指导性文件
GUIDANCE NOTES
GD14-2017

中 国 船 级 社

CHINA CLASSIFICATION SOCIETY

船舶网络系统要求及安全评估指南

Guidelines for Requirement and Security Assessment of Ship Cyber System

（2017）

生效日期：**2017** 年 **7** 月 **20** 日

目　录

前　言

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

基于提升应对网络风险威胁意识的迫切需求，IMO 海上安全委员会在其第 96 届大会通过并随后发布了《海事网络风险管理暂行指南》（MSC.1 Circ.1526）通函，提出了对网络风险的应对措施，国际海事界对该问题的认识正不断提升。

为此，CCS 组织编制了本指南，其目的旨在规范船舶网络的建设工作，并对其实施有效评估，使有关的管理人员和技术人员理解船舶网络安全的重要性,形成综合提升船舶网络系统建设水平、威胁防御能力的新观念，保障船舶网络环境的稳定性，并为智能船舶的功能应用建立基本的条件与保障。

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

第 1 章 通则

1.1一般要求

1.1.1 本指南为船舶（包括船舶及海上设施）网络系统的建设过程提供指导，以保障网络系统具备安全性及必要的威胁防御能力。

1.1.2 本指南为船舶网络系统提供一套基于风险的安全评估方法。

1.1.3 船东/船舶管理公司对网络风险管理的计划和程序，应视为对现有国际安全管理（ISM）规则和国际安保（ISPS）规则中风险管理要求的补充。

1.1.4 本指南针对船舶网络安全建设及评估，包含以下主要内容：

1.1.4.1 从资源、程序、风险三个要素指导船舶网络系统建设；

1.1.4.2 网络系统产品及船舶网络安全评估要求；

1.1.4.3 船舶附加标志校验要求。

1.2 适用范围

1.2.1 本指南适用于船载网络系统和设备。

1.3 规范性引用文件

1.3.1 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。

序号	文件编号	文件名称
1		中国船级社《钢质海船入级规范》（2015）及其修改通报
2		中国船级社《智能船舶规范》
3	IEC 62443-2-1	《工控网络与系统信息安全标准综述 2-1：工业自动化和控制安全管理系统》
4	IEC 62443-3-3	《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》
5	ISO/IEC 27001:2013	《信息技术 安全技术 信息安全管理体系 要求》
6	ISO 17894-2005	《海上用可编程电子系统的开发和使用总则》
7	GBT 22239-2008	中华人民共和国国家标准《信息系统安全等级保护基本要求》

序号	文件编号	文件名称
8	ISO/IEC 15288:2002	《系统工程 系统生存周期过程》
9	GBT 20270-2006	中华人民共和国国家标准《信息安全技术 网络基础安全技术要求》
10	GBT 20984-2007	信息安全技术 信息安全风险评估规范
11	GBT 31509-2015	信息安全技术 信息安全风险评估实施指南
12	GBZ 24364-2009	信息安全技术 信息安全风险管理指南
13	GBT 26333-2010	工业控制网络安全风险评估规范
14	MSC.1-Circ.1526	国际海事组织（IMO）《海事网络风险管理暂行指南》
15		波罗的海航运协会（BIMCO）《船舶网络安全指南》
16		国际信息系统审计协会（ISACA）《COBIT5：企业 IT 治理和管理的业务框架》
17		国际信息系统审计协会（ISACA）《COBIT5：过程推动》
18		美国互联网安全中心（CIS）《网络防御的关键安全控制》（Version 7.0）
19		美国国家标准与技术研究院（NIST）《信息物理系统框架》（Release 1.0）
20	NIST Special Publication 800-53 Revision 4	美国国家标准与技术研究院（NIST）《信息系统与组织的安全及隐私控制》
21	NIST Special Publication 800-94	美国国家标准与技术研究院（NIST）《入侵检测和预防系统指南》

1.4 评估报告及附加标志

1.4.1 对于网络系统产品，经申请，并经CCS审图和评估，向其签发评估报告。

1.4.2 对于船舶网络系统，经申请，并经CCS审图和评估合格，向船舶授予如下附加标志：

Cyber Security

1.4.3 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《钢质海船入级规范》第1篇第2章第9节的规定。

1.5 图纸资料

1.5.1 申请网络安全评估的网络系统产品，应提交如下适用的图纸资料，由CCS审查或批准：

（1）网络系统的拓扑结构图，至少包含网络系统的下列信息：

①网络拓扑结构，能够清晰的显示网络传输介质与各接入系统、设备间的连接及访问关系；

②路由器的布置，以及连接路由器的网络区域；

③系统防火墙的布置及接入方式，并划分其安全防护区域；

④船载工作站、服务器的布置及接入方式；

⑤接入网络的系统、设备，如通过路由器连接或直连接入网络的通信导航系统、机舱状态监控系统、显示控制单元等；

⑥入侵检测、入侵防御系统的布置及接入方式（适用时）；

（2）硬件规格说明书，至少包含：

①网络传输介质的规格及最大数据传输流量；

②网络传输介质采用的主要通信协议标准；

③接入网络设备的基本参数，如传输端口、子网掩码、网关地址、接受的通信协议等；

（3）网络系统硬件安装说明，至少包含：

①通过图示或文字，说明路由器、防火墙、工作站、服务器等的安装位置及安装方式；

②为保护硬件设备免受物理损伤所采取的必要措施（适用时）；

③安装在特殊区域的设备对环境条件（温度、压力）的要求；

（4）系统运行及试验程序，至少包含如下操作：

①系统运行及启用；

②系统配置的初始化及变更；

③船岸通信（适用时）；

④系统数据流量监控及威胁防御设备的设置；

⑤用户访问权限的管理、变更、监控；

⑥系统及数据的备份、恢复；

（5）系统配置文件，至少包含：

①接入船舶网络的设备、系统列表，包含版本号、安装维护日期、在网络系统中的标识名称等基本信息；

②网络数据流量限定值；

③系统投入运行后，各设备开放的端口；

④允许访问船舶网络的用户及授予的权限；

⑤系统对限制访问地址的设定，如系统白名单；

⑥远程用户访问权限（适用时）；

对系统配置文件的相关说明，至少包含：

② 配置文件在船上存储及备份的位置；

②为保护系统配置文件免受恶意读取或篡改所采取的必要措施；

（6）系统测试记录。

1.5.2 申请网络安全附加标志的船舶，应提交如下适用的图纸资料，由CCS审查或批准：

（1）满足 1.5.1（1）要求，且符合实船布置的船舶网络拓扑结构图；

（2）满足 1.5.1（5）要求，且符合实船布置的系统配置文件；

（3）对网络系统开发方的船舶网络安全评估报告（详见**附录 7**）；

（4）网络运维规章制度，应包含日常运维、升级及安全审计等；

（5）人员管理制度，应包含人员能力评估方法及评估计划、培训计划等；

（6）供应商网络使用管理制度，应包含外部人员使用数据或访问受控资源的管理办法，数据使用要求和控制规则等；

（7）备份与灾难恢复管理方法，应包含应急计划，备份计划等内容。

（8）其中（4）-（7）有关材料，如在船舶图纸送审期间无法提供，可在实船验证前完成，并由现场验船师验证。

1.5.3 船上应方便获得下列资料：

（1）符合 1.5.1（1）要求的船舶网络拓扑结构图；

（2）按网络实际情况同步更新的系统配置清单；

（3）防火墙运行日志，能够显示被过滤/阻止的行为和数据记录；

（4）网络系统更新记录；

（5）入侵检测、入侵防御系统的运行日志（适用时）；

（6）漏洞扫描、渗透测试系统的运行日志（适用时）；

（7）CCS 签发的船舶网络安全评估报告。

1.6 申请与费用

1.6.1. 申请

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

1.6.1.2. 如果申请船舶网络安全的系统和/或船舶中没有进行过相应评估，本社在接受其申请之前，应进行预评估。

1.6.2. 费用

1.6.2.1. 申请人应按本社费规或/和合同和/或协议支付评估费和交通费，以及其他必要的费用。

1.6.2.2. 由于申请方的原因，造成评估中止或使本社与评估有关的活动重复进行，申请方也应向本社支付相应费用。

1.7 责任及其限定

1.7.1. 责任和义务

1.7.1.1. 公司责任和义务

(1) 本社的网络安全评估并不解除公司、管理层、高级船员或船员必须符合国际公约、规则、导则和船旗国赋予的有关安全和环境保护法规的义务。

(2) 公司应负责：

① 将评估的目的和范围通知涉及评估人员或组织机构内的场所或单位；

② 指派负责的人员陪同评估人员；

③ 向评估人员提供其必需资源，以确保验证过程的有效性和效率；

④ 按评估人员要求，提供便利和客观证据；

⑤ 配合评估人员以达到评估目标；

⑥ 对公司网络安全相关体系文件和船舶实施网络安全评估。

(3) 获得评估报告或附加标志后，公司应：

① 保持船舶网络及相关体系文件有效运行；

② 及时通知本社有关网络及相关体系文件的重大变更情况，包括网络架构、配置文件、体系文件的重大调整和具有新危险的操作改变。这类变更可能引起网络安全评估报告失效；

③ 当有要求时，申请附加评估；

④ 及时通知本社其所管理船舶的变更情况。

1.7.1.2. 本社责任和义务

(1) 本社确保船舶网络安全系统或船舶评估过程按本指南和船旗国有关要求（如有时）予以实施。

(2) 本社确保在本社组织范围内具备涉及下列方面的能力：

① 理解和实施受评估的船舶、系统必须满足的规范和规则；

② 实施有关船舶网络安全评估报告和附加标志的批准、检验和授予活动；

③ 船舶操作的实践经验。

(3) 本社船舶网络安全评估服务的管理应：

① 由具有实践知识的人员进行；

② 确保评估人员符合涉及规定的教育、培训、工作和评估经验的要求；

③ 所指派的评估人员具备适当的资格和经验，并与所评估的系统和/或船舶的规模和/或复杂程度相适应。

1.7.1.3. 评估组责任

(1) 评估人员应负责：

① 有效地计划和履行指定的职责；

② 确保符合适用的要求和其他适当的指示；

③ 报告评估中所遇到的任何影响评估过程的重大问题；

④ 必要时，聘请专家提供技术协助，以满足评估的适任要求；

⑤ 及时与公司和/或船上管理层清楚交流关于网络安全基本要求的不符合条目；

⑥ 结论清晰明确并及时报告评估结果；

⑦ 向公司或船上管理层提交评估报告；

⑧ 验证公司所采取的纠正措施的有效性。

(2) 评估相关的文件和资料应按保密要求处理。

(3) 当评估员发现严重不合格以及被认为对安全构成了严重的威胁并危及环境的技术缺陷，应提请公司注意。

(4) 当评估组由两名及以上的评估员组成时，由指定的评估组长负责评估组的管理和评估控制。

1.7.1.4. 责任限定

(1) 本社将确保船舶网络安全评估的完整性和有效性，并当本社授权代表船旗国主管机关的情况下，接受主管机关的监督。

(2) 本社签发的网络评估报告或授予的附加标志仅表明本社在时公司/船舶已按照指南满足船舶网络安全要求，但不能保证随后不出现公司和/或船舶对船舶网络安全架构、配置及相关体系文件的擅自变更和主观上未有效实施网络安全建设要求而导致与所签发证书不符的情况。持续符合船舶网络建设要求是公司和/或船舶的责任。

