Engineering Technology and Development, 工程技术与发展 (12)2020,2
ISSN:2661-3506 (Online) 2661-3492(Print)

基于等保 2.0 工业控制系统网络安全技术防护方案

王鹏博
河南省正龙煤业有限公司城郊煤矿 河南 476600

摘 要：随着工业 4.0、工业互联网、中国制造 2025 等再工业化革命战略的不断推进，原本封闭的工业控制系统变得越来越开放，随之面临了新的挑战，病毒、木马、勒索软件以及黑客、敌对势力对工业控制系统进行了攻击。本文通过对当前我国工业控制系统网络安全现状分析后，提出一种基于等级保护 2.0 标准的工业控制系统网络安全技术防护方案。该防护方案通过构造 1 个管理中心，安全通信网络、安全区域边界、安全计算环境三重防护手段，实现对工业控制系统网络安全的事前预防、事中响应、事后审计的可信、可控、可管的纵深防护设计。

关键词：等级保护 2.0；工业控制系统；网络安全；防护方案

一、引言

自 2019 年 5 月 13 日起，公安部正式发布了三项标准，对网络安全等级保护的新要求也达到了新的水平。同时，作为关键信息基础设施的工业控制系统也被涵盖在等级保护的范围内。在内部，它分为一般要求和扩展生产管理系统的要求。本文重点关注“保护网络安全的信息安全技术的基本要求”的标准，结合工业控制系统网络安全的现状，对基于等级保护 2.0 的工业控制系统网络安全保护系统进行研究。

二、基于等保 2.0 工业控制系统网络安全技术防护的基本背景

等保的全称为“网络安全等级保护”，是我国网络安全领域的基本国策与核心制度。在网络安全建设初期，我国社会主要应用的制度为等保 1.0，其从物理、网络、主机、应用、数据五个角度入手，对网络安全防护提出了技术要求，同时从制度、机构、人员、系统建设以及系统运维五个角度入手，对网络安全防护提出了管理要求。辩证地看，等保 1.0 在推动我国网络安全建设兴起与发展的同时，也存在诸多问题。例如，基于等保 1.0 的网络安全防御工事以被动防护为主，对风险的主动感知能力比较弱；等保 1.0 在覆盖范畴上存在一定局限性，与云安全、大数据、工业控制等新科技、新概念存在不兼容问题

为了解决此类缺陷短板，同时也为了使我国网络安全防护体系建设得更加健全，等保 2.0 适时而出，在法律规定、技术要求、管理要求、实施标准、覆盖领域等各个方面都有了明显的优化调整。例如，在法律规定方面，等保 2.0 以《中华人民共和国网络安全法》为支撑，对以社会企业为代表的网络运营者提出了硬性要求，若不遵守和落实网络安全等级保护的各项要求，将代表着对公共法律的触犯；在技术要求方面，等保 2.0 对前代制度的相关内容进行了整合与细化，形成了物理和环境、网络和通信、设备和计算、应用和数据四个层次；在管理要求层面，等保 2.0 将机构与人员两部分安全管理要求合而为一，并建立起了更严格的定级测评体系；在实施标准方面，等保 2.0 除了“通用要求”以外，还融入了“扩展要求”，以此满足不同网络应用场景、不同技术体系的特定安全防护需求；在覆盖领域方面，云计算、移动网络、物联网、工业控制等网络发展新产物被纳入到制度体系之中，与我国社会的发展实情高度贴合。

三、基于等保 2.0 工业控制系统网络安全技术防护的问题

（一）控制系统有漏洞

由于工业控制系统早期在设计时候，主要考虑系统的稳定性、实时性以及可靠性，并没有考虑安全问题。所以导致工业控制系统漏洞不断爆出，据国家信息安全漏洞共享平台 CNVD 统计的工控漏洞截至 2020 年 2 月 18 号有 2353 个漏洞。其中西门子、施耐德、研华的产品漏洞最多，高中危漏洞占 95% 以上。

（二）工业控制系统网络边界相对模糊

现阶段，工业控制系统已实现了由集中控制系统、分散控制系统到现场总线控制系统的逐步发展，其与工业管理网、公共互联网的通信连接也日趋紧密。在此背景下，工业控制系统相对封闭化、独立化的网络状态被打破，进而造成了其网络边界的严重模糊。这样一来，无法厘清网络边界，也就很难实现网络安全防护体系的覆盖化部署，使得越权操作、违规外联、非法访问等负面现象时有发生，对工业控制系统的安全稳定运行与工业生产活动的顺利高效开展构成了极大威胁。

（三）无法检测到工业控制网络中的异常流量

由于缺乏对工业控制系统中网络流量，病毒，特洛伊木马和其他恶意程序的监视和审计，因此无法检测到非法用户操作，错误操作和网络上的 DDOS 攻击。在深入分析时无法对异常流量进行定位、追踪和责任划分。

