

中国造船工程学会标准制修订项目立项申请书

项目名称（中文）	船舶整船及 CBS 网络安全测试方法		
项目名称（英文）	Test methods for ship-wide and CBS cybersecurity		
制修订	☒ 制定 ☐ 修订	被修订标准号	
被修订标准名称		编制周期	☐ 12 个月 ☐ 18 个月 ☒ 其他 <u>6 个月</u>
起草单位 （不少于 3 家）	招商局工业智能科技（江苏）有限公司、中国船级社、水上载运装备安全研究院（宁波）有限公司、上海交通大学、江苏科技大学、上海研途船舶海事技术有限公司		
联系人	何慕之	地址	上海市嘉定区银翔路 819 弄 1 号楼 18f
电话	15821729073	邮箱	hemuzhi@cn-syst.com
技术与市场发展背景	一、船舶网络安全威胁日趋严峻 随着船舶数字化、智能化程度的不断提升，船载计算机系统（CBS）在船舶推进、导航、操舵、电站管理、货物管理等核心功能中的广泛应用，船舶已从传统的孤立系统演变为高度互联的信息物理系统。这一发展趋势在提升运营效率的同时，也使得船舶面临日益严峻的网络安全风险。 近年来，涉及船舶、港口、码头的网络攻击事件时有发生。2023 年 1 月，挪威船级社 DNV 的船队管理和运营平台“ShipManager”遭受勒索软件攻击，影响约 70 家客户公司和约 1000 艘船舶。同年的另一起事件中，美国船舶制造巨头宾士域集团因网络安全事件蒙受高达 8500 万美元（约合人民币 6.1 亿元）的损失。2021 年 9 月，南非码头运营商 Transnet 受到勒索软件攻击；2020 年 4 月，地中海航运（MSC）遭恶意软件攻击，进一步凸显了网络安全的重要性。 有别于常见的办公信息系统网络安全，船舶网络安全更侧重于操作技术（OT）类船舶计算机控制设备。网络事件可能直接影响船舶航行安全、人命安全、海上环境保护以及业务数据安全，可能造成极为严重的后果。船舶网络安全是守护生命、环境与贸易畅通的战略要务。 二、国际法规强制实施，行业进入“网络安全新纪元” 为应对日益增长的船舶网络安全风险，国际船级社协会（IACS）于 2022 年发布 UR E26《船舶网络韧性》（Cyber Resilience of Ships）和 UR E27《船载系统和设备网络韧性》（Cyber Resilience of On-Board Systems and Equipment），这两项要求是船舶行业首个强制性网络安全标准，其核心目标是建立船舶网络韧性，确保关键系统在遭受网络攻击时具备有效防护能力，并在事件发生后能够实现		



