文章编号:1671-4598(2023)02-0129-06 DOI:10.16526/j.cnki.11—4762/tp.2023.02.020 中图分类号:TP311 文献标识码:A

舰船电站网络控制系统可信性分析设计技术

张 峰[1],吴立金[2]
(1.中国人民解放军91404部队,河北 秦皇岛 066001;
2.中国船舶集团有限公司 综合技术经济研究院,北京 100081)

摘要:舰船电站网络控制系统由分层、局部向扁平、全局方向发展,信息安全问题可能直接导致功能安全失效,迫切需要开展相应的可信性分析设计;针对舰船电站网络控制系统面临的功能安全、信息安全等可信问题,通过从舰船电站网络控制系统中的系统、数据、网络3方面分析了可信性风险与设计需求,提出了相应的舰船电站网络控制系统可信性分析技术、数据可信性设计技术和网络可信性设计技术,保障舰船电站网络控制系统的可信性,为舰船电站网络控制系统研制过程中开展可信性分析设计提供了技术支撑。

关键词:网络控制系统;可信性设计;控制系统可信;网络可信;数据可信

Credibility Analysis and Design Technology of Ship Power Station Network Control System

ZHANG Feng[1], WU Lijin[2]
(1. No. 91404 Troops of PLA, Qinhuangdao 066001, China;
2. China Institute of Marine Technology&Economy, Beijing 100081, China)

Abstract: The network control system of ship power station is developing from layered, local to flat and global direction. A information security problem may directly lead to functional safety failure, and it is urgent to carry out the corresponding credibility analysis and design. Aiming at the credibility problems such as functional safety and information security of the ship power station network control system, the credibility risk and design requirement are analyzed from the system, data and network, and the credibility technologies of system analysis, data design and network design are proposed to ensure the credibility of the ship power station network control system, which provides the technical support for the credibility analysis and design of the equipment network control system.

Keywords: network control system; credibility design; control system credibility; network credibility; data credibility

0 引言

当前,控制系统正向网络化、分布化、智能化方向发展。分布式控制系统(DCS)、工业以太网、现场总线控制系统(FCS)均为典型的网络控制系统。随着网络控制系统技术发展,封闭环境逐渐打破,功能安全和信息安全问题关联交织,亟需考虑系统可信性[1]。例如,2013年“震网”蠕虫病毒攻击伊朗的铀浓缩设备,造成伊朗核电站推迟发电。2014年土耳其境内的伊拉克向土耳其输出原油的输油管道由于黑客关闭了报警、切断了通信联系,给管道内的原油大量增压,引发爆炸,然而在爆炸将管道破坏前,却没有引发一个遇险信号。2021年4月11日,“以色列网络袭击”使伊朗纳坦兹核设施的电力系统发生故障。

可信性是系统需要时按要求执行的能力包括可靠性、可用性、恢复性、维修性,以及在某种情况下如耐久性,安全性和安保等其他特性。舰船电站网络控制系统是应用在装备中的典型网络控制系统,如何对应用在装备中的网络控制系统进行可信设计、提高系统安全运行能力,是当前装备研制中面临的重要问题。以舰船电站网络控制系统为典型对象,面向网络控制系统可信性技术现状,从设备与控制系统、数据、网络3方面分析了可信性需求,提出了对应的可信性设计技术,通过配置网络内部及其边界防护方案,审计网络中数据的使用、保证设备、系统和芯片的安全可控;实时感知内部、外部的安全风险,建立响应恢复机制,及时应对可信威胁,为提升装备网络控制系统可信性提供技术支撑。

1 舰船电站网络控制系统结构及原理

舰船电站网络控制系统是一个集散型控制系统,由信息管理层、监测控制层、现场设备层共3层构成,如图1所示。

舰船电站网络控制系统原理是:现场设备层、监测控制层通过现场总线技术形成分布式控制网络,通过现场总线、信息集成等技术对发电机组进行运行控制、信息共享;信息管理层通过网关与现场总线连接,与控制设备交互信

收稿日期:2022-07-04; **修回日期**:2022-08-02。
作者简介:张 峰(1979-),男,河北昌黎人,大学本科,高级工程师,主要从事软件试验和测评技术方向的研究。
通讯作者:吴立金(1987-),男,山东潍坊人,硕士,高级工程师,主要从事软件可信性与测评技术方向的研究。
引用格式:张 峰,吴立金.舰船电站网络控制系统可信性分析设计技术[J].计算机测量与控制,2023,31(2):129-134.

