指导性文件
GUIDANCE NOTES
GD014-2024

中　国　船　级　社

船舶网络安全指南

2024

2024 年 7 月 15 日生效

北京

目　　录

第1章　通则

第1节　一般规定

1.1.1 适用范围

1.1.1.1 本指南适用需要满足及自愿申请中国船级社（China Classification Society, CCS）船舶网络安全附加标志及网络安全评估的船舶（含海上设施）和船载计算机系统（Computer Based System, CBS）。

1.1.1.2 本指南给出了船舶和船载计算机系统的网络安全要求。

1.1.1.3 本指南要求适用的船载计算机系统，系指利用数据对船舶及设备的物理过程进行监测或控制，如受到网络事件影响，可能会对人员安全、船舶安全和/或海事环境造成危害的船载操控系统（Operation Technology System, OT 系统），包括但不限于：

（1） 推进系统；
（2） 操舵系统；
（3） 锚泊和系泊系统；
（4） 发电和配电系统；
（5） 火灾探测和灭火系统；
（6） 舱底水和压载水系统，装载计算机系统；
（7） 水密完整性和进水探测系统；
（8） 照明（如应急照明，低位照明，航行灯等）；
（9） 任何提供安全功能的 CBS，其中断或功能受损可能对船舶操作构成风险（如应急切断系统、货物安全系统、压力容器安全系统、气体探测系统等）；
（10） 法规要求的航行系统；
（11） CCS 规范和法规要求的内部和外部通信系统。

1.1.1.4 与 1.1.1.3 提及的系统采用网际互连协议（Internet Protocol, IP）连接的系统，其接口在本指南要求适用范围内，如：

（1） 乘客或访客服务和管理系统；
（2） 面向乘客的网络；
（3） 办公管理网络；
（4） 船员娱乐系统；
（5） 任何永久或暂时连接到 OT 系统的其他系统（如维护期间）。

1.1.1.5 法规或 CCS 要求的航行系统和无线电通信系统可采用 IEC 61162-460 或其它同等标准作为本指南第 2 章第 3 节 SL0 级要求的替代，安装部署到船舶时，应满足本指南第 4 章第 3 节 SL0 级相关的要求。

1.1.1.6 不在 1.1.1.3-1.1.1.6 范围内的计算机系统可参考本指南要求。

1.1.1.7 本指南所述船舶网络包含指南适用系统以及支撑其稳定、安全、可靠运行的网络设施，包括计算、安全、存储、通信及网络等设备。

1.1.2 船舶及船载计算机系统网络安全最低要求

1.1.2.1 2024 年 7 月 1 日及以后签订建造合同的以下船舶至少需要满足本指南的第 4 章第 3 节 SL0 级对应的相关要求：

（1） 国际航行客船（包括高速客船）；

（2） 500 总吨及以上的国际航行货船；

（3） 500 总吨及以上的国际航行的高速船；

（4） 500 总吨及以上的海上移动式钻井平台；

（5） 其他自航海上移动平台（例如海上风机作业平台、起重平台、钻井支持平台、居住平台等）。

1.1.2.2 除 1.1.2.1 规定的船舶外，国内航行的船舶和国际航行的其它船舶可以参考执行，自愿申请满足本指南的相关要求，如：

（1） 军船和运兵船；

（2） 小于 500 总吨的货船；

（3） 非机动船；

（4） 制造简陋的木船；

（5） 客运游艇（乘客不超过 12 人）；

（6） 非营业性游艇；

（7） 渔船；

（8） 特定海上设施（如浮式生产储油卸油装置、浮式储油船等）等。

1.1.2.3 在 1.1.2.1 规定的船舶包含 1.1.1.3 提及的系统和 1.1.1.4 提及的接口时，至少需要满足本指南的第 2 章第 3 节 SL0 级对应的相关要求或同等要求。

1.1.3 船载计算机系统网络安全要求适用性判定

1.1.3.1 判定船舶网络中 CBS 是否满足本指南相关要求，可按图 1.1.3.3 中流程进行。

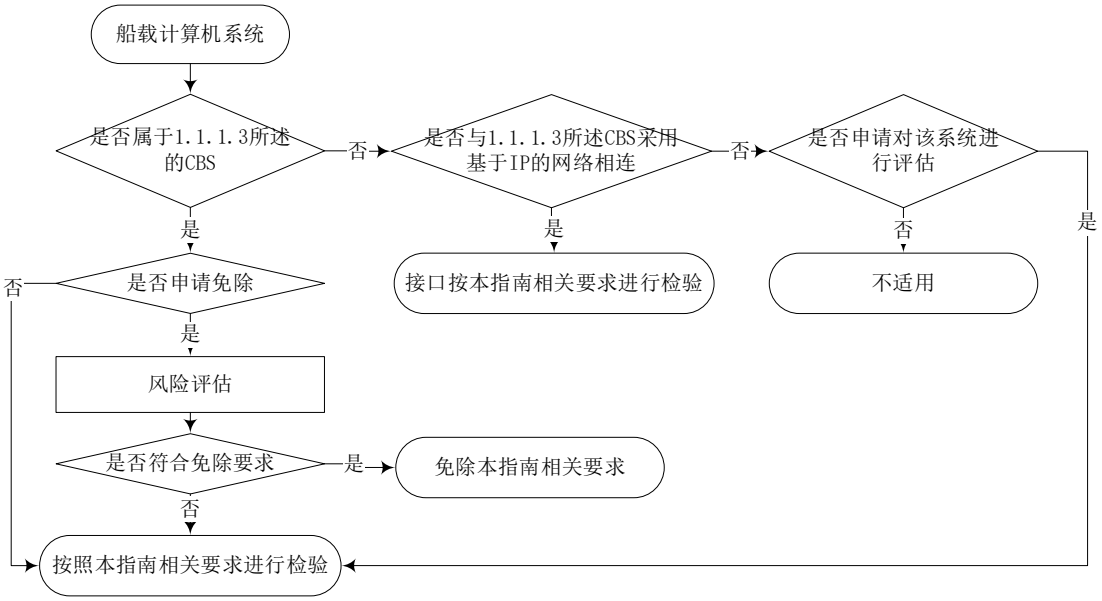


图 1.1.3.1 CBS 安全检验/评估判定流程

第2节 术语及规范引用

1.2.1 术语及定义

1.2.1.1 访问控制（**Access Control**）：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。

1.2.1.2 攻击面（**Attack Surface**）：未经授权的用户可以访问系统并提取数据的所有可能点的集合。攻击面包括两类：数字和物理。数字攻击面包括连接到组成网络的所有硬件和软件。这些包括应用程序、代码、端口、服务器和网站。物理攻击面包括攻击者可以物理访问的所有终端设备，如台式机、硬盘设备、笔记本电脑、移动电话、可移动设备和随意丢弃的硬件。

1.2.1.3 鉴别（**Authentication**）：对实体特征的正确性提供保证。

1.2.1.4 补偿措施（**Compensating Countermeasure**）：替代或补充内在安全功能以满足一个或多个安全需求的对策。

1.2.1.5 计算机系统（**Computer Based System, CBS**）：一种可编程的电子设备，或一组可互操作的可编程电子设备，为达到一个或多个特定目的而组织起来，如信息的收集、处理、维护、使用、共享、传播或处置。船载 CBS 包括 IT 和 OT 系统。CBS 可以是通过网络连接的子系统的组合。船载 CBS 可以直接或通过公共通信方式（如互联网）与岸上的 CBS、其他船舶的 CBS 和/或其他设施连接。

1.2.1.6 网络（**Network**）：两台或多台计算机之间的一种连接，以通过约定的通信协议进行数据通信。

1.2.1.7 网络安全（**Cyber Security**）：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。

1.2.1.8 网络攻击（**Cyber Attacks**）：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形式的攻击性操作。

1.2.1.9 网络事件（**Cyber Incident**）：任何针对或影响一个或多个船载 CBS 的有意或无意的攻击行为所导致的事件，该攻击行为对船载系统、网络和计算机或它们处理、存储或传输的信息造成实际的或潜在的不利后果，这可能需要采取相应措施来减轻后果。网络事件包括未经授权访问、滥用、修改、销毁或不当披露在船载 CBS 中生成、存档或使用的信息，或在连接该系统的网络中传输的信息。网络事件不包括系统故障。

1.2.1.10 网络韧性（**Cyber Resilience**）：减少发生网络事件并减轻其影响的能力，这些网络事件是由船舶安全操作的操控系统（OT）的中断或损坏引起的，这类中断或损坏可能导致危及人身、船舶安全和/或对环境构成威胁。

1.2.1.11 纵深防御（**Defense in Depth**）：集成人员、技术和操作能力的信息安全策略，在组织的多个层次和任务中建立可变防护。

1.2.1.12 隔离区（**Demilitarized Zone, DMZ**）：含有并将组织的对外服务提供给外部网络的物理或逻辑子网。它的目的是加强内部网络对外部信息交换的安全策略，并在保护

内部网络免受外部攻击的同时，为外部、不受信任的源提供对可发布信息的受限访问。

1.2.1.13 拒绝服务攻击（**Denial of Service, DoS**）：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。

1.2.1.14 重要系统（**Essential System**）：为船舶的推进、操纵和安全提供必要的服务的计算机系统。重要服务包括“主重要服务”及“次重要服务”；主重要服务是指那些需要持续运行以保持推进和转向的服务；次重要服务是指那些不一定需要持续运行以维持推进和转向，但对维持船舶安全是必要的服务。

1.2.1.15 防火墙（**Firewall**）：一种逻辑或物理屏障，用于监控通过预定义规则输入和输出的网络流量。

1.2.1.16 固件（**Firmware**）： 嵌入电子设备中的软件，为工程产品和系统提供控制、监控和数据操作。这些通常是自带的，用户无法操作。

1.2.1.17 加固（**Hardening**）：系指通过减少攻击面来降低系统脆弱性的行为。

1.2.1.18 信息技术（**Information Technology, IT**）：不同于操控技术（OT），侧重于将数据作为信息使用的设备、软件和相关网络。

1.2.1.19 信息系统（**Information Technology System，IT 系统**）：主要指使用计算机技术，微电子技术，电气手段，管理船舶营运过程的数据及流程的系统。

1.2.1.20 集成系统（**Integrated System**）：为达到一个或多个特定目的而组织的由许多相互作用的子系统和/或设备组成的系统。

1.2.1.21 入侵检测系统（**Intrusion Detection System, IDS**）：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。

1.2.1.22 入侵防御系统（**Intrusion Prevention System，IPS**）：用以识别和阻止恶意流量或违规操作的设备或软件。

1.2.1.23 逻辑网段（**Logical Network Segment**）：与“网段”相同，两个或多个逻辑网段共享相同的物理组件[1]。

1.2.1.24 网段（**Network Segment**）：本指南中，网段是指 OSI 二层以太网段(广播域)[2]。

1.2.1.25 网络交换机（**Network Switch/ Switch**）： 通过使用分组交换来接收、处理数据并将数据转发到目的地，从而将计算机网络上的设备连接在一起的设备。

1.2.1.26 恶意软件（**Malware**）：泛指能传染计算机系统并影响其性能的软件。

1.2.1.27 网络传输介质（**Network Transmission Media**）：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 逻辑网络驻留在相同的物理网络上，但在数据链路或网络层（OSI Layer 2 和 3）进行分段和管理。
2 注（TCP/IP）：网络地址规划由其 IP 地址和网络掩码作为前缀。网络段之间的通信只能通过在网络层(OSI layer 3)使用路由服务来实现。

1.2.1.28 攻击性网络行为（**Offensive Cyber Manoeuvre**）：导致 OT 或 IT 系统被拒绝、降级、中断、破坏或操纵的行为。

1.2.1.29 操控系统（**Operation Technology System**）：用于提供控制、报警、监视、安全或内部通信功能的计算机系统。

1.2.1.30 操控技术（**Operational Technology, OT**）：用于监测和控制船载系统的设备、传感器、软件和相关网络。操控系统可以被认为是专注于使用数据来控制或监测物理过程。

1.2.1.31 补丁（**Patch**）： 旨在更新已安装软件或支持数据的软件，以解决安全漏洞和其他错误或改进操作系统或应用程序。

1.2.1.32 物理网段（**Physical Network Segment**）：同“网段”。物理组件不能与其他网段共享 [3]。

1.2.1.33 协议（**Protocol**）：网络中计算机用来通信的一组通用规则和信号。协议可以实现数据通信、网络管理和安全。船载网络通常基于 TCP/IP 栈或各种现场总线实现通信。

1.2.1.34 恢复（**Recovery**）：制定并实施适当的活动，以维持韧性计划，并恢复因网络安全事件而受损的任何能力或服务。恢复功能支持用户及时恢复正常操作，以减少网络安全事件的影响。

1.2.1.35 风险评估（**Risk Assessment**）：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。

1.2.1.36 风险管理（**Risk Management**）：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。

1.2.1.37 安全区域（**Security Zone**）：在本指南的适用范围内需要相同访问控制策略 CBS 的集合。每个安全区域由一个或一组接口组成，在这些接口上应用访问控制策略。

1.2.1.38 船东/公司（**Shipowner/Company**）：船舶所有者或者其他组织或个人，如管理者、代理或承租人，向船舶所有人承担船舶经营责任，并在承担责任后同意承担其相应的义务和责任。在初始建造期间，船东可以是船厂或系统集成商（建造商或船厂）。交船后，船东可以将部分责任委托给船舶经营公司。

1.2.1.39 供应商（**Supplier**）：硬件和/或软件产品、系统组件或设备（硬件或软件）的制造厂或提供者，包括作为系统或子系统一起运行的应用程序、嵌入式设备、网络设备、主机设备等。供应商负责向系统集成商提供可编程设备、子系统或系统。

1.2.1.40 系统（**System**）：为实现一个或多个特定目的而组织的交互可编程设备和/或子系统的组合。

1.2.1.41 系统类别（**System Category**）：基于计算机系统功能对船舶和人员的安全以及对环境的危害划分系统类别，主要分为 I 类、II 类、III 类系统，详细定义见 CCS《钢质

3 分段将网络划分为多个物理段或子网，对进出的数据包进行控制。网络层（OSI layer 3）和应用层（OSI Layer 7）都能允许或阻止连接和数据交换。流量管理和包过滤都可以由单个软件或硬件设备来管理。

海船入级规范》第 7 篇第 2 章第 6 节 2.6.3 条。

1.2.1.42 系统集成商（**Systems Integrator**）：负责将供应商提供的系统和产品集成到船舶设计要求规定的系统中，并提供集成系统的特定人员或组织。系统集成商还可能负责船上系统的集成。除非与其他组织签订合同/指定职责，否则该角色应由船厂承担。

1.2.1.43 可信平台模块（**Trusted Platform Module, TPM**）：一种植于计算机内部为计算机提供可信根的芯片。

1.2.1.44 不可信网络（**Untrusted Network**）：在此指南的适用性范围之外的任何网络。

1.2.1.45 虚拟局域网（**Virtual Local Area Network , VLAN**）：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。

1.2.1.46 虚拟专用网（**Virtual Private Network, VPN**）：建立在现有物理网络之上的虚拟网络，为网络或设备之间的数据传输提供安全的通信隧道，利用隧道、安全控制和端点地址转换，提供专用线的使用感受。

