工业互联网
典型安全解决方案案例汇编
（V1.0）

工业互联网产业联盟（AII）

2017 年 11 月

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目　录

前　言

为落实《中国制造 2025》规划，工信部明确了工业转型升级的重点领域和工作要求。工业互联网作为新一代信息技术与工业系统深度融合形成的产业和应用生态，是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果。它通过智能机器 间的连接并最终将人机连接，结合软件和大数据分析，重构全球工业、激发生产力，让世界更美好、更快速、更安全、更清洁且更经济。工业互联网的发展得到全球主要国家以及我国政府的高度重视和积极推进，产业界也正在加速开展相关探索和实践。

工业互联网广泛应用于能源、交通以及市政等关系国计民生的重要行业和领域，已成为国家关键信息基础设施的重要组成部分。工业互联网打破了传统工业相对封闭可信的制造环境，病毒、木马、高级持续性攻击等安全风险对工业生产的威胁日益加剧，一旦受到网络攻击，将会造成巨大经济损失，并可能带来环境灾难和人员伤亡，危及公众安全和国家安全。工业互联网自身安全可控是确保其在各生产领域能够落地实施的前提，也是产业安全和国家安全的重要基础和保障。

本案例汇编了工业互联网领域七个领域十八个典型安全解决方案案例，可作为工业互联网生态链上下游供应商、工业企业用户等在规划、建设和运营工业互联网时的安全参照。

本汇编由中国移动通信集团公司牵头编制，重点参与单位有中国信息通信研究院、启明星辰信息技术集团股份有限公司、北京威努特

技术有限公司、中国电子信息产业集团第六研究所、北京奇安信科技有限公司（360 企业安全）等。

本报告的参编人：张峰、田慧蓉、李转琴、张尼、陶耀东、郑凌鹏、卢凯、訾立强、齐旻鹏、张扬；其中，林欢等协助审核了全文，并提出了诸多宝贵意见，在此一并致谢！

工业互联网的发展将是一个持续演进的过程，安全风险和应对措施也会随之持续演进和不断完善；联盟将持续跟进国内外工业互联网安全发展趋势和产业界反馈的意见，在持续研究的基础上对汇编进行修订或发布新版本的案例汇编。

工业互联网产业联盟 安全组

二〇一七年十一月

1. 工业互联网安全概述

1.1 工业互联网概述

工业互联网的内涵用于界定工业互联网的范畴和特征，明确工业互联网总体目标，是研究工业互联网的基础和出发点；工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。其本质是以机器、原材料、控制系统、信息系统、产品以及人之间的网络互联为基础，通过对工业数据的全面深度感知、实时传输交换、快速计算处理和高级建模分析，实现智能控制、运营优化和生产组织方式变革。

1.2 工业互联网安全架构

工业互联网的安全需求可从工业和互联网两个视角分析。从工业视角看，安全的重点是保障智能化生产的连续性、可靠性，关注智能装备、工业控制设备及系统的安全；从互联网视角看，安全主要保障个性化定制、网络化协同以及服务化延伸等工业互联网应用的安全运行以提供持续的服务能力，防止重要数据的泄露，重点关注工业应用安全、网络安全、工业数据安全以及智能产品的服务安全。因此，从构建工业互联网安全保障体系考虑，工业互联网安全体系框架，如图 所示，主要包括五大重点，设备安全、网络安全、控制安全、应用安全和数据安全。

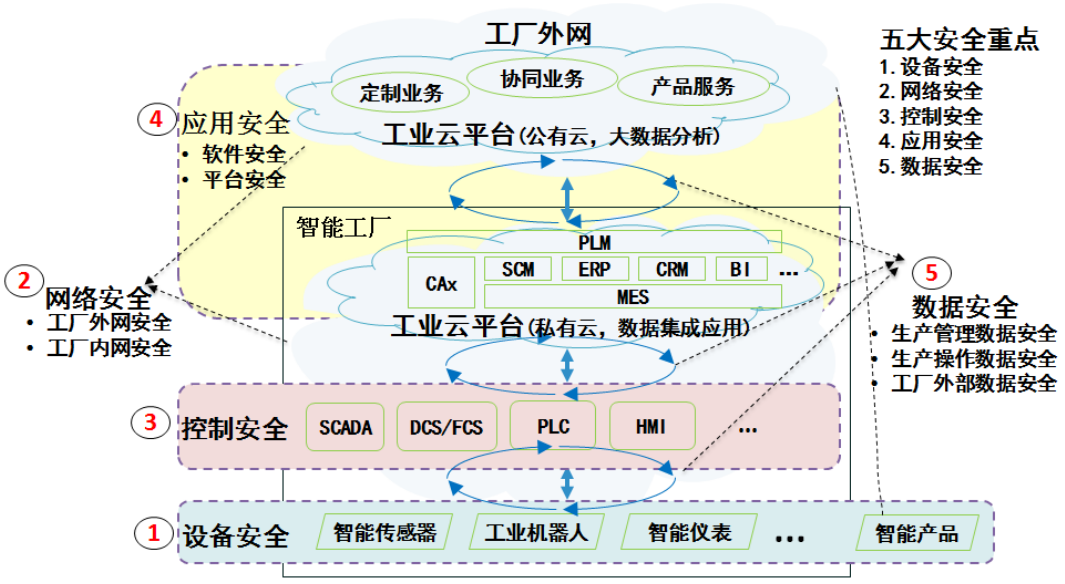

图 1 工业互联网安全体系

- **设备安全**是指工业智能装备和智能产品的安全，包括芯片安全、嵌入式操作系统安全、相关应用软件安全以及功能安全等。
- **网络安全**是指工厂内有线网络、无线网络的安全，以及工厂外与用户、协作企业等实现互联的公共网络安全。
- **控制安全**是指生产控制系统安全，主要针对 PLC、DCS、SCADA 等工业控制系统的安全，包括控制协议安全、控制平台安全、控制软件安全等。
- **应用安全**是指支撑工业互联网业务运行的应用软件及平台的安全，包括各类移动应用；
- **数据安全**是指工厂内部重要的生产管理数据、生产操作数据以及工厂外部数据（如用户数据）等各类数据的安全。

1.3 工业互联网典型安全问题

新一轮的工业革命是工业互联网蓬勃发展的原动力。反之，工业互联网的快速发展又改变或催生了工业生产的设计、生产、物流、销售和服务模式。大规模个性化定制、远程运维和工业云等新兴业态崭露头角，并引起广泛关注。同时，“数字化、智能化、网络化”为特征的工业互联网既面临传统 IT 的安全威胁，也面临以物理攻击为主的信息通信技术（简称 ICT）的安全威胁。

安全保障能力已成为影响工业互联网创新发展的关键因素。随着互联网与工业融合创新的不断推动，电力、交通、市政等大量关系国计民生的关键信息基础设施日益依赖于网络，并逐步与公共互联网连接，一旦受到网络攻击，不仅会造成巨大的经济损失，更可能造成环境灾难和人员伤亡，危及公众生活和国家安全。

工业领域安全防护急需加强和提升。目前，工业领域安全防护采用分层分域的隔离和边界防护思路。工厂内网与工厂外网之间通常部署隔离和边界防护措施，采用防火墙、虚拟专用网络、访问控制等边界防护措施保障工厂内网安全。企业管理层网络主要采用权限管理、访问控制等传统信息系统安全防护措施，与生产控制层之间较多的采用工业防火墙、网闸、入侵防护等隔离设备和技术实现保护“数据安全”。生产控制层以物理隔离为主，工业私有协议应用较多，工业防火墙等隔离设备需针对专门协议设计。企业更关注生产过程的正常进行，一般较少

在工作站和控制设备之间部署隔离设备、进行软件升级，一般也不安装病毒防护软件以避免带来功能安全问题。控制协议、控制软件在设计之初也缺少诸如认证、授权、加密等安全功能，生产控制层安全保障措施的缺失成为工业互联网演进过程中的重要安全问题。

未来工业互联网安全主要面临以下几方面的问题：

（1）生产设备安全问题开始凸现。传统生产设备以机械装备为主，重点关注物理和功能安全。但未来的生产模式更强调终端的生产角色的扁平、协同，导致生产设备数字化、信息化、网络化、智能化水平不断提升；生产环节中人机交互过程逐渐减少甚至消失（如无人工厂、自动驾驶）。上述因素导致一些安全隐患难以发觉，更重要的是导致海量设备直接暴露在网络攻击之下。木马病毒能够在这些暴露的设备之间的以指数级的感染速度进行扩散。这种情况下，工业设备就成为安全攻击的“肉鸡”武器。近期美国域名服务商被大量终端设备攻击事件说明了这种攻击方式的巨大危害。

（2）端到端生产模式下的网络安全问题。为追求更高的生产效率，工业互联网开始承担从生产需求起至产品交付乃至运维的“端到端”的服务。比如大规模个人定制的服装行业，个性化定制的家电行业已经开始实现从由生产需求起至产品交付“端到端”的生产服务模式。无人化生产模式下，工厂网络迅速向“三化（IP 化、扁平化、无线化）+灵活组网”方向发展，工厂网络开始直接面临众多传统 IT 安全挑战。工业网络灵活组网的需求使网络拓扑的变化更加复杂，导致传统基于静态防护策略和安全域的防护效果下降。工业生产网络对信息交互实时性、可靠性的要求，难以接受复杂的安全机制，极易受到非法入侵、信息泄露、拒绝服务等攻击。“端到端”的生产模式、无人化生产发展趋势使得工业互联网安全防护的边界空前扩张，对安全防护机制的要求空前提高。

（3）控制安全问题。当前工厂控制安全主要关注控制过程的功能安全，信息安全防护能力不足。现有控制协议、控制软件等在设计之初主要基于 IT 和 OT 相对隔离以及 OT 环境相对可信这两个前提，同时由于工厂控制的实时性和可靠性要求高，诸如认证、授权和加密等需要附加开销的信息安全功能被舍弃。IT 和 OT 的融合打破了传统安全可信的控制环境，网络攻击从 IT 层渗透到 OT 层，从工厂外渗透到工厂内。遗憾的是，目前缺乏有效的应对 APT（Advanced

Persistent Threat，高级持续性威胁）攻击检测和防护手段。令业界最为担心的是控制安全问题最接近物理实体安全。从某种意义上，物理空间的损害成为现实。

（4）应用安全问题。网络化协同、服务化延伸、个性化定制等新模式新业态的出现对传统公共互联网的安全能力提出了更高要求。工业应用复杂，安全需求多样，因此对工业应用的业务隔离能力、网络安全保障能力要求都将提高。

（5）数据安全问题。数据是工业互联网的核心，工业数据由少量、单一、单向正在向大量、多维、双向转变，具体表现为工业互联网数据体量大、种类多、结构复杂，并在 IT 和 OT 层、工厂内外双向流动共享。工业领域业务应用复杂，数据种类和保护需求多样，数据流动方向和路径复杂，不仅对网络的可靠、实时传递造成影响，对重要工业数据以及用户数据保护的难度也陡然增大。

综上所述，数字化的、网络化、智能化生产设备安全、端到端生产模式下的网络安全，、生产控制系统安全、应用安全和数据安全是工业互联网发展急需解决的问题，其中终端设备安全、生产控制系统安全和数据安全尤为急迫。

2. 智能制造行业典型安全解决方案

智能制造就是将信息能力嵌入到制造过程，通过信息技术提高传统制造的智能化水平，打造智能工厂，提升企业的制造能力，改善资产运营效率。

本案例汇编包括两个智能制造行业的典型安全解决方案。

2.1 案例一：某汽车制造企业安全解决方案

2.1.1 概述

近几年，我国乃至全球汽车行业正在蓬勃发展，而在发展的同时，工业控制系统的安全问题成为制约行业发展的瓶颈。为了预防和减少汽车制造业在生产过程中的安全事故，保障员工的生命和企业的财产安全，现提出了在汽车制造生产过程中全面控制事故发生的有效安全防护措施。

2.1.2 典型安全问题

- 管理网络与生产网络之间、生产网络生产区与控制区之间、各生产区域之间缺乏必要的隔离控制措施，迫切需要对其进行安全防护；
- 工程师站、操作员站等主机可能会遭受病毒、蠕虫、木马等恶意软件入侵；
- 无法实现对工业网络中的恶意攻击行为、误操作行为等的实时检测和记录。

2.1.3 安全解决方案

- 在管理网核心交换机和生产网核心交换机之间部署工业防火墙，A 网 B 网冷备，与原有传统防火墙组成全面的边界安全隔离措施，完善网络边界的安全防护；
- 在虚拟服务器与生产服务器之间部署工业防火墙，对生产服务器设置对外只读控制策略，防止生产服务器数据被恶意篡改。

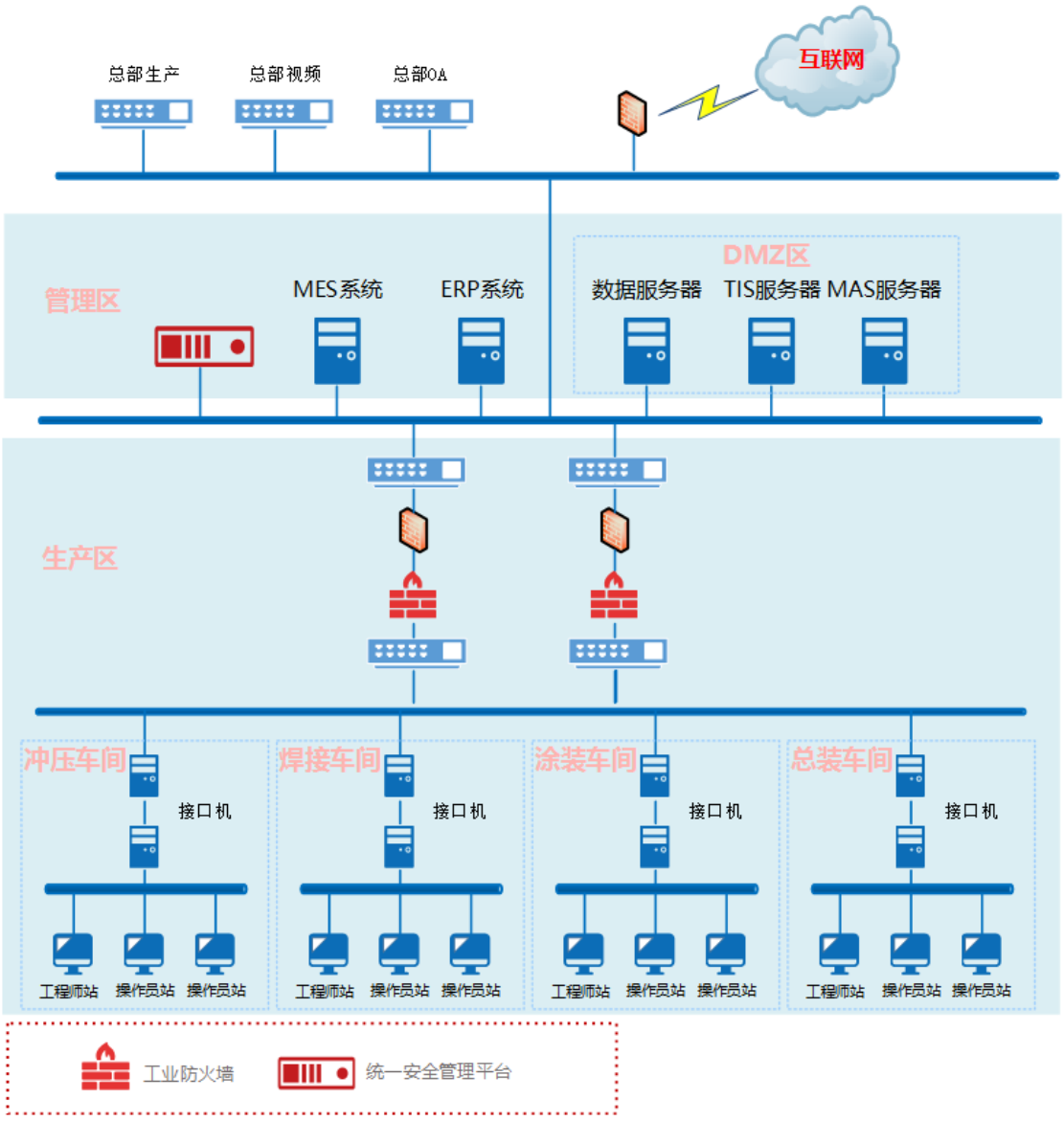

图 2 某汽车制造企业安全规划

2.1.4 小结

结合风险分析和案例技术分析，本解决方案具备如下特点：

- 实施网络边界划分、逻辑隔离和访问控制，满足行业政策法规及技术要求；
- 避免 PLC 被恶意攻击造成重大生产事故、人员伤亡和社会影响；
- 避免办公网被攻击造成病毒扩散导致工控主机操作指令下发失败及监控延时。

2.2 案例二：某先进制造企业安全解决方案

2.2.1 案例概述

某车辆制造集团在国家工信部 451 号文的指导下高度重视工业控制系统安全，在 2012 年印发了《工业控制系统信息安全管理办法（试行）》。

下属某公司为提高复杂产品的工艺创新能力、缩短产品研制周期、提高市场应变能力不断采用先进的协同设计与过程控制应用，按照信息安全同步建设、同步规划的思想，需要在使用先进的协同设计与过程控制应用时，从订单、设计、工艺、生产各环节中同步保障其信息安全。

作为国家重要的大型装备制造企业，该公司不仅承担着国家机车车辆制造的任务，为自身创造利润，也为国家的机车车辆走向世界付出努力，需要不断提高生产力，优化生产结构，所以必须“两化融合”且依赖先进的信息化手段。近年来引进了大批的国外的先进数控机床及技术，并且公司也在开展 DNC 网络的建设，生产网的互联性已有大幅提高。随着技术发展也引入了一些安全隐患：

通过建立符合某公司工控系统的信息安全管理体系、信息安全技术防护体系、信息安全运行体系，并将三个体系与 IT 安全现有体系融合，形成“三个体系，一个中心”的信息安全保障体系框架，实现办公网和生产网信息安全一体化管理和监控，支撑该公司智能制造生产和应用。

2.2.2 典型安全风险

先进制造工控系统中大量使用数控机床，一般有铣床、磨床、洗床、加工中心等，主体品牌有西门子、法兰克、马扎克等国外品牌，以及海天龙门、永进等国内品牌。通常设备接口有 RS232、RJ45 两种。工控网络的生产与管理网的管理关系如下图所示：

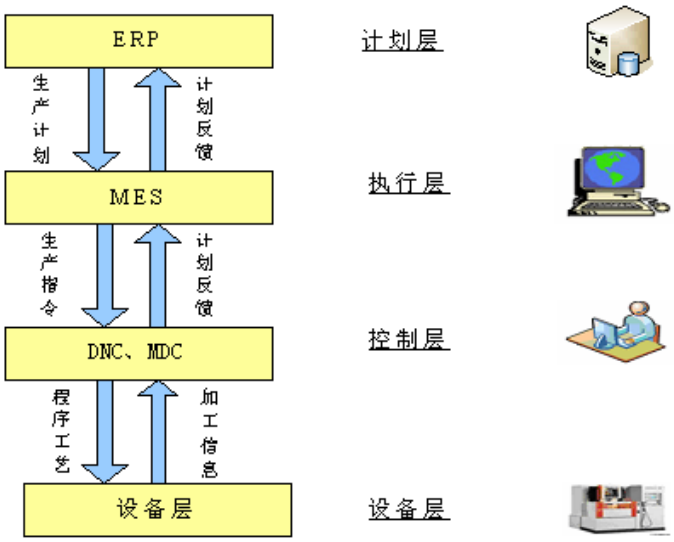

图 3 工控生产网与管理网的关系

传统车间里的机床设备基本都是通过串口连接，存在大量串网转换装置，如下图示意：

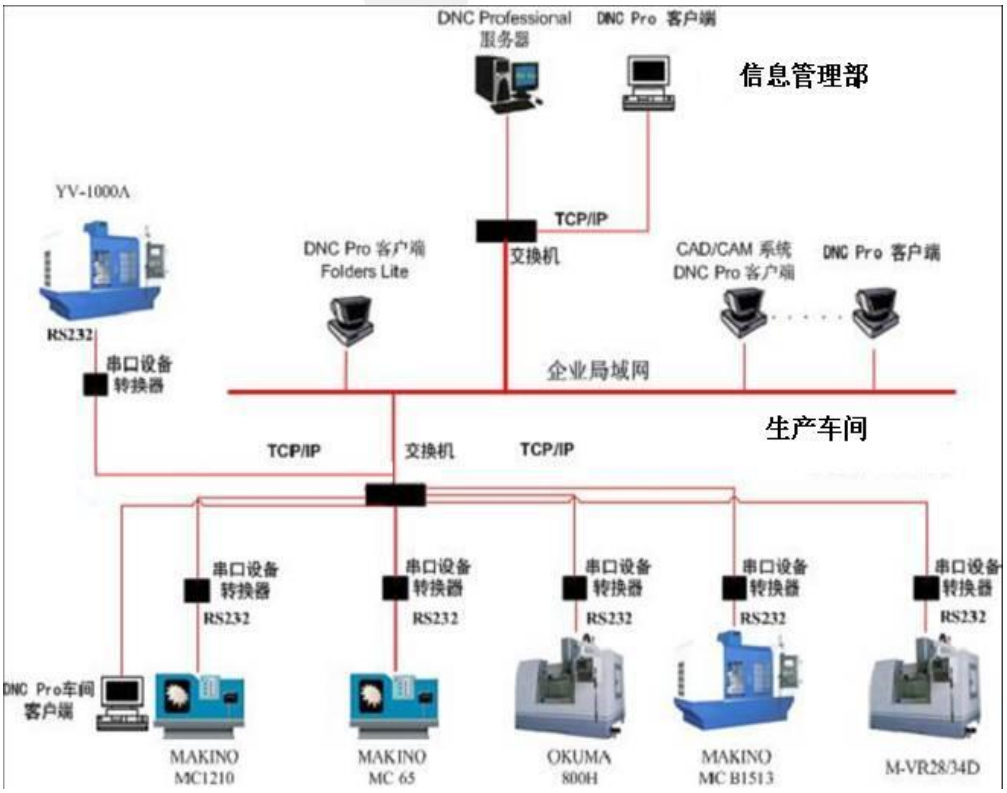

图 4 车间网络连接示意图

为提升机床效率和利用率，逐步建立 DNC 网络，可实现统一的机床管理和实时监测，同时使设计和生产直接连接，DNC 通常国外使用的品牌有 Cimco 和

Predator。国内提供 DNC 网络的主要是数码大方和蓝光，DNC 传输主要是基于 TCP/IP 协议，DNC 的采集是通过 OPC、MODBUS 及厂家自身协议等。数控系统的管理流程如下图所示：

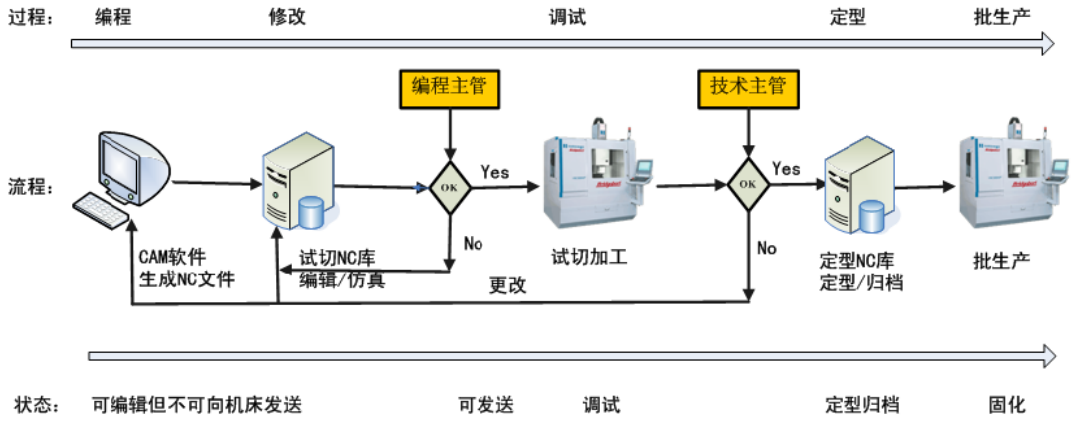

图 5 数控系统管理流程

该类系统安全面临的风险主要有如下：

（1） 大多 CNC 设备采用国外品牌，面临着国外厂商运维时重要数据如生产数量、NC 文件泄露的风险。

（2） 工控网络与管理网中的 DNC 服务器连接时，在提高效率的同时也面临着被感染病毒、恶性攻击的风险。

（3） 诸多工厂通过使用 U 盘将 NC 文件传入高精类数控设备或连入网络传输数据，可能会被传染病毒或恶意代码，进而严重影响生产的产量、质量及效率。

（4） 第三方人员（尤其是远程的国外人员）在远程维护高精类机床设备时可能会有相关生产数据的信息泄密，直接影响着企业声誉、国家命脉。

（5） 未对操作站主机及服务器端进行必要的安全配置，使得一旦能接触访问到该主机则被攻击的成功机会很高。

（6） 无线客户端和接入点的认证措施不足，使得很容易在车间中被人盗取或滥用。

除此之外，也存在管理方面的缺乏相应的信息安全责任人、供应商管理不严格、安全培训意识不足等问题。

2.2.3 安全解决方案

在保证系统可用性前提下，对工业控制系统进行防护，实现“垂直分层，水平分区。边界控制，内部监测”。

“垂直分层、水平分区”即对工业控制系统垂直方向化分为四层：现场设备层、现场控制层、监督控制层、生产管理层。水平分区指各工业控制系统之间应该从网络上隔离开，处于不同的安全区。