	快速恢复与持续运行。 UR E26 和 UR E27 构建了船舶网络安全的“双支柱”——前者锚定整体韧性，后者锁定设备安全，推动行业从被动防御转向韧性增强建设。2023 年发布的 Rev.1 版本进一步明确：2024 年 7 月 1 日及之后签约建造的国际航行客船、500 总吨及以上货船、高速船、海上移动式钻井平台等船舶，必须满足最低网络安全要求。鉴于 IACS 成员拥有全球 90%以上入级船舶，不满足新规要求的船舶将无法进入国际航运市场，海事行业由此迈入了网络安全新纪元。 三、行业痛点：有要求，无方法 目前 CCS《船舶网络安全指南》（2025 版）虽已系统规定了船舶和 CBS 的网络安全技术要求，IACS UR E26/E27 亦明确了船舶应具备的网络安全能力，但上述文件均定位于“要求”而非“测试方法”，未规定如何通过系统化的测试手段验证这些要求的符合性。目前在船舶网络安全测试领域，尚无任何标准统一规定测试项目、测试深度、测试方法及结果判定准则，各相关方在开展网络安全符合性验证时无据可依。这一“有要求、无方法”的局面，已成为制约船舶网络安全要求有效落地的关键瓶颈。 四、市场需求快速增长 从市场规模来看，全球海事网络安全市场正以显著速度扩张。根据市场研究机构 Fortune Business Insights 发布的报告，2025 年全球海事网络安全市场规模已达 46.8 亿美元，预计将从 2026 年的 52.6 亿美元增长至 2034 年的 130.6 亿美元，预测期内复合年增长率为 12.0%。另有市场研究机构 Value Spectrum 预测，全球海事网络安全市场将从 2024 年的 36.8 亿美元增长至 2029 年的 65.5 亿美元，复合年增长率为 12.4%。尽管上述数据涵盖港口、航运公司 IT 系统等更广泛的海事领域，但其增长趋势充分反映了船舶网络安全需求的迫切性。 随着 IACS UR E26/E27 的强制实施，船舶产业链条上的船东、设计院与船厂、系统集成商、产品供应商、船级社等各相关方都需要按照新要求开展设计、建造、运营和验证工作。在此背景下，一套系统化、可操作、可复现的整船及 CBS 网络安全测试方法标准，已成为行业各方的共同期盼。
标准必要性和可行性	一、必要性 1. 填补国内整船及 CBS 网络安全测试标准空白 目前国内尚无专门针对船舶整船及 CBS 网络安全测试方法的团体标准、行业标准或国家标准。CCS《船舶网络安全指南》侧重于技术要求和分级体系，IACS UR E26/E27 提出了目标要求，但均未提供系统化的测试方法。本标准将填补这一空白，为船舶网络安全符合性验证提供统一、可操作的技术依据。 2. 支撑 IACS UR E26/E27 的强制实施 UR E26/E27 已对 2024 年 7 月 1 日之后签约建造的新船强制生效。然而，新规仅给出了原则性规定，在执行层面缺少具体实施要求，国内外也无成熟经验和案例可以借鉴。船厂、设备供应商和船东亟需一套系统化的测试方法来验证产品及整船的网络安全合规性。本

标准将为行业提供可直接操作的测试技术规范，有效支撑 UR E26/E27 的落地实施。

3. 与 CCS《船舶网络安全指南（2025）》、IACS UR E26、UR E27 保持技术协调统一

本标准与 CCS《船舶网络安全指南（2025）》、IACS UR E26、UR E27 保持技术协调统一。IACS UR E26/E27 规定船舶网络韧性目标要求，CCS 指南规定船舶网络安全检验原则；本标准定位为配套测试方法团体标准，不新增安全能力要求，重点解决“如何验证是否达到上述文件规定的安全能力”；标准测试输出的缺陷分级、测试结论可支撑船级社 FAT、SAT、设备型式验证检验工作，与现有船级检验实践形成互补，不替代 CCS 指南及 IACS UR 系列要求。

4. 服务船舶工业高质量发展和国家战略需求

船舶网络安全是智能船舶、自主船舶发展的基础保障。工业和信息化部明确提出，要加快数字技术、绿色技术和人工智能赋能，强化标准引领，建设先进的研发体系、制造体系和产业体系。交通运输部等七部门联合印发的《关于“人工智能+交通运输”的实施意见》亦提出了加快智能产品创新的重点任务。建立完善的船舶整船及 CBS 网络安全测试标准体系，有助于提升我国船舶工业的核心竞争力和国际话语权，支撑我国从造船大国向造船强国迈进。

5. 保障国家海事安全与海洋权益

船舶网络攻击可能导致推进失控、导航失灵、货物泄漏等灾难性后果。通过标准化的测试方法系统性识别和消除船舶网络安全隐患，能够有效降低网络事件对船舶安全运营的威胁。

二、可行性

1. 方法学基础成熟，国内外标准可借鉴

本标准技术内容可基于 GB/T 35673《工业通信网络 网络和系统安全 系统安全要求和安全等级》（等同采用 IEC 62443-3-3）的系统要求（SR）体系、IACS UR E26/E27 的船舶网络安全要求以及 IEC 62443 系列标准，以标识和鉴别（IAC）、使用控制（UC）、系统完整性（SI）、数据保密性（DC）、受限数据流（RDF）、事件及时响应（TRE）、资源可用性（RA）七大基本要求为测试框架构建了完整的测试方法框架。