(3) 证书的保持是根据船舶持续符合本指南要求的条件而决定的。当公司和船舶拒绝本社评估员对公司和/或船舶进行审核，或因证书和其他服务而不付款,或有证据表明公司和船舶放弃了船舶网络安全评估的责任和义务,本社保留撤消和注销网络评估报告及附加标志的权力。

1.8 信息提供、保密和申诉

1.8.1 信息提供

1.8.1.1 各有关方应向本社提供船舶网络系统评估所需要的充分和正确的信息。

1.8.1.2 获得本社船舶网络安全评估证书和附件标志的船舶在其证书有效期内所发生的网络安全事件信息应及时通知本社。

1.8.2 保密

1.8.2.1 本社在船舶网络安全系统及船舶评估过程中所接触到的所有敏感和机密信息绝不向任何合同以外的个人和组织，包括本社内与该服务无关的人员泄露，但法律法规要求的除外。

1.8.3 申诉

1.8.3.1 如果船舶管理公司或船东对本社执行的评估有任何抱怨，可书面要求本社在评估完成日期起30天内重新进行评估。

1.9 定义

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

1.9.2 资产管理：对任意数据，计算机或设备的控制。

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

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

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

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

1.9.7 拒绝服务攻击（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。

1.9.8 防火墙：防止对网络系统设施和信息未授权访问的逻辑或物理阻断。

1.9.9 缺陷：非预期的软件功能。

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

1.9.11 入侵检测系统（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。

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

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

1.9.14 恶意软件：泛指能传染计算机系统并影响其性能的软件。

1.9.15 信息技术（IT）：用于管理和处理信息所采用的各种技术及系统。

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

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

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

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

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

1.9.21 服务提供商：提供和执行软件维护的公司或个人。

1.9.22 虚拟局域网（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。

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

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

1.9.25 广域网络（WAN）：一种跨区域、国家或国际边界的网络。

1.9.26 Wi-Fi：一种允许电子设备连接到一个无线局域网的技术。

1.9.27 网络拓扑：网络形状，或网络在物理上的连通性。

1.9.28 网络拓扑结构：用传输媒体互连各种设备的物理布局。

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

1.9.30 上位机：可以直接发出操控命令的计算机。

1.9.31 下位机：直接控制设备获取设备状况的计算机。

1.9.32 工作组：将局域网中不同的电脑按功能分别列入不同的组中，以方便管理。

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

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

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

1.9.36 机密性：使信息不泄露给未授权的个人、实体、过程或不使信息为其利用的特性。

1.9.37 完整性：保证控制信息及控制系统不会被有意地或无意地更改或破坏的特性。

1.9.38 可用性：数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

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

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

第 2 章 网络系统要求

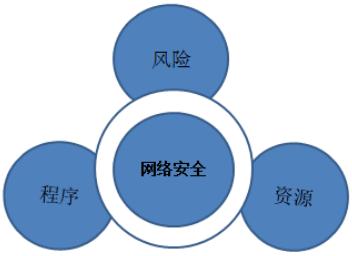
2.1 一般要求

2.1.1 网络结构

2.1.1.1 船舶网络基本可划分为两层。底层是由各系统的监控单元构成的控制网络（OT 网络），这些网络通常采用如 CAN、Modbus 等现场总线技术实现，接入网络的系统，包括分布于机舱的主推进监控系统、辅机监控系统、电站监控系统、火灾报警系统等以及驾驶台上的导航系统、综合船桥系统等，负责采集和监视全船设备的运行状态数据，通过网络传送给顶层的管理系统，同时接受和执行顶层管理系统的控制命令，实现设备控制。船舶的顶层网络（IT 网络），主要由标准化操作站（显控台）、服务器等构成，这些网络通常采用以太网络等实现，各分系统网络通过网关与顶层网络相连，从而实现了各系统间的数据传输与数据共享。

2.1.2 要素划分

2.1.2.1 基于船舶网络的复杂性，将船舶网络建设要求划分以下三个要素，船东/船舶管理公司、系统开发方、运维方在研发、实施、维护、退役系统时应予以综合考虑：



（1）资源：资产及资产的标识、对资产的访问、所处的物理环境、所产生的数据，资产使用中参数的配置要求；

（2）程序：为网络安全管理需要制定的管理程序、规章制度、设立的管理机构、确定人员所承担的角色及作用、业务流程的流转过程、网络建设及运维要求等；

（3）风险：网络安全所面临的风险，如何规划，识别及评估，风险发生后如何应对等。

2.2 资源

2.2.1 资产管理（Asset Management，AS）

2.2.1.1 利用访问控制和认证协议搭建网络，设备连接到网络前，必须通过授权及认证，接入网络的设备及系统进行登记，并控制授权，限制如移动存储介质、非内部所有的系统/组件/设备、网络可访问存储设备的使用。

2.2.1.2 对网络中使用的设备，应手动或通过适当的探测或扫描工具，建立设备目录，并保持更新，设备目录至少包括：设备名称，设备用途，设备所在位置，责任人，所属部门，网络地址等信息。

2.2.1.3 对网络中使用的软件及组件，应手动或采用适当的工具，建立软件及组件目录，制定可运行软件及组件的白名单，并保持更新，该目录应有软件名称及版本等信息，以便跟踪。

2.2.1.4 识别网络中数据流及协议，确定网络域之间、工作组之间、上位机、下位机、服务器、客户端、操作站、监控站之间的数据流、应用的协议等。

2.2.1.5 对于网络系统所涉及的加密证书，应采用相应的系统进行管理，管理的数据项至少包括人员、设备、证书、发行和到期日、证书发起人等。通过使用加密证书，网络系统应能对用户访问、OT 系统数据传输、便携式设备接入等关键操作进行验证。

2.2.1.6 对于网络中的资产（如硬件、设备、数据和软件），可按类别、关键性、业务价值进行分类，划分优先级，建立网络安全要求。根据网络安全要求层次，利用防火墙及访问列表等，依据功能形成不同 VLAN。

2.2.1.7 对于网络中的资产（如硬件、设备、数据和软件）安装应遵循 CCS 规范-第 7 篇自动化系统相关要求，安装位置可参见《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》中物理安全相关要求。

2.2.2 标识及认证（Identify and Authorize，IA）

2.2.2.1 对网络系统中的用户（人员、软件、设备）及账号进行标识和认证，并对网络访问实现多因素认证，对接入设备实现动态地址分配等认证方式。制定标识管理办法，如禁止使用公共符号进行标识。

2.2.2.2 对网络中已识别的人员、组织、角色和设备授予相应的角色。

2.2.2.3 建立和实施系统用户授权管理。

2.2.3 访问管理（Access Management，AM）

2.2.3.1 采取必要的技术措施，对所有访问网络系统的账户进行监控，如确定账户的使用期限，清理不必要的用户和管理员账户，禁用已过期的、与任何业务无关的账户，超时注销，若干次尝试登录失败后账户锁定等。应定期对账户进行管理及审查。

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

2.2.3.3 严格口令管理，及时更改系统安装时的预设口令，杜绝弱口令、空口令。

2.2.3.4 定期对网络中系统及设备的端口、服务等进行检查，停用无用的后台程序和进程，关闭无关的端口和服务。

2.2.3.5 授权第三方（设备供应商、系统开发方、系统维护方等，下同）访问网络系统时，需进行审核。定期对第三方的访问权限进行审核，确认其在可控范围内。

2.2.3.6 第三方的访问，需使用多因素认证，或强密码。第三方在网络系统中的行为日志应能被记录并保存。

2.2.3.7 第三方接入网络系统时（必要时），需授权最小的访问权限，采用专用的安全的存储介质，如非必要时，

不允许第三方进行数据的收集与存贮。

2.2.3.8 针对特定的工作需求、特殊系统的特权帐户，应采取特殊的网络访问限制。

2.2.4 数据管理（Data Management，DM）

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

2.2.4.2 禁止在非专用通道或网络区域内传输 OT 系统的命令和控制信号。

2.2.4.3 如有第三方使用数据，则需制定相应的数据使用要求和控制规则。

2.2.4.4 如使用第三方提供的服务或数据，应保证服务安全和数据安全。

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

2.2.4.6 对公司及人员隐私数据进行管理，遵循国家或当地的法律法规要求。

2.2.4.7 对隐私数据的访问和分发进行严格控制。

2.2.4.8 船员和船东/船舶管理公司的隐私数据与其他数据的存储应相互隔离。

2.2.5 配置管理与补丁（Configuration Management，CM）

2.2.5.1 船舶网络系统具备系统配置文件，且内容至少满足本指南第 1 章 1.6.1（5）的要求。

2.2.5.2 系统配置文件应便于升级，以快速识别网络系统中接入设备、系统的变化情况。

2.2.5.3 应建立网络系统中关键设备的配置定期审核制度。

2.3 程序

2.3.1 管理程序（Management Program, MP）

2.3.1.1 船东/船舶管理安全管理体系文件中应包含网络安全策略、网络安全管理制度、网络安全操作规程、基本配置要求等内容。

2.3.1.2 船上及公司的网络系统主要负责人员应持有相应程序。

2.3.2 组织机构（Organization Structure, OS）

2.3.2.1 船东/船舶管理公司应设立主管船舶网络安全的专门机构，可由机务部兼任，也可以是专门部门。无论如何应有专人负责。

2.3.2.2 该机构负责制定船舶网络安全管理的各项程序。

2.3.2.3 船东/船舶管理公司应建立船舶网络安全岗位管理程序，明确岗位设置、值班要求、人员配备，管理流程及沟通合作机制。

2.3.3 人员管理(Employee Management, EM)