“边界控制，内部监测”即对系统边界即各操作站、工业控制系统连接处、无线网络等要进行边界防护和准入控制等。对工业控制系统内部要监测网络流量数据以发现入侵、业务异常、访问关系异常和流量异常等问题。

系统面临的主要安全威胁来自于黑客攻击、恶意代码（病毒蠕虫）、越权访问（非授权接入、移动介质、弱口令、操作系统漏洞、误操作和业务异常等，因此，其安全防护应在以下方面予以重点完善和强化，具体如下：

（1） 在 CAM 终端、工艺终端上安装防病毒软件配合终端安全管理系统，可实现 CAM 终端、工艺终端的 USB、光驱、无线等接口进行严格外设控制；

（2） 对工业控制网络进行安全配置核查审计，对于安全配置较差的设备在保证生产的前提下进行安全配置修改，实现对工控网络设备安全配置进行审计与完善；

（3） 根据数据传递方向在生产管理网与管理网间部署网闸或工业防火墙，在机床前部署 CNC 防护装置，实现了阻断来自管理网的非法行为和对机床的非法行为的访问控制；

（4） 在生产车间部署工控异常监测系统，实时监测针对工控系统入侵行为及异常行为。

（5） 在机床前端部署适用于工业现场的专用防火墙，对工控异常访问行为及违法操作进行安全防护。

（6） 部署工控信息安全统一管理平台，用于对工业控制环境的统一安全管理，在实现网络进行可用性与性能的监控、事件的分析审计预警、风险与态势的度量与评估、流行为的合规分析的同时，还承载着对工控安全设备统一管理的职能，是工业控制网络信息安全管理的统一平台。

本次项目范围涉及该公司生产网、管理网和工控 DNC 网络三大安全区域的

加工终端、设计终端、工艺终端、CAM 终端等工控系统的用户终端，含有 PDM、MES、CAM 等类型的 DNC 系统以及机床装置和机器人装置等智能装置。项目蓝图如下：

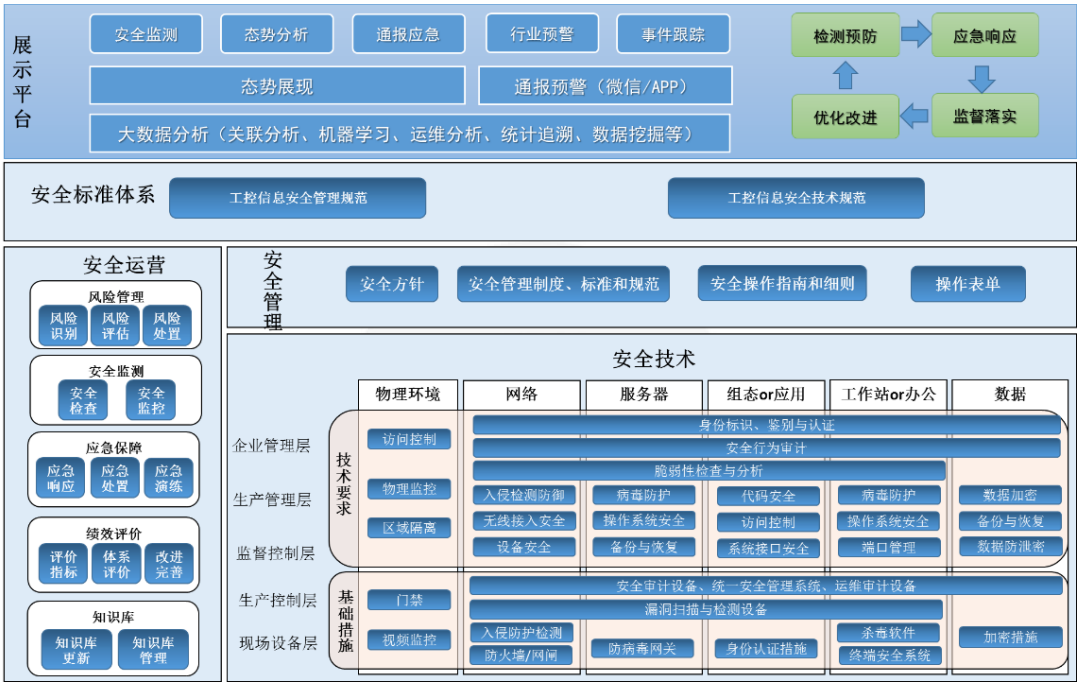

图 6 工控系统安全解决方案蓝图

建设内容包括如下几方面:

（1） 建设一套基于最新协同设计与过程控制的从研发产品设计、工艺编制、后置处理、数控加工代码生成、仿真及代码传输、加工等全生命周期的信息安全保障体系。

（2） 建设一套安全区域清晰、技术安全防护措施到位的、统一管理的工控安全网络，针对现场设备层、生产控制层建设完备的边界防护、恶意代码防护、异常检测、机床设备运维审计、无线安全防护等信息安全防护体系，并形成公司信息安全技术规范。

（3） 在公司现有的信息安全管理和运维体系支撑平台上扩充工业控制信息安全管理功能，规范生产系统运维工作和流程，明确工控系统运营各方的安全职责、工作要求、评价办法、考核标准，通过常态化的检查实现评估，并实现 KPI 考核，改进在生产安全中不断完善发展信息安全，并形成公司工控系统信息安全管理规范。

（4） 在全厂信息安全统一平台上实现生产网、办公网的信息安全统一监控，收集的信息包括各类信息安全设备日志和报警、系统安全日志、行业预警信息等，实现监测预防、应急响应、监督落实、优化改进等闭环的信息安全工作流程。

2.2.4 小结

某先进制造公司通过对其生产网络及工控系统进行安全建设，有效的减少了由于工控网内部病毒木马造成的工业数据丢失、泄密以及停车风险，大大提高了工控系统生产效率。

3. 智慧交通行业典型安全解决方案

智慧交通是在交通运输领域充分利用物联网、云计算、移动互联网等新一代信息技术，通过建设实时的交通信息综合分析与联动平台，实现交通运输资源配置优化，为社会提供更安全、更高效、更便捷、更舒适的交通运输服务。

本案例汇编包括三个智能交通行业的典型安全解决方案。

3.1 案例一：城市轨道交通信息系统安全解决方案

3.1.1 概述

城市轨道交通是城市建设史上最大的公益性基础设施，其运行安全事关人民生命财产安全，因此，需按照国家及行业相关要求做好轨道交通控制系统的安全防护，特别是信号系统的全面防护。

3.1.2 典型安全问题

（1） 目前，多数城市轨道交通系统部署防病毒和防火墙这两类安全设备进行安全防护，防病毒软件的病毒库升级迟缓或不升级，甚至部分轨道交通信号系统未部署任何安全措施；

（2） 缺乏安全隔离保护措施，已有防火墙的策略大部分配置为全通，同时无法识别工业专有协议；

（3） 运维人员缺乏必要的权限管理、监控审计措施；

（4） 信号系统各环节各自为战，缺乏统一的安全管理。

3.1.3 解决方案

（1） 对关键主机和服务器进行安全防护和移动存储介质管理，阻止各类已知或未知恶意软件的感染、运行和扩散，保障信号系统的运行安全和数据安全；

（2） 对信号系统与对外接口的网络边界进行安全隔离防护，阻止任何来自信号系统外的非授权访问，有效抑制病毒、木马在信号系统网络中的传播和扩散，

保障列车运行安全；

（3） 采取监测审计措施，实时发现并记录针对信号系统的攻击和破坏行为，为工业控制网络安全事件调查提供依据；

（4） 结合信号系统业务特点，对各级维护人员的操作行为进行管控，保证每个维护人员的身份及操作指令的合法性；

（5） 对信号系统网络中的安全设备和主机进行集中安全管理，同时对各类安全日志进行汇总分析。

3.1.4 典型部署

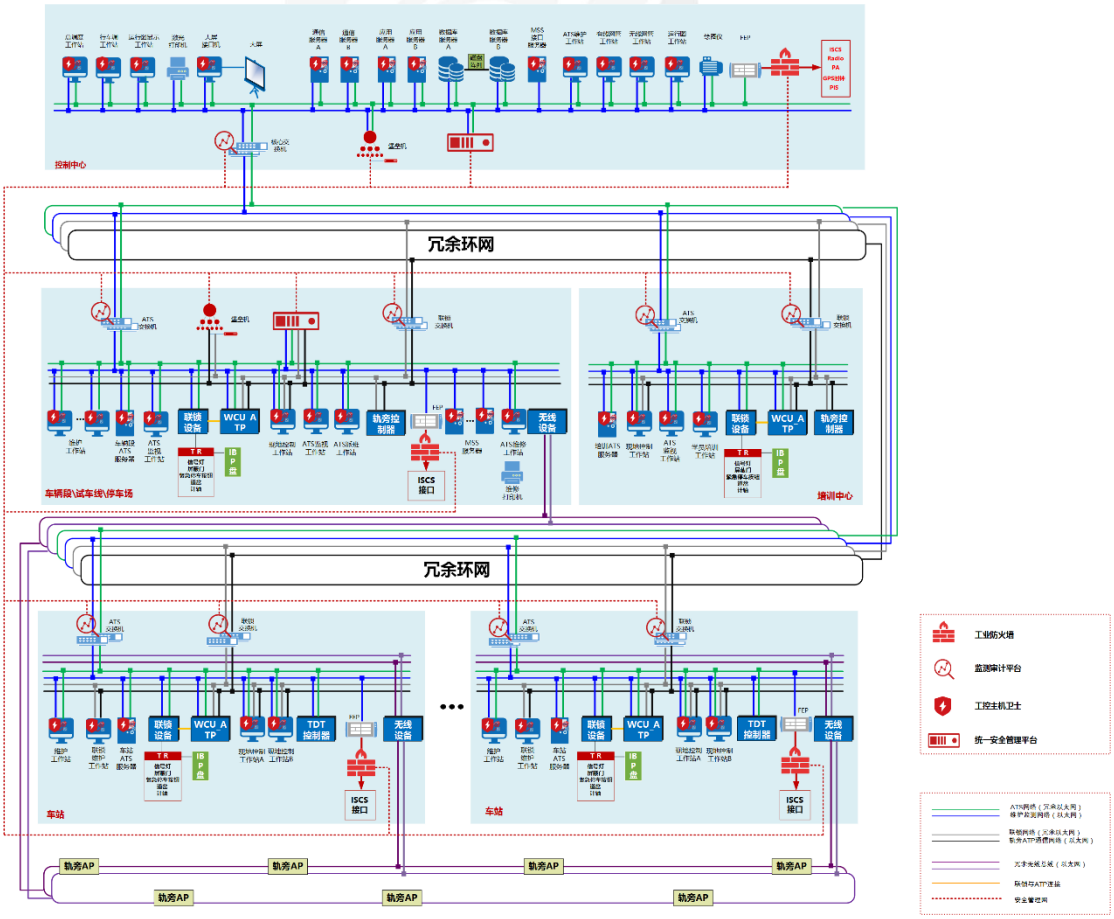

图 7 工控网络安全部署拓扑架构

（1） 在关键主机和服务器上部署工控主机卫士和安全 U 盘，采用“白名单”技术阻止未授权程序运行，保障信号系统的运行安全和数据安全，同时利用安全 U 盘保证主机间数据交换安全；

（2） 在信号系统与对外接口之间部署工业防火墙，运用“白名单+智能学

习”技术建立工控网络安全通信模型，阻断一切非法访问，仅允许可信的流量进出信号系统；

（3） 在各级交换系统内旁路部署监测审计平台，对各级交换系统间的通信流量进行深度分析，利用流量中的元素（时间、IP、协议、指令）来判断各级操作的合法性；

（4） 在控制中心和车辆段网络旁路部署工控堡垒机，通过严格的权限控制和操作行为审计，加强对信号系统维护人员的行为管理，从而达到消隐患、避风险的目的；

在控制中心、车辆段部署统一管理平台，对工控主机卫士、监测审计平台、工业防火墙进行集中管理，并根据实际需求输出不同类型、不同维度的分析报告。

3.1.5 小结

本解决方案具备如下特点：

（1） 满足国家等级保护政策需求、满足工信部工业控制系统安全防护指南中的技术需求；

（2） 通过部署不同维度的安全产品，形成一个以安全管理平台为中心的纵深防御的安全体系，真正做到“进不来-拿不走-打不开-改不了—赖不掉”。

3.2 案例二：某市地铁综合监控系统安全解决方案

地铁综合监控系统(Integrated Supervisory and Control System)简称 ISCS，是根据轨道交通线路特点和技术发展情况量身定制的大型综合自动化系统，通过综合监控系统可实现城市轨道交通信息互通、资源共享，并能够提升自动化水平和提高城市轨道交通运营的安全性、可靠性和响应性，最终达到减员增效的目的。

3.2.1 案例概述

某市地铁 X 号线综合监控系统主要由中央级综合监控系统、车站级综合监控系统、车辆段综合监控系统和其他辅助功能子系统（例如培训管理系统、集中告警系统、软件测试平台和网管系统等）等多个部分组成。通过综合监控骨干传

输网将以上各部分联接起来，形成一个有机整体。由于综合监控系统是地铁线路运营的核心系统，其信息安全状况直接影响整个线路的运营安全，因此，某市在既有线路安全运营的经验基础上，在地铁 X 号线在建设之初就将综合监控系统的信息安全防护进行了优先考虑。

3.2.2 典型安全需求

综合监控系统的安全防护措施主要针对中央网络。能够对业务访问关系进行检测、能够对上报的事件进行关联分析，识别出重要报警，同时，对不重要的报警进行智能过滤，此外，分析报表采用对比分析的方法。监控各个网络设备、操作系统等日志信息，以及安全产品的安全事件报警信息等，以便及时发现正在和已经发生的安全事件，例如网络蠕虫攻击事件、非授权漏洞扫描事件、远程口令暴力破解监测事件等，及时协调和组织各级安全管理机构进行处理，及时采取积极主动措施，保证网络和业务系统的安全、可靠运行。

监测综合监控系统中央网络，着重检测中央网络的 PSCADA 和 BAS 业务，能够基于业务主要协议发现 PSCADA 和 BAS 的业务异常。同时，能够检测到其他系统的网络异常。

可以掌握综合监控系统各个系统中存在的安全漏洞情况，结合当前安全的安全动态和预警信息，有助于各级安全管理机构及时调整安全策略，开展有针对性的安全工作。

实时监控各种安全设备、控制设备和网络设备的运行状态和网络运行拓扑状态，为网络安全管理人员提供统一的运行状态信息，并根据确定的规则，提供预警和告警，保证网络和业务系统的安全、可靠运行。

通过所掌握的全网安全运行动态，有针对性指导各级安全管理机构做好安全防范工作，特别是针对当前发生频率较高的攻击做好预警和防范工作。

根据安全事件生成的事件通知单的处理过程进行管理，将所有事件响应过程信息存入后台数据库，并可生成事件处理和分析报告。

3.2.3 安全解决方案

安全防护方案以某市地铁 X 号线一期工程综合监控系统结构示意图进行说

明：

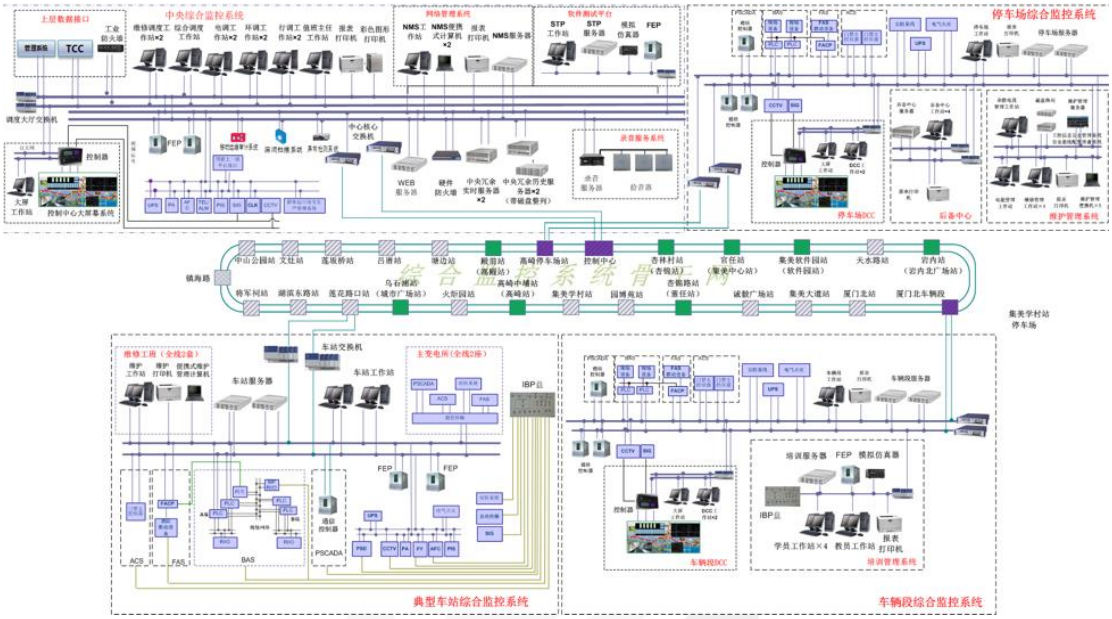

图 8 综合安全监控系统架构图

工控信息安全产品分别部署在中心综合监控系统与停车场综合监控系统，其中：

工业防火墙、工控异常检测系统、工控漏洞扫描系统、移动运维审计系统部署在中央综合监控系统；

工控信息安全管理系统与安全基线配置核查部署在停车场综合监控系统。

需要说明的是：停车场综合监控系统维护管理服务器具备 windows 环境，工控信息安全管理平台与安全基线配置核查系统都可以安装在这台服务器上，只要网络可达，即可以从中央综合监管系统任何工作站通过 web 访问的方式访问该系统，从而实现工控信息安全管理与安全基线配置核查工作。

（1） 工控信息安全管理系统

工控信息安全管理系统与安全基线配置核查系统为软件，都安装在停车场综合监控维护管理服务器上。

工控信息安全管理系统可对某市地铁综合监控网络中的网络设备、主机及服务器等资产管理、风险管理、事件管理、网管等功能。

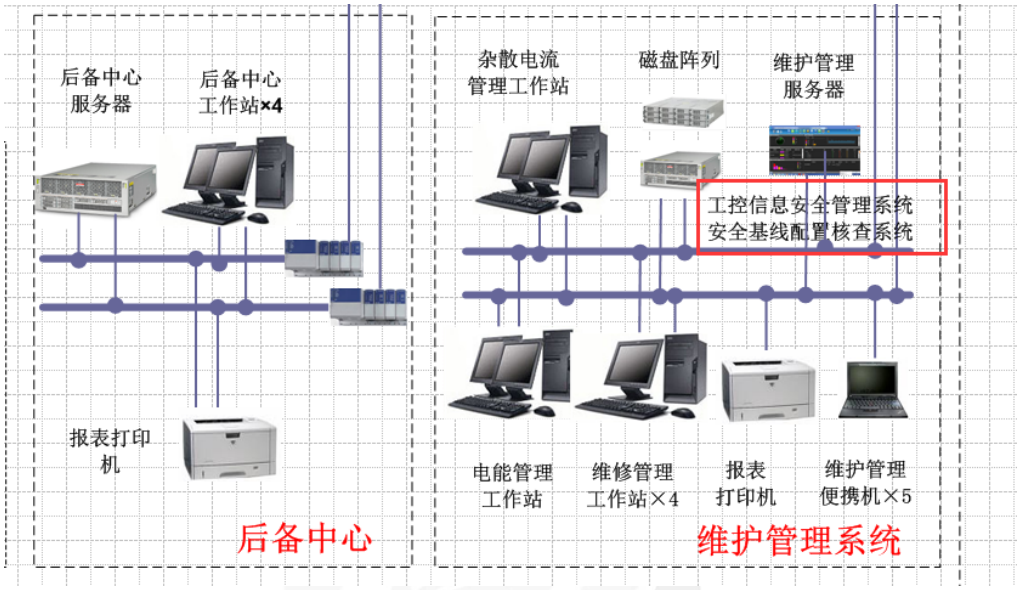

图 9 工控信息安全管理系统部署图

（2） 工控异常检测系统

工控异常检测系统为硬件设备，部署在中央综合监控系统的核心交换机上，通过在交换机上做端口镜像配置，将中央级综合监控的网络流量镜像给工控异常检测设备进行分析，检测中央网络的 PSCADA 和 BAS 业务异常和入侵行为。

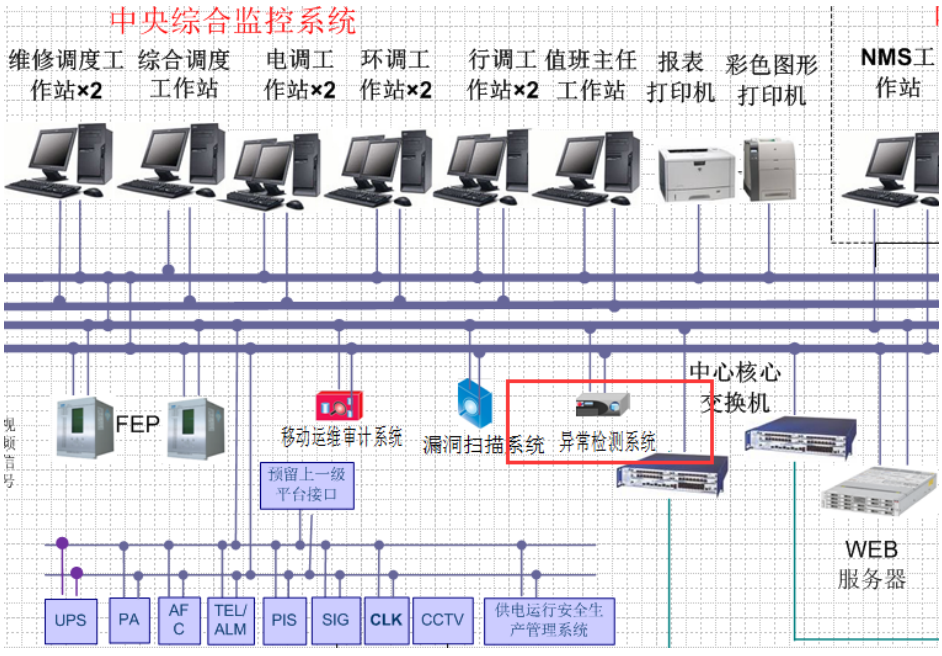

图 10 工控异常检测系统部署图

（3） 工业防火墙

工业防火墙为硬件设备，部署在中央综合监控系统管理服务、TCC 等上层数据接口区域网络边界处，串接在管理服务、TCC 等上层数据接口与中央综合监控系统核心交换机之间进行访问控制，对工控协议包括 OPC 和 MODBUS 深度协议解析。

