指导性文件
GUIDANCE NOTES
GD17-2023

中　国　船　级　社

船舶网络安全指南

2023

2023 年 5 月 1 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 本指南适用于申请中国船级社（China Classification Society, CCS）船舶网络安全附加标志的船舶及网络安全评估的船载计算机系统（Computer Based System, CBS），海上设施可参照执行。

1.1.1.2 本指南给出了船舶及船载计算机系统的网络安全要求。

1.1.1.3 本指南安全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/或环境造成危害的船载 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） 货物管理系统（限于安全相关部分）；

（7） 舱底水和压载水系统，压/排载控制系统，装载计算机系统；

（8） 锅炉控制系统；

（9） 洗涤塔控制系统和其他需要符合船级社或国际防污染公约相关要求的系统；

（10） 水密完整性和进水探测系统；

（11） 照明（如应急照明，低位照明等）和航行信号系统；

（12） 任何其他中断或功能受损可能会对船舶运行造成风险的操控系统(Operation Technology System, OT 系统)；

（13） 与（1）-（12）采用网际互连协议（Internet Protocol, IP）连接的系统，其接口在本指南网络安全要求适用范围内，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）。

1.1.1.4 与 1.1.1.3（1）-（12）处于同一安全区域的其它系统应满足本指南网络安全要求。

1.1.1.5 对于航行和无线电系统，可采用 IEC 61162-460 或 IEC 63154 标准可以作为本指南的替代，其采用的安全标准应不低于本指南要求。

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网络安全要求。

1.1.1.7 本指南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，包括计算、安全、存储、通信及网络等设备。

1.1.2 安全基本要求

1.1.2.1 本指南适用的 CBS 应满足本指南第 2 章适用要求。

1.1.2.2 申请本指南相关附加标志的船舶应满足本指南第 3 章要求，所包含在 1.1.1.3 范围内的 CBS，还应满足本指南第 2 章适用要求。

1.1.2.3 判定船舶网络中 CBS 是否满足本指南相关要求，可按图 1.1.2.3 中流程进行。

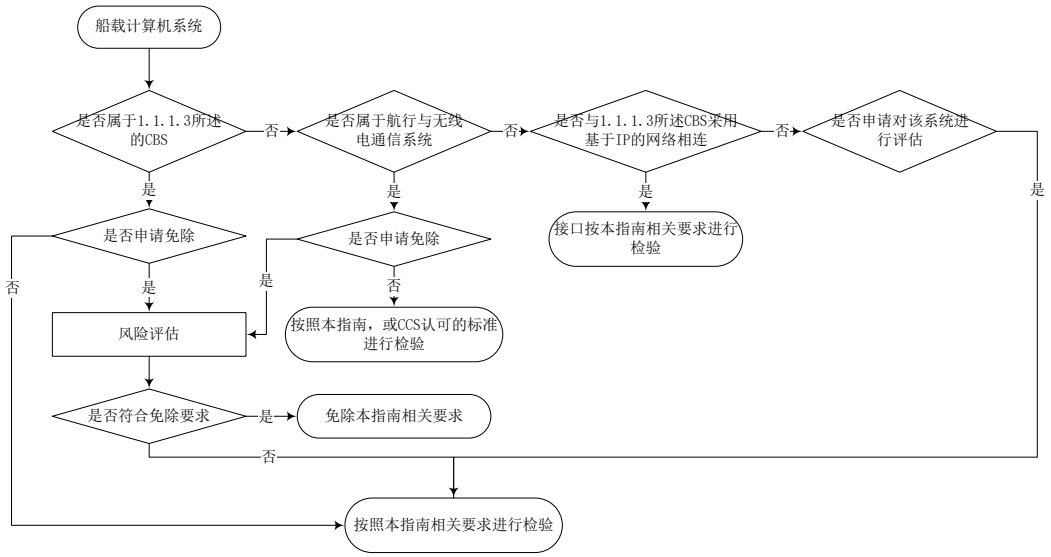


图 1.1.2.3 CBS 安全检验/评估判定流程

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 资产管理（**Asset Management**）：对任意数据，计算机或设备的控制。

1.2.1.3 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织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。

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

1.2.1.5 授权（**Authorization**）：防止未授权用户访问或使用系统，即规定了用户对数据的访问权限。

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

1.2.1.7 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的解决方案。

1.2.1.8 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。

1.2.1.9 计算机网络（**Computer 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。

1.2.1.10 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。

1.2.1.11 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型式的攻击性操作。

1.2.1.12 网络事件（**Cyber Incident**）：由恶意威胁者违反安全策略导致的影响系统完整性、可用性和/或保密性的行为或事件。

1.2.1.13 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。

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

1.2.1.15 缺陷（**Defect**）：非预期的软件功能。

1.2.1.16 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。

1.2.1.17 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。

1.2.1.18 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。

1.2.1.19 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。

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

1.2.1.21 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。

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

1.2.1.23 信息安全（**Information Security**）：针对信息的安保措施，防止对其未经授权

的访问，关闭，修改或销毁。

1.2.1.24 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。

1.2.1.25 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。

1.2.1.26 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。

1.2.1.27 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。

1.2.1.28 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]。

1.2.1.29 网段（**Network Segment**）：本指南中，网段是指 Layer-2 以太网段（一个广播域）[②]。

1.2.1.30 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。

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

1.2.1.32 网络拓扑结构（**Network Topology**）：用传输介质互连各种设备的物理布局。

1.2.1.33 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。

1.2.1.34 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。

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

1.2.1.36 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。操控技术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。

1.2.1.37 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。

1.2.1.38 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 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 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。

1.2.1.39 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。

1.2.1.40 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。

1.2.1.41 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。

1.2.1.42 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。

1.2.1.43 路由器（**Router**）：一种用于建立通过一个或不止一个计算机网络的路径的功能单元，例如从卫星通信网络将数据转至船用计算机网络。

1.2.1.44 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。

1.2.1.45 船舶设计方/船厂（**Ship Designer/Shipyard**）：实施将船东提供的船舶规格演变为完整船舶的过程，包括概念、合同和详细设计的管理。负责船舶建造，并负责在船舶建造过程中满足适用规章制度的要求和实施船舶设计规范。同时，负责将供应商提供的系统和产品集成为一个集成系统。

1.2.1.46 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。

1.2.1.47 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。

1.2.1.48 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。

1.2.1.49 系统类别（**System Category**）：在 IACS UR E22 中定义的基于其对系统功能的影响划分的系统类别，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 2.6.3。

1.2.1.50 系统集成商（**System 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。

1.2.1.51 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。

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

1.2.1.53 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。

1.2.1.54 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。

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

1.2.2 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。

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

第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	最低网络防御能力
2	SL1	抵御偶发的网络事件
3	SL2	抵御利用少量资源发起的网络事件
4	SL3	抵御利用丰富资源发起的网络事件
5	SL4	抵御有组织有目的的网络事件

