自主可控下信息安全的研究与应用

Research and Application of Information Security under Autonomous Control

陈光林

Guanglin Chen

中国平煤神马集团中平信息技术有限责任公司　中国·河南 平顶山 467000

China Pingmei Group Zhongping Information Technology Co., Ltd., Pingdingshan, Henan, 467000, China

摘　要：根据“企业两化融合到一定程度，网络安全威胁向其加速渗透，工业领域面临的信息安全形势日益紧迫，亟需加速完善工业信息系统安全保障体系”的难题，论文从安全通信网络、安全区域边界、安全计算环境、安全管理架构等多个维度出发，分析建设集团统一的工业云信息安全防护体系势的必要性和相关关键技术。

Abstract: According to “enterprise two fusion to a certain degree, the network security threats to accelerate penetration, information security situation faced by the industry is increasingly urgent, needs to accelerate improving the industrial information system security system”, starting from the dimensions of secure communication network, secure area boundary, secure computing environment and security management architecture, this paper analyzes the necessity and related key technologies of building a unified industrial cloud information security protection system of the group.

关键词：自主可控；系统自愈；安全防护体系；安全机制

Keywords: autonomous control; system self-healing; safety protection system; safety mechanism

DOI: 10.12346/etr.v3i2.3489

1 引言

工业控制系统作为工业企业生产运行的中枢神经，是企业关键信息的基础设施，在信息化时代扮演着越来越重要的角色。随着两化融合的不断加深，物联网、大数据、人工智能等先进技术在企业生产控制系统中的应用以及工控系统网络信息安全问题越来越突出，工控网络安全成为企业开展正常生产经营活动必不可少的重要保障。

针对“工业信息系统逐步从单机走向互联、从封闭走向开放，网络安全威胁向其加速渗透，工业领域面临的信息安全形势日益紧迫，亟需加速完善工业信息系统安全保障体系”的难题，本项目从安全通信网络、安全区域边界、安全计算环境、安全管理架构等多个维度，全方位研究集团企业云信息安全防护架构，提升各生产企业的整体网络安全，确保设备、系统、网络的可靠性、稳定性，减少人员的工作量，提高安全生产管理水平、工作效率和管理效率[1]。

经过十多年的发展，中国平煤神马集团两化融合建设成果丰硕。自行开发或联合开发各类信息化系统，并打造成为行业内领先的工业云，涵盖集团安全、生产、管理各个领域。随着集团工业云流量的逐年增长，网络攻击的频率和严重程度都在逐年提高，遭受网络攻击后的自愈能力越来越差，因此建设集团统一的工业云信息安全防护体系势在必行。

2 项目技术创新点

①研究了构建纵深信息安全防护体系，有效抵御护网行动攻击。

②研究了工业控制系统信息安全防护架构，并完成了中平神盾系列产品研发，提升集团工业控制信息安全水平。

③在不影响矿井原有生产系统网络结构的情况下，研究

【作者简介】陈光林（1969-），男，中国河南永城人，本科，工程师，从事企业智能化改造、智能矿山建设及互联网云中心方面的研究和应用工作。

了对边缘层接入设备访问流量进行全过程监、控、审。

④在集团平台侧综合运用下一代防火墙、云平台的基于 SDN 和 NFV 技术的 VFW 功能，实现集团云平台内部业务的南北向七层防护、东西向流量隔离。

⑤通过具备沙箱技术和在线安全服务的 WEB 应用防护系统对集团工业云的互联网发布流量进行攻击过滤。

⑥在集团办公城域网内通过多标签协议交换技术构建逻辑专网，实现生产业务数据的保密传输。

3 集团整体安全建设

根据等级保护安全技术要求第三级中三重防护的思想和控制要求，安全技术体系建设包括安全计算环境防护建设、安全区域边界防护建设、安全通信网络防护建设，以及安全管理中心建设等几个方面。