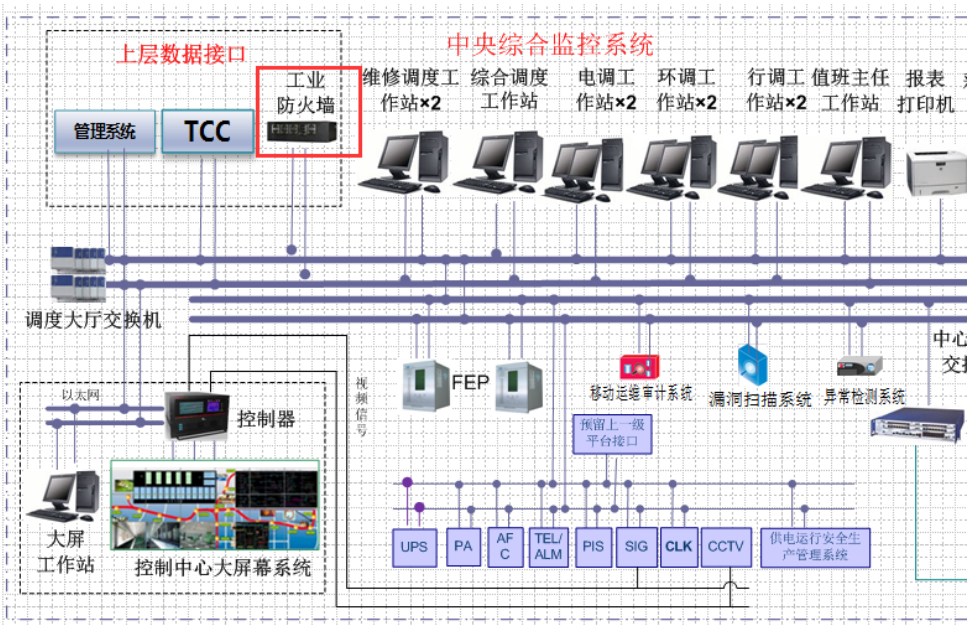

图 11 工控防火墙部署图

（4） 工控运维审计系统

工控运维审计为移动设备，当某市地铁 X 号线综合监控系统中的 PLC 工控设备或工作站、服务器、网络设备需要进行维护操作时，将设备携带至现场使用，维护完毕后带回中心进行数据同步。

工控运维审计系统，能够全程记录现场运维人员对设备的操作行为，用于事前警示与事后定责。可以避免运维设备自身感染的恶意代码扩散到脆弱的工业控制系统。可以对上传下载数据进行管理，避免上传数据感染病毒，存储备份下载的配置数据。移动运维审计与管理系统可以在运维的过程中，将设备配置数据进行存储备份。

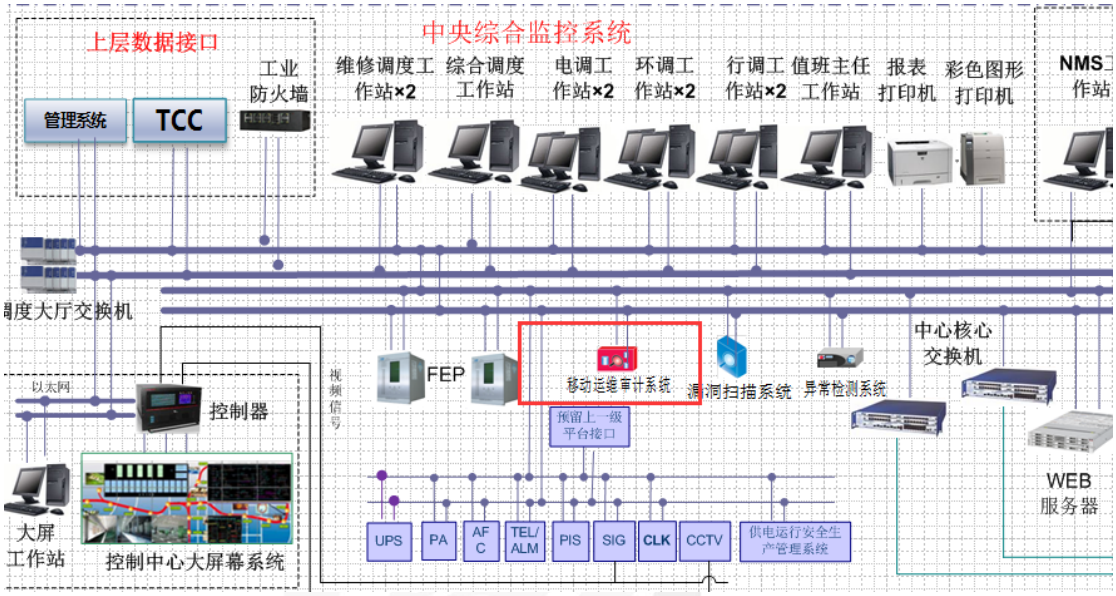

图 12 工控运维审计系统部署图

（5） 漏洞扫描系统

漏洞扫描系统为硬件设备，部署在中央综合监控系统与核心交换机相连，对综合监控系统中的工控设备、工作站、服务器、网络设备等进行脆弱性扫描和管理。

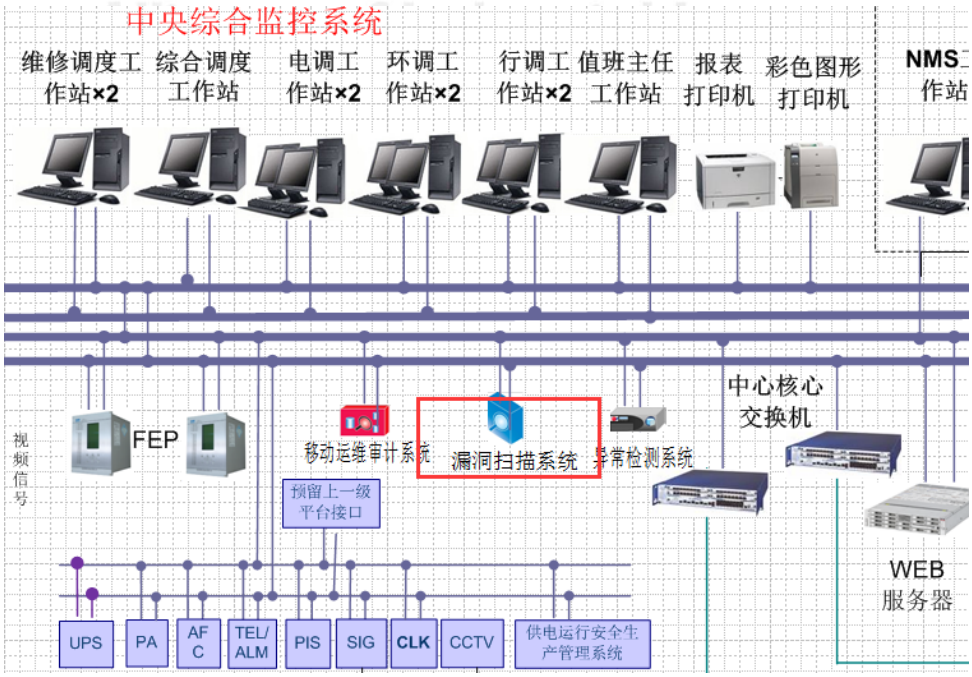

图 13 工控漏洞扫描系统部署图

（6） 安全基线配置核查系统

安全基线配置核查系统为软件，安装在停车场综合监控维护管理服务器上。安全基线配置核查系统具有通过远程方式或本地方式对 IT 资产进行安全配置核查的能力，能够核查信息系统中的主机操作系统、数据库、网络设备、安全设备等，确保各类 IT 自查符合预设的配置规范要求。系统具有友好的人机界面和丰富的报表系统，实现了配置安全检查工作的智能化、自动化。

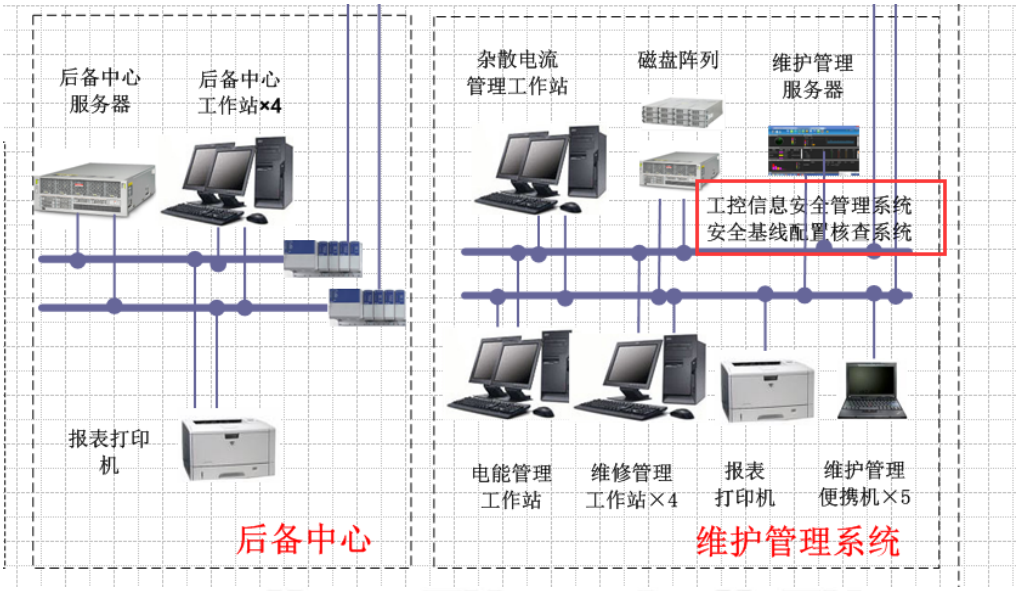

图 14 工控安全基线配置核查系统部署图

3.2.4 小结

从该项目的实施可以看出，地铁综合监控系统仍然以保障安全运营为首要目的，所以在安全建设方面是仍以业务影响最小化需求，目前在边界防护、入侵监测和安全审计方面是保障安全的第一步，以满足等级保护技术要求为基础。该项目的实施经验可以为其他地铁综合监控系统的安全防护作为参考。

3.3 案例三：公车管家系统安全解决方案

公车管家系统是基于运营商的车联网“云-管-端”架构设计的车辆管理系统，基于运营商 TSP 平台为政府和企事业单位提供车辆监控等车联网服务，实现清晰、高效与安全用车。公车管理平台实时掌握车辆动态，通过对数据进行采集、

分析、提取、分享和决策，对车辆和驾驶人提供综合服务，解决公车私用滥用、管理考核、费用管理、车辆调度、行车安全等问题。通过实现车辆管理集中化、跟踪监控全程化、在线派车电子化、统计分析多维度的目标，帮助用车单位提升管理水平、实现精细化管理。

3.3.1 案例概述

公车管家系统由多形态车载智能终端（OBD模块、智能后视镜、车机）、运营商通信网络（TD-LTE无线网）和TSP平台（公车管家业务管理系统）等多个部分组成。车载智能终端收集车辆信息（GPS信息、速度信息、车辆状态信息、故障检测、油耗分析、行驶情况、故障预警以及驾驶行为信息等），通过无线网络传送至TSP平台，平台分析处理后实时掌握车辆状态，同时可以对车载智能终端进行远程管控。由于车辆信息和管控指令均通过公共网络传输，因此对于系统网络数据传输的安全性需要进行重点考虑。

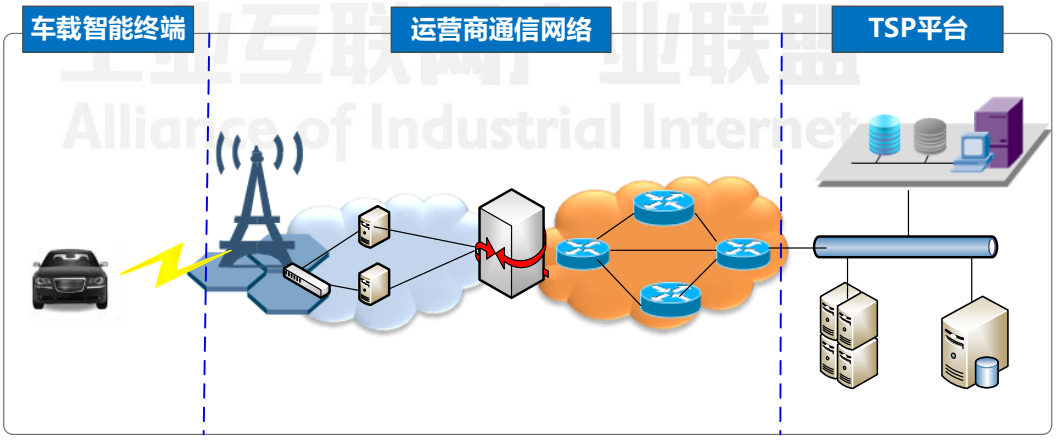

图 15 公车管家系统网络结构图

3.3.2 典型安全需求

基于公车管家系统的系统结构和业务特点，其存在的主要安全需求如下：

- 攻击者可以通过网络进行嗅探与监听，获取通过明文传输的用户数据或业务数据等敏感信息，进而通过贩卖敏感信息等方式损害系统正常运行

或侵害用户权益。因此保证网络数据传输的机密性是系统最主要的安全需求。

- 攻击者可以利用系统在网络中传输的数据缺乏完整性保护的漏洞，对截取的网络数据进行篡改后继续发送，导致系统处理错误数据，形成错误分析结果，影响系统业务的正常服务。还可能篡改对平台对终端发送的管控命令，影响终端设备正常运行。因此系统需要能对对网络数据传输的完整性和伪造信息的鉴别进行有效保障。
- 攻击者可以利用系统身份鉴别机制不完善的漏洞，伪造或冒用他人身份接入系统，窃取系统信息、篡改系统数据，破坏系统资源，影响系统的正常运行。同时合法用户也可以借此通过否认已执行的行为或行为发生的时间，进行违规或非授权操作并避免责任追究。因此完善的身份鉴别机制是系统安全运行的必要保障。

3.3.3 安全解决方案

公车管家密码安全系统由 TSP 平台、移动通信网络、密钥管理系统、车载智能安全终端、业务加密网关和远程管理终端 6 部分组成，系统网络结构如下图所示。

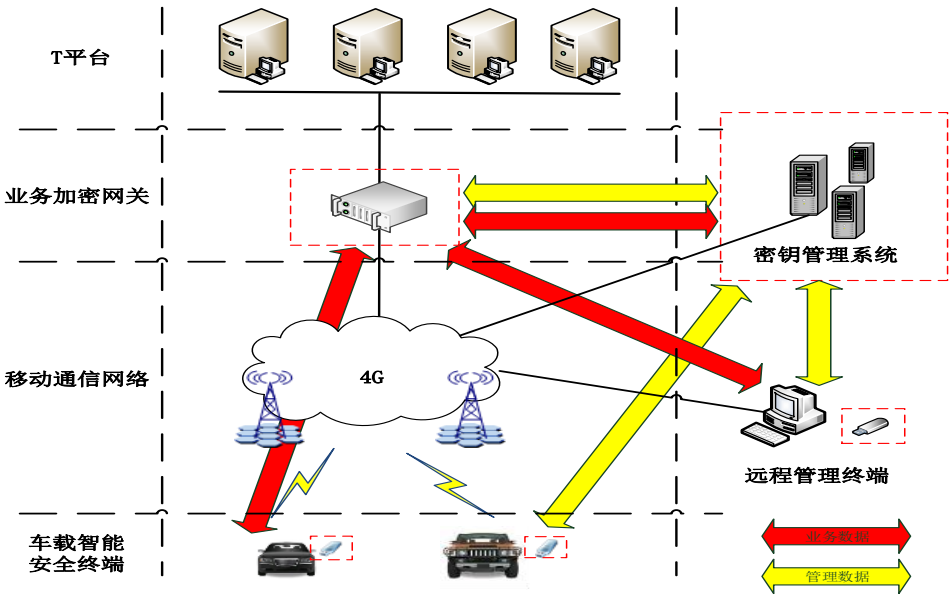

图 16 公车管家密码安全系统网络结构图

TSP 平台和移动通信网络为运营商公车管家系统现有设施，其中 TSP 平台上部署若干应用服务器，为公车管家系统提供包括车辆位置信息、行驶轨迹监测等应用服务，移动通信网络为 TD-LTE 移动通信网，负责承载系统各类应用数据和管理数据的传输。

密钥管理系统负责系统内所有密码设备密码资源的全生命周期管理，同时对其实施在线安全管控。车载智能安全终端通过无线通信模块接入无线网络与业务加密网关建立安全隧道，保护系统业务数据安全传输。远程管理终端为用户普通 PC，通过安装客户端软件和专用可插拔安全硬件与业务加密网关建立 SSL VPN 隧道，满足用户安全的查询、管理系统信息的使用需求。

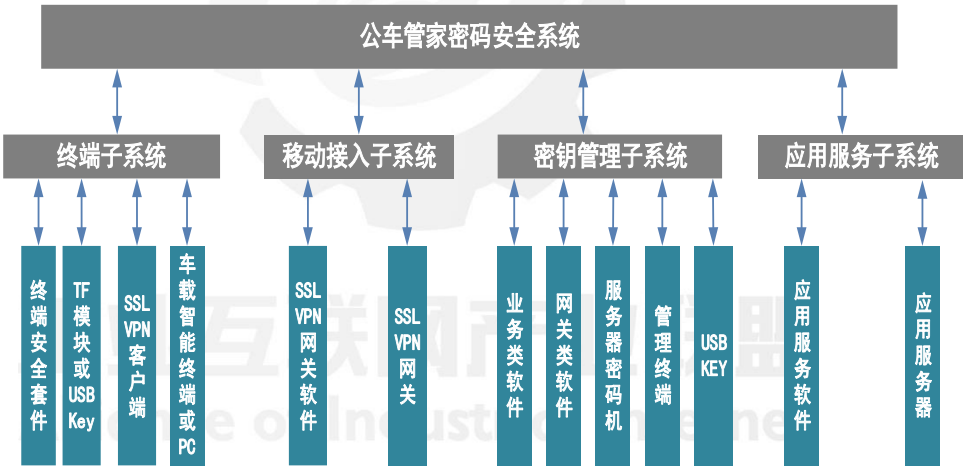

图 17 公车管家密码安全系统组成图

系统通过基于独立硬件实现的符合国家商密标准的安全隧道实现对系统业务数据在线传输的安全保护，保证其机密性、完整性和有效性，解决了信息窃取、信息篡改和非法远程控制等问题。通过基于证书、非对称算法和私有协议的身份认证机制实现了系统对终端设备的有效接入控制，避免了身份冒用、身份伪造等安全问题。

通过以上安全措施的实施，可以保证车辆信息能够安全上传 TSP 平台，用户可以在自有 PC 安全的通过 TSP 平台查询系统信息，同时保证非法终端无法接入系统，间接对 TSP 平台的安全防护能力有一定提升。

3.3.4 方案特点

- 独立硬件加密，安全稳定

系统内密码设备的基础密码服务全部由独立专用硬件实现，包括物理噪声源生成真随机数、密码芯片进行算法计算、专用存储单元存储密码资源等。

- 国家商密认证，自主可靠

系统使用的密钥格式、密码算法和密码协议符合国家商密标准，安全设备取得国家密码管理局认证的商用密码产品型号。

- 在线设备管控，实施快捷

密管系统负责系统密码设备密码资源的产生、存储、注入、销毁等全生命周期管理，还支持对终端设备进行实时在线安全管控。

- 协议策略配置，灵活透明

安全方案密码协议基于网络层实现，对用户业务系统透明，满足用户多样化使用需求。

3.3.5 小结

该项目的实施解决了公车管家系统网络数据传输的安全性需求，整套安全体系对业务系统透明，不影响业务系统的正常运行。该项目的技术方案在设计阶段以通用化、标准化为原则，普遍适用于工业互联网、物联网等领域的业务系统，能够有效提升系统网络数据传输安全性。

3.4 案例四：轨道交通信息系统安全解决方案

轨道交通是城市重要的公共交通工具，信息系统安全关系到乘客人身安全和地铁设备安全；因此，需要按照国家政策、标准要求，实施完善的、整体的安全防护措施。

3.4.1 概述

轨道交通信息系统主要由综合监控系统（ISCS）和信号系统（CBTC）组成。ISCS 主要由中央级系统、车站级系统、网络管理系统、仿真培训系统、设备维护管理系统等构成，自动售检票系统（AFC）是综合监控系统的重要组成部分。CBTC 系统通过无线通信媒体来实现列车和地面设备的双向通信，用以代替轨道电路作为媒体来实现列车运行控制。

3.4.2 典型安全需求

（1）目前，轨道交通行业的信息安全主要侧重于 IT 网络安全防护，轨道交通的业务系统（ISCS、CBTC）缺乏防护措施，还未能形成有效防护体系。

（2）信息系统的安全防护还处在分散防护阶段，缺少整体安全运营平台。

（3）基于业务特点，主机操作系统和杀毒软件不能及时升级，操作系统漏洞、病毒、木马对综合监控系统和信号系统的主机造成威胁，基于黑名单的杀毒软件不能有效应对。

（4）虽然综合监控系统和信号系统为封闭网络，但黑客仍可以借助应用软件漏洞，通过 U 盘摆渡等方式进行信息安全攻击。

（5）目前的 CBTC 系统在车载和地面间通信部分主要采用 WIFI 通信，应用层采用专有算法进行加密，但由于各厂家加密实现代码可能存在缺陷，车地通信仍存在一定的安全风险。