2.3.3.1 建立人员管理制度，规范人员的审查、离岗、考核等流程，例如，船上任何控制 OT 系统的人员需要进行资格审查，人员离岗时需进行权限及相关设备资源的调整等。

2.3.3.2 制定培训计划，定期组织网络系统规范操作培训，提高相关人员的安全意识，明确安全职责。

2.3.3.3 明确船东/船舶管理公司及第三方的职责及网络系统访问要求。

2.3.4 建设管理(Development Management, DM)

2.3.4.1 制定船舶网络安全目标，确定船舶网络范围及明确船舶网络安全目标要求。

2.3.4.2 依据船舶网络范围及船舶网络安全要求，进行网络方案设计，制定工作计划，形成配套文件体系，并获得批准实施。

2.3.4.3 慎重选择网络中的设备，在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务，确保产品安全可控，产品采购和使用符合国家的有关规定。

2.3.4.4 设备、软件、应用及系统在船舶上实施前，必须先进行功能、安全需求测试，未经测试不允许实施，测试环境要与实际运行环境物理分开，测试数据和测试结果可控。

2.3.4.5 船舶网络建设过程要有专门的部门或人员负责工程实施过程的管理。

2.3.4.6 船舶网络交付前应进行安全评估。

2.3.4.7 船舶网络交付时应提供交付清单，至少包括第 1 章 1.5.1（1）-（3）中的主要资料。

2.3.4.8 船舶网络建设应确保供应商的选择符合国家的有关规定。

2.3.5 运维管理(Operations Management, OM)

2.3.5.1 船东/船舶管理公司建立网络运维制度，制度中应包括：限制哪些基于计算机的维修协助或分析方法可适用，系统如何修补和更新，以及网络系统的维护人员如何培训和认证去识别报告异常及可能表明安全和安保问题的迹象。

2.3.5.2 对网络系统中的设备运行状况、网络流量、用户行为进行日志记录，进行安全审计，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，

2.3.5.3 报警管理，对网络运行情况进行实时监视，对异常情况进行报警，对产生网络风暴的设备进行隔离。对网络故障进行监控，便于及时采取措施，恢复网络正常运行；对网络的关键性指标等进行监控，可对数据记录进一步分析，生成审计报表，审计记录应受到保护，防止未预期的删除，修改或覆盖等。

2.3.5.4 制定供应商网络使用管理制度，明确第三方对企业资源（数据，系统和网络资源）访问及预防措施，并对其访问进行系统性监测，以确保其访问是可信的。

2.3.5.5 加强对技术服务的信息安全管理，在安全得不到保证的情况下禁止采取远程在线服务。

2.3.5.6 采用安全评估工具或过程定期对当前船舶网络安全状态进行评估，弥补不足及差距。

2.4 风险

2.4.1 风险管理(Risk Management, RM)

2.4.1.1 建立风险管理办法，确保风险管理的程度、类型和可见度与风险及系统对船舶安全的重要性相匹配。

2.4.2 风险评估(Risk Assessment, RA)

2.4.2.1 定期评估资产安全，识别漏洞及威胁，分析漏洞及威胁发生的可能性及对业务流程造成的影响，确定其严重性，以确定更新的优先顺序及风险应对策略。

2.4.2.2 分析内部或外部的威胁，对其识别并记录。

2.4.2.3 检测安全设备及其状态报告，并通过日志和警报报告揭示威胁和风险。

2.4.3 防御管理(Defense Management, DM)

2.4.3.1 密切关注产品漏洞和补丁发布，严格软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入。升级移动设备、便携式设备、工作站、服务器和相关软硬件系统，以及网络设备，如防火墙、路由器、交换机的安全配置，防止利用已公布的漏洞信息的攻击；入侵检测、恶意代码检测和补丁管理需注意 OT 系统与 IT 系统的不同，关键 OT 系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证。

2.4.3.2 基于资产管理划分的优先级，对船舶网络进行分级保护。

2.4.3.3 对通信路径和信息（例如，电子邮件或社交通讯方式）进行审查，检测和删除任何危险的文件、附件或链接。

2.4.3.4 建立通信地址白名单，如电子海图、导航系统、综合船桥系统等如需进行数据传递时，明确访问机制。

2.4.3.5 管理所有设备的远程登录，远程控制，对于第三方设备（例如，分包商/供应商），发布访问网络的最低安全标准，并在访问之前执行安全扫描。

2.4.3.6 限制使用外部设备，当在笔记本、工作站、服务器上连接移动存储介质，如 U 盘、移动硬盘、光盘等时，禁止其自动执行，并进行防病毒、反间谍软件的扫描；（病毒查杀的程度以及软件更新）。

2.4.3.7 风险报警管理，及时提示风险发生的设备或区域。

2.4.4 网络监测(System and Security Continuous Monitoring, SCM)

2.4.4.1 对无线网络进行检测，防止未经授权的接入点访问网络系统或基础设施。

2.4.4.2 对工作站、服务器和移动设备进行连续自动监测，并对检测事件进行日志记录，对异常行为进行报警，通过分析网络信号、行为或流量，实现网络攻击行为的探测，过滤恶意内容，防止潜在的网络安全事件。

2.4.4.3 对 VPN 流量进行保护性审查和过滤防止远程连接系统的恶意软件没有经过安全监控包通过 VPN 进入主要网络系统，终止任何关键系统或部件的边界之外的所有 VPN，并在监测所访问节点。

2.4.4.4 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，识别威胁采取行动。

2.4.5 事故响应及应急(Incident Response, IR)

2.4.5.1 结合历史经验，制定应急计划，至少包括，人员沟通方式、危险控制措施、灾难恢复计划等。

2.4.5.2 定期对应急计划进行审核、更新。

2.4.6 备份恢复(Recovery, RE)

2.4.6.1 制定备份计划，定义备份范围，如业务信息、系统数据及软件系统等；规范备份方式、频度、存储介质和保存期等；依据数据的重要性和对系统运行的影响，制定数据的备份策略和恢复策略等。

2.4.6.2 定期进行备份，对备份数据进行测试，确保备份数据正常工作，当采用远程备份和云服务时，要确保跨网络移动时的物理安全或加密。

2.4.6.3 定期测试恢复程序，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。

第 3 章 网络系统产品的评估

3.1 一般要求

3.1.1 本章适用于由船舶网络系统的开发方申请，CCS提供针对网络系统产品设计、开发、安装等环节的评估服务。

3.1.2 网络系统产品系指为实现船舶系统及设备互联互通而构建的网络体系结构，包括接入网络的主要系统/设备。

3.1.3 对网络系统产品的主要评估方式为：

（1）预评估：参考附录1 船舶网络安全预评估表中有关资源部分的内容，对网络系统产品进行风险分析，为后续评估提供指导。

（2）详细评估：根据网络系统要求，对船舶网络系统产品的进行网络安全评估。

3.1.4 详细评估完成后，由CCS向申请方签发评估报告。

3.1.5 对于智能船舶，对网络系统产品的评估结果达到各项评估基线值后，其系统允许在待申请/已申请CCS网络安全附加标志的船舶上安装、运行。

3.1.6 CCS对网络系统产品的评估独立于船舶的产品检验工作，二者不可相互替代或覆盖。

3.2 详细评估

3.2.1 详细评估通过全面分析船舶网络系统产品的评估指标，识别系统中存在的安全风险，综合评判系统应对网络风险的能力。

3.2.2 CCS按照资源、程序、风险三个分类开展详细评估。

3.2.3 详细评估的步骤如下：

（1）系统开发方提交申请。

（2）CCS依据**附录3 船舶网络安全详细评估表（产品）**进行评估。

（3）CCS依据**附录5 船舶网络安全详细评估基线值**中必要项目的要求判定评估结果，如符合要求，则进行步骤（4）；如不符合要求，则网络系统产品不满足本指南要求，进行步骤（5）。

（4）CCS依据**附录5 船舶网络安全详细评估基线值**中的基线分值判定评估结果。

（5）CCS签发评估报告（详见**附录6 船舶网络安全评估报告（产品）**）。

3.2.4 必要时，详细评估的部分技术指标需经CCS检测及试验得出。具体要求见本指南3.2.5节和3.2.6节。

3.2.5 安全漏洞扫描

3.2.5.1 CCS通过技术手段，对网络系统产品进行全面的检测和漏洞扫描，定位漏洞分析原因，并将结果作为详细评估的结论之一。

3.2.5.2 CCS向申请方提供漏洞扫描测试报告。

3.2.6 渗透测试

3.2.6.1 CCS通过技术手段，对网络系统产品进行全面的渗透测试，并将结果作为详细评估的结论之一。

3.2.6.2 测试通过CCS建立的渗透测试环境，对船舶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。

