# 工业互联网
# 典型安全解决方案案例汇编

## （2020）

工业互联网产业联盟
Alliance of Industrial Internet

工业互联网产业联盟（AII）
2021 年 11 月

工业互联网产业联盟
Alliance of Industrial Internet

# 目　录

1. 工业互联网安全概述 ..... 1
1.1 工业互联网安全形势 ..... 3
1.2 工业互联网安全挑战 ..... 6
2. 典型安全解决方案 ..... 9
2.1 案例一：某炼化生产企业生产环境安全解决方案 ..... 9
2.1.1 方案概述 ..... 9
2.1.2 典型安全问题 ..... 9
2.1.3 安全解决方案 ..... 13
2.1.4 小结 ..... 21
2.1.5 单位基本信息 ..... 21
2.2 案例二：卡奥斯工业互联网平台安全解决方案 ..... 22
2.2.1 方案概述 ..... 22
2.2.2 典型安全问题 ..... 23
2.2.3 安全解决方案 ..... 25
2.2.4 小结 ..... 39
2.2.5 单位基本信息 ..... 43
2.3 案例三：化纤行业工控安全解决方案 ..... 44
2.3.1 方案概述 ..... 44
2.3.2 典型安全问题 ..... 45

工业互联网产业联盟
Alliance of Industrial Internet

2.3.3 安全解决方案 ..... 46
2.3.4 小结 ..... 57
2.3.5 单位基本信息 ..... 59
2.4 案例四：鲁布革水电厂工业互联网电力监控系统综合安全防护解决方案 ..... 60
2.4.1 方案概述 ..... 60
2.4.2 典型安全问题 ..... 61
2.4.3 安全解决方案 ..... 63
2.4.4 小结 ..... 70
2.4.5 单位基本信息 ..... 70
2.5 案例五：智慧矿山工业互联网安全纵深防御体系建设 ..... 71
2.5.1 方案概述 ..... 71
2.5.2 典型安全问题 ..... 72
2.5.3 安全解决方案 ..... 73
2.5.4 小结 ..... 80
2.5.5 单位基本信息 ..... 80
2.6 案例六：智慧水务典型安全解决方案 ..... 80
2.6.1 方案概述 ..... 80
2.6.2 典型安全问题 ..... 81
2.6.3 安全解决方案 ..... 83
2.6.4 小结 ..... 91

工业互联网产业联盟
Alliance of Industrial Internet

2.6.5 单位基本信息 ..... 91
2.7 案例七：工业 5G 边缘计算平台安全解决方案 ..... 92
2.7.1 方案概述 ..... 92
2.7.2 典型安全问题 ..... 92
2.7.3 安全解决方案 ..... 94
2.7.4 小结 ..... 100
2.7.5 单位基本信息 ..... 100
2.8 案例八：大型排水集团生产控制系统安全解决方案 ..... 101
2.8.1 方案概述 ..... 101
2.8.2 典型安全问题 ..... 102
2.8.3 安全解决方案 ..... 103
2.8.4 小结 ..... 113
2.8.5 单位基本信息 ..... 114
2.9 案例九：5G+智慧轨道交通安全解决方案 ..... 115
2.9.1 方案概述 ..... 115
2.9.2 典型安全问题 ..... 119
2.9.3 安全解决方案 ..... 122
2.9.4 小结 ..... 132
2.9.5 单位基本信息 ..... 133
2.10 案例十：某 5G+智慧轨道交通安全解决方案 ..... 134
2.10.1 方案概述 ..... 134

工业互联网产业联盟
Alliance of Industrial Internet

2.10.2 典型安全问题 ..... 136
2.10.3 安全解决方案 ..... 136
2.10.4 小结 ..... 143
2.10.5 单位基本信息 ..... 143
2.11 案例十一：青岛海尔 5G 智慧工厂安全防护应用案例 ..... 145
2.11.1 方案概述 ..... 145
2.11.2 典型安全问题 ..... 146
2.11.3 安全解决方案 ..... 147
2.11.4 小结 ..... 153
2.11.5 单位基本信息 ..... 154
2.12 案例十二：面向钢铁行业一体化平台安全解决方案 ..... 155
2.12.1 方案概述 ..... 155
2.12.2 典型安全问题 ..... 157
2.12.3 安全解决方案 ..... 159
2.12.4 小结 ..... 174
2.12.5 单位基本信息 ..... 175
3. 结束语 ..... 177

工业互联网产业联盟
Alliance of Industrial Internet

# 前　言

工业互联网作为“新基建”的七大领域之一，其重要性上升到一个新的高度。工业互联网的投资和建设将加快我国智能制造步伐，激发新型消费和投资、促进就业创业、解放生产力、打造经济发展新动能，对人们生产生活带来重大而深远的影响。2020年12月，工业互联网专项工作组印发《工业互联网创新发展行动计划（2021-2023年）》，明确了以落实企业主体责任为导向、以加强安全供给为重点、以培育安全产业为支撑、以强化技术监测服务能力为抓手的工作思路，力争建立起制度更加健全、技术更加先进、政企更加协同安全保障体系。

目前，工业互联网安全仍然面临很多新挑战和问题亟待解决，5G、边缘计算、大数据、人工智能等新技术与工业互联网技术的融合为工业互联网安全带来新的挑战，使传统工业控制系统和自我防护能力差的设备连接到互联网，打破了传统工业网络相对封闭、值得信赖的环境，使得大规模工业控制系统和生产系统成了网络攻击的重点目标。

为使广大工业互联网从业者能了解工业互联网安全的发展情况，工业互联网产业联盟安全组启动编写了《工业互联网典型安全解决方案案例汇编（2020）》，报告汇编了业内优秀的安全解决方案，希望为解决工业互联网安全的新挑战和突出问题提供有益参考，共同促进工业互联网安全工作的建设。

本报告是在工业和信息化部网络安全管理局指导和支持下，由中国移动通信集团有限公司牵头编制，工业互联网产业联盟安全组多家企业参加编写完成。主要参与单位有：中国信息通信研究院、东软集团股份有限公司、青岛海尔工业智能研究院有限公司、北京双湃智安科技有限公司、江苏亨通信息安全技术有限公司、江苏亨通工控安全研究院有限公司、北京神州绿盟科技有限公司、奇安信科技集团股份有限公司、北京启明星辰信息安全技术有限公司、中国联合网络通信有限公司南京市分公司、南京地铁集团有限公司、江苏启明星辰信息安全技术有限公司、中兴通讯股份有限公司、南京中新赛克科技有限责任公司、江苏省互联网行业管理服务中心、南京钢铁有限公司。

本报告的参编人：张峰、田慧蓉、陶耀东、柯皓仁、李江力、于乐、刘晓曼、张弘扬、付俊、苏海洋、谷久宏、刘海洋、申枭、刘小兰、王菁、王敏、沈海峰、范春朝、向海洲、辛毅、林云云、周荣。

工业互联网产业联盟
Alliance of Industrial Internet

工业互联网产业联盟 安全组

二〇二一年三月

# 1. 工业互联网安全概述

## 1.1 工业互联网安全形势

随着我国工业互联网的蓬勃发展，工业互联网已成为中国制造企业转型升级的必然选择，也是我国数字经济发展的重要组成部分。这都离不开国家对于工业互联网建设的大力推动和支持，2021 年政府工作报告中指出“发展工业互联网，搭建更多共性技术研发平台，提升中小微企业创新能力和专业化水平”，这是“工业互联网”第三次被写入政府工作报告，足以体现我国对工业互联网的重视。

自《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》将安全保障与网络、平台建设列为工业互联网三大体系之后，各上级单位高度重视工业互联网安全，相继发布了一系列工业互联网安全方面的指导意见和要求。

2019 年 7 月，工信部等十部门印发的《工业互联网安全工作的指导意见》中，指导企业建立监督检查、信息共享和通报、应急处置等工业互联网安全管理制度，构建企业安全主体责任制，探索构建工业互联网安全评估体系。2019 年 9 月，工业和信息化部发布《省级工业互联网安全监测与态势感知平台建设指南》，指导各地工业和信息化主管部门、地方通信管理局建设专业化安全监测和预警通报技术手段。

2020 年 3 月，工信部发布了《工业和信息化部办公厅关于推动工业互联网加快发展的通知》，明确提出加快新型基础设施建设、加快拓展融合创新应用、加快健全安全保障体系、加快壮

大创新发展动能、加快完善产业生态布局、加大政策支持力度等6个方面20项具体举措。2020年5月，工信部发布《工业和信息化部关于工业大数据发展的指导意见》要求强化数据安全，构建工业数据安全管理体系；加强工业数据安全产品研发。2020年12月，工业互联网专项工作组印发《工业互联网创新发展行动计划（2021-2023年）》，明确了以落实企业主体责任为导向、以加强安全供给为重点、以培育安全产业为支撑、以强化技术监测服务能力为抓手的工作思路，力争切实建立起制度更加健全、技术更加先进、政企更加协同的安全保障体系。安全部分主要包括四方面内容：一是落实企业主体责任，实施分类分级管理；二是强化产业协同，推进供给侧加快创新；三是加强示范引领，促进安全产业发展壮大；四是坚持专项带动，提升安全技术监测服务能力。

2021年1月，工信部印发《开展工业互联网企业网络安全分类分级管理试点工作的通知》，启动部署分类分级试点工作。实施工业互联网企业网络安全分类分级管理制度，要着力打造“1+4”的制度体系。“1”是《工业互联网企业网络安全分类分级管理指南》（简称《管理指南》）明确将工业互联网企业分为联网工业企业、平台企业、标识解析企业三类，结合企业所属行业的重要性、企业规模、应用工业互联网程度、网络安全风险程度等因素，将企业分成三个级别，同时明确定级流程和安全管理、支持保障等方面的要求。“4”是《工业互联网企业网络安全分类分级防护规范》（简称《安全规范》），针对联网工业企业、

平台企业、标识解析企业以及工业互联网数据四类对象，分别明确防护要点和不同级别的网络安全防护要求。结合各地工业互联网发展实际，目前选定上海、江苏、广东等 15 个省（区、市）232 家重点工业行业的重点企业参与试点。通过试点进一步完善《管理指南》，提升《安全规范》的科学性、有效性和指导性，形成可复制可推广的安全管理模式。

2021 年 3 月，工信部刘烈宏副部长在工业互联网企业座谈会上讲话并指出：一是加强基础设施建设。推进内、外网建设改造和标识解析规模化应用。深化“5G+工业互联网”融合发展。加快专业型平台、特色型平台、跨行业跨领域平台建设。二是持续深化融合应用。将工业互联网技术、模式等与各行业的生产实践、行业特性、知识经验紧密结合，打造一批融合应用典型案例，带动形成系统性推广模式。三是夯实产业发展根基。要聚焦核心技术和能力短板，继续组织实施创新发展工程，加强技术攻关和关键产品研发，助力工业补齐短板、锻造长板。四是培育壮大产业生态。积极协调各方资源和力量，推动形成主体多元、协同创新的产业生态，打好“团体赛”。鼓励地方结合当地实际，探索各具特色发展模式。五是提升安全保障水平。坚持发展与安全并重，落实好主体责任，完善网络安全分类分级管理制度建设，加大网络安全投入力度，加强网络安全技术监测。

