工业控制网络的安全防护策略分析

高 磊
中国宝武马鞍山钢铁股份有限公司长材事业部 安徽 马鞍山 243000

摘 要：技术的拓展与革新为行业带来升级新思路的同时，也带来了负面影响，就工业控制网络的构建来讲，其受到网络完全问题的影响，可能出现经济损失的问题，因此需要针对这一层面准确分析，并结合分析结果制定对应的解决方案。本文将就目前工业控制网络的安全问题展开讨论，并根据分析的结果整理解决思路，以期提升工业控制网络的安全性能。

关键词：工业控制网络；安全防护；策略

引言：近年来，信息化技术在企业工业生产中应用愈加广泛和深入，企业智能化和自动化水平的提高，也广泛推广开来工业控制网络的应用。在工业控制网络中大量采用 TCP/IP 技术，愈加紧密联系着企业办公网络，因此也逐渐从封闭转为开放系统，其设计上对互联互通所需通信安全缺乏考虑，因此在开放工业控制网络系统过程中，其与外界隔离变弱、安全隐患问题凸显，需加强安全防御以保证工业生产顺利[1]。

1 工业控制系统网络结构及体征

随着科技的发展，工业控制网络体系不断的发展和完善。由原本独立元件所构成的控制体系，逐渐发展为电脑总控的控制体系 (DCS), 又到当下总控系统。工控系统已经由单一网络结构发展成面前集控制、监管、数据收集为一体的复杂网络控制体系。同时现在的工业控制体系也融入了许多科技前沿的元素。例如，在控制中使用可编程控制器 (PLC) 进行工业遥控完成机器的操作，以及通过电子设备建立机器间通信从而使机器工作效率更加精准高效。就目前工业控制体系来看它不再像以往传统控制体系那样单一“孤单”工控体系逐渐走进并融入当下互联网的“大家庭”之中[2]。虽然这种发展趋势有着很大的优势，但是它的弊端也是不可忽视的——结合互联网意味着工控体系的安全问题也将会如同如今互联网系统中所出现的网络安全那样出现信息泄露。所以怎样保证工业网络系统安全将成为急需解决的主要问题。

2 工业控制网络存在风险与安全问题

2.1 保护力度不足

很多管理者对工业控制网络安全防护认识比较浅显，认为要实现安全防护只需在与外部网络间建立物理隔离系统即可，因此重点在外部网络布设管理与技术，对工业控制网络本身安全问题和漏洞防护不足，实际构建的保护系统问题较多，结构、设备、行为和技术等要素未充分应用，缺乏足够保护力度。具体体现，一是结构方面风险评估不到位，未设置网络边界保护管理举措，导致相关企业设置的生产控制网与信息网直接连接通过VPN 即可完成访问，SCADA 系统中数据信息会被外部获取，在有防火墙的情况下也会因为与管理信息网处于同网段面临安全风险。二是设备方面，由于相关技术发展较晚，很多工业控制安全系统设备进口国外，在发现缺陷、协议问题后而及时修复难度大，进而无法实现自主管控，不利于组件可靠性输出，导致工业控制网络系统风险管理能力不足。三是行为方面，主要就是安全审计作业设置的缺失，IP 公用情况比较常见，系统出现异常行为后无法及时察觉的主要原因就是设计的保护防御体系监控、审计能力不足。四是技术方面，由于缺乏自主研发设备因此在控制系统管理方面由于薄弱的自主自控能力，无法由其中的服务无法进行可信计算模式计算[3]。

2.2 设备资产监管程度不够

相关企业在开展设备监管的环节，对于其中所包含的类型和数量的认知不够清晰，使得所构建的资产视图并不具备现实作用，出现设备变更等也难以形成对应的报告，无从考证设备重置的状态。并且部分企业所构建的业务系统中缺少对终端设备接入的管理措施，为外部网络攻击提供跳板，对于全面掌控能力的提升是种抑制。因此，所形成的网络不具备及时感知安全问题的能力，自然难以对攻击事件作出反应，给出反制的方案。

2.3 运维管理不完善

单位内安全组织机构人员职责不完善，缺乏专业的人员。没有针对信号系统成立专门的安全管理部门，未明确相关业务部门的安全职责和职员的技能要求，也缺乏专业安全人才。未形成完整的网络安全管理制度政策