1.2.2 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。

1.2.2.1 CCS《钢质海船入级规范》及其修改通报。

1.2.2.2 IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels。

第3节 船舶网络安全分级及附加标志

1.3.1 船舶网络安全分级

1.3.1.1 船舶网络安全分为 5 个级别：

船舶网络安全分级表 表 1.3.1.1

序号	级别	防御能力
1	SL0	满足最低安全要求（UR E26）的防御能力
2	SL1	抵御偶发的网络事件的防御能力
3	SL2	抵御利用少量资源发起的网络事件的防御能力
4	SL3	抵御利用丰富资源发起的网络事件的防御能力
5	SL4	抵御有组织有目的的网络事件的防御能力

1.3.2 船舶网络安全附加标志

1.3.2.1 对于船舶，经申请，并经 CCS 审图和评估/检验合格，可授予船舶网络安全附加标志：

Cyber Security (M, P[SL0]/S[SLx])

其中，M表示满足船舶网络风险管理要求，P表示满足船舶网络安全最低技术要求，S表示满足船舶较高的网络安全技术要求。

（1） M 船舶应满足本指南第 4 章第 2 节要求；

（2） P 船舶应满足本指南第 4 章第 3 节中 SL0 对应的要求，与 IACS UR E26 Rev1 对应，CBS 应不低于第 2 章第 3 节 SL0 对应的要求，与 IACS UR E27 Rev1 对应；

（3） S 分为 4 个等级（SL1~SL4），其中 SL4 为最高等级，船舶应分别满足本指南第 4 章第 3 节中 SL1~SL4 对应的要求，CBS 应不低于第 2 章第 3 节 SL1~SL4 对应的要求；

（4） 船舶网络安全附加标志与船舶、产品网络安全等级的对应关系见表 1.3.2.1

船舶网络安全附加标志与船舶、产品网络安全等级对应关系 表 1.3.2.1

	范围	要求	
		船舶级	产品级*
M	本指南适用系统	满足网络风险管理	-
P		SL0（E26）	SL0（E27）
S		SL1	SL1
		SL2	SL2
		SL3	SL3
		SL4	SL4

注*：其中 CBS 的安全等级原则上应不低于船舶的安全等级。

1.3.2.2 船舶在申请网络安全相关附加标志时，可根据船舶网络安全预期与 CCS 协商确定应满足的网络安全等级。

1.3.2.3 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 CCS 相关要求。

1.3.3 申请

1.3.3.1 申请 CCS 进行船舶网络安全检验/评估的系统和/或船舶，应向 CCS 或 CCS 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。

第4节 免除申请

1.4.1 申请免除

1.4.1.1 当指南适用的 CBS 要免除相关安全要求时，供应商或系统集成商/船厂应向 CCS 提出申请。

1.4.1.2 申请免除的 CBS 应按 1.4.2 所列要求开展，并满足 1.4.3 免除接受准则，提供相关 CBS 的网络风险评估报告，作为免除系统处于可接受风险水平的证据。

1.4.2 CBS 网络安全风险评估

1.4.2.1 网络安全风险评估时，应考虑 CBS 的类别，分析其预期运行环境（识别网络事件发生的可能性及其对人身安全、船舶安全或海洋环境的影响），分析攻击面（考虑 CBS 的连接等级、可能的便携式设备接口、逻辑访问限制、系统集成或系统间的接口包括非船载系统的远程访问等），从资产脆弱性、内部和外部威胁、网络事件潜在影响等因素进行评估，风险评估方法可参考本指南附录 1。

1.4.3 CBS 网络安全要求免除接受准则

1.4.3.1 当 CBS 为以下情况之一时，原则上不允许申请免除

（1） 当 CBS 为 III 类计算机系统时；

（2） 当 CBS 是本指南适用范围中规定的具有多种重要功能的综合控制系统时。

1.4.3.2 当 CBS 满足以下全部条件时，可以申请免除

（1） CBS 是孤立的（如与其它系统或网络无 IP 连接）；

（2） CBS 应没有可访问的物理接口；

（3） CBS 位于物理访问受控制的区域。

1.4.4 免除批准

1.4.4.1 结合具体船舶，按照 1.4.2 所列要求，提供满足 1.4.3 免除准则的 CBS 网络风险评估报告。

1.4.4.2 当不能满足 1.4.3.2 全部条件，但可以向 CCS 提供合理解释和证据，也可以申请免除，CCS 有权根据情况要求其提供附加文件。

1.4.4.3 在接受免除时，CCS 对其风险控制措施进行评估确认风险水平可控，可在产品阶段批准风险评估报告，CCS 船舶审图验船师结合船舶应用场景，批准该 CBS 在具体船舶的相关要求免除。

第2章　产品网络安全要求

第1节　一般规定

2.1.1 一般要求

2.1.1.1 本章所述产品包括但不限于：

（1） 本指南 1.1.1.3 提及的 CBS 及实现本指南 1.1.1.4 规定接口的系统或设备；

（2） CCS 认为必要的网络设备（如边界防火墙、核心交换机等）；

（3） 申请方要求的其他系统/设备。

2.1.1.2 CBS 中的主机、软件程序、嵌入式设备、网络设备、云虚拟设备等，满足的最低要求应根据所在系统级别而定。

2.1.1.3 网络设备系指网络中将各类服务器、终端设备、应用终端等节点相互连接的专用软硬件系统/设备，包括网络交换设备（交换机、网桥等）、网络路由设备（路由器等）、网络安全系统/设备（防火墙、安全网关、入侵检测系统、安全审计系统、加解密系统等）、网络接入设备（网络接口卡、无线接入点等）等。应用在 CBS 中的网络设备应至少满足本指南 2.3.1 和 2.3.2 相应安全等级的要求。单独申请认证的网络设备应满足该类设备的指南要求，或 CCS 认可的等效要求。

2.1.1.4 船用产品的网络要求以安全要求为核心，其通信要求及可靠性要求以满足其业务预期为基准。

2.1.1.5 产品网络安全要求以表 2.1.1.5 所列七个要素为核心，根据产品网络安全分级，提出了具体要求。

船舶产品网络安全要求要素　表 2.1.1.5

序号	基本安全要素	说明
1	标识和鉴别	在允许访问系统之前，识别并验证所有用户（人员、软件进程和设备）
2	使用控制	为通过身份鉴别的用户（人员、软件进程或设备）分配权限，以便系统执行请求的授权操作，并监控权限使用情况
3	系统完整性	确保系统的完整性，防止未授权操作
4	数据保密性	确保通讯信道和存储区域的数据的保密性，防止未授权的披露
5	受限数据流	通过区域和管道对系统进行分段，限制不必要的数据流动
6	事件及时响应	对违背网络安全要求的行为作出响应，通知有关人员，报告必要的证据，并在发现事件时及时采取措施
7	资源可用性	确保系统的可用性，防止重要服务受到影响或拒绝服务

2.1.2 基本安全要求

2.1.2.1 重要系统的安全措施不应对系统可用性造成不利影响。安全措施的实施不得导致安全功能、控制功能、监测功能等的丧失。

2.1.2.2 安全区域边界处于故障关闭状态或孤岛模式时，不应影响重要系统的基本功能。

2.1.2.3 系统在设计时，应确保船舶、系统、人员和货物安全所需数据的保密性、完整性和可用性。

2.1.2.4 为满足一个或多个安全要求，可以使用补偿措施代替或补充固有的安全能力。补偿措施应遵循以下原则：

（1） 补偿措施应符合原规定要求的意图和严格性，应“不低于”其他要求；

（2） 系统要求提供的安全能力，可以由其他设备或系统提供。对于系统的型式认可，补偿措施应在 CBS 中实施，即不依赖于船上安装或操作程序相关的边界防护；

（3） 应同时遵循第 3.1.3 节安全能力说明文件描述的原则。

第2节 产品网络安全分级

2.2.1 产品网络安全分级

2.2.1.1 产品网络安全分为 5 个等级（SL0~ SL 4）见表 2.2.1.1。

船舶产品网络安全分级 表 2.2.1.1

序号	分级	本指南对应要求	防御能力
1	SL 0	见 2.3-2.4 节	满足 CBS 最低网络安全要求（UR E27）的防御能力
2	SL 1		抵御偶发的网络事件的防御能力
3	SL 2		抵御利用少量资源发起的网络事件的防御能力
4	SL 3		抵御利用丰富资源发起的网络事件的防御能力
5	SL 4		抵御有组织有目的的网络事件的防御能力

第3节 系统要求

2.3.1 CBS 安全要求

2.3.1.1 标识和鉴别

（1） 人员身份标识和鉴别

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.1	CBS 应能标识并鉴别所有访问系统的人员	√	√	√	√	√
SR1.1 RE1	CBS 应能唯一标识和鉴别所有人员			√	√	√
SR1.1 RE2	CBS 应对通过不可信网络访问的人员采用多因素身份认证	√*[4]	√*[5]	√	√	√
SR1.1 RE3	CBS 应对所有人员采用多因素身份认证					√

（2） 进程和设备标识和鉴别

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.2	CBS 应能标识和鉴别所有通过接口访问的进程和设备	√*	√*	√	√	√
SR1.2 RE1	CBS 应能唯一标识和鉴别所有软件进程和设备				√	√

（3） 账户管理

4 √表示适用。

√*表示与不可信网络连接时适用。

5 √*表示 IEC 62443-3-3 对应级别中不适用，但本指南中适用于与不可信网络相连的情形。

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.3	CBS 应提供支持授权用户管理所有账户的能力，包括添加、激活、修改、禁用和删除	√	√	√	√	√
SR1.3 RE1	CBS 应支持统一账户管理的能力				√	√

（4） 标识管理

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.4	CBS 应提供通过用户、组、角色或控制系统接口支持标识管理的能力	√	√	√	√	√

（5） 鉴别管理

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.5	CBS 应提供以下能力： ① 初始化鉴别符（令牌、密码、指纹等）内容； ② CBS 安装时要求修改所有鉴别符的默认值； ③ 修改/更新所有鉴别符； ④ 在存储和传输时，保护所有鉴别符不受未经授权的披露和修改	√	√	√	√	√
SR1.5 RE1	对于软件和设备用户，CBS 应能通过硬件机制（如 TPM）保护相关鉴别符				√	√

（6） 无线访问管理

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.6	CBS 应对无线通信的所有用户(人员、软件进程或设备)进行标识和鉴别	√	√	√	√	√
SR1.6 RE1	CBS 应对所有使用无线通信的用户(人员、软件进程或设备)提供唯一标识和鉴别能力			√	√	√

（7） 口令强度

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.7	对于口令认证的 CBS，应能通过设置最小长度和多种字符类型，配置口令强度	√	√	√	√	√
SR1.7 RE1	CBS 应防止任何人员在一定的口令更换周期内重复使用密码。此外还应能限制人员口令的最短和最长使用期限				√	√
SR1.7 RE2	应能限制所有用户口令的最短和最长使用期限					√

（8） PKI 证书

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.8	当采用 PKI 技术时，CBS 应能根据最佳实践运行 PKI，或从现有 PKI 中获取公钥证书			√	√	√

（9） 公钥认证强度

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.9	当采用公钥认证时，CBS 应能： ① 通过检查证书签名的有效性验证证书； ② 通过构建到一个接受的可信 CA 的证书路径来验证证书，或者在自签名证书的情况下，通过将子证书部署到所有与颁发证书的主体通信的主机来验证证书； ③ 通过检查给定证书的撤销状态来验证证书； ④ 建立用户(人员、软件进程或设备)对相应私钥的控制； ⑤ 将已验证的身份映射到用户(人员、软件进程或设备)			√	√	√
SR1.9 RE1	CBS 应根据普遍接受的安全行业实践和建议，通过硬件机制保护相关的私钥				√	√

（10） 身份鉴别反馈

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.10	CBS 应在认证过程中对鉴别反馈信息模糊处理	√	√	√	√	√

（11） 失败登录尝试

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.11	CBS 应能限制任何用户(人员、软件进程或设备)连续无效访问尝试，尝试次数可配置；应能配置拒绝访问时间，或直至管理员解锁为止 对于代表其运行重要服务或服务器的系统账户，应能禁止交互式登录	√*	√	√	√	√

（12） 系统使用告知

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.12	CBS 应具有在身份验证前显示系统使用告知信息的能力。信息应能由授权人员设置	√*	√	√	√	√

（13） 不可信网络的访问

编号	要求	SL0	SL1	SL2	SL3	SL4
SR1.13	CBS 应能监测和控制所有通过不可信网络的访问方式	√*	√	√	√	√
SR1.13 RE1	除指定角色的许可，CBS 应拒绝不可信网络的访问请求	√*	√*	√	√	√

2.3.1.2 使用控制

（1） 授权实施

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.1	CBS 应能在所有交互接口上为所有人员分配权限，以	√	√	√	√	√

	控制系统的使用，支撑实施职责分离和最小特权					
SR2.1 RE1	CBS 应能在所有接口上为所有用户（人员、软件进程和设备）分配权限，以控制系统的使用，支撑实施职责分离和最小特权			√	√	√
SR2.1 RE2	CBS 应能授权用户或角色，定义和修改所有人员或角色到权限的映射			√	√	√
SR2.1 RE3	CBS 应支持管理员在可配置时间或事件期间，手动覆盖当前人员的授权 ①				√	√
SR2.1 RE4	当某个操作可能严重影响船舶安全时，如操作模式切换，应支持双重许可/确认					√

① 在发生紧急情况或其他严重事件时，需对自动机制实施受控、审计和手动覆盖。管理员利用当前用户能够快速对异常情况做出反应，而无需关闭当前会话，再以更高权限的用户建立一个新会话。

（2） 无线使用控制

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.2	CBS 应根据普遍接受的安全行业惯例，授权、监测和限制无线连接的使用	√	√	√	√	√
SR2.2 RE1	CBS 应能识别并报告在系统物理环境中传输的未经授权的无线设备				√	√

（3） 便携式和移动设备的使用控制

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.3	CBS 支持便携式和移动设备的使用时，应能： ① 将便携式和移动设备限制在设计允许或授权的范围内； ② 限制与便携式和移动设备之间的代码和数据传输 ②	√	√	√	√	√
SR2.3 RE1	CBS 应能验证试图连接到某个区域的便携式或移动设备是否符合该区域的安全要求				√	√

② 特定系统可接受端口限制/阻塞。

（4） 移动代码

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.4	CBS 应能控制移动代码技术的使用，如 Javascripts、ActiveX 和 PDF	√	√	√	√	√
SR2.4 RE1	CBS 应能在允许代码执行之前，验证移动代码的完整性				√	√

（5） 会话锁定

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.5	CBS 应具备会话锁定能力，在可配置的不活跃时间后自动或手动启动。会话锁定将通过人员或其他授权人员重新进行身份验证建立访问	√	√	√	√	√

（6） 远程会话终止

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.6	CBS 应能在一段闲置时间后自动终止远程会话，或者由发起会话的用户手动终止远程会话，该时间可配置	√*	√*	√	√	√

（7） 并行会话控制

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.7	CBS 应能在会话中限制每个接口的并发会话数量，该并发数可配置				√	√

（8） 可审计事件

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.8	CBS 应能生成与安全相关的可审计记录，类别至少包括：访问控制、操作系统事件、备份和恢复事件、配置更改、通信中断	√	√	√	√	√
SR2.8 RE1	CBS 应能集中管理可审计事件，并将整个控制系统的多个组成部分的审计记录汇编成一个系统范围（逻辑或物理）的、时间相关的审计追踪。控制系统应提供以行业标准格式导出这些审计记录的能力，以供标准商业日志分析工具分析，例如，安全信息和事件管理（SIEM）				√	√