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

3.2.6.4 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。

3.2.6.5 渗透测试完成后，CCS向申请方提供渗透测试报告。

3.3 评估报告

3.3.1 评估完成后，由CCS向申请方签发**附录6 船舶网络安全评估报告（产品）**。

3.3.2 报告将对网络系统产品应对威胁的能力进行评定，并针对评估结果提出建议的改进措施。

第 4 章 船舶网络系统的评估

4.1 一般要求

4.1.1 本章适用于由船东/船舶管理公司申请，CCS提供针对实船网络系统运行、管理、维护等环节的评估服务。

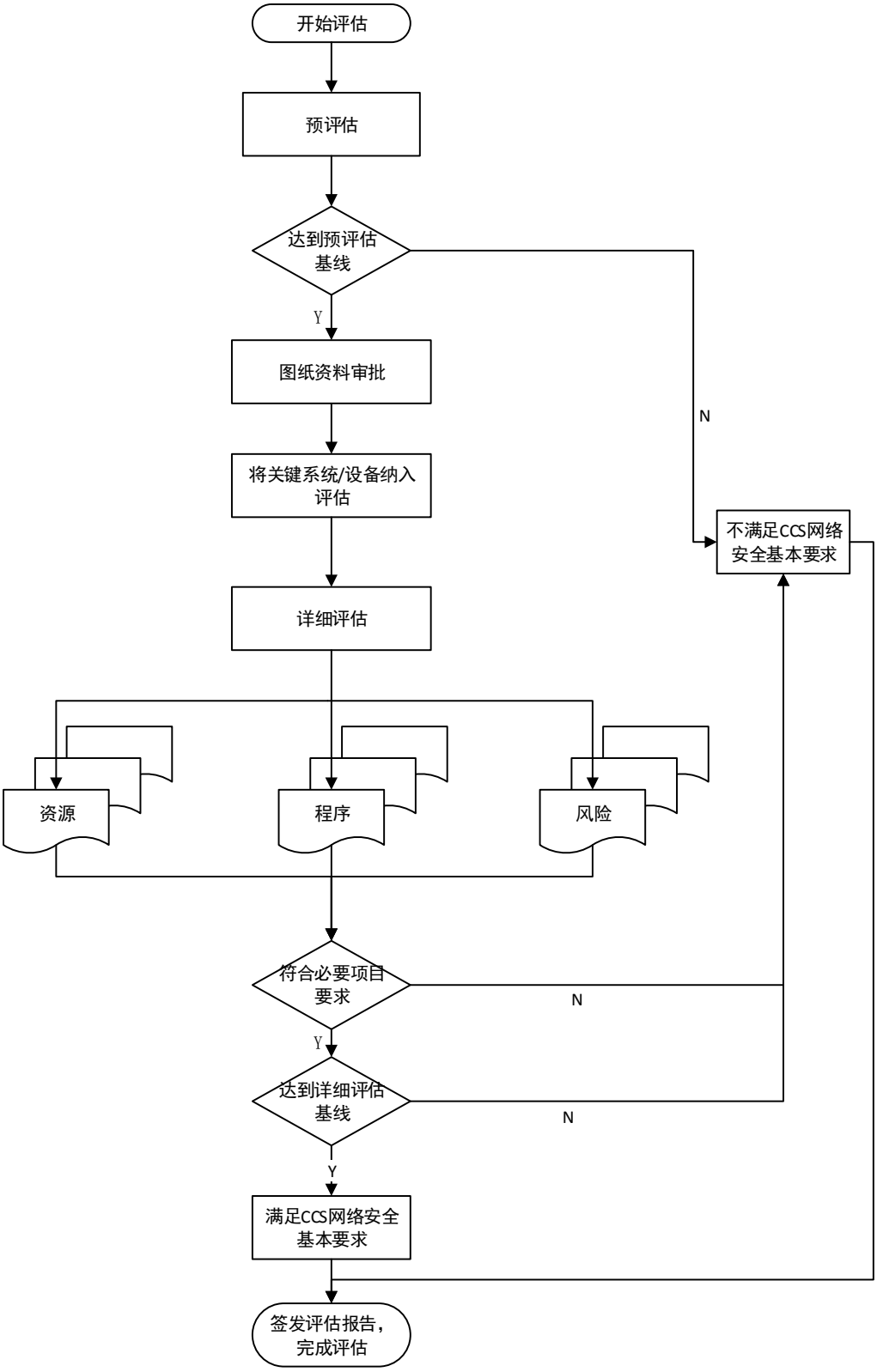
4.1.2 对船舶网络系统的主要评估方式为：

（1）预评估：参考《附录1 船舶网络安全预评估表》对船舶网络进行风险分析，掌握船舶网络系统的总体情况；

（2）详细评估：根据网络系统要求，对船舶网络系统进行分类安全评估。

4.1.3 预评估、详细评估均完成后，由CCS向申请方签发评估报告。

4.1.4 船舶网络系统评估的步骤示意如下：


开始评估
预评估
达到预评估基线
Y
N
图纸资料审批
将关键系统/设备纳入评估
详细评估
不满足CCS网络安全基本要求
资源
程序
风险
符合必要项目要求
N
Y
达到详细评估基线
N
Y
满足CCS网络安全基本要求
签发评估报告，完成评估

4.2 预评估

4.2.1 预评估作为网络安全评估活动的初始工作，应由船东/船舶管理公司完成。

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

4.2.3 预评估阶段通过如下几个方面掌握船舶网络的基本情况：

（1）了解ISPS Code是否在船东/管理公司及船舶上有效应用；

（2）掌握应用于船舶的，用以防范网络威胁的主要管理程序、技术手段；

（3）掌握易受网络攻击的关键设备、系统；

（4）掌握易受网络攻击的设备、系统的操作过程；

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

（6）了解船舶网络系统的主要使用者，及其操作过程中可能面临的风险点；

（7）了解设备厂商对船舶网络及其设备的维护、升级等技术支持情况。

4.2.4 预评估应按照**附录2 船舶网络安全预评估表**的内容开展。

4.3 详细评估

4.3.1 详细评估通过全面分析船舶网络中的评估指标，识别船舶网络中存在的安全风险，并分析船舶应对网络风险的能力。

4.3.2 CCS对已完成预评估，且达到基线分值的船舶网络系统实施详细评估。

4.3.3 CCS按照资源、风险、程序三个方面开展评估。

4.3.4 详细评估的步骤如下：

（1）船东/船舶管理公司提交申请。

（2）CCS根据网络系统在船舶的运行情况，根据**附录2 船舶网络系统/设备评定表**评定纳入详细评估表的船舶系统/设备。

（3）CCS依据**附录4 船舶网络安全详细评估表（船舶）**进行评估。

（4）CCS依据**附录5 船舶网络安全详细评估基线值**中必要项目的要求判定评估结果，如符合要求，则进行步骤（4）；如不符合要求，则船舶网络系统不满足本指南要求，进行步骤（5）。

（5）CCS依据**附录5 船舶网络安全详细评估基线值**中的基线分值判定评估结果。

（6）CCS签发评估报告（详见**附录7 船舶网络安全评估报告（船舶）**）。

4.4 安全问题的反馈

4.4.1 船东/船舶管理公司应建立适当的操作程序，在设备、系统受到威胁或发生安全问题时，及时的与生产厂

家沟通，反馈问题，并使设备、系统得到维护。

4.4.2 设备、系统生产厂家应及时的维护、修复系统，减小网络事件对船舶造成进一步影响。

4.5 评估报告

4.5.1 评估完成后，由CCS向申请方签发**附录7 船舶网络安全评估报告（船舶）**。

4.5.2 报告将对船舶网络应对威胁的能力进行评定，并针对评估结果给出建议的改进措施。

第 5 章 附加标志检验

5.1 一般要求

5.1.1 由船上，或船东/船舶管理公司向CCS申请船舶网络安全检验。

5.2 检验

5.2.1 初次检验

5.2.1.1 初次检验至少应包括如下项目：

（1）图纸资料已审批；

（2）核查《船舶网络安全评估报告（船舶）》，预评估、详细评估结果符合本指南的有关要求；

（3）确认船上备有相关图纸资料、手册、程序及记录文件。

5.2.1.2 经初次检验，确认船舶符合本指南的有关要求，由CCS为船舶授予网络安全附加标志。

5.2.2 建造后检验

5.2.2.1 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。

5.2.2.2 年度检验时，CCS应实船检查以下项目：

（1）《船舶网络安全评估报告（船舶）》；

（2）船舶网络运行日志，确认运行状况良好；

（3）船舶网络安全的评估指标变化情况；

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

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

5.2.4 如船舶超出限期仍未完成网络安全整改，由CCS撤销船舶网络安全附加标志。

附录 1 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	

分类	评估项目	说明	得分
程序（总分：120 基线分值：70）		职责清晰的程序文件。	
	是否对公司的网络安全水平定期评审？（10 分）	公司对网络安全水平定期评估，并相应的调整管理措施。	
	针对接入船舶网络中的系统，是否已由系统开发方签署保密方面的协议条款？（5 分）		
	公司是否强调了对设备密码的设置措施？（5 分）		
	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 2 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	是否与其他网络相连（Y/N）	是否纳入详细评估(Y/N)	备注
通信系统	卫星通信设备			
船桥系统	网络电话（VOIP）			
	无线网络（WLANs）			
	通用报警系统			
	定位系统（GPS 等）			
	电子海图系统（ECDIS）			
	动力定位（DP）系统			
	与电子导航系统和推进/操纵系统关联的系统			
	自动识别系统（AIS）			
	全球海上遇险和安全系统（GMDSS）			
	雷达设备			
	航行数据记录仪（VDR）			
	惯性导航系统（INS）			
	其他监测和数据采集系统			
推进、机械设备管理、电力控制系统	柴油机			
	锅炉控制系统			
	辅助安全系统			
	电站及电源管理系统			
	自动化监控系统			

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

分类	系统/设备	是否与 其他网络相连 （Y/N）	是否纳入详细 评估(Y/N)	备注
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			
火灾及火源控制	火灾监测系统			
	探烟系统			
	防火门控制系统			
	消防泵控制和监测系统			
	灭火系统			
	危险气体探测系统			
	碳氢气体探测系统			
乘客服务管理系统	资产管理系统			
	医疗记录			
	乘客登船访问系统			
	基础设施支持系统（如域名系统、用户认证/授权系统）			
乘客网络	乘客的 Wi-Fi 或局域网登录			
	娱乐系统			
	通信系统			
核心基础设施系统	路由器			
	交换机			
	防火墙			
	虚拟专网（VPN）			
	虚拟局域网（VLAN）			
	入侵防御系统			
	安全事件日志系统			

分类	系统/设备	是否与 其他网络相连 （Y/N）	是否纳入详细 评估(Y/N)	备注
信息管理系统	信息管理系统（备件物料管理、PMS 管理、人事管理、培训等系统）			
个人设备	船员的个人设备、局域网或 WiFi 接入互联网			
智能系统	智能航行			
	智能船体			
	智能机舱			
	智能能效管理			
	智能货物管理			
	智能集成平台			
其他系统	本表未涵盖，但接入船舶网络的其他系统			