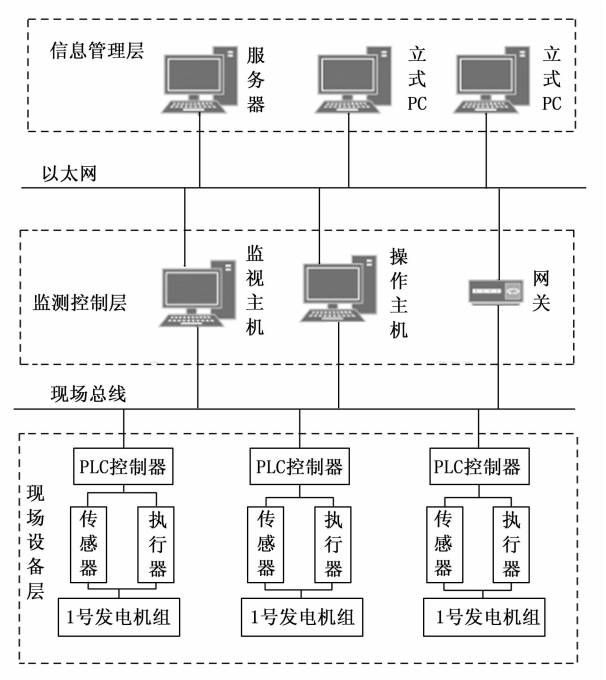

图 1 舰船电站网络控制系统结构

息[2]，通过网络控制技术实现了舰船电站一体化管控[2-12]。

网络控制协议在各种网络控制系统中得到广泛部署，如 OPC 协议、Modbus 协议、DNP3 协议、Profinet 协议等，这些协议用于控制网络的不同区域；提供不同的验证数据完整性和可信性的方法，网络控制系统常见的组网方式如表 1 所示。

表 1 网络控制系统组网方式

网络类型	组网方式
内有线网络	现场总线
	工业以太网
	工业 PON(无源光网络)
	时间敏感网络 TSN
	确定性网络 DetNet
无线网络	MulteFire
	5G URLLC
SDN 网络	软件定义网络(SDN)
广域有线网络	MPLSVPN 网络
	基于 OTN 的传输专网
	云化专线 CloudVPN
	软件定义的广域网(SD-WAN)
广域无线网络	LTE
	NB-loT
	5G

舰船电站网络控制系统实时性、同步通信等特殊需求使其更容易受到干扰影响。网络控制系统漏洞的类型分别广泛，包括跨站脚本、数字错误、代码注入等 30 多种，其中缓冲区溢出、输入验证和信息泄露是出现最多的漏洞类型[13-14]。当前，网络控制系统中，针对控制协议的恶意软件增多；对装备的运行使用造成严重影响。随着数据为中心（数据驱动、共享）的控制互联，数据可信对装备运行使用越来越重要。系统软件、网络技术从专有到通用，控制环境开放化（IT 和 OT 融合），控制系统、运行设备、智能终端等面临严峻的安全可信挑战。可信计算、智能动态防御、拟态防御等可信防护技术也应运而生。

2 舰船电站网络控制系统可信性分析技术

2.1 控制系统可信性需求分析

2.1.1 工业协议风险

Modbus、S7、OPC、IEC104、Profibus 等工业协议在设计初期主要是为了保证生产的连通性和稳定性，协议的应用、传输没有加密措施，没有认证措施，可信风险极大。

OPC（olefor process control）一项应用于自动化行业及其他行业的数据可信交换可互操作性标准，常用在现场总线的“上游”，作为其他协议与基于 Windows 的计算网络之间的网关。OPC 协议的可信缺陷主要有：