2. 行业需求迫切，应用前景广阔

随着 UR E26/E27 的强制实施，船舶产业链各相关方对网络安全测试方法的需求日益迫切。CCS 已组织开展系列船舶网络安全培训和宣贯工作。本标准可广泛应用于船舶设计建造环节的设备选型和系统集成验证、设备认证环节的产品网络安全能力认证、船舶检验环节的 FAT/SAT 及营运检验，应用场景清晰、市场前景广阔。

3. 政策环境有利，标准体系协同

国家层面积极推动船舶网络安全标准体系建设。我国已主导发布 ISO 23799:2024《船载网络安全风险评估方法》，国家标准计划《船舶与海上技术 船载网络安全风险评估方法》正在批准中。CCS 三部网络安全指南（2025）已正式生效。本标准的制定将与上述标准形成有机协同，进一步完善我国船舶网络安全标准体系。



	本标准充分考虑不同测试应用场景差异，将测试划分为实验室仿真靶场测试、新船 FAT/SAT 测试、营运实船测试，针对不同场景设置测试项裁剪约束；对于资源受限的船载嵌入式 CBS 设备，规定基于风险评估的测试裁剪原则：高安全风险 CBS 的基础系统要求(SR)原则上不允许裁剪，仅可对增强要求（RE）依据风险评估做合理裁剪，裁剪理由完整记入测试报告，保障不同类型船载设备测试方法具备可落地性。
国内外情况 简要说明	国际层面：IACS UR E26 (Rev.1)《船舶网络韧性》和 UR E27 (Rev.1)《船载系统和设备网络韧性》规定了船舶和 CBS 的网络安全要求，2024 年 7 月 1 日起强制实施。上述要求的技术基础主要源自 IEC 62443-3-3（系统安全要求与安全等级）和 IEC 62443-4-2（组件技术安全要求），形成了从通用工控安全到船舶行业落地应用的标准传导链条。IMO MSC-FAL.1/Circ.3/Rev.3《海事网络风险管理指南》提供了高层级的风险管理框架，ISO 23799:2024《船舶与海洋技术 船载网络安全评估》在此基础上进一步规定了从资产识别、威胁分析、脆弱性评估到风险量化计算的完整方法，为船舶确定目标安全等级（SL-T）提供了方法论基础。目前国际上尚无专门针对船舶网络安全的完整测试方法标准。然而，上述国际标准均侧重于规定“应达到什么要求”或“如何评估风险”，目前尚无专门针对船舶网络安全“如何测试验证”的完整测试方法标准。 国内层面：CCS《船舶网络安全指南》（2025）规定了船舶和 CBS 的网络安全要求及检验要求。CCS《船舶网络防火墙检验指南》和《船舶网络交换机检验指南》（2025 版）同期生效。等同采用 ISO 23799 国家标准《船舶与海上技术 船载网络安全风险评估方法》已进入批准阶段。GB/T 35673-2017（等同 IEC 62443-3-3）为工业通信网络安全系统安全提供了基础技术框架。上述标准共同构成了从“要求”到“评估”的技术支撑体系，但在“测试验证”环节仍存在空白——目前国内尚无船舶整船及 CBS 网络安全测试方法的专项标准，导致各方在开展符合性验证时缺乏统一的技术依据。
标准适用范围 和主要技术内容	一、适用范围 本标准适用于新建船舶和现有船舶的整船及 CBS 网络安全符合性验证。本文件不涉及船上涉密信息系统的保密性测试。 三、主要技术内容 本标准规定了船舶整船及 CBS 网络安全测试方法，包括测试对象与等级、测试准备与条件、CBS 级测试方法、整船级测试方法以及测试判断准则。主要技术内容如下： （1）测试对象与等级：将测试划分为 CBS 级和整船级两个层级；规定了测试 CBS 的识别原则，以及通过风险评估确定测试项目的方法。 （2）测试准备与条件：规定 CBS 级和整船级测试准备及测试工作环境要求。 （3）CBS 级测试方法：覆盖标识和鉴别（IAC）、使用控制（UC）、系统完整性（SI）、数据保密性（DC）、受限数据流（RDF）、事件及时响应（TRE）、资源可用性（RA）七大基本要求共 40 余项安全