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要求，S表示满足船舶较高的网络安全要求。

（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，CBS 应不低于第 4 章 第 3 节 SL0 对应的要求；

（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。

船舶网络安全附加标志与网络韧性等级对应关系 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	SL0
S		SL1	SL1
		SL2	SL2
		SL3	SL3
		SL4	SL4

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船级社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，应向 CCS 提出申请。

（1） 申请免除的 CBS 应按 1.4.2 所列要求开展，并满足 1.4.3 网络风险控制要求，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、逻辑访问限制等内容），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。

1.4.3 CBS 网络风险控制要求

1.4.3.1 当 CBS 满足以下全部条件时，可以免除网络安全相关要求:

（1） 网络安全风险评估已充分考虑 CBS 可能的漏洞、面临的威胁及网络事件潜在的影响；

（2） 考虑到 CBS 的复杂性、连接性、物理和逻辑接入点（包括无线接入点）等因素，CBS 的攻击面已最小化；

（3） CBS 的功能和作用不应受其他 CBS 或网络设备网络事件的影响，也不能将网络事件的影响传播给其他 CBS 或网络设备；

（4） CBS 不提供关键服务或多船服务；

（5） CBS 位于受控访问区域；

（6） 对 CBS 与其他 CBS 的连接进行充分的分析、确定和记录。尤其，CBS 不得通过基于 IP 网络连接到其他 CBS 或设备；

（7） CBS 的物理接口应对不可信/不安全的可移动设备不可用；

（8） 应对安装在 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、提供者和维护者的证据；

（9） CBS 应制定维护策略，其中 CBS 不应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;

（10） CBS 提供随时检查其功能完整性和服务质量的方法，包括检查硬件和软件完整性；

（11） CBS 应提供合适的接口，允许本地手动控制，此类接口不会扩大其攻击面（另请参见（2）点）；

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

1.4.4 免除批准

1.4.4.1 提供按照 1.4.2 所列要求开展，满足 1.4.3 网络风险控制要求的 CBS 网络风险评估报告。

1.4.4.2 当不能满足 1.4.3.1 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 当网络风险评估能够证明不会影响操作安全时，CCS 可接受其免除，其 CBS

网络风险评估报告需经 CCS 审图验船师批准。

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 产品的网络安全要求应按本章要求执行，包括但不限于：

（1） 本指南 1.1.1.3 包含的 CBS；

（2） CCS 认为必要的网络设备；

（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、云设备等，满足的最低要求应根据所在系统级别而定，网络设备还应满足本指南 2.3.2 的附加要求。

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、集线器、网桥等）、网络路由设备（路由器等）、网络安全设备（防火墙、网关、入侵检测设备、安全审计设备、加解密设备等）、网络接入设备（网络接口卡、无线接入点等）等。其中影响 CBS 基本功能或船舶航行安全的网络设备应进行认可。这些网络设备也可与 CBS 系统一起进行认可。

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

2.1.1.6 对于航行和无线电系统，IEC 61162-460 可以作为 SL0 的替代，但在应用这些标准时应确保产品具备与 SL0 要求的同等或更高的网络韧性。

2.1.2 基本安全要求

2.1.2.1 安全措施不应影响重要系统功能（影响健康、安全、环境和设备可用性的功能），除非经过了风险评估。

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“高于和超出”其他要求（而不仅仅是符合其他要求）；

（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。

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 最低韧性要求（UR E27）
2	SL 1		抵御偶发的网络事件
3	SL 2		抵御利用少量资源发起的网络事件
4	SL 3		抵御利用丰富资源发起的网络事件
5	SL 4		抵御有组织有目的的网络事件

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	√*①	√②	√	√	√
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） 帐户管理

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帐户的能力，包括添加、激活、修改、禁用和删除	√	√	√	√	√

① √表示适用。

√*表示与不可信网络连接时适用。

②√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 RE1	CBS 应支持统一帐户管理的能力				√	√

（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帐户，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	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
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 Java 脚本、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） 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。 单条审计记录应包括时间戳、来源(发端设备、软件进程或人员用户帐号)、类别、类型、事件 ID 和事件结果	√	√	√	√	√
SR2.8 RE1	CBS 应能集中管理审计事件，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） 审计存储容量

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。管理制度应提供审计机制，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	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	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	√	√	√	√	√
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、密钥大小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 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	应在 DoS 事件期间以降级模式操作	√	√	√	√	√
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				√	√

（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	应能对事件进行比较分析以发现违规、异常等行为			√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
RE1						
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　程序要求

2.4.1.1 系统/设备的开发应遵循安全开发生命周期流程，在各阶段（包括需求分析、设计、实施、验证、发布、维护、退役等）中考虑网络安全因素。

2.4.1.2 供应商应制定程序和技术控制措施，建立质量保证（QA）流程，以确保：

（1） 保护用于代码签名的私钥免受未授权的访问或修改；

（2） 在发布前测试更新的安全性；

（3） 应记录各阶段发生并处理的安全问题；

（4） 向用户提供产品安全更新的相关信息，产品安全更新的信息一般包括：

① 应用安全补丁的产品版本号；

② 关于如何手动和通过自动化流程安装已批准补丁的说明；

③ 明确将补丁应用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 安装未批准或非资产所有者部署的补丁可能导致的风险。

（5） 为用户提供产品依赖的组件或操作系统安全更新的文件，包括但不限于说明产品是否与依赖的组件或操作系统安全更新兼容；

（6） 用户能验证其适用产品及版本安全更新的真实性；

（7） 制定文档系统描述其网络纵深防御等安全策略、各网络安全产品在安全防御策略中的作用、安全防御策略所应对的威胁，以及针对产品相关的已知安全风险的缓解措施，包括遗留代码相关的风险；

（8） 制定文档描述产品预期由其他设备或系统提供的安全防御措施；

（9） 制定进行产品安全加固的指导文件，并包括对以下方面的说明和建议：

① 产品的集成说明，包括第三方组件的集成；

② 产品与用户应用程序的 API 接口/协议；

③ 实施和维护安全防御策略；

④ 配置和使用支持本地安全策略的选项/功能，以及每个安全选项/功能的说明；

a) 对产品纵深防御策略的作用；

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。

（10） 制定支持产品管理、监控、事件处理和安全评估的安全工具的使用说明和建议；

（11） 定期安全维护说明和建议；

（12） 向供应商报告产品安全事件的说明；

（13） 产品维护和管理的安全最佳实践说明。

第3章　产品检验/评估

第1节　一般规定

3.1.1 检验/评估流程

3.1.1.1 本指南适用的 CBS，其网络安全要求应按照 3.1.2 提交产品网络安全相关的图纸资料及试验资料，并按照本章第 2 节 要求进行测试验证。

3.1.1.2 当产品的网络安全测试验证是产品检验/认可的工作环节时，验证结果可作为产品认可/检验环节的部分成果。

3.1.1.3 对于单独申请网络安全评估的产品，应按照 3.1.2 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，可向其签发附录 3 产品网络安全评估报告。