1）OPC 使用 DCOM 与 RPC 技术，受到 DCOM 与 RPC 漏洞的影响，导致易受到攻击[15-16]。

2）OPC 运行于 Windows 系统，容易受到 Windows 漏洞的攻击影响。

3）主机运行的可靠性影响 OPC 系统的可靠性。

4）OPC 主机常使用弱可信认证机制和弱口令。

5）系统启用了与控制系统无关的服务，导致非必须的进程和端口。

6）受限于维护等因素，网络控制系统通常升级困难，不可信的授权机制在使用[6]。

Modbus 一种串行通信协议，常用来连接监控计算机和远程终端控制系统（RTU）[17]。Modbus 协议的可信缺陷主要有：

1）缺少认证的相关机制。Modbus 采用 TCP 协议，已知目标 IP 时利用 502 端口可建立连接，当携带设备支持的功能码，就能够建立 Modbus 会话[18]。

2）缺乏数据加密。Modbus 协议以明文的形式传输，通过抓包技术可获取并解析处数据，可以伪造假冒的合法数据包对工控设备进行欺骗[19]。

3）缺乏数据检验，ModbusTCP 实现中，检验和是在传输层而非应用层生成，使得假冒命令更加容易。

2.1.2 控制设备风险

国内用的控制设备基本上来自西门子、AB、施耐德等国外厂商，这些控制设备设计的时候多数是为了实现功能，没有相应的安全设置或相应的安全功能模块[20]，存在较多漏洞，甚至后门，一旦被攻击利用会导致严重后果。

2.1.3 应用软件风险

网络控制系统中使用的 Sixnet、iFix、SIMATIC、HollySys 等组态软件存在大量的安全漏洞，严重影响安全运行[21]。

2.1.4 操作系统风险

操作员站、工程师站、工业服务器使用 Windows 系统，

存在安全漏洞。并且考虑到工业系统运行的稳定性，操作系统很少打补丁，容易遭受恶意攻击。

2.1.5　人机操作风险

上位机操作人员具有较高操作权限，能够执行状态变更、程序下装、执行操作等重要行为，当出现误操作时会导致事故发生，造成损失。

2.1.6　管理意识风险

各项制度、规范、标准，将人和技术结合在一起，以确保技术防护手段能够真正发挥作用。用户安全意识不足是很多安全事件产生的根本原因。

装备网络控制系统应用嵌入式系统＋微处理器＋应用软件的新模式，面临攻击范围扩大、扩散速度增加、漏洞影响扩大等威胁[13]，应分别从设备可信、协议可信、软件可信 3 方面采取可信性设计措施[3]。

2.2　控制数据可信性需求分析

控制数据可信保证数据在生命周期内的机密性、完整性、可用性[4]。装备网络控制系统数据类型包括运行数据、用户数据、设备数据、外部数据、基础数据等，控制数据可信贯穿于整个装备网络控制系统架构。

从风险的位置看，数据可信风险包括内部风险和外部风险。内部风险主要源于内部网络、设备内部、控制平台内部等，主要包括内网健壮性以及内网病毒风险等；外部风险主要源于外部网络，包括外部攻击、病毒入侵等。从风险产生的环节看，数据的感知、传输、存储和处理都会受到不同的威胁。数据感知的主要威胁包括数据窃取、数据受损、节点故障、隐私侵犯等；数据传输的主要威胁包括数据泄露、数据篡改、数据破坏等；数据存储和处理的主要威胁包括数据泄露、数据破坏等。

控制数据可信防护需要从数据可信管理、数据可信技术两方面进行防护。

2.2.1　数据可信管理

建立装备网络控制系统全产业链数据可信管理体系，包括管理策略、分级分类的管理制度，明确数据可信包含的责任和目标。

1）数据可信管理策略：加强对装备网络控制系统数据的可信监督检查；加强数据各环节的可信防护能力；加大对管理者的数据可信意识培训；定时定期对涉及数据的使用者进行检查；及时对应用平台、设备进行可信检查、维护、升级。

