案例

长扬科技（北京）有限公司

主标题：地铁信号系统等级保护（三级）实施方案

副标题：基于 CBTC 系统的工控防护解决方案

引言：企业概况 XXX，项目建设的政策、业务创新等驱动因素等

长扬科技是北京国资委和经信委投资、指导下的创新型高新技术企业，汇集中国工业网络安全人才最集中最精英的企业，是中国工业网络事业的第一批践行者。公司聚焦工业网络安全及安全大数据领域，为客户持续提供覆盖工控系统整个生命周期的网络安全解决方案和安全服务，致力于成为工业互联网安全行业应用专家。

公司产品及解决方案主要应用于工业控制网络、物联网及关键基础设施网络安全防护领域，在石油化工、煤炭、电力、轨道交通、高铁、公共安全、军队军工、智能制造及政府教育等行业做了大量的工业网络安全行业研究和实践，对于工业网络安全场景化应用认知和落地能力业界领先。

随着计算机和网络技术的发展，特别是信息化与信号系统深度融合，CBTC 系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与 PIS 网络、语音广播等其他子系统互联，甚至与公共网络连接，造成病毒、木马等威胁向 CBTC 系统扩散。一旦 CBTC 系统的信息安全出现漏洞，将对城市轨道交通

的稳定运行和旅客的人身安全造成重大影响。

本项目以“安全分区、网络专用、三网隔离、分级防护”为原则，以 GB/T 22239 为标准，在技术层面实现地铁基于 CBTC 的信号系统内各子系统统一技术架构和标准，建设满足信息系统安全等级（三级）要求的防护方案。

一、项目概况

地铁信号系统是保证列车安全、准点、高密度运行的重要技术装备。本方案是针对 Y 市某号线信号系统的符合等级保护（三级）要求的安全防护建设方案。

1. 项目背景

目前基于无线局域网的 CBTC 系统的可用性、可靠性等均能满足当前城市轨道交通安全高效运营的需要，是实现轨道交通高安全、高速度和高密度的最佳技术之一。但 CBTC 系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与 PIS 网络、语音广播等公共网络连接，造成病毒、木马等威胁向 CBTC 系统扩散，信号系统安全问题日益突出。一旦 CBTC 系统的信息安全出现漏洞，将对城市轨道交通的生产运行和国家安全造成重大隐患。

Y 市地铁运营公司在《轨道交通信息安全技术架构》中提出信息安全建设的总体目标为：全面防护、保护重点、专区专用、强化边界，旨在提升信息安全的预警能力、保障能力、检测能力、应急能力和恢复能力。要求以 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》等相关技术标准为基础，“安全分区、网络专用、三网隔离、分级防护”为原则，在技术层面要求各系统统一技术架构和标准，按信息系统安全等级（三级）要求建设、实施。

目前 Y 市某号线信号系统是采用基于通信的列车控制系统（CBTC）。鉴于信号系统在轨道交通中的重要性，结合公安部网监和 Y 市市轨道交通有限公司的要求，将 Y 市某号线信号系统信息安全保护等级定为三级（S3A3G3）。

2. 项目简介

本方案针对 Y 市某号线信号系统，进行了符合等级保护（三级）要求的实施方案设计，提出一个基于纵深防御的分域安全防护与运维保障体系，同时它也是基于信号系统内生特性的安全防护体系。本方案在控制中心、各设备集中站、车

辆段和停车场等从边界隔离防护和访问控制、入侵防御、监测审计和主机安全方面，进行了合理的安全部署设计和安全服务咨询设想，提供实际的安全防护产品部署建议与选型建议。

3. 项目目标

依据工信部《工业控制系统信息安全防护指南》指导要求，结合信息安全等级保护（三级）符合性要求，轨道交通信号系统安全防护建设目标如下：

（1）完善轨道交通信号系统安全防护技术体系：

梳理、分析轨道网络整体情况，从网络层次划分、网络分区分域、网络边界划分、纵深防御等方面提供适用于轨道交通信号系统的网络规划思路；

（2）完善轨道交通信号系统安全防护管理体系：

梳理轨道交通信号系统安全防护方面的组织机构、管理制度、人员管理、系统建设管理、资源保障、监督检查等方面的信息，进行需求分析并提出解决思路，为轨道交通信号系统管理体系建设及整改工作提供参考；