2021 年 3 月 8 日，工信部肖亚庆部长在两会“部长通道”上讲话并指出：第一，要打好基础。在原有基础上，未来几年要把工业互联网发展的基础打好。未来几年工业互联网的发展仍然

是一个非常关键的时期。第二，要在融合上下功夫。就是保障工业互联网在发展过程中，将各个行业、各个企业、各个层级相互融合，通过工业互联网产生更多的创新应用，使它为经济发展起到助力和促进作用。第三，工业互联网发展过程中，我们还要把发展和安全平衡好。工业互联网发展，大家也担心安全问题，也关心知识产权保护。我们一手坚定不移抓发展，一手坚定不移保证安全、保护知识产权，把两者结合好，促进工业互联网健康有序发展。工业互联网的发展，未来的前景是非常好的，我们现在有很多应用的场景，在各地已经展现出来了。下一步，随着“5G+工业互联网”的发展，将产生更多的实际应用场景，这些发展会给大家呈现更多的好应用，为满足人民日益增长的美好生活需要，也为我们经济发展，提供更多的载体、平台和融合的空间。

### 1.2 工业互联网安全挑战

工业互联网涉及的各个层面、环节都可能面临安全风险。在工业互联网安全工作深入推进过程中，一系列新兴和固有的安全问题亟待解决。

#### （1）万物互联的信任体系问题

进入工业互联网时代，人机物要逐步“上网”，“上网”以后如何认证、确保海量设备的安全接入成为实现万物互联的信任问题。同时，企业与企业之间、行业与行业之间要解决跨区域、跨行业的交叉互信问题。

#### （2）新技术融合带来新风险

工业互联网技术与 5G、边缘计算等新技术的融合以及第三

方协作服务的深度介入增加了信息泄露、数据窃取的风险。5G 协议的全面互联网化，被外部攻击的可能性显著增加。边缘计算对工业互联网数据就近处理减少了敏感数据泄露的风险，但安全防护能力不及云中心，对原有的集中式内容监管模式带来挑战。

**（3）工业数据泄露风险加剧**

5G 边缘计算中心通过 API 接口开放给第三方应用，让工业互联网数据在不同应用间共享，这大大增加数据传输和存储的安全风险。由于数据打通导致风险加剧、数据庞杂导致难度加大，而工业数据安全关系着国家安全。工业互联网协同制造倡导的个性化定制、服务化转型都涉及大量用户隐私，用户隐私极易被泄露。关键工业数据成为国家关键数据资源，一旦被窃取将直接威胁国家安全。

**（4）暴露面持续增大**

工业互联网打破了传统网络安全界限。随着 5G+工业互联网、工业上云等工作的推进，工业企业 IT 和 OT 不断融合，企业内部工业网络、管理网络与互联网逐步打通，网络日益开放，大量工业互联网设备暴露在互联网上且不断增多，导致大量网络安全威胁从外网向工业内网延伸渗透。暴露在互联网的工业互联网设备长期遭受恶意嗅探。

**（5）漏洞病毒依旧突出**

由于工业互联网设备软件更新缓慢、用户及厂商通常无法及时发现或修复漏洞，导致设备漏洞较多。同时，设备漏洞易被攻击者利用来构建完整攻击链路，并获取更高权限，甚至制造病毒

长期危害工业互联网安全。近几年全球水电、核电、制造等重要行业的企业遭受病毒攻击和感染的事件众多，造成了大范围停电、生产线停摆等重大影响。2020 年上半年我国联网工控设备累计发现 946 个漏洞隐患，中高危漏洞占比高达 91%。

**（6）APT 攻击危害大**

APT 针对性强、破坏性大，威胁工业活动。工业互联网直接关系到生产和经济活动，成为了 APT 攻击的重点目标。

**（7）重点行业监控和管理系统存高危隐患**

大多数传统工业控制系统和设备更关注系统的实时性与业务的连续性，而网络安全防护能力不足。重点行业如能源、金融、物流、智能制造等，其大型工业云平台和系统持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击。仅水电行业和医疗健康行业，暴露在互联网上的系统中存在高危漏洞隐患的占比分别为 25%和 72%，部分遭受境外恶意嗅探。

工业互联网产业联盟
Alliance of Industrial Internet

# 2. 典型安全解决方案

## 2.1 案例一：某炼化生产企业生产环境安全解决方案

### 2.1.1 方案概述

某炼化生产公司在业务向数字化转型的过程中，初步形成了生产执行层、操作控制层、管理决策层三层一体的信息化架构体系。随着信息系统与生产系统不断的融合，整个生产环境的网络安全建设就十分重要。该公司已经先后建成投入各类应用系统140余套，经过现场调研评估，我们发现用户的网络存在缺少有效隔离、安全加固、审计监控、终端防护、运维审计和安全管理等六类安全问题。参照分层分区、集中管理和技管结合这三点建设思路，根据现场网络业务系统情况，从终端、网络、平台等维度部署安全设备，为安全管理提供数据和响应支持，最终保护其生产网络环境的平稳运行。本方案能够提供多层次的安全管理，能够实现事前可检测与事后可溯源的全方位立体式的审计功能，很好的提升了用户生产环境的网络安全技术能力。在重视技术手段进行安全防护的同时，我们帮助客户建立起了安全管理体系，为用户提供了更全面的网络安全保障。

### 2.1.2 典型安全问题

随着工业领域的不断发展，各国抛出了各自的全新发展理念，如德国的工业4.0，美国的先进制造和中国的“中国智造”“两化融合”等。工信部印发的《工业互联网创新发展行动计划（2021-2023年）》将推动信息技术（IT）网络与生产控制（OT）网络融合作为重点行动内容之一。各国都不约而同的在强调工业

控制网络与外部管理信息网络的融合，以便更精准的控制工业系统，提高生产效率。

在某公司炼化生产工作不断提升的同时，其信息化建设也在同步进行，符合国家 IT 与 OT 网络融合的总体行动方针。公司先后建成投入各类应用系统 140 余套，初步形成了生产执行层、操作控制层、管理决策层三层一体的信息化架构体系。其目前有 DCS 系统 19 余套，主要装置都采用了 DCS 系统，主要厂商有 YOKOGAWA，HONEYWELL 和浙江中控等。随着该公司的业务生产向数字化转型的过程中，为了实现感知式管理生产过程，整个生产环境的网络安全建设就十分重要。该公司生产环境原有拓扑示意图如图所示。

工业互联网产业联盟
Alliance of Industrial Internet

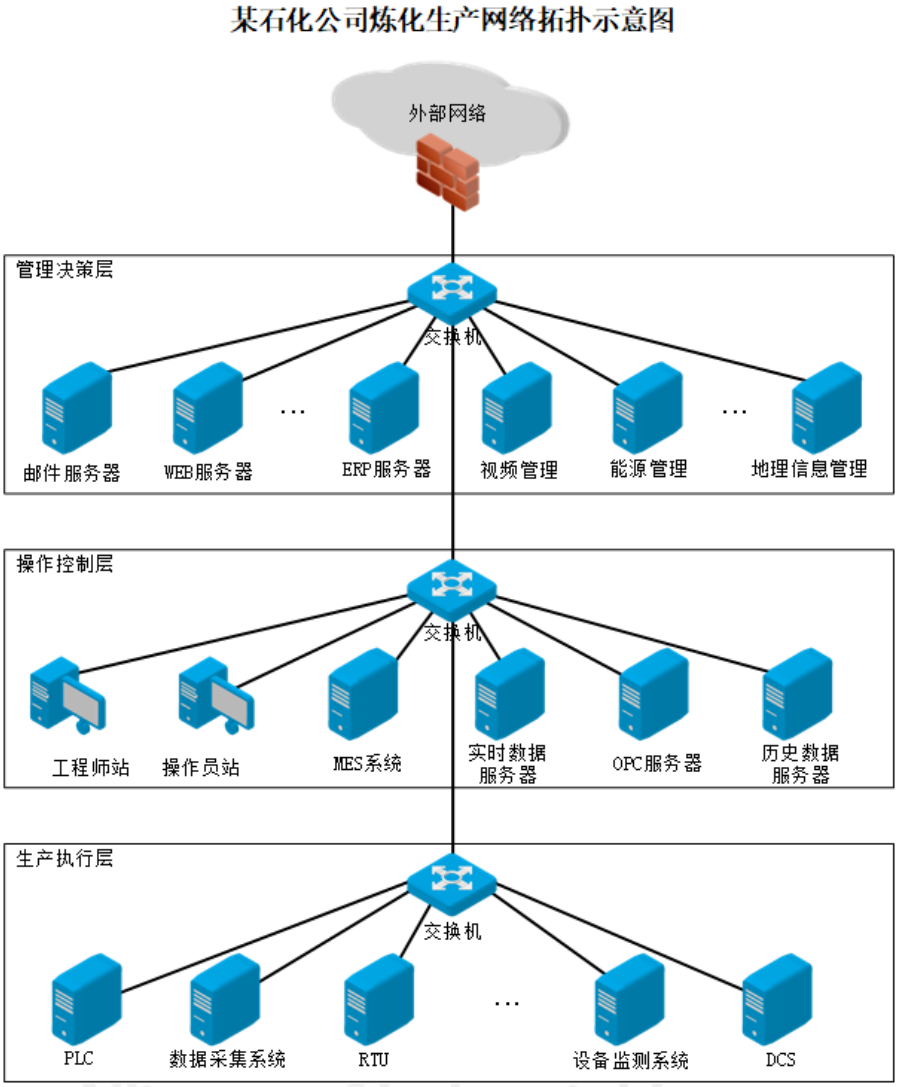


图 1　某石化公司炼化生产网络拓扑示意图

石化公司的生产相关网络环境根据生产需要及总公司相关规定分为三层，底层包含生产设备 PCS 的过程控制层，中间层为生产操作控制层，有工程师站、操作员站等，其中的 MES 系统作为数据采集及处理单元，起到承上启下的作用。最上层为管理决策层，ERP 系统通过 MES 系统提供的数据支撑对整个生产过程进行管理，此外该层还有邮件服务器和 WEB 服务器等非生产必须的网络服务。