（9） 可审计日志存储容量

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.9	CBS 应根据公认的日志管理和系统配置建议，分配足够的审计记录存储空间。应提供审计机制，以减少超出这种能力的可能性	√	√	√	√	√
SR2.9 RE1	当分配的审计记录存储达到最大审计记录存储容量的可配置百分比时，CBS 应能发出警告				√	√

（10） 审计处理失败响应

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.10	CBS 应能在审计处理失败的情况下，提醒人员以防止重要服务和功能的损失 CBS 应根据公认的行业惯例和建议，支持采取适当措施以应对审计处理失败事件	√	√	√	√	√

（11） 时间戳

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.11	CBS 应能提供用于生成审计记录的时间戳	√	√	√	√	√
SR2.11 RE1	CBS 应能以一定的频率同步内部系统时钟，该频率可配置				√	√

SR2.11 RE2	应保护时间源不受未经授权的更改，并应在更改时生成审计事件					√

（12） 不可否认性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR2.12	CBS 应能判定给定的人员是否采取了特定的操作				√	√
SR2.12 RE1	CBS 应能判定给定的用户（人员、软件进程或设备）是否采取了特定的操作					√

2.3.1.3 系统完整性

（1） 通信完整性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.1	CBS 应能保护传输信息的完整性 注：无线网络应采用加密机制。	√	√	√	√	√
SR3.1 RE1	CBS 应能使用密码机制来识别通信过程中信息的改变	√*	√*	√*	√	√

（2） 恶意代码防护

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.2	CBS 应能采用保护机制，防止、检测、报告恶意代码或未经授权的软件，减轻其影响；并应能更新保护机制	√	√	√	√	√
SR3.2 RE1	CBS 应能在所有接口采用恶意代码防护机制			√	√	√
SR3.2 RE2	应能管理恶意代码防护机制				√	√

（3） 安全功能验证

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.3	CBS 应支持验证安全功能的预期操作，并在 FAT（Factory Acceptance Test 工厂试验），SAT（Site Acceptance Test 现场试验）和定期维护期间发现异常时报告。这些安全功能应包括支持本指南中规定的安全要求的所有适用功能①	√	√	√	√	√
SR3.3 RE1	CBS 应能采用自动化机制，支持 FAT、SAT 和定期维护期间的安全验证管理 注：信息采集、报告生成等验证管理方式的自动化				√	√
SR3.3 RE2	应能在正常操作过程中验证安全功能					√

① 安全功能验证包括杀毒软件功能的验证，标识、鉴别和使用控制方法的验证，IDS 触发规则的验证。

（4） 软件和信息完整性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.4	CBS 应能检测、记录、报告和防止未授权更改软件和信息			√	√	√
SR3.4 RE1	CBS 应能在完整性验证发现差异时，使用自动工具通知特定人员				√	√

（5） 输入有效性验证

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.5	CBS 应验证所有用于控制或直接影响 CBS 动作的输入语法和内容	√*	√	√	√	√

（6） 确定性输出

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.6	如果攻击导致正常操作无法维持，应将输出或自身状态设置为预定值（断电、保持、固定值）	√	√	√	√	√

（7） 错误处理

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.7	应能识别并处理错误状态，并支持进行有效修补。处理措施不应提供可能被对手利用来攻击系统的信息，除非披露这些信息对及时排除问题是必要的			√	√	√

（8） 会话完整性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.8	应能保护会话的完整性。CBS 应拒绝任何无效会话 ID 的使用。	√*	√*	√	√	√
SR3.8 RE1	应能在用户注销或其他会话终止时（包括浏览器会话）使会话 ID 失效	√*	√*	√*	√	√
SR3.8 RE2	应能为每个会话生成唯一的会话 ID，并将所有非预期的会话 ID 视为无效。				√	√
SR3.8 RE3	应能使用普遍接受的随机来源生成唯一的会话 ID					√

（9） 审计信息保护

编号	要求	SL0	SL1	SL2	SL3	SL4
SR3.9	应能保护审计信息和审计工具（如有）不受未授权的访问、修改和删除			√	√	√
SR3.9 RE1	应能在一次性写入硬盘上生成审计记录					√

2.3.1.4 数据保密性

（1） 信息保密性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR4.1	应能支持显式读授权，保护信息的保密性，无论是存储信息还是在传输中的信息。	√	√	√	√	√
SR4.1 RE1	应能保护存储信息和远程访问会话信息通过不可信网络时的保密性			√	√	√
SR4.1 RE2	应能保护通过任何区域边界的信息的保密性					√

（2） 信息持久性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR4.2	组件退役或服务释放时应能清除所有相关读授权的信息			√	√	√
SR4.2 RE1	应能防止通过易失性共享内存资源进行未授权和非计划的信息传输				√	√

（3） 使用加密

编号	要求	SL0	SL1	SL2	SL3	SL4
SR4.3	如需要加密，应根据普遍接受的安全行业实践和建议，使用加密算法、密钥长度和密钥建立和管理机制	√	√	√	√	√

2.3.1.5 受限数据流

（1） 网络分段

编号	要求	SL0	SL1	SL2	SL3	SL4
SR5.1	应能从逻辑上将控制系统网络与非控制系统网络进行分段，从逻辑上将重要系统网络与其他控制系统网络进行分段		√	√	√	√
SR5.1 RE1	应能将控制系统网络与非控制系统网络进行物理分段，并将重要系统网络与其他控制系统网络进行物理分段			√	√	√
SR5.1 RE2	应能向控制系统网络、重要系统网络或其他网络提供网络服务，而不连接到非控制系统网络				√	√
SR5.1 RE3	应能从逻辑上和物理上隔离提供主重要服务的重要系统网络和提供次重要服务的重要系统网络					√

（2） 区域边界保护

编号	要求	SL0	SL1	SL2	SL3	SL4
SR5.2	应能监测和控制区域边界的通信，根据基于风险等方式划分区域		√	√	√	√
SR5.2 RE1	应默认拒绝所有网络流量，允许例外网络流量（也称为拒绝所有，例外允许）			√	√	√
SR5.2	应能防止任何通过控制系统边界的通信（也称为孤岛				√	√

RE2	模式）					
SR5.2 RE3	当边界保护机制发生操作故障(也称为故障关闭)时，应能防止通过控制系统边界的任何通信。这种“故障关闭”功能的设计应不影响安全相关功能的运行				√	√

（3） 系统外通信的限制

编号	要求	SL0	SL1	SL2	SL3	SL4
SR5.3	应能防止从 CBS 以外的用户或系统接收社交媒介、邮件等通信信息		√	√	√	√
SR5.3 RE1	应能防止传递和接收社交媒介、邮件等通信信息				√	√

（4） 应用分区

编号	要求	SL0	SL1	SL2	SL3	SL4
SR5.4	应支持根据关键程度对数据、应用和服务进行分区		√	√	√	√

2.3.1.6 事件的及时响应

（1） 审计日志可访问性

编号	要求	SL0	SL1	SL2	SL3	SL4
SR6.1	应支持授权的人员和/或工具以只读方式访问审计日志	√	√	√	√	√
SR6.1 RE1	应能使用应用程序编程接口（API）提供对审计记录的程序化访问				√	√

（2） 持续监控

编号	要求	SL0	SL1	SL2	SL3	SL4
SR6.2	应使用普遍接受的安全行业实践和建议，持续监控所有安全机制的性能，以及时发现、表征和报告安全漏洞			√	√	√

2.3.1.7 资源可用性

（1） 抗拒绝服务攻击

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.1	应能在 DoS 事件期间维持重要功能 ①	√	√	√	√	√
SR7.1 RE1	应能管理通信负载（如使用速率限制），以减轻 DoS 事件的影响			√	√	√
SR7.1 RE2	应能限制所有用户（人员、软件进程和设备）引发 DoS 事件对其他 CBS 或网络造成的影响				√	√

①注：可接受计算机系统面对 DoS 事件时降级运行，但不得以可能导致危险情况的方式失效。应考虑基于过载的 DoS 事件，如网络容量被试图淹没的情况，计算机资源被试图消耗的情况

（2） 资源管理

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.2	应能通过安全功能限制资源的使用，防止资源耗尽。	√	√	√	√	√

	例如，CBS 应能够为高优先级进程优先分配系统资源					

（3） 系统备份

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.3	应能标识和定位关键文件，对用户级和系统级信息（包括系统状态信息）进行备份，而不影响设备的正常运行。具体备份要求参考本指南第 4 章第 3 节事件恢复相关要求	√	√	√	√	√
SR7.3 RE1	应能验证备份机制的可靠性			√	√	√
SR7.3 RE2	应能根据可配置的频率自动执行备份功能				√	√

（4） 控制系统恢复和重建

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.4	应能在中断或故障后恢复并重建到已知的安全状态	√	√	√	√	√

（5） 电源

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.5	电源切换应不影响现有安全状态或预设的降级模式	√	√	√	√	√

（6） 网络和安全配置设置

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.6	应能根据供应商推荐的网络和安全配置设置 CBS 的通信量。CBS 应为网络和安全配置提供接口	√	√	√	√	√
SR7.6 RE1	应能生成安全配置报告，可采用 CSV、JSON、XML 等格式				√	√

（7） 最小功能

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.7	应明确禁止和/或限制使用不必要的功能、端口、协议和/或服务	√	√	√	√	√

（8） 控制系统组件清单

编号	要求	SL0	SL1	SL2	SL3	SL4
SR7.8	应记录已安装组件及其关联属性的列表			√	√	√

2.3.2 网络设备附加安全要求

2.3.2.1 网络设备还应满足如下附加安全要求：

（1） 诊断和测试的物理接口

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR2.13	应对用于工厂诊断和测试的物理接口进行防护，防止未			√	√	√

	授权使用					
NDR2.13 RE1	应能主动监测网络设备的诊断和测试接口，并生成通过接口访问的审计日志				√	√

（2） 支持更新

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR3.10	网络设备应支持升级和更新		√	√	√	√
NDR3.10 RE1	网络设备应对所有软件更新和升级的真实性和完整性进行验证			√	√	√

（3） 物理篡改防护和检测

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR3.11	应具备防篡改和检测机制，防止未授权的物理访问			√	√	√
NDR3.11 RE1	网络设备应能向接收者自动通报发现的未授权物理访问尝试，所有篡改通报应记入审计日志，作为整体日志功能的一部分				√	√

（4） 提供产品供应商可信根

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR3.12	应能提供并保护产品供应商制造设备用作可信根的密钥和数据的保密性、完整性、真实性			√	√	√

（5） 提供资产所有方的可信根

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR3.13	网络设备应： ① 提供并保护资产所有方的密钥和数据的保密性、完整性、真实性； ② 不依赖设备所处安全区域之外的组件			√	√	√

（6） 引导启动完整性

编号	要求	SL0	SL1	SL2	SL3	SL4
NDR3.14	应能在启动前验证组件启动过程所需的固件、软件和可配置数据的完整性		√	√	√	√
NDR3.14 RE1	网络设备应在启动前使用供应商的可信根验证启动过程所需的固件、软件、可配置数据的真实性			√	√	√

（7） 入侵防范

编号	要求	SL0	SL1	SL2	SL3	SL4
ADD1	具备入侵防范功能的网络设备应能对收集的信息进行分析，发现入侵事件		√	√	√	√
ADD1 RE1	具备入侵防范功能的网络设备在检测到入侵事件时，能够采取记录事件、自动发出安全警告或阻断等安全措施			√	√	√

（8） 安全审计

编号	要求	SL0	SL1	SL2	SL3	SL4
ADD2	具备安全审计的网络设备应能监测、记录审计目标的网络运行状态、网络安全事件 注：不同类型网络安全专用产品的安全审计目标不同，审计目标通常包括主机、网络、数据库、应用等		√	√	√	√
ADD2 RE1	应能对事件进行比较分析以发现违规、异常等行为			√	√	√
ADD2 RE2	应将网络运行状态日志和网络安全事件日志存储于非易失性存储介质中，本地或外发日志保存时间不少于6个月			√	√	√

第4节 安全开发周期要求

2.4.1.1 系统/设备的开发应遵循安全开发生命周期中各阶段的网络安全要求，至少包含以下因素：

（1） 安全需求分析，需求分析应明确系统/设备所需要的预期安全环境和安全功能，安全需求可从安全环境、威胁模型、安全需求审计等方面予以考虑；

（2） 安全设计，供应商选择适用的编程语言、体系结构、防御机制、平台、通信协议、密码等方式方法实现系统/设备安全需求；

（3） 安全实施，系统/设备实现过程符合安全需求和安全设计要求。在实施过程中需注意应用规范编码、使用代码分析工具、使用安全测试工具、人工审核代码安全等方面；

（4） 验证，对系统/设备进行安全性验证的过程，用以确认系统/设备是否满足本指南2.2.1条相应安全等级要求。应对测试过程发现问题予以记录，并反馈安全实施过程予以修复，对于修复后系统/设备还应进行验证，最终实现在发布前将安全风险降低至可控范围；

（5） 发布，系统/设备在发布前，应对前期开发过程中所有过程/记录进行安全审查，确认安全开发过程中所有安全问题都已经得到修复或者缓解。产品通过安全评审后可以进行发布；

（6） 维护，供应商应对产品定期进行安全评估，确认产品是否存在安全风险，必要时应进行补丁等安全信息更新；

（7） 退役，系统/设备从运行环境中移除，断开与环境中的任何接口，对系统/设备中的重要信息应进行处理（备份/删除），确保系统/设备退役后内部信息被永久删除；

2.4.1.2 供应商应编制安全开发生命周期文档，用以确认系统/设备满足安全开发生命周期要求。文件应包含以下内容：

（1） 私钥控制文件，以保护用于代码签名的私钥免受未经授权的访问或修改（如适用）；

（2） 安全更新文档，制定程序确保向用户提供有关产品安全更新的文件（如通过建立网络安全联络机制或用户可以访问的定期更新文档），包括但不限于：

① 应用安全补丁的产品版本号；

② 关于如何手动和自动安装已批准补丁的说明；

③ 明确安装补丁后对于产品可能产生的任何影响，包括重新启动；

④ 关于如何验证已安装批准补丁的说明；

⑤ 安装未经批准或非资产所有者部署的补丁可能导致的风险。

（3） 相关组件/操作系统的安全更新文档，以说明产品是否与依赖的组件或操作系统安全更新兼容；

（4） 安全更新交付程序，供应商应制定质量保证（QA）流程，用以规定产品更新发布前的安全测试，并可以确保产品用户能验证其适用产品及版本安全更新的真实性；

（5） 产品纵深防御策略，用于描述产品的安全纵深防御策略，以支持安装、操作和维护，包括：

① 产品提供的安全能力及其在纵深防御策略中的作用；

② 纵深策略战略所应对的威胁；

③ 针对与产品相关的已知安全风险的用户缓解策略，包括与遗留代码相关的风险。

（6） 预期外部环境中的纵深防御措施，描述产品预期的由外部环境（如物理布置、策略和程序）提供的纵深安全防御措施；

（7） 安全加固指南，产品安装和维护时的加固指南，主要信息包括：

① 产品（包括第三方组件）与其安全环境的集成；

② 产品的应用程序编程接口/协议与用户应用程序集成；

③ 实施和维护产品的纵深防御策略；

④ 配置和使用支持本地安全策略的安全选项/功能，以及每个安全选项/功能：

a) 对产品纵深防御战略的作用；

b) 对可配置值和默认值的描述，包括每个值如何影响安全性，以及每个值对业务的潜在影响；

c) 设置/更改/删除相关值；

⑤ 所有安全相关工具和实用程序的使用说明和建议，这些工具和实用程序支持产品安全性的管理、监控、事件处理和评估；

⑥ 定期安全维护活动的说明和建议；

⑦ 向产品供应商报告产品安全事件的说明；

⑧ 产品维护和管理的最佳安全实践说明。

2.4.1.3 供应商应制定程序和技术控制措施，建立质量保证流程用以规定产品安全开发过程中的各阶段和安全开发生命周期文档编制。该程序文件和安全开发生命周期文档应提交 CCS 审核，应满足以下要求：

