工业控制网络信息安全的防护措施与应用

杨乐，刘洪具
云南昆钢电子信息科技有限公司，云南 安宁 650302

摘　　要： 工业控制网络作为现代工业自动化系统的核心组成部分，随着信息技术的快速发展和工业互联网的普及，工业控制网络的复杂性和连接性显著增加，同时也带来了更多的安全挑战和威胁。本文分析工业控制网络的基础架构，并提出了符合工业控制网络信息安全的防护控制措施，包括硬件措施以及软件措施，并探讨了工业控制网络信息安全的应用策略，为全面加强工业控制网络信息安全水平提供参考性意见。

关 键 词： 工业控制网络；信息安全；防护措施；应用探究

Protection Measures and Applications of Industrial Control Network Information Security

Yang Le, Liu Hongju
Yunnan Kungang Electronic Information Technology Co., Ltd., Anning, Yunnan 650302

Abstract: Industrial control network is the core component of modern industrial automation system. With the rapid development of information technology and the popularization of industrial Internet, the complexity and connectivity of industrial control network have increased significantly, but also brought more security challenges and threats. This article analyzes the infrastructure of industrial control networks and proposes protective control measures that comply with information security in industrial control networks, including hardware and software measures. It also explores application strategies for information security in industrial control networks, providing reference opinions for comprehensively strengthening the level of information security in industrial control networks.

Keywords: industrial control network; information security; protective measures; application exploration

前言：

随着工业控制网络的数字化和网络化程度提升，传统的安全措施已经不再足够应对复杂和精密的攻击手段，恶意软件、远程入侵和物理层攻击等安全威胁，可能导致设备瘫痪、生产中断甚至环境污染等严重后果，深入研究工业控制网络信息安全，探索和实施新的安全防护技术和策略势在必行，以保护关键基础设施的安全和稳定性[1]。国际上已有多项研究和标准提出了针对工业控制网络安全的技术和实践指南，如 ISA-99标准、NIST 特别出版物800-82等，这些标准和指南为工业控制系统的安全实施提供了框架和指导。随着技术的迅猛发展和新兴威胁的出现，仍然需要不断更新和完善安全措施，以应对日益复杂的威胁环境。

一、工业控制网络的基础架构

（一）分布式控制系统（DCS）

DCS 是专门设计用于大规模工业过程控制的系统，其架构和功能使其能够有效地监视、控制和优化复杂的生产过程[2]。以下将详细介绍 DCS 的基础架构及其关键特征。DCS 的基础架构通常由以下几个关键组成部分构成：1）控制器：DCS 系统包含多个分布式控制器，控制器分布在整个生产设施中的关键位置，通过专用的通信网络进行连接和协作，每个控制器负责执行特定的控制任务，例如监控和调节生产过程中的温度、压力、流量等参数。2）输入 / 输出模块：输入 / 输出模块是 DCS 系统与生产设备、传感器和执行器之间的接口；输入模块负责接收来自生产设备和传感器的数据，如温度、压力、流量等实时信息；输出模块则向执行器发送控制命令，如调节阀门、启动 / 停止电机等操作[3]。3）操作站：操作站是 DCS 系统的用户界面，用于操作员监视和控制生产过程，操作站通常提供直观的图形化界面（GUI），显示实时数据、报警信息和生产状态，且操作员可以通过操作站执行生产调度、设备配置和故障排除等操作。4）通信网络：DCS 系统依赖于

杨乐，1991 年 4 月，男，汉族，四川省宣汉县，大学本科，工控安全。

可靠的通信网络，以实现控制器、输入 / 输出模块和操作站之间的数据交换和信息传递，不同的通信网络通常采用工业以太网、现场总线或专用的 DCS 通信协议，确保数据传输的实时性和稳定性。

（二）分层网络架构

工业控制网络的基础架构中，分层网络架构能够满足工业自动化系统对数据传输、控制和监控的高要求，该架构将网络按功能和安全性需求划分为不同的层次，每个层次承担特定的任务和功能，以确保系统的可靠性、安全性和效率 [4]。

分层网络架构通常包括以下控制层、操作层以及信息层。其中，控制层是工业控制网络中最核心的一层，主要用于实时控制和监控生产过程，DCS 集成了多个分布式控制器，用于大规模工业过程控制，支持复杂的控制策略和实时数据处理；操作层提供用户界面和操作平台，使操作员能够监视和控制工厂设备及生产过程，SCADA 系统提供直观的人机界面（HMI），显示实时数据、报警信息和生产状态，操作员可以通过这些界面进行生产调度和设备管理 [5]；信息层用于处理和管理工业控制系统中生成的大量数据，并支持上层决策和管理。主要包括：MES 系统以及 ERP 系统，MES 系统负责优化生产过程、实时跟踪和调度生产任务，提升生产效率和资源利用率，ERP 系统集成了企业各个部门的信息和业务流程，支持物料管理、财务管理等企业级功能。