附录 3 船舶网络安全详细评估表（产品）

Form CYBER-DD

评估申请方：　　评估系统：

评估方：　　评估日期：

注：1.需在打“X”的环节对评估要求予以关注。

2.编号标识含“”的为详细评估的必要项目（需完全满足评估要求）。*

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
	×	×		**资源**	**访问管理**	*AM1	IT+OT	确认网络中所有物理安全设备（摄像机、传感器、电子门锁、网络访问等）存在密码，并满足要求：（1）非默认；（2）非简单加密。	0:所有设备无密码保护 1:部分设备有密码保护，且为默认或简单加密 2:网络中 50%以下设备有密码保护，且为非默认或非简单加密 3:网络中 50%以上设备有密码保护，且为非默认或非简单加密 4:所有设备有密码保护，且为非默认或非简单加密	
×	×	×		**资源**	**访问管理**	AM2	OT	针对接入网络的控制系统，限定特定的角色和用户登录。	0:所有控制系统未限定特定角色和用户 1:网络中 50%以下的控制系统限定特定角色和用户 2:无控制系统 3:网络中 50%以上的控制系统限定特定角色和用户 4:所有控制系统限定了特定角色和用户	
×				**资**	**访问**	AM3	IT	船舶网络支持跨系统的单点登录（SSO）方式，以保证登录访问的可	0:船舶网络不支持 SSO 1:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				源	**管理**			追溯性。	2:- 3:- 4:船舶网络支持 SSO	
×	×	×		**资源**	**访问管理**	*AM4	IT+OT	船舶网络应依据用户角色、工作职责分配系统和数据的访问权限。	0:未按照用户角色、职责分配权限 1:- 2:- 3:- 4:已按照用户角色、职责分配权限	
×	×	×		**资源**	**访问管理**	AM5	OT	管理人员应全面掌握和控制接入船舶网络的控制、通信系统等，并设置系统白名单。	0:未设置网络白名单 1:- 2:- 3:- 4:已设置网络白名单	
×				**资源**	**访问管理**	*AM6	IT+OT	根据网络安全层次要求，搭建管理网络的基础设施，利用防火墙及访问列表，形成 VLAN，将个人、管理、控制、通信网络分开，互相独立。	0:各网络未独立 1:- 2:- 3:- 4:各网络独立，且形成 VLAN	
×	×	×		**资源**	**访问管理**	AM7	IT	配置网络系统中的屏幕锁以限制访问。	0:所有屏幕未配置屏幕锁 1:网络中 50%以下的系统配置屏幕锁 2:- 3:网络中 50%以上的系统配置屏幕锁 4:所有屏幕已配置屏幕锁	
×	×	×		**资源**	**访问管理**	AM8	IT	使用和配置帐户锁定，在尝试登录失败后，按标准时间锁定账户。	0:所有接入网络的系统不具备登录失败后的锁定功能 1:网络中 50%以下的系统具备登录失败后的锁定功能 2:- 3:网络中 50%以上的系统具备登录失败后的锁定功能 4:所有接入网络的系统具备登录失败后的锁定功能	
×	×	×		**资源**	**访问管**	AM9	IT	对有访问敏感数据或系统的所有用户帐户，需要多因素身份验证。多因素身份验证可以通过使用智能卡、证	0:所有系统未设置多因素验证或密码 1:部分系统设置密码（短于 8 个字符） 2:网络中 50%以下的系统设置密码（长于 8 个字符),	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
					理			书、一次性密码（OTP）的标记，或生物识别技术。	或使用多因素验证 3:网络中 50%以上的系统设置密码（长于 8 个字符），或使用多因素验证 4:所有系统已设置多因素验证或长密码（长于 8 个字符）	
×	×			**资源**	**访问管理**	AM10	IT	不支持多因素身份验证的，用户帐户将被要求在系统上使用长的密码（长于 8 个字符）。	0:未使用长密码 1:- 2:- 3:- 4:已使用长密码	
	×	×		**资源**	**访问管理**	AM11	IT	确保所有帐户的用户名和认证证书在网络中使用加密的通道传输。	0:系统账户和证书采用明文传输 1:账户和证书采用软件功能加密传输（如压缩包加密等） 2:账户和证书采用互联网加密传输（如 CA 证书等） 3:账户和证书采用互联网、局域网通用加密传输（如 VPN 加密） 4:账户和证书采用私有协议加密传输	
×	×			**资源**	**资产管理**	AS1	IT	确认对所有系统证书文件进行了加密，这些文件仅限于管理员账户访问。	0:所有证书文件均未加密 1:部分证书文件已加密，但访客或临时用户组仍可访问 2:50%以下的证书文件已加密 3:50%以上的证书文件已加密 4:所有证书文件均已加密	
×				**资源**	**资产管理**	AS2	IT	对于采用动态主机配置协议（DHCP）分配地址的船舶网络，应自动存储网络配置日志。	0:采用 DHCP 时，未自动存储网络配置日志 1:- 2:未采用 DHCP 3:- 4:采用 DHCP 时，已自动存储网络配置日志	
×				**资源**	**资产管**	AS3	IT	利用访问控制和认证协议搭建网络，如 802.1x 协议，控制设备到网络的连接。	0:采用访问控制和认证协议 1:- 2:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
					理				3:- 4:采用访问控制和认证协议	
×	×			**资源**	**资产管理**	AS4	IT	在连接到船舶网络之前，应使用客户端证书来验证登录账户的有效性。	0:所有客户端不具备证书验证账户 1:网络中 50%以下的系统具备证书验证账户 2:- 3:网络中 50%以上的系统具备证书验证账户 4:所有客户端具备证书验证账户	
×	×			**资源**	**资产管理**	AS5	IT+OT	至少包括两个同步时间源，使所有的服务器和网络设备定期获取时间信息，并保持记录的时间戳一致。	0:不具备两个同步时间源 1:- 2:- 3:- 4:具备两个同步时间源	
×	×	×		**资源**	**资产管理**	*AS6	IT	船舶上的服务器已被设置在一个内部的 VLAN 中。	0:服务器未布置在 VLAN 中 1:- 2:- 3:- 4:服务器已布置在 VLAN 中	
×				**资源**	**标识与认证**	IA1	IT+OT	自动识别接入网络的所有系统清单，清单中至少记录设备的网络地址、机器名称。应计入清单的系统包括但不限于台式机、笔记本电脑、服务器、网络设备（路由器，交换机，防火墙等），打印机，存储区域网络，IP 电话、多宿主地址，虚拟地址，船用控制系统，通信导航系统等等。	0:不具备系统识别清单 1:- 2:具备系统识别清单，但经核对清单内容不满足要求 3:- 4:具备系统识别清单，且经核对，清单内容满足要求	
×	×	×		**资源**	**标识与认证**	IA2	IT+OT	对已识别的人员、组织、角色和设备进行标识，并授予相应的角色。制定标识管理办法，如禁止使用公共符号进行标识。	0:未标识 1:已具备标识管理办法但未执行 2:- 3:已标识但未具备标识管理办法 4:已标识且具备标识管理办法	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
×				**资源**	**配置管理**	*CM1	IT+OT	应建立网络环境的标准安全配置，配置中应记录接入网络的各系统版本，并实时更新。	0:不具备安全配置 1:- 2:具备安全配置，但不能实时更新 3:- 4:具备安全配置，且能实时更新	
×				**资源**	**配置管理**	CM2	IT+OT	船舶网络的基本配置和设置应能被自动记录，且易于追溯。	0:配置不能被自动记录并保存 1:- 2:- 3:- 4:配置能被自动记录并保存	
×	×	×		**资源**	**数据管理**	DM1	IT	对网络服务器、工作站、设备的远程管理应在安全的环境中进行，对于 telnet、VNC、RDP 等弱加密协议，仅允许在二次加密的网络环境下运行，如 SSL、TLS、IPSec。	0:网络设计未采用加密协议，或二次加密技术 1:- 2:- 3:- 4:网络设计采用加密协议，或二次加密技术	
×	×			**资源**	**数据管理**	*DM2	IT	应定期对数据进行自动备份，防止数据意外或不慎遗失。	0:不具备定期数据备份机制 1:- 2:- 3:- 4:具备定期数据备份机制	
×	×			**资源**	**数据管理**	DM3	OT	控制系统网络与其他系统网络之间应有流量（如通过 VPN 等访问）的监测保护装置/程序，以限制数据流量的类型、协议和数据源。	0:控制系统网络不具备流量保护装置/程序 1:- 2:- 3:- 4:控制系统网络具备流量保护装置/程序	
×	×			**资源**	**数据管理**	DM4	OT	流量的控制与识别应避免在控制系统的网络中进行。	0:不满足要求 1:- 2:- 3:- 4:满足要求	
×	×			**资**	**数**	DM5	IT	将公司、船员的隐私数据与其他数据	0:隐私数据未被隔离存储	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				源	**据管理**			的存储分离，以避免这部分数据的泄露。	1:- 2:- 3:- 4:隐私数据已被隔离存储	
×	×	×		**资源**	**数据管理**	DM6	IT	对访问隐私数据库的人员及系统用户权限予以严格限制。	0:未限制访问隐私数据库的权限 1:- 2:- 3:- 4:已限制访问隐私数据库的权限	
×	×			**资源**	**访问管理**	AM1	IT	确保所有无线通信至少利用高级加密标准（AES），且应至少使用 Wi-Fi 访问保护（WPA2）技术。	0:所有无线通信未利用高级加密标准 1:- 2:无无线设备 3:- 4:所有无线通信利用高级加密标准	
×	×			**资源**	**访问管理**	AM2	IT+OT	确保接入网络的每个系统仅开放必须的端口、协议和服务。	0:网络中存在端口、协议和服务的冗余开放 1:- 2:- 3:- 4:网络中不存在端口、协议和服务的冗余开放	
×		×		**资源**	**访问管理**	AM3	IT	确认无线网络通信应使用相应的安全认证协议（如 EAP/TLS 等）。	0:所有无线通信未利用安全认证协议 1:- 2:无无线设备 3:- 4:所有无线通信利用安全认证协议	
×	×	×		**风险**	**事故响应与应急**	*ER1	OT	当控制系统面临登录失败和/或锁定，以及断电、重启等事件时，不影响关键操作安全。	0:经验证不满足要求 1:- 2:- 3:- 4:经验证满足要求	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
×	×			风险	事故响应与应急	ER2	IT	确保每个系统都会自动备份至少每周一次，对于存储敏感信息的系统频率应更高。为了确保从备份中快速恢复系统的能力，操作系统、应用软件和机器上的数据应该被包含在整个备份过程中。	0:未按相应的频率、内容要求进行备份 1:自动备份至少每周进行一次，但未完全备份操作系统、应用软件和数据 2:网络中 50%以下的系统自动备份，且满足相应的备份频率、内容要求 3:网络中 50%以上的系统自动备份，且满足相应的备份频率、内容要求 4:网络中每个系统能够自动备份，且满足相应的备份频率、内容要求	
×	×			风险	防御管理	DE1	IT	船舶对外通信过程中，应具备对通信路径和内容进行筛查的功能，以检测和删除任何危险的文件、附件或链接。	0:不具备要求的筛查功能 1:- 2:- 3:- 4:具备要求的筛查功能	
×	×	×		风险	防御管理	DE2	IT+OT	系统能够在未经授权的配置更改时发出警报及提醒。这包括检测新的监听端口，新的管理用户，组和本地策略对象（如适用）的变化，以及在系统上运行的新服务。	0:系统不能够发出配置更改的警报及提醒 1:- 2:- 3:- 4:系统能够发出配置更改的警报及提醒	
×	×			风险	防御管理	DE3	IT+OT	任何未经授权的服务或数据传输应被封锁，并产生一个警报。	0:不具备要求的封锁功能 1:- 2:具备要求的封锁功能，不能发出警报 3:- 4:具备要求的封锁功能，且能发出警报	
×	×			风险	防御管理	DE4	IT	在网络路由器的 ACL(访问控制列表)上使用基于 DLP（数据丢失防护）系统。	0:未使用 DLP 系统 1:- 2:- 3:- 4:已使用 DLP 系统	
	×	×		风	风险	RA1	IT+OT	进行外部和内部渗透测试，以模拟可能出现的网络攻击。渗透测试应从外	0:未进行渗透测试 1:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				险	**评估**			部网络的周边（即，互联网或无线网络周围的组织），以及从其内部的边界（即，在内部网络）来模拟外部和内部人的攻击。	2:进行渗透测试，未定期封闭漏洞 3:- 4:进行渗透测试，并定期封闭漏洞	
	×	×		**风险**	**风险评估**	RA2	IT+OT	应监控任何用于执行渗透测试用户或系统帐户，以确保它们只被用于合法的目的，并在测试结束后删除系统账户。	0:未进行渗透测试 1:- 2:进行渗透测试，但未删除测试账户 3:- 4:进行渗透测试，并删除测试账户	
	×	×		**程序**	**建设管理**	SD1	IT+OT	确保应用程序中的开发构件（示例数据和脚本；未使用的库、组件、调试代码；或工具）不包括在部署的软件中，或在生产环境中访问。	0:开发构件不满足要求 1:- 2:- 3:- 4:开发构件满足要求	
×		×		**程序**	**建设管理**	SD2	IT+OT	应限制访问程序源代码。	0:不具备源代码访问保护、防止反编译的措施 1:- 2:- 3:- 4:具备源代码访问保护、防止反编译的措施	
×				**程序**	**建设管理**	SD3	IT+OT	开发、测试和运行环境应分离，以减少未授权访问或改变运行环境的风险。	0:开发、测试和运行环境未分离 1:- 2:- 3:- 4:开发、测试和运行环境分离	
×				**程序**	**管理程序**	MP1	IT+OT	船东/船舶管理公司与系统开发方的协议应包括信息和网络技术服务，以及相关网络安全风险处理的要求。	0:未签订协议 1:- 2:已签订协议，但不包括对网络风险的处理要求及程序 3:- 4:已签订协议，且包括对网络风险的处理要求及程序	