2）数据分级分类制度：依照控制数据可信的重要性、可信目标、影响范围与严重程度，将数据分为不同的敏感级：一般数据、重要数据、敏感数据。

3）明确数据可信责任和目标：管理者需要深入了解“四问”“四知”。四问：哪些数据需要保护、这些数据面对什么威胁、谁负责保护受威胁数据、如何保护受威胁数据。四知：知悉控制数据可信保护的政策、方法、要求和期望。

2.2.2　数据可信技术

构建数据可信技术体系，保证全生命周期的数据可信，具体包括：终端加密、认证机制、数据审计等数据感知技术；访问控制、存储加密、备份和恢复、数据分布地图等数据存储技术[22-23]；数据加密、安全技术保护、消息认证技术、数据识别技术、数据转流审计及分布地图等数据传输技术；使用授权、数据销毁、数据脱敏等数据处理技术。

2.3　控制网络可信性需求分析

控制网络可信指工厂内有线网络、无线网络的可信以及工厂外与用户、协作系统等事项互联的功能网络可信。目前控制网络可信风险主要包括：部分现有控制网络已经存在威胁；控制网、管理网以及上级管理网之间缺乏系统有效的防护策略，现有防火墙、网闸等形同虚设；控制网与管理网边界不清晰，控制网存在多个数据出口且无防护措施；控制网络普遍无审计措施；无线设备管理不完善，无线网络可信问题较突出，面临 DoS 攻击、DDoS 攻击、假冒攻击、中间人攻击、跨异构网络的网络攻击等。

网络可信防护内容具体可分为 3 类：

1）内部网络可信需求：区域划分与隔离、数据传输完整性、网络异常监测、无线网络攻击的防护、网络入侵防范、恶意代码防范、网络可信审计、数据传输保密性保护、网络访问控制。