二、工业控制网络信息安全的防护措施

（一）硬件防护

1. 硬件隔离

硬件隔离的基本原理是将控制系统的关键组件（如处理器、存储器、接口电路板等）在物理上隔离开来，使得这些组件只能通过安全授权的方式进行访问和通信。在设计阶段，通过在硬件布局上的物理分隔来隔离不同的功能模块或子系统，防止电路干扰和数据泄露 [6]。实际可以利用虚拟化技术或安全隔离技术，在同一物理设备上实现逻辑上的分隔，确保各个功能模块之间的数据和指令不会相互干扰或交叉感染。

在设计和布局控制系统时，将处理器、存储设备、网络接口等关键部件物理上分离，使它们不直接暴露在外部网络或未授权访问之下，可以采用专门设计的硬件安全模块，如安全加密卡、安全芯片等，用于存储和处理敏感数据。并通过物理接口限制对其访问，在此基础上通过物理锁定、门禁系统和视频监控等手段，限制对控制系统物理访问的权限，并实施严格的访问控制策略。

2. 固件加密

固件加密作为工业控制网络信息安全的关键技术之一，主要用于保护设备的固件和操作系统免受未经授权的访问和篡改 [7]。通过对固件进行加密，可以有效防止恶意攻击者在设备启动时篡改系统设置、植入恶意代码或获取敏感数据，从而提升系统的整体安全性和稳定性。固件加密的标准如下表 1 所示

表 1 固件加密的标准

标准	特点
AES	对称加密算法，密钥长度为 128 比特、192 比特或 256 比特，加密速度快且安全性高。
RSA	非对称加密算法，密钥长度通常为 1024 比特或 2048 比特，用于密钥交换和数字签名。
ECC	椭圆曲线加密，密钥长度通常为 256 比特或更小，适用于资源受限设备，效率高。
SHA-256	安全哈希算法，生成 256 比特的哈希值，用于验证数据完整性和真实性。
HMAC	基于哈希的消息认证码，结合安全哈希算法和秘密密钥，用于数据完整性验证。

固件加密通过对固件镜像、操作系统和关键数据进行加密处理，将其转化为加密格式存储在设备中。后续在设备启动时，只有经过授权的密钥可以解密固件，确保设备只能加载和执行经过认证的安全固件，需要选择强大和安全的加密算法，如 AES（高级加密标准），确保固件和数据在传输和存储过程中的机密性和完整性 [8]。在此基础上严格管理加密密钥的生成、存储和分发过程，确保密钥仅限授权人员访问和使用，防止密钥泄露和滥用风险，并采用技术手段和安全措施，防止恶意用户或黑客通过反向工程手段破解加密算法或获取加密数据的明文信息。

（二）软件防护

工业控制网络的信息安全是确保工业自动化系统稳定运行和生产安全的重要组成部分。软件防护涉及到工业控制系统中软件的安全设计、开发、部署和维护等方面，实际需要制定和遵循安全编码标准，如 CERT 编码规范和 OWASP 安全开发指南，确保软件在设计和开发阶段考虑到安全性 [9]。在此基础上实施漏洞评估和静态代码分析，及时发现和修复软件中的潜在漏洞和安全问题，并实施最小权限原则，确保软件只能访问其必需的资源和功能，减少恶意操作的风险。

三、工业控制网络信息安全的应用策略

（一）多因素身份验证

多因素身份验证（MFA）在工业控制网络信息安全中扮演着关键角色，通过结合两个或多个不同的身份验证因素，提高了系统对身份验证的准确性和安全性。传统的用户名和密码登录方式存在被破解或盗用的风险，而 MFA 通过引入额外的因素，如手机验证码、硬件令牌、生物识别等，显著增加了攻击者获取合法访问的难度。

在工业控制网络中，MFA 的应用可以有效保护关键系统和数据免受未经授权的访问。例如，在访问控制系统中，操作人员需要除了用户名和密码外，还需通过手机短信或安全令牌生成的动态验证码进行验证。这种额外的安全层级不仅限制了攻击者通过简单的密码猜测或窃取进行登录，还确保只有经过授权的人员才能访问系统。