附录 4 船舶网络安全详细评估表（船舶）

Form CYBER-DS

评估申请方：　　评估系统：

评估方：　　评估日期：

注：1.需在打“X”的环节对评估要求予以关注。

2.编号标识含“”的为详细评估的必要项目（需完全满足评估要求）。*

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
	×	×		**资源**	**访问管理**	*AM1	IT+OT	确认网络中所有物理安全设备（摄像机、传感器、电子门锁、网络访问等）存在密码，并满足要求：（1）非默认；（2）非简单加密。	0:所有设备无密码保护 1:部分设备有密码保护，且为默认或简单加密 2:网络中 50%以下设备有密码保护，且为非默认或非简单加密 3:网络中 50%以上设备有密码保护，且为非默认或非简单加密 4:所有设备有密码保护，且为非默认或非简单加密	
	×	×		**资源**	**访问管理**	*AM2	IT+OT	保障系统和设备安全，限制访问关键系统、设备，仅授权人员具有适当访问权限。	0:系统和设备的访问无权限控制 1:部分系统和设备的访问有权限控制，但访客或临时用户组也可访问 2:网络中 50%以下系统和设备的访问有权限控制，且仅授权人员具备权限	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									3:网络中 50%以上系统和设备的访问有权限控制，且仅授权人员具备权限 4:所有系统和设备的访问有权限控制，且仅授权人员具备权限	
	×	×		**资源**	**访问管理**	AM3	IT	应采用适当的网络用户组策略，且在非组内用户访问网络时禁用共享功能。	0:不具备网络用户组策略 1:具备网络用户组策略，但非组内用户访问网络时共享功能未被禁用 2:具备网络用户组策略，但非组内用户访问网络时 50%以下的共享功能被禁用 3:具备网络用户组策略，但非组内用户访问网络时 50%以上的共享功能被禁用 4:具备网络用户组策略，且非组内用户访问网络时共享功能被禁用	
	×	×		**资源**	**访问管理**	*AM4	IT	在第三方（供应商、人员、程序）授权网络访问前，需进行审核，并定期对第三方（供应商、人员、程序）的访问权限进行审查，确认在可控范围内。	0:未定期审核第三方访问权限，不具备相应管理程序 1:- 2:- 3:- 4:定期审核第三方访问权限，具备相应管理程序	
	×	×		**资源**	**访问管理**	AM5	IT	第三方（供应商、人员）的访问，需使用双因素认证，或强密码。	0:第三方访问时无双因素认证/强密码 1:- 2:- 3:- 4:第三方访问时有双因素认证/强密码	
	×	×		**资源**	**访问管理**	AM6	IT	第三方（供应商、人员）的远程访问，需进行通信跟踪和登记的行为日志。	0:第三方访问时无通信跟踪手段和行为日志 1:- 2:- 3:- 4:第三方访问时有通信跟踪手段和行为日	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									志	
×	×	×		资源	访问管理	AM7	OT	针对接入网络的控制系统，限定特定的角色和用户登录。	0:所有控制系统未限定特定角色和用户 1:网络中 50%以下的控制系统限定特定角色和用户 2:无控制系统 3:网络中 50%以上的控制系统限定特定角色和用户 4:所有控制系统限定了特定角色和用户	
×	×	×		资源	访问管理	*AM8	IT	船舶网络应依据用户角色、工作职责分配系统和数据的访问权限。	0:未按照用户角色、职责分配权限 1:- 2:- 3:- 4:已按照用户角色、职责分配权限	
×	×	×		资源	访问管理	AM9	OT	管理人员应全面掌握和控制接入船舶网络的信息、控制、通信系统等组件，并设置系统白名单。	0:未设置网络组件白名单 1:- 2:- 3:- 4:已设置网络组件白名单	
	×	×		资源	访问管理	AM10	IT	过滤已知的恶意 IP 地址（黑名单）。	0:未过滤 IP 地址 1:- 2:- 3:- 4:已过滤 IP 地址	
	×	×		资源	访问管理	AM11	IT	存储在系统上的所有信息（文件系统、网络共享、应用程序或数据库）都应被保护，只有授权的个人有访问的权限。	0:所有系统文件未设置授权访问权限 1:部分系统文件设置了授权访问权限，但访客或临时用户组仍可访问 2:网络中 50%以下的系统文件设置了授权访问权限 3:网络中 50%以上的系统文件设置了授权访问权限	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									4:所有系统文件已设置授权访问权限	
	×	×		**资源**	**访问管理**	AM12	IT	所有系统帐户已禁用了任何与业务流程无关的帐户。	0:未禁用 1:- 2:- 3:- 4:已禁用	
	×	×		**资源**	**访问管理**	AM13	IT	确保所有的帐户都具备一个被监控和执行的有效期。	0:所有账户都不具备有效期 1:部分账户具备有效期，但管理中未予完全执行 2:网络中 50%以下的账户具备有效期 3:网络中 50%以上的账户具备有效期 4:所有账户都具备有效期，但管理中予以完全执行	
×	×	×		**资源**	**访问管理**	AM14	IT	配置网络系统中的屏幕锁以限制访问。	0:所有屏幕未配置屏幕锁 1:网络中 50%以下的系统配置屏幕锁 2:- 3:网络中 50%以上的系统配置屏幕锁 4:所有屏幕已配置屏幕锁	
×	×	×		**资源**	**访问管理**	AM15	IT	使用和配置帐户锁定，在尝试登录失败后，按标准时间锁定账户。	0:所有接入网络的系统不具备登录失败后的锁定功能 1:网络中 50%以下的系统具备登录失败后的锁定功能 2:- 3:网络中 50%以上的系统具备登录失败后的锁定功能 4:所有接入网络的系统具备登录失败后的锁定功能	
×	×	×		**资源**	**访问管**	AM16	IT	对有访问敏感数据或系统的所有用户帐户，需要多因素身份验证。多因素身份验证可以通过使用智	0:所有系统未设置多因素验证或密码 1:部分系统设置密码（短于 8 个字符） 2:网络中 50%以下的系统设置密码（长于	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
					理			能卡、证书、一次性密码（OTP）的标记，或生物识别技术。不支持多因素身份验证的，用户帐户将被要求在系统上使用长的密码（长于8个字符）。	8个字符），或使用多因素验证 3:网络中 50%以上的系统设置密码（长于8个字符），或使用多因素验证 4:所有系统已设置多因素验证或长密码（长于8个字符）	
	×			资源	资产管理	AS1	IT	船舶网络中应有一个扫描工具，通过该工具连接到网络环境中，并扫描 IPV4 或 IPV6 网络地址，初步识别出接入网络的主机设备。	0:不具备设备扫描工具 1:- 2:- 3:- 4:具备设备扫描工具	
×	×			资源	资产管理	AS2	IT	对于采用动态主机配置协议（DHCP）分配地址的船舶网络，应自动存储网络配置日志。	0:采用 DHCP 时，未自动存储网络配置日志 1:- 2:未采用 DHCP 3:- 4:采用 DHCP 时，已自动存储网络配置日志	
	×	×		资源	资产管理	AS3	IT	避免将虚拟计算机接入船舶网络。	0:有虚拟计算机接入船舶网络 1:- 2:- 3:- 4:无虚拟计算机接入船舶网络	
	×	×		资源	资产管理	AS4	IT	对外来系统及设备进行登记，并控制授权，限制移动存储介质、外部所有的系统/设备、网络可访问存储设备的使用。	0:未控制授权，不具备相应管理程序 1:已具备相应管理程序但未执行 2:- 3:已控制授权，不具备相应管理程序 4:已控制授权并具备相应管理程序	
	×	×		资源	资产管	AS5	IT	在独立的物理或逻辑主机上运行关键服务，如 DNS、文件、邮件、Web 和数据库服务。	0:未在独立主机上运行关键服务 1:- 2:- 3:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
					理				4:在独立主机上运行关键服务	
	×	×		资源	配置管理	CM1	IT	将配置文件存储在安全配置的服务器上，或离线机器上。	0:配置文件未按要求存储 1:- 2:- 3:- 4:配置文件已按要求存储	
	×	×		资源	配置管理	CM2	IT	对配置文件的所有更改都应在记录后上报给公司。	0:未上报公司 1:- 2:- 3:- 4:能够上报公司	
×	×	×		资源	数据管理	*DM1	IT	应定期对数据进行自动备份，防止数据意外或不慎遗失	0:不具备定期数据备份机制 1:- 2:- 3:- 4:具备定期数据备份机制	
×	×			资源	数据管理	DM2	OT	控制系统网络与其他系统网络之间应有流量（如通过 VPN 等访问）的监测保护装置/程序，以限制数据流量的类型、协议和数据源。	0:控制系统网络不具备流量保护装置/程序 1:- 2:- 3:- 4:控制系统网络具备流量保护装置/程序	
×	×			资源	数据管理	DM3	OT	流量的控制与识别应避免在控制系统的网络中进行。	0:不满足要求 1:- 2:- 3:- 4:满足要求	
×	×			资源	数据管理	DM4	IT	将公司、船员的隐私数据与其他数据的存储分离，以避免这部分数据的泄露。	0:隐私数据未被隔离存储 1:- 2:- 3:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									4:隐私数据已被隔离存储	
×	×			**资源**	**数据管理**	DM5	IT	对访问隐私数据库的人员及系统用户权限予以严格限制。	0:未限制访问隐私数据库的权限 1:- 2:- 3:- 4:已限制访问隐私数据库的权限	
	×	×		**风险**	**事故响应与应急**	ER1	IT	建立需要参与网络事件的响应人员联络单，联络单应包含船公司人员、网络系统实施方。	0:未建立网络事件联络单 1:- 2:- 3:- 4:已建立网络事件联络单	
×	×	×		**风险**	**事故响应与应急**	ER2	IT	确保每个系统都会自动备份至少每周一次，对于存储敏感信息的系统频率应更高。为了确保从备份中快速恢复系统的能力，操作系统、应用软件和机器上的数据应该被包含在整个备份过程中。	0:未按相应的频率、内容要求进行备份 1:自动备份至少每周进行一次，但未完全备份操作系统、应用软件和数据 2:网络中 50%以下的系统自动备份，且满足相应的备份频率、内容要求 3:网络中 50%以上的系统自动备份，且满足相应的备份频率、内容要求 4:网络中每个系统能够自动备份，且满足相应的备份频率、内容要求	
	×	×		**风险**	**事故响应与应急**	*ER3	IT	应具备保留备份历史文件的能力，以便在恶意软件感染事件发生时，可从感染事件前的备份恢复系统。	0:备份历史文件未妥善保存 1:- 2:- 3:- 4:备份历史文件妥善保存	
	×	×		**风**	**事**	ER4	IT	确保备份通过物理安全或加密的	0:未采用备份文件的保护措施	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				险	**故响应与应急**			保护。	1:- 2:- 3:- 4:已采用备份文件的保护措施	
	×	×		**风险**	**事故响应与应急**	ER5	IT	确保至少有一个不通过操作系统调用的、连续可定位的备份位置。	0:不具备要求的备份位置 1:- 2:- 3:- 4:具备要求的备份位置	
	×	×		**风险**	**防御管理**	DE1	IT	启用恶意代码防御功能，例如数据执行保护（DEP），地址空间布局随机化（ASLR），虚拟化/容器化等。	0:不具备要求的防御功能 1:- 2:- 3:- 4:具备要求的防御功能	
×	×			**风险**	**防御管理**	DE2	IT	船舶对外通信过程中，应具备对通信路径和内容进行筛查的功能，以检测和删除任何危险的文件、附件或链接。	0:不具备要求的筛查功能 1:- 2:- 3:- 4:具备要求的筛查功能	
	×	×		**风险**	**防御管理**	DE3	IT+OT	船舶应通过相应的设备与软件，对网络整体采取必要的安全监控措施。	0:不具备要求的安全监控设备或软件 1:- 2:- 3:- 4:具备要求的安全监控设备或软件	
	×	×		**风**	**防御**	DE4	IT	船舶应安装具有防病毒、反间谍软件、个人防火墙和入侵防御系统	0:不具备要求的防御系统 1:- 2:具备要求的防御系统，但不能够发送到	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				险	**管理**			（IPS）功能的工作站或服务器。所有的恶意软件检测事件应该被发送到公司的反恶意软件管理工具和事件日志服务器。	公司 3:- 4:具备要求的防御系统，且能够发送到公司	
	×	×		**风险**	**防御管理**	DE5	IT	启用域名系统（DNS）查询日志记录，以检测主机名、查找已知恶意域名。	0:未启用 DNS 1:- 2:- 3:- 4:已启用 DNS	
	×			**风险**	**防御管理**	DE6	IT	使用基于网络的反恶意软件工具来识别所有网络流量中的可执行文件，并使用基于签名的检测技术，在恶意内容到达端点前进行识别和过滤。	0:不能识别并检测网络流量中的可执行文件 1:- 2:- 3:- 4:能够识别并检测网络流量中的可执行文件	