（3）完善轨道交通信号系统安全防护运维体系：

梳理、分析轨道交通信号系统的运维体系，从运维管理制度、操作流程的规范化、关键技术控制点等方面提供运维体系建设及完善思路，挖掘运维平台潜在风险和盲区，为完善轨道交通运维平台提供解决思路。

本方案针对 Y 市某号线信号系统进行细致的分析，并结合等级保护（三级）基本要求以及信号系统的特殊安全需求提出一个基于纵深防御的分域安全防护与运维保障体系。协助客户出具《信息系统安全等级保护定级报告》、《信息系统安全等级保护备案表》并在当地公安机关完成信息系统等保备案，然后依照等级保护安全技术要求，将从网络安全、主机安全、数据安全以及应用安全四个方面对轨道交通信号系统的安全防护分别展开预评估与整改。

本项目的目标是在 Y 市地铁某号线信号系统正式开通运营之前完成一次等级保护三级测评工作。

二、项目实施概况

本节重点详尽描述，技术与业务结合，工业互联网技术如何助力业务提升与

创新，如何解决企业痛点和难点，其核心价值体现在哪些方面。此处可以有几句统领性描述。

结合等级保护（三级）基本要求以及信号系统的特殊安全需求，对于 Y 市轨道交通某号线信号系统信息安全建设，以适度风险为核心，以重点保护为原则，从业务的角度出发，重点保护重要的业务系统。本方案将从网络安全、主机安全、数据安全以及应用安全四个方面对轨道交通信号系统的安全防护分别展开阐述。

1. 项目总体架构和主要内容

为提升成熟轨道交通各子系统网络安全防护能力，长扬科技在充分了解 CBTC、ISCS、AFC、PIS 等系统的网络结构和安全现状的基础上，深度融合轨交业务系统，构建从边界防护、流量检测审计、主机终端安全、持续运维安全的纵深防御技术体系。在不破坏原有网络结构情况下，轨交解决方案能切实有效的保护系统安全，防止木马、蠕虫、黑客等各种威胁和攻击，保障轨道交通安全稳定运行

（1）网络边界安全防护

CBTC、ISCS、PIS 等系系统之间存在互联接口，但缺乏可靠的技术隔离手段进行区域隔离，给整个轨道交通系统留下安全隐患，长扬科技通过在控制中心 ATS 网络与互联系统间（PIS、ISCS、PA 等）接口的网络边界位置，部署工业网闸(IAD 智能保护平台)。互联网络之间进行网络连接时，可以基于 IP 地址、MAC 地址等对请求连接主机的身份进行鉴别，禁止未通过身份鉴别的主机之间建立网络连接，互联接口具备访问控制措施，基于智能学习的白名单和黑名单的访问控制。访问控制主、客体粒度细化到 IP 地址、MAC 地址、应用协议及应用数据，包括生产数据上传和调度指令的下发； 支持 FTP、HTTP、Modbus/TCP、OPC、IEC-104、MMS、DNP3 等并且能够对各类数据包进行快速有针对性的捕获与深度解析常用工控协议传输的数据格式的鉴别与过滤。对互联网络之间的访问行为进行实时数据包抓取和分析，对异常行为进行检测，实时阻断威胁事件；涵盖了各大主流工控设备的设备及协议漏洞库，可以基于已知设备及协议的漏洞库黑名单机制保护工业控制网络避免受到已知漏洞的危害。针对外部系统边界采用专用的安全通道进行内外网信息交换，业务数据通过物理隔离、协议隔离、内容隔离

等措施使外部系统网络数据及有害数据信息无法进入 ATS 网络。

在控制中心 ATS 与各区域边界位置部署工业防火墙。实现隔离与访问控制，根据数据包的源地址、目的地址、传输层协议、应用层协议、端口（对应请求的服务类型）、时间、用户名等信息执行访问控制规则识别工控网络中已知的安全威胁。

（2）网络流量安全

外部攻击和内部误操作行是引发城市轨道交通安全问题的重要因素，长扬科技通过在关键位置控制中心、车辆段、停车场和设备集中站的维护网接入交换机处旁路部署网络工业网络监测审计平台。对全网数据流量、网络数据智能学习生成白名单规则，结合黑名单规则统一规则部署进行协议级审计，实时监控控制网络安全，发现异常行为及病毒木马。