（6）需要对运维人员的身份进行认证管理，缺少对操作行为进行审计。

3.4.3 解决方案

（1）主机安全加固：在 ISCS 系统主机、服务器、AFC 系统的中央计算机系统 LCC、各车站计算机系统 SC、各车站终端设备 SLE 的主机进行安全加固。

（2）网络边界隔离：在 ISCS、CBTC 与其它系统边界处进行网络隔离。

（3）移动介质防护：针对 ISCS 系统、AFC 系统、CBTC 中使用专用的移动存储设备，进行安全防护，消除此处隐患。

（4）网络安全审计：对 ISCS 系统、AFC 系统和 CBTC 系统网络进行协议

审计、流量审计，掌握网络安全信息。

（5）无线入侵防御：采用无线入侵防御系统，监控非法无线热点和可能的非法无线入侵。防止车地 WIFI 通信被恶意入侵。

（6）安全运营：建设工业安全运营中心，遵循发现、阻断、取证、溯源、研判、拓展的安全业务闭环，完成威胁处置。

（7）定期检查：定期对封闭网络的安全运营状况进行检查。

3.4.4 典型部署

1．综合监控系统信息安全部署方案：

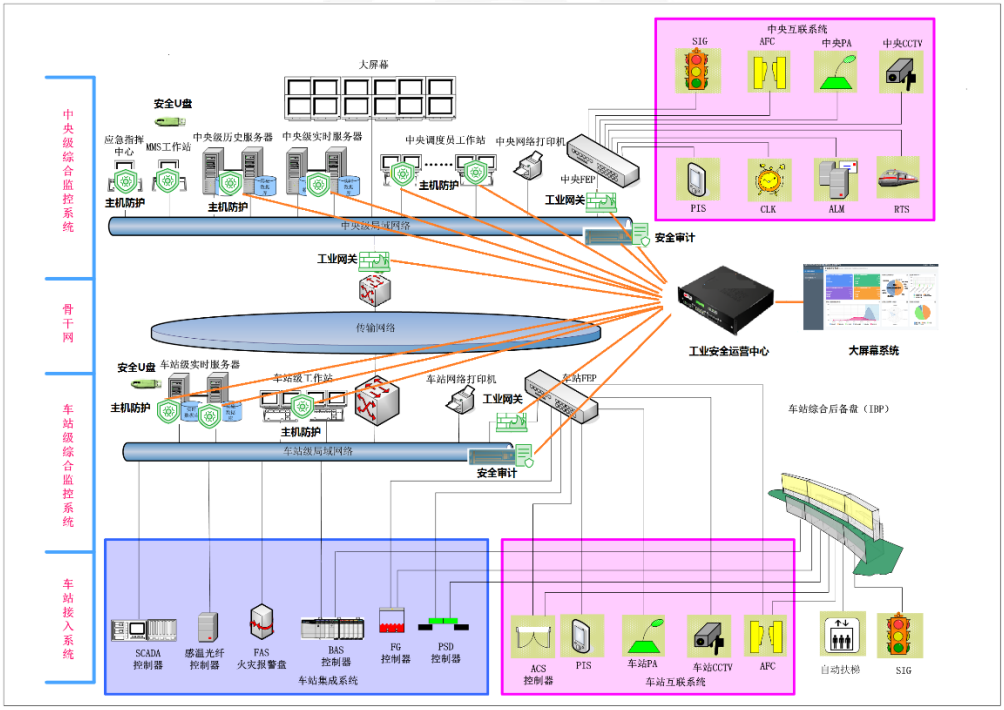

图 18　ISCS 安全方案部署示意图

（1）主机安全加固：在综合监控系统、AFC 系统的主机、服务器上进行安全加固，部署白名单工业主机安全防护软件。

（2）纵向分层隔离：中央综合监控系统与车站级综合监控系统的边界处进行网络隔离，部署工业安全网关。

（3） 横向分区隔离：在综合监控系统与其它系统边界处进行网络隔离，部署工业安全网关。

（4）移动介质防护：针对综合监控系统、AFC 中使用专用安全 U 盘，专网

专用，避免病毒通过 U 盘引入。

（5）网络安全审计：在综合监控网络核心交换机处，部署基于镜像流量机制的工业安全审计设备，进行协议审计、流量审计，掌握监控网安全信息。

（6）无线入侵防御：部署无线入侵防御系统，监控非法无线热点和可能的非法无线入侵，防止车地 WIFI 通信被恶意入侵。

（7）安全运营：部署工业安全运营中心，对综合监控系统网络流量进行分析，收集各安全设备的日志，结合定期导入的专业威胁情报大数据，进行威胁分析和整体安全运营。

（8）定期检查：配备临检工具箱，定期对封闭网络的安全运营状况进行检查。

2．信号系统信息安全部署方案：

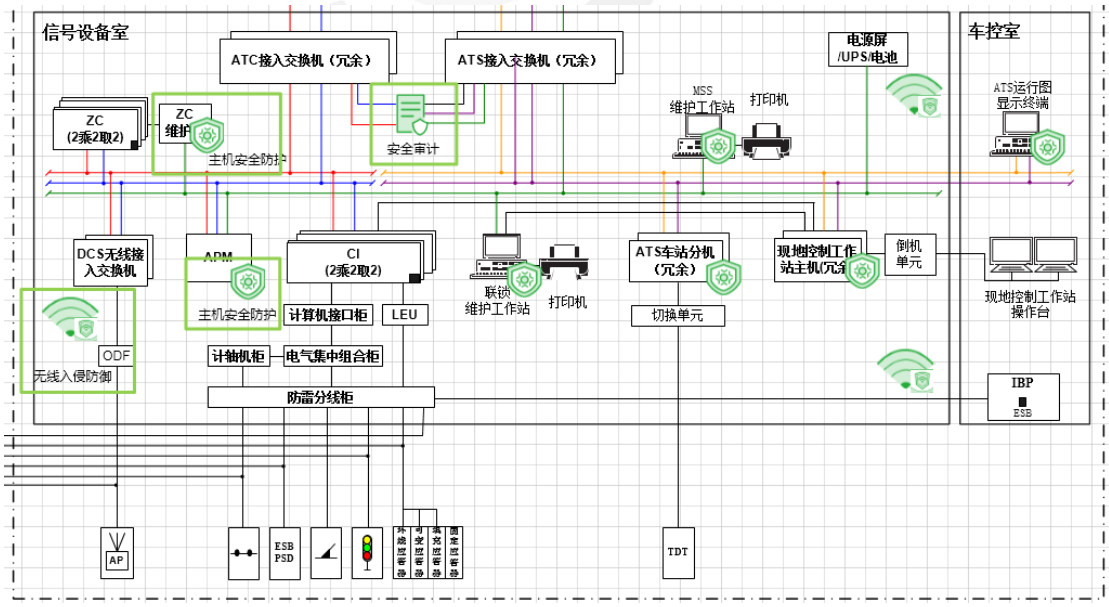

图 19　CBTC 安全方案部署示意图

（1）主机安全加固：在 CBTC 主机、服务器的主机上进行安全加固，部署白名单工业主机安全防护软件。

（2）移动介质防护：针对 CBTC 中使用专用安全 U 盘，专网专用，避免病毒通过 U 盘引入。

（3）网络安全隔离：在 CBTC 与其它系统边界处进行网络隔离，部署工业安全网关。

（4）网络安全审计：在 CBTC 网络核心交换机处，部署基于镜像流量机制

的工业安全审计设备，进行协议审计、流量审计，掌握监控网安全信息。

（5）无线入侵防御：部署无线入侵防御系统，监控非法无线热点和可能的非法无线入侵，防止车地 WIFI 通信被恶意入侵。

（6）安全运营：部署工业安全运营中心，对信号系统网络流量进行分析，收集各安全设备的日志，结合定期导入的专业威胁情报大数据，进行威胁分析和整体安全运营。

（7）定期检查：配备临检工具箱，定期对封闭网络的安全运营状况进行检查。

3.4.5 小结

轨道交通信息系统安全以网络安全法、等级保护制度为依据，以保障安全运营为目标，通过对主机、控制器、网络及网络设备进行安全配置，结合部署安全防护设备，形成涵盖综合监控系统和信号系统的完整防护体系，从信息安全角度，确保轨道交通安全运营。

4. 能源石化行业典型安全解决方案

智慧能源是基于互联网技术体系，综合利用物联网、云计算、大数据等信息通信技术对各种能源的生产、存储、输送、使用进行监测、控制、运营等，将能效技术与智能技术相结合，实现能源的高效使用，更好地解决能源节约和应对气候变化等问题。

本案例汇编包括四个能源石化行业的典型安全解决方案。

4.1 案例一：某环保局典型安全解决方案

4.1.1 案例概述

随着我国经济的发展，对能源的消耗不断增加，导致环境污染问题愈加突出。为配合国家关于节能减排、能源的监控与管理要求，某北部省的一个省会城市开展了节能减排监控管理平台的建设工作，该平台是把所有电力、钢铁、烟草等制造企业端的能源数据通过基于无线传感器物联网的监测数据采集上来，实现制造企业的能耗、减排的指标进行监控和管理。

为满足企业端与市级平台安全对接，保证企业网与市节能减排监控管理平台网络安全隔离的基础上，上传监控数据。涉及 250 多家的该市的制造企业端将通过在边界安全区部署工业安全隔离网闸来完成这一目标。

4.1.2 典型安全需求

由于本项目接入的制造企业诸多，一方面不要因与各企业连接而传入病毒、恶意代码等，另一方面需要准确的接收来自各企业的数据。具体需求包括：

（1） 支持电力、钢铁、烟草等制造企业端各类工控组件产生的工业监测数据（如 Modbus 等协议）通过安全隔离网闸上传至市节能减排监控管理平台中；

（2） 工业安全隔离网闸须能够满足应用层单向隔离的情况下，实现工业监测数据的上传；

（3） 工业专用的无线传感器设备能够直接通过安全隔离网闸进行单向数

据传输；

（4） 支持应用层数据单向传输，能够自定义 TCP 应答报文限制。（粒度 1 个字节）

（5） 支持 TCP、UDP 自定义访问通道，支持源地址、目的地址、目的端口的访问控制，支持生效时段控制策略、提供访问任务的单独启停控制。UDP 协议支持组播。

（6） 支持内、外网主机系统分别采用冗余双系统启动模式:当 A 系统运行失败后，能从 B 系统启动，且 A、B 系统可互为备份。

（7） 支持 IPV6、IPV4 双栈接入，内外网主机之间采用私有通讯协议。

4.1.3 安全解决方案

该项目中传感器采用了 LoRa 采集终端和网关，传感器系统通过 UART 口与终端连接，传感器系统将电机计量数据透明传输给终端，终端将自动上传电机数据到网关。传输数据时采用了 MODBUS 协议。

针对上述需求，通过大量的测试对比，最终选择了工控安全隔离与信息交换系统，部署在各企业接收器端，详细网络拓扑图如下所示：

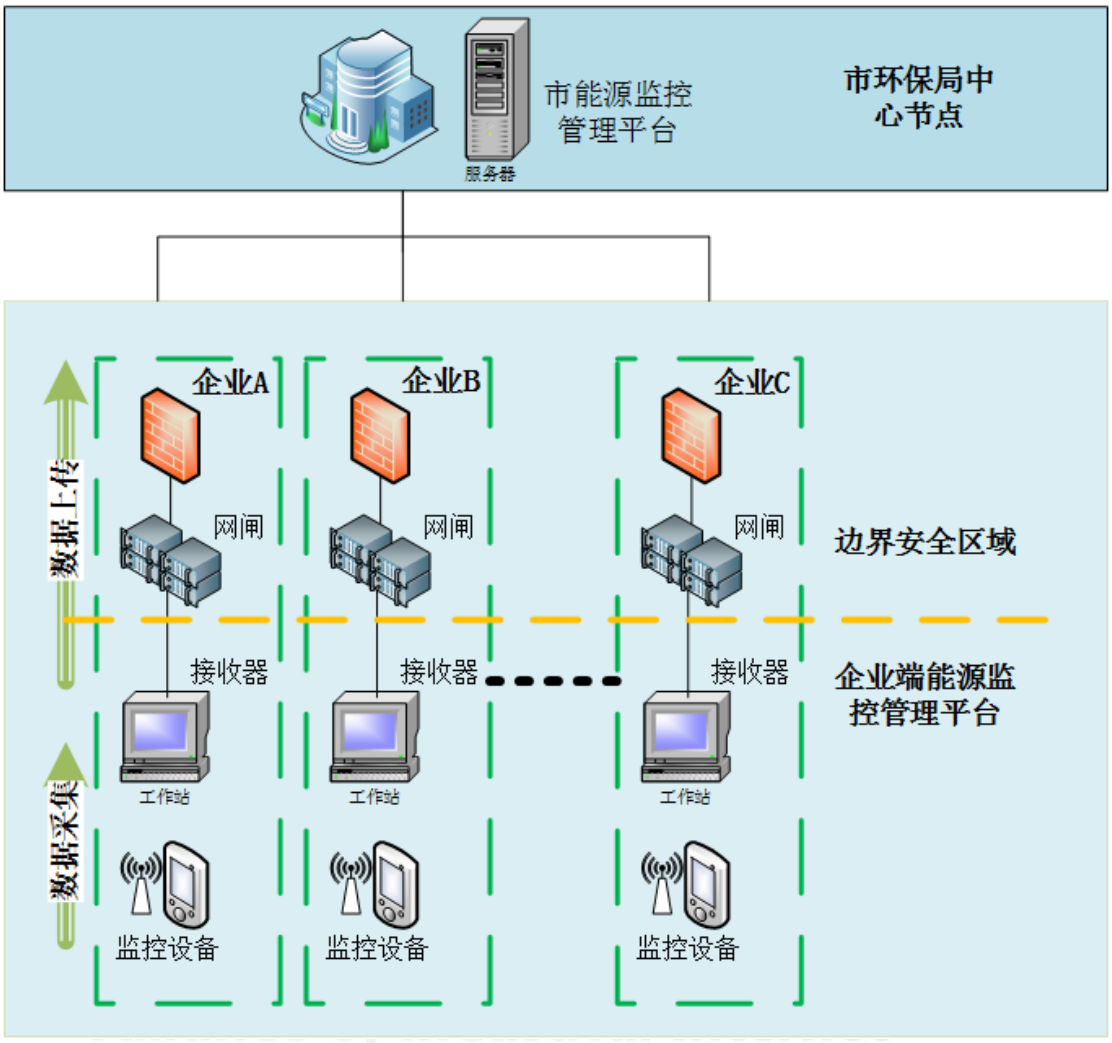

图 20 工控安全隔离与信息交换系统部署拓扑图

最终满足了需求里的全部内容，实现了各制造企业端各类工控组件产生的工业监测数据（如 Modbus 等协议）通过安全隔离网闸上传至市节能减排监控管理平台中；实现了如下效果：

（1） 应用层数据单向传输，能够自定义 TCP 应答报文限制。（粒度 1 个字节）。

图 21 网闸配置界面 1

（2） TCP、UDP 访问通道，支持源地址、目的地址、目的端口的访问控制，支持生效时段控制策略、提供访问任务的单独启停控制。

图 22 网闸配置界面 2

（3） 同时为防止系统故障，设置了内、外网主机系统分别采用冗余双系统启动模式:当 A 系统运行失败后，能从 B 系统启动，且 A、B 系统可互为备份。

图 23 网闸配置界面 3

（4） 为保障自身隔离设备的安全，还提供了 IPV6、IPV4 双栈接入，内外网主机之间采用私有通讯协议。

图 24 网闸配置界面 4

4.1.4 小结

从该项目中看出，环保的实时监测的业务需求仍是环保单位的重中之重，所以在安全建设方面是仍以最小化需求，目前隔离是保障安全的第一步。而隔离时是选择工业防火墙还是工业网闸，是根据企业数据传输的频率、方向及反馈的实时性几个方面要求来决策。该项目也可供诸多其它行业 SCADA 监测系统的安全防护作为参考。

4.2 案例二：某燃气企业安全解决方案

4.2.1 概述

城市燃气随着业务的飞速发展，及人力成本的上升，管网的不断变长以及复杂化，原有的燃气工控系统的“监而不控”方式已经无法适应，迫切需要对其控制系统进行安全防护。

4.2.2 典型安全问题

（1） 调度中心、站场、阀室未采取横向逻辑隔离措施；

（2） 工控网络的各门站、储配站、输配站内部之间未采取安全隔离和防病毒措施；

（3） 现场工程师站，操作员站，服务器等工控主机缺乏安全加固措施。

4.2.3 解决方案

（1） 对调度中心、有人值守站控系统、无人值守站控系统边界进行访问控制、病毒防护，保护系统数据不被非法访问、窃取或篡改，保障工控网络安全运行；

（2） 在工作站和服务器上部署终端防护软件，阻止非法程序和未经授权软件运行，保障主机全生命周期的安全；

（3） 对工控网络中传输的数据进行实时监测，记录，审计，及时发现网络违规操作和异常行为，实现事前部署，事中监控，事后追溯；

（4） 对工业网络中的安全设备进行统一的配置和管理，并对其日志信息进行统一收集、管理和分析。

4.2.4 部署方案

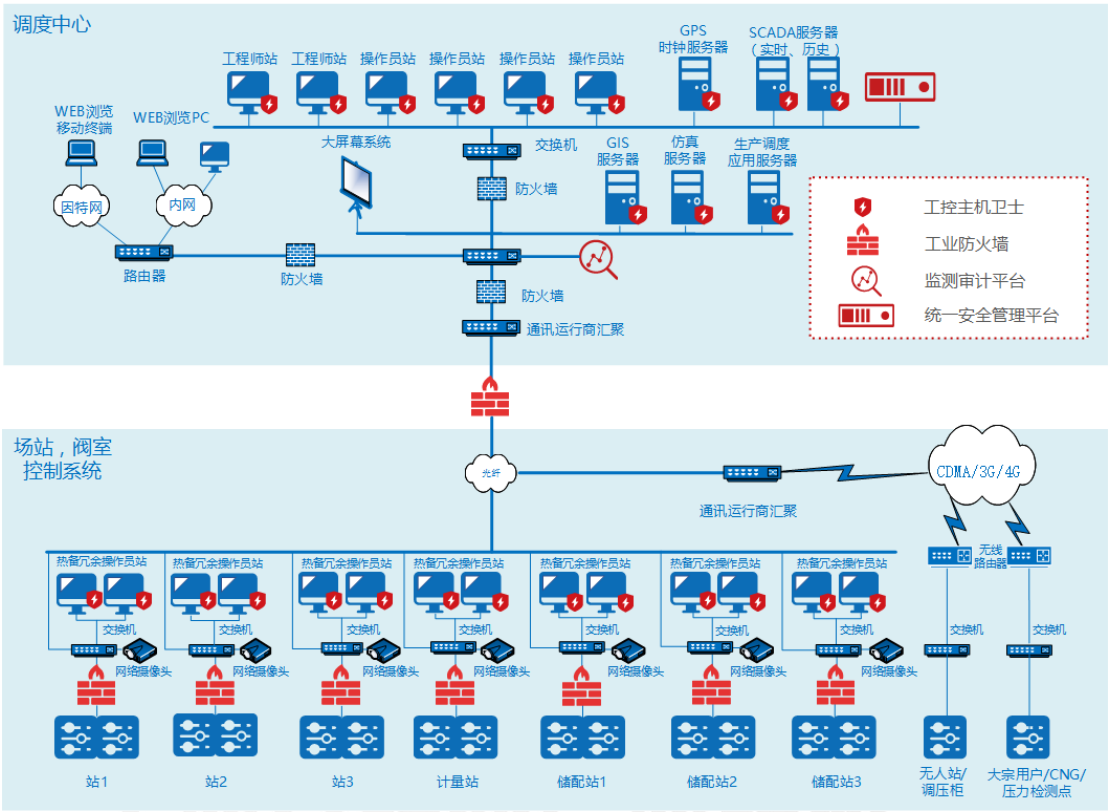

图 25 燃气企业工控安全方案拓扑图

（1） 边界、区域安全防护

a) 在调度中心各区域边界部署工业防火墙，对各区域进行逻辑隔离，并根据业务需要进行访问控制策略设置；

b) 在调度中心和有人值守站控系统、无人值守站控系统之间部署工业防火墙进行网络层级间的安全隔离和防护；

c) 在各场站 PLC/RTU 等工控设备的网络出口位置部署工业防火墙，以达到重要工控装置的单体设备级安全防护。

（2） 主机安全防护

在调度中心和各场站的工程师站、操作员站及服务器上部署工控主机卫士，保护各主机免受病毒、木马、蠕虫等恶意代码的侵袭。

（3） 网络监测与审计

在调度中心核心交换机上旁路部署安全监测审计平台，实时发现针对 PLC、DCS 等重要工业控制系统的攻击和破坏行为，以及病毒、木马等恶意软件的扩

散和传播行为，为工业控制网络安全事件调查提供依据；

（4） 集中管理

在调度中心部署统一安全管理平台，实现对全网中各安全设备、系统及主机的统一配置、全面监控、实时告警、流量分析等。

4.2.5 小结

该解决方案具备如下特点：

（1） 实现了调度中心与各场站的安全隔离，避免非授权访问和恶意攻击，保护燃气系统网络边界安全；

（2） 避免工控系统主机遭受恶意软件感染和扩散，避免通过普通 U 盘感染主机，保护工控主机安全；

（3） 阻止病毒木马程序进入调度中心和场站操作员站、工程师站和服务器，降低系统被攻击利用的风险；

（4） 实现网内安全产品统一管理，日志统一收集，提高了运维人员的工作效率，降低人力投入成本。

4.3 案例三：某石油石化企业安全解决方案

4.3.1 概述

通过分析石油企业在各生产环节中所面临的信息安全问题，提出了保障生产信息网络安全的防护解决方案，同时具体提出了企业应采取的安全策略和解决措施，阐明了全面构筑工控信息安全体系，消除网络安全隐患，做到防患于未然。

4.3.2 典型安全风险

（1） 油田网络容易遭受病毒等恶意代码的侵袭；

（2） 缺乏监测及防御人为恶意或者无意的违规操作行为的技术手段；

（3） 对外部、内部的网络攻击行为缺乏防御手段；

（4） 安全事件发生后不能迅速定位找出问题根源。

4.4.3 解决方案

（1） 针对油田各生产环节的网络边界和各网络内部区域之间的采取安全隔离和访问控制措施，防止用户的越权访问和非法入侵行为；

（2） 对工控网络中的场站服务器、实时数据库、生产调度系统等主机进行加固，保障主机及其运行数据的安全；

（3） 提供安全数据交换介质，杜绝移动存储介质“滥用”的安全隐患，保障工控主机间数据交换安全；

（4） 提供工控网络操作行为监测审计功能，帮助企业建立网络监测审计机制；

（5） 对油田各层级网络中的安全设备或系统进行集中管理，实现全局配置、集中监控、统一管理，提高管理人员的工作效率，降低企业的人员投入成本。

4.3.4 典型部署

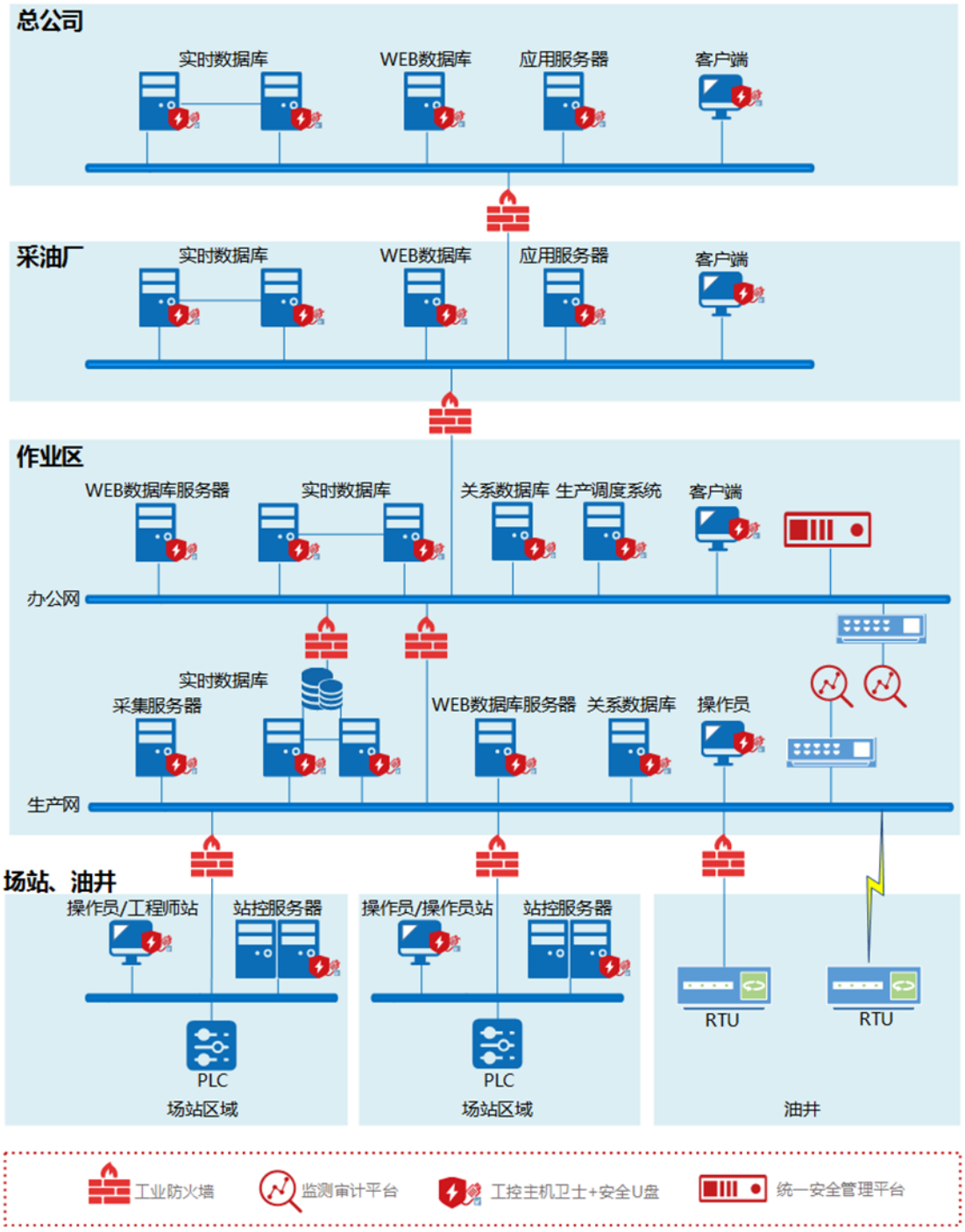

图 26 工控安全规划与访问控制拓扑图

（1） 边界、区域边界防护

在采油厂、作业区、场站油井边界及作业区区域边界部署工业防火墙，对各层级用户和外来的访问进行控制，保障采油厂、作业区等重要生产区域网络的可

用性和安全性。

（2） 主机安全防护

在采油厂、作业区、场站油井的实时数据库、关系数据库、生产调度系统等重要主机系统部署工控主机卫士。采用“白名单”防护机制，保证只有安全的软件程序才能够在主机系统中运行，同时对主机操作系统、注册表等进行防护。

（3） 数据交换安全

采用安全 U 盘作为数据交换介质，避免不安全的移动存储介质进入工控网络影响生产网络的正常运行。

（4） 网络监测审计

在作业区的办公网和生产网旁路部署监测审计平台，监控和记录用户对数据库、生产调度系统、采集服务器的违规操作、误操作行为，为事后调查取证提供依据。

（5） 集中管理

在作业区的办公网中部署统一管理平台，对整个工控网络中的安全设备和系统进行统一策略配置下发、状态集中监控、网络流量分析。实时掌握工业控制网络运行状态，便于出现问题及时溯源定位。

4.3.5 小结

该解决方案具备如下特点：

（1） 阻止病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行；

（2） 阻止非授权软件或进程的安装和运行，防止恶意代码攻击；

（3） 防止操作员使用移动介质带入的病毒在生产网中扩散；

（4） 实时检测工控网络中的恶意攻击、误操作、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播，帮助客户及时采取应对措施，避免发生安全事故。