经过我们的现场调研与评估，发现该公司的网络环境主要有

以下六大问题。

**1、 未划分安全域**

目前石化公司未进行安全域划分，各子系统没有进行有效隔离，并且各层间

通信也没有做适当的隔离，处于边界不清，缺失边界访问控制的状态。需要在不间断业务的情况下，理清各业务系统关系，并加入有效隔离机制。

**2、 安全配置不全**

安全配置不全面问题较突出，在网设备没有进行安全加固，如补丁更新、密

码强度与期限等配置。需要对在网设备进行全面排查并进行安全加固。

**3、 监控手段缺失**

目前网络中缺少安全风险监控手段，不能及时了解网络运行情况，一旦出现

问题，不能快速完成响应的处理动作。需要配置相应的审计手段，对网络中的流量进行全面监控，及时发现并处理风险监控手段。

**4、 防护软件缺失**

工程师（操作员）站无防护软件，且多使用较老版本的 Windows 平台且无

补丁更新，同时缺少身份认证，接入控制手段。需要对工程师站进行终端安全软件部署，在操作系统不能更新的情况下保证

终端安全。

**5、 运维审计缺失**

导致设备配置变更记录缺失，一旦出现问题，无法快速定位到相关设备及相

关人员。

**6、 管理流程待完善**

安全管理流程不完善，易导致因人为因素或流程科学性导致的数据泄露，引

入恶意代码等问题。

**2.1.3 安全解决方案**

根据现有网络客观情况，网络中突出问题及等级保护等相关规定，制定了本方案。本方案增强用户网络的互通能力，建立多层级网络安全体系，实现跨系统的互操作。基于原来的业务网络结构，推动信息技术（IT）网络与生产控制（OT）网络融合。

本方案决定遵循以下原则进行部署。

- **垂直分层，水平分区原则**

以不中断现有业务为前提，最大程度保持现有网络拓扑，保持原有生产网络的三个层级，即生产执行层、操作控制层和管理决策层，但要对各层之间部署有效的隔离措施和监管技术手段。同时，要对同层各生产环节进行分区管理，对内服务的系统不宜与对外服务的系统处于同一分区，生产系统与非生产系统不宜划分为同一区，如管理层中负责企业资源管理的 ERP 系统与对企业外提供 WEB 服务的系统不宜划分为同一区域管理。

- **技术与管理并重原则**

目前客户方除需要技术手段确保信息安全外，更重要的是补足管理制度方面的短板，把管理措施和技术措施有机结合起来，依靠管理措施来弥补技术措施的缺陷，保障安全技术措施的正确实施，更有效保障炼化生产的整体安全性。

- **集中管理原则**

统一管理是建设信息安全等级保护深度防御系统的基本要求。同时，在全面推广信息安全等级保护深度防御工程时，按照统一信息系统安全管理的规范进行规划和设计，确保信息安全防护水平的一致。对业务系统范围内的资源和用户进行统一标记，按照访问控制策略来进行实施，对于各个终端、服务器和边界的事件应统一由审计中心进行分析和响应。另外，应建立全系统范围的网络管理和监控系统，做到管理全局统一，监控严密，响应及时。

根据以上原则，有如下防护方案。

工业互联网产业联盟
Alliance of Industrial Internet

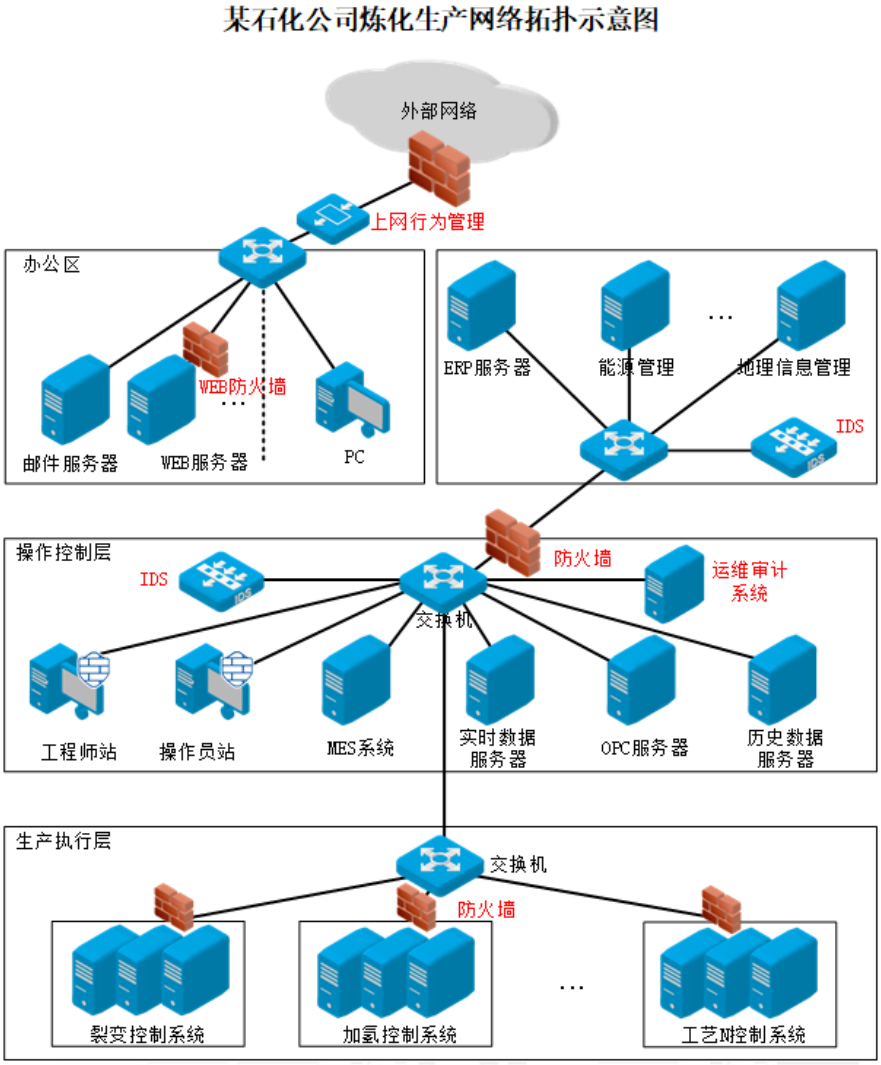


图 2　某石化公司炼化生产网络拓扑示意图

方案中首先对各生产系统进行层次和区域的划分，对生产环境和非生产环境进行区分管理，并根据需要部署工业级防火墙，确保环境得到纵向的纵深防御能力，并对生产环境进行横向分区隔离，保证跨域访问能够被控制。在网络中需要部署入侵检测系统，在不影响现有网络状况及运行的情况下，对网段上监听，采集网络数据，及时检测出网络中出现的异常数据及非法入侵，对网络中的活动进行审计，生成完整记录，便于事件追溯。同时，对生产网络内部终端等进行加固并部署完全软件进行对主机内

部的软件流量等的管控。

具体实施方案如下:

**1、 主机安全方面**

根据石化公司系统现状，工程师（操作员）站主机使用的是 Windows 操作系统，且版本较老，有存在安全漏洞风险。并且，这些主机存在未管控的 USB 端口及光驱，使用时很容易将病毒木马带入终端，然后通过终端散播到网络的各个区域，最终致使整体生产网络瘫痪。

通过部署工控主机安全防护软件，确保这些设备的安全。工控主机安全防护软件采用“白名单”管理技术，通过对数据采集和分析，生成工业控制软件正常行为的白名单，与现网中的实时传输数据进行比较、匹配、判断，做到只有确认合法的软件才可以运行。如果发现其用户节点的行为不符合白名单中的行为特征，其主机安全防护系统将会对此行为进行阻断或告警，以此避免主机网络受到未知漏洞威胁。

**2、 网络隔离方面**

生产执行层、操作控制层和管理决策层隔离及各生产工艺间需要部署防火墙并开启访问控制功能，实现逻辑隔离和报文过滤。

防火墙通过会话状态检测、包过滤及协议深度访问控制，阻止各类非授权访问行为。使用白名单防护策略，缺省禁掉所有访问，只有配置可信的流量才可通过防火墙进行跨域信息交换。同时，可以对操作人员与设备进行基于 IP、MAC、协议或任意组合方式的访问进行控制。

### 3、 威胁检测方面

在生产执行层和管理层的汇聚交换机处做接口流量镜像，旁路部署入侵检测系统，在网络上监听、采集网络数据，实时检测网络中出现的异常数据、非法入侵，根据预定义策略实时报警，并完整记录检测情况，便于之后的事件追溯。

入侵检测系统通过对攻击或入侵的检测及响应，可以有效地发现和防止大部分的网络犯罪行为，给网络安全管理提供了一个集中、方便、有效的工具。使用入侵检测系统的数据检测、主动扫描、网络审计、统计分析功能，可以进一步监控网络故障，完善网络管理。

### 4、 运维审计方面

在过程控制网络中部署一套运维审计系统，运维审计系统旁挂部署在该区域核心交换机。通过该系统实现运维人员仅能通过运维审计系统访问所需运维的设备，避免运维人员直接访问服务器区对重要服务器进行配置更改等。

### 5、 WEB 防护方面

在对外提供 WEB 服务的区域部署 WEB 防火墙，用于有效弥补出口防火墙对 WEB 应用攻击防护能力不足的问题，该产品针对安全漏洞、攻击手段及最终攻击结果进行扫描、防护及诊断，提供综合 WEB 应用安全解决方案。

事前，WEB 应用防火墙能够提供 WEB 应用漏洞扫描功能，检测 WEB 应用程序是否存在 SQL 注入，跨站脚本漏洞；事中，WEB 应用防火墙能够对黑客入侵行为、SQL 注入/跨站脚本等各类 WEB

应用攻击、DDoS 攻击进行有效检测和阻断；事后，针对当前的安全热点问题，网页篡改及网页挂马，提供诊断功能，降低安全风险。

**6、 上网行为管理方面**

在互联网出口部署上网行为管理产品，有效控制内部上网行为可能引入的风险。所部署的上网行为管理产品拥有丰富的上网行为管理、审计以及专业的流控功能，致力于控制互联网用户和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析。通过优化上网管理，有效提高企业内部 IT 资源的使用安全，帮助企业提高生产力，提升网络资源利用率，降低法律风险。

在做到技术层面的防护同时，我们同样重视安全管理方面的建设。安全管理体系建设的核心思想是调整原有管理模式和管理策略，形成统一的系统整体安全管理体系。

**7、 人员安全管理制度方面**

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。

确定公司由统一的人事管理部门负责人员管理，这里的人员安全管理主要指对关键岗位人员进行的以安全为核心的管理，例如对关键岗位的人员采取在录用或上岗前进行全面、严格的安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统账户和相关权限等措施。

**8、 系统运维管理制度方面**

- **环境和资产安全管理制度**

环境包括计算机、网络机房环境以及设有网络终端的办公环境，明确环境安全管理的责任部门或责任人，对重要区域设置门禁控制手段或使用视频监控等措施。资产包括介质、设备、设施、数据、软件、文档等，应明确资产安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单。

- **设备和介质安全管理制度**

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面做出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。