2）外部网络可信要求：数据传输完整性、数据传输保密性、网络入侵防范、恶意代码防范、网络可信审计、网络访问控制、网络集中管控。

3）边界可信防护要求：网络边界隔离、网络边界访问控制、网络边界可信审计、网络边界恶意代码防范。

3　舰船电站控制系统可信性设计技术

3.1　设备可信性设计技术

3.1.1　操作系统/应用软件可信设计

1）固件可信增强，可从操作系统内核、协议栈等方面进行可信增强，阻止恶意代码传播与运行，力争实现设备固件的自主可控。

2）漏洞修复，对工业现场常见的设备进行漏洞扫描与挖掘，发现操作系统和应用软件中存在的安全漏洞，并及时进行修复。

3）补丁升级，针对网络控制系统现场设备的安全漏洞，及时采取补丁升级措施，并在补丁安装前对补丁进行严格的可信评估和测试验证。

3.1.2　硬件可信设计

1）硬件可信增强，利用可信芯片或可信固件作为信任根，为现场设备安全启动、数据安全传输提供支持和保护[5]。

2）运维监测控制，部署在机组主控 DCS 系统等重要控制系统的操作员站、工程师站、历史站，对外部存储设备、USB 接口设备识别与管控[24]。

3.2 系统可信性设计技术

3.2.1 协议可信设计

1）身份认证：在控制协议通信过程中加入认证方面的约束，避免攻击者通过截获报文获取合法地址建立会话，影响控制过程可信。

2）访问控制：建立基于角色的访问机制，对用户权限进行划分。

3）传输加密：采用加密措施保证通信双方的信息不被第三方获取。

4）健壮性测试：控制协议应用到工业现场之前通过健壮性测试，如风暴测试、饱和测试、语法测试、模糊测试等。

3.2.2 应用可信防护

1）权限设置：不同的应用程序应根据不同的对象设置不同的权限，以最小权限完成的相关任务。

2）病毒防护：应用程序应该具有查杀病毒、木马等检测手段，做好预防和恢复相关措施。

3）防止篡改：利用完整性校验技术对程序校验，及时发现应用程序的篡改情况；对软件重要代码进行加密。

4）协议过滤：通过防火墙技术对协议数据过滤，对通信内容进行监测跟踪。

5）补丁升级：应用程序的变更、升级应经过严格测试，并有回退计划，重要补丁应尽快测试、部署。

3.3 软件可信性设计技术

软件可信性设计方法主要包括避错设计、容错设计、排错设计、预错设计等。避错设计是传统的可靠性设计技术，体现了以预防为主的思想，贯穿于软件开发的全过程，主要方法由结构化设计、贯彻相关设计标准和编码标准等。避错是舰船电站网络控制系统软件可信性的基本方法，但只能达到一定的限度。要想进一步提高可信性，需要进行容错设计。软件容错设计是在系统存在故障的情况下，发现故障并纠正故障，使系统运行不受影响，或将故障影响降到可接受范围，设计方法主要错误检测、错误处理、错误恢复等。排错设计主要是在开发阶段进行排错和运行阶段进行校正性维护与预防性维护。预错主要通过定性的等级评价或定量的概率评价对故障进行预测。软件可信性设计技术如图 2 所示。

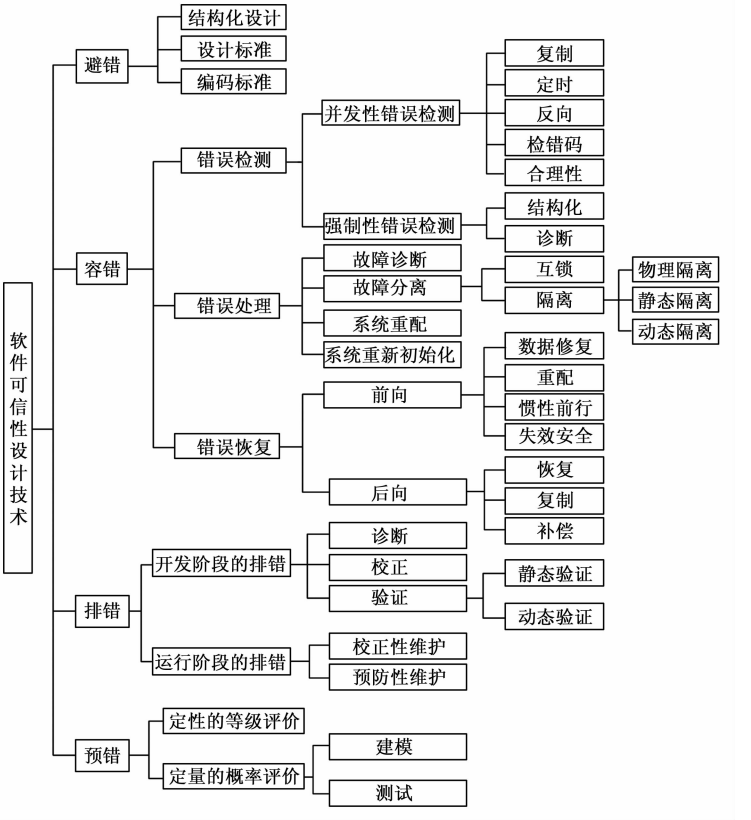

图 2 舰船电站软件可信性设计技术

4 舰船电站控制数据可信性设计技术

4.1 数据分级分类要求

对数据内容的理解，并对数据进行分级分类；根据数据类别和密级对需要保护的数据进行定位和标记；根据数据类别和密级，结合数据的创建者、流转情况、分布情况、使用方式分析数据的风险情况及信任情况；根据不同风险和信任情况制定出多样的响应方式对数据进行保护[14]。

数据分级分类主要依照控制数据可信的重要性、可信目标、影响范围与严重程度，将互联网相关数据分为不同的敏感级：一般数据、重要数据、敏感数据。

1）一般数据：装备控制数据发生泄露时，对与装备网络控制系统相关的生产商、服务提供商、用户等造成一定影响，但不会对财产和人身安全构成危害，影响范围与程度有限。

2）重要数据：数据一旦泄露，会对装备网络控制系统运行造成较大影响，在一定范围内影响经济消息或造成财产损失，或对用户的人身和财产造成较大影响，或产生安全事故。

3）敏感数据：装备网络控制系统的数据活动中，与军事利益密切相关，或关系到装备隐私，一旦未经授权泄露、丢失、滥用、篡改或销毁，造成严重后果，严重影响装备实战能力或产生重大安全事故。