3.1 系统设计标准

本项目是根据《信息安全技术 网络安全等级保护基本要求 第 1 部分：安全通用要求》的基本要求和安全目标，参照《信息安全技术 网络安全等级保护设计技术要求 第 1 部分：通用设计要求》具体内容，针对第三级系统提出的安全保护设计方案。

3.2 安全计算环境防护设计

依据等级保护要求第三级中设备和计算安全、应用和数据安全等相关安全控制项，结合安全计算环境对于用户身份鉴别、自主与标记访问控制、系统安全审计、恶意代码防护、安全接入连接、安全配置检查等技术设计要求，安全计算环境防护建设主要通过身份鉴别与权限管理、安全通信传输、主机安全加固、终端安全基线、入侵监测 / 入侵防御、漏洞扫描、恶意代码防护、Web 应用攻击防护、网络管理监控、安全配置核查、安全审计，重要节点设备冗余备份，以及系统和应用自身安全控制等多种安全机制实现。

3.3 安全区域边界防护设计

网络层架构设计：主要网络设备、安全设备的业务处理能力应能满足业务高峰期需要，保证各项业务运行流畅 , 避免将重要网络区域部署在网络边界处且没有边界防护措施。

安全域及安全子域划分：在同一个管理机构的管理控制之下，保证遵循相同的安全策略；具有相似的业务类型或相似的用户群体，安全需求相近，保证遵循相同的安全策略；具有相同的物理位置或相似的运行环境，有利于采取统一的安全保护机制；面临相似的安全威胁，需采用相似的安全控制措施来保证安全性。

3.4 安全通信网络防护设计

安全通信网络对通信安全审计、通信数据完整性 / 保密性传输、远程安全接入防护等安全设计要求，安全通信网络防护建设主要通过通信网络安全传输、通信网络安全接入及通信网络安全审计等机制实现。功能设计包括：通信网络安全传输、远程安全接入防护、通信网络安全审计。

3.5 安全管理体系设计

安全管理体系设计包括安全策略和管理制度建设、安全管理机构和人员建设、安全建设管理及安全运维管理等几个部分。安全策略和管理制度是对信息安全目标和工作原则的规定，其表现形式是一系列安全策略体系文件，是信息安全保障体系的核心。信息安全领导小组应由单位高层领导和有关部门的管理人员组成，负责协调、指导及管理信息安全各个方面的工作。安全建设管理应贯穿信息系统整个生命周期。

3.6 安全防护部署设计方案

中国平煤神马集团核心网络分为外网和内网，外网区域直接采用公网地址，主要用于集团对外业务的发布。基层单位办公局域网和单位工业网之间均部署硬件防火墙或者网闸，进行边界防护。

边界防护设计：工业防火墙在工控协议方面做了深度的解析，对基于 IP、MAC、工控协议或任意组合方式的访问进行控制，用户根据具体需求设置更细粒度的策略。在工业防火墙上启用白名单功能，将工控网络中可信的软件或程序放入白名单，可以有效阻止恶意病毒和木马的入侵或非法程序的运行 [2]。

3.7 安全监测与审计方案设计

安全审计通过收集并分析系统日志等数据，从而发现违反安全策略的行为。安全审计主要侧重于事后分析，当发生安全事故或者发生违反安全策略的行为之后，通过检查、分析、比较审计系统收集的数据，从中发现违反安全策略的行为 [3]。

3.8 Web 应用安全防护设计

Web 应用安全网关能够快速识别防护常见的 Web 攻击：如基于 HTTP 协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼攻击；SQL 注入攻击、XSS 攻击等 Web 攻击；爬虫、CGI 扫描、漏洞扫描等攻击。其安全防护主要体现在针对 Web 攻击的防护、Web 非授权访问防护、Web 恶意扫描防护、Web 应用合规、应用交付服务等方面。