- **日常运行维护制度**

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理；制订设备操作管理、业务应用操作管理、变更控制和重用管理、信息交换管理相应的管理制度；制定与信息系统安全管理相配套的规范和操作规程并落实执行；正确实施为信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施，对运行安全进行监督检查。

- **集中安全管理制度**

信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全

配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理。

- **事件处置与应急响应制度**

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。落实安全事件报告制度，信息系统发生较大、重大、特别重大安全事件时，用户单位按照相应预案开展应急处置，并及时向受理备案的公安机关报告。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。

- **系统建设管理制度**

系统建设管理的重点是与系统建设活动相关的过程管理，由于主要的建设活动是由服务方（如集成方、开发方、测评方、安全服务方等）完成，运营使用单位人员的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等活动的管理责任部门、具体的管理内容和控制方法，并按照管理制度落实各项管理措施，完整保存相关的管理记录和过程文档。

- **系统安全管理制度**

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。定期对信息系统安全状况进行自查，信息系统安全状况未达到安全保护等级要求的，

应当进一步开展整改。

### 2.1.4 小结

本方案的主要价值有三点。首先在于保护其生产网络环境的平稳运行，达到“只有可信任的设备才能接入控制网络”“只有可信任的消息才能在网络上传输”“只有可信任的软件才允许被执行”的防护效果。其次本方案部署了多维度的审计系统，从上网行为审计到攻击行为审计，从管理层到生产执行层部署了全面的审计系统，确保能够提供事前可检测与事后可溯源的全方位立体式的审计手段。以上两点强化了企业的自身防护与审计技术能力，初步建立了集中化安全态势感知和综合防护系统，提升了网络和数据安全技术能力。也为后续接入区域级平台形成多方联动、运行高效的技术服务保障体系做好准备。最后，在重视通过技术手段进行安全防护的同时，同样重视客户安全管理体系的建设，帮助用户分别在人员安全管理、系统运维管理、系统建设管理、系统安全管理等方面建立了制度性要求，通过二者的有机结合，更好地为用户提供信息安全保障。

### 2.1.5 单位基本信息

东软创立于 1991 年，是中国第一家上市的软件公司，一直以来致力于信息技术的创新。东软以软件技术为核心，面向全球市场提供成熟先进的网络安全产品与服务、提供智慧城市、医疗健康与社会保障、智能汽车互联等领域的创新型解决方案。目前，东软在全球拥有近 20000 名员工，在中国建立了覆盖 60 多个城市的研发、销售及服务网络，在美国、日本、欧洲等地设有子公

司。

东软网络安全事业部成立于 1996 年，连续多年保持稳健增长。以业务驱动安全为核心，致力于业务安全的技术研究，为客户提供基于业务安全的网络安全防御体系。为适应云计算、移动互联网、物联网、大数据、关键基础设施等新技术在各种网络环境中的应用，东软陆续推出 160G 数据中心防火墙、虚拟安全网关、桌面型无线安全网关、云安全交付网关、自主可控国产芯片网关、预警威胁管控平台等系列产品。东软 NetEye 旗下产品及服务被广泛应用于能源、政府、金融、电信、医疗等行业。

东软网络安全业务在未来将通过自身行业安全积累，凭借 IT 技术优势和经验，融合云计算、大数据、人工智能等新技术，积极适应网络安全市场新需求，引领网络安全市场新变化。

## 2.2 案例二：卡奥斯工业互联网平台安全解决方案

### 2.2.1 方案概述

为了让海尔卡奥斯工业互联网平台融合全新的工业安全理念和工业信息安全技术并为工业企业在物联网时代下提供完整信息安全解决方案。卡奥斯工业安全态势感知平台应用而生。

卡奥斯工业安全态势感知平台，是集安全态势感知和安全运营于一体的综合性工业网络安全平台。以卡奥斯工业互联网平台企业用户资产为防护目标，以用户数据安全为核心，基于整体环境动态地洞悉安全风险，以安全大数据为基础，从全局视角对安全威胁进行发现识别、理解分析和响应处置。最终形成针对网络安全的决策与行动，是网络安全能力的有效落地策略。

参考《工业互联网创新发展行动计划》建立企业级安全服务平台。平台辐射卡奥斯生态内的上万家客户。为平台客户赋能安全能力，推动工业互联网网络安全技术与工业机理模型的融合创新。

工业互联网是连接工业全系统、全产业链、全价值链，支撑工业智能化发展的关键基础设施，具有开放、互联、跨域、融合等特点，这是工业互联网的独特优势，也是工业互联网发展的一个重要前提和基础。同时由于它打破了以往相对清晰的安全边界，因此也带来了新的安全难题。特别是与互联网相连后，既面临来自互联网的外部威胁，又与工业生产等内部安全问题相互交织。

为解决这些问题，夯实安全基础，保障工业互联网安全发展，海尔建立了卡奥斯工业安全态势感知平台，平台集安全态势感知和安全运营于一体，是行业内首个打通工业互联网工业网络安全要素的安全监测服务平台。平台基于整体环境，以安全大数据为基础，工业企业内外网安全监测为核心、协同联动和信息共享为驱动，从全局视角对安全威胁进行发现识别、理解分析和响应处置。最终形成针对网络安全的决策与行动。

### 2.2.2 典型安全问题

#### 1、 建立家电行业工业互联网系统安全防护体系顶层设计

目前在工业的安全防护建设中，所采用的仍然是传统的针对IT 系统的安全防护理论与防护体系，这在面对工业控制系统网络安全防护的特殊要求面前显得力不从心。此外，目前所推出的各类工业网络的安全防护解决方案，并没有对这些安全防护产品

之间的关系进行统筹考虑与分析，缺乏对工业控制网络的安全防护问题的顶层设计。

通过本项目的建设，可以形成一个情报收集、维护、使用的综合型平台，使情报有效落地，更高效的利用情报完善攻击发现、事件分析响应、事件处置及预防等相关工作。

**2、 建立工业信息安全的态势感知能力**

在实际工作过程中发现，企业对自己所处网络环境的安全状况并不清晰。对自己在公网上的暴露程度不了解，对已经发生的网络安全事件不敏感，对网络安全没有预知能力也没有应对能力。

通过建立态势感知平台实现对安全状况的综合分析和量化评估。比如，对资产暴露发生的变化及安全问题出现进行全面、快速和准确地捕获和分析，帮助企业了解其暴露在互联网中的资产的状况和安全威胁，帮助监管单位了解区域内资产的安全态势，并实现实时、动态的可视化展现，展现的内容包括全国基于地理信息的综合态势，基于漏洞严重性、影响范围等综合因素的漏洞态势。

采用工业互联网基于业务关联的资产风险评估模型，实现准确实时的在线资产风险评估、监测单位风险评估、区域风险评估和行业风险评估，及时掌握工业互联网资产、监测单位的安全态势觉察、跟踪和分析。通过资产风险评估模型，能够实时掌握工业互联网资产整体风险态势、监测企业的风险态势、区域风险态势和行业风险态势，及时预警通报所监测范围内的安全威胁、安全风险和安全隐患；利用精确的地图定位抓重点，知短板，重点

进行问题的问题整改。

**3、 建立工业网络安全管理体系**

工业生产中，连续生产是第一要素，如何结合工业生产的特点，合理的对工业网络安全进行管理是解决工业网络安全的难点。目前所采用的安全管理方法，往往会与企业的业务需求产生冲突，甚至为了追求可用性而牺牲安全。建立一套行之有效而且能够适用于工业生产特点的安全管理体系势在必行。

**4、 建立有效的工业互联网综合防护体系**

在工业企业的日常运营中出现网络安全问题，往往不能及时的定位、解决。而且问题往往会涉及多个设备，需要跨多个厂家多个专业来解决。对企业而言，问题不能在第一时间解决造成了问题扩散，增加了问题造成的损失。对设备厂家也需要浪费大量人力物力协助企业来解决问题。

通过企业风险评估和上报的安全事件全面感知工业互联网安全态势，掌握重点企业安全现状，落实安全管理职责，协助企业进行安全检查和事件整改，加强与外部资源联系例如工控系统集成商或者原厂的合作，通过实时的威胁情报分享和风险通报，形成协同安全解决方案。

**2.2.3 安全解决方案**

海尔承接国家战略，集成工业互联网企业生产网络安全全要素，建设工业互联网安全态势感知系统，形成安全可视化运营平台。全面掌握工业互联网企业下属所有工厂的生产网络运行状态，包括关键事件、安全态势、资产统计、漏洞展现、威胁告警等，

建立三级联动的综合防护体系。平台解决工业互联网企业工业网络监控能力和分析能力不足导致的工业安全威胁不可知的问题，降低资产威胁分析的成本，提高威胁告警精准度，同时平台提供安全防护、安全态势感知、威胁处置、应急响应四类网络安全服务，全方位助力工业互联网企业智能制造安全升级。