（3）主机安全防护

在系统中工控主机不能安装杀毒软件或杀毒软件不能及时更新升级，一旦遇到新的漏洞将影响业务的安全运营，长扬科技通过在控制中心、车站、车辆段、停车场等处的工作站和服务器部署工控主机卫士终端安全防护产品，开启主机白名单安全防护，监控工控主机的进程状态、网络接口状态、USB 端口状态，以白名单的技术方式，禁止一切非法进程的加载和启动，从而使工控网络中的上位机、服务器等抵御木马、工控病毒等恶意程序的攻击。切断病毒和木马的传播与破坏路径，彻底解决主机不能安装杀毒软件或病毒库升级后影响程序运行的问题。

（4）统一安全管理

为实现对轨道交通系统防护设备的集中管理，帮助工作人员全面了解和掌握各个系统的安全状态。长扬科技通过在车辆段部署统一安全管理平台，统一管控所有工控网络安全设备与安全防护手段，将系统的工控网络安全现状实时、全面地进行监控。对于保护终端所产生的安全事件和平台系统事件进行行为关联性追踪，找到引起当前结果事件的源头事件，为分析从源头事件到结果事件的整个过程提供依据。建立工业控制网络日常行为基准，对当前网络的异常行为做实时动态的行为审计，找到控制网内符合协议规范，但不符合企业日常生产规律的隐秘异常的行为，帮助发现内部误操作，内部攻击等不易发现的安全威胁。专业的工业控制网络拓扑构建和管理工具，提供丰富的资产信息展示功能，同时关联多种

安全分析工具，呈现丰富的功能视图，对拓扑管理进行颠覆式的功能改进，帮助用户最大化的了解自身工业控制网络，以及提高全面的安全态势感知能力。

信号系统网络安全部署示意图如下所示：

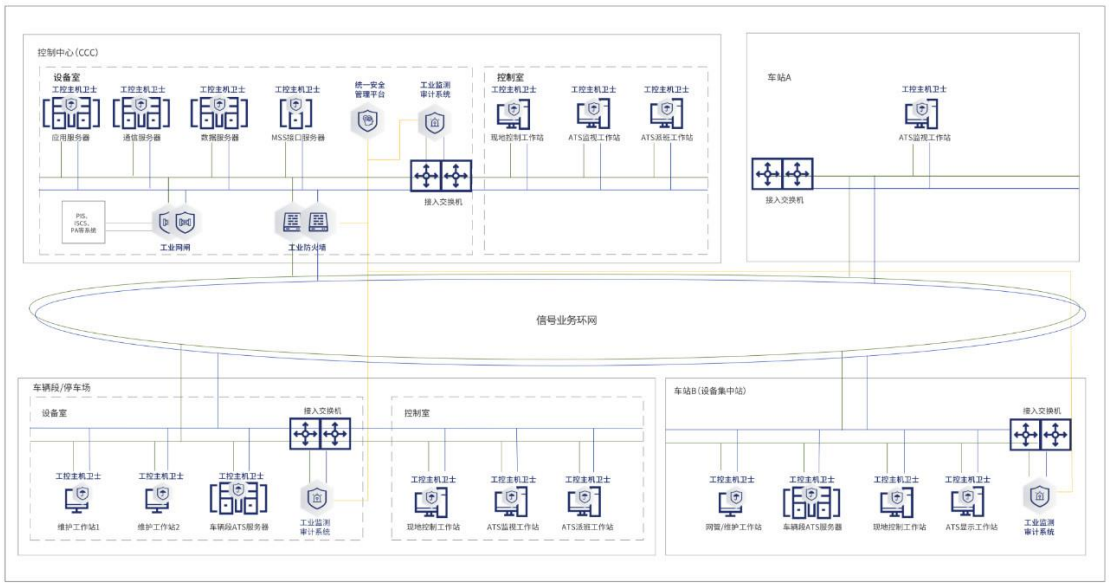

图 1　信号系统网络安全部署示意图

2.安全架构

在本项目中，在基于信号系统自身的信息采集与传输上，在不改变原有网络结构，不影响原有工控网络系统正常生产运行的情况下，基于旁路的方式部署监测审计平台旁路监听。在通信安全、传输协议和标准方面，具备专业协议深度解析，已经支持的工控协议深度解析是 GOOSE，SV，MMS，IEC104，DNP3，OPC，S7，Modbus/TCP，Profinet，Ethernet/IP 等协议，并可对协议数据包深度解析。在配置方式上，采用 WEB 配置 IP 地址，不需要串口线、CLI，方便现场实施部署。网络拓扑管理采用专业的工业控制网络拓扑构建和管理工具，提供丰富的资产信息展示功能，同时关联多种安全分析工具，呈现丰富的功能视图，对拓扑管理进行颠覆式的功能改进，帮助用户最大化的了解自身工业控制网络。