3.1.1.4 当产品已具有产品型式认可证书，且证明其满足安全开发生命周期，则可按如下要求提交简化的图纸和试验资料：

（1） 系统说明书（含资产清单）；

（2） 网络系统拓扑图；

（3） 测试报告，证明其已进行安全设计、开发、建造、配置和测试，必要时 CCS 可按照本章第 2 节 要求进行验证；

（4） 型式认可证书，证明其满足相关安全能力要求。

3.1.2 图纸资料及试验资料

3.1.2.1 应按表 3.1.2.1 提交图纸资料批准或备查。

图纸资料汇总表　　表 3.1.2.1

序号	需要提交的文件	备注
1	系统/设备说明书	Ⓐ
2	软件说明书	Ⓐ
3	网络系统拓扑图	Ⓐ
4	系统/设备配置文件	Ⓐ
5	操作手册	Ⓐ
6	脆弱性分析文档	Ⓘ
7	安全开发生命周期文档	Ⓐ
8	产品网络安全试验大纲	Ⓐ
9	产品维护计划	Ⓐ
10	产品网络事件响应及恢复计划	Ⓐ
11	变更管理计划	Ⓐ
12	产品网络安全试验报告	Ⓦ

符号说明：
Ⓐ提交 CCS 批准；
Ⓘ提交 CCS 备查；
Ⓦ需 CCS 产品验船师见证。

3.1.2.2 提交文件的具体要求如下：

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

① 产品应满足船用环境条件；

② 系统/设备资产清单：

a) 硬件资产清单包括系统的硬件组成（含计算机、网络设备、存储设备、智能终端设备等），并描述其对应的功能、技术特征（品牌、制造商、型号、主要技术数据）、类别、接口（串口、网口）等信息；

b) 软件资产清单包括操作系统/固件、操作系统提供和管理的网络服务、应用软件、数据库、配置文件，并描述其对应的版本信息（包括补丁版本）、许可信息（含有效日期）及更新日志、维护策略（如本地与远程、定期与临时等）和责任人、基于角色和职责等的访问控制策略（例如读、写和执行权限）。

③ 明确系统所有输入输出接口形式；

④ 冗余设置及转换机制详细说明（如有时）；

⑤ 数据安全措施、用户访问控制的详细说明。

（2） 软件说明，至少应包括下列内容的适用部分：

① 安装的软件列表和版本号，许可证有效期和更新日志等；

② 对于每一硬件单元中安装的基本软件的描述；

③ 数据需求，保持软件运行的数据，与其他系统交互的数据；

④ 冗余系统间的切换机制（如有时）。

（3） 系统网络拓扑图，采用物理和逻辑拓扑结构描述网络流或数据流（源、目标、协议、协议细节、物理实现），并包含设备名称、IP、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。

（4） 系统/设备配置文件，应针对每个适用的安全要求给出推荐的配置，并包含以下适用内容：

① 网络数据流量限定值；

② 设备开放的端口；

③ 用户访问权限配置清单；

④ 系统对限制访问地址的设定，如系统白名单；

⑤ 远程用户访问权限（适用时）；

⑥ 配置文件存储及备份的方式；

⑦ 系统配置文件免受未授权访问保护措施。

（5） 操作手册（包括故障处理说明），应包含以下适用内容：

① 涉及系统启动、功能恢复、维护和定期试验、数据安全性及数据备份、用户权限配置、系统重置及恢复、故障定位和修理、系统更新、以及其他用户需注意的事项等方面的使用说明；

② 使系统满足预期安全要求所必须的相关使用程序和说明；

③ 软件维护和使用说明（含软件和硬件变更管理的必要程序）。

（6） 脆弱性分析文档，至少包括对产品涉及网络安全要素（如所有提交评估的文档和产品本身等）进行分析，说明在预期使用环境中产品是否存在明显可利用的脆弱性。如果有，应列出所有存在的明显脆弱性及可利用方式，并需明确说明该脆弱性风险可控及补偿措施。

（7） 安全开发生命周期文档，至少包括本章第 2.4.1.2 条要求的内容；

（8） 产品网络安全试验大纲，至少包含如下内容：

① 测试装置；

② 测试项目，包含第 2 章 第 1 节 和第 3 节的适用要求；

③ 初始条件

④ 测试方法；

⑤ 结果评估衡准；

⑥ 参照标准。

（9） 产品维护计划，至少包括：

① 维护内容；

② 维护方式；

③ 维护周期。

（10） 产品网络事件响应及恢复计划，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。

（11） 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。

（12） 产品网络安全试验报告，依据产品网络安全试验大纲，验船师应现场见证测试的执行，审核试验报告。

第2节 测试验证

3.2.1 一般要求

3.2.1.1 应根据产品的目标运行区域的安全级别，确定系统及组件应满足的安全级别，并按 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 试验项目应涵盖目标安全级别所适用的要求，对于船舶网络防火墙还应按照CCS《船舶网络防火墙检验指南》执行。

3.2.1.3 系统/设备的试验应至少进行安全漏洞扫描或渗透测试、负载或压力测试、网络连接测试。

3.2.1.4 网络设备试验应至少进行安全漏洞扫描或渗透测试、网络风暴测试、负载或压力测试、性能测试（如最大连接数、最大并发数等）。

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 也可要求其提供必要的图纸、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 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 压力测试

（1） 通过技术手段，对产品进行压力测试，并将结果作为测试验证的结论之一；

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

（3） 压力测试完成后，申请方应提供测试报告供 CCS 验证。

3.2.2.5 负载测试

（1） 通过技术手段，对产品进行负载测试，并将结果作为测试验证的结论之一；

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

（3） 负载测试完成后，申请方应提供测试报告供 CCS 验证。

3.2.2.6 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。

3.2.2.7 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） 确认网络监控设备的监控功能应在网络系统中正常运行，具体如下：

① 显示物理架构图的功能；

② 报警功能；

③ 日志功能；

④ 流量显示；

⑤ 设置配置功能；

⑥ 故障恢复支持功能。

（3） 测试完成后，申请方应提供测试报告供 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、网络架构、安全区域、边界防护、网络冗余、通信安全、恶意代码防范、入侵防范、身份鉴别、访问控制、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	事件恢复