数据分级分类通过调研访谈对样本采样，通过机器学习对样本进行聚类分析，分析数据实现分级分类，提取特征进行策略应用。

4.2 数据可信性设计技术

敏感数据可信处理主要是：对敏感数据进行加密处理；对敏感数据的外传进行提请审批；对敏感数据外传进行阻断处理；对敏感数据的外传进行多种方式告警；对敏感数据外传的详情进行审计；对存储的敏感数据进行转发和移动/删除。具体设计技术为：

1）数据监控，监控所有 TCP/UDP 网络链接，分析应

用协议所传输的内容，发现并记录可能违反数据可信策略的时间，监控网络数据流向、终端数据流向等。

2）网络保护，对 HTTP 和 HTTPS 协议的网络数据流量实施进行内容恢复和扫描，进行审计和阻断。

3）终端保护，扫描并发现终端上的敏感信息分布和不当存储，监控对敏感数据的使用并进行实时保护。

4）数据发现，扫描各类服务器及存储，结合终端保护模块可对终端进行扫描，生成敏感信息分布热力图、数据分布地图，对敏感数据定位。

5）数据管理，基于 Web 界面的综合管理平台，可配置基于用户角色的数据防泄露策略和系统管理选项。管理平台可视化程序敏感数据分布状况好可信态势，可生成泄露事件日志和报表，帮助用户采取进行审核、审计和补救措施。

4.3　数据可信性检查验证要求

软件设计要素之一的数据设计包括数据库、数据文件和全局数据结构的定义，是确定整个系统和软件所有数据的关键阶段。设计数据分析评价在该软件设计中每个数据项的描述和预期的使用。数据分析确保数据的结构和预期的使用将不违反安全性需求。在执行设计数据分析中使用的一项技术是将该设计逻辑中的每一个数据项的描述同其使用进行比较。共享存储器和动态存储器分配可能影响到数据的完整性，还应该保护数据项不被未授权的应用程序覆盖。软件数据设计分析验证检查单如表 2 所示。

表 2　数据可信性分析验证检查单

序号	检查项	是否满足
1	应确保将安全关键的数据与其他数据隔离开来，并使非安全关键部件不能访问安全关键数据；	
2	数据传送过程中应对安全关键数据进行加密操作，以保护数据内容；	
3	对包含安全关键数据的数据库和数据文件都要进行文档化。	
4	数据区隔离。为防止程序把数据错当指令来执行，要采用将数据和指令分隔存放的措施。	
5	算法所使用的存储空间应该是完全确定的。例如，不采用动态堆空间。	
6	对在接口中使用的安全关键数据，都要有唯一的标识符。	
7	数据传输报文应是预先规定的格式和内容。每次传输应包、数据类型或报文内容的字或字符串，至少应使用奇偶校验检查以及累加和来验证数据传输的正确性，在验证数据传输正确性之前任何来自数据传输报文的信息都不得使用；	
8	软件应能判断操作员的输入操作正确与否，在遇到不正确的输入和操作时，能够拒绝操作的执行，并提醒操作员注意错误的输入和操作，同时指出错误的类型和纠正措施；	
9	在进行数学运算时，应仔细考虑浮点数接近零的处理方式，在可能发生下溢时，使用适当小的浮点数来替代零，以避免下溢情况的发生。在含有浮点数的关系判断中，不应直接进行相关相等关键的判断。	
10	应防止对数据的非授权的无意的存取或修改。	
11	对于安全关键信息与其他信息之间应保持一定的码距，使安全关键信息不会因一位或两位差错而引起系统故障。	
12	对安全关键的信息和数据，应保存在多种或多个不同芯片中，并进行表决处理。	
13	输入的数据元素应以显示参数的形式传给另一个模块接口。调用模块无需知道数据是如何被调用的。	