（1） 私钥控制文件

如果系统包含为使用户能够验证其真实性而进行数字签名的软件，则适用此要求。 供应商应提供管理文件，证明其策略、程序和技术控制措施已到位，以保护用于代码签名的私钥的生成、存储和使用免受未经授权的访问。策略和程序应规定角色、职责和工作过程。技术控制应包括物理访问限制和用于存储私钥的加密硬件(例如硬件安全模块)。

（2） 安全更新文档

供应商应提供管理文件，证明在组织内建立了流程，以确保安全更新可通知到用户，向用户提供的信息应包括本指南 2.4.1.2（2）所列的项目。

（3） 相关组件/操作系统的安全更新文档

供应商应提供本指南 2.4.1.2（3）要求的管理文件，证明组织内已建立了流程，以确保

用户知道系统是否与其依赖软件的更新版本（新版本、操作系统或固件的补丁）兼容，这些通知信息应描述如何管理不进行更新的风险。

（4） 安全更新交付程序

供应商应提供本指南 2.4.1.2（4）要求的管理文件，证明组织已建立流程，确保向用户提供系统安全更新，并描述用户如何验证更新后软件的真实性。

（5） 产品纵深防御策略

供应商应提供本指南 2.4.1.2（5）要求的管理文件，证明组织已建立了流程，以记录纵深防御策略，以减轻 CBS 中软件在安装、维护和运行期间的安全威胁。威胁可能是安装未经授权的软件，补丁程序中的弱点，在船舶运行阶段篡改软件。

（6） 预期外部环境中的纵深防御措施

供应商应按本指南 2.4.1.2（6）要求提供管理文件，证明组织已建立流程，以明确记录期望外部环境(如物理布置、策略和程序)提供的纵深防御措施。

（7） 安全加固指南

供应商应提供本指南 2.4.1.2（7）要求的管理文件，证明组织已建立流程，以确保为系统制定了加固指南。指南应具体描述如何通过删除/禁止/禁用不必要软件、账户和服务等降低系统的脆弱性。

第3章　产品检验/评估

第1节　一般规定

3.1.1 检验范围

3.1.1.1 本章产品检验/评估适用的范围包含 2.1.1.1 规定的产品。

3.1.2 检验/评估流程

3.1.2.1 检验范围适用的产品，应向 CCS 提出检验申请。其中，CCS 规范要求认可或自愿认可的产品，可结合产品初次认可、认可变更、换证向 CCS 提出；CCS 规范未要求认可的产品可结合产品检验提出。

3.1.2.2 产品网络安全相关的图纸资料应按照 3.1.3 提交，产品检验要求应按照本指南第 3 章第 2 节要求进行，验证合格后向其签发认可证书或产品证书。

3.1.2.3 自愿申请网络安全评估的产品，应向 CCS 提出书面申请，必要时可签订评估服务合同和/或协议。

3.1.2.4 申请网络安全评估的产品，应按照 3.1.3 提交图纸资料，按照第 3 章第 2 节进行测试验证，经 CCS 审图和见证测试验证合格，向其签发产品网络安全评估报告。

3.1.2.5 供应商应遵循本指南 2.4 安全开发生命周期的要求，并通过现场审核验证。

3.1.2.6 当产品已通过网络安全能力验证后，则可按表 3.1.3.1 备注 2）所标识提交简化的图纸和试验资料。

3.1.2.7 网络设备可单独或作为系统组件与系统一起提交申请。

3.1.3 图纸资料及试验资料

3.1.3.1 应按表 3.1.3.1 提交图纸资料供 CCS 批准或备查。

图纸资料汇总表　　**表** 3.1.3.1

序号	需要提交的文件	提交
1	CBS 资产清单	Ⓐ[1)2)]
2	网络拓扑图	Ⓐ[1)2)]
3	安全能力描述	Ⓐ[1)]
4	安全能力试验大纲	Ⓐ[1)]
5	安全配置指南	Ⓘ[1)]
6	安全开发生命周期	Ⓐ[1)]
7	维护和验证计划	Ⓘ[1)]
8	支持网络事件响应及恢复计划的信息	Ⓘ[1)]
9	变更管理计划	Ⓘ[1)]
10	配置核查报告	Ⓘ[2)]

符号说明：

X：适用

Ⓐ：提交 CCS 批准；

Ⓘ：提交 CCS 备查；

[1)]：未取得网络安全能力认证时提交；

[2)]：已取得网络安全能力认证时提交。

3.1.3.2 提交文件的具体要求如下：

（1） CBS 资产清单，应包括：

① 硬件资产清单，至少包含：

a) 硬件组件名称清单（如主机设备、嵌入式设备、网络设备）；

b) 品牌/制造商；

c) 型号/类型；

d) 功能/用途简述；

e) 物理接口（如网络、串口）；

f) 系统软件（如操作系统、固件）的名称/类型；

g) 系统软件的版本和补丁级别；

h) 支持的通信协议。

② 软件资产清单，至少包含：

a) 软件组件清单（如应用软件、实用软件）；

b) 安装的硬件组件；

c) 品牌/制造商；

d) 型号/类型；

e) 功能/用途简述；

f) 软件版本。

（2） 网络拓扑图，采用物理和逻辑拓扑结构（也可采用一份综合拓扑图）描述网络流或数据流（源、目标、协议、物理实现），可包含设备名称、IP 地址、网络区域边界等：

① 物理网络拓扑图描述系统物理架构，能够清晰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：

a) 所有终端和网络设备，包括冗余单元；

b) 通信线缆（网络，串口连接），包括 I/O 通信单元；

c) 与其他网络或系统的通信线缆连接。

② 逻辑网络拓扑图描述系统软件组件间的网络或数据流向，包括：

a) 通信终端（如工作站，控制器，服务器等）；

b) 系统内网络设备（交换机，路由器，防火墙）的布置；

c) 船载工作站、服务器、控制器等终端的布置及接入方式；

d) 物理和虚拟计算机；

e) 物理和虚拟通信线路；

f) 通信协议。

（3） 安全能力描述，说明 CBS 及其软硬件组件如何满足所要求的安全能力，至少含以下适用内容：

① 描述与其他 CBS 的网络接口，包括目的 CBS、数据流和通信协议；

② 描述与不可信网络的网络接口。描述接口如何满足与不可信网络连接时的附加要求，并包括相关的操作程序或操作人员说明；

③ 详细描述安全区域边界的保护组件；

④ CBS 所有硬件和软件如何满足各项安全能力要求；

⑤ 要求不能完全满足的部分，提供有效补偿措施。

（4） 安全能力试验大纲，应为每项适用的要求单列章节，并说明以下内容：

① 必要的测试设置（即确保可重复测试，且预期结果相同）；

② 测试设备；

③ 初始条件；

④ 测试方法、详细测试步骤；

⑤ 结果评估衡准；

⑥ 参照标准（如有时）。

（5） 安全配置指南，目标是确保安全功能的实施符合第 4 章要求和系统集成商的所有规范（如用户账户、授权、密码策略、设备的安全状态、防火墙规则等），并包含以下适用内容：

① 安全功能的建议配置及默认值；

② 网络数据流量限定值；

③ 设备开放的端口；

④ 用户访问权限配置清单；

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方式；

⑧ 系统配置文件免受未授权访问保护措施。

（6） 安全开发生命周期文档，应至少包括本指南第 2.4.1.2 条要求的内容，说明供应商的流程和控制措施，并说明软件更新与补丁情况；

（7） 维护和验证计划，应包括与安全有关的系统维护和测试程序，以及用户如何按照第 2 章 2.3.1.3（3）的要求验证系统安全功能操作正确性的说明，至少包括：

① 维护内容；

② 维护方式；

③ 维护周期。

（8） 支持网络事件响应及恢复计划的信息，至少应包括：

① 受损系统的隔离位置；

② 网络事件或网络异常的报警和指示说明；

③ 网络事件可能导致的主要后果说明；

④ 响应方案，优先考虑不依赖于直接关闭或转移到本地控制的方案（如有时）；

⑤ 本地控制信息，用于本地操作因网络事件而失效的系统；

⑥ 通过审计记录取证的说明，审计记录的要求参考 SR2.8；

⑦ 备份，相关要求参考 SR7.3；

⑧ 恢复，恢复和重建要求参考 SR7.4；

⑨ 受控关机、回滚、重置、重启方案。

（9） 变更管理计划：

① 依据变更程序，明确变更管理职责、范围、流程等。

（10） 配置核查报告，由供应商签署的报告，证明供应商已完成设计、施工、测试，并按照安全配置指南和加固指南完成安全功能的配置和加固。

第2节 测试验证

3.2.1 一般要求

3.2.1.1 应根据产品申请的安全级别，按 CCS 批准的产品网络安全试验大纲，在 CCS 或经 CCS 认可的试验机构完成相关测试验证。

3.2.1.2 试验项目应涵盖本指南第 2 章对应安全级别所适用的要求，对于船舶网络防火墙应按照 CCS《船舶网络防火墙检验指南》执行。

3.2.1.3 系统/设备的试验还应进行安全漏洞扫描或渗透测试、网络连接测试，以验证系统/设备的整体网络安全状态。

3.2.1.4 网络设备试验还应进行安全漏洞扫描或渗透测试、网络风暴测试、性能测试，以验证网络设备的网络安全状态及性能。网络设备作为系统的组件时，可结合系统设备一起测试。

3.2.1.5 通过系统/设备网络安全漏洞扫描，确认无高风险项，或当存在高风险项时可举证出已采取了有效风险缓解措施。

3.2.1.6 相关测试项目可采用测试工具执行，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。

3.2.1.7 如产品无法确定在船舶系统中的具体应用场景时，CCS 可验证在有限使用情景下的网络安全要求。为完成测试验证，CCS 也可要求供应商提供必要的图纸、详细资料、测试报告和与供应商声明标准相关的验证，在完成要求的检查和测试后可出具有限使用情景下的验证结果。

3.2.2 测试验证

3.2.2.1 在 CCS 验船师见证下，进行如下试验项目：

（1） 试验前检查产品资产清单、安全配置、网络拓扑、接口等的符合性；

（2） 核查系统/设备的安全配置，特别是船舶网络防火墙、路由器、交换机等网络设备的安全配置；

（3） 应对设备按照 2.3.1-2.3.2 和 3.2.1.3-3.2.1.7 要求进行适用测试；

（4） 根据系统/设备的安全基本级别及是否存在远程连接或远程维护，根据第 2 章第 3 节确定需要满足的技术条款，然后确定测试方法及可验证衡准。

3.2.2.2 安全漏洞扫描

（1） 通过技术手段，对产品进行全面的检测和漏洞扫描，定位漏洞分析原因，并将结果作为测试验证的结论之一；

（2） 漏洞扫描完成后，申请方应提供测试报告供 CCS 验证。

3.2.2.3 渗透测试

（1） 通过技术手段，对产品进行全面的渗透测试，并将结果作为测试验证的结论之一；

（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协助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 CCS 验证。

3.2.2.4 网络风暴测试

（1） 通过技术手段，对网络设备进行网络风暴抑制能力测试，并将结果作为测试验证的结论之一；

（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 CCS 验证。

3.2.2.5 网络连接测试

（1） 通过技术手段，对网络系统产品进行网络连接测试，验证网络设备连接的操作性和功能，并将结果作为测试验证的结论之一；

（2） 测试完成后，申请方应提供测试报告供 CCS 验证。

3.2.3 变更

3.2.3.1 供应商/系统集成商应定义变更的分类

（1） 根据可能对安全能力产生的预期影响对变更的内容进行分类；

（2） 定义变更分类与软件版本/修订之间的关系。

3.2.3.2 对产品安全能力产生影响的变更应提交至 CCS 批准，必要时进行相应的试验。

3.2.3.3 变更说明应至少包含表 3.2.3.3 描述的内容。

变更描述信息 **表** 3.2.3.3

活动	描述
目的	描述变更的原因
分类	根据修改策略定义修改的类型
设计	描述并执行所需的设计活动，包括更新相关文件
版本	根据修改策略进行版本更新
后果	分析修改可能产生的影响
批准	确保修改供应商和客户接受
实施	描述并执行需要的实施活动
验证	根据程序进行测试、验收、相关者见证、报告等相关活动

第4章　船舶网络安全要求

第1节　一般规定

4.1.1 一般要求

4.1.1.1 应对船舶网络安全风险进行管理，并建立和实施有效的船舶网络安全风险管理制度，使船舶网络保持一定的韧性，以应对网络威胁。

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

4.1.1.3 识别、保护、检测、响应、恢复为支持船舶有效网络风险管理的五个功能要素，本章所有网络安全要求都基于这五个功能要素提出。具体定义如下：

（1） 识别：建立对船上系统、人员、资产、数据等信息的全面了解；

（2） 保护：制定并采取适当的保障措施，以保护船舶免受网络事件的影响，并最大限度地保障船舶持续运行；

（3） 检测：制定并采取适当的措施，以检测和识别船舶发生的网络事件；

（4） 响应：针对发现的船舶网络事件，制定并采取适当的措施和动作；

（5） 恢复：制定并采取适当的措施和动作，以恢复因网络事件而受损的船舶运行业务所需的功能或服务。

第2节　M 标志要求

4.2.1 一般要求

4.2.1.1 船舶网络安全风险管理制度应纳入安全管理体系，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。

4.2.1.2 安全管理体系的安全和环境保护方针应包含船舶网络风险管理的内容。

4.2.1.3 安全管理体系的责任和权限信息中应包含涉及网络风险管理的责任和权限，应设立船舶网络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）。

4.2.1.4 船舶所属公司应持有有效的符合 ISM/NSM 规则要求的 DOC 证书，船舶应持有有效的符合 ISM/NSM 规则要求的 SMC 证书。

4.2.1.5 安全管理体系的建设，可参考本指南附录 2、CCS《海事网络风险评估与管理体系指南》和 IMO《海上网络风险管理指南(MSC-FAL.1/Circ.3)》。