（二）采用 CAN 总线通信控制技术

CAN 总线通信技术广泛应用于控制和监控设备之间的数据交

换，CAN 总线作为一种专门设计用于实时数据传输和控制的通信协议，具有高效、可靠和实时性强的特点[10]。通过使用加密技术对 CAN 总线上的数据进行加密，可以防止未经授权的访问和数据篡改。此外，还可以实施身份验证机制，确保只有经过授权的设备和节点才能参与通信。CAN 总线通信参数如表2所示。

表2 CAN 总线通信参数

标准	特点
通信速率	典型的通信速率包括1 Mbps、500 kbps、250 kbps、125 kbps 等，根据具体应用选择。
通信协议	CAN 总线通常采用 ISO 11898标准，定义了物理层和数据链路层的通信协议。
帧格式	CAN 总线支持标准帧和扩展帧两种帧格式。标准帧包含11位标识符，扩展帧包含29位标识符。
网络拓扑结构	CAN 总线通常为主从架构，支持多主机和多从机的连接，也可用于星型拓扑。
硬件实现	CAN 总线硬件实现包括 CAN 控制器、收发器和总线线缆。控制器执行 CAN 协议，收发器负责信号调制和解调，总线线缆负责数据传输。

一方面，通过在 CAN 总线网络中实施严格的访问控制策略，限制设备和节点的访问权限，可以有效减少潜在的攻击风险。例如，只允许特定的控制器或传感器节点发送指定类型的命令或数据。另一方面，实施实时监测和响应措施也是保护 CAN 总线安全的重要手段。建立监控系统来检测异常数据流量或不正常的通信模式，并能够快速响应和隔离潜在的安全事件，以减少的损失和影响。

（三）优化网络分割和隔离

物理隔离可以通过物理隔墙、空气间隔和电缆分离等手段将关键设备和系统分离开来，防止因某个区域受到攻击而影响其他区域。逻辑隔离则通过虚拟局域网（VLAN）子网划分和访问控制列表（ACL）等技术，将不同功能和安全级别的设备分隔开来，减少攻击面。

在网络架构设计中引入安全边界和网络隔离区域，通过防火墙和安全网关来控制不同区域之间的通信流量，只允许经过授权的数据流进入或离开特定区域。与此同时，建立综合的访问控制策略和身份验证机制也是关键步骤，实施基于角色的访问控制（RBAC）和多因素身份验证（MFA），确保只有经过授权的用户和设备可以访问其特定的网络区域和资源。

结语：

综上所述，工业控制网络信息安全的各项策略和技术应用，包括硬件和软件防护。在实际应用阶段，为了提升安全性，需要采用多因素身份验证、CAN 总线通信控制技术以及网络分割与隔离等措施，从根本上提升系统的整体安全性和稳定性。硬件防护通过硬件隔离和固件加密确保设备和数据的物理安全和完整性；软件防护则通过安全开发、配置管理和访问控制策略保障软件层面的安全性。多因素身份验证提升了用户认证的安全性，而 CAN 总线技术的安全应用和网络分割隔离则有效控制了数据通信和系统访问的安全风险。综合采用这些信息安全措施不仅有效应对当前日益复杂的安全威胁，为工业控制系统提供了全面的防护和持续改进的路径，以确保其在高度互联和自动化环境中的安全运行和可靠性。

参考文献：

[1] 李璇. 工业信息控制网络信息安全的防护措施与应用［J］. 信息记录材料，2022(007):023.

[2] 王泓霖. 论可信计算3.0技术对工业互联网云平台安全防护的重要性［J］. 移动信息，2023，45(6):184-185.

[3] 杨轶茜，张龙山. 大数据背景下工业控制网络信息安全防护存在的问题及措施［J］. 网络安全和信息化，2023(3):119-121.

[4] 刘双龙，卢永慧. 石化企业 DCS 工业控制系统信息安全防护系统的开发和应用［J］. 化学工程与装备，2022(3):153-155.

[5] 闫印强，杨利达. 工业控制区全流量日志分析应用研究［J］. 工业信息安全，2022(9):39-45.

[6] 吕蒙. 工业控制系统网络信息管理及其安全防护策略［J］. 中国科技期刊数据库 工业 A，2022.

[7] 郭怡安，曹德舜，李娜. 基于信息安全与功能安全融合的安全控制系统设计方案研究［J］. 安全、健康和环境，2023，23(5):22-27.

[8] 李实，万佳蓉，林显盛. 基于蜜罐的工控网络安全防护技术研究进展［J］. 信息技术与网络安全，2022(002):041.

[9] 杨凡，丁之，王扬，等. 基于 SDN 和集成学习的工业控制网络安全防护系统［J］. 现代电子技术，2024,47(6):22-26.

[10] 蒲永杰. 工业控制系统网络安全防护措施的研究［J］. 设备管理与维修，2022(21):114-115.