网络安全防护技术和测评方法

郭一力
北京市地铁运营有限公司通信信号分公司　北京　100082

摘　要：工业控制系统网络安全防护技术和测评方法规定了工业控制系统安全防护技术要求、保障要求和测试评价方法，包括物理环境安全防护、网络通信安全防护、网络边界安全防护、工业主机安全防护、控制设备安全防护、数据安全防护、防护产品安全、系统集中管控、软件开发安全防护、系统维护安全防护相关的要求和测试评价方法。

关键词：网络安全；防护；评测

Network security protection technology and evaluation methods

Yili Guo
Communication Signal Branch of Beijing Metro Operation Co., Ltd. Beijing 100082

Abstract: The industrial control system network security protection technology and evaluation methods specify the requirements, protection requirements, and testing evaluation methods for industrial control system security protection technology. This includes physical environment security protection, network communication security protection, network boundary security protection, industrial host security protection, control device security protection, data security protection, security of protective products, centralized system management and control, software development security protection, system maintenance security protection, and related requirements and testing evaluation methods.

Keywords: cybersecurity; Protection; Evaluation

一、术语和定义

1、工业控制资产

工业生产控制过程中具有价值的软硬件资源和数据 。

注：包括控制设备、工业主机、系统终端、客户端、网络设备、应用程序、工业数据、安全防护系统等。

2、中心控制室

位于组织内，具有生产操作、过程控制、安全保护、专用仪器仪表维护和生产管理等功能的综合性场所。

3、现场控制室

位于组织内生产现场，具有生产操作、过程控制和安全保护等功能的场所。

4、现场专业设备机房

位于组织内生产现场，用于安装工业控制系统机柜及其他设备的场所。

5、工业系统主机

工业生产控制各业务环节涉及组态、工作流程和工艺管理、状态监控、运行数据采集以及重要信息存储等工作的设备。

注：包括工程师站（终端）、操作员站（客户端）、服务器等。

6、双机热备

通过网络连接主机和备机，正常情况下主机处于工作状态，备机处于监视状态，一旦主机异常，备机自动代替主机，继续运行。

二、概述

工业控制安全防护对象包括：现场设备层、现场控制层和过程监控层工业控制系统资产。

此方法给出了物理环境安全防护等八项技术要求指标和软件开发安全防护等两项保障要求指标，安全防护目的包括如下内容。

a）安全防护技术要求 ：

1）物理环境安全防护的目的是防止人员未经授权访问、损坏和干扰工业控制系统资产，避免受到外部物理环境因素影响，保护工业控制系统的外部运行环境；

2）网络通信安全防护的目的是保护工业控制系统中传输的数据的完整性和保密性,维护工业控制系统内部以及与外部网络之间信息的安全传输；

3)网络边界安全防护的目的是安全访问工业控制系统，避免非授权访问， 及时发现并有效保护工业控制系统免受恶意入侵和攻击。

4）工业主机安全防护的目的是有效控制工业主机访问行为，避免非授权访问，防止工业主机受到非法入侵或造成

工业数据泄漏；

5）控制设备安全防护的目的是安全访问控制设备，阻止非授权访问， 避免控制设备受到恶意入侵、攻击或非法控制；

6）数据安全防护的目的是保护数据全生存周期的完整性和保密性，防止未经授权使用和处理数据、恶意篡改和窃取数据等现象发生。

7）防护产品安全的目的是产品功能安全可靠、管控策略有效，避免因产品自身功能缺陷给工业控制系统的正常运行带来安全隐患；

8）系统集中管控的目的是集中维护和管控工业控制系统，统一制定与部署安全策略，集中响应安全事件。

b）安全防护保障要求:

1）软件开发安全防护的目的是控制工业控制系统软件的安全开发，避免软件自身存在安全隐患；

2）系统维护安全防护的目的是有效控制系统维护过程，避免系统在维护过程中受到干扰、恶意入侵、或发生数据泄露、被破坏或篡改等现象。

本文所提出的安全防护技术要求和保障要求分为四个等级，与《网络安全等级保护基本要求》GB/T22239 -2019、《信息安全技术 工业控制系统信息安全分级规范》GB/36324-2018 提出的相应安全保护等级要求保持一致，并按梯次推进的方式给出了不同安全保护等级 ICS 所对应的技术要求和保障要求。