来规划安全建设和设计工控系统安全需求。另外将工业控制系统的运维工作外包给第三方人员后并无相关的审计和监控措施，当第三方运维人员进行设备维护时，业务系统的运营人员不能及时了解第三方运维人员是否存在误操作行为，一旦发生事故无法及时准确定位问题原因、影响范围和责任追究。目前 CBTC 系统的网络采用物理隔离，基本可以保证正常生产经营。但是管理网接入工控系统网络后，工控系统网络内部的安全防护措施无法有效抵御来自外部的攻击和威胁，而且由于与管理网的数据安全交互必须在工控网络边界实现，因此做好边界保护尤为重要。

3 工业控制网络的安全防护策略

3.1 准确认识工业控制网络特点

在研究工业控制网络安全防御体系过程中，要掌握对应的作业项目和安全保护需求。工业控制网络安全保护需求与信息网络是存在差别的，因此不可直接使用信息网络中安全体系，需掌握工业控制网络安全防御体系要求。首先，对于工业控制网络来说，其业务请求响应时间段、难以随时更新，因此采取的加密等安全保护机制要满足响应要求、通信协议要。对 OPC 协议采取信息网络中加密机制会增加业务响应时间，不利于保证其运行安全性与稳定性。因此对于工业控制网络要保证袖完整的协议报文，传输两端要保证合法性身份。其次网络环境进行清晰界定，保证边界明确，有信息网络联通性强，因此操作行为、终端设备连接中会出现其局限内容不明、网络编制模糊的情况，复杂的网络环境加大了安全保护方面控制难度加大。工业控制网络则具有清晰可信的边界特点，因此可在可控网络环境中开展重点设备连接通信协议和其他操作行为，通过相关措施明确各种操作行为边界，形成有限的研究对象[4]。最后，设计安全防御体系过程中要结合工业控制网络特点，充分考量所使用理论是否适合实际项目。

3.2 建立统一监测管理平台

根据等级保护制度要求规定，重要等级在第二级以上的信息系统需要在网络中建立统一集中管理中心，通过统一安全管理平台能够对网络设备、安全设备、各类操作系统等的运行状况、安全日志、配置策略进行集中监测、采集、日志范化和归并处理，平台可以呈现 CBTC 系统中各类设备间的访问关系，形成基于网络访问关系、业务操作指令的工业控制环境的行为白名单，从而可以及时识别和发现未定义的行为以及重要的业务操作指令的异常行为。可以设置监控指标告警阈值，触发告警并记录，对各类报警和日志信息进行关联分析和预警通报[5]。

3.3 重视杀毒软件的应用和安装

在计算机中合理安装杀毒软件，有着保护网络安全运行的作用，同时也能为用户使用提供良好的环境。杀毒软件还有防护病毒侵入的功能。杀毒软件必须具有清除病毒、预防病毒以及查找病毒等功能，对于那些恶意侵害的木马、病毒进行清理，时刻为网络环境提供安全保护。杀毒软件包含了多种功能，所以合理使用杀毒软件有着重要意义。杀毒软件和多种计算机防护系统组成了计算机防御程序，杀毒软件是其中非常重要的部分，所以需要对其应用进行重视。

3.4 健全网络安全管理制度，配备和培训专业人员

逐步建立健全工业控制网络安全的专门管理机构，制定安全方针和管理制度，完善企业内部的网络安全防护策略和流程，明确工控系统安全防护管理职责，加强人员培训及专业人员队伍建设，强化相关专业人员的安全防护意识，落实工控系统安全防护策略，制定工控系统网络安全的应急预案并定期组织演练，规范工业控制系统的数据备份及快速恢复机制，提升安全应急处置水平[6]。

结束语：工业控制网络打破了原有的相对的独立和隔离，与外界网络互联越来越多，且近年来专门针对工业控制系统的网络攻击愈发频繁。针对工业控制网络的安全防护风险，各企业应根据工控系统的实际配置情况进行深入分析，制定安全防护策略，以及建立起企业工控网络全寿命周期的安全纵深防御体系，抵御日渐增加的工业控制系统网络安全风险。

参考文献：

[1]张宇亮,金忠新,李杨.铝工业控制系统网络安全分析及策略[J].轻金属,2021,No.491(09):58-65.

[2]闫飞.工业控制系统终端设备信息安全防护体系研究[J].仪器仪表用户,2021,26(01):80-82.

[3]王迎,许剑新.工业控制系统安全风险分析与对策[J].自动化博览, 2021,35(S2):76-82.

[4]淮文军,王峰,陈夏裕等.工业互联网环境下水务工控系统网络安全防护研究 [J]. 电脑编程技巧与维护,2021,000(001):157-158,172.

[5]宋甜.工业控制网络的安全防护策略分析[J].中国设备工程,2021(12):115-116.

[6]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.