4.4 案例四：某煤化工企业安全解决方案

4.4.1 概述

化工行业渗透各个方面，是国民经济中不可或缺的重要组成部分，其安全健康发展对于人类经济、社会发展具有重要的现实意义。化工行业的安全影响较之其他行业，存在危害大、范围广、影响时间长等特点，因此保证化工行业生产系统安全运行，特别是保护工业控制系统不被非法破坏显得尤为重要。

4.4.2 典型安全问题

（1） 办公网对生产网的入侵风险；

（2） 对于误操作或非法行为等风险缺乏管控；

（3） 上位机对各生产功能区的PLC和DCS等设备的越权访问、误操作等；

（4） 缺乏事件追踪及调查取证技术手段。

4.4.3 解决方案

（1） 对化工生产网络边界、各车间边界实施访问控制和病毒防护，对关键控制系统进行有效保护，避免指令数据等被非法访问、窃取或篡改；

（2） 对化工生产网重要主机进行安全防护，只允许“白名单”列表中的程序执行，有效检测工作站、服务器上的违规、异常操作并加以阻止；

（3） 采用技术手段，监测、记录化工生产网络中的异常行为并实时告警，为用户制定安全防护策略提供技术支撑，同时为安全事件调查取证提供依据；

（4） 对安全设备进行集中管理，实现对各安全设备、系统及主机的统一配置、全面监控等，杜绝由于事件分散，无法关联分析而导致的安全事件。

4.4.4 典型部署

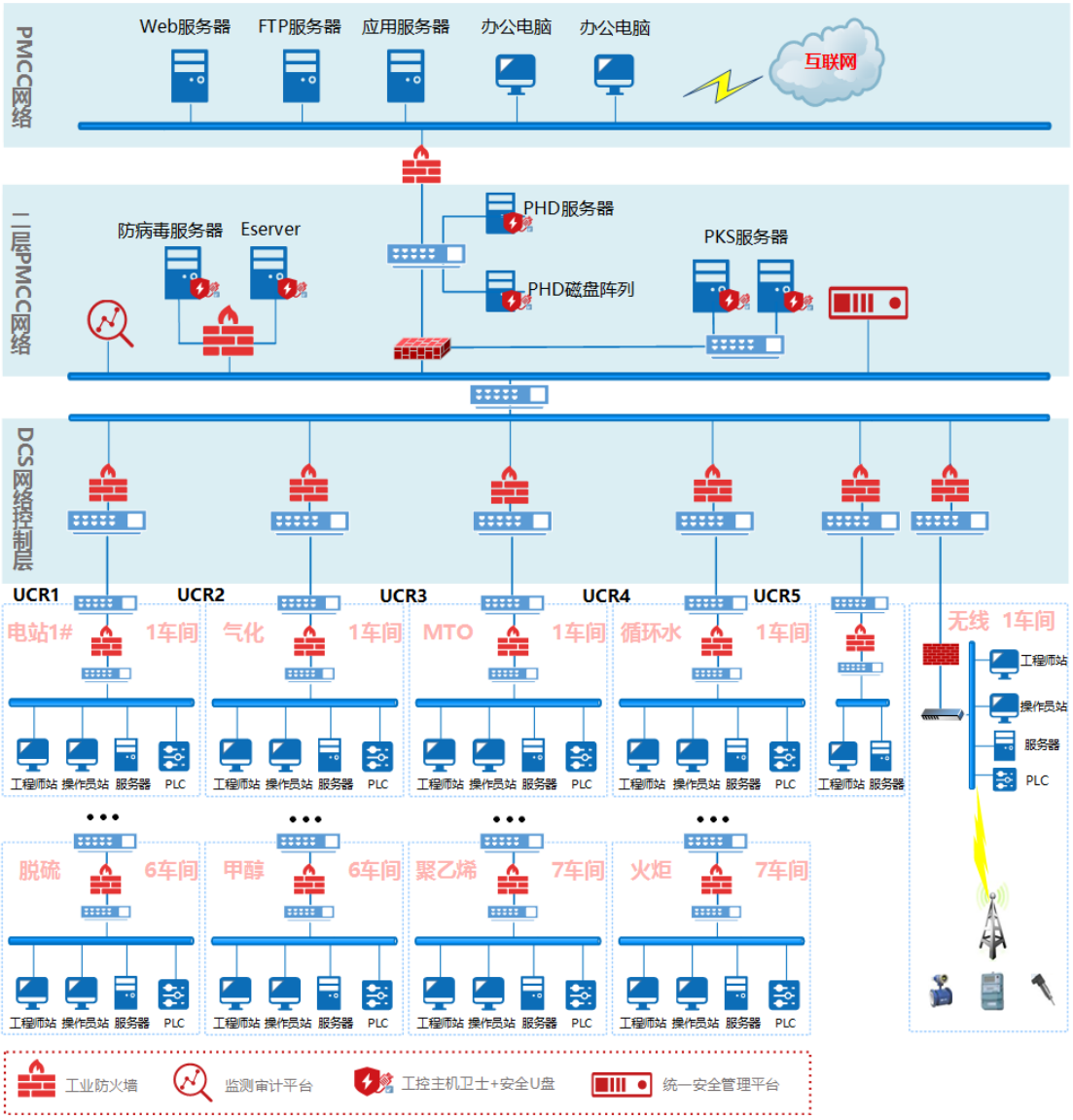

图 27 煤化工企业工控安全方案拓扑图

（1） 边界、区域安全防护

a) 在控制网控制器出口部署工业防火墙对不同区域控制器做逻辑隔离，避免未经授权的命令下发至控制器，保护控制器的数据传输安全；

b) 在控制网和数据监控网交换机之间部署工业防火墙，阻止来自区域之间的入侵攻击和非法访问等，实现横向隔离，将危险源控制在区域内；

c) 在 MES 交换机、工程师站、防病毒服务器前端部署工业防火墙实现边界安全防护，阻止区域间的越权访问、入侵攻击和非法访问等。

（2） 主机安全防护

在工程师站、操作员站及应用服务器上部署工控主机卫士，采用轻量级应用“白名单”机制，有效阻止病毒、木马及 0-day 漏洞的感染和被利用，保障工控主机安全。

（3） 网络监测与审计

在控制网和监控网汇聚交换机上旁路部署安全监测与审计平台，对整个生产控制网络中的流量进行全面无缝监控审计，实现事后可追溯。

（4） 集中管理

在数据监控网中部署统一安全管理平台，对整个生产网络中安全设备和系统进行统一策略配置下发、状态集中监控、网络流量分析等，实时掌握工业控制网络运行状态，出现问题及时溯源定位。

4.4.5 小结

结合风险分析和案例技术分析，本解决方案具备如下特点：

（1） 满足国家及行业政策法规及相关技术要求；

（2） 提高企业整体安全防护水平，保障生产安全稳定运行；

（3） 提供安全审计手段，协助管理员快速发现并解决安全问题；

（4） 通过统一安全管理平台，有效提高工作效率，降低运维成本。

5．水务电力行业典型安全解决方案

智慧水务是通过物联网、云计算、移动互联网技术实现对水务数据的分布式采集与统一处理，从而实现对城市供排水系统运行状态的实时感知，以更加精细和动态的方式管理水务系统的整个生产、管理和服务流程，从而达到“智慧”的状态。

智能电网基于先进的传感测量技术、先进的控制技术、先进的决策支持系统等，以实现电网可靠、安全、经济、高效、环境友好和使用安全为目标。其主要特征包括自愈、激励和包括用户、抵御攻击，提供定制化的用户用电需求和不同发电形式的接入、调配和输配电等，实现电网的高效运行。

本案例汇编包括三个水务电力行业的典型安全解决方案。

5.1 案例一：某智能电网安全解决方案

随着电力行业构建智能电网、跨区域输电、清洁能源等发展，电网的可靠性与安全性尤为重要，变电站作为连接发电与输配电的重要环节，逐步在从传统的变电站转换为智能变电站，已成为智能电网管理调度的灵魂与核心，也产生了诸多的信息安全问题。

国家能源局对电力行业的信息安全已明确提出相应要求，发电、输电、变电、配电行业等严格按照 14 号令及 36 号文件的要求执行，保证安全生产。

5.1.1 案例概述

国家能源局积极响应国家网络安全战略要求，为保障基础能源设施的安全，每年组织对系统内部进行安全大检查。检查标准参照电力行业 14 号令及 36 号文相关要求。

国家电网某市调控中心积极配合安全检测工作，对于智能变电站的信息安全风险尤为重视。客户要求对智能电站存在的风险点、风险识别与分析、风险控制等几个方面进行安全加固。主要需求如下：

（1） 需要对智能电站网络通信流量进行实时呈现展示；

（2） 对内外部的网络通信指令进行深度解析，并识别哪些为异常指令；

（3） 能针对特定通信指令、安全事件进行溯源；

（4） 需要满足 14 号令、36 号文件要求。

5.1.2 典型安全风险

针对变电站的网络安全区及网络访问通信框图如下：

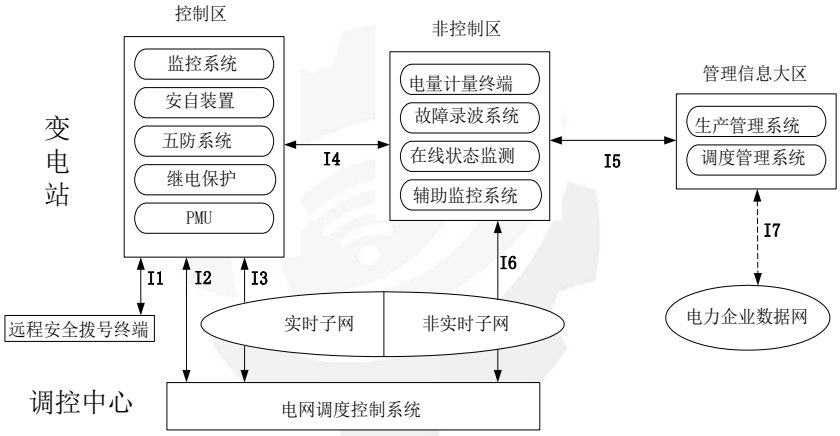

图 28 网络安全区及网络访问通信框图

变电站电力监控系统安全分区表				
序号	业务应用或设备	控制区	非控制器	管理信息大区
1	变电站监控系统	变电站监控系统		
2	五防系统	五防系统		
3	广域相量测量装置	广域相量测量装置		
4	继电保护	继电保护装置及管理模块		
5	安全自动控制	安全装置及管理模块		
6	火灾报警	火灾报警		
7	电能量采集装置		电能量采集装置	
8	故障录波		故障录波装置	
9	一次设备在线监测		一次设备在线监测	
10	辅助设备监控		辅助设备监控	
11	生产管理			生产管理终端

智能变电站是通过专线向上连接，所以安全风险主要集中在内部和运维时的风险，如下：

（1） 能够接受来自其它调度控制系统的刀闸闭合可能导致的系统中断。虽然智能变电站通过专线与调度连接，所以能够接受来自其它调度系统的指令。

（2） 可能接受错误的遥控，遥测，造成系统的失控。

（3） 机器人巡检路线可能会被远程控制，远程运维的误操作导致造成控制系统跳变、错误动作、停机等事故。

5.1.3 安全解决方案

目前智能变电站的三层两网是目前最常见的一种网络设计架构，是指三层设备通过两层网络互联，及过程层和站控层交换机独立配置，防护系统部署如下图所示。

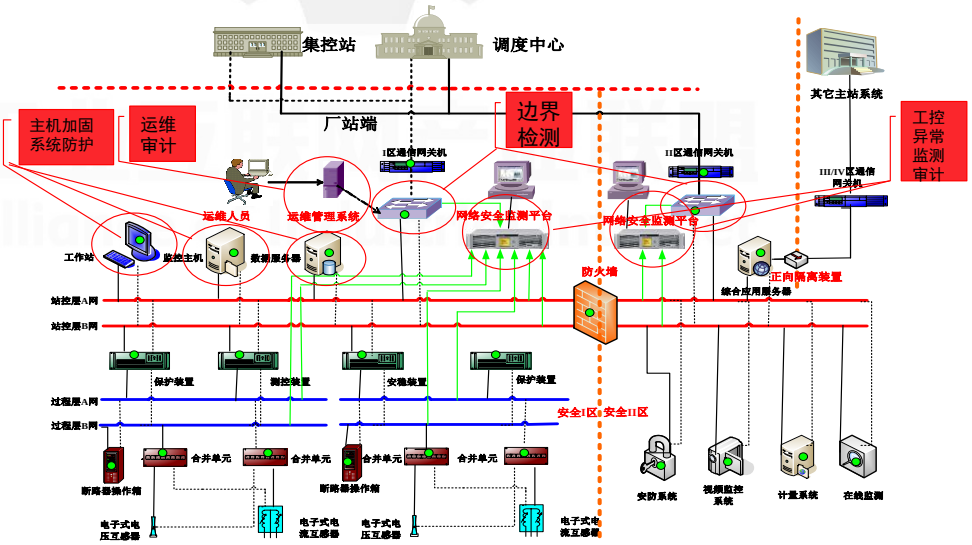

图 29 工控安全防护系统部署图

基于电力 36 号文安全防护要求结合指南，针对智能电站二次监控系统的安全防护内容包括：

（1） 网络边界安全域划分和防护

在安全 I 区、II 区网络边界各横向纵向核心交换机处，旁路部署边界工业防火墙。

（2） 终端安全防护

在安全 I 区、II 区各操作站和工程师站上部署主机加固系统，实现对各终端的安全防护。

（3） 异常网络行为监控与审计

在安全 I 区、II 区网络边界各横向纵向核心交换机处部署工控异常监测与审计产品，满足对异常通讯协议、异常指令的识别解析、异常流量、异常网络行为的实时监控，流行为的展示等需求。

（4） 运维审计过程安全防护

在各安全 I 区 II 区内部署工控运维审计系统，满足对运维过程的安全审计的需求。

5.1.4 小结

实施完上述安全系统后，与指南对应并结合 36 号文要求将达到如下效果：

（1） 可配合管理制度对实现对操作员站、工程师站外设的严格控制。可实现对工程师站、操作员站的 USB、光驱、无线等接口进行严格外设控制。

（2） 实现对工控网络设备安全配置进行审计与完善。

（3） 实现了阻断来自管理网的非法行为。实现了对变电站的非法行为的访问控制。尤其是基于 61850 的访问控制；实现对远程访问行为的访问控制及加密。

对所有设备操作的日志进行记录可供日后溯源；强化工业控制网络设备身份认证；实时监测针对变电站监控系统的异常流量、异常指令的监测、异常指令的识别解析。

（4） 实现了来自调度内部或运维时带来的病毒和恶意代表的防护；及时发现系统的问题和脆弱性，以便提前进行修补；实现了主机的强认证和避免主机的弱口令。

（5） 能提前获知工控系统的安全配置现状并根据需求提前防护；加强工业控制设备的身份认证强度；对工控异常访问行为及违法操作进行安全防护；清晰了解工业控制系统的资产情况；加强组态软件身份认证强度；保证重要工业数据安全性。

5.2 案例二：某变电站二次系统信息安全综合监管解决方案

5.2.1 案例概述

本项目需要在某供电局调度主站建设一套集中管理平台，管理各个变电站监管数据的集中展现与处理，选择几个变电站作为项目试点。

项目的总体需求分为主站需求、变电站资源管控需求与安全管控需求，本项目主站需求对应“平台”，用于收集、展现资源管控、安全管控的数据；

资源管控需求对应“网管”，用于对变电站数据性能、状态数据监视；

安全管控需求对应“安全”，用于变电站安全审计、配置核查、流量审计、终端防护数据的采集与监视。

其中本案例主要是做的是“安全管控”方面内容。

5.2.2 典型安全风险

变电站安全风险主要有如下方面：

（1） 变电站工作站缺乏统一管理

站内信息化程度越来越高，无人值守站也随之增多，现阶段二次安全防护主要侧重于边界安全，缺乏变电站内部安全防护

（2） 缺少移动介质接入监视

无法对监视后台、维护工作站的外接 U 盘/移动硬盘/手机等移动介质进行防范和监视；

（3） 缺少安全日志审计

无法对站内设备进行安全日志审计，无法及时发现和记录一些违规事件，安全预警、恶意代码、信息危害、系统状态等进行监视

（4） 缺少安全配置基线核查工具

缺少对站内设备进行安全基线核查工具，无法提前发现站内设备存在的系统弱口令、漏洞隐患、违规软件等进行监视

（5） 缺少报文审计工具

缺乏工具化的手段，对主子站通信的报文信息进行升级，无法判断报文通信

合规性性。

5.2.3 安全解决方案

系统实现如下功能：

（1） 安全审计

记录安全审计日志，包括设备的日志、站端采集的报文以及非法互联事件等内容。

日志审计：实现主机以及安全设备（如防火墙、正反向隔离装置、纵向加密装置、入侵检测装置等安全设备）的日志采集；实现工作站配置核查的核查结果数据采集，如漏洞、病毒扫描等日志。

报文审计：记录报文数据，并根据主站下发的查询条件反馈相应的报文数据；

非法互联审计：记录设备与设备之间非法互联通信，记录设备之间非法通信的时间、通信流量、及对应的报文索引，可根据报文索引查询对应的报文记录；

记录新设备非法接入，包括 U 盘非法接入工作站、移动终端非法接入网络等事件。

（2） 配置核查管理（主站端）

实现对站端设备的配置核查，站端设备包括工作站、服务器、网络设备等。主站端负责管理核查基线，并下发到站端。功能包括：

a) 内置本集团二次系统安全防护配置基线检查和电力行业等级保护合规性脚本库。支持安全基线检查项自定义功能，支持检查项参数化功能。
b) 支持对多种操作系统、网络设备（如交换机、路由器、防火墙等）以及数据库的核查基线；支持对主流数据库（如 MySQL 等）的安全配置检查。
c) 支持对安全对象的配置脆弱性进行全面检查，识别内容应包括操作系统和网络设备和数据库等的账号、口令、授权、日志安全要求、不必要的服务、启动项、注册表、会话设置等配置。
d) 支持利用预设的管理员账号、密码信息内实现对操作系统、数据库和网络设备的安全配置检查，预设信息支持主站端维护，并下发站端作为检查策略。

e) 支持灵活的检查任务制定功能，可以在主站端设定手动、定时和离线任务的配置任务检查方式。支持实时显示检查任务进度和检查任务状态。

（3） 工作站配置核查（客户端）

实现从主站下载基线功能，主站可通过命令下发，站端接收主站的基线文件，并自动更新最新核查基线。实现基线版本管理、基线升级日志等管理功能。

工作站端功能模块包括客户端的安装程序，以及装置的基线管理功能。客户端安装程序需实现友好安装界面，并实现从站端装置的升级程序、更新核查基线文件等功能。

核查要求包括：

a) 支持对站端的工作站、监控主机等设备的核查；

b) 支持通过安装代理或非代理等方式进行核查；

c) 支持 Linux、Windows 等操作系统；

对工作站进行监控，采集配置信息，并建立基线进行比对，告警。要求支持检查的配置信息包括：

a) 系统弱口令检查

b) 防病毒软件检查

c) 系统补丁检查

d) 软件安装记录检查

e) 软件卸载记录检查

f) 系统进程与服务黑白名单检查

g) 非法外联检查

h) 网络连接异常监控

i) 外接存储设备核查

工作站对 U 盘/移动硬盘等设备进行接入控制，未认证的 U 盘/移动硬盘自动被工作站操作系统禁止接入。

（4） 安全管控告警

对变电站二次设备非正常运行状态进行告警，具体包括但不限于非法设备接入告警、设备离线告警、配置核查告警、业务行为异常告警。

告警数据可来源各个模块并进行综合展示及查询，响应主站召唤上送告警或

站端主动上送告警信息。功能如下：

非法设备接入告警功能包括：对非法的 IP/MAC 设备接入、对非法 IP 地址段使用和接线错误、对接入工作站的未认证的 U 盘设备等进行告警

定时对工作站等计算机设备进行配置核查，根据核查结果进行告警。

提供告警记录的实时查询，可根据分类、分级进行查询。

将告警信息推送到资源管控运维装置。

（5） 远程通信

实现与主站通信，接收主站运维终端注册信息、配置核查相关核查基线库、病毒库等核查信息、指令，并将安全审计日志、配置核查结果等信息上送到主站。主站与站端的通信规约宜应通过 61850 规约进行通信，双方应约定信息模型。

与主站传送的信息包括且不限于如下：

运维终端注册信息：注册的运维终端注册信息，下发到站端；

安全审计日志：包括从被监视设备的采集的安全审计日志，支持压缩后上传；

配置核查、病毒库信息：包括工作站核查所需的配置核查、病毒扫描等信息；

告警信息：包括非法终端接入告警、配置核查告警、非法外接存储设备告警等；

应该提供与主站之间的通道运行状态进行监视，如通道中断应该进行告警。

（6） 级联需求

主站平台与子站平台需要实现子站平台告警信息上传至主站平台，主站平台对子站平台进行配置核查任务调度，主站平台对所有变电站进行 U 盘签发。

设备部署图如下：

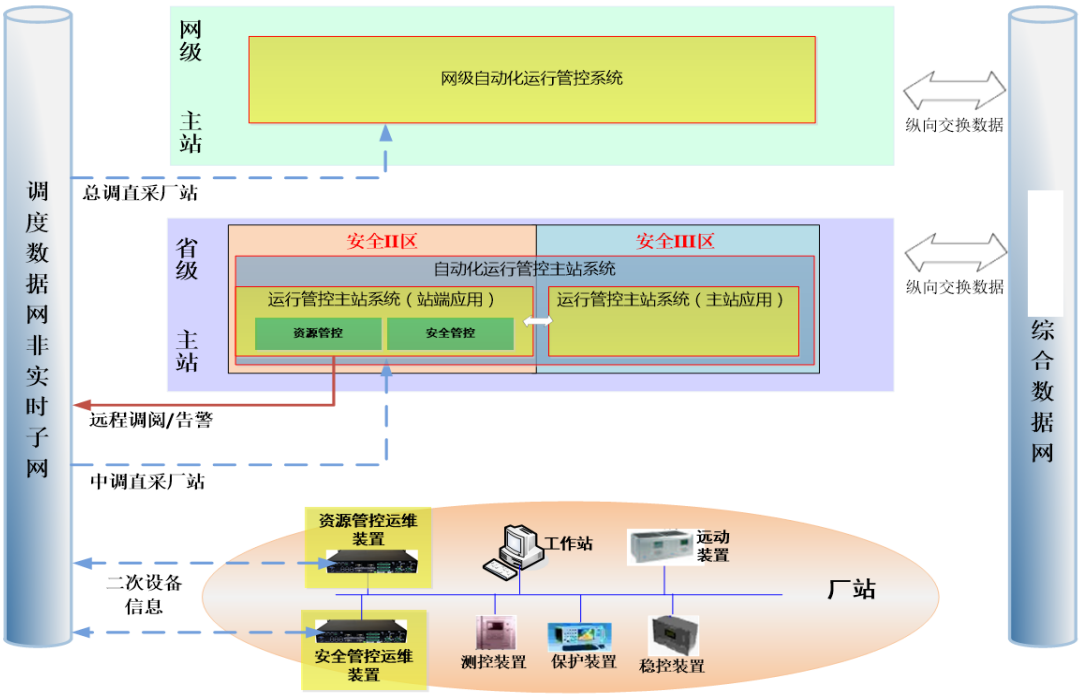

图 30 工控安全部署图

5.2.4 小结

该项目解决了变电站安全审计、配置核查、流量审计、终端防护四个方面的安全问题，并开创性的将安全监管与变电站的业务系统相结合，大大提高了安全运维的效率，使得变电站的信息安全可见可查可控。

5.3 案例三：某电力企业安全解决方案

5.3.1 概述

电力行业是国民经济的基础产业，保证持续、高效的电力供应是关系到国计民生的大事，也是电力部门工作注目的焦点。电力系统的运行涉及到发电厂、变电站、调度中心;发、输、配电系统一体化，系统包括了各种独立系统和联合电网的控制保护技术、通信技术、运行管理技术等。随着电力行业的不断发展，基于互联网的跨地区、全行业系统内部信息网开始逐步建立，网上应用着各种电力

业务及办公系统，电力信息网络系统的网络安全问题愈来愈显得重要，迫切需要做好各类电力系统的安全防护，避免“乌克兰电网事件”重演。

5.3.2 典型安全风险

（1） 工业控制网络安全防护能力不足，系统之间缺乏访问控制和入侵防御机制，不能防范非法终端接入网络;