4.3.2 资产清单

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.2.1	应对资产进行管理，对资产进行分类和标识，并对资产的使用、物理传输、存储、保护、处置等制定规范化要求	√	√	√	√	√
4.3.2.2	应提供本指南适用范围内各系统完整清单汇总，并在	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	船舶全生命周期内保持最新： ① 资产清单应包含船舶适用的所有 CBS，以及支撑其稳定安全可靠运行的网络、服务、计算、存储等设备； ② 每个 CBS 及设备还应具有满足 3.1.2.2（1）②所要求的详细清单； ③ 资产清单中应包含 CBS 及设备其物理位置、功能、IP 地址、所属安全区域（如有时）进行描述					

4.3.3 资产保护

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.3.1	应根据资产类别或制造商的建议对资产进行保护，如提供必要的访问控制手段，以防止数据在存储、处理和传输过程中遭受未授权访问、误用和/或损坏			√	√	√
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工业界认可的加密算法进行加密				√	√

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、软件进程和设备根据其职责或预期功能需要来访问	√	√	√	√	√
4.3.5.2	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 进行安装、集成、维护、维修、更换、处置等操作的各相关方进入，以免妨碍船舶的有效和高效运行	√	√	√	√	√
4.3.5.3	应限制主管当局、技术人员、代理、港口和码头官员	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	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	船载网络的接入点除非在监督下或根据文件规定的程序(如维护)进行连接，否则应采用物理和/或逻辑隔离	√	√	√	√	√
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或其他网络(如访客专用接入网络或访客娱乐活动专用网络)隔离的独立计算机	√	√	√	√	√
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 网络架构

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.6.1	船舶网络架构设计应确保船舶网络具有韧性，即由于网络设备故障或网络事件导致的船舶网络某一部分故障，不应影响其他连接到该网络的系统	√	√	√	√	√
4.3.6.2	船舶网络设计应按照“最小功能”原则，即只提供必要的功能，限制非必要功能的使用，禁用不必要的功能、端口、协议、服务、默认共享等	√	√	√	√	√

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同安全要求，安全区域的网络应在逻辑上或物理上与其他区域或网络进行隔离	√	√	√	√	√
4.3.7.2	应根据系统类型（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 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	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	用要求； ② 属于安全系统的 CBS 应归入单独的安全区域； ③ 无线设备应归入单独的安全区域； ④ 航行和通信系统不得与机械、货物系统处于同一安全区域； ⑤ 本指南适用范围之外的 CBS 应与本指南所要求的安全区域进行物理分隔。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； ⑥ 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； ⑦ 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					
4.3.7.3	一个安全区域内的 CBS 不应依赖于其他安全区域的网络通信、应用或服务	√	√	√	√	√
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	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下，除允许外，受控接口拒绝所有通信	√	√	√	√	√
4.3.8.3	任何连接安全区域和不可信网络间的设备（如防火墙）应： ① 保护安全区域内的网络不发生数据流量过高和其他可能影响网络资源服务质量的事件； ② 防止安全区域内的网络从 CBS 以外的用户或系统接收社交媒介、邮件通信信息	√	√	√	√	√
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		√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
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或限制			√	√	√
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或限制				√	√
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	网络设计应包括限制数据流量的方法，以通过满足预期最高的数据流，并将拒绝服务（DoS）和网络风暴/高流量的风险降至最低	√	√	√	√	√
4.3.10.2	数据流量的计算应至少考虑网络容量、预期应用的数据速度要求和数据格式	√	√	√	√	√
4.3.10.3	CBS 应能够为高优先级进程优先分配系统资源		√	√	√	√
4.3.10.4	船舶网络应能够为高优先级 CBS 优先分配网络资源		√	√	√	√
4.3.10.5	船舶网络应能够在受到 DoS 攻击期间以降级模式运行，并发出报警			√	√	√
4.3.10.6	应采用校验技术或密码技术保证通信过程中数据的完整性				√	√
4.3.10.7	当数据的完整性遭到破坏时，应自动通知责任船员				√	√
4.3.10.8	若船岸通信涉及控制指令或与船舶安全相关的数据交换，应选用专用通道或采用加密认证技术实现身份认证、访问控制和数据加密传输				√	√
4.3.10.9	为保护关键数据而使用密码技术时，应基于安全需求考虑对系统性能和系统故障恢复能力的潜在影响				√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.10.10	若使用加密技术，则应 ① 按照行业最佳实践执行； ② 加密方案中应说明使用的算法、协议和密钥（包含密钥强度、到期日期）以及密钥使用情况				√	√
4.3.10.11	应采用密码技术保证通信过程中数据的保密性					√

4.3.11 恶意代码防范

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.11.1	应对本指南适用的 CBS 进行恶意软件（如病毒、蠕虫、木马、间谍软件）防护	√	√	√	√	√
4.3.11.2	具有标准操作系统的 CBS 可使用工业标准防恶意软件，操作系统应保持最新状态，并安装、定期维护防恶意软件，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）	√	√	√	√	√
4.3.11.3	对于无法安装防恶意软件的系统，应采用单独安全区域、操作程序、物理保障措施或厂商推荐的方式进行防护	√	√	√	√	√
4.3.11.4	应在关键网络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		√	√	√	√
4.3.11.5	系统应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库		√	√	√	√
4.3.11.6	应在关键网络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				√	√
4.3.11.7	系统应采用免受恶意代码攻击的技术措施，及时识别入侵和病毒行为，并将其有效阻断				√	√
4.3.11.8	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					√

4.3.12 入侵防范

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.12.1	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		√	√	√	√
4.3.12.2	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		√	√	√	√
4.3.12.3	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		√	√	√	√
4.3.12.4	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			√	√	√

4.3.13 身份鉴别

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.13.1	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	√	√	√	√	√
4.3.13.2	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	√	√	√	√	√
4.3.13.3	当远程访问和维护时，应采取必要措施防止鉴别信息在网络传输过程中被窃听	√	√	√	√	√
4.3.13.4	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					√

4.3.14 访问控制

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.14.1	应根据船舶和岸基人员的角色和责任分配登录帐户，限制激活的时期，不再需要时予以注销	√	√	√	√	√
4.3.14.2	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来防护	√	√	√	√	√
4.3.14.3	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	√	√	√	√	√
4.3.14.4	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船员。当不需要时，管理员权限应删除。在任何情况下，管理员权限的使用应始终限于功能需要	√	√	√	√	√
4.3.14.5	所有新帐户或进程的默认权限配置应尽可能低。在必要时允许提升权限，如使用有限期权限或一次性使用凭证。应避免权限随着时间而积累，如定期对用户和进程帐户进行审计	√	√	√	√	√
4.3.14.6	应重命名或删除默认帐户，修改默认帐户的默认口令		√	√	√	√
4.3.14.7	应及时删除或停用多余的、过期的帐户，避免共享帐户的存在		√	√	√	√