	×	×		**风险**	**防御管理**	*DE7	IT	除经公司授权外，限制外接设备的使用。配置笔记本电脑、工作站和服务器，使它们不会从可移动介质（USB 令牌、USB 硬盘驱动器、CD/DVD、FireWire 设备、外部串行技术装置，以及网络共享设备等）自动运行。当可移动设备插入时，应自动进行反恶意软件扫描。	0:未限制外接设备的使用 1:- 2:限制外接设备的使用，但不具备反恶意软件扫描功能 3:- 4:限制外接设备的使用，且具备反恶意软件扫描功能	
	×			**风险**	**防御管理**	DE8	IT	当船舶使用入侵防御系统形成隔离网络（DMZ）时，配置监控系统，使在数据传输时，至少自动记录数据流量的主要信息。	0:存在被入侵防御系统隔离的网络，但不能记录数据流量的主要信息 1:- 2:不存在被入侵防御系统隔离的网络 3:- 4:存在被入侵防御系统隔离的网络，且能	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									记录数据流量的主要信息	
	×			风险	防御管理	DE9	IT	部署入侵检测系统、外网隔离系统网络,以通过签名、网络行为分析，或其他机制来分析数据流量。	0:未按要求部署隔离系统网络 1:- 2:- 3:- 4:按要求部署隔离系统网络	
	×			风险	防御管理	DE10	IT	应部署基于网络的 IPS（入侵防御系统）设备，并作为 IDS（入侵检测系统）的补充，阻断已知的恶意网络签名及潜在的攻击行为。	0:未按要求部署 IPS 系统 1:- 2:- 3:- 4:按要求部署 IPS 系统	
	×			风险	防御管理	DE11	IT	为了帮助识别通过防火墙的隐蔽数据，应配置防火墙会话跟踪机制，以定位异常的 TCP 会话连接。	0:不具备防火墙会话跟踪机制 1:- 2:- 3:- 4:具备防火墙会话跟踪机制	
	×			风险	防御管理	DE12	IT+OT	监控网络中所有数据流量。	0:不具备网络数据流量监控功能 1:- 2:- 3:- 4:具备网络数据流量监控功能	
	×			风险	防御管理	DE13	IT	配置网络漏洞扫描工具来检测连接到有线网络的无线接入点，且船上应有一个授权的无线接入点列表。	0:未配置漏洞扫描工具 1:- 2:- 3:- 4:已配置漏洞扫描工具	
	×			风险	防御管理	DE14	IT+OT	配置网络边界设备，包括防火墙、基于网络的 IPS、入站和出站代理，并详细记录所有控制装置的流量。	0:不能记录控制装置的流量 1:网络中 50%以下的控制装置流量能够被记录 2:- 3:网络中 50%以上的控制装置流量能够被	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									记录 4:能够记录所有控制装置的流量	
	×			风险	防御管理	DE15	IT	限制在所有的网络浏览器和电子邮件客户端中使用不必要的脚本语言。	0:网络浏览器和电子邮件客户端中未限制脚本语言的使用 1:- 2:- 3:- 4:网络浏览器和电子邮件客户端中限制了与系统无关的脚本语言的使用	
	×			风险	防御管理	DE16	IT+OT	在网络边界部署自动化工具，以定期监控敏感信息、关键词，以发现未授权的数据溢出。	0:未按要求部署定期监控工具 1:- 2:- 3:- 4:已按要求部署定期监控工具	
	×			风险	防御管理	DE17	IT	部署 Web 应用防火墙保护 Web 应用（WAFS），检测所有连接 Web 应用的常见攻击方式，包括但不限于跨站点脚本、SQL 注入、命令注入和目录遍历攻击等。对于不是基于 Web 的应用程序，应部署特定的应用程序防火墙。	0:未部署应用程序防火墙 1:- 2:- 3:- 4:已部署应用程序防火墙	
	×			风险	风险评估	RA1	IT	应能够记录所有的 URL 访问请求，以确定潜在的恶意活动，并协助事件处理程序识别潜在的妥协。	0:未记录 URL 访问请求 1:- 2:- 3:- 4:能够记录 URL 访问请求	
	×			风险	风险评估	RA2	IT	扫描并阻止含有恶意内容的，进入船舶网络的电子邮件附件。	0:邮件客户端不具备电子邮件附件扫描及阻止功能 1:- 2:- 3:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									4:邮件客户端具备电子邮件附件扫描及阻止功能	
	×	×		风险	风险评估	RA3	IT	当需使用 USB 驱动器写入数据时，船舶应仅允许特定的设备访问，且应保留所有 USB 设备的授权记录。	0:未限制 USB 访问设备，且未保留授权记录 1:- 2:已限制 USB 访问设备，但未保留授权记录 3:- 4:已限制 USB 访问设备，且已保留授权记录	
×	×			风险	风险评估	RA4	IT	在网络路由器的 ACL(访问控制列表)上使用基于 DLP（数据丢失防护）系统。	0:未使用 DLP 系统 1:- 2:- 3:- 4:已使用 DLP 系统	
	×	×		风险	风险评估	RA5	IT	对已确定业务需要，并已接入的无线设备，应仅允许访问授权的无线网络。对于不需要无线业务的主机，在其配置中禁用无线网络。	0:所有设备未限制无线网络的特定授权与使用 1:网络中 50%以下的设备按要求限制无线网络的特定授权与使用 2:无无线设备 3:网络中 50%以上的设备按要求限制无线网络的特定授权与使用 4:所有设备按要求限制无线网络的特定授权与使用	
×	×			风险	风险评估	RA6	IT	确保所有无线通信至少利用高级加密标准（AES），且应至少使用 Wi-Fi 访问保护（WPA2）技术。	0:所有无线通信未利用高级加密标准 1:- 2:无无线设备 3:- 4:所有无线通信利用高级加密标准	
×	×			风	风	RA7	IT	确认无线网络通信应使用相应的	0:所有无线通信未利用安全认证协议	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
				险	险评估			安全认证协议（如 EAP/TLS 等）。	1:- 2:无无线设备 3:- 4:所有无线通信利用安全认证协议	
	×	×		风险	风险评估	RA8	IT	除业务需要外，禁用无线外设访问的设备（如蓝牙）。	0:未禁用 1:- 2:- 3:- 4:已禁用	
	×	×		程序	建设管理	SD1	OT	保持控制和非控制系统环境的独立，不允许系统开发方监控控制系统。	0:系统开发方可以监控控制系统 1:- 2:- 3:- 4:系统开发方不可以监控控制系统	
	×	×		程序	建设管理	SD2	IT+OT	应识别接入船舶网络，进行信息处理的设施资产，编制并维护这些资产的清单。	0:未编制资产清单 1:- 2:- 3:- 4:编制资产清单	
	×	×		程序	建设管理	SD3	IT+OT	设备的使用应加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。	0:设备的存储容量不具有冗余度，对系统性能已造成影响 1:- 2:- 3:- 4:设备的存储容量具有一定的冗余度，以保证系统的正常运行	
	×	×		程序	建设管理	SD4	IT+OT	为防止自然灾难、恶意攻击或事件，应设计和采取物理保护措施。	0:对于存在被破坏风险的基础设施，未采取相应的物理保护措施 1:- 2:- 3:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									4:对于存在被破坏风险的基础设施，已采取相应的物理保护措施	
		×		程序	建设管理	SD5	IT	对影响信息安全的人员、业务过程、信息处理设施、系统、供应商服务等的变更应加以控制。	0:公司不具备针对系统变更的控制程序 1:- 2:- 3:- 4:公司具备针对系统变更的控制程序	
	×	×		程序	建设管理	SD6	IT	记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。	0:网络安全日志未受到保护，或无网络安全日志 1:- 2:- 3:- 4:网络安全日志受到保护	
	×	×		程序	人员管理	PE1	IT+OT	上述清单中所维护的资产应分配所有权和安全职责，并落实管理责任人。	0:未按要求实施 1:- 2:- 3:- 4:按要求实施	
	×	×		程序	人员管理	PE2	IT	公司的所有人员（必要时包括第三方人员），应受到适当的网络安全意识及安全策略的定期培训。	0:公司从未组织网络安全定期培训 1:- 2:公司组织网络安全培训，但并未制度化 3:- 4:公司组织网络安全定期培训	
	×	×		程序	管理程序	*MP1	IT	公司应建立系统实施和维护程序，并将其文件化。	0:未按要求建立程序 1:- 2:- 3:- 4:已按要求建立程序	
	×			程序	管理程	MP2	IT	船岸间应有正式的信息传输策略、程序和控制措施，以保护通过使用各种类型通信设施的信息传输。	0:未编制船岸通信管理操作程序 1:- 2:-	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
					序				3:- 4:编制船岸通信管理操作程序	
	×			程序	管理程序	MP3	IT	船东/船舶管理公司与系统开发方的协议应包括信息和网络技术服务，以及相关网络安全风险处理的要求。	0:未签订协议 1:- 2:已签订协议，但不包含对网络风险的处理要求及程序 3:- 4:已签订协议，且不包含对网络风险的处理要求及程序	
	×			程序	管理程序	MP4	IT	网络安全策略应由公司定义、批准、发布并传达给员工和相关外部方。	0:未按要求发布安全策略 1:- 2:- 3:- 4:按要求发布安全策略	
		×		程序	管理程序	MP5	IT	应定期评审船舶网络是否符合公司的安全政策和相关标准。	0:未按要求进行定期评审 1:- 2:- 3:- 4:按要求进行定期评审	
	×			程序	管理程序	MP6	IT	在访问控制策略要求下，对操作系统和应用的访问应通过安全登录程序加以控制。	0:不具备安全登录程序 1:- 2:- 3:- 4:具备安全登录程序	
	×			程序	管理程序	MP7	IT	应实施相应的程序来保护远程访问、处理或存储的信息。	0:有远程访问功能，但不具备远程访问程序 1:- 2:无远程访问功能 3:- 4:有远程访问功能，且具备远程访问程序	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
	×			程序	管理程序	MP8	IT	应制定和实施网络管理和控制程序，以保护系统中信息和应用程序的安全。	0:不具备网络管理和控制程序 1:- 2:- 3:- 4:具备网络管理和控制程序	
	×	×		程序	管理程序	MP9	IT	对于可能超越船舶网络控制程序的软件的使用应加以限制。	0:存在超越船舶网络控制程序的软件，但在管理中未予限制 1:- 2:不存在超越船舶网络控制程序的软件 3:- 4:存在超越船舶网络控制程序的软件，并在管理中予以限制	
	×	×	×	程序	管理程序	MP10	IT	应按照公司所采纳的信息分类机制建立和实施处理资产的程序。	0:公司不具备船舶网络基础设施的资产处理程序 1:- 2:- 3:- 4:公司具备船舶网络基础设施的资产处理程序	
	×	×	×	程序	管理程序	MP11	IT	应按照公司所采纳的分类机制实施可移动介质的管理程序。	0:公司不具备船舶网络中可移动介质的管理程序 1:- 2:- 3:- 4:公司具备船舶网络中可移动介质的管理程序	
		×		程序	管理程序	MP12	IT	在岗位终止或变更后对网络角色予以调整。	0:未按要求及时调整用户角色 1:- 2:- 3:- 4:按要求及时调整用户角色	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
	×	×		程序	管理程序	MP13	IT	应定期评审并记录公司信息的保密性要求。	0:公司未定期评审信息保密要求 1:- 2:- 3:- 4:公司定期评审信息保密要求	
	×	×		程序	管理程序	MP14	IT	应有控制在船舶网络中安装软件的程序。	0:不具备相应的控制程序 1:- 2:具备相应的控制程序，但未按要求实施 3:- 4:具备相应的控制程序，且按要求实施	
		×	×	程序	管理程序	MP15	IT	公司应定期评审已实施网络安全连续性计划的控制程序，以确保在任何情况下控制程序的及时性和有效性。	0:公司未定期评审控制程序 1:- 2:公司进行过控制程序的评审，但未形成制度 3:- 4:公司定期评审控制程序	
	×	×		程序	管理程序	MP16	IT	应产生记录用户活动、异常情况、故障和网络安全的事件日志，并保持定期评审。	0:公司对相应的网络安全日志未进行评审，或无网络安全日志 1:- 2:公司对相应的网络安全日志进行评审，但未形成制度 3:- 4:公司对相应的网络安全日志予以定期评审	
		×		程序	运维管理	OM1	IT	应及时得到现有系统的技术缺陷及漏洞，评价公司对这些缺陷及漏洞的暴露程度，并采取适当的措施来处理相关的风险。	0:公司不能够及时得到船舶网络存在的漏洞信息 1:- 2:公司能够及时得到船舶网络存在的漏洞信息，但未采取相应的措施进行维护 3:- 4:公司能够及时得到船舶网络存在的漏洞	

