3.3.4.1.			
		P/S	3.3.4.2.	（1） （2） （3） （4） （5）	□ □ □ □ □	
		P/S	3.3.4.3.	（1） （2）	□ □	
		P/S	3.3.4.4.		□	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
	资产清单	P/S	3.3.5.1	（1）硬件设备 （2）软件清单	☐ ☐	
		P/S	3.3.5.2.		☐	
	网络测试	P/S	3.3.6.1.	（1） （2） （3） （4） （5） （6） （7） （8） （9）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
		P/S	3.3.6.2.		☐	
		P/S	3.3.6.3.		☐	
区域边界	边界防护	P/S	3.4.1.1.	（1） （2）	☐ ☐	
		P/S	3.4.1.2.		☐	
		P/S	3.4.1.3.		☐	
		P/S	3.4.1.4.		☐	
		P/S	3.4.1.5.		☐	
		P/S	3.4.1.6.		☐	
		P/S	3.4.1.7.		☐	
		P/S	3.4.1.8.		☐	
		P/S	3.4.1.9.		☐	
	恶意代码防范	P/S	3.4.2.1.		☐	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
		P/S	3.4.2.2.		☐	
		P/S	3.4.2.3.		☐	
		P/S	3.4.2.4.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.4.2.5.		☐	
		P/S	3.4.2.6.		☐	
		P/S	3.4.2.7.		☐	
		P/S	3.4.2.8.		☐	
	入侵防范	P/S	3.4.3.1.		☐	
		P/S	3.4.3.2.		☐	
		P/S	3.4.3.3.		☐	
		P/S	3.4.3.4.		☐	
		P/S	3.4.3.5.		☐	
		P/S	3.4.3.6.		☐	
		P/S	3.4.3.7.		☐	
		P/S	3.4.3.8.		☐	
		P/S	3.4.3.9.		☐	
		P/S	3.4.3.10.		☐	
	监测与报警	S	3.4.4.1.		☐	
		S	3.4.4.2.		☐	
		S	3.4.4.3.		☐	
		S	3.4.4.4.		☐	
		S	3.4.4.5.	（1） （2）	☐ ☐	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
				（3） （4） （5） （6）	□ □ □ □	
		S	3.4.4.6.	（1） （2） （3）	□ □ □	
		S	3.4.4.7.		□	
		S	3.4.4.8.		□	
		S	3.4.4.9.	（1） （2） （3） （4） （5）	□ □ □ □ □	
		S	3.4.4.10.		□	
		S	3.4.4.11.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
	访问控制	P/S	3.4.5.1.		□	
		P/S	3.4.5.2		□	
		P/S	3.4.5.3.	（1） （2） （3）	□ □ □	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
				（4） （5） （6）	□ □ □	
		P/S	3.4.5.4.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
		P/S	3.4.5.5.	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
		P/S	3.4.5.6.	（1） （2） （3） （4）	□ □ □ □	
		P/S	3.4.5.7.	（1） （2） （3）	□ □ □	
		P/S	3.4.5.8.	（1） （2） （3） （4）	□ □ □ □	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
				（5） （6） （7） （8） （9） （10）	□ □ □ □ □ □	
		P/S	3.4.5.9.	（1） （2） （3） （4） （5）	□ □ □ □ □	
区域边界	远程运维	P/S	3.4.6.1		□	
		P/S	3.4.6.2		□	
		P/S	3.4.6.3	（1） （2） （3） （4） （5） （6）	□ □ □ □ □ □	
		P/S	3.4.6.4	（1） （2）	□ □	
计算环境	身份鉴别	P/S	3.5.1.1.		□	
		P/S	3.5.1.2.			
	数据安全	P/S	3.5.2.1.		□	
		P/S	3.5.2.2.	（1） （2）	□ □	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
				（3） （4） （5） （6） （7） （8） （9）	□ □ □ □ □ □ □	
		P/S	3.5.2.3.		□	
		P/S	3.5.2.4.	（1） （2） （3） （4） （5）	□ □ □ □ □	
		P/S	3.5.2.5.		□	
		P/S	3.5.2.6.		□	
		P/S	3.5.2.7.		□	
		P/S	3.5.2.8.		□	
	系统安装与更新	P/S	3.5.3.1	（1） （2） （3） （4） （5）	□ □ □ □ □	
		P/S	3.5.3.2	（1） （2） （3）	□ □ □	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
	应急响应	P/S	3.5.4.1.	（1） （2） （3） （4） （5）	☐ ☐ ☐ ☐ ☐	
		P/S	3.5.4.2		☐	
		P/S	3.5.4.2.		☐	
		P/S	3.5.3.3.		☐	
	备份	P/S	3.5.5.1.		☐	
		P/S	3.5.5.2.		☐	
安全审计	配置要求	P/S	3.6.1.1.		☐	
		P/S	3.6.1.2.	（1） （2） （3） （4） （5） （6） （7） （8） （9） （10） （11） （12） （13） （14） （15）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	