4.2.1.6 最新有效的管理体系文件和相关人员资料、管理记录（如有时，包括报告、日志、记录表单等）应在船上随时可用。

4.2.1.7 发生重大变化时，应将相关文件资料提交给 CCS，以确认船级附加标志是否继续有效。

4.2.1.8 发生重大网络事件时，应及时通知 CCS，并提交事故信息、事故处理措施及解决方案。

4.2.2 管理制度

4.2.2.1 有效的安全风险管理制度系指基于风险的可持续改进的管理制度。

4.2.2.2 管理制度中应包含运维管理的内容，包括但不限于：

（1） 人员管理，包括录用与离岗、培训与管理、第三方人员等；

（2） 风险管理，包括漏洞识别与修补、风险评估等；

（3） 安全检查，包括常规检查和全面检查等；

（4） 变更管理，包括变更申报、审批和实施等；

（5） 事件与应急管理，包括应急计划制定和演练，以及事件报告、响应和改进等；

（6） 备份与恢复管理，包括备份策略制定、备份实施和恢复等；

（7） 服务供应商管理，包括产品供应商、通信服务供应商和外包运维服务商等；

（8） 密码管理，包括采用的密码标准、相关技术和产品等；

（9） 环境管理，包括登船访问、机房维护等；

（10） 资产管理，包括资产清单的创建与维护、资产新增、更新、报废等；

（11） 介质管理，包括登记管理、物理传输、使用和报废等；

（12） 设备管理，包括设备维护、出场/回场、报废、接口管控等；

（13） 网络和应用系统安全管理，包括账户管理、安装与升级、配置管理、访问控制、恶意代码防范、运维操作等；

（14） 云计算管理（如有时），包括平台的选择、数据防泄漏等；

（15） 移动互联管理（如有时），包括无线接入管控等；

（16） 物联网管理（如有时），包括感知节点、网关节点的新增和变更的全过程管理，以及保密性管理和可用性管理等；

（17） 大数据管理（如有时），包括数字资产安全管理策略、分类分级保护策略、自动脱敏等。

4.2.2.3 开展运维管理活动时，应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） 资产的安全管理，包括资产登记、变更等；

（3） 日常运维、应急准备、应急响应、定期检查/检测等；

（4） 服务供应商的安全管理；

（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）。

4.2.2.4 当船舶网络系统存在新建和/或重大改建的情况时，如改造网络基础设施、开发并上线新的应用系统等，管理制度中还应纳入建设管理的内容，包括但不限于：

（1） 确定需求，包括需求的编制、论证和通过等；

（2） 规划设计，包括方案编制、安全措施选择和方案论证等；

（3） 工程实施，包括责任人确定、实施方案制定和执行、第三方监理等；

（4） 产品采购和使用，包括合规性、选型等；

（5） 软件开发，包括代码编写、安全性测试、发布/更新等；

（6） 测试验收，包括测试方案制定、实施等；

（7） 系统交付，包括交付清单、应用培训等；
（8） 云服务商管理（如有时），包括合规性、服务协议、数据泄露保护等；
（9） 移动互联管理（如有时），包括软件的分发渠道、开发方等；
（10） 大数据管理（如有时），包括合规性、数据安全等。

4.2.2.5 开展建设管理活动时，应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） 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。

4.2.3 风险管理

4.2.3.1 应实施 CCS《海事网络风险评估与管理体系指南》附录 1 的措施。

4.2.3.2 应识别网络安全方面的培训需求，并纳入管理体系的培训项目中。

4.2.3.3 应按适当的分类方式识别并建立船舶网络风险管理的资产清单和网络拓扑图，并对其进行实时维护。

4.2.3.4 对于已识别的资产进行风险评估，可参考 CCS《海事网络风险评估与管理体系指南》附录 2 和本指南附录 1。

4.2.3.5 对所有已识别的船舶、人员和环境风险，制定和实施适当的安全措施。

4.2.3.6 对于网络事件，应制定和实施适当的发现、响应、恢复和防止再发生的措施。

第3节 P 标志和 S 标志要求

4.3.1 一般要求

4.3.1.1 船舶网络设计应以风险评估为原则，满足船舶网络业务预期。

4.3.1.2 本节所有网络安全要求与 4.1.1.3 条定义的五个功能要素的对应关系见表 4.3.1.2。

网络风险管理的功能要素与船舶网络安全要求关系表 **表 4.3.1.2**

功能要素	网络安全要求
识别	资产清单
保护	资产保护、资产处置、物理访问控制、网络防护、安全区域、边界防护、网络冗余、通信安全、入侵防范、身份鉴别、访问控制、恶意代码防范、远程访问、远程维护、无线通信、移动介质安全、变更管理、脆弱性管理
检测	网络运行监测、安全审计
响应	事件响应
恢复	恢复和备份

4.3.2 资产清单

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.2.1	应提供本指南适用范围内各 CBS、连接船上和岸端 CBS 的网络的资产清单，资产清单应： ① 包含 1.1.1.3 条中所有的 CBS（如适用）； ② 在船舶整个生命周期内保持更新，更新记录应包含软件和硬件修改可能引入的新漏洞以及功能性依赖或连接的变化情况； ③ 如果清单中包括保密信息(如 IP 地址、协议、端口号)，则应采取特别措施，将此类信息的访问限制为只有授权人员才能访问。	√	√	√	√	√
4.3.2.2	资产清单应包括适用范围内所有硬件和软件，至少包含 3.1.3.2（1）中所列的信息以及 CBS 所属的系统类别和安全区域；CBS 软件应按照船东在船舶网络安全管理计划中制定的软件维护和更新管理策略进行维护和更新	√	√	√	√	√

4.3.3 资产保护

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.3.1	应对资产管理制定规范化要求，制定资产分类和标识要求，明确资产的使用、物理传输、存储、保护、处置等要求			√	√	√
4.3.3.2	重要系统数据的备份（无论是临时的还是永久的），应该用与原始数据同等的保护手段				√	√
4.3.3.3	存储在便携式设备上的关键或敏感信息应采用行业最佳实践加密算法进行加密				√	√

4.3.4 资产处置

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.4.1	应制定资产安全处置程序，至少应包括以下内容： ① 明确数据删除前获得了授权； ② 对于关键数据，制定必要的安全措施，以防止资产处置过程中信息泄露； ③ 明确资产处置的措施，至少应包含资产移除的时间、归还资产的验证和记录方式、授权移除资产人员的身份、角色等信息； ④ 需销毁的资产或数据，应采取必要的安全措施，确保存储设备在销毁前受保护的资产或数据销毁后无法重建和恢复					√

4.3.5 物理访问控制

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.5.1	本指南适用的 CBS 和网络，以及存储在这些系统中的信息应只允许授权人员根据其职责或预期功能需要进行访问	√	√	√	√	√
4.3.5.2	Ⅱ类和Ⅲ类 CBS 一般应位于受控空间，以防止未授权的访问，或应安装在可上锁的机柜或控制台。这些位置应便于船员和需要使用 CBS 的相关方执行安装、集成、操作、维护、维修、更换、处置等任务，以免妨碍船舶的正常和高效运行	√	√	√	√	√
4.3.5.3	应限制主管当局、技术人员、代理、港口和码头官员以及船东代表等访客使用船上计算机，例如在监督下使用	√	√	√	√	√
4.3.5.4	船上Ⅱ类和Ⅲ类 CBS 网络的接入点应在监督下或根据文件规定的程序(如维护)进行连接，否则应进行物理和/或逻辑阻断	√	√	√	√	√
4.3.5.5	如访客有临时连接的需求(如打印文件)，应使用与所有船载网络隔离的独立计算机或其他网络(如访客专用接入网络或乘客娱乐活动专用网络)	√	√	√	√	√
4.3.5.6	访客离开或授权船员的访问权限到期后应及时收回		√	√	√	√
4.3.5.7	机房（或类似场所）出入口应配置电子门禁系统，控制、鉴别和记录进入的人员			√	√	√
4.3.5.8	对 II 类和 III 类 CBS 的物理访问，应有相应的日志记录，至少记录： ① 访问人员身份； ② 访问时间； ③ 访问目的				√	√
4.3.5.9	用于物理访问控制的物理安全设备（如监视摄像机、入侵检测器、电子锁等）应： ① 具有强身份认证方法，如密码、智能卡、令牌等。如采用密码，则应为非默认值，保持密码的复杂性，并定期更新； ② 定期进行测试，确保其工作在正常作业状态； ③ 记录的数据应经授权才可进行维护和访问					√

4.3.6 网络防护

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.6.1	应防止网络发生过高数据流量和其它可能损害网络资源服务质量的事件	√	√	√	√	√
4.3.6.2	本指南适用的 CBS 应按照“最小功能”原则配置，即只提供必要的功能，限制非必要功能的使用，禁用或限制非必要的功能、端口、协议、服务、默认共享等	√	√	√	√	√

4.3.6.3	网络设计应满足预期通过的数据流量，并将拒绝服务（DoS）和网络风暴/高流量的风险降至最低，数据流量的估算应至少考虑网络容量、预期应用的数据速度和数据格式	√	√	√	√	√

4.3.7 安全区域

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.7.1	本指南适用的所有 CBS 应划入安全区域并满足相应的安全策略和安全能力，各安全区域之间应进行物理或逻辑隔离，只有经过明确允许的流量才能通过安全区域边界。	√	√	√	√	√
4.3.7.2	一个安全区域可以包含多个 CBS 和网络，所有的 CBS 和网络都应符合本指南本章及第 2 章中的适用要求	√	√	√	√	√
4.3.7.3	根据系统类型（I、II、III 类）、资产重要性、系统功能等因素将船舶网络划分为不同的安全区域，并满足以下要求： ① 提供安全功能的 CBS 应归入单独的安全区域，并与其他安全区域进行物理分段； ② 航行和通信系统不得与机械、货物系统处于同一安全区域，如果航行和/或无线电通信系统是按照 1.1.1.5 条中其他等效标准批准，则该类系统应划入单独的安全区域； ③ 无线设备应位于单独的安全区域； ④ 本指南适用范围之外的 CBS 和网络，应与本指南所要求的安全区域进行物理分段。或者，如果这些系统能够满足安全区域的同等要求，则可视为该安全区域的一部分； ⑤ 应能够在不影响安全区域内 CBS 主要功能的情况下，手动隔离一个安全区域； ⑥ 定义安全控制策略时，应将网络的访问或操作功能与角色相关联	√	√	√	√	√
4.3.7.4	OT 系统与 IT 系统之间应划分为不同区域，区域间应采用单向的技术隔离手段				√	√
4.3.7.5	应建立 DMZ，以减少可信网络与不可信网络之间的直接通信					√

4.3.8 边界防护

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.8.1	安全区域应通过防火墙或 4.3.7 所要求的其他同等手段进行保护，具备监测和控制区域边界通信的能力	√	√	√	√	√
4.3.8.2	安全区域边界设备应具备日志留存能力，日志要求见 SR2.8	√	√	√	√	√
4.3.8.3	应在网络边界或区域之间根据访问控制策略设置访问		√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	控制规则，默认情况下，除允许外，受控接口拒绝所有通信					
4.3.8.4	应删除多余或无效的访问控制规则，优化访问控制列表		√	√	√	√
4.3.8.5	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		√	√	√	√
4.3.8.6	应能根据会话状态信息允许/拒绝数据流进出		√	√	√	√
4.3.8.7	应在 OT 系统与 IT 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		√	√	√	√
4.3.8.8	应在安全区域之间的边界防护机制失效时，及时进行报警		√	√	√	√
4.3.8.9	应能够对非授权设备私自联到船舶内部网络的行为进行检查和限制				√	√
4.3.8.10	应能够对船载 CBS 非授权联到船舶外部网络的行为进行检查和限制				√	√
4.3.8.11	边界防护机制失效时应禁止所有流量通过，这种故障关闭模式不应影响系统的安全功能				√	√
4.3.8.12	应对进出网络的数据流实现基于应用协议和应用内容的访问控制					√

4.3.9 网络冗余

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.9.1	应提供关键网络、计算、存储及连接线缆等设备的硬件冗余，保证系统的可用性				√	√
4.3.9.2	冗余系统在发生故障时，应具有足够的自我诊断能力，以便有效地转移到备用单元				√	√
4.3.9.3	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，且应具备高可用性，其布置应确保其中一个防火墙单元发生故障或网络事故时，另一个单元仍能保持船舶网络的安全					√

4.3.10 通信安全

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.10.1	若使用加密技术，则应采用公认的安全行业惯例或最佳实践，在加密方案中应说明使用的算法、协议和密钥（包含密钥长度、到期日期）以及密钥使用情况	√	√	√	√	√
4.3.10.2	船舶网络应能够为高优先级 CBS 优先分配网络资源		√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.10.3	应采用密码技术保证通信过程中数据的完整性				√	√
4.3.10.4	当数据的完整性遭到破坏时，应自动通知责任船员				√	√
4.3.10.5	应采用密码技术保证通信过程中数据的保密性					√

4.3.11 入侵防范

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.11.1	应在关键网络节点处监测网络攻击行为。可以通过使用 IDS、IPS 等系统来实现		√	√	√	√
4.3.11.2	当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应发出报警		√	√	√	√
4.3.11.3	应对网络管理终端的接入方式或接入网络地址范围进行限制		√	√	√	√
4.3.11.4	应进行数据输入有效性验证，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			√	√	√

4.3.12 身份鉴别

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.12.1	CBS 应能对用户的身份进行鉴别，满足 2.3.1.1（1）SR1.1 和 SR1.1 RE2 的要求	√	√	√	√	√
4.3.12.2	应对用户进行身份标识，对登录用户进行身份鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换			√	√	√
4.3.12.3	应采用口令、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					√

4.3.13 访问控制

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.13.1	应通过文件系统、网络、应用程序或数据库的访问控制列表对 CBS 及其相关信息进行保护。应根据船舶和岸基人员的角色和责任分配登录账户，限制激活的时期，不再需要时予以注销	√	√	√	√	√
4.3.13.2	访问控制策略不应对系统的功能产生不利影响，需要强访问控制的 CBS 可使用强加密密钥或多因素身份验证进行防护	√	√	√	√	√
4.3.13.3	允许完全访问系统配置和所有数据的管理员权限，只应授予经过培训的、因职责需要的船员	√	√	√	√	√
4.3.13.4	所有用户仅拥有实现其功能必须的最小权限，即操作权限不应高于完成预定任务所需的权限级别	√	√	√	√	√

4.3.13.5	所有新账户的默认权限配置应尽可能低。在必要时允许提升权限，如使用临期权限或一次性使用凭证。应定期对用户和进程账户进行审计，避免权限随着时间而积累	√	√	√	√	√

4.3.14 恶意代码防范

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.14.1	应对本指南适用的 CBS 进行恶意代码（如病毒、蠕虫、木马、间谍软件）防护	√	√	√	√	√
4.3.14.2	具有标准操作系统的 CBS 应安装、维护并定期更新采用工业标准的防恶意代码软件，除非此类软件的安装影响到 CBS 的功能和服务水平（如执行实时任务的II类和III类 CBS）	√	√	√	√	√
4.3.14.3	对于无法安装防恶意代码软件的 CBS，应采用操作程序、物理防护或厂商推荐的方式进行防护	√	√	√	√	√
4.3.14.4	应在船舶网络边界节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新		√	√	√	√
4.3.14.5	应在船舶网络边界节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新		√	√	√	√
4.3.14.6	系统应具备恶意代码保护机制管理能力，这种机制通常由端点基础设施集中管理或 SIEM 解决方案实现				√	√