## 1、 项目总体架构和主要内容

### （1）技术架构

平台主要包括应用服务层、数据采集层、数据存储、数据分析层等内容，整体组成如下图 1 所示：

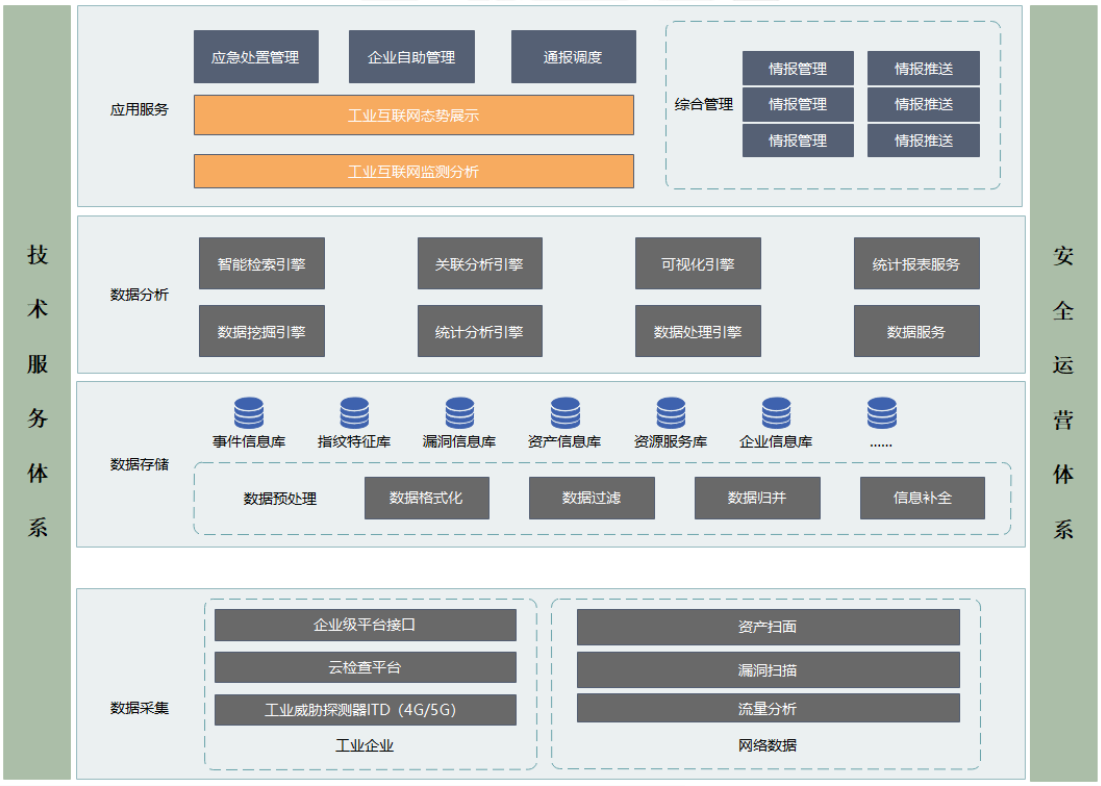


图 3　技术架构图

- **数据采集层**

为实现工业互联网安全监测预警平台的价值，首先需要对重点单位工业互联网网络空间进行资产探测，发现工业互联网资产

后进行资产识别和漏洞识别，为后续的应用系统开发提供基础支撑。

- **数据存储层**

数据存储层为整个系统提供了底层的数据存储服务，工业互联网安全监测预警平台作为一个大数据平台需要采集存储分析海量数据，因此为了支持本地私有云海量数据的存储与快速查询，数据中心采用自主研发优化的智能检索引擎 ES，满足大量的数据搜索请求和数据存储等需求，实现更高的查询性能。ES 提供了一个分布式多用户能力的全文搜索引擎，基于 RESTful web 接口，能够达到实时搜索，稳定，可靠，快速，安装使用方便。在不考虑网络性能的前提下，支持 2000 亿条日志记录以上的入库和查询，响应时间需要在 3 秒之内。

- **数据分析层**

数据分析层主要目的在于为上层应用系统提供数据加工、统计、计算等相关能力。数据分析包含了智能检索引擎、数据挖掘引擎、关联分析引擎、统计分析引擎、3D 可视化引擎和数据处理引擎等，为在上层提供多种查询、分析及计算以支撑不同的应用系统，为上层应用系统提供数据支撑。

- **应用服务层**

应用服务层根据平台建设目标和实际业务需求，从功能和业务角度建设完成包括工业互联网监测分析、工业互联网态势感知、通报调度、企业自助管理、服务商自助管理、应急调度管理和综合管理等功能，实现工业互联网网络空间安全监测和态势感知能

力，实现重点单位、资产和工业互联网风险的监测、分析、预警和风险可视化，形成重点单位工业互联网安全服务能力建设的解决方案，提高工业互联网安全综合保障能力和水平。

**（2）功能架构**

发现和识别暴露在工业互联网的资产，监测和分析工业互联网的风险和威胁，实现工业互联网的网络安全态势觉察、跟踪和分析，全面掌握工业互联网的安全态势、安全威胁、安全风险和安全隐患，及时向企业预警通报安全风险和安全事件，根据预警级别进行快速准确的应急处置，形成平台与国家工业互联网网络安全安全监测与态势感知平台的情报推送和情报共享服务，平台与工业企业的协调联动、情报共享的预警通报和响应处置机制。

主要功能如下图所示：

图 4　功能组成

- **工业互联网扫描系统**

工业互联网扫描系统包括资产探测引擎、漏洞扫描引擎和调

度引擎。通过扫描引擎可实现对所辖工业互联网应用站点、工控系统、物联网系统等进行隐匿探测，发现工业互联网资产并对资产进行 IP 准确定位和漏洞识别，为监测预警平台实时监测、数据分析和风险评估提供原始数据。

- **工业互联网安全监测系统**

工业互联网安全监测系统作为整个中心的数据归集和处理基础系统的数据分析的展示，完成数据监测分析的统计汇总，从功能维度对于数据监测结果进行汇总分析与统计展示，主要采用统计分析引擎、关联分析引擎、智能检索引擎等技术，从应用站点、工控系统、物联网系统、监测单位和工业互联网综合分析等功能实现风险分析、漏洞分析和资产风险管理等功能。

- **工业互联网态势感知系统**

工业互联网态势感知系统包括应用站点态势感知、工控系统态势感知、物联网系统态势感知、监测单位态势感知等功能，通过漏洞分析、风险分析等技术，从业务角度分析并实现工业互联网资产、监测单位和整体的安全态势觉察、跟踪和分析，并通过大屏实现可视化呈现，全面掌握重点单位工业互联网的安全态势，及时预警所监测范围内的安全威胁、安全风险和安全隐患，整体提升工业互联网态势感知和风险预警能力。

- **运营服务系统**

运营服务系统是整个业务运营人员进行日常管理、安全服务的业务平台，实现资产管理、工业企业管理、运营信息管理和系统配置等日常管理服务，为业务服务平台提供基础数据资源；基

于综合管理根据风险级别和漏洞等级等进行研判分析并快速进行通报处置和资源调度，形成平台和工业企业的协调联动的预警通报和响应处置机制，协调工业企业进行现场检查、协调处置等安全服务，提高工业互联网安全态势感知、工业互联网资产监督管理、工业互联网安全事件预防和安全威胁的处置能力；实现平台与工业企业之间的日常管理、通知公告、事件上报等一站式安全管理服务，推动工业互联网社会综合治理向深层次发展，整体提升工业互联网安全防护水平。

- **信息共享系统**

利用工业互联网安全监测系统检测的安全漏洞、接收的安全事件同步给信息共享系统，同时该系统通过采集云端获取 APT 及高级威胁事件分析、安全事件分析、影响范围较广的关键漏洞分析等威胁情报信息，将其中抽取出来的攻击手法分析、攻击组织分析、攻击资源分析等信息与安全事件进行关联分析，分析确认的信息存入到共享信息库中。利用数据服务接口，向本地其他系统及有关部门进行情报报送和信息共享。

**2、 网络、平台或安全互联架构**

工业安全态势感知平台由流量管理平台、白名单管理平台和威胁探测器组成。

首先在各工厂的核心交换机、汇聚交换机旁路部署网络威胁探测器，持续对工厂内的网络资产、漏洞、威胁等情况进行监测和分析并采用 4G 或有线方式通讯将威胁事件数据上报到工业互联网威胁监测平台，实现对各厂区的工控网络安全状态的监测，

最新的工业威胁探测器可以根据实际情况选择合适的配置，既可以通过流量管理平台上报数据，也可以直接接入态势感知平台。其次将海尔原有的流量管理平台、白名单管理平台以及流量探针、网闸、防护墙、主机防护等安全设备接入工业安全态势感知平台。实现海尔所有网络安全设备的统一管控，和数据汇总分析。最后部署展示大屏，态势感知平台分级展示实时数据，包括：实时告警、攻击来源、网络威胁、系统安全、用户行为、资产分布、网络拓扑、攻击者/资产威胁溯源等内容。

平台部署如下图所示：

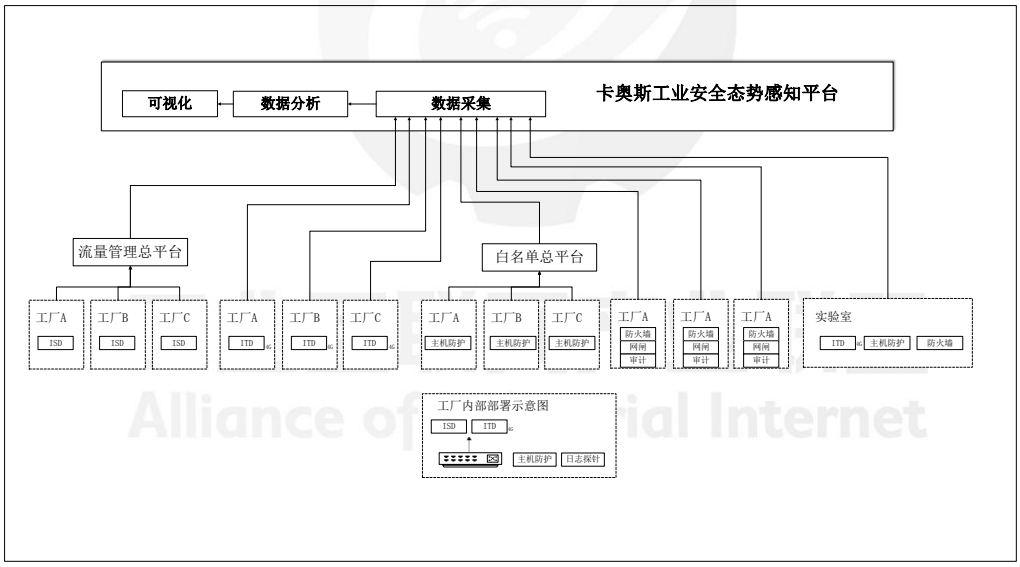


**图 5　平台部署网络架构**

平台的威胁检测分析系统和运营管理系统，依托 “九天”情报系统和“哈莫韦”工业网络安全实验室，针对工业互联网行业特点，建立从基础信息采集、到数据分析的一体化威胁情报分析，通过搭建威胁监测、分析管理平台，将 “九天”系统的威胁分析能力和“哈莫韦”工业网络安全实验室的研究成果，有效串联至卡奥斯工业安全态势感知平台各业务环节，为工业安全态

势感知平台的安全稳定运行提供坚强支撑。

系统通过在本地提供相关的Web服务和API接入的方式协助安全管理人员进行威胁分析，最终实现将威胁情报与安全运营的高效对接。

图 6　技术架构

## 3、 具体应用场景和安全应用模式

### （1）应用场景

平台专门针对工控环境进行异常监测、发现、告警和安全审计。对工控系统的资产进行实时发现和监测，帮助用户实现工控系统的“可视化”。基于工控协议的深度解析（DPI）技术，实时检查工控协议异常通信，并通过智能学习建模技术，帮助用户快速建立网络基线，识别出系统中存在网络异常事件。在此基础上支持漏洞木马、病毒以及其他网络攻击行为的检查，实时发现信息安全威胁和其造成的系统运行异常，协助运营人员第一时间进行响应处理，对工控系统进行全方位监测和保护。