4.3.15 远程访问

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.15.1	与或通过不可信网络通信，CBS 应满足指南第 2 章第 3 节所有与不可信网络相关的要求	√	√	√	√	√
4.3.15.2	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	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.15.3	不应将任何船载 CBS 的 IP 地址暴露给不可信网络	√	√	√	√	√
4.3.15.4	不应将数据包从不可信网络直接路由到安全区域	√	√	√	√	√
4.3.15.5	应通过具有端点认证能力的安全连接（如 VPN）与不可信网络进行通信	√	√	√	√	√
4.3.15.6	应保护远程访问会话和传输信息的完整性	√	√	√	√	√
4.3.15.7	应确保信息只被授权人员可读	√	√	√	√	√
4.3.15.8	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	√	√	√	√	√
4.3.15.9	应限制与船载 CBS 通信的源地址，避免陌生地址的攻击行为	√	√	√	√	√
4.3.15.10	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）	√	√	√	√	√
4.3.15.11	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： ① 应采用认证的加密虚拟专用网络（如 VPN）或专用通道进行通信； ② 在船端和远程控制端应明确显示操作控制权的位置； ③ 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； ④ 应优先传输控制信号		√	√	√	√

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 应制定支持计划，并提供给所有相关方； ⑤ 在远程维护期间，授权人员应能随时中断和中止，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；	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	⑦ 当访问尝试失败时，在预设时间内限制下一次尝试。当访问尝试次数达到预定值时，应阻止其继续认证； ⑧ 如果由于某种原因远程维护中断，将通过自动注销终止访问					

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、实施和维护中确保： ① 网络事件不传播到其他控制系统； ② 只有授权用户才能访问无线网络； ③ 只有授权进程和设备才能使用无线网络通信； ④ 在无线网络中传输的信息应保证保密性和完整性	√	√	√	√	√
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	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				√	√

4.3.18 移动介质安全

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.18.1	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	√	√	√	√	√
4.3.18.2	除 4.3.5.5 条中提到的独立计算机外，其他可物理访问的计算机和网络端口应禁止可移动介质的使用	√	√	√	√	√
4.3.18.3	应制定移动介质的使用策略，包括： ① 恶意代码扫描； ② 文件或数据扫描； ③ 软件合法性验证（通过数字签名或水印等）	√	√	√	√	√
4.3.18.4	用于船员操作或供应商维护的移动和便携式设备的连接端口，应采取措施防止预定设备以外的连接	√	√	√	√	√
4.3.18.5	已采用逻辑或物理阻塞的端口应有明确标识	√	√	√	√	√
4.3.18.6	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	√	√	√	√	√
4.3.18.7	应禁止便携式设备自动执行软件代码，手动执行软件代码应事先验证	√	√	√	√	√

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，包括通信链路故障和移动介质连接故障； 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	√	√	√	√	√
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 应该是被动而不是主动防护，主动防护可能影响 CBS 性能； ③ 相关人员应经过培训并适任 IDS	√	√	√	√	√

4.3.20 安全审计

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.20.1	应执行日志管理，根据需要分配存储空间，至少保留一个最小船舶检验周期		√	√	√	√
4.3.20.2	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		√	√	√	√
4.3.20.3	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息		√	√	√	√
4.3.20.4	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		√	√	√	√
4.3.20.5	系统应为授权用户提供审核日志的只读访问权限		√	√	√	√
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	应对审计进程进行保护，防止未授权的中断				√	√
4.3.20.9	若审计进程发生中断时，应提醒相关人员，以防止其他重要功能的丧失				√	√
4.3.20.10	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					√

编号	要求	SL0	SL1	SL2	SL3	SL4
	分析					
4.3.20.11	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	应制定船舶网络事件响应计划，包含相关突发事件及应对网络安全事件的措施	√	√	√	√	√
4.3.21.2	船舶的事件恢复计划应包含： ① 所有 CBS 以及支撑其稳定安全可靠运行的网络、服务、计算、存储等设备的事件响应计划，具体内容见 3.1.2.2（10）； ② 安全事件报告和处置规定，明确不同安全事件的报告、处置和响应流程，人员沟通方式、现场处理和事件报告责任人名单、外部技术支持联系人名单（如系统支持供应商、网络管理员)等	√	√	√	√	√
4.3.21.3	船厂应确保这些计划的准确性和有效性，并在交船时提供给船东	√	√	√	√	√
4.3.21.4	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最新	√	√	√	√	√
4.3.21.5	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	√	√	√	√	√
4.3.21.6	事件响应计划应在船舶营运期间保持更新	√	√	√	√	√
4.3.21.7	用于本地控制和监视的 CBS 应是独立的，不依赖与其他 CBS 的通信来实现预期运行	√	√	√	√	√
4.3.21.8	事件响应如需要网络隔离，则应满足： ① 应可以手动或自动终止与某个网段的通信； ② 应能根据程序物理隔离网段，例如，通过操作网络设备上的物理 ON/OFF 开关或类似动作，如断开路由器/防火墙的电缆。设备上应有说明和清晰标记，允许人员以有效的方式隔离网络； ③ 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； ② 脱离系统； ③ 将控制权限转移到其他系统或操作人员； ④ 将 CBS 输出或自身状态设定为预定值（断电、保持、固定值等）；	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
	⑤ 其他补偿措施; ⑥ 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					

4.3.22 事件恢复

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.22.1	应制定船舶网络事件恢复计划，以支持 CBS 因网络事件造成中断或故障后恢复到运行状态	√	√	√	√	√
4.3.22.2	船舶的事件恢复计划应包含： ① 所有 CBS 以及支撑其稳定安全可靠运行的网络、服务、计算、存储等设备的事件恢复计划，具体内容见 3.1.2.2（10）; ② 恢复程序、人员沟通方式、现场处理和事件报告责任人名单、外部技术支持联系人名单（如系统支持供应商、网络管理员)等	√	√	√	√	√
4.3.22.3	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	√	√	√	√	√
4.3.22.4	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。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	√	√	√	√	√
4.3.22.5	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，以及如何获得岸上援助，还应提供船上恢复所需的工具	√	√	√	√	√
4.3.22.6	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	√	√	√	√	√
4.3.22.7	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	√	√	√	√	√
4.3.22.8	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	√	√	√	√	√
4.3.22.9	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	√	√	√	√	√
4.3.22.10	应确保数据可从安全副本或介质中恢复	√	√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.22.11	应考虑使用离线备份来降低恶意软件对在线备份的影响	√	√	√	√	√
4.3.22.12	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映像（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	√	√	√	√	√