3.9 VPN 综合安全网关

VPN 安全网关具备 SSL VPN、IPSec VPN 和拨号接入网

（下转第 135 页）

雨水口支管与雨水口允许偏差如表 1 所示。

表 1 允许偏差

序号	项目	允许偏差（mm）	检验频率		检验方法
			范围	点数	
1	井框与井壁吻合	≤10	每座	1	用钢尺量测
2	井框与周边路面吻合	−5～0		1	用钢尺量测
3	雨水口与路边线间距	≤20		1	用钢尺量测
4	井内尺寸	0～+20		1	用钢尺量，取最大值

准备做好对地质、水文和地下管线的调查和勘测工作，制定安全技术措施；所用管材、砖、砂、石等材料应堆放整齐，距沟边 1.0m 以外；沟槽两边设置临时排水沟，以免雨水流入沟内造成塌方；沟槽两端和交通道口设置明显的安全标志，夜间加挂红灯。开挖前，施营人员必须向司机进行详细交底，交底内容应包括挖槽断面、堆土位置、地下设施以及施工安全技术要求；沿线应根据生产和居民的需要设置便道或便桥，在便桥两侧应设置坚固的栏杆，确保安全；准备好沟槽开挖时的排水设备 [4]。

5 结语

施工技术和管理人员一定要保证生产组织系统、质控系统完善。创优各项工作，施工期间随时记录，留下必要的影像资料，质量管理进行全方位质量控制，解决全部问题。

参考文献

[1] 张孟然.国外市政工程项目进度管理对我国的启示[J].中国住宅设施,2012(2):56-58.

[2] 余波.浅析市政给排水工程的规划与设计[J].科技资讯,2012(1):54.

[2] 刘庆峰.浅析市政给排水工程项目进度管理的新模式[J].科技资讯,2011(1):28-30.

[3] 梅润华.浅谈市政工程的造价管理控制——以苏州污水处理厂改造为例[J].科技创新导报,2010(29):194.

[4] 朱华希.试论市政工程给水排水施工管理[J].现代物业(上旬刊),2011(5):78-79.

（上接第 130 页）

关等综合安全接入能力。VPN 安全网关支持标准加密协议，密码算法不仅支持国际标准 RSA 系列、AES 系列、DES 系列、MD5、SHA 系列等；还支持国密标准的 SM1~SM4 系列，支持国密 Ukey[4]。

3.10 APT 攻击检测系统

APT 检测系统采用中国领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤；同时可结合人工服务，有效发现 APT 攻击 [5]。

4 社会效益分析

项目通过对集团工业云的信息安全架构进行整体设计，构筑工业云信息安全防护体系，提高企业生产控制系统安全防御能力。有计划、分步骤地为各个生产业务单元工控网络提供一个可控、可靠、可信的网络空间环境，有效保护生产控制系统、服务器、工作站、控制器等免遭病毒、木马以及恶意攻击的破坏，确保生产控制网络的传输、接入和运行安全可控。通过此次信息安全架构的设计与实施，大大提高了集团工业云的承载能力，并为下一步集团智能化的发展提供了较为充足的性能余量。

5 结语

在互联网及大数据技术大发展的背景下，在国家政策、中国平煤神马集团领导层的高度重视和大力支持下，自主可控的信息安全项目必将为中国平煤神马集团信息化的发展提供更强有力的网络支撑，为集团的多业务网络整合提供更好的网络基础条件，同时也为同行及相关行业的网络升级改造提供参考样板。

参考文献

[1] 方兴东,胡怀亮.自主可控是实现网络强国的基本前提和阶段性目标[J].信息安全与通信保密,2014(9).

[2] 魏帅岭,侯立根,李星,等.三级等级保护下医院网络边界安全的防护与设计[J].网络安全技术与应用,2019(12).

[3] 柳婵娟.网络安全审计与监控系统的设计与实现[J].电脑知识与技术·学术交流,2008(25).

[4] 王炜.给明文协议加密[J].网管员世界,2009(16).

[5] 赵澄,方建辉,姚明海.工业控制网络中APT攻击检测系统设计[J].计算机测量与控制,2018(26).