5　舰船电站控制网络可信性设计技术

5.1　网络可信性设计技术

网络可信性设计技术主要通过网络与边界的划分隔离、访问控制、机密性与完整性保护、异常监测、入侵防范、可信审计等方式保证，网络信息传输的可信性。网络可信防护重点关注控制系统与信息系统之间，对内部云平台的访问，接入云平台、信息系统、工业控制系统的设备，接入云平台的智能产品、智能终端等。具体技术包括：

1）网络隔离技术：通过专用物理硬件和安全协议在不同网络之间架构器安全隔离网墙，使两个系统在空间上物理隔离，同时又能过滤数据交换过程中的病毒、恶意代码等信息，常用工具包括防火墙、网闸、物理隔离卡、安全路由等[7]。

2）加解密技术：加密技术是网络可信防护的一项重要保密措施，利用技术手段把重要数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密），加密技术包括两个元素：算法和密钥。常用的攻击包括密码算法、安全协议、VPN 等。

3）认证技术：认证技术是确认操作者身份的过程而产生的有效解决方法。所有对用户的授权是针对用户数字身份的授权，认证手段包括基于信息秘密的身份认证（如静态密码）、基于生物特征的身份认证（如生物识别）、基于信任物体的身份认证（如智能卡、短信秘密、动态口令、数字签名等）[8]。

4）入侵检测技术：入侵检测是通过对行为、安全日志或审计数据或其他网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图，作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持等[23]。常用攻击包括基于协议的入侵检测、基于异常行为的入侵检测、基于特征的入侵检测等[9]。

5）恶意代码防护技术：常见的恶意代码包括计算机病毒、特洛伊木马、计算机蠕虫、后门、逻辑炸弹等。恶意代码防护技术主要包括基于主机的恶意代码防护技术和基于网络的恶意代码防护技术。

6）监测审计技术：监测技术包括数据采集技术、关联分析技术、预警技术，审计技术包括逻辑命令自动识别技术、正则表达式匹配技术、会话重建技术、多线程协议还原技术等。

5.2 某控制网络典型可信防护措施

针对某型装备控制网络，根据网络特性，制定了以下的典型可信防护措施：

1）优化网络结构，通过在关键网络节点和标识解析节点采用双机热备和负载均衡技术，通过合理的网络结构和设置提高网络的灵活性和可扩展性[10]。

2）网络可信接入，接入网络的设备具有唯一标识，网络对接入的设备进行身份认证。

3）网络可信边界，根据重要程度将整个网络划分为不同的可信域，形成纵深防御体系。

4）网络可信传输，利用加密技术防止非法窃取，采取校验机制保障篡改被有效甄别。

5）设备可信防护，网络设备与标识解析节点启用安全登录方式，对远程登录的源地址限制，对登录用户进行身份鉴别，登录过程采取完备的登录失败处理措施。

6）可信监测审计，通过漏洞扫描工具等探测系统漏洞，及时预警；记录设备运行信息和用户活动，对安全事件告警；监测内部人员错误操作或越权操作，及时告警。

6 结束语

舰船电站网络系统信息技术（IT）与操作技术（OT）融合，控制范围从局部扩展到全局，并且控制监测上移、实时控制下移，信息安全与功能安全交织，危害范围扩大、程度加深。然而，舰船电站网络控制系统在安全可信方面的测评标准体系尚不完善，网络、设备、系统的可信防护变得尤为重要[11]，并且舰船电站网络控制系统是应用于装备上的系统，由于军事使用需求，在可信性设计方面需要将“风险”与“可信”进行平衡，以满足装备实时性、易用性、可靠性等使用需求，强调信任则会提高风险，强调风险则会较低效率。因此，舰船电站网络控制系统在研制过程中，应针对不同的数据和不同的使用场景，进行风险分析、可信设计，配合自适应的可信防护响应机制来实现。网络控制系统可信防护理念是：1）可知，风险评估、安全培训、形势跟踪；2）安全，安全应用、安全设备、安全网络；3）可管，管理制度、管理措施、管理水平；4）可防，主机防护、边界防护、网络防护。通过分析了装备网络控制系统可信性需求，提出了对应的可信性设计措施，为舰船电站网络控制系统以及其他装备中的网络控制系统开展可信性防护设计提供了技术支持。

参考文献：

[1] 吴立金，韩新宇，闫 然，等. 舰船装备软件可信性分析设计技术研究 [J]. 计算机测量与控制，2018，26（12）：130－135，170.