4.3.23 变更管理

编号	要求	SL0	SL1	SL2	SL3	SL4
4.3.23.1	应进行变更管理，按流程进行变更，变更记录应包含以下信息： ① 变更需求； ② 变更时间； ③ 变更的影响； ④ 变更前测试； ⑤ 变更后验证； ⑥ 中止变更并从失败变更中恢复的程序和方法； ⑦ 变更信息记录和传达		√	√	√	√

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）		√	√	√	√

编号	要求	SL0	SL1	SL2	SL3	SL4
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/S）附加标志的船舶。

5.1.1.2 本章规定的特别要求是对 CCS 入级船舶检验要求的补充。其检验可与 CCS 规范规定的相同类型检验，也就是初次入级、年度和特别检验同时进行。

5.1.2 图纸资料

5.1.2.1 申请船舶网络安全附加标志的船舶，应将下列图纸资料提交批准：

（1） 船舶网络风险管理相关体系文件；

（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 5.1.2.1 所示。

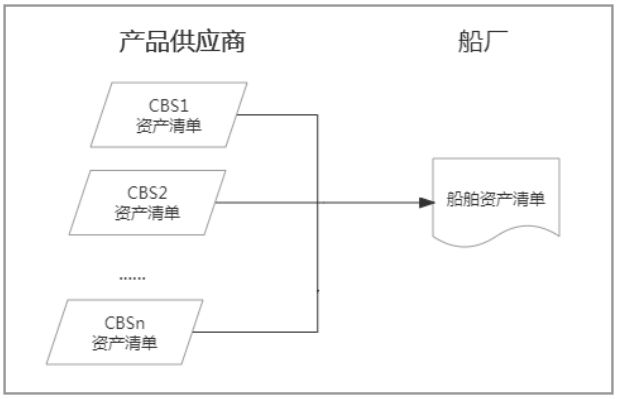


图 5.1.2.1 船舶资产清单

（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：

① 清晰标识安全区域和每个 CBS；

② 简述每个 CBS 的功能及其所属安全区域；

③ 描述相同安全区域内的 CBS 之间的通信目的和特征；

④ 描述不用安全区域内 CBS 之间的通信和特征,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）；

⑤ 描述安全区域内的 CBS 和其他不可信网络之间的通信和特征，包括离散信号、串行通信和基于 IP 的网络通信、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） 船舶网络安全设计方案，所有通过产品/系统来实现的安全要求，至少应包含以下内容：

① 区域划分原则和边界防护措施；

② 网络冗余（如适用）；

③ 通信量计算（含流量分配/控制策略）；

④ 完整性校验技术（如适用）；

⑤ 密码技术（如适用）；
⑥ 恶意软件防护机制，如防范的恶意代码类型、更新方法或替代措施；
⑦ 入侵防范；
⑧ 身份鉴别；
⑨ 访问控制策略，如 CBS 的物理位置和物理访问控制措施、无需进行识别和认证的、船员可用的接口、符合最小权限原则的逻辑访问控制措施；
⑩ 移动介质安全，如通过物理方式限制访问的任何物理接口端口的规定（例如端口阻断器或锁定机柜）；
⑪ 网络运行监测，说明网络风暴/过量流量发生时的探测、报警和响应措施，生成和存储安全事件记录的功能描述（至少包含登录活动、配置活动和物理设备的连接/断开连接）；
⑫ 无线通信，如无线网络的边界控制、防止用户和设备未经授权访问无线网络的策略；
⑬ 远程访问和维护方案（如适用）。

（5） 船舶网络事件响应计划；
（6） 船舶网络事件恢复计划；
（7） 备份计划；
（8） 系统变更记录（如适用）；
（9） 系统更新方案（如适用）；
（10） 免除网络要求的系统清单及其风险评估报告（如有时）；
（11） 资产管理规定，说明资产保护和处置程序；
（12） 船舶网络安全试验大纲，应明确试验的初始条件、试验方法、试验工具、验收标准。

5.1.2.2 申请船舶网络安全附加标志的船舶，必要时，应提供船舶产品的网络安全测试报告供现场验船师查阅。

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	船级社			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	船舶资产清单	Ⓐ			M, P, S
3	网络拓扑图	Ⓐ			M, P, S
4	船舶网络安全设计方案	Ⓐ			P, S
5	船舶网络事件响应计划		Ⓐ		P, S
6	船舶网络事件恢复计划		Ⓐ		P, S
7	备份计划		Ⓐ		
8	系统变更记录			Ⓐ	P, S
9	系统更新方案			Ⓐ	P, S

序号	图纸名称	船级社			适用附加标志
		船舶审图	建造中检验	建造后检验	
10	免除网络要求的系统清单及风险评估报告	Ⓐ			P, S
11	资产管理规定			Ⓐ	P, S
12	船舶网络安全试验大纲		Ⓐ		P, S

符号说明：
Ⓐ提交 CCS 批准。

第2节 初次入级检验

5.2.1 一般要求

5.2.1.1 本章所述的特别要求与授予船舶的附加标志密切相关。当船舶具有多个附加标志时，每个附加标志的特别要求均适用。

5.2.1.2 授予附加标志的设备和系统，如发生变更、损坏和故障等影响附加标志保持的情况，船东应及时通知 CCS，并申请临时检验。

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） 为进一步分析船舶网络管理状况，可要求船舶提交附录 5、附录 6 作为参考；

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

（1） 确认安装的 CBS 符合资产清单；

（2） 资产的管理规定，包括资产标识、资产保护、资产处置，确认资产管理规定满足本指南 4.3.3 和 4.3.4 条适用要求；

（3） 检查物理访问控制措施，确认 CBS 位于受控的区域，对物理安全设备，如电子门禁系统、监视摄像机、入侵检测器、电子锁等进行效用试验（如有）；

（4） 确认安全区域符合第 5 章第 1 节批准的网络拓扑图（如通过网络扫描）；

（5） 现场验船师应见证试验大纲中的所有试验，包括：

① 边界防护机制效用试验，确认安全区域边界只能通过明确允许的流量；

② 冗余试验；

③ 通信功能及安全验证（如“最小功能”原则、负载测试、网络风暴测试、加密技术等）；

④ 防恶意软件效用试验，确认已获批准的防恶意软件或其他补偿性措施是有效的（例如，通过使用可靠的防恶意软件测试文件进行测试）；

⑤ 入侵防范试验；

⑥ 身份鉴别试验；

⑦ 访问控制试验，确认用户帐户按照职责和最小特权隔离原则配置，以及临时帐户已被删除等；

⑧ 远程访问和远程维护功能试验；

⑨ 无线网络功能及安全试验；

⑩ 移动介质安全策略验证，如确认移动和便携式设备的使用仅限于授权用户、接口端口只能由特定的设备类型使用、这些设备上的文件将不会自动执行、文件不能从这些设备传输到系统、网络访问仅限于特定的 MAC 或 IP 地址、端口被禁用、端口被物理阻塞等；