构架如下图所示：

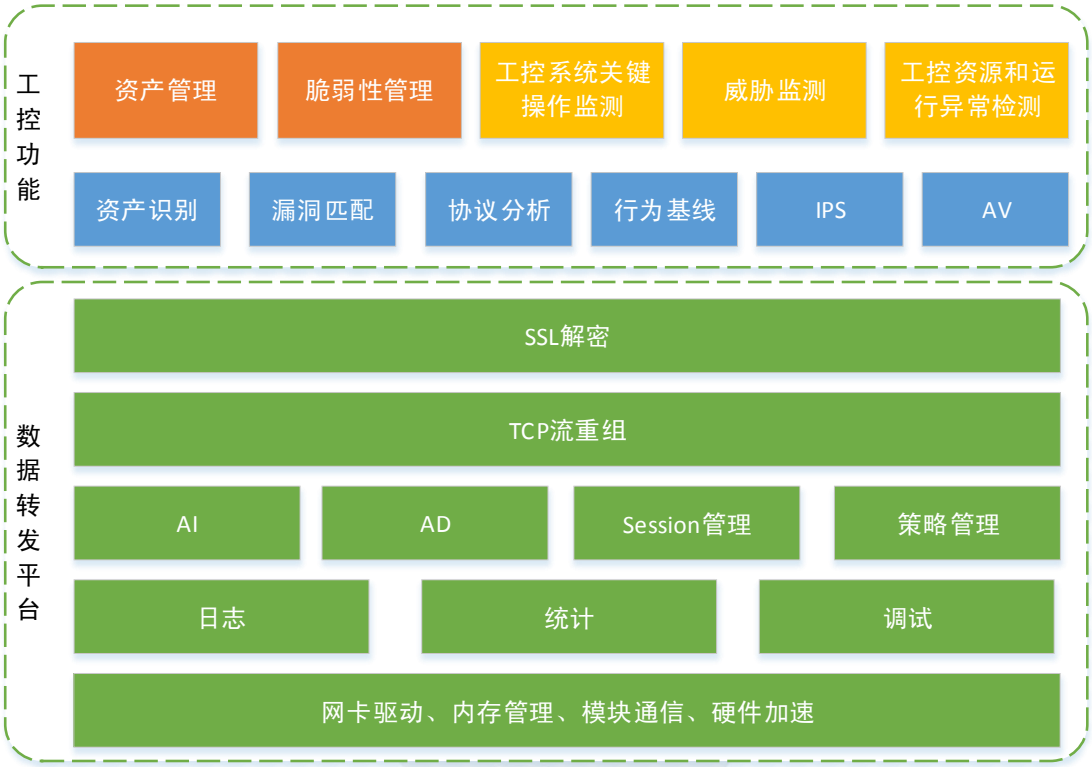


图 7　工业威胁发现分析构架

**（2）创新模式**

海尔智研院利用业界领先的大数据能力、威胁情报能力、工业数据分析能力及可视化能力，建立一套完整的三级联动的安全运营体系，构建以工业企业内外网安全监测为基础、以协同联动和信息共享为驱动，以安全运营为核心的三级联动综合防护体系及创新解决方案，该方案自下而上包括部署在工厂中的工业威胁探测器部署在集团的工业安全运营中心和部署在安全管理部门的工业互联网威胁监测平台。通过部署在各个工厂的工业威胁探测器自动分析工业协议、发现异常流量、感知网络威胁，并将工厂的安全风险上报给集团的工业安全运营中心，集团运营人员能够全面掌握集团工业安全现状，快速安排问题排查和事件处置，

同时将重大的安全事件上报给工业互联网威胁监测平台，安全管理部门的运营人员通过企业风险评估和上报的安全事件全面感知工业互联网安全态势，掌握重点企业安全现状，落实安全管理职责，协助企业进行安全检查和事件整改，加强与外部资源联系例如工控系统集成商或者原厂的合作，通过实时的威胁情报分享和风险通报，形成协同安全解决方案。同时利用海尔智研院强大的城市公共安全服务能力为工业企业进行赋能，完成工业互联网系统保护包括设备或系统上线前的检查、应急服务及日常支撑为工业企业进行安全赋能，形成以内外网监测为基础、以协同联动和信息共享为驱动，以安全运营为中心，以业务服务为目标的面向工业企业的工业互联网综合安全防护体系。如下图所示。

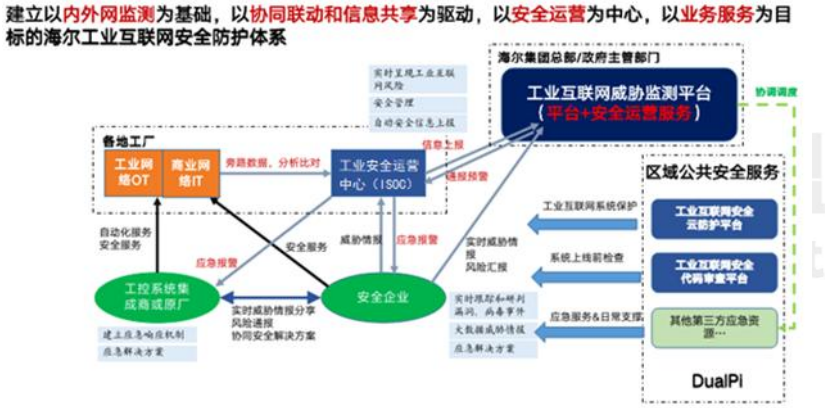


图 8　COSMOPlat 三级联动安全防护体系

## 4、 安全及可靠性

产品采用必要的安全技术与防护策略，加强系统在网络安全、主机安全、数据安全等方面的安全防护能力，基本边界访问控制、病毒木马监测、系统漏洞扫描、日志安全审计以及统一权限管理等业务功能，确保平台在数据获取、系统访问过程中的机密性、完整性、可控性，有效防范和处置各种潜在的威胁。

针对不同的应用场景设定防护级别，需要进行网络安全域防护，增强网络边界病毒防范功能，实现对各种网络病毒、恶意代码的检查、拦截、隔离、分析等功能，并建立 DMZ 区，设立单向隔离设备，与互联网接口直联的数据进行隔离、防护。建立 DMZ 区，在互联网接口侧配置防火墙和入侵防御设备，解决直联互联网的安全问题；指挥平台下发的数据通过单向隔离系统倒入 DMZ 区，并对下发的数据进行审计和记录，最大限度的保障平台核心数据安全，防止信息泄露。

应用安全设置权限管理包含用户认证、权限管理的功能，支持统一化认证、授权和审计，实现对资源的访问控制，以及对用户、角色以及用户组的有效管理。通过帐号、密码、验证码的方式对访问系统的用户身份进行验证，基于用户角色所赋予的权限对系统管理功能和数据进行访问控制。严格权限划分，避免权限滥用、违规、误操作，对本地敏感信息。

数据安全，对于涉及重保对象等敏感数据，进行数据漂白、改造、加密等数据脱敏操作，防止数据泄漏。对重保用户信息、重保网站数据等敏感数据，需要根据实际场景来选择适当的脱敏规则并进行脱敏处理。

在数据存储前，需要对不同来源的各种数据进行数据的预处理，包括数据的归一化、归并、聚合处理，保证数据格式的统一，方便使用。数据处理体系建设的目的是将各种结构化、半结构化、非结构化的数据转换为数据元模型中的统一表达的数据，存入数据存储库中，并在此基础上完成数据的质量管理和数据有效性监

测等。

**图 9　数据处理体系**

数据处理过程包含以下步骤：数据调研、数据模型建设、标准建设、数据实施、数据资产管理、数据质量管理、数据应用等。子系统支持将采集的数据经过适度的数据处理后，形成统一数据模型，将数据存储在 ES 与 Postgresql 中。

**5、 其他亮点**

**（1）构建在线监测网络，直观掌控安全态势**

基于多源数据支持安全威胁监测以及安全威胁突出情况的分析展示。综合利用各种获取的大数据，利用大数据技术进行分析挖掘，实时掌握网络攻击对手情况、攻击手段、攻击目标、攻击结果以及网络自身存在的隐患、问题、风险等情况，对比历史数据，形成趋势性、合理性判断，为通报预警提供重要支撑。该模块支持对网络空间安全态势进行全方位、多层次、多角度、细粒度感知，包括但不限于对工业互联网平台、重点行业、重点单位、重点网站，重要信息系统、网络基础设施等保护对象的态势

进行感知。主要包括态势分析和态势呈现。

针对重保单位、网站数据采集分析，通过监测分析子系统对DDos攻击监测、高级威胁攻击检测与APT攻击检测、IDS检测等功能，通过恶意代码检测、异常流量分析、威胁分析等技术进行宏观分析后，以监管单位为视角，对本项目监管范围下的单位安全状态进行监测。并且根据系统内置的风险评估算法给出当前被监管单位的整体安全评估。

充分利用工业企业现有安全监测平台和接口，整理工业企业现有安全监测能力，通过互联网主动探测和工业网络流量采集解析，利用工业协议深度解析和工业流量分析进行威胁分析，发现工业企业的网联资产，识别工业企业的内外网安全威胁，实现企业侧安全监测、威胁分析、威胁预警、协同处置和应急响应，开展资产探查、安全监测、威胁预警、威胁信息推送、工业安全咨询、等保合规、工业现场检查和工业应急响应等安全服务，帮助工业企业构建全天候、全方位的安全监测和威胁感知能力，提高工业企业的安全管理能力，保障工业企业安全生产。

**（2）实现多维风险监测，增强威胁发现能力**

汇聚网络侧和企业侧安全监测和态势感知平台的共享信息，结合国家态势感知平台的共享信息，构建基础资源库、知识库和威胁信息库等信息资源；结合专业机构的认定结果和处置建议，有针对性的开展日常信息运营，包括威胁分析、资产审核，提升安全威胁信息共享能力，实现工业互联网综合态势可视化，完成与国家平台信息共享和联动。

构建工业互联网安全知识库。通过网络侧、企业侧数据上报、与第三方平台数据对接、数据挖掘、企业上报等多种方式获取最全面、最权威的安全知识库。包括漏洞库、应急处置经验库、设备指纹库、恶意网络资源库、恶意程序库等，提供工业互联网异常监测能力，保障工业互联网安全。

构建威胁信息库。通过网络侧、企业侧数据上报、数据挖掘、第三方平台数据对接等多种方式获取最全面、最权威的威胁信息库，包括主机受控事件库、数据泄露事件库、信息篡改事件库、信息仿冒事件库、网络攻击事件库、有害程序事件库、高级威胁事件库、异常违规行为事件库、设备设施故障事件库，提供威胁分析和态势感知能力，提升工业互联网安全保障能力。

**（3）建立协同联动体系，提高事件处置效率**

以安全数据共享、安全监测业务协同、安全处置协同联动为核心，基于工业互联网安全监管机构、工业互联网企业、运营商与工业企业，构建以工信部、省级监管机构、工业企业、运营商为主的协同监测和多级联动管理架构，实现工业互联网安全监测、预警通报、应急处置、处置溯源和信息共享，形成上下联动、政企协同的工业互联网安全管理系统。

**（4）基于业务的工业安全运营**

实现被动到主动的转变：根据本地数据结合云端大数据及威胁情报，结合服务过程中发现的工业安全事件，针对可能发生的攻击行为提前做好响应对策，并通过专业化的保障服务，使监管具备处理突发事件的技术实力，提高安全事件响应与处理能力。