4.3.15 远程访问

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.15.1	应提供用户手册，以控制对船载 IT 和 OT 系统的远程访问，并应明确访问人员的角色和权限	√	√	√	√	√
4.3.15.2	不应将任何船载 CBS 的 IP 地址暴露给不可信网络	√	√	√	√	√
4.3.15.3	应通过具有端点身份验证、完整性保护、网络或传输层验证和加密能力的安全连接（如 VPN）与不可信网络进行通信，应确保授权信息的保密性	√	√	√	√	√
4.3.15.4	船载 CBS 应具备如下能力： ① 具有从船端终止连接的能力。在船员明确接受之前，不得进行任何远程访问； ② 能够控制远程会话的中断，以免影响 OT 系统的安全功能或 OT 系统数据的完整性和可用性； ③ 提供日志功能，记录所有远程访问事件并保留一段时间，以便对远程连接进行离线审查，例如在检测到网络事件后	√	√	√	√	√
4.3.15.5	应对任何通过不可信网络的访问行为进行监测（例如记录、显示、报警）和控制（例如拒绝、限制）	√	√	√	√	√
4.3.15.6	从船东、操作人员和供应商特定位置建立远程连接进行船舶操控时，应满足以下要求：		√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	① 在船端和远程控制端应明确显示操作控制权的位置； ② 船舶与远程控制端应有应答机制，保证通信连接，当远程连接断开时，船端应有提示； ③ 应优先传输控制信号					
4.3.15.7	应限制与船载 CBS 通信的源地址，避免陌生地址的攻击行为			√	√	√

4.3.16 远程维护

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.16.1	当远程访问用于远程维护时，除满足 4.3.15 条要求外，还应满足以下要求： ① 应提供文件说明如何与岸端连接和集成； ② 维护的补丁和更新在安装前应进行测试和评估以确保有效，且不会导致不可接受的影响或网络事件； ③ 远程更新前，供应商应提供针对上述内容的确认报告； ④ 供应商应向船东提供更新支持计划，具体参见 2.4.1.2（4）（5）（6）条； ⑤ 在远程维护期间，授权人员应能随时中断和中止会话，并可以回滚到系统之前的安全配置； ⑥ 任何用户从一个不可信网络访问本指南适用范围内的 CBS 时，都需要多因素身份认证； ⑦ 在预设的次数内访问失败后，再次访问需等待一段预设的时间； ⑧ 如果由于某种原因远程维护中断，将通过自动注销功能终止系统访问	√	√	√	√	√

4.3.17 无线通信

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.17.1	无线通信网络应在设计、实施和维护中，保护传输的信息不被操纵或泄露，网络事件不传播到其他控制系统，无线通信网络的访问应进行限制： ① 只有授权用户才能访问无线网络； ② 只有授权进程和设备才能使用无线网络通信	√	√	√	√	√
4.3.17.2	应采用符合行业标准和最佳实践的加密机制，包括加密算法、密钥强度等，以确保在无线网络上传输信息的完整性和保密性	√	√	√	√	√
4.3.17.3	无线网络上的设备只能在无线网络上通信(即它们不应是“双归属”)	√	√	√	√	√
4.3.17.4	III 类系统不应采用无线数据链路，除非经 CCS 依据其可接受的国际或国家标准进行工程分析后特别考虑	√	√	√	√	√

4.3.17.5	对采用无线通信技术进行控制的 OT 系统，应能识别其物理环境中未授权的无线设备，对试图接入或干扰控制系统的行为发出报警和控制（例如拒绝、限制）				√	√

4.3.18 移动介质安全

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.18.1	应制定移动介质使用策略，仅限授权人员使用。通过移动介质将数据上传到 CBS 或从 CBS 下载数据之前应进行扫描，通过数字签名和/或水印检查移动介质是否存在恶意软件和/或验证软件的合法性	√	√	√	√	√
4.3.18.2	只有经过授权的移动介质才能连接到 CBS，并满足 2.3.1.2（3）SR2.3 条要求。对不能完全满足要求的 CBS，需要对接口进行物理阻塞	√	√	√	√	√
4.3.18.3	应禁止便携式设备自动执行软件代码	√	√	√	√	√
4.3.18.4	使用无线连接的移动和便携式设备应满足 4.3.17 相关的要求	√	√	√	√	√
4.3.18.5	已采用逻辑或物理阻塞的端口应有明确标识		√	√	√	√

4.3.19 网络运行监测

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.19.1	应对本指南适用的船舶网络进行持续监测，并在发现网络异常、故障或能力退化时发出报警	√	√	√	√	√
4.3.19.2	网络监测内容至少应包含以下几个方面： ① 网络流量，如网络流量异常； ② 网络连接，包括通信链路故障； ③ 设备管理活动，如访问异常、操作系统攻击事件、配置更改； ④ 非授权移动设备的连接； ⑤ 如果网络带宽利用率超过产品供应商规定的异常阈值，则应发出报警； ⑥ 安全事件应具有满足 2.3.1.2（8）SR2.8 条要求的日志	√	√	√	√	√
4.3.19.3	如安装了 IDS，则 IDS 应满足以下要求： ① IDS 应由相应 CBS 的供应商进行合格认证； ② IDS 应设置为被动模式，不得激活可能影响 CBS 性能的保护功能； ③ 使用 IDS 的人员应适任	√	√	√	√	√
4.3.19.4	本指南适用范围内的 CBS 和网络应能对本指南要求的安全功能进行诊断，可采用设备的自诊断功能或网络监控工具(如 ping、traceroute、ipconfig、netstat、nslookup、Wireshark、nmap 等)对 CBS 的完整性和安全状态进行诊断，并提供维持安全功能的手段，以保证船舶安全运行	√	√	√	√	√

4.3.20 安全审计

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.20.1	应制定审计管理制度，包含日志管理、审计处理失败响应计划。审计日志应至少保留一个船舶检验周期		√	√	√	√
4.3.20.2	审计记录应包括事件的日期和事件、用户、事件类型、事件是否成功及其他与审计相关的信息		√	√	√	√
4.3.20.3	系统应为授权用户提供审核日志的只读访问权限		√	√	√	√
4.3.20.4	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计，如访问控制、错误请求、操作系统事件、备份和恢复事件、配置更改、潜在的侦查活动等		√	√	√	√
4.3.20.5	应对审计记录进行保护，定期备份，避免受到非预期的删除、修改或覆盖等			√	√	√
4.3.20.6	作为审计的一部分，应对存储容量进行监控，并在超过容量阈值之前向相关人员发出报警，以防止审计记录丢失				√	√
4.3.20.7	应对远程访问、互联网访问等用户行为单独进行行为审计和数据分析				√	√
4.3.20.8	应提供审计事件的集中管理。如采用 SIEM 技术将日志数据、安全报警和事件聚合，为安全监控提供实时分析				√	√
4.3.20.9	应保护时间来源，防止未授权的更改。如发生了修改，应记录该事件					√

4.3.21 事件响应

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.21.1	船东应制定船舶网络事件响应计划，计划包含一套预先设定的指令或程序文件，用于检测、响应和限制网络事件的后果	√	√	√	√	√
4.3.21.2	参与船舶设计和建造阶段的各相关方应向船东提供信息，以便在第一次年度检验时完成事件响应计划的制定。在船舶的营运期间，事件响应计划应保持更新（如有维护时）	√	√	√	√	√
4.3.21.3	事件响应计划应提供程序，通过通知主管当局、报告事件的必要证据和采取及时纠正措施，以响应检测到的网络事件，将影响限制在初发网络分段内。计划至少应包含以下信息： ① 受损系统的隔离断点； ② 网络事件或网络异常报警和指示说明； ③ 网络事件可能导致的后果；	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	④ 响应方案，优先考虑不切断系统或转移到独立或本地控制的方案（如有）； ⑤ 受损系统的独立和本地控制信息，用于独立操作因网络事件而失效的系统（如适用）					
4.3.21.4	事件响应计划应以硬拷贝的形式保存，以防止电子存储设备的完全丢失	√	√	√	√	√
4.3.21.5	SOLAS 第 II-1 章 31 条要求的用于本地备用控制的 CBS 应独立于主控制系统，包括能够实现有效本地操作的必要的人机界面	√	√	√	√	√
4.3.21.6	用于本地控制和监视的 CBS 应是独立的，不依赖与其他 CBS 通信来实现其预期运行	√	√	√	√	√
4.3.21.7	若本地控制和监视系统通过网络与远程控制系统或其他 CBS 进行通信，则应划为一个单独的安全区域，并满足本节 4.3.7 和 4.3.8 条关于区域划分和边界防护的相关要求。对于特殊情况，经 CCS 同意可特别考虑	√	√	√	√	√
4.3.21.8	事件响应计划中涉及网络隔离，则应满足以下要求： ① 应能根据预定的程序终止与其他安全区域的双向通信，如通过操作网络设备上的物理开关 ON/OFF 或断开连接路由器/防火墙的线缆等类似操作。设备上应有清晰的说明和标记，以协助操作人员有效隔离网络； ② 应识别单个系统的数据对系统功能和操作正确性（包括安全）的影响，明确标识系统隔离时，如何对数据或功能输入进行补偿	√	√	√	√	√
4.3.21.9	如网络事件影响到系统或网络，使其无法按要求提供预期的服务能力，则受影响的系统或网络应能回退到最低风险状态。回退措施可包括： ① 使系统完全停止或回退到其他预定义的安全状态； ② 脱离系统； ③ 将控制权限转移到其他系统或操作人员； ④ 其他补偿措施	√	√	√	√	√
4.3.21.10	应在足以使船舶保持安全状态的时间范围内恢复到最低风险状态	√	√	√	√	√
4.3.21.11	供应商和集成商应从设计阶段开始考虑系统回退到最低风险状态的能力	√	√	√	√	√

4.3.22 恢复和备份

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.22.1	本指南适用的 CBS 应具有恢复和备份能力，以使船舶在发生网络事件后快速、安全地恢复航行和运行状态	√	√	√	√	√
4.3.22.2	船东应制定船舶网络事件恢复计划，以支持 CBS 因网	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	络事件造成中断或故障后恢复到运行状态					
4.3.22.3	参与船舶设计和建造阶段的各相关方应向船东提供信息，以便在第一次年度检验时完成恢复计划的制定。在船舶的营运期间，恢复计划应保持最新（如维护时）	√	√	√	√	√
4.3.22.4	恢复计划应易于船员和外部人员理解，并包括必要的说明和程序以确保故障系统的恢复。如需岸上支持，则应提供岸上联系方式。此外，船上还应提供必要的软件恢复介质或工具	√	√	√	√	√
4.3.22.5	在制定恢复计划时，应综合考虑各系统及子系统，制定以下恢复目标： ① 系统恢复：应根据恢复时间目标（RTO）规定恢复通信能力的方法和程序。RTO 为恢复所需通信链路和处理能力所需的时间; ② 数据恢复：应根据恢复点目标（RPO）规定恢复 OT 系统安全状态和船舶安全运行所需数据的方法和程序。RPO 为可以容忍的数据缺失的最长时间	√	√	√	√	√
4.3.22.6	恢复目标确定后，应创建一份潜在网络事件清单，并根据清单制定恢复计划，恢复计划应包含以下信息： ① 完整且最新的逻辑网络图； ② 所有组件的当前配置信息； ③ 在不中断冗余、独立或本地控制的情况下恢复故障系统的程序； ④ 备份和安全存储信息的程序； ⑤ 负责恢复故障系统的责任人员名单； ⑥ 沟通程序和外部技术支持联系人名单，包括系统支持供应商、网络管理员等	√	√	√	√	√
4.3.22.7	恢复计划应优先考虑船舶的操作和航行，以确保船上人员的安全	√	√	√	√	√
4.3.22.8	负责网络安全和协助网络事件的人员应可获得船上和岸上的硬拷贝恢复计划	√	√	√	√	√
4.3.22.9	恢复计划责任人员执行恢复操作时，应避免破坏有关事件原因的重要信息和证据（如擦除驱动器）。必要时，应获得专业的网络事件响应支持，以协助保存证据，同时恢复运行能力	√	√	√	√	√
4.3.22.10	船东应制定备份计划，内容应包括备份范围、备份方式和频率、存储介质和保留期限。备份计划提供的信息和设施应足以使系统从网络事件中恢复，并对备份进行定期维护和测试	√	√	√	√	√
4.3.22.11	应确保数据可从安全副本或介质中恢复	√	√	√	√	√
4.3.22.12	应考虑使用离线备份来降低恶意软件对在线备份的影	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	响					
4.3.22.13	CBS 和网络还应具备以下功能： ① 受控关机，允许其他连接的系统提交/回滚挂起的事务、终止进程、关闭连接等，使整个系统处于安全、一致和已知的状态； ② 重置，指导系统完成关机、清除内存并将设备重置为其初始化状态的过程； ③ 回滚，将系统返回至先前的配置和/或状态，以恢复系统的完整性和一致性； ④ 重启，从只读源启动并重新加载所有软件和数据的新镜像（例如，在回滚操作之后）。重启时间应与系统的预期服务兼容，不得使其他系统或其所属系统处于不一致或不安全的状态 应向船上人员提供有关如何执行上述操作的文件，以快速和安全地从网络事件可能造成的损害中恢复	√	√	√	√	√

4.3.23 变更管理

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.23.1	应根据《钢质海船入级规范》第 7 篇第 2 章第 6 节 2.6.10 变更管理的要求制定变更管理程序	√	√	√	√	√

4.3.24 脆弱性管理

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.24.1	应采取必要的措施识别安全漏洞和隐患，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		√	√	√	√
4.3.24.2	漏洞管理通过维护设备的功能、配置、操作、软件、固件、操作代码等来保持更新，至少应包含以下措施： ① 记录设备当前安装版本； ② 定期确定每个设备可用的升级和更新； ③ 对补丁进行评估，确保其不会对设备或系统的可靠性和可操作性产生负面影响（可通过仿真环境测试）； ④ 在合适的情境下（如，不会造成意外停机、中断等）进行补丁安装； ⑤ 补丁安装后及时更新资产清单信息（如版本信息、功能等）		√	√	√	√
4.3.24.3	应定期开展漏洞扫描，通过实施补丁或其他缓解措施来减少系统存在的安全漏洞		√	√	√	√

第5章　船舶网络安全检验

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（M, P[SL0]/ S[SLx]）附加标志的船舶。

5.1.1.2 船舶网络安全检验可与 CCS 规范规定的相同类型检验同时进行，也就是初次入级、年度、中间和特别检验。

5.1.2 图纸资料

5.1.2.1 申请 Cyber Security（M）附加标志的船舶，应按照指南第 4 章第 2 节的规定，提交船舶网络风险管理相关体系文件。

5.1.2.2 申请 Cyber Security(P[SL0])和 Cyber Security(S[SLx])附加标志的船舶，应按照指南第 4 章第 3 节的规定，提交以下图纸资料：

（1） 指南 3.1.3 要求的已批准的产品图纸；

（2） 船舶资产清单，船舶资产清单应包含指南适用范围内的所有系统和设备，船舶资产清单是系统资产清单的集合，每个系统应有独立的资产清单，如图 5.1.2.2 所示。此外，由系统集成商交付的符合指南第 4 章要求的网络设备也应包含在船舶资产清单中。

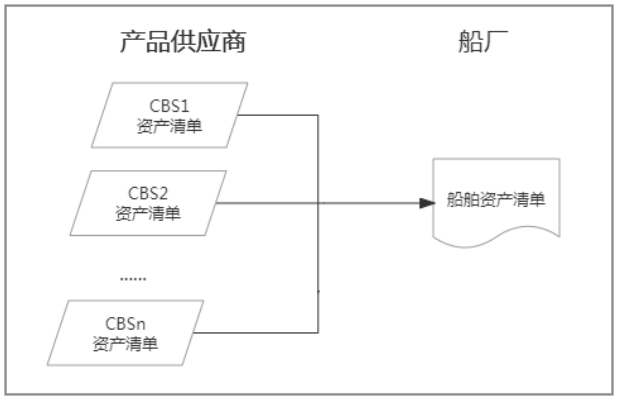


图 5.1.2.2 船舶资产清单

（3） 网络拓扑图，即能够识别各船载 CBS 之间、CBS 与外部设备或网络之间的物理或逻辑连接的框图，网络拓扑图应能清晰标识安全区域和每个 CBS 的物理位置。