测试评价方法是针对 ICS 运营单位执行本文件安全防护技术要求和保障要求的情况进行测试评价的一般方法，也可根据自身关注点自行调整测试评价指标。

三、安全防护措施的约束条件

工业控制系统安全防护措施的约束条件包括：

1、工业控制系统采用的网络边界隔离等技术防护手段应符合国家和所在行业规定要求，并采用经具备资格的第三方机构检测合格的安全产品；

2、数据传输和存储过程中所采用的密码技术应经过国家密码主管部门核准；

3、任何情况下都不应因采用安全防护技术措施而影响工业控制系统的正常运行或对系统的安全功能产生不利影响，例如：不应锁定用于基本功能的账户、不应因部署安全措施而显著增加延迟并影响系统的响应时间、不应因安全措施失效导致系统的基本功能中断等；

四、物理环境安全防护要求

第一级

机房、中心控制室、现场控制室应位于具有防震能力的建筑物内 ， 并应具有所在建筑物符合当地抗震设防标准的证明 。

第二级

机房、中心控制室、现场控制室应避免设在建筑物的高层或地下室、以及用水设备的下层或隔壁，如不可避免，应采取有效的防水、 防潮措施。

第三级~第四级

本项要求包括：

1、机房、中心控制室、现场控制室应避开发生火灾危险程度高的区域；

2 机房、中心控制室、现场控制室应避开产生粉尘、油烟 、有害气体源以及存放腐蚀、易燃、易爆物品的地方；

3、机房、中心控制室、现场控制室应避开低洼、潮湿、落雷、 重盐害区域和地震频繁的地方；

4、机房、中心控制室、现场控制室应避开强振动源和强噪声源；

5、机房、中心控制室、现场控制室应避开强电磁干扰源；

6、如以上无法避免，应采取相应措施。

五、访问控制要求

来访人员进入机房、中心控制室、现场控制室前应提出申请并通过审批，应记录其随身携带的设备、进出时间和工作内容，应有专人陪同并限制和监控其活动范围；

机房、中心控制室出入口应安排专人值守或配置电子门禁系统，控制、识别和记录人员的进出，人员进出记录应至少保存六个月。

六、电力供应要求

对于第三级应采用冗余或并行的电力电缆线路为机房、中心控制室的计算机系统供电、输入电源应采用双路市电自动切换供电方式。

七、网络通信安全防护要求

1、单个工业控制系统可单独划分安全域并可划分独立子网，每个安全域应尽量少设置网络出口；

2、网络设备的业务处理能力应满足业务高峰期需要，并具备冗余空间 ；

3、网络各个部分的带宽应满足业务高峰期需要，并具备冗余空间；

4、通信线路、关键网络设备和关键计算设备的硬件应进行冗余配置。

八、网络设备防护要求

1、应及时修改默认用户和默认口令，口令长度应不少于 8 位（特殊关键设备建议不少于 16 位）且为字母、数字或特殊字符的组合，用户名和口令不应相同，不应明文存储口令，每三个月应更换一次口令；

2、网络设备的标识应唯一，不应使用网络地址等易被仿冒的设备标识；

3、同一网络设备的用户标识应唯一，多个人员不应共用一个账号；

4、应对网络设备的管理员登录地址进行限制；

5、应关闭不需要的网络端口和服务，如使用 SNMP 服务，应采用安全性增强版本，并应设定复杂的共享控制字段，不应使用公共或私有的默认字段。

九、网络边界安全防护要求

工业控制系统与组织管理信息系统等其他系统之间应进行物理隔离，如有信息交换需求，应采用单向技术隔离手段，单向隔离装置的策略配置应安全有效；

工业控制系统与广域网的纵向交界处应设置访问控制设备，设备的策略配置应安全有效，并应实现双向身份核验、访问控制和数据加密传输；

应采取无线安全检测防护措施并识别和阻断未经授权的无线设备接入工业控制网络，应具有对无线扫描、无线破解、无线拒绝服务等攻击行为进行检测和阻断的功能。

十、安全审计

审计测试仅限于对软件和数据的只读访问，非只读的访问仅用于对系统文件的单独复制，审计完成时应擦除这些复制或按审计文件要求保留这些文件并给予适当保护。

应定义审计阈值，当存储空间接近极限时，应采取备份覆盖等安全措施以正常执行审计功能；

应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录和保护并定期备份，避免受到未预期的删除、修改或覆盖等，记录保存时间应不少于六个月；