[2] 张 俊，宋立忠. 舰船电站网络控制系统设计 [J]. 舰船电子工程，2006（4）：152－153，157.

[3] 杨祖业，李 媛，马秀丽. 面向智能装备的工业互联网平台参考架构 [J]. 中国仪器仪表，2019（6）：31－36.

[4] 张雪莹，陈雪鸿，杨帅锋. 工业互联网数据安全标准体系研究 [J]. 网络空间安全，2019，10（10）：86－92.

[5] 杨睿超，岳剑晖，杭 肖. 浅谈工业互联网环境下的工业控制系统安全防护 [J]. 网络安全技术与应用，2020（5）：108－109.

[6] 梁雨锋，汪 萌，赵军凯，等. 有色金属行业典型工业控制系统通信协议安全性分析 [C] //信息网络安全，2016（s）：94－100.

[7] 李志红. 计算机网络隔离技术浅析 [J]. 数字技术与应用，2012（11）：194.

[8] 韩 慧. 计算机网络办公自动化及安全策略研究 [J]. 信息技术与信息化，2015（11）：114－116.

[9] 武传坤. 物联网安全关键技术与挑战 [J]. 密码学报，2015，2（1）：40－53.

[10] 刘晓曼，李 艺，吴 昊. 工业互联网安全架构及未来发展思考 [J]. 保密科学技术，2019（3）：12－19.

[11] 李向东，耿立校，肖美玲，等. 工业互联网平台安全问题探析 [J]. 网络安全技术与应用，2021（5）：120－122.

[12] 夏 晶. 基于 Labview 的舰船综合监控网络设计与管理研究 [J]. 舰船科学技术，2018，40（22）：184－186.

[13] 刘廉如，张 尼，张忠平. 工业互联网安全框架研究 [J]. 邮电设计技术，2019（4）：53－57.

[14] 张雪莹，杨帅锋，王冲华，等. 工业互联网数据安全分类分级防护框架研究 [J]. 信息技术与网络安全，2021，40（1）：2－9.

[15] 袁 蓉. 煤矿安全生产执行系统的研究与设计 [J]. 煤矿机电，2013（4）：43－48.

[16] 冯 涛，鲁 晔，方君丽. 工业以太网协议脆弱性与安全防护技术综述 [J]. 通信学报，2017，38（S2）：185－196.

[17] 张 渝，刘 枫. 一种 Modbus 远程监控系统框架及其实现与教学应用 [J]. 西南大学学报（自然科学版），2010，32（9）：126－129.

[18] 洪轶群. 烟草工业控制系统信息安全检测技术研究 [J]. 网络安全技术与应用，2020（2）：122－124.

[19] 倪光南. 工业物联网安全与核心技术国产化 [J]. 物联网学报，2018，2（2）：1－7.

[20] 张 娜. 工业控制网络安全风险及防护策略 [J]. 安全、健康和环境，2020，20（1）：39－43.

[21] 刘丽华. 工业信息安全思考与建议 [J]. 无线互联科技，2019，16（1）：125－126.

[22] 蒋融融，翁正秋，陈铁明. 工业互联网平台及其安全技术发展 [J]. 电信科学，2020，36（3）：3－10.

[23] 郭宏刚. 入侵检测系统在开放式网络中的设计与实现 [J]. 河北公安警察职业学院学报，2010，10（2）：53－55.

[24] 吴 鹏，朱 军，韩永磊. 离散型制造企业工控网络安全技术应用研究 [J]. 信息技术与网络安全，2019，38（4）：42－45.