（2） 由于流程工业生产特点，目前未部署任何工业控制信息安全审计措施，出现信息安全事件没有证据可查、可追溯;

（3） 由于工业系统特点，大量主机未安装防病毒软件或长期未更新病毒库;

（4） 大量上位机的操作系统属于老旧系统，存在高危漏洞;

（5） 工业控制信息安全不能做到统一管理，存在信息孤岛。

5.3.3 解决方案

（1） 边界隔离（生产控制区和非控制区之间）

部署具备隔离保护功能的安全设备实现网络分层分区，边界访问控制，避免无授权设备对区域的访问，实现基于通信“白环境”边界攻击防御；

（2） 区域隔离（生产控制大区内部）

采取接入控制措施实现基于区域和功能的网络划分及隔离，对工业专有协议进行深度解析，建立通讯“白环境”，阻止区域间的越权访问，病毒、蠕虫扩散和入侵，将危险源控制在有限范围内；

（3） 重要系统隔离

采取安全隔离措施，对 PLC、DCS 等工控设备或系统安全漏洞利用等行为进行阻断，同时阻止操作员或工程师有意无意的非法操作；

（4） 工控网络监测与审计

采用安全审计功能，对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等进行集中收集、自动分析，及时发现各种违规行为和病毒、黑客的攻击行为；

（5） 主机安全防护

对主机进行安全防护，阻止非授权及恶意软件运行，同时对操作系统进行加

固，如注册表、配置文件等；

（6） 入侵检测系统

检测网络通讯流量中的入侵行为，分析潜在威胁并进行安全审计；

（7） 统一安全管理

集中管理安全设备，如工业防火墙、工控主机卫士、监测审计平台等，实现工控网络的拓扑管理、安全配置及安全策略管理、设备状态监控、告警日志等。

5.3.4 典型部署

✧ 火电业务场景

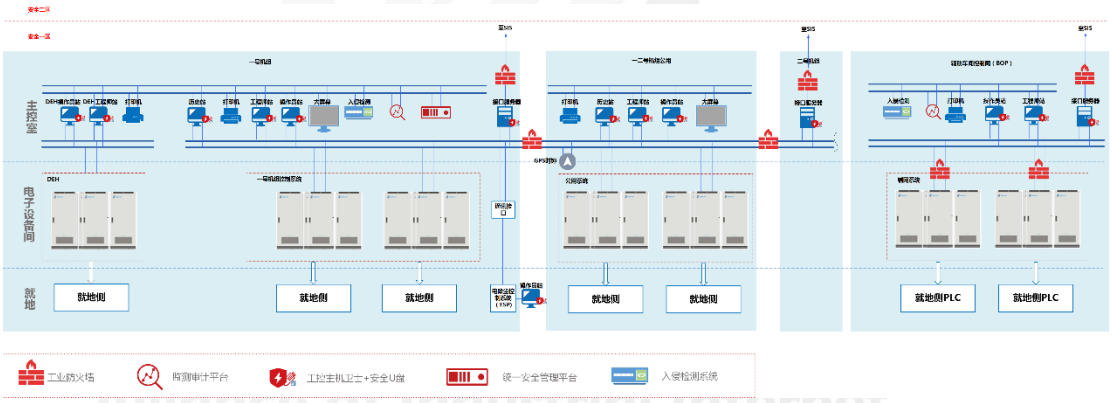

图 31 火电场景安全部署图

（1） 在安全 I 区所属的一号机组、二号机组、辅助车间控制网与安全 II 区的 SIS 系统网络边界部署工业防火墙；

（2） 在安全 I 区内一号机组、二号机组与共同使用中央空调系统、压缩空气系统、凝结水系统、脱硫公用系统、电气公用系统的公用系统网络边界部署工业防火墙，保证安全 I 区内一号机组、二号机组控制系统免受来自于公用系统的安全风险；

（3） 在安全 I 区的操作员站、工程师站、历史服务器上安装工控主机卫士，只允许白名单列表中的程序执行，避免非授权访问，同时实施移动存储介质安全管控，保证主机间数据交换安全；

（4） 在一号、二号机组控制系统交换机上旁路部署监测审计平台，对控制系统进行监控、告警、审计，及时发现安全问题；

（5） 旁路部署统一安全管理平台，实现主辅网安全系统的统一管理和日志汇总分析。

✧ 水电业务场景

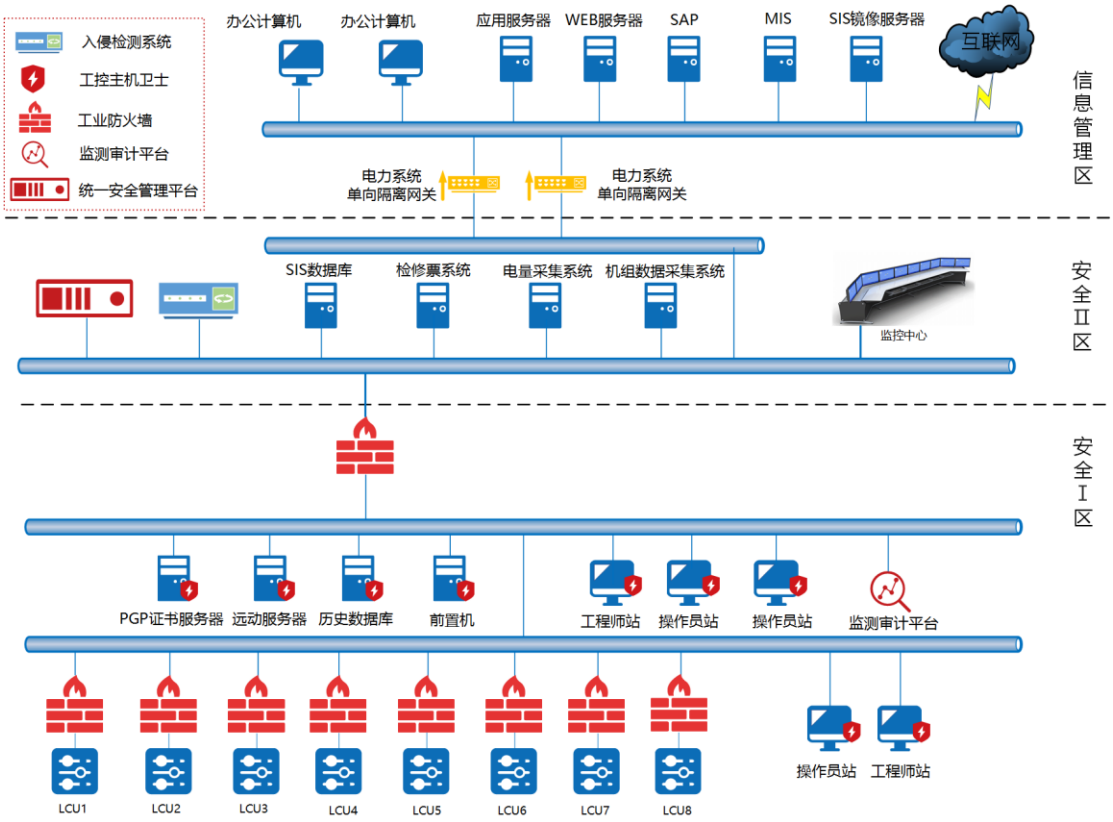

图 32 水电场景安全部署图

（1） 在安全 I 区内的 LCU 本地控制单元前部署工业防火墙，通过工控协议深度解析及应用协议白名单机制，实现安全 I 区内不同 LCU 本地控制单元的独立安全；

（2） 安全 I 区与安全 II 区之间部署工业防火墙，通过对 OPC 数据采集协议进行深度解析，实现两个不同安全等级区域间的信息安全保护及网络隔离；

（3） 在安全 I 区内旁路部署安全监测审计平台，实时监测记录误操作和各类违规行为；

（4） 在安全 I 区内所有操作员站、工程师站、应用服务器、数据库服务器上部署工控主机卫士，避免相应恶意软件、误操作等带来的安全风险；

（5） 在安全 I 区、安全 II 区内，旁路部署入侵检测系统，实现监测控制大区内病毒、木马及恶意攻击行为等，保护生产控制大区内工控设备及系统免遭恶

意代码的攻击；

（6） 在生产控制大区内部署统一安全管理平台，实现工业防火墙、监测审计平台、工控主机卫士等的集中管理和日志归并分析，降低运维难度难度，提升安全防护效率。

✧ 风电业务场景

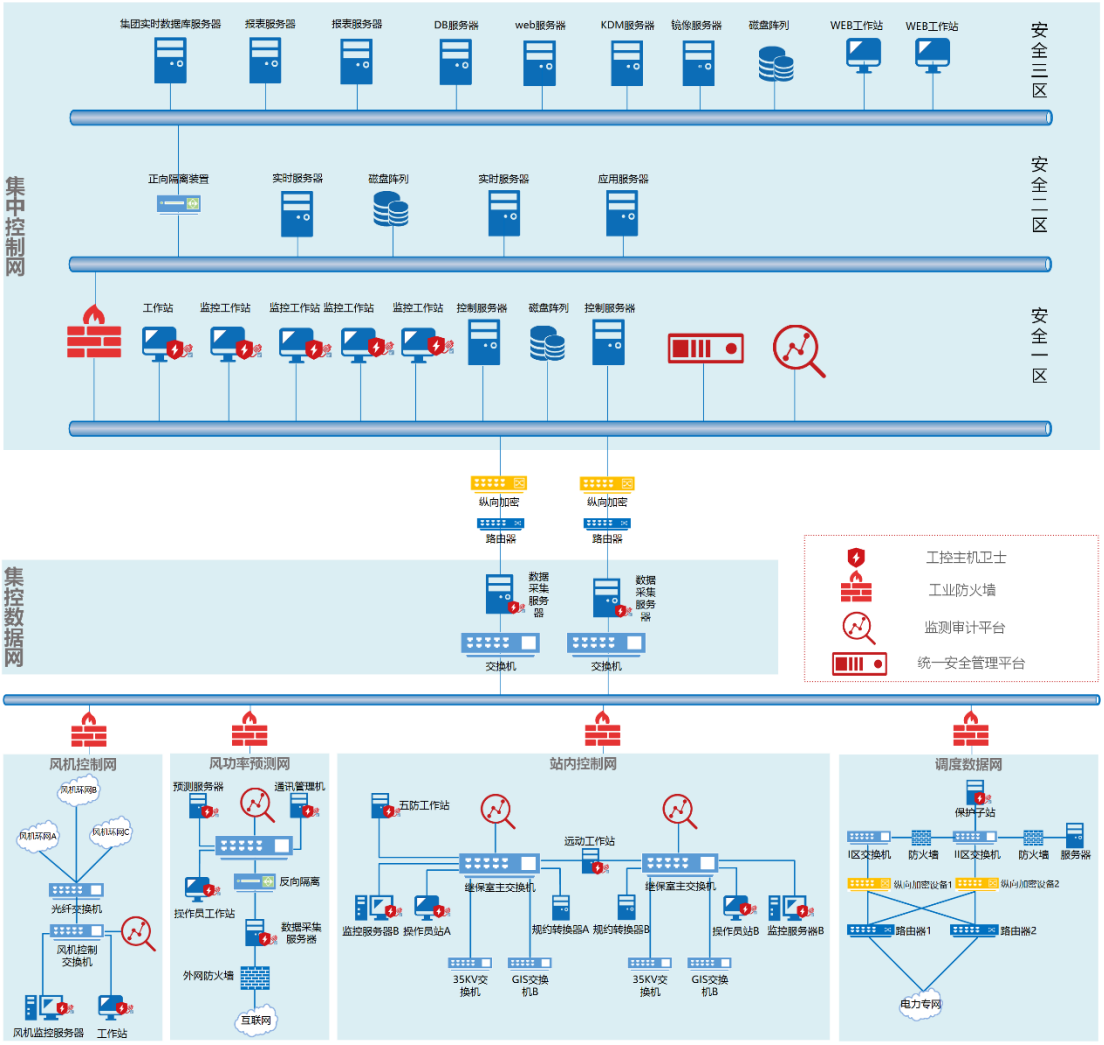

图 33 风电场景安全部署图

（1） 在集中控制网与调度数据网、风控率预测网、站内控制网、风机控制网间加装工业防火墙，通过协议深度解析和严格访问控制策略，避免各控制网络遭受来自于其它系统的网络攻击行为；

（2） 在各控制网内旁路部署安全监测与审计系统，实现对安全 I 区内各种恶意攻击行为的及时告警及记录，为工控网络安全问题提供追踪溯源技术手段；

（3） 在安全 I 区和各控制网操作员站、工程师站、应用服务器、数据库服务器上部署工控主机卫士软件，保护主机和服务器免遭恶意攻击；

（4） 在集中管理区部署统一安全管理平台，实现工业防火墙、监测审计平台、工控主机卫士的集中管理。

5.3.5 小结

本解决方案按照电力系统 36 号文、工业控制系统系统信息安全防护指南等政策法规要求，结合火电、水电、风电的自身特点，从网络防护、主机防护、安全审计、入侵检测、统一管理等方面提出了电力行业的信息安全技术解决方案，从而在满足政策法规的技术上，整体提升电力系统信息网络的安全防护等级。

5.4 案例四：核电信息系统安全解决方案

核电作为一种安全、清洁、低碳、可靠的能源，是重要的能源组成部分。根据我国核电发展规划，到 2020 年，核电运行装机容量将从现有的 1000 万 kW 发展到 4000 万 kW，在建装机容量 1800 万 kW。在国家发电行业中，核电比重越来越大，对工业及居民用电影响力也不断增加。

核对于各个国家来说，一旦出现安全事故，都是影响其国家战略发展的。因此，各国尤其是我国，对于核电的投资、建设和运营以及后续的闭堆，都是极为谨慎的。但是，正因为核电的战略意义，许多核电站都成为了不法分子、敌对势力有组织、有预谋的逐渐渗透、潜伏、直到有目的地发动网络攻击的主要目标。因此，在核电行业方面，工业控制系统信息安全极其重要。

5.4.1 概述

原则上可以将发电厂基于计算机及网络技术的业务系统划分为生产控制大区和管理信息大区，并根据业务系统的重要性和对一次系统的影响程度将生产控制大区划分为控制区（安全 I）和非控制区（安全 II 区），重点保护系统生产控制以及直接影响电力生产的系统。

实际应用在核电厂的数字化仪控系统主要包括反应堆保护系统和核电站控制系统两大部分。系统主要接口包括与堆外监测系统的接口、与核反应堆保护系统的接口、与地震监测系统的接口、与全厂辅助系统（BOP）的接口、与电厂监控信息系统（SIS）的接口。这些接口的类型主要包括：堆芯控制专用的数据接口，专用的 MODBUS 接口，标准 OPC 接口、标准 ProfiBus 接口、Modbus 接口等。

5.4.2 典型安全需求

（1）目前，核电厂生产网络中的上位机多数使用老旧版本微软操作系统，由于生产控制网络的封闭及控制系统对业务实时性要求较高，无法进行正常的系统漏洞升级操作，导致使用的微软操作系统存在大量安全漏洞。

（2）核电厂生产网络中的工程师站、操作员站和服务器大多没有安装任何杀毒软件，或者安装杀毒软件但限于工业网络现状长期没有进行代码更新，缺少恶意代码防护功能。

（3）核电厂生产网络信息交互通常通过移动 U 盘等介质进行，移动介质在管理网和生产网之间交叉使用，难免会感染病毒或恶意代码，进而导致上位机被攻击。

（4）根据 ICS-CERT 和 CNVD 权威统计，目前常用的工业控制软件（如 DCS 控制软件等），均或多或少存在安全漏洞，使核电控制系统存在威胁。

（5）核电厂工业网络缺乏边界防护措施，部分部署传统防火墙，但是无法识别工业协议，也就无法防范来自外部的工业攻击。

（6）核电厂生产控制网络内无安全区域规划，所有设备及控制设备及服务器均通过核心交换机进行数据交互。交互过程中无安全防护，数据在传输过程中容易受到攻击或篡改。

（7）核电厂生产控制网络存在远程维护通道，很多工业控制设备维护依赖提供商，由此也带来了入侵的途径，存在一定的安全隐患。

（8）工业通讯协议脆弱，部分在用协议缺乏认证、缺乏授权、缺乏加密。

（9）核电厂生产控制网络内工控账户缺乏分级保护措施，身份认证基本采用简单的用户名密码方式，存在身份冒用的风险。

（10）核电厂生产控制网络缺乏重要工业数据的分级分类管理和备份措施，存在数据丢失的安全风险。

5.4.3 解决方案

（1）主机安全加固：核电 DCS 所使用的工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。

（2）移动介质防护：在控制网中，采用专用的移动存储设备，进行安全防护，消除此处隐患。

（3）应用安全防护：在主机上采取安全措施，对操作行为进行审计。远程接入设备时，应采用具有会话认证、加密与抗抵赖等安全机制的安全防护措施。

（4）横向边界防护：核电厂生产控制大区与管理信息大区之间通信应当部署电力专用横向安全隔离装置。核电厂（DCS）系统部署在控制区，与核电厂厂级监控系统优化功能进行信息交换应当部署逻辑隔离措施。

（5）纵向边界防护：核电厂控制大区系统与调度系统通过电力调度数据网进行远程通信时，采用认证、访问控制、加密等技术措施实现数据的远方安全传输以及纵向边界的安全防护。

（6）第三方边界防护：核电厂控制大区中的业务系统与环保、安全等政府部门进行数据通信时，其边界应采用防护方式进行隔离。

（7）网络安全审计：对控制区网络进行协议审计、流量审计，进行网络入侵检测，掌握网络安全信息。

（8）无线入侵防御：采用无线入侵防御系统，监控非法无线热点和可能的非法无线入侵。

（9）数据安全：定期对关键业务的数据进行备份，并实现历史归档数据的异地保存。关键主机、网络设备或关键部件应当进行相应的冗余配置。控制区的业务一定要使用冗余配置。

（10）安全运营：建设工业安全运营中心，通过监测全网流量、收集安全设备日志，发现网络中的已知威胁和未知威胁，遵循发现、阻断、取证、溯源、研

判、拓展的安全业务闭环，完成威胁处置。

（11）定期检查：配置检查工具，定期对封闭网络的安全运营状况进行检查。

防护方案设备部署情况如下图所示：

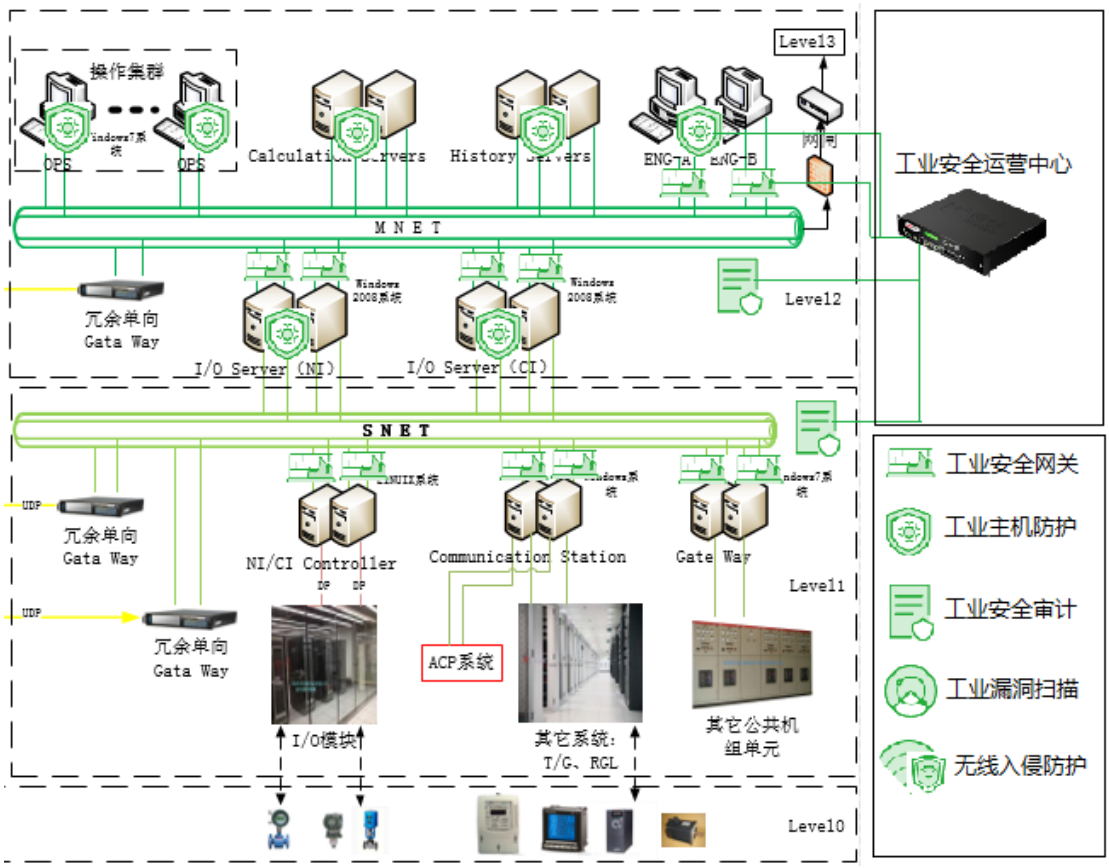

图 34 核电厂信息安全方案部署示意图

5.4.4 小结

针对我国核电站的特点，开展核电仪控系统、安全级与非安全级系统、相关信息系统的安全建设势在必行，发现问题、解决问题，同时与设备厂商、核能设计有关单位、核电工程实施公司等建立我国自主的核电信息安全标准化体系、安全防护方案，保障我国核电站的信息安全，避免发生美、德、韩等国类似的核电信息安全事件，更可以保障我国核电“走出去”的发展战略。

6．烟草行业典型安全解决方案

随着人们对健康的重视，全国正在大力开展禁烟运动，同时市场需求使然，广大消费者也对烟草品质提出了更高的需求。烟草行业作为传统制造行业，其生产经历了从田间到仓储、烘烤、制丝、卷制、包装、销售等工艺流程，每一个工艺流程都有不同自动化制造设备参与其中，而烟草自动化更重要的在于制程可视、系统监管全方位及制造绿色三个层面，从而实现烟草生产的最佳质量控制。

本案例汇编包括两个烟草行业的典型安全解决方案。

6.1 案例一：某卷烟厂典型工控安全解决方案

烟草行业在生产系统中大量使用了工业控制系统，在两化融合的大趋势下，行业中的工业控制网络与办公网络的互联互通是一个必然的趋势。从烟草行业普遍性角度来看，工业控制网络与办公网络的连接基本上没有进行任何逻辑隔离和检测防护，工业控制网络基本上不具备任何发现、防御外部攻击行为的手段，外部威胁源一旦进入公司的办公网络，则可以一通到底的连接到工业网络的现场控制层网络，直接影响工业生产。另一方面工业控制网络内部设备如各类操作站、终端等，大部分采用 Windows 系统，为保证工业软件的稳定运行无法进行系统升级甚至不能安装杀毒软件，存在着大量漏洞，在自身安全性不高的情况下运行，因此工业控制系统的安全风险不言而喻。

6.1.1 案例概述

某烟草工业责任有限责任公司在工控安全建设方面存在着一些亟需解决的问题，在制丝、卷包、物流、动力这几个工控系统网络中针对于工控安全的防护措施存在不足。工控网络边界访问控制策略缺失，服务器或操作站感染病毒后，很可能迅速通过工控网络传播到其他设备直接影响 HMI、PLC 等设备的正常运行。此外，针对整个制丝集控网络中存在的风险情况不能及时掌握，缺少针对工控异常行为的检测手段。综合上述卷烟厂工控系统实际情况，亟需通过本项目提高工控安全建设以提高防护水平，确保卷烟生产平安有序进行。

某烟厂通过本次工控安全建设项目建设，实现了以下目标：

（1） 管理人员对目前自身工控系统所存在风险能够精确掌握。

（2） 在对生产网和管理网边界进行隔离，确保管理网对生产网访问的安全性。

（3） 技术人员对生产网中入侵、异常行为的及时发现，对现场设备进行深度防护。

（4） 管理人员、技术人员对整个工控系统各类设备运行状况、安全状况统一管理。

6.1.2 典型安全风险

通过对某烟草工业有限责任公司制丝、卷包、物流、动力四类工控系统现状分析后，发现 A 烟草工业有限责任公司工控系统目前存在以下一些风险：

（1） 管理网和生产网互联，管理网风险容易引入生产网。

随着工控系统的集成化越来越高，烟草生产系统各个子系统的互联程度大大提高。管理网中的 MES 系统需要与制丝、卷包、物流、动力能源各个车间互联，对各个车间下发生产数据。但在管理网和生产网边界访问控制策略缺失等问题导致一旦管理网服务器感染病毒后，可以迅速通过工控网络传播到现场控制设备，直接影响操作员站、工程师站故障，影响正常生产。