（4） 网络安全设计说明书，至少应包括以下信息：

① 描述网络拓扑图中的安全区域及其包含的 CBS；

② 描述相同安全区域内的 CBS 之间的通信目的和特征（如协议和数据流向）；

③ 描述不同安全区域内 CBS 之间的通信目的和特征（如协议和数据流向），包括区域边界设备及允许通过区域边界的流量（如防火墙规则）；

④ 描述安全区域与不可信网络之间的通信，包括串口通信和基于 IP 协议的通信目的和特征（如协议和数据流向）、区域边界设备及允许通过区域边界的流量（如防火墙规则）；

⑤ 无线网络设计，说明无线网络设计方案，包括如何实现单独的安全区域、区域边界设备配备及允许通过区域边界的流量（如防火墙规则）；

⑥ 物理访问控制措施，对于需要立即访问的 CBS，若其人机界面已经位于物理访问控制区域，则无需进行用识别和身份验证。此类设备应在本文件中说明；

⑦ 恶意代码防护机制，概述每个 CBS 采用的恶意代码防护机制，对安装防恶意代码软件的 CBS，应说明如何保持软件更新；

⑧ 描述远程访问控制和通信情况。应对每个 CBS 进行识别，确定其是否可以远程访问或通过安全区域边界与不可信网络进行通信，如是，则应说明符合指南第 4 章 4.3.15 和 4.3.16 条相关要求；

⑨ 移动介质使用和管理策略；

⑩ 事件响应和恢复计划，应包含 4.3.21 和 4.3.22 条中要求的内容，其中指南第 3 章 3.1.3 条要求的产品网络事件响应及恢复计划应作为重要输入信息；

⑪ 备份计划；

⑫ 补偿措施说明（如有时）；

（5） 船舶网络安全测试大纲应包括在测试期间更新和记录结果的方法，并规定必要的测试环境、测试设备、初始条件、测试方法、详细的测试步骤、预期结果及接受准则。船舶网络安全测试大纲至少应验证以下内容：

① 指南适用范围内的 CBS 均包含在资产清单中，且所有软件为最新版本，如通过漏洞扫描工具或开机时核查软件版本进行验证；

② 网络安全区域及相关系统和设备布置与资产清单、网络安全拓扑图、网络安全设计说明书等相关文件描述一致，可通过现场检验、网络扫描和/或其他方法验证；

③ 安全区域边界只允许已批准的网络安全设计说明书中描述的流量通过，可通过评估防火墙规则或端口扫描来验证；

④ CBS 的组件位于只有授权人员可以进入的受控区域；

⑤ 边界保护设备抗拒绝服务（DoS）攻击的有效性（如适用），并确保对源自每个网段内部的过高数据流提供保护。拒绝服务（DoS）测试应涵盖网络风暴（即，试图消耗网段上的可用容量）和应用层攻击（即，尝试消耗网络中选定端点的处理能力）；

⑥ “最小功能”测试，通过分析评估和端口扫描来测试是否已根据供应商提供的加固指南移除或禁止了 CBS 中非必要功能、端口、协议和服务，可参考指南第 2 章 2.4.1.2（7）所要求的产品安全加固的指导文件；

⑦ 恶意软件防护或其他补偿措施的有效性，可使用可靠的反恶意程序测试文件进行测试；

⑧ 用户账户是根据职责分离和最少特权的原则配置的，且临时账户已被删除；

⑨ 无线网络依据各供应商提供的批准文件，采用安全无线通信协议（如通过使用网络协议分析工具进行验证），只有授权的设备才能接入无线网络；

⑩ 网络监控和保护机制：

- 测试断开的网络连接时会触发报警，并记录事件；
- 测试检测到异常高的网络流量时会生成报警和日志；
- 证明 CBS 将以安全的方式应对网络风暴，同时考虑单播和广播消息（另见测试项目⑤）；

- 验证可审计记录的生成（记录安全相关事件）；
- 如有入侵检测系统，则验证该系统是被动部署的，不会激活可能影响 CBS 预期操作的保护功能；

⑪ CBS 及网络安全功能验证程序的有效性；

⑫ 船舶安全所需的本地控制可以独立于任何远程或自动控制系统进行操作，应通过断开本地控制系统与其他系统/设备的网络进行测试；

⑬ 网络隔离的有效性，应通过断开所有穿越安全区域边界的网络，证明安全区域内的 CBS 在没有与其他安全区域或网络进行网络通信的情况下能够保持足够的操作功能；

⑭ 回退到最低风险状态，验证 CBS 在遭遇网络事件时，能够按照指南第 4 章第 3 节 4.3.21.9 条的措施，使系统恢复到合理的安全状态。例如，允许操作员通过其他方式执行控制和监测功能，使系统维持其基本服务。该测试可测试项目⑤一起进行；

⑮ 与不可信网络连接时，应满足指南第 2 章第 3 节与不可信网络连接时适用的相关要求，可使用协议分析工具进行分析；

⑯ 当远程用户进行远程访问时，应对以下内容进行验证：

a) 多因素身份认证；
b) 对登录失败次数进行限制，当远程用户建立会话时，应有提示信息；
c) 由船上负责人员确认后远程连接；
d) 船上人员可以手动终止远程连接，或者在一段非活跃时间后，自动终止；
e) 远程会话应形成审计日志，日志内容参见指南第 2 章第 3 节 2.3.1.2（8）条；
f) 相关供应商应提供操作手册及程序。

⑰ 移动介质使用控制，确保：

a) 只有授权用户才能使用移动或便携式设备；
b) 端口只能被特定设备使用；
c) 文件不能直接从移动介质传递到 CBS；
d) 移动介质中的文件不能自动执行；
e) 移动介质对网络访问应仅限于特定的 MAC 或 IP 地址；
f) 不使用的端口被关闭或物理阻塞。

⑱ 补偿措施测试（如有时）。

（6） 恢复和备份计划程序以及由供应商提供的 CBS 恢复和备份操作手册；

（7） 船舶网络安全管理计划，至少应包含以下内容：

① 变更管理程序，应依据《钢质海船入级规范》第 7 篇第 2 章第 6 节 2.6.10 变更管理的要求制定变更管理程序，主要包括硬件、软件的修改、安全补丁等；

② 安全区域边界设备（如防火墙）的管理，包括最小功能原则、明确允许的流量、防止拒绝服务（DoS）事件等；

③ 恶意代码防护管理，包括防护软件的维护及更新、物理防护及操作程序、移动介质的适用及访问控制等；

④ 物理和逻辑访问控制，包括系统和设备的物理访问控制、对访客的物理访问控制、对网络访问点的物理访问控制、访问控制凭证管理、最小权限策略等；

⑤ 保密信息的管理，包括保密信息、授权人员可获得的信息、 无线网络中传输的信息等；

⑥ 通过不可信网络进行远程访问及通信的管理要求，至少包括用户手册、角色及

许可、补丁及更新、远程更新前的确认、中断、停止及回滚等；

⑦ 移动介质管理要求，包括移动介质管理策略及程序、端口的物理阻塞、授权人员使用、仅支持授权设备的连接、考虑恶意软件的感染风险等；

⑧ CBS 和网络异常的管理活动，包括发现和识别异常活动、 安全可审计记录的检查、检测事件的说明或程序、上述活动可与事件响应一起管理；

⑨ CBS 和网络中安全功能的测试和定期维护管理；

⑩ 事件响应计划，至少应：

a) 说明谁、何时以及如何应对网络事件；
b) 描述对本地/手动控制的程序或说明；
c) 描述对隔离安全区域的程序或说明；
d) 描述在网络事件发生时，CBS 的预期行为。

⑪ 事件恢复和备份计划，至少应包括：

a) 说明谁、何时以及如何从网络事件中恢复；
b) 考虑可接受的停机时间、可供选择的其他控制手段、供应商支持及 CBS 重要性后，指定的备份计划，包括备份频率、备份维护和测试等；
c) 用于执行备份、关闭、复位、恢复和重新启动 CBS 的程序手册。

5.1.2.3 申请网络安全附加标志的船舶，各阶段应提交的图纸及其适用的附加标志见表 5.1.2.3。

图纸资料汇总表 表 5.1.2.3

序号	图纸名称	CCS			适用附加标志
		船舶审图	建造中检验	建造后检验	
1	网络风险管理相关体系文件			Ⓐ	M
2	批准的产品文档	Ⓡ			P, S
3	船舶资产清单	Ⓐ			M, P, S
4	网络拓扑图	Ⓐ			M, P, S
5	船舶网络安全设计说明书	Ⓐ			P, S
6	船舶网络安全测试大纲		Ⓐ		
7	船舶网络安全管理计划			Ⓐ[1)]	
8	免除网络要求的系统清单及风险评估报告	Ⓐ			P, S

符号说明：

Ⓐ提交 CCS 批准 Ⓡ提交 CCS 参考

[1)] 船舶在第一次年度检验前，由船舶现场验船师批准

第2节 初次入级检验

5.2.1 一般要求

5.2.1.1 船舶网络安全检验要求与其取得的网络安全附加标志密切相关。当船舶取得多个网络安全附加标志时，每个附加标志的要求均适用。

5.2.1.2 船舶网络安全测试大纲的所有测试应由 CCS 见证，其中部分测试项目（如 5.1.2.2(5)⑤-⑮项、供应商提供的 CBS 恢复和备份操作手册中的测试项），若其安全功能已经在 CBS 认证期间进行了测试，经 CCS 确认后可以免除。CBS 认证期间，如部分要求是通过补偿措施满足的，或在 CBS 认证后进行了修改，则相关测试不能免除。

5.2.2 检验和试验项目

5.2.2.1 申请 Cyber Security(M)附加标志的船舶，应完成以下检验项目：

（1） 确认船舶安全管理体系文件中已纳入网络风险管理项目；

（2） 确认船舶网络管理运行状况良好；

（3） 检查网络风险管理相关体系文件，确认其满足第 4 章第 2 节的要求。

5.2.2.2 申请 Cyber Security(P[SL0])和 Cyber Security(S[SLx])附加标志的船舶，应根据船舶网络安全测试大纲、恢复和备份计划程序以及由供应商提供的 CBS 恢复和备份操作手册，完成现场检验。

5.2.3 授予附加标志

5.2.3.1 检验/评估完成后， CCS 为船舶授予相应等级的附加标志。

第3节 建造后检验

5.3.1 一般要求

5.3.1.1 在船舶首次年度检验之前的适当时间，船东应向 CCS 提交船舶网络安全管理计划，记录本指南适用范围内的网络安全管理情况。

5.3.1.2 船舶网络安全管理计划经 CCS 批准后，船东应在首次年度检验中通过提供记录或其他文件证明其遵守了批准的船舶网络安全管理计划中所述流程。

5.3.1.3 后续船舶网络安全管理计划如有变更，应重新进行验证。

5.3.2 年度检验

5.3.2.1 年度检验应对以下项目进行确认：

（1） 网络风险管理制度或体系运行情况符合 M 后缀标志的要求（适用时）；

（2） 已遵照执行了已批准的变更管理流程；

（3） 已考虑 CBS 中软件的已知漏洞和功能依赖性，与供应商合作，按照变更管理程序安装安全补丁和更新其他软件并保存变更记录；

（4） 已更新船舶资产清单；

（5） 更新了网络拓扑图，安全区域边界遵照船舶网络安全管理计划进行了管理；

（6） 所有反恶意软件都保持维护和更新；

（7） 按照管理要求使用移动介质；

（8） 按照管理要求进行访问控制，应包含：

① 人员根据职责授权访问 CBS；

② 只有经过授权的设备才能连接到 CBS；

③ 访客可根据相关政策和程序访问 CBS。

（9） 凭据、密钥、保密信息、证书、相关 CBS 文档和其他敏感信息根据相关政策和程序进行管理和保密；

（10） 远程访问按照相关要求及用户手册已被记录并留存日志；

（11） 通过检查安全日志和调查 CBS 中的报警，定期监测了 CBS 中的异常情况；

（12） 定期测试或验证了 CBS 中的安全功能；

（13） 船舶具备一定事件响应、事后恢复的能力：

① 船上负责人员能够执行事件响应计划；

② 船上负责人员能够执行本地/手动控制、安全区域断开/隔离程序或说明；

③ 已根据事件响应计划对任何网络事件做出了响应；

④ 船上负责人员可获得事件恢复的说明和/或程序；

⑤ 已为船上负责人员提供恢复所需的设备、工具、文件和/或必要的软件和数据；

⑥ 根据策略和程序对 CBS 进行了备份；

⑦ 停机、复位、恢复和重新启动的说明手册和程序可供船上负责人员使用。

5.3.3 中间检验

5.3.3.1 中间检验与年度检验要求相同。

5.3.4 特别检验

5.3.4.1 船东应根据船舶网络安全测试大纲，基于年度检验项目开展安全功能测试，其中部分安全功能可依据变更记录进行测试。

附录1　船舶 CBS 风险评估

第1节　一般规定

1.1　一般要求

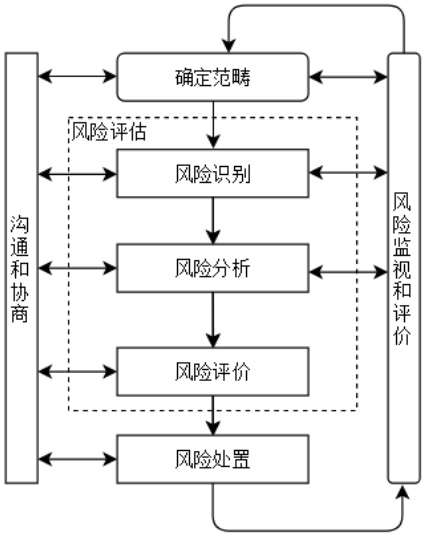
1.1.1　船东/船公司/供应商应对船舶 CBS 系统面临的威胁，以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对船舶造成的影响。

1.1.2　本指南提供一套完整的风险评估流程，仅供参考，也可采用其他经 CCS 认可的风险评估方法。

第2节　风险管理

2.1　风险管理过程

2.1.1　船舶 CBS 系统网络安全风险管理过程见图附录 1-2.1.1 风险管理过程。



图附录 1-2.1.1 风险管理过程

2.2　风险要素关系

2.2.1　风险评估基本要素包括资产、威胁、脆弱性和安全措施，并基于以上要素开展风险评估。

2.2.2　开展风险评估时，基本要素之间的关系如下：

（1）　风险要素的核心是资产，而资产存在脆弱性；

（2）　安全措施的实施通过降低资产脆弱性被利用难易程度，抵御外部威胁，以实现对资产的保护；

（3）　威胁通过利用资产存在的脆弱性导致风险；

（4）　风险转化成安全事件后，会对资产的运行状态产生影响。

2.3 风险评估过程

（1） 收集有关船舶系统、设备和连接的信息，以确定风险评估的范围。并应通过图纸资料进行补充，以便更好的了解系统/设备互连;