生命周期				分类别	子类别	编号	应用系统	评估内容	评估指标	得分
系统设计	系统实施	系统运行	系统退役							
									信息，且已采取相应的措施进行维护	
			×	程序	运维管理	OM2	IT	不再需要的介质，应使用正式的程序可靠并安全地处置。	0:公司不具备设备报废程序 1:- 2:- 3:- 4:公司具备设备报废程序	
			×	程序	运维管理	OM3	IT	包含储存介质的设备应进行验证，以确保在报废处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。	0:未按要求处置报废设备 1:- 2:- 3:- 4:按要求处置报废设备	
		×		程序	运维管理	OM4	IT	网络安全事件应尽可能快地响应，并通过适当的管理渠道向有关方报告。	0:未按要求报告网络安全事件 1:- 2:- 3:- 4:按要求报告网络安全事件	
	×	×		程序	运维管理	OM5	IT	应具有与网络安全事件响应相一致的文件化程序。	0:不具备相应的管理程序 1:- 2:- 3:- 4:具备相应的管理程序	

附录 5 船舶网络安全详细评估基线值

1.产品：

评估对象⑦		资源	风险	程序
IT	基线值	62	17	10
	总分	104	28	16
	必要项目	AM1、AM4、AM6、AS6、CM1、DM2	-	-
OT	基线值	31	12	10
	总分	52	20	16
	必要项目	AM1、AM4、AM6、CM1	ER1	-

2.船舶：

评估对象		资源	风险	程序
IT	基线值	58	72	67
	总分	96	120	112
	必要项目	AM1、AM2、AM4、AM8、DM1	ER3、DE7	MP1
OT	基线值	14	10	12
	总分	24	16	20
	必要项目	AM1、AM2	-	-

*1.基线分值代表网络系统产品或船舶网络系统在详细评估阶段应达到的基本分数。

2.IT 与 OT 的评估达到各自的基线值时，认为评估结果满足要求。

3.

附录 6 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：

1） IT系统

资源：**分

程序：**分

风险：**分

2） OT系统

资源：**分

程序：**分

风险：**分

3. 评估过程描述：

4. 评估结论：

详细评估结果满足/不满足本社《船舶网络系统要求及安全评估指南》有关要求。

5. 改进措施：

6. 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 7 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：

2.1. 预评估

资源：**分

程序：**分

风险：**分

2.2. 详细评估

1） IT系统

资源：**分

程序：**分

风险：**分

2) OT系统

资源：**分

程序：**分

风险：**分

3. 评估过程描述：

4. 评估结论：

预评估结果满足/不满足本社《船舶网络系统要求及安全评估指南》有关要求。

详细评估结果满足/不满足本社《船舶网络系统要求及安全评估指南》有关要求。

5. 改进措施：

6. 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 _____

时　间
Issued on _____

_____
中 国 船 级 社
CHINA CLASSIFICATION SOCIETY

注：☒ — 适用　　☐ — 不适用

* 不适用者划去

附录 8 船舶工控系统防火墙设置附加建议

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

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

下面是通用规则：

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

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

下面是防火墙规则制定中要特别注意的：

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