	能力的测试方法，以及网络设备专项测试（ND）。 （4）整船级测试方法：规定网络分段与边界防护、网络风暴、渗透测试、应急响应与恢复、本地独立操作、冗余与容错、管理与流程、网络配置与监控、数据保密性与使用集成等 10 大类整船级测试方法； （5）测试判断准则：规定缺陷级别划分（A/B/C/D 四级）和测试结果判定准则（通过/有条件通过/不通过）。
工作进度安排	草案提交：2026 年 7 月 预期立项：2026 年 8~9 月 预期发布：2026 年 12 月
标准预期实施应用方案	1. 船舶设计建造环节。本标准可作为新建船舶网络安全设计的验证依据，在船舶设计、设备选型、系统集成等阶段指导网络安全测试工作的开展。 2. 设备认证环节。本标准可作为船载计算机系统及网络设备网络安全能力认证的测试依据，支撑设备供应商进行产品级的网络安全合规验证。 3. 船舶检验环节。本标准可作为船级社开展船舶网络安全检验的技术依据，支撑 FAT（工厂验收测试）、SAT（现场验收测试）及营运检验中的网络安全测试工作。 4. 行业推广。通过中国造船工程学会的平台优势，面向会员单位和行业企业开展标准宣贯和培训，推动标准在船舶行业的广泛应用。
经费保障	提供团体标准编制所需的经费。（含学会标准管理费用、标准编制过程中因技术交流、调研等发生的差旅费、会议费、审查费、专家咨询费等）。
技术基础及研究团队	本标准技术内容基于 GB/T 35673《工业通信网络 网络和系统安全 系统安全要求和安全等级》（等同采用 IEC 62443-3-3）的系统要求(SR)体系、IACS UR E26/E27 的船舶网络安全要求以及 IEC 62443 系列标准，以标识和鉴别（IAC）、使用控制（UC）、系统完整性（SI）、数据保密性（DC）、受限数据流（RDF）、事件及时响应（TRE）、资源可用性（RA）七大基本要求为测试框架构建了完整的测试方法框架。 主编单位招商局工业智能科技（江苏）有限公司（简称“招商智科”）是招商局集团旗下招商船舶工业集团所属全资子公司。公司围绕船舶智能化控制技术和岸端数字化两个方向布局，是招商船舶工业集团智能化、数字化业务的资源整合和市场转化平台。在船舶网络安全领域，招商智科已取得多项标志性成果：2024 年底成功获取中国船级社（CCS）江苏分社颁发的船舶网络防火墙型式认可证书，系江苏省首份；2025 年 12 月申请了基于数字孪生的船舶网络安全靶场仿真装置及实验平台发明专利，该装置可有效提升测试的有效性、全面性和一致性；2026 年成功中标山东港口陆海装备集团海工公司 12600DWT 多用途船用网络安全系统采购项目。在网络安全测试服务方面，公司已具备漏洞扫描、渗透测试、压力负载、网络风暴、性能测试、访问控制及提权测试、密码完整性测试等多项测试能力。

	起草成员熟悉 GB/T 35673、IEC 62443、IACS UR E26/E27 等国内外标准，已积累多个 CBS 系统和整船网络安全测试的实船数据与经验，能够为标准编制提供充分的实践支撑。		
申请立项单位 意见	(盖章) 2026 年 9 月 15 日		
标准化学术 委员会意见	(签名、盖章) 年 月 日	中国造船工 程学会意见	(签名、盖章) 年 月 日

注：如本表空间不够，可另附页。