（2） 网络访问关系无审计。

由于工控系统的特殊性，设备之间访问关系以及访问所使用的协议、端口都比较固定，因此如果出现设备间的异常访问则应及时关注是否为入侵行为。某烟草工业有限责任公司内有些工控系统经过多次技改建设，存在整个工控系统内设备间访问关系不明确的现象，目前没有任何在网络层面和业务层面对系统内设备异常访问的发现及审计。

（3） 工控设备存在风险。某烟草工业有限责任公司现场所使用的西门子 S7-300、S7-200 的 PLC 以及所使用的主要组态软件 Ifix 在投产运行后未进行过更新存在着大量漏洞，时刻威胁着工控设备正常运行。

图 35 漏洞扫描结果 1

图 36 漏洞扫描结果 2

（4） 工业协议存在风险。目前 A 烟草工业有限责任公司工控系统中所使用的 OPC、Profinet 等工业协议更多的是考虑协议传输的实时性等符合工业需求，但是在安全性方面考虑不足，存在着泄露信息或指令被篡改等风险

（5） 缺乏统一监控管理。

目前在某烟草工业有限责任公司缺乏统一有效的信息安全监控工具对工业控制系统中的网络设备、服务器、数据库等进行有效安全监控和管理，在工业控制系统和控制网络的设备出现故障时，不能提供及时的预警和故障定位，造成排障时间较长。

6.1.3 安全解决方案

本方案的整体思路主要依据行业网络安全“分级分域、整体保护、积极预防、动态管理”的总体策略。首先对某烟厂整个工控系统进行全面风险评估掌握目前

工控系统风险现状；通过管理网和生产网隔离确保生产网不会引入来自管理网风险，保证生产网边界安全；在各车间内部工控系统进行一定手段的监测、防护，保证车间内部安全；最后对整个工控系统进行统一安全呈现，将各个防护点组成一个全面的防护体系，保障其整个工业控制系统安全稳定运行。

（1） 全面风险评估

对某烟厂整个工控网的评估，整体思路如下图所示：

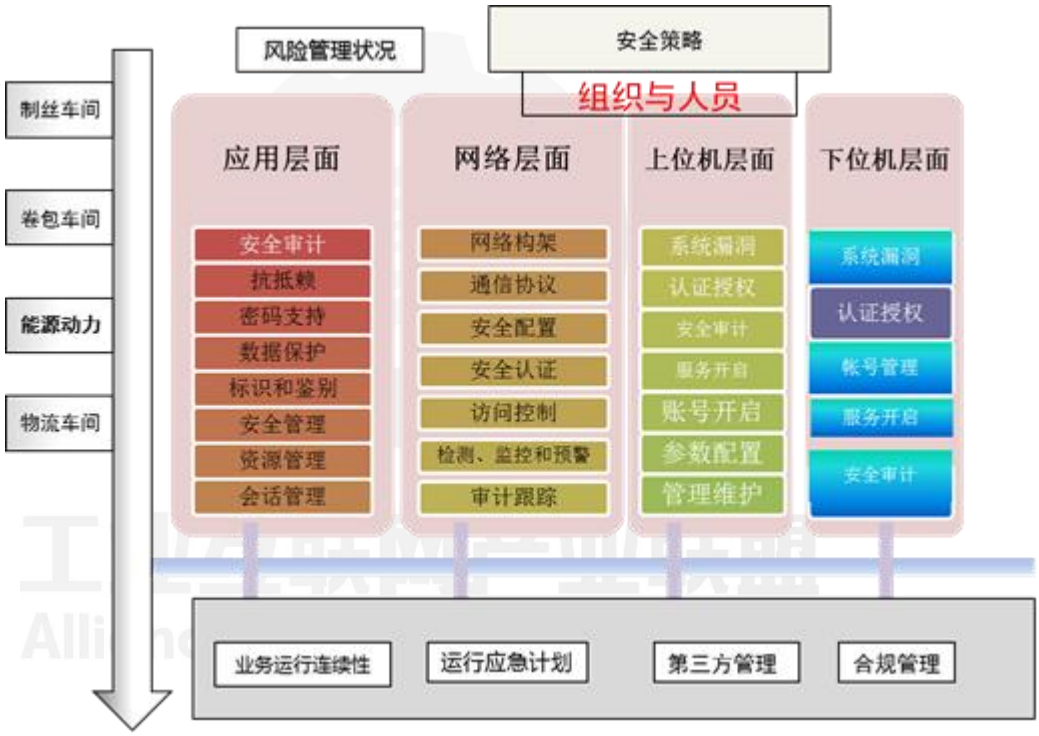

图 37 风险测评思路图

技术方面是从应用、网络、上位机、下位机几个层面展开。

管理方面是从合规、组织与人员、风险管理、安全策略、业务连续性、第三方管理等方面展开。

最终通过风险评估准确了解工控网络系统安全现状，详细掌握工控系统威胁和风险;通过评估结果，找出工控安全的具体建设需求，以便真正满足企业的实际情况，为进一步提出安全建议提供有力支撑;通过评估找出安全隐患的轻重缓急，以确保工控安全建设的阶段，合理规划工控安全建设和安全投入;通过评估提高相关人员安全意识，以便落实国家及行业主管单位的人员安全培训及意识培养的要求。

（2） 管理网和生产网隔离

风险分析中已经分析了管理网和生产网互联互通所存在的风险。根据国际国内的各类工控安全相关标准以及行业内部于 2014 年下发的《烟草工业企业生产网与管理网网络互联安全规范》中，都对管理网和生产网互联安全问题进行了着重关注。

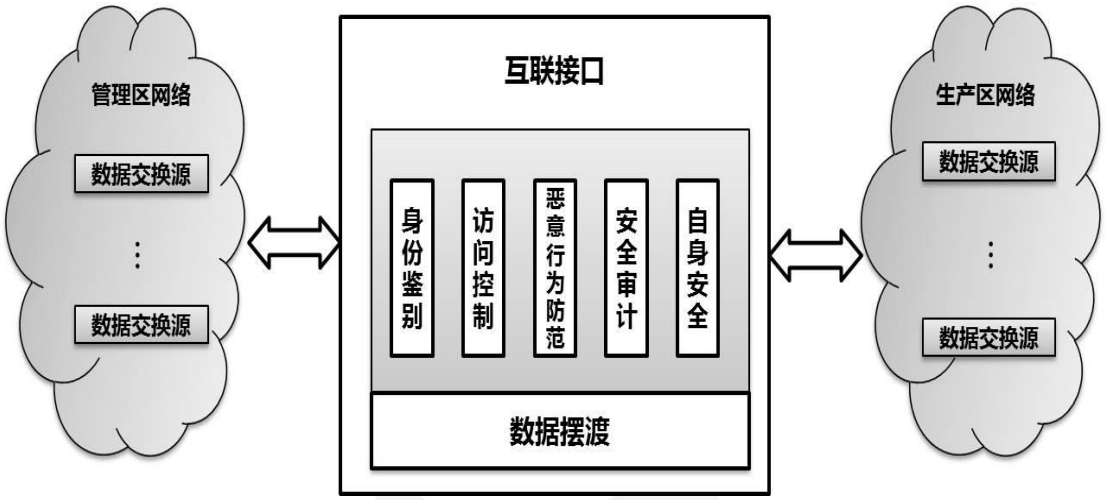

图 38 管理网与生产网安全隔离

针对这一问题，本解决方案在某烟厂各车间工业控制系统生产网和管理网边界都应该部署工业防火墙进行管理网和生产网的逻辑隔离，对两网间数据交换进行安全防护，确保生产网不会引入管理网所面临风险。

（3） 各车间内监测与防护

在管理网和生产网隔离中已经对生产执行层和各个车间生产网络进行了逻辑隔离，确保管理网风险不会引入各车间生产网。那么对于各车间内部的安全风险，应如何处理来确保各车间内部的安全性？在各车间内部，前面已经分析了主要包括以下几方面风险：1）各类操作站的安全风险；2）网络访问关系不明确；3）PLC 等工控设备安全风险； 4）通讯协议存在风险； 5）无线通信安全性不足。针对各方面风险采取对应的防护手段如下：

在操作员站、工程师站、HMI 等各类操作站部署安全系统对主机的进程、软件、流量、U 盘的使用等进行监控，防范主机非法访问网络其它节点；

部署工业异常监测系统，监测工控网络的相关业务异常和入侵行为，通过工控网络中的流量关系图形化展示梳理发现网络中的故障，出现异常及时报警；

部署工业漏洞扫描系统，发现各类操作系统、组态软件、以及工业交换机、PLC 等存在的漏洞，为车间内各类设备、软件提供完善的漏洞分析检测。

在 PLC 前端部署工业防火墙，对 PLC 进行防护。

在车间现场通过部署 WiFi 入侵检测设备，对烟草工业控制系统中的 AGV 小车等其他无线网络进行安全防护。

（4） 统一安全管理

对于管理人员，面对整个企业各个车间内繁多的各类工控网络设备、服务器、操作站以及安全设备，如何高效管理，掌握各个点的风险现状，对整个工控系统安全现状能够统一掌握，及时处理各类设备故障与威胁同样是工控安全建设至关重要的一环。

针对这一情况，通过在生产执行层部署工业控制信息安全管理系统，对烟草生产中各车间工控系统进行可用性、性能和服务水平的统一监控管理。包括各类主机、服务器、现场控制设备、以及各类网络设备、安全设备的配置及事件分析、审计、预警与响应，风险及态势的度量与评估，对整个系统面向业务进行主动化、智能化安全管理，保障烟草工业控制系统整体持续安全运营。

从管理人员的角度，对于丝叶生产系统整体安全状况以及系统中的操作站、服务器、PLC 以及安全设备的运行状态需要及时掌握。

防护方案设备部署情况如下图所示：

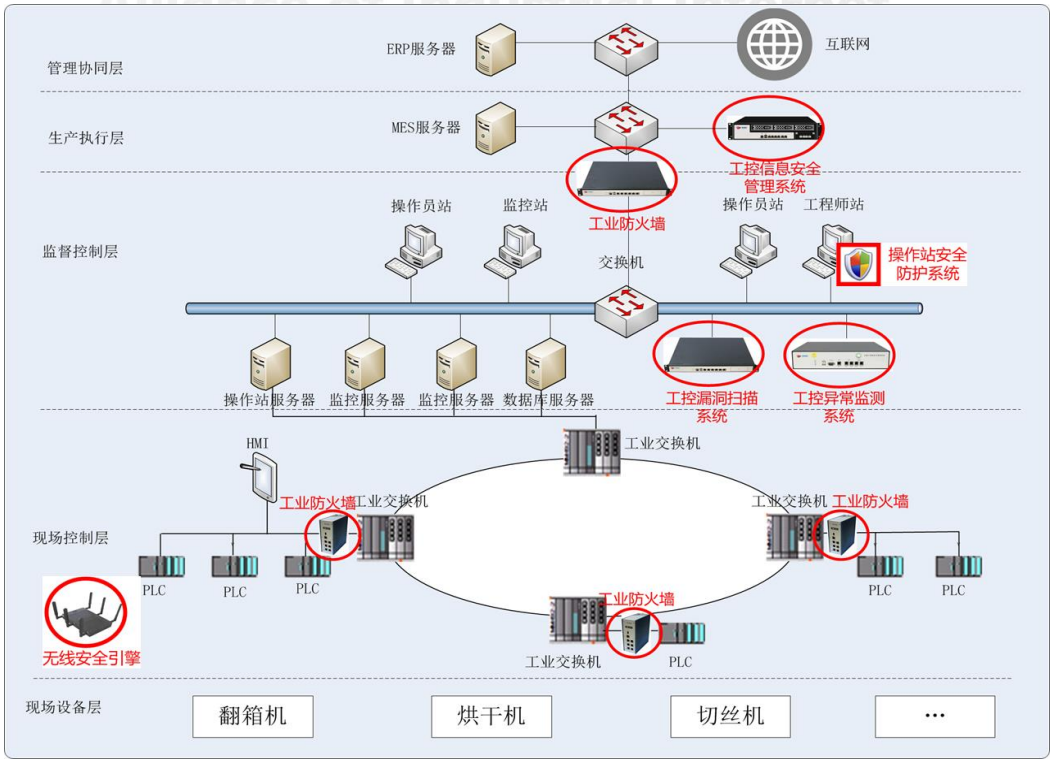

图 39 工控安全防护方案设备部署图

6.1.4 小结

某卷烟厂在本次工控安全建设项目中，通过全面风险评估可以切实让生产运维人员和管理人员清晰获悉自身工控网络中的风险，以便提前做到适度防护，提升了运维人员效率，为管理人员对安全的规划提供了有力的支撑；通过生产网和管理网隔离实现了对 MES 系统到制丝、卷包等车间的访问控制，阻断来自管理网的非法行为；经过多项安全防护措施后，能够有效的保障工控网中网络、主机应用等各层面的多数安全问题发生，降低公司生产业务中断的风险；通过统一安全管理平台建设对某卷烟厂中各车间工控系统进行安全性、可用性、性能和服务水平的统一监控管理减少可能潜在的风险隐患，减少信息系统故障、人员流失带来的经济损失。

6.2 案例二：某烟草企业安全解决方案

6.2.1 概述

随着烟草行业的蓬勃发展，企业信息化应用水平不断提高，绝大多数烟厂实现了企业计划层与车间执行层的双向信息流交互，通过信息集成、过程优化及资源优化，实现物流、信息流、价值流的集成和优化运行，很大程度上提高了企业敏捷性，随之而来的安全问题也逐步凸显，加强烟草各环节工业控制系统的安全防护显得尤为重要。

6.2.2 典型安全问题

（1） 办公网与生产网之间不同安全等级的用户存在越权访问的安全风险；

（2） 缺乏防范 DDOS 攻击、Flood 攻击的手段；

（3） 主机感染病毒造成网络性能严重下降，甚至网络通信中断等；

（4） 病毒在生产网边界和各个安全区域之间扩散。

6.2.3 解决方案

（1） 对各系统边界采取访问控制、病毒防护措施，保护操作指令免遭非法访问、窃取或篡改，保障工控网络的安全运行；

（2） 对烟草系统工控网络中重要服务器、操作员站、工程师站进行安全防护，杜绝软件肆意安装、U 盘滥用等行为；

（3） 对烟草工控网络信息流进行实时监测，记录各类异常操作和违规行为，做到事前部署，事中监控，事后追溯；

（4） 对工控网络中的安全设备进行集中统一管理，实现全局配置、集中监控、统一管理，提高管理人员的工作效率，降低人员投入成本。

6.2.4 部署方案

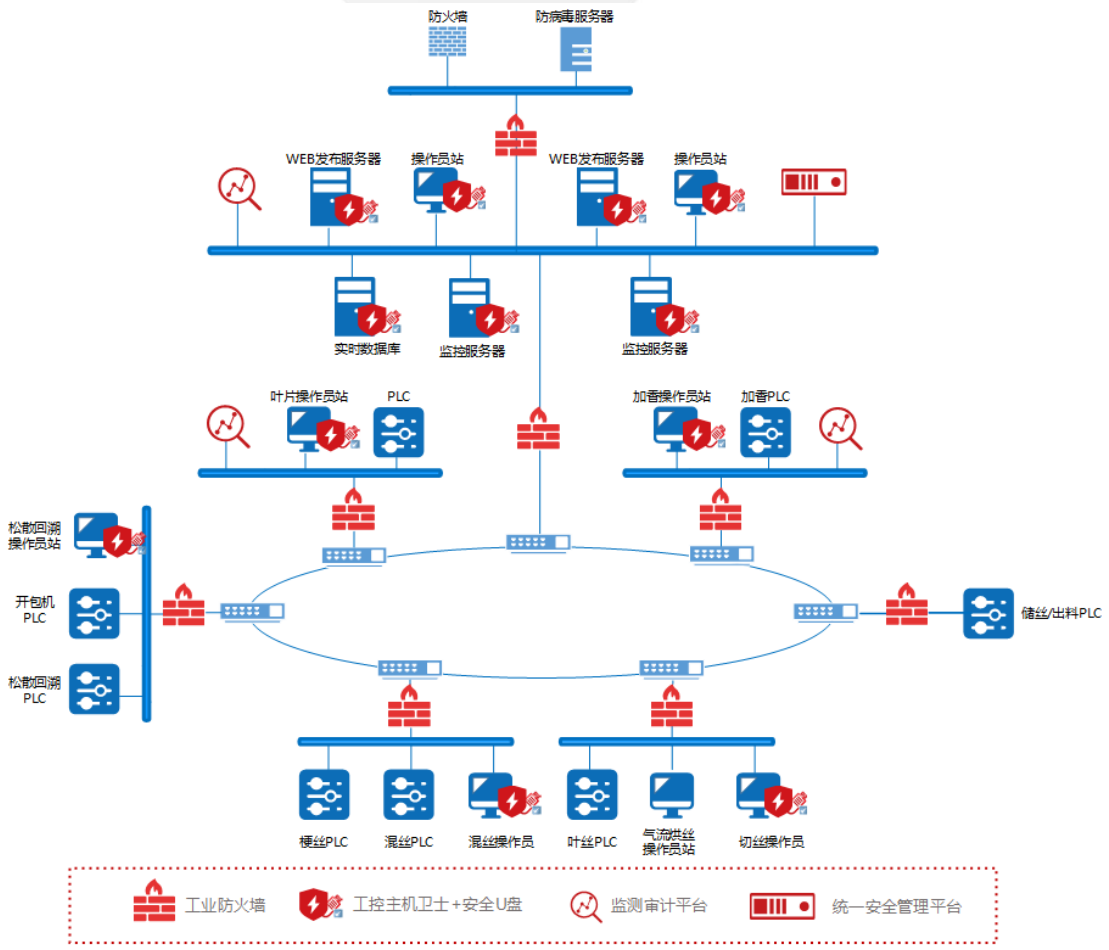

图 40 烟草企业工控安全拓扑图

（1） 边界、区域安全防护

通过在管理区与生产区边界、储丝区、掺配区、烘丝区、叶片区等各作业区的 PLC 前端部署工业防火墙，防范 DDOS 攻击和越权访问；

（2） 主机安全防护

在各操作站上部署工控主机卫士和安全 U 盘，防止除了与制丝相关业务系统外的非授权软件使用，实现整个制丝环节的安全可控；

（3） 网络监测与审计

在制丝各环节网络交换机上旁路部署监测审计平台，对工业网络的数据流量、网络会话、攻击威胁行为做全面的审计，便于事后追踪溯源；

（4） 集中管理

在以太网监控终端区域旁路部署统一安全管理，实现安全设备集中管理和各类日志的汇总分析。

6.2.5 小结

该解决方案具备如下特点：

（1） 满足国家能源局的合规性要求；

（2） 实现对各类已知及未知恶意代码的安全防范，保障工控网络安全；

（3） 对烟草工业网络实施安全域划分、逻辑隔离和访问控制，防范恶意攻击和病毒扩散，保障烟草生产正常运行。

7．工业控制系统安全测评技术方案

工业控制系统主要基于传感器、物联网、云计算、移动互联网等现代信息通信技术，实现对工业生产过程的精准控制和资源调度。从安全视角来看，工业控制系统不仅面临着传统的 ICT 安全风险，同时也面临着 PLC、DCS、SCADA 等工控环境的特定协议、规程的安全风险。结合《网络安全法》的要求，需要针对工控系统开展全面的例行安全测评，切实提高工控系统的安全等级。

本案例汇编包括两个安全测评领域的典型解决方案。

7.1 工业控制系统网络健壮性检测方案

7.1.1 概述

工业控制系统（ICS）是几种类型控制系统的总称，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其它控制系统（如可编程逻辑控制器（PLC））。工业控制系统广泛应用于核设施、电力、石化、化工、冶金、食品、市政、先进制造等国家关键基础设施的运行控制过程中，是国家关键基础设施的“中枢神经”。随着我国“两化融合”工作的不断深化，工业控制系统面临的内外部安全威胁日益严重，保障工业控制系统信息安全已经上升为国家层面的安全战略。

针对工业控制系统信息安全的问题，工控系统厂商、安全产品厂商、行业机构等信息安全干系方从不同的视角提出了一些安全解决方案，但这些解决方案大都是从“病了吃药”的角度提出的。从根源上，更要增加工控系统自身的免疫力和提升自身的抵抗力。

7.1.2 网络健壮性测试平台

阿基里斯认证是一项被用户、行业组织和供应商广泛认可和推荐的行业网络安全国际标准，西门子、施耐德、ABB 等公司的自动化产品均通过了阿基里斯认证的所有要求，使得阿基里斯认证成为事实上的行业标准。

阿基里斯测试平台（Achilles Test Platform，以下简称 ATP）是为工业设备提供网络健壮性测试而设计的平台，主要测试对象为可编程逻辑控制器（PLC）、分布式控制系统（DCS）控制器等，ATP 也可以测试任何有 Ethernet 端口和网络堆栈实现的设备，如服务器、HMI、工程师站、网络设备等。阿基里斯测试平台提供主动式先期预防的技术解决方案以提升网络可靠性和安全性，并可验证产品受到网络攻击时的耐受力，通过阿基里斯测试的产品，被证明已经达到通讯可靠性的最高标准要求，可以有效防范上万种“零日漏洞”以及其他未公开的漏洞或隐患。

7.1.3 工控系统健壮性检测方案

（1） 连接配置

在进行设备测试时阿基里斯测试平台支持两种组网方式，一种是直接测试工控设备，另一种是桥接到工控设备和上位机中间。

a) 直接测试工控设备

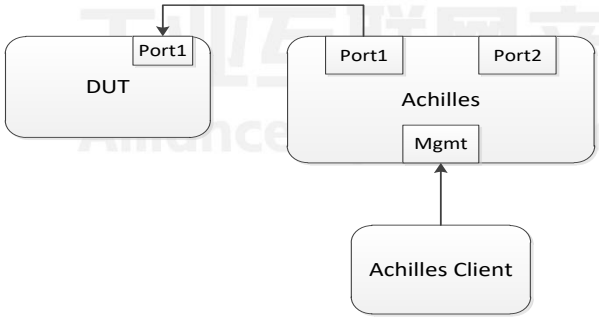

图 41 直连方式

b) 桥接到工控设备与上位机之间

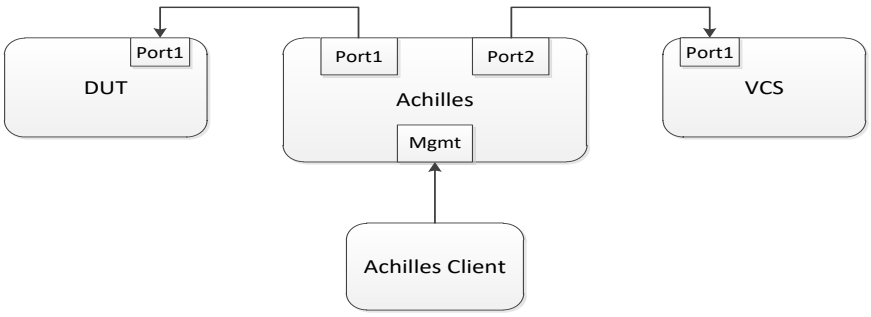

图 42 桥接方式

阿基里斯测试平台与被测设备（Device Under Test，以下简称 DUT）的连接如上图所示，针对不同的测试对象、测试要求，拓扑结构会作出某些调整，应以具体情况为准。

在 ATP 与 DUT 实现物理连接后，将对 ATP 配置界面进行具体配置。该操作主要是用来填写 ATP、DUT 的 IP 地址与 MAC 地址，以便实现两者的互联互通。并可以开启相应的监视器，以查看在通信过程中 DUT 的端口或者协议是否正常工作。