安全运营团队围绕态势感知平台系统，通过资产梳理、安全事件监测、流量深度分析、事件通报，应急处置、重要时期安全保障等一系列安全措施，协助省监管部门更全面、更准确、更高效地行使工业安全监管职能。

### 2.2.4 小结

卡奥斯工业安全态势感知平台集安全态势感知和安全运营于一体，平台基于整体环境，以安全大数据为基础，工业企业内外网安全监测为核心、协同联动和信息共享为驱动，从全局视角对安全威胁进行发现识别、理解分析和响应处置。最终形成针对网络安全的决策与行动。

图 10　卡奥斯工业安全态势感知平台

在安全态势感知方面，平台对接了在工厂部署的工业主机安全防护软件、流量探针产生的安全数据，同时平台具备很好的可扩展性，后续可以迅速对接于工厂部署的工业防火墙、网闸、工业日志审计设备等产生的安全数据，全面掌握集团下属所有工厂的生产网络运行状态。

在安全运营方面，平台提供安全可视化视图，支持安全事件调查、取证、溯源和处置等功能联动，支持安全决策，并建立安全咨询、安全培训、安全检查、风险评估、应急响应等安全服务。

**图 11　工业威胁态势**

卡奥斯工业安全态势感知平台，目前已囊括海尔集团分布在全国各地的厂区，与各厂区建立的安全防护体系数据共享，集成流量管理平台和白名单管理平台数据，以工业网络资产为核心，从工业威胁、资产漏洞、异常行为等多维度分析呈现综合安全态势。

而三级联动的服务机制，能够迅速沟通安全服务商和企业单位。形成准确有效的服务订单，安全服务商和被服务企业均能获得最优的效益。平台可以向客户提供多种安全服务和安全产品，所提供的服务和产品能够最限度符合目标企业的真正需求。平台依靠自己的安全分析检测能力，在向企业提供预警能力的同时，向企业提供最优的解决方案。平台能够提供的服务有：

- **传统信息安全咨询：**为客户提供专业的传统信息安全咨

询服务。

- **工业信息安全咨询：**为客户提供专业的工业信息安全咨询服务。
- **提供系统方案：**为客户提供系统性的信息安全解决方案。
- **信息系统安全体系建设建议：**为客户提供信息安全体系建设建议。
- **安全培训：**各类信息安全培训服务，可定制。
- **常规安全检查：**使用专业工具，对信息系统和工业控制系统进行安全检

查。

- **等保定级测试：**依据国家相关标准，按信息系统定义的安全级别进行全

面的安全检测，确保系统的满足所以定义的安全级别要求。

- **安全风险评估：**依据国家标准，对信息系统、工业控制系统涉及的所有

资产(硬件、软件、网络、文档和管理制度)进行全面的评估，并提供相应的整改建议。

- **渗透测试：**从攻击者角度发现外网系统、网站、工控系统等存在的安全

隐患，深度挖掘渗透测试范围内各个层面的安全漏洞。

- **安全审计：**通过对各类日志的分析，及时发现入侵痕迹分析，找出潜在

威胁。

- **应急响应：**7*24 小时远程及时响应。

本项目建成后，将快速面向服务的家电企业，形成良好的工业互联网和网络安全产业生态，形成示范效应，提升相关重点企业工业互联网工控安全防护能力，促进我国工业信息安全产业发展，为重点企业打造工业互联网安全“软环境”，降低企业工业控制信息化的复杂度，从而让重点工业充分享受信息化产业带来的便利，为国家推进工业互联网创新示范基地和网络安全创新基地发挥积极的引领、示范、推动作用，社会效益十分显著，可用以下方面概括:

**（1）有利于推动重点企业网络安全防护的跨行业协作和信息共享，掌握整体安全趋势，降低整体安全风险**

网络安全是全局性问题，任何一个网络安全问题都不能靠单一的企业/行业来解决。只有各方联动协作，形成合力，提供更有价值的信息，通过威胁情报、安全事件、安全响应能力、安全知识等在工业互联网重点企业、安全企业、自动化集成商之间的开放共享，有利于区域、行业及重点企业掌握工业互联网的安全现状、网络漏洞和威胁情况，为政府机构、安全厂商、企事业用户提供解决工业互联网高速发展的安全问题，为我国实现全局统筹的网络安全防御体系提供尝试，降低工业互联网重点企业乃至国家网络信息安全风险。

**（2）有利于降低工业企业安全事件平均解决时间长减少生产停机时间，推进工业互联网快速发展**

工业互联网企业的工业控制过程是其产生效益的主要环节。

工业互联网安全监测预警系统与安全运营中心联动，企业的工业生产、采集控制、运行管理的信息安全中枢，可以保障对下游控制对象等工业生产现场环节的生产信息采集及运行控制安全可靠，保证对上游计划管理层的各信息管理系统（如 ERP 等）提供的生产运行信息、统计数据等真实可信，防止恶意攻击造成的灾难事件，大大提高了整个工业控制过程自动化领域的信息安全保障水平。工业互联网安全监测预警系统集成应用构建的“协同开放，监测响应”的应用模式，能够改善智能制造、家电等领域的重点企业工业互联网安全状态，降低工业企业安全事件平均解决时间长减少生产停机时间，有利于推进工业互联网快速发展，符合国家信息安全的战略需求。

**（3）培养人才，培养威胁情报领域安全人才队伍**

项目过程中建立了威胁情报分析中心和威胁情报使用培训，培养了大量的威胁情报领域的专业人才，同时加速了相关单位技术人员的技术交流工作，在威胁情报开发、利用、部署方面积累大量的经验，最终大大增强了信息安全的后备力量。

**2.2.5 单位基本信息**

本案例由青岛海尔工业智能研究院有限公司和双湃智安科技有限公司合作建设。

青岛海尔工业智能研究院有限公司（简称“智研院”），成立于 2016 年 4 月，是国内第一家互联网型工业智能研究院，是集技术创新、工业智能、产业孵化等多种功能于一体的智能制造平台。定位为构建全球工业智能领域一流资源共创共赢生态系

统，输出中国智能制造落地技术，为大中小企业产业转型升级提供大规模定制整体解决方案。包括高端人才培育、高附加值的咨询服务，整厂/端到端全流程解决方案服务，软硬件集成解决方案等，依托海尔安全运营平台-海安盾在安全态势感知、安全大数据分析方面，平台具有安全技术基础。

双湃智安科技有限公司是专注于“工业互联网安全”创新性科技企业，致力于给客户提供简单、适用、易获取的安全服务和解决方案。依托工业安全大数据和超过 15 年的安全专家及工控专家团队，保护数字化转型时代下工业资产、运营和人员免受网络安全威胁，最大限度地提升企业工业控制网络的可靠性和安全性，提高企业生产力。

## 2.3 案例三：化纤行业工控安全解决方案

### 2.3.1 方案概述

近年来，工业控制系统信息安全事件不断发生，“震网”、“火焰”、“毒区”、“Havex”等恶意软件严重影响了关键工业基础设施的稳定运行，充分反映了工业控制系统信息安全面临的严峻形势。

各个工业行业频发的信息安全事故表明，一直以来被认为相对安全、相对封闭的工业控制系统已经成为不法组织和黑客的攻击目标，黑客攻击正在从开放的互联网向封闭的工控网蔓延。在电力、化工、煤炭、交通、冶金等行业均遭受到了严峻的工业控制网络安全威胁，急需加大在工业控制网络安全方面的投入，防止工业企业受到针对工业控制系统的网络攻击行为。

由于起步较晚，我国工业控制系统信息安全保障能力方面存在较大不足。当前我国工业控制系统核心软硬件设备的自主可控水平严重低下，基本的安全防护严重不足，网络接入控制混乱，外包维护管理缺乏，有很多工控系统需要依赖厂商才能维护，在培训教育和应急响应方面的力度也相当有限。面对复杂的工控安全形势，我国加强工业控制系统信息安全的保障工作迫在眉捷。

港虹公司工控网络安全建设项目建设完成后，能够全面提升企业生产网络的整体安全，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。

**2.3.2 典型安全问题**

**1、 工控网络存在一定的脆弱性**

**（1）存在后门：**已建项目主要软硬件多为进口，可能存有后门；

**（2）易被攻击：**广泛使用无线通信，易被监听、窃密和干扰；

**（3）接入风险：**部分网络借用公共电信网络和互联网组网，增加了网络接入风险。

**2、 工控网络面临着现实和潜在的威胁**

**（1）现实威胁：**U 盘滥用、病毒肆虐、软件乱装、违规操作、缺少有效的访问控制手；

**（2）潜在威胁：**攻击化纤行业工控系统技术门槛越来越低，易被信息战攻击。

3、 工控网络安全防护体系尚未形成

（1）**资产混乱：**关键资产底数不清楚；

（2）**维护不当：**严重漏洞难以及时处理，系统软件补丁管理困难，难以应对 APT 攻击；

（3）**风险增加：**工业化程度的深入推进加速了网络安全风险的暴露。

### 2.3.3 安全解决方案

1、 体系设计

（1）安全区域边界

● 工控防火墙

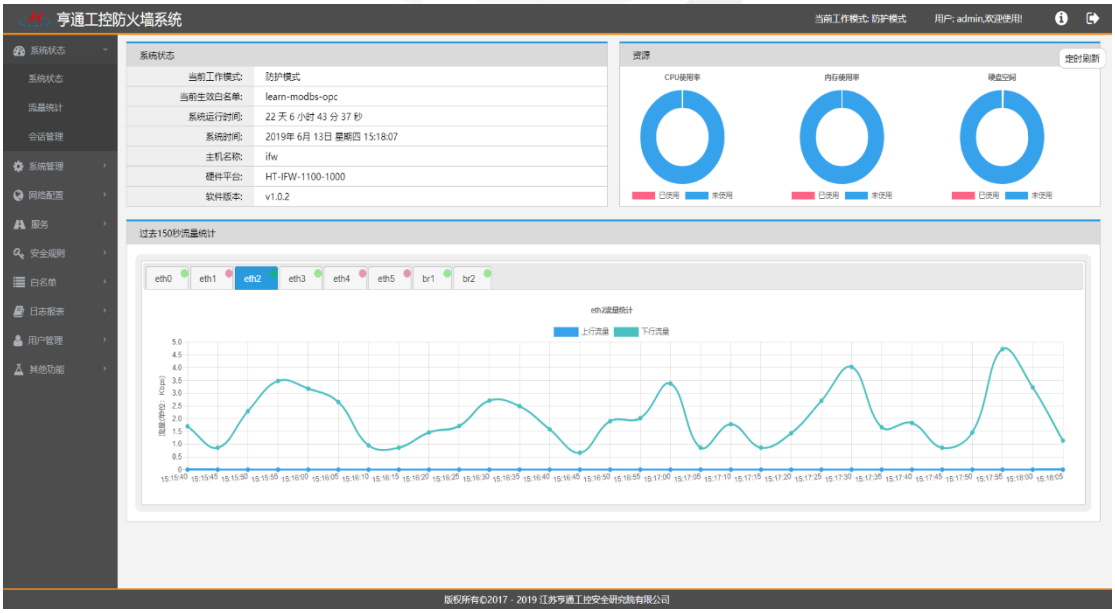


图 12　工控防火墙

工业防火墙可以采用黑、白名单的安全策略，过滤一切非授权访问，保证只有可信任的数据才允许通过，为控制网与管理信息网的连接、控制网内部各区域的连接提供安全保障。本次工控防火墙部署在各个生产车间接入交换机出口处以及关键设备前