3. 安全及可靠性

本项目不仅仅是 Y 市轨道交通信号系统信息安全防护试点项目，更是为轨道交通行业的网络安全防护做出了技术示范作用，优化管理流程，切实保证了信号系统免受病毒、恶意代码等威胁，保持安全稳定运行的状态。安全框架参考《信

息安全技术 信息系统等级保护安全设计技术要求》进行设计，在管理方面同时参考《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》以及27001 安全管理指南，使建成后的等级保护体系：

1、资产安全以资产安全为核心，资产管理包括安全设备管理、工控设备管理、网络设备管理。对网络系统内未知的设备接入、异常连接、异常流量进行实时告警，迅速发现网络系统中异常情况。保障资产按时按规定的正常运行和及时检测出资产的异常行为。

2、区域防护借鉴了纵深防御的思想，形成以边界监测、区域监测、终端监测的防护体系。

三、项目创新点和实施效果

1. 项目先进性及创新点

（1）全系列的工控安全产品

提供全系列工控安全产品，可以满足不同工控系统信息安全防护项目的需要。

（2）一键式部署

产品采用 EB 配置，不需要串口线、CLI，方便现场实施部署，所有黑名单规则、白名单规则可以统一调入到规则库，进行一键式部署，方便快捷，可自动调整安全规则及保护策略之间的冲突，简化部署过程

（3）硬件平台安全

硬件方面适应工控系统冗余、时延、可靠性、环境等各方面的要求：1) 硬件设计支持硬件加密。在现场能够实现多种灵活的安装方式，包括导轨安装、机柜安装等。2) 可以在各种行业需要的环境下运行，扩展性强，无风扇全封闭设计，达到工业级的可靠性和稳定性 MTBF 标准和工业级宽温标准。3) 支持多电源冗余和端口故障时的自动硬件旁路转换。端口设计上采用与数据网分离的管理网端口，并支持千兆以太网。

2. 实施效果

本项目实现了项目目标需求，解决了网络系统风险管理与入侵防护；在网络层面生产网边界，实现网络接口安全；通过区域隔离，结合黑\白名单的访问控制实现恶意代码防范。对系统运用的多项先进技术，系统整体性能和安全性进行日常维护管理。完善了 Y 市轨道交通信号系统信息安全保护体系，为等保测评的顺利通过提供了安全保障。

（1）入侵检测：

对网络的当前和历史行为与事件进行工业控制安全入侵分析、检测与发现，对缓冲区溢出、SQL 注入、DoS 攻击、蠕虫病毒、木马后门、aveX、Sand-Worm、Stuxnet 等各类黑客攻击和恶意流量进行实时检测及报警，发现 APT 攻击和工业病毒的入侵痕迹，并通在安全管理平台显示、日志数据库记录，提供对应的防护修护策略

（2）工业协议深度解析：

目前已经支持的工控协议深度解析是 GOOSE，SV，MMS，IEC104，DNP3，OPC，S7，Modbus/TCP，Profinet，Ethernet/IP 等协议，为工控网络安全领域最多

（3）访问控制：

对数据流量进行管控，通过端口、地址、协议等方式对数据流量进行筛选，保证流量合法性。

（4）实时报警：

所有部署的安全设备都能由安全管理平台统一控制配置、管理安全终端，对安全终端部署安全规则，监测终端所在网络的通信流量与安全事件。对于保护终端所产生的安全事件和平台系统事件进行行为关联性追踪，找到引起当前结果事件的源头事件，为分析从源头事件到结果事件的整个过程提供依据。

（5）流量审计：

对工控网络中存在的所有活动提供协议审计、行为审计、内容审计、流量审计，生成完整记录便于事件追溯。基于工业协议的深度包解析白名单和黑名单的工控异常行为审计，协助用户发现网络中存在的违规下发的控制操作。