应具备集中管理审计事件的能力，包括：用户登录/退出事件、连接超时事件、配置变更、时间/日期变更、审计接入、用户名/口令创建和修改等。

十一、工业主机安全防护要求

用户身份鉴别信息丢失或失效时，应具有安全重置身份鉴别信息的功能；

身份鉴别信息不易被冒用，口令应采用数字、字母和特殊字符混排等无规律的组合方式，口令长度应不少于 8 位（特殊关键设备建议不少于 16 位），每三个月应更换 1 次，更新的口令至少 5 次内不应重复；如设备口令长度不支持 8 位或其他复杂度要求，应使用所支持的最长长度并缩短更换周期；可使用动态密码卡等一次性口令认证方式，口令应加密存储。

第三级应采用口令、密码和生物识别等两种或两种以上组合的鉴别方式对用户身份进行鉴别、且其中至少一种鉴别方式应使用密码技术实现。

十二、数据安全防护要求

应在传输过程中对重要数据进行完整性校验或采用密码技术保护重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据和重要配置数据等；

应采用密码技术保护重要数据在传输过程中的保密性，包括但不限于鉴别数据和重要业务数据等；

十三、数据备份恢复要求

应定期对工艺参数、配置文件、设备运行数据、生产数据、控制指令等重要业务数据进行备份。

应对重要数据进行本地备份，应每天进行一次差分备份并至少每月进行一次全备份，数据发生较大调整后应立即进行全备份，应在场外存放备份存储媒体。

应至少每三个月对所备份的重要数据进行一次恢复测试，备份数据应能可用。

应根据数据备份的需要对重要存储媒体实行异地备份，存储地的环境要求和管理方法应与本地备份相同。

十四、防护产品安全要求

应为管理角色进行分级并使不同级别的管理角色具有不同的管理权限。

任何用户在执行安全功能前均应进行身份鉴别，若采用口令方式鉴别，应对口令长度和口令复杂度进行检查。

当已通过身份鉴别的管理角色无操作的时间超过规定值但又继续操作时，产品应具备对该管理角色的身份进行重新鉴别的功能。

应为管理角色登录设定一个可修改的鉴别尝试阈值，当不成功登录尝试超过阈值时，系统应能阻止管理角色的进一步鉴别请求。

十五、轨道交通工业控制系统网络边界安全防护方式

在控制中心列车自动监控系统与外部互联系统（如综合监控系统、信号系统、乘客信息系统、广播系统）等边界处串接部署工业控制系统专用防火墙。

利用白名单技术形成协议级安全基线，为每组通信对象配置应用协议报名单，如列车自动监控系统与综合监控系统、列车自动监控系统与乘客信息系统等。

在工业控制系统网络的工作站、服务器等主机设备上部署安全防护软硬件设备，采用白名单的形式，代替传统反病毒软件。

十六、测试评价总结

本项内容包括 ：

1、对测试评价过程及记录进行梳理、汇总，分析评价现有系统安全防护措施与标准要求的差距，以及这些距可能导致系统面临的网络安全威胁，并对威胁的严重程度进行客观分析和判断；

2、对存在的不足和面临的网络安全威胁，提出针对性的安全防护整改措施和解决方案，明确下一步整改计划，包括责任单位或部门、责任人、整改内容和完成时间、整改目标；

3、对测试评价过程中生成的过程文档归档保存。

结论：

通过合理性安全防护设计，针对工业系统特殊性的安全技术措施以及规范性测评方法，形成一套完整的网络安全防护保障，同时加强专业性的安全防护培训，提高技术人员网络安全意识，有效解决工业系统自身的运行情况，从多方面进行防护处理，从而提高整安全稳定运行，从而更好的为社会、企业和公众服务。

参考文献：

[1]信息安全技术 工业控制系统信息安全分级规范[GB/T 36324-2018].

[2]信息安全技术工业控制系统风险评估实施指南[GB/T 36466-2018].

[3]信息安全技术网络安全等级保护安全设计技术要求[GB/T 25070-2019].

[4]信息安全技术网络安全等级保护基本要求[GB/T 22239-2019].

本文作者曾参与制定中华人民共和国国家标准，《信息安全技术 工业控制系统 安全防护技术要求和测试评价方法》GB/T40813-2021，并于 2021 年 10 月 11 日发布，2022 年 5 月 1 日实施。