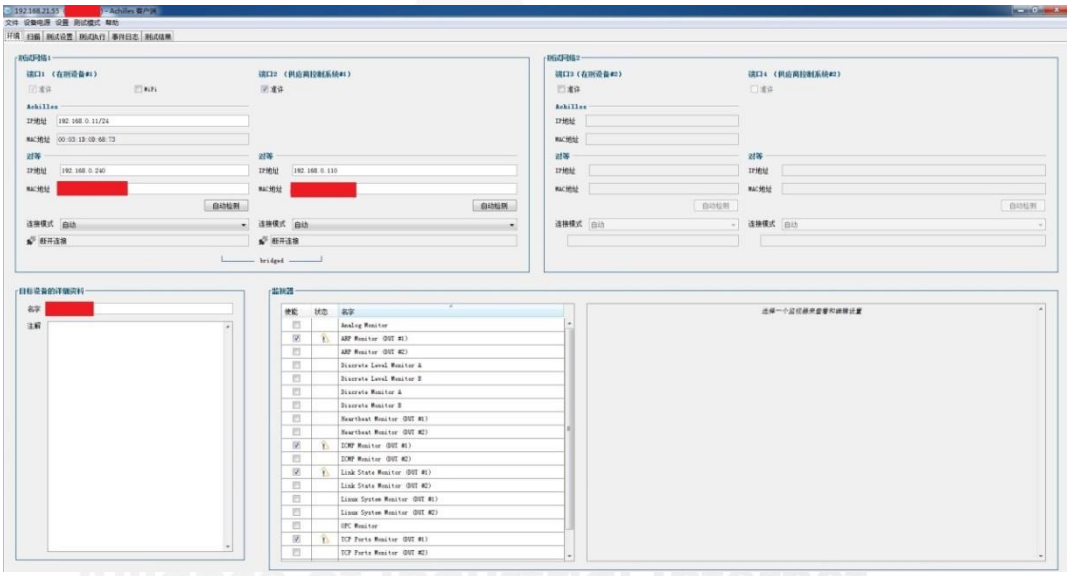

图 43　ATP 配置界面

配置完成后，需要对 DUT 进行端口扫描，为后期测试项的执行做好前期准备工作。端口扫描界面如下图所示：

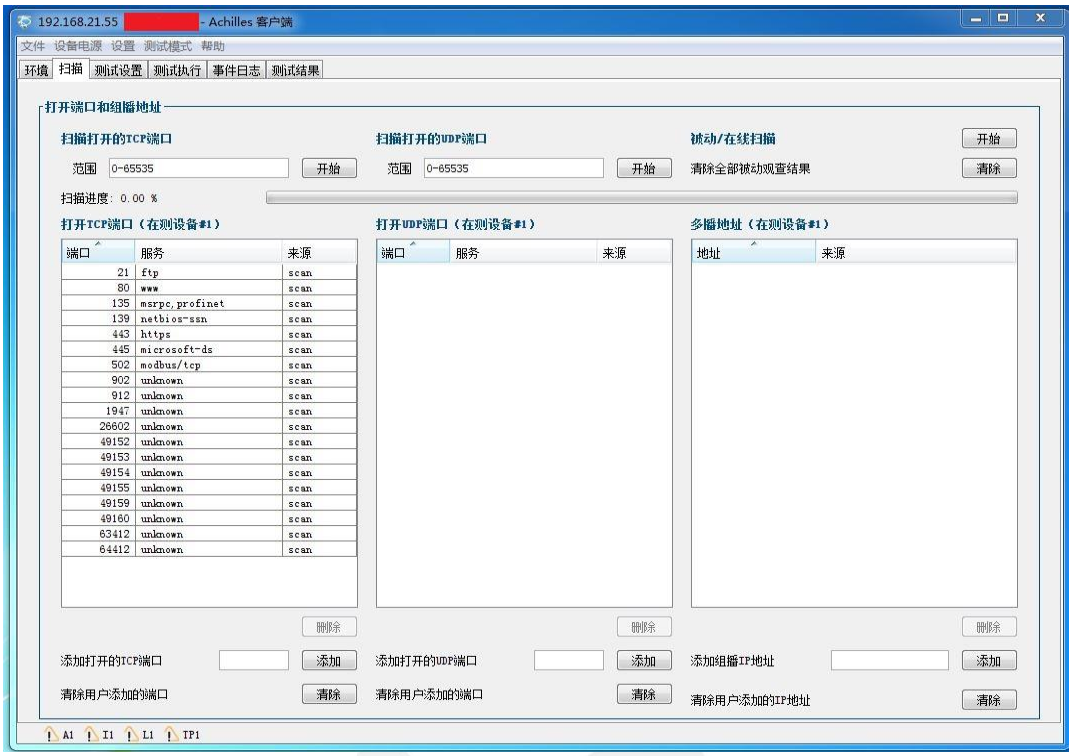

图 44　端口扫描界面

（2） 检测执行

ATP 与 DUT 实现连接以及配置和端口扫描等测试前准备工作后，开始具体的测试过程。阿基里斯测试主要分为两个等级：一级和二级，针对不同的检测级别，ATP 中包含不同的测试项，如以下两表格所示：

表 1　Level-1 测试项

协议类型	Level-1 测试项
Ethernet	Ethernet Unicast Storm (L1)
	Ethernet Multicast Storm (L1)
	Ethernet Broadcast Storm (L1)
	Ethernet Fuzzer (L1)
	Ethernet Grammar (L1)
ARP	ARP Request Storm (L1)
	ARP Host Reply Storm (L1)
	ARP Cache Saturation Storm (L1)
	ARP Grammar (L1)
IP	IP Unicast Storm (L1)
	IP Multicast Storm (L1)
	IP Broadcast Storm (L1)
	IP Fragmented Storm (L1)

	IP Fuzzer (L1)
	IP Grammar - Header Fields (L1)
	IP Grammar - Fragmentation (L1)
	IP Grammar - Options Fields (L1)
ICMP	ICMP Storm (L1)
	ICMP Grammar (L1)
	ICMP Type/Code Cross Product (L1)
TCP	TCP Scan Robustness (L1)
	TCP SYN Storm (L1)
	TCP/IP LAND Storm (L1)
	TCP Fuzzer (L1)
	TCP Grammar (L1)
UDP	UDP Scan Robustness (L1)
	UDP Unicast Storm (L1)
	UDP Multicast Storm (L1)
	UDP Broadcast Storm (L1)
	UDP Fuzzer (L1)
	UDP Grammar (L1)

表 2　Level-2 测试项

协议类型	Level-2 测试项
Ethernet	Ethernet Unicast Storm (L1/L2)
	Ethernet Multicast Storm (L1/L2)
	Ethernet Broadcast Storm (L1/L2)
	Ethernet Fuzzer (L1/L2)
	Ethernet Grammar (L1/L2)
	Ethernet VLAN Grammar(L2)
	Ethernet LLC/SNAP Grammar(L2)
	Ethernet VLAN/LLC/SNAP Chaining(L2)
	Ethernet Data Grammar(L2)
ARP	ARP Request Storm (L1/L2)
	ARP Host Reply Storm (L1/L2)
	ARP Cache Saturation Storm (L1/L2)
	ARP Grammar (L2)
IP	IP Unicast Storm (L1/L2)
	IP Multicast Storm (L1/L2)
	IP Broadcast Storm (L1/L2)
	IP Fragmented Storm (L1/L2)

	IP Bad Checksum Storm(L2)
	IP Fuzzer (L1/L2)
	IP Grammar - Header Fields (L1/L2)
	IP Grammar - Fragmentation (L1/L2)
	IP Grammar - Options Fields (L1/L2)
	IP Data Grammar(L2)
ICMP	ICMP Storm (L1/L2)
	ICMP Fuzzer(L2)
	ICMP Grammar (L2)
	ICMP Type/Code Cross Product (L1/L2)
TCP	TCP Scan Robustness (L1/L2)
	TCP SYN Storm (L1/L2)
	YCP SYN Storm from Broadcast(L2)
	TCP/IP LAND Storm (L1/L2)
	TCP URG Storm(L2)
	TCP FIN Strom(L2)
	TCP RST Storm(L2)
	TCP Closed Receive Window Storm(L2)
	TCP Segment Reassembly Storm(L2)
	TCP Fuzzer (L1/L2)
	TCP Grammar-Header Fields (L2)
	TCP Grammar-Contextually Invalid Packets(L2)
	TCP Priority Traffic Interleaving(L2)
	TCP Timestamp Manipulation(L2)
	TCP/IP Grammar (L2)
	TCP Selective Acknowledgement(L2)
	TCP Receive Window(L2)
	TCP Data Grammar(L2)
	TCP Maximum Concurrent Connections(L2)
	TCP Initial Sequence Number Randomness Check(L2)
UDP	UDP Scan Robustness (L1/L2)
	UDP Unicast Storm (L1/L2)
	UDP Multicast Storm (L1/L2)
	UDP Broadcast Storm (L1/L2)
	UDP Fuzzer (L1/L2)
	UDP Grammar (L2)
	UDP Data Grammar (L2)

通过测试设置，选择测试所需的 ATP 中不同测试项，作为测试执行的测试案例，在测试执行界面执行已选择的测试项，进行被测设备网络健壮性检测。如下图所示：

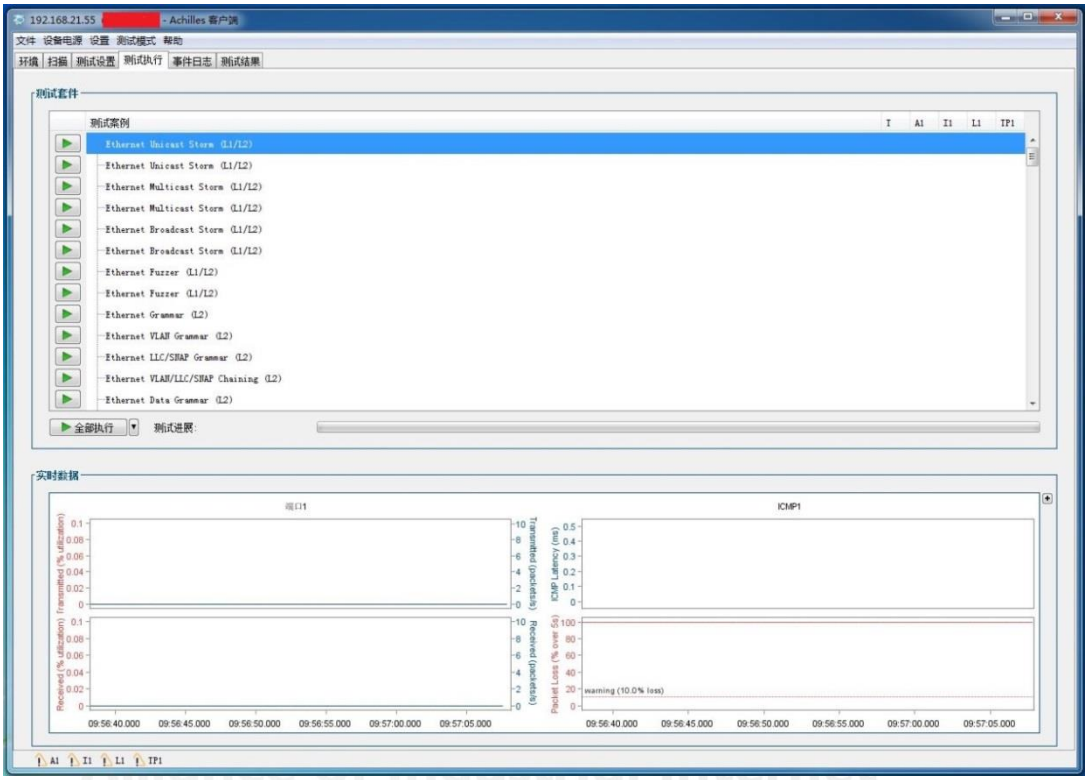

图 45　测试执行界面

测试过程中发现的问题会在事件日志中详细说明，用以指导测试产品厂商进行产品改进。在测试结果界面，保存的信息包括：测试结果、测试参数、测试环境信息、监视图表、事件日志、抓包分析或流量分析。最终，阿基里斯测试平台会针对测试过程生成 PDF 报告，通过分析测试数据，可以自动判断被测设备是否通过认证。

7.2.4 小结

基于上述工控安全健壮性测评思路，2016 年对国内某 LK 系列可编程控制器开展了阿基里斯认证工作，分别对基础 TCP/IP 协议栈、工业应用层总线开展了 Fuzzing 测试、风暴测试、资源耗尽型测试、错误数据型测试和完整性测试工作。经过近一个月的迭代测试，被测公司通过不断优化代码，攻克了恶意攻击、不完

整报文、广播风暴等多种情景下，控制器底层控制总线仍可保持正常运行的技术难关，最终通过认证，并于 2017 年 3 月 1 日获得 Achilles Level I 认证证书，成为国内首家获得该认证的大型 PLC 供应商。

7.2 工业控制系统等级保护测评方案

7.2.1 案例概述

《网络安全法》自 2017 年 6 月 1 日起正式施行，其中第三十一条规定如下：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

工业控制系统（Industrial control system，以下简称 ICS）在能源、交通、水利等关键信息基础设施中普遍应用，应对各行业工业控制系统执行网络安全等级保护制度并实行重点信息安全保护。

7.2.2 工控系统等保工作现状

近两年来，国家为掌握关键信息基础设施的 ICS 信息安全态势，国家网信部门、公安部门和其它机关、行业主管单位组织了多次专项安全检查，通过此种方式可有效的督促 ICS 运营者落实网络安全相关工作。

国家陆续出台或修订了与 ICS 信息安全相关的政策、法律法规、技术标准，如：2016 年《工业自动化和控制系统网络安全 集散控制系统(DCS)第 2 部分：管理要求》正式发布、2016 年 11 月工信部正式发布《工业控制系统信息安全防护指南》、2017 年 6 月 1 日将正式实施《网络安全法》等。

由于 ICS 应用的行业的特殊性以及针对 ICS 的信息安全产品体系尚不成熟等原因，目前部分 ICS 运营者更倾向于 ICS 控制系统厂商提供适用于其系统与工程的安全解决方案，诸如艾默生、ABB、施耐德、和利时等厂商也推出了自主设计的信息安全解决方案。

7.2.3 工控系统等保测评工作实践方案

工业控制系统的信息安全等级保护工作的工作思路是：以等级保护测评过程管理指南为基础，以《信息系统安全等级保护基本要求》为核心，以具体测评对象所属行业的信息安全要求为重点，结合已有对工业控制系统信息安全的研究成果，对具体的服务范围、测评方法、过程均进行了针对性的设计。以下以电力行业某发电厂的 DCS（分布式控制系统）等级保护测评服务为分析对象来进行说明。

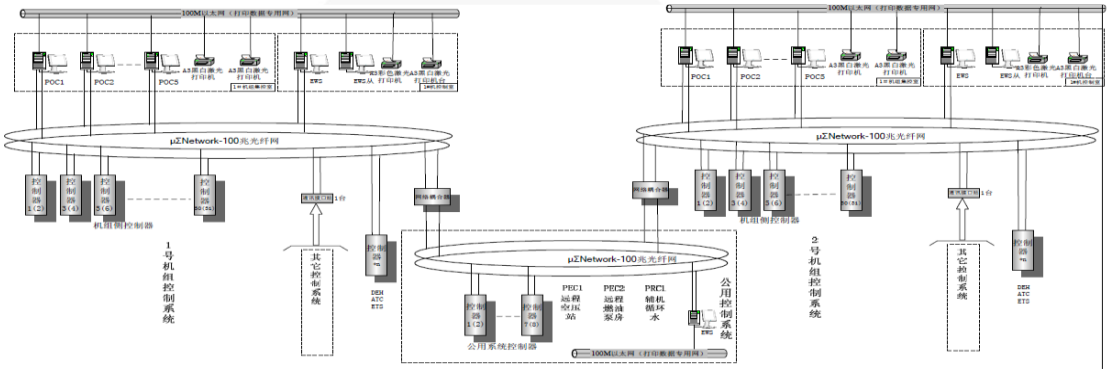

图 46　DCS 系统结构图

此厂的 DCS 系统#1、#2 机组分别配备 6 台操作员站，1 台历史站，1 台工程师站，1 台通讯站，一台激光彩色打印机。同时#0 机组为公用控制系统，包括了远程空压站、远程燃油泵房、辅机循环水等的具体控制。DCS 系统及生产区域系统（如 NCS、TL、FW 等）的数据通过网络单向隔离器与 SIS 系统连接。

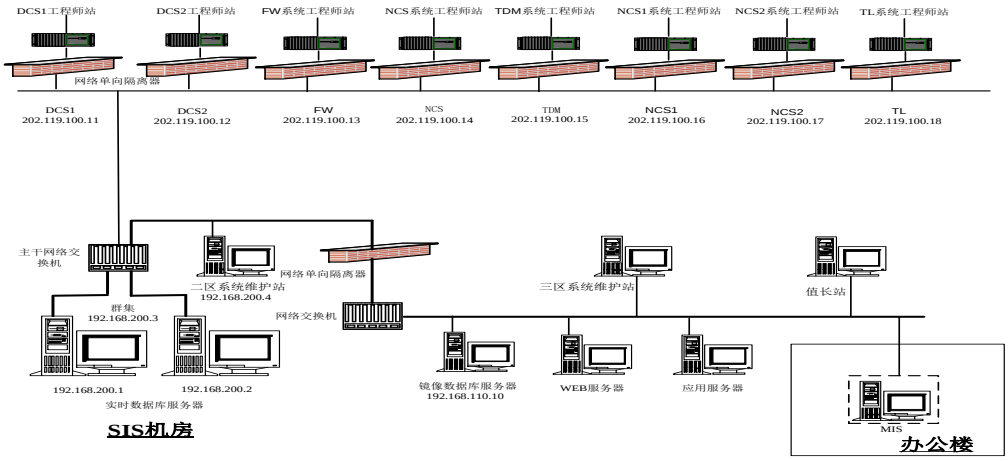

图 47　SIS 系统网络拓扑图

（3） 测评内容的变化

针对电厂的 DCS 系统（三级）信息安全等保测评工作时，在项目准备阶段，对本项目的内容进行了分析，将进行两方面工作：等级保护测评与生产控制区信息安全风险评估。其中，等级保护测评针对 DCS 系统进行符合性测评，风险评估为用户提供生产控制区整体安全风险量化评估工作以便客户更加直观的了解到生产控制区域内存在的信息安全风险及进行相关整改规划。

c)　等级保护测评

本项目的测评对象为电厂生产控制 I 区内的 DCS 系统，该 DCS 系统依据《信息系统安全保护等级定级指南》、《电力行业信息系统等级保护定级工作指导意见》定为三级信息系统，在进行等级保护测评时，应依据《信息系统安全等级保护基本要求》的三级系统基本要求与《电力行业信息系统安全等级保护基本要求》中对应等级相关新增、增强要求指导测评工作。

依据上述标准、规范要求，编制《某电厂 DCS 系统信息安全等级保护测评作业指导书》来具体指导测评工作。

d)　生产控制区信息安全风险评估

针对工业控制系统应用领域存在信息安全基础差、信息安全风险高的普遍状况，在实施工业控制系统类信息安全等级测评项目时，也为用户提供厂级信息系统或生产大区的信息系统风险评估服务。

上述某电厂 DCS 系统的等级测评过程中，项目团队依据《信息安全技术 信息安全风险评估规范》（GB/T 20984—2007）、《电力监控系统安全防护评估方案 》（国能安全〔2015〕36 号附件 7）对该电厂生产控制区的系统进行了风险评估。

（4） 测评过程的变化

上述某电厂 DCS 系统的等级测评过程遵循《信息系统安全等级保护测评过程指南》(GB/28449-2012) 中的相关要求，同时结合工控系统进行了相关的补充与改进，具体测评过程流程图如下图所示：

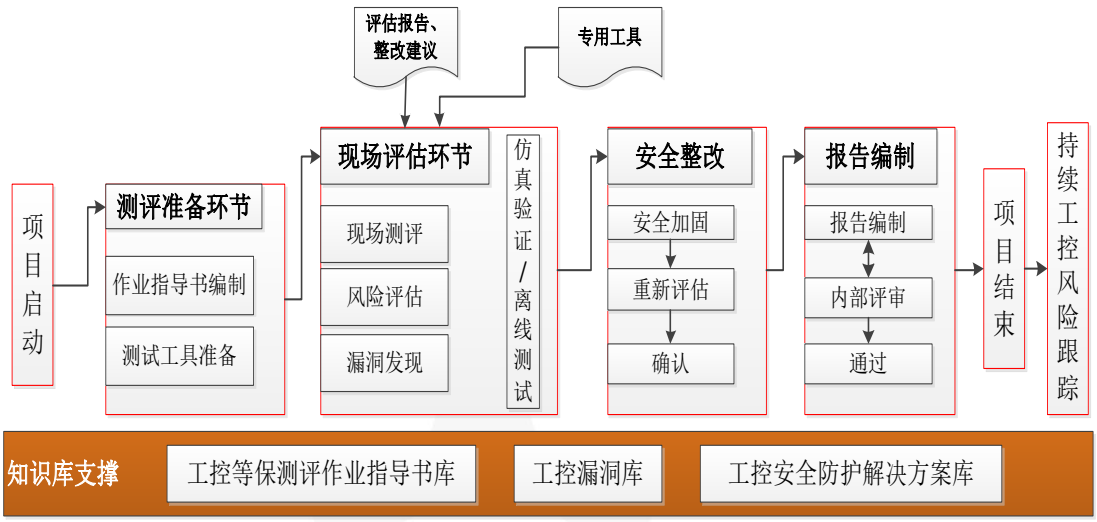

图 48 测评过程流程图

（5） 测评工具的使用

在目前对工业生产控制系统的等级保护测评中，针对三级及三级以上的系统一般不采取工具测试（漏洞扫描与渗透测试）。建议在条件许可的情况下，应对三级及三级以上的系统采用专项的工具测试，而不能因避免风险而盲目放弃工具测试。已投入运行的工业控制系统大都存在主机操作系统老旧、应用软件信息安全设计缺失等问题，工具测试更具有必要性，在工具测试阶段一般遵循如下原则：

a) 工具的选用

基于业界多种检测测评工具，不仅包括信息安全等级保护工具箱，也包括专用于设备健壮性检测的国际、国内认证工具。在对工控系统进行等级保护信息安全测评的过程中，针对客户的具体需求以及被测对象的特点合理选用工具执行工具测试。

b) 测试原则及方法选择

工具测试的基本原则是不影响被测对象的正常业务使用，特别是对工业控制系统而言，业务的连续性更为重要，同时针对被测对象的所有计算机终端选取不低于 70%比例进行工具测试，必须涵盖所有主机类型（工程师站、历史站、操作员站、服务器）。在上述某电厂 DCS 系统的测评过程中，项目组采用了专用的测评工具箱，在其两机组停机检修期间进行了#1 号机组的全网工具检测及对所有的工程师站、操作员站进行了漏洞扫描；对#0 号机组、#2 号机组的工程师站、操作员站进行了离线式的工具扫描。

c) 测试对象

在工具测试对象的选择上，由于工业控制系统的特殊性，要遵循如下条件：

对于部分被测系统，若有 1:1 建设的仿真验证环境（如核电、轨道交通行业的工控系统大都有与现场完全一致的验证环境），可在仿真验证环境下进行工具测试。

主机类设备应包含至少全部终端的 70%以上，保证测试的覆盖面。

在选取测试对象时，对于控制类设备或智能设备，在与客户达成一致意见时，可采用专用设备进行专项测试。

目前很多已投运的工业控制系统并没有使用关系型数据库，上位机软件缺少信息安全功能设计。在测试对象选取的过程中，针对软件平台等在使用工具测试的基础上加强手工检查与验证。

7.2.4 小结

通过专业化工业控制系统信息安全服务队伍，研发典型工业控制系统研究基础平台，提供面向工业控制系统的包括软件测评、设备安全认证、系统风险评估、信息安全等级保护测评等服务。

等保安全测评实践，以解决工业控制系统用户的切实信息安全问题为目标，落实“整体规划、按类部署、分步实施、跟踪风险”的信息安全建设整改思路，研究工控信息安全技术及提升工控信息安全服务项目的实施方法。

8. 结束语

工业控制系统在我国的电力、水利、污水处理、石油化工、冶金、汽车制造、交通运输、航空航天等诸多现代化工/农业领域有着广泛的应用，其中超过 80%的涉及国计民生的关键基础设施与工业控制系统有关，都依靠工业控制系统来实现调度自动化和作业自动化。

然而随着信息技术和网络技术的飞速发展，网络安全的边界早已超越了地域限制，甚至连网络边界也已经模糊，导致网络信息安全事件层出不穷，面对日益严重的安全威胁形势，我国应积极加强对工业控制系统的安全体系化研究，从安全规划、安全防护、安全运营、安全测评、应急保障等各方面，提出针对性安全解决方案方案，并积极进行技术试点，探究技术可行性，逐步形成可推广、可复制的最佳实践，切实提升我国工业互联网安全技术水平。