（四）工业主机存在大量安全问题

工业场景中使用的操作员站、工程师站以及工业数据库主机大部分为 Windows 的操作系统，如 Windows XP、

Windows7、Windows Server2003、2008 等操作系统，这些操作系统微软已经不再提供相应的服务。还有这些工业主机安装杀毒软件不足，即使安装了杀毒软件，由于兼容性问题、操作系统多样性以及病毒库需要定期更新等问题，导致杀毒软件在工业主机上无法很好的使用，安全问题屡有发生。另一方面，移动存储介质的不规范使用，病毒、木马等恶意软件的攻击，工艺、配方泄密等安全问题不断发生。

（五）人员安全意识薄弱、缺乏安全培训

工业控制系统的运维工作通常由设备管理部门的工程师和生产车间工作人员完成，这些人员平时对生产安全意识较强，注重工业控制系统的可用性，但对工业控制系统网络安全风险关注较少，系统安全意识薄弱，企业的资金预算不足，缺少相应的网络安全培训计划。

四、基于等保 2.0 工业控制系统网络安全技术防护的策略

（一）访问控制

在工业防火墙中设置精简且必要的访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。访问控制规则对数据包的源地址、目的地址、工控协议、源端口、目的端口，请求服务进行检查，实现数据的安全传输。

（二）强化边界防护力度

在等保 2.0 制度的导向之下，企业必须要对工业控制系统的网络边界作出细化明确，并制定出多元着手的安全防护技术方案。例如，可在工业控制系统的网域边缘设置准入隔离设备，并部署出工业网闸、工业防火墙等防御工事，以此在网络边界构筑起多层结合的安防壁垒，对外部环境中违规接入、非法入侵的威胁主体进行强效隔离。再如，可在防火墙的应用基础上，依托其病毒库建立起风险代码排查机制，对病毒库中已录入的病毒、木马、危险数据包等进行动态监测与同步反馈。

（三）入侵防范

在工业网络中的交换机旁路部署监测审计设备，对网络中的数据流量进行实时解析。同时利用白名单、黑名单规则库，实时监测针对网络攻击、异常操作、非法设备接入以及蠕虫、病毒等恶意软件的入侵并实时报警，同时详实记录一切网络通信行为，包括指令级的协议通信记录。

（四）安全审计

在网络核心部署运维堡垒机，针对运维人员在远程运维设备时，进行操作记录、分析、审计，为事后追溯提供依据。同时，利用监测审计设备白名单自学习机制，对异常通信行为进行审计并告警。

（五）安全管理中心设计

通过在生产管理层部署工控安全管理平台，实现对安全设备统一管理与监控。从整体视角进行安全事件分析、安全攻击溯源、安全事件根因挖掘等，为工控系统网络当前的状态以及未来可能受到的攻击做出态势评估与预测，为专业人员提供可靠、有效的决策依据，最大限度上降低工控系统可能遭受的风险和损失，提升企业安全防护整体水平。

（六）安全管理和人事管理机构。

安全管理系统机构及其人员管理系统的建设情况将能够在很大程度上决定整个安全管理系统构建的结果。在安全和人事管理机构中的相关网络安全管理团队小组可以由各个部门中的高级部门经理和各种部门领导人员组成，并通过这个人员组成机构负责协调和管理整个工业控制系统网络安全防护体系的各个方面，其中主要包括人事机构组成中的人才招聘、工作人员轮换、安全知识培训及教育管理等方面的内容。

五、结束语

总而言之，与前代制度相比，等保 2.0 的严格度更高、覆盖面更广、内容更精细、角度更多元，为广大企业的网络安全防护建设提出了新要求、指明了新方向。在实践中，企业应围绕物理环境、网络边界、异常感知、运维管理等多个方面，构建出完善、科学的安全防护技术体系，以将工业控制系统的运行质量始终维持在较高水平，为生产活动提供出稳定优质的工控保障。

参考文献：

[1] 李云飞 . 网络安全等级保护 2.0 工业控制系统安全测评实践 [J]. 网络安全技术与应用 , 2020(09):21-23.

[2] 安成飞 . 等保 2.0 下工业控制系统安全防护 [J]. 自动化博览 , 2019,36(S2):102-105.

[3] 赵峰 , 马跃强 . 基于等保 2.0 工业控制系统网络安全技术防护方案的设计 [J]. 网络安全技术与应用 , 2020(05):109-111.

[4] 王红岗 . 工业控制系统网络安全分析与管理策略探究 [J]. 化工管理 , 2020(11):93-94.

通讯作者：王鹏博，1993 年 10 月，男，汉族，河南永城人，现任河南省正龙煤业有限公司城郊煤矿助理工程师，本科。研究方向：计算机科学与技术。