类别	子类别	适应级别	评估条款	详细	是否满足	备注
		P/S	3.6.1.3.	（1） （2） （3）	☐ ☐ ☐	
		P/S	3.6.1.4.	（1） （2） （3） （4） （5） （6） （7） （8） （9） （10） （11）	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	
	安全审计（日志）	S	3.6.2.1.		☐	
		S	3.6.2.2.	（1） （2） （3） （4）	☐ ☐ ☐ ☐	
		S	3.6.2.3.		☐	
		S	3.6.2.4.		☐	
		S	3.6.2.5.		☐	
		S	3.6.2.6.		☐	
		S	3.6.2.7.		☐	
		S	3.6.2.8		☐	

附录 6 船舶工控系统防火墙设置附加建议

在公共服务器配置一台两个端口的防火墙而不设置隔离区，规则的制定则显得尤其重要。至少所有规则中都应包含 IP 地址和端口号。地址部分的规则应当阻止来自办公网地址的主机与控制网络中的一部分公共服务器(比如海量数据记录系统)的通信，任何企图进入控制网络的属于办公网的 IP 地址都是不允许的。此外，端口部分的规则要关注协议的安全性。由于潜在的网路侦听和修改，允许 HTTP、FTP 或者其他不安全的协议穿越防火墙是一种安全风险。制定规则时，控制网路外的主机对网内的主动连接应当被拒绝，只允许网内主机主动发起的连接。

如果使用了带隔离区的架构，办公网络与控制网络中可以配置为不存在直接的连接。除了一些特殊情况，任何一方的终点都将是隔离区中的服务器。控制网络与办公网络通信中，可以使用“组合”协议。即当一种协议用于控制网与隔离区的通信时，它最好就别再应用于办公网络与隔离区的通信。

下面是通用规则：

- 对内规则是被禁止的，接入控制系统中设备的操作必须经过隔离区。
- 对外规则必须被限制，只用于必要的通信。
- 从控制网络到办公网的连接必须通过服务和端口严格控制源和目的。

除去这些规则外，防火墙还应当配置外出过滤规则，以阻止伪造的 IP 数据包从控制网络或者隔离区出逃。由防火墙的各个接口地址对比外出数据包的源 IP 地址实现这一功能，以防止控制网络被通信欺骗(比如伪造 IP)。

下面是防火墙规则制定中要特别注意的：

- 基础的规则是拒绝一切。
- 控制网络环境和办公网间端口通信及服务批准时，应该具体问题具体分析。对于每次数据的出入，都必须有商业理由，并且有记录在案的风险分析和责任人。
- 如果状态合适，所有允许规则应该包含 IP 地址和 TCP/UDP 指定端口。
- 所有规则都应该限制通信使用制定 IP 地址或地址段。
- 禁止所有控制网络和办公网的直连，所有通信的终点都是隔离区。
- 当一种协议用于控制网与隔离区的通信时，它就不再应用于办公网络与隔离区的通信。
- 从控制网络到办公网的连接必须通过服务和端口严格控制源和目的。
- 控制网络和隔离区的外出包，必须具备控制网络或隔离区制定正确的 IP 地址。

所有防火墙管理的通信都应当包含一个独立、安全管理的网络或者多因素认证的加密网络。此外对于特定管理情况，通过 IP 地址也可以对通信做出限制。