⑪ 网络监测与功能验证试验；

⑫ 审计功能测试；

⑬ 事件响应与恢复计划验证，确认计划中的程序和说明是正确和有效，如本地独立控制、网络隔离、审计记录的使用、备份、恢复、受控关机、复位、回滚和重新启动等。

⑭ 设计方案中的补偿措施验证（如适用）。

5.2.3 授予附加标志/签发报告

5.2.3.1 检验/评估完成后，由 CCS 向申请方签发附录 4 船舶网络安全评估报告（船舶），为船舶授予相应等级的附加标志。

5.2.3.2 船上应永久存放船舶网络安全评估报告以备检查。

第3节 建造后检验

5.3.1 年度检验

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

（1） 网络系统总体运行情况；

（2） 网络系统维护情况记录；

（3） 网络系统中接入系统/设备的故障/失效情况和原因分析；

（4） 船员的网络安全培训情况记录。

5.3.1.2 年度检验应完成以下检验项目：

（1） 检查船舶网络运行日志，确认系统运行状况良好；

（2） 检查变更记录，确认所有变更不影响系统原有安全水平；

（3） 检查漏洞扫描报告，确认系统定期进行漏洞扫描；

（4） 检查系统安装更新记录，确认系统软件定期进行维护升级。

5.3.1.3 中间检验和特别检验项目同年度检验。

5.3.2 临时检验

5.3.2.1 当船舶网络系统发生下列情况时，船东/船舶管理公司应申请临时检验：

（1） 船舶网络拓扑结构发生变化；

（2） 新增指南适用的 CBS；

（3） 原批准的 CBS 硬件或软件发生变化；

（4） 网络设备配置发生变化；

（5） 其他可能影响附加标志保持的情况。

附录1　船舶 CBS 风险评估

第1节　一般规定

1.1 一般要求

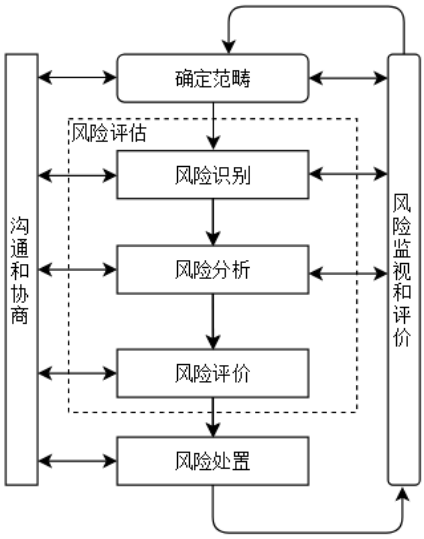
1.1.1　船东/船舶管理公司应根据船舶网络资产面临的威胁，以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对船舶造成的影响。

1.1.2　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　船舶系统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提高资产脆弱性被利用的难度，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 风险评估准备

2.3.1　风险评估准备，评估准备阶段应包括：

（1）　确定风险评估的目标；

（2） 确定风险评估的对象、范围和边界；
（3） 组建评估团队；
（4） 开展前期调研；
（5） 确定评估依据；
（6） 建立风险评价准则；
（7） 制定评估方案。

2.4 风险识别

2.4.1 资产识别

（1） 资产分类，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。船东/船舶管理公司提交图纸、资料、管理规程等，也可根据资产的表现形式，将资产分为 IT 设备、IT 系统、OT 系统等，详见表附录 1-2.4.1（1）。

资产分类示例 **表附录 1-2.4.1（1）**

资产类别	资产名称	示例说明
IT 设备资产	网络设备	路由器、网关、交换机、防火墙、AC 控制器、AP 发射器、CCTV 摄像头、IP 电话机、卫通服务器等网络通信与安全设备
	计算机	台式/便携工作计算机、服务器、CCTV 主机、配载仪、液位遥测终端、锅炉操控终端等船舶配备的 IT 计算机
IT 系统资产	操作系统和应用系统	操作系统、邮件系统、CCTV 系统、乘客或访客服务和管理系统、网络管理系统、船员福利系统、其他与 OT 相连接的系统
OT 系统资产	通信系统	卫星通信系统（SATCOM）、综合通信系统（ICS）、语音互联网协议（VOIP）
	推进、机械和动力控制系统	发动机调速器系统、燃油系统、报警监控系统、电源管理系统
	航行和无线电系统	电子海图显示和信息系统（ECDIS）、无线电探测和测距（RADAR）、自动识别系统（AIS）、全球定位系统（GPS）、动态定位系统（DPS）、全球海上遇险安全系统（GMDSS）、航行数据记录仪（VDR）和综合导航系统（INS）
	货物管理系统	货物控制系统、压载水系统（BWS）

说明：以上资产分类作为示例，供参考。

（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，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；

④ 资产重要性等级，根据船舶系统自身特点，选择资产保密性、完整性和可用性最为重要的一个属性作为资产的最终赋值，也可以根据资产保密性、完整性和可用性的不同等级及其赋值进行加权计算得到资产的最终赋值结果。最终资产赋值可以划分为不同级别。如，1～3 个等级（分别对应：低、中、高）。根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步风险评

估。

2.4.2 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。分类方法可参考《ISO/IEC 27005:2018 信息技术-安全技术-信息安全风险管理》。

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

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，针对每一项需要保护的资产识别出可能被威胁利用的弱点，并对弱点的严重程度进行评估。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/船舶管理公司，以及相关业务领域和硬件方面的专业人员。脆弱性识别采取的方法主要有：问卷调查，工具检测，人工核查，文档查阅，渗透性测试等。

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 1-2.4.3（1）。

脆弱性识别内容 **表附录 1-2.4.3（1）**

类型	识别对象	识别方面
技术脆弱性	物理环境	从物理位置选择、物理访问控制、安装要求、供配电、防潮防静电、电磁防护等方面进行识别。
	网络设备和结构	从网络结构设计、通信安全、边界保护、访问控制、网络隔离/分段、网络配置、网络元余等方面进行识别。
	主机系统	从身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、补丁安装、资源控制、系统配置、注册表加固、系统管理、等方面进行识别。
	应用系统（含 IT 应用系统和 OT 系统）	从身份鉴别、访问控制、数据安全、备份、应急响应、安全审计、密码保护等方面进行识别。
管理脆弱性	技术管理	从物理环境管理、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，即是否真正的降低了系统的脆弱性，抵御了威胁。对有效的安全措施继续保留，对确认为不适当的安全举措应核实是否取消、修正或替代。

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

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：

$$风险值= R（A, T, V）= R（L（T, V）, F（Ia, Va））$$

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。

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 1-2.6.2。

风险等级 **表附录** 1-2.6.2

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。
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。安全措施的选择将从管理与技术两个方面考虑。安全措施的选择与实施应参照信息安全的相关标准进行。