（2） 通过本文件中的评估等级或风险评估方法，评估不同的系统参数。这些参数的组合最终将形成评估范围内每个系统的风险等级;

（3） 根据之前评估的风险等级，通过定义和实施相关安全措施，确定是否处理风险，直到残余风险水平被认为是可接受的。

2.4 风险识别

2.4.1 资产识别

（1） 资产分类

根据 IACS UR E22 要求，基于系统功能故障的影响将计算机系统分为三类，参见表附录 1-2.3.1（1）所示。

计算机系统的分类　　表附录 1-2.3.1（1）

类别	影　响	典型系统功能
I	这些系统的故障不会对人员的安全、船舶的安全以及环境产生危害	——监测、信息和管理功能
II	这些系统的故障最终会对人员的安全、船舶的安全以及环境产生危害	——对保持船舶处于正常运营和起居状况所必要的报警、监测和控制功能
III	这些系统的故障即刻会对人员的安全、船舶的安全以及环境产生危害或灾难	——保持船舶推进和操舵的控制功能 ——船舶安全功能

资产分类，可将资产按照层次可划分为业务资产、系统资产、系统组件和单元资产，也可根据资产的表现形式，将资产分为 OT 系统、IT 系统等。本文件依据表附录 1-2.3.1（1），对 UR E26 的 CBS 系统进行了分类建议，详见表附录 1-2.3.1（2）。需注意，实际 I-III 类别的划分需根据各 CBS 系统的网络连接和系统功能故障的影响程度确定。例如一个 III 类 CBS 系统提供了独立的有效备份或可避免风险的方案，则可降低为 II 类系统。

CBS 的分类示例　　表附录 1-2.3.1（2）

序号	CBS 类别	CBS 名称	建议分类
1	推进系统	推进控制系统	III
		主机控制系统（各种形式）	III
		齿轮箱/离合器控制系统	III
		螺距控制系统	III
		侧推控制系统	II/III（取决于作业场景）
		推进辅助系统	II
		能源供给系统（油、气、电池）	III

2	操舵系统	操舵装置控制系统	III
		舵机液压单元控制检测系统	II
3	锚泊和系泊系统	锚系泊控制监测系统	II
		系泊绞车控制和监视系统	II
		锚泊定位系统（结合 DP 和锚链）	III
4	发电和配电系统	主发电机控制系统	III
		电池管理系统	III
		功率管理系统	III
5	火灾探测和灭火系统	火灾探测控制和报警系统	II
		防火门控制系统	II
		水雾灭火系统	II
		消防泵控制系统	II
		机舱固定灭火系统	II
6	舱底水和压载水系统，装载计算机系统	压载水控制和监控系统	II
		舱底水控制和监控系统	II
		装载计算机系统	II
		阀门遥控系统	II
		油水分离器	II
		生活污水处理装置	II
		焚烧炉、洗涤塔控制系统	II
7	水密完整性和进水探测系统	水密门控制和监控系统	II
		进水检测系统	II
		舷门控制系统	II
8	照明	应急照明	III
		低位照明	III
		航行灯控制	III
9	提供安全功能的系统	应急切断系统	III
		燃气安全系统	III
		货物安全系统	II
		压力容器安全系统	III
		气体探测系统	II

		点火源控制	III
		ESL（船岸连接系统）	III
10	航行设备	ECDIS（电子海图系统）	II
		ECS(国内航行船舶电子海图系统)	II
		电罗经	II
		计程仪	II
		测探仪	II
		AIS（自动识别系统）	II
		RADAR	II
		BNWAS	II
		艏向/航迹控制系统	II/III（取决于是否应用于自主航行）
		VDR（航行数据记录仪）	II
		驾控信息显示系统	I
11	内通设备	广播系统	II
		通用报警	II
		自动电话	II
		双向语音通信	II
12	无线电设备	GMDSS 组合台	II
		VHF	II
		MF/HF	II
		C 站	II
		NAVTEX	II
		其他卫星通信系统	I/III（取决于是否应用于远程控制通信）
13	多功能综合系统	全回转推进器控制系统	III
		INS（综合导航系统）	II
		IBS（综合船桥系统）	II
		ICS（综合通信系统）	II
		IAS（集成自动化系统）	II /III（取决于是否有控制能力）
14	智能系统	依据智能船舶规范执行	

（2） 资产赋值，按照船舶网络资产清单根据资产的保密性、完整性和可用性三个安全属性以及所属 I-III 类别这个重要属性，为资产赋值。

① 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；

② 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；

③ 根据资产在可用性上的不同要求，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；

（3） 资产重要性等级，结合船舶系统自身特点，可根据资产所属计算机类别，以及保密性、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。

2.4.2 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。表附录 1-2.3.2 例举了基于表现形式的威胁识别内容。

威胁识别内容 **表附录** 1-2.3.2

序号	威胁类别	威胁描述
1	操作失误	操作人员在工作中发生错误或疏忽，包括操作错误、维护失误等
2	越权滥用	超越自己的权限访问了无权访问的资源，或滥用自己的职权，做出破坏系统的行为，包括非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密等
3	行为抵赖	操作用户对自己的操作行为不承认，包括原发抵赖、接收抵赖、第三方抵赖
4	恶意代码	感染了在系统中执行恶意任务的程序代码，包括病毒、木马、蠕虫、后门、间谍软件、窃听软件、流氓软件、网络钓鱼、僵尸网络、逻辑炸弹、恶意脚本等
5	网络攻击	利用工具和技术，通过网络对系统进行攻击和入侵，包括网络探测、信息采集、嗅探、漏洞探测、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏、口令攻击、密码分析、拒绝服务等
6	物理破坏	系统/网络被非法用户进行物
7	系统故障	软硬件故障或环境原因导致业务中断
8	通信中断	通信意外故障造成传输中断
9	社会工程	非法用户通过社交手段获得系统/网络有关保密信息
10	管理不到位	系统/设备的管理不到位、使用不规范等

（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：

① 以往安全事件报告中出现过的威胁及其频率统计；

② 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；

③ 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。

（3） 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）。

2.4.3 脆弱性识别

（1） 脆弱性识别的内容，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。

① 脆弱性识别的数据应来自于船东/船公司/供应商，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。

② 脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、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。参见表附录 1-2.3.3。

脆弱性识别内容 **表附录** 1-2.3.3

类型	识别对象	识别方面
技术脆弱性	物理设施	从 CBS 所处环境的保护、设备设施管理、便携式设备和移动介质等方面进行识别
	网络结构	从网络结构设计、边界保护、内外部访问控制策略、网络设备安全配置等方面进行识别
	系统软件	从补丁安装、物理保护、用户账户、口令策略、资源共享、事件审计、访问控制、系统配置、注册表加固、网络安全、系统管理等方面进行识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、数据完整性、通信、鉴别机制、密码保护等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别

（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，脆弱性严重程度越高。如，1～3 个等级（分别对应：低、中、高）。

2.4.4 已有安全措施识别

在识别脆弱性的同时，应对已采取安全措施的有效性进行识别确认。安全措施的确认将评估其有效性，即是否真正地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措施和保护性措施。

预防性措施可以降低威胁利用脆弱性导致安全事件发生的可能性，例如以下措施：

（1） 通过风险评估充分考虑 CBS 可能的漏洞、面临的威胁及网络事件潜在的影响；

（2） 对 CBS 与其他 CBS 的连接进行充分的分析、确定和记录；

（3） 对安装在 CBS 上的软件进行识别，并提供每个应用软件、操作系统和固件（如适用）的用途、名称、版本等证据；

（4） 为船员组织网络安全培训。

保护性措施可以减少因安全事件发生后对船舶或系统造成的影响，例如以下措施：

（1）CBS 位于受控访问区域；

（2）CBS 的物理接口对不可信/不安全的可移动设备不可用；

（3）制定 CBS 维护策略，其中 CBS 不与不可信网络建立永久或临时连接，或使用不可信/不安全的可移动设备；

（4）制定事件响应计划和恢复计划，包含船舶发生网络事件时如何处理 CBS 的说明。

2.5 风险分析

2.5.1 在完成资产识别、威胁识别、脆弱性识别，以及已有安全措施确认后，船东/船公司/供应商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。

2.5.2 船舶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；

（6） 风险计算原理范式如下：

$$\text{风险值} = R(A, T, V) = R(L(T, V), F(Ia, Va)) \quad (1)$$

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。

2.6 风险评价

2.6.1 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化处理。不同的等级分别代表系统资产风险严重程度的高低。等级数值越大，脆弱性严重程度越高。如，1～3 个等级（分别对应：低、中、高）。

2.6.2 应根据所采用的计算方法，计算系统资产面临的风险值，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。见表附录 1-2.5.2。

风险等级 **表附录 1-2.5.2**

等级	标识	描述
3	高	风险高。系统、数据不可用，严重影响安全操作，对船舶运营造成重大影响
2	中	风险适中。未经授权访问船舶网络、系统、数据和其他资源，影响船舶日常运营，但影响面和影响程度不大

等级	标识	描述
1	低	风险低。对系统、数据的可用性造成影响较小，通过简单的措施可弥补或有替代措施

2.7 风险处置措施

2.7.1 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。安全措施的选择应从管理与技术两个方面考虑。当一方面的安全措施不足以达到可接受的残余风险水平时，船东/船公司/供应商应采取管理和技术二方面相结合的措施。

2.7.2 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，经批准后则纳入应急计划，并定期开展演练。

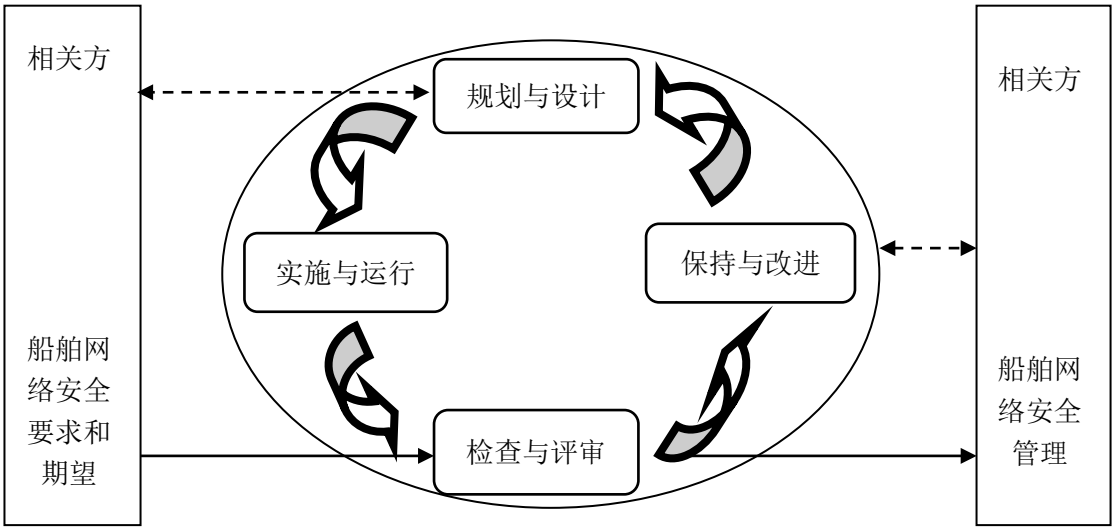
附录2　船舶网络安全管理

第1节　一般规定

1.1 一般要求

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。

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，如图附录 2-1.1.2 所示。



图附录 2-1.1.2 网络安全风险管理制度体系

第2节　管理制度

2.1 制度与文件

2.1.1　应包含安全运维管理的内容，包括但不限于本附录第 4 节和第 5 节所列各适用的管理活动。如适用时，尚应包含安全建设管理的内容，包括但不限于本附录第 6 节所列各适用的管理活动。

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。

2.1.3　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。

2.1.4　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。

2.1.5　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。

2.1.6　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 制定与发布

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　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。

2.3 审核与改进

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。

2.3.2　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。

2.3.3　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

3.1 机构与岗位

3.1.1　网络建设方和/或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。

3.1.2　决策层一般为指导和管理网络安全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。

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。

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。

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。

3.2 授权与审批

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。

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。

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。

3.3 沟通与合作

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。

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。

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。

3.3.4 密切关注主管机关、CCS 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

4.1 人员管理

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。

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。

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。

4.2 风险管理

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。

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网络安全事件时；
（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。

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。

4.2.4 运维期间的网络安全风险评估应包含技术检测。

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）。

4.3 安全检查

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。

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。

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。

4.4 变更管理

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。

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。

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。

4.5 事件与应急管理

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。

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。

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。

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

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。

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。

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。

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。

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。

4.6 备份与恢复管理

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。

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。

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。

4.7 服务供应商管理

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。

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需履行的网络安全相关义务。

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。

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。

4.7.5 对外包运维服务商，尚应符合下列要求：

（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。

4.8 密码管理

4.8.1 应遵循密码相关要求。

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。

4.9 保密管理

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。

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。

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 运维管理补充要求

5.1 环境管理

5.1.1 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。

5.1.2 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。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.1.6 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。

5.1.7 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。

5.1.8 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）。

5.2 资产管理

5.2.1 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。

5.2.2 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。

5.2.3 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。

5.3 介质管理

5.3.1 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。

5.3.2 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。

5.3.3 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。

5.3.4 介质报废时，应按照正式程序进行可靠的、安全的处置。

5.4 设备管理

5.4.1 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。

5.4.2 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。

5.4.3 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。

5.4.4 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。

5.4.5 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。

5.4.6 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。

5.4.7 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。

5.5 网络和应用系统安全管理

5.5.1 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。

5.5.2 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。

5.5.3 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。

5.5.4 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。

5.5.5 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。

5.5.6 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。

5.5.7 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。

5.6 云计算管理

5.6.1 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。

5.6.2 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。

5.6.3 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。

5.6.4 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。

5.7 移动互联管理

5.7.1 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。

5.8 物联网管理

5.8.1 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。

5.8.2 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。

5.8.3 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。

5.9 大数据管理

5.9.1 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。

5.9.2 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。

5.9.3 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。

5.9.4 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6节 建设管理补充要求

6.1 确定需求

6.1.1 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。

6.1.2 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。

6.1.3 所确定的安全需求和目标应经过船东同意。

6.2 规划设计

6.2.1 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。

6.2.2 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。

6.2.3 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。

6.3 工程实施

6.3.1 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。

6.3.2 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。

6.3.3 应通过第三方工程监理控制项目的实施过程。

6.4 产品采购和使用

6.4.1 应确保网络安全产品采购和使用符合有关规定。

6.4.2 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。

6.4.3 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。

6.5 软件开发

6.5.1 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。

6.5.2 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。

6.5.3 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。

6.5.4 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。

6.5.5 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。

6.5.6 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。

6.5.7 自行开发的，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。

6.5.8 外包开发的，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。

6.6 测试验收

6.6.1 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。

6.6.2 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。

6.6.3 应谨慎选择测试数据，并加以保护和控制。

6.7 系统交付

6.7.1 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。

6.7.2 应对负责运行维护的技术人员进行相应的技能培训。

6.7.3 应提供建设过程文档和运行维护文档。

6.8 云服务商管理

6.8.1 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。

6.8.2 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。

6.8.3 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。

6.8.4 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。

6.8.5 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。

6.8.6 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。

6.8.7 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。

6.9 移动互联管理

6.9.1 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。

6.9.2 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。

6.9.3 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。

6.9.4 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。

6.10 大数据管理

6.10.1 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。

6.10.2 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。

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。