



指导性文件
GUIDANCE NOTES
GD14-2024

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	2
第 1 节	一般规定	2
第 2 节	术语及规范引用	4
第 3 节	船舶网络安全分级及附加标志	9
第 4 节	免除申请	10
第 2 章	产品网络安全要求	11
第 1 节	一般规定	11
第 2 节	产品网络安全分级	12
第 3 节	系统要求	12
第 4 节	安全开发周期要求	23
第 3 章	产品检验/评估	26
第 1 节	一般规定	26
第 2 节	测试验证	29
第 4 章	船舶网络安全要求	31
第 1 节	一般规定	31
第 2 节	M 标志要求	31
第 3 节	P 标志和 S 标志要求	33
第 5 章	船舶网络安全检验	46
第 1 节	一般规定	46
第 2 节	初次入级检验	49
第 3 节	建造后检验	50
附录 1	船舶 CBS 风险评估	52
附录 2	船舶网络安全管理	60

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 1.1.1.3-1.1.1.5 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 1.1.3.1 中流程进行。

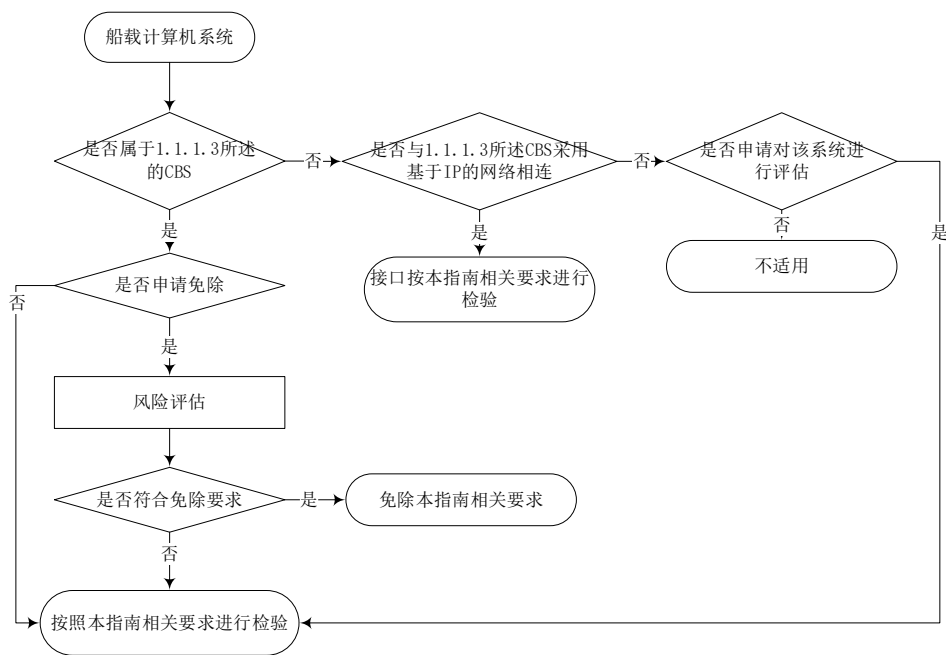


图 1.1.3.11 CBS 安全检验/评估判定流程

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。

1.2.1.28 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 操作系统（**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

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。

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。

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 4 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~SL4）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	√*	<u>√*</u>	√	√	√

(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、报告和防止未经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。	√*	<u>√*</u>	√	√	√
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	√*	<u>√*</u>	<u>√*</u>	√	√
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 RE2	应能防止任何通过控制系统边界的通信（也称为孤岛模式）				√	√
SR5.2	当边界保护机制发生操作故障(也称为故障关闭)时，				√	√

RE3	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，防止未经授权使用			√	√	√
NDR2.13	应能主动监测网络设备的诊断和测试接口，并生成通过				√	√

RE1	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和完整性。

（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 ¹⁾
6	安全开发生命周期	Ⓐ ¹⁾
7	维护和验证计划	① ¹⁾
8	支持网络事件响应及恢复计划的信息	① ¹⁾
9	变更管理计划	① ¹⁾
10	配置核查报告	① ²⁾

符号说明：

X: 适用

Ⓐ: 提交 CCS 批准；

①: 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经授权访问保护措施。
- (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 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，禁用或限制非必要功能、端口、协议、服务、默认共享等	√	√	√	√	√

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/385042220323011301>