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。

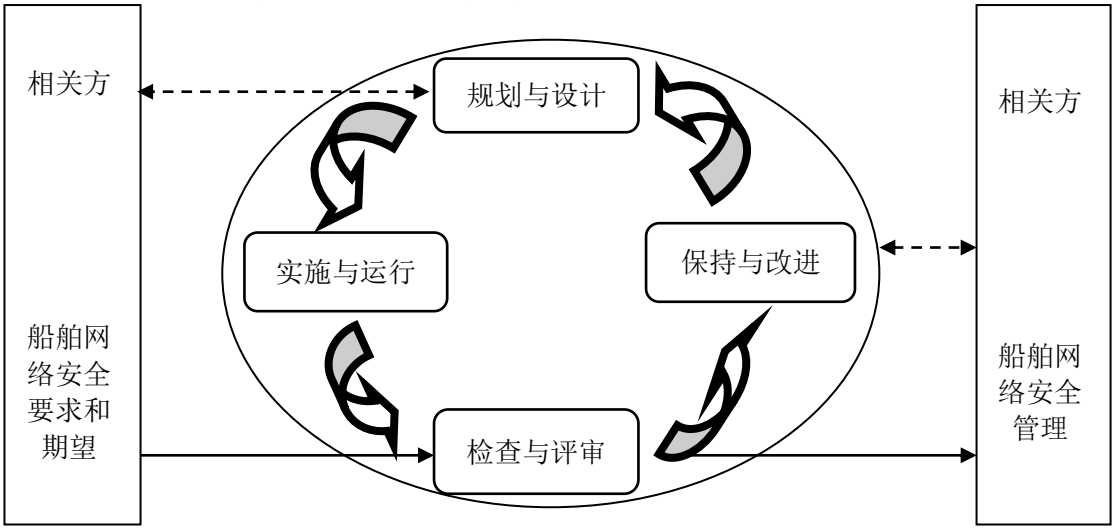
附录2　船舶网络安全管理

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

第4节 基本管理要求

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信息安全事件时；
（2） 当重大改变发生或提出时；
（3） 组织内部确定有必要时，或外部组织要求时。

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漏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。

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

附录3　船舶网络安全评估报告（产品）

Form CYBER-RD

中　国　船　级　社

China Classification Society

船舶网络安全评估报告（产品）

工作控制号：

申请方：

应上述申请方的申请，下列署名验船师于　　年　月　日对如下系统：

申请方开发的船舶网络系统“　　”（版本号：　　）

完成了网络安全评估。

1. 申请方图纸资料的批准号为：

2. 评估结果：

3. 评估过程描述：

4. 评估结论：

5. 详细评估结果

申请系统满足/不满足本社《船舶网络安全指南》有关要求。

6. 改进措施：

7. 其他

本报告内容仅代表本社评估时的船舶网络系统安全状态，当船舶网络系统发生拓扑结构变更时，申请方应立即向本社申请评估，必要时，本社将更新本报告。

地　点
Issued at _____

中 国 船 级 社
CHINA CLASSIFICATION SOCIETY

时　间
Issued on _____

注：☒ — 适用　　☐ — 不适用

* 不适用者划去

附录4　船舶网络安全评估报告（船舶）

Form CYBER-RS

中　国　船　级　社
China Classification Society

船舶网络安全评估报告（船舶）

工作控制号:

申请方:

应上述申请方的申请，下列署名验船师于　　年　月　日对如下船舶：

船名：　　，CCS No.：

完成了网络安全评估。

1. 申请方图纸资料的批准号为：

2. 评估结果：

3. 评估过程描述：

4. 评估结论：

评估结果满足/不满足本社《船舶网络安全指南》有关要求。

5. 改进措施：

6. 其他

通常，本报告有效期一年，本报告内容仅代表本社评估时的船舶网络系统安全状态，当船舶网络系统发生拓扑结构变更时，申请方应立即向本社申请评估，必要时，本社将更新本报告。

地　点
Issued at _____

中 国 船 级 社
CHINA CLASSIFICATION SOCIETY

时　间
Issued on _____

注：☒ — 适用　　☐ — 不适用

* 不适用者划去

附录5　船舶网络安全预评估表

Form CYBER-P

评估申请方：　　评估系统：

评估方：　　评估日期：

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

分类	评估项目	说明	得分
程序（总分：120 基线分值：70）	公司是否强调了对设备密码的设置措施？（5 分）		
	船员是否能意识到网络攻击的后果？（10 分）	通过公司的信息安全培训了解。	
	船员是否了解网络系统中用户及管理员的职责？（5 分）	同上。	
	船员是否意识到，使用未授权的移动数据存储设备存在风险？（5 分）	同上。	
	船员是否意识到，打开电子邮件附件和附件链接存在风险？（5 分）	同上。	
	公司是否为船员执行了网络安全的培训程序？（10 分）		
风险（总分：60 基线分值：35）	通过网络收到，或邮件下载的文件是否设置了自动打开？（10 分）		
	接入船舶网络的主机已安装了入侵检测、病毒防御、流量分析软件？（15 分）		
	接入船舶网络的主机是否能够对日志和报警监控，并进行记录？（15 分）		
	网络系统已执行了渗透测试？（10 分）	通过专业的渗透测试系统实施。	
	网络系统已执行了漏洞扫描？（10 分）	通过专业的漏洞扫描系统实施。	

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

附录6　船舶网络系统/设备评定表

Form CYBER-K

评估申请方：　　评估船舶：

评估方：　　评估日期：

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

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

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

分类	系统/设备	是否与船外网络相连（Y/N）	备注
	智能集成平台		
其他系统	本表未涵盖，但接入船舶网络的其他系统		

附录7　船舶工控系统防火墙设置附加建议

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

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

下面是通用规则：

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

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

下面是防火墙规则制定中要特别注意的：

- 基础的规则是拒绝一切。
- 控制网络环境和办公网间端口通信及服务批准时，应该具体问题具体分析。对于每次数据的出入，都必须有商业理由，并且有记录在案的风险分析和责任人。
- 如果状态合适，所有允许规则应该包含 IP 地址和 TCP/UDP 指定端口。
- 所有规则都应该限制通信使用指定 IP 地址或地址段。
- 禁止所有控制网络和办公网的直连，所有通信的终点都是隔离区。
- 当一种协议用于控制网与隔离区的通信时，它就不再应用于办公网络与隔离区的

通信。

- 从控制网络到办公网的连接必须通过服务和端口严格控制源和目的。
- 控制网络和隔离区的外出包，必须具备控制网络或隔离区指定正确的 IP 地址。
- 控制网路中的设备不能接入互联网。
- 即使有防火墙的保护，控制网络不可以直接接入互联网。

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