端，根据区域边界数据交换规则通过检查数据包的源地址、目的地址、传输层协议和请求的服务的基础上，经过工控协议深度检查，防病毒检测、确定是否允许该数据包通过该区域边界；根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界，以防范来自边界的攻击行为，当检测到攻击行为时采取相应动作并通知安全管理中心。

- **工业安全网闸**

工业互联网产业联盟
Alliance of Industrial Internet

**图 13　工业安全网闸**

在（港虹公司）管理信息网与生产控制网之间部署工业安全网闸实现逻辑隔离与数据的安全传输，系统采用专用信息摆渡机制，解决了由于网络隔离引起的数据交换问题，既保持了网络之间隔离的特性，同时又提供了一种安全、有效的数据传输途径，采用非标准协议构成安全隧道，保障了数据传输的安全性，彻底杜绝了因办公网络的接入使业务系统感染病毒、木马的可能，消除了安全隐患。

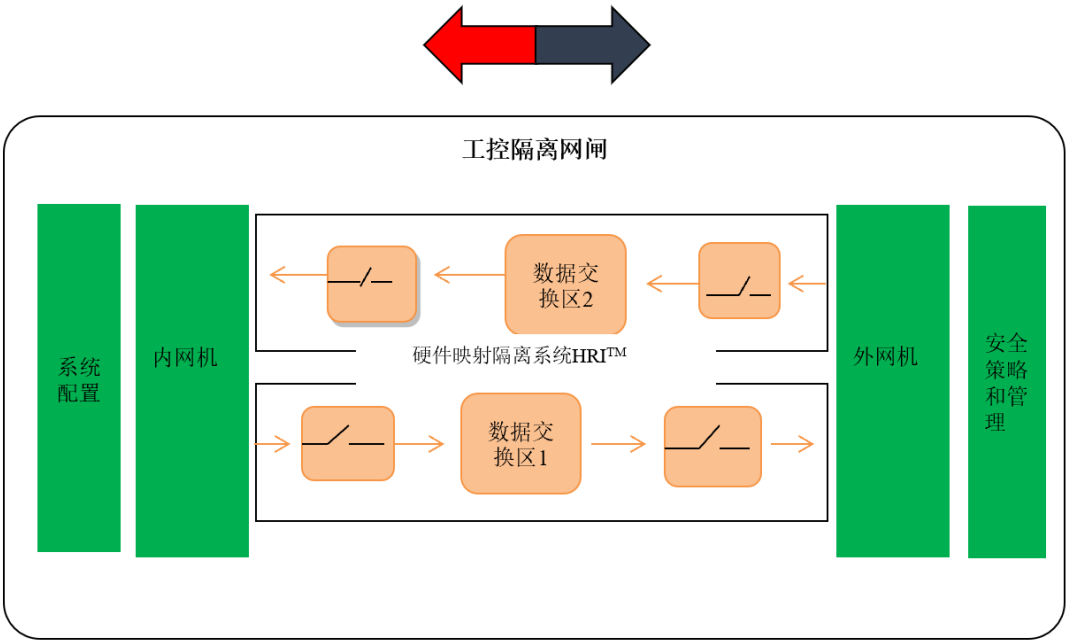


图 14　工控隔离网闸

- **工控安全监测审计系统**

工控安全监测审计系统是针对工业控制网络数据通信进行安全审计的平台。本次部署在汇聚层的三层交换机节点上，抓取网络中的所有数据，通过实时动态分析、数据流监控、网络行为审计等技术，快速识别工业控制网络中存在的异常行为，对异常流量及时发出告警。

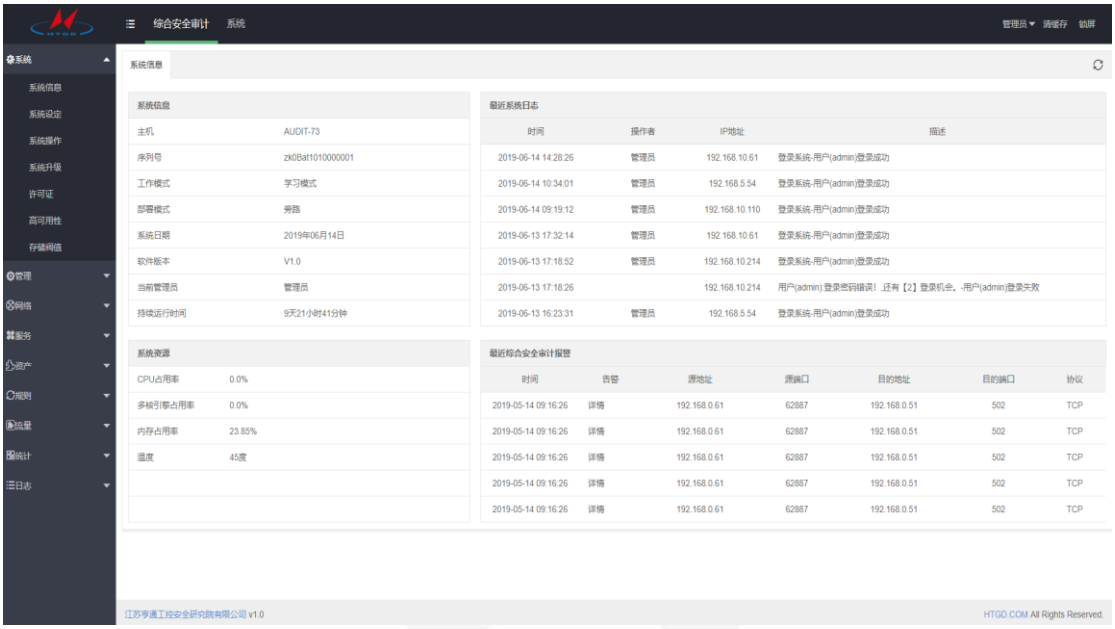


**图 15　工控安全监测审计系统**

主要功能包括网络监测、安全审计、核心安全规则库、流量异常告警、自动化网络行为分析。

**（2）安全计算环境**

- **主机安全**

通过工控主机防护系统从主机层面进行安全防护。同时可以配合基线检查、漏洞扫描、恶意代码监测等其他手段配合的方式，全方位的对生产控制层主机进行防护。

工业控制系统内的操作站、工程师站部署的多为 Windows 操作系统，工业控制网络为封闭环境，与互联网没有连通，终端升级较为困难；同时为了系统的运行稳定，考虑到兼容性企业也不会去主动升级，加上系统服役较长，因此在长期运行后会积累大量的安全漏洞，并且终端缺少安全防护措施，操作人员的安全意识普遍缺乏，综合以上情况，工业控制系统面临着严重威胁，给安全生产带来极大的隐患。

工控主机防护系统部署在生产网络中的各个 PC 端，专门针对工业控制系统的环境特点研发而成，依据程序特征建立操作系统运行的安全白环境，并且禁止非授信程序运行，解决了操作系统因无法升级补丁带来的安全问题，保证了系统的稳定运行；并且工控主机防护系统区别于传统的杀毒软件，不依赖于特征库，不用频繁升级，完美适配工控环境；除了限制未授权程序执行外，还具备监控注册表、侦测网络非法外联、限制移动存储介质非法接入等功能。

- **工控运维审计系统**

Alliance of Industrial Internet

**图 16　工控运维审计系统 1**

工控企业网络庞大、设备种类和数量较多且分散，维护需要记忆各种设备的 IP 地址和账号口令，对运维人员的工作提出很大挑战；同时运维人员对服务器、网络设备、工控设备的补丁升级、管理配置等所有重要操作行为都缺乏审计措施，出现问题后无法进行追溯；如通过第三方厂商进行维护，还必须提供账号和口令，存在敏感信息外泄的可能，在管理上存在安全隐患。本次通过部署工控运维审计系统，集中访问控制与授权，实现单点登

录（SSO）和细粒度的命令集访问授权。基于用户的审计将直接审计到人，实现从登到退出的全过程操行为审计，满足合规管理和审计要求。

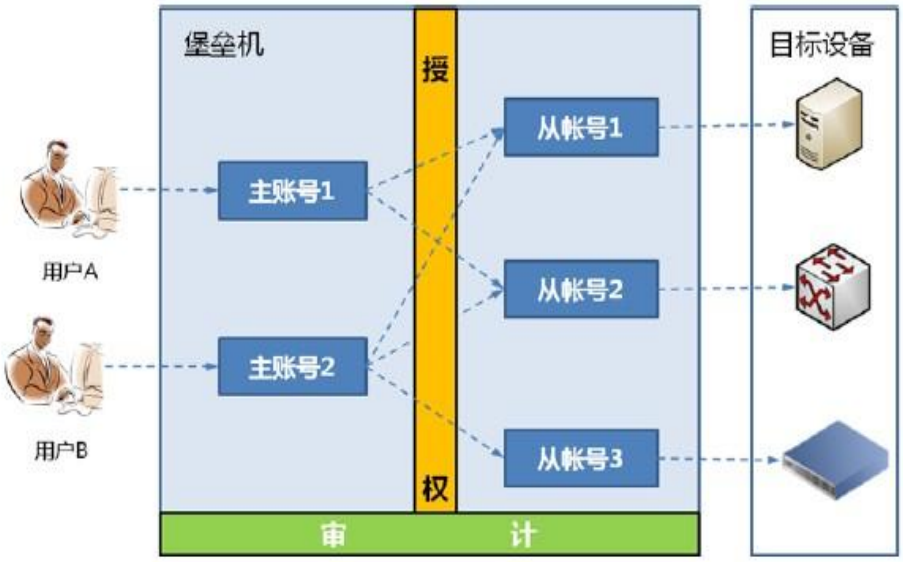


图 17　工控运维审计系统 2

- **统一安全管理平台**

由于生产控制网络中涵盖各类控制设备、网络交换设备、工控主机、OPC 服务器以及安全防护设备种类繁多，安全管理人员在运维大量的工业安全设备时需要逐个登录管理，导致工业网络中出现问题时得不到及时的排查，需要人工定位后再登录相应的安全设备判断问题原因，这样一来就延长了生产系统停车时间。本次部署统一安全管理平台，为运维管理人员提供全面了解资产安全现状，管理网络安全防护设备的平台的集中统一管理平台，实现安全防护设备的政策下发、运维管理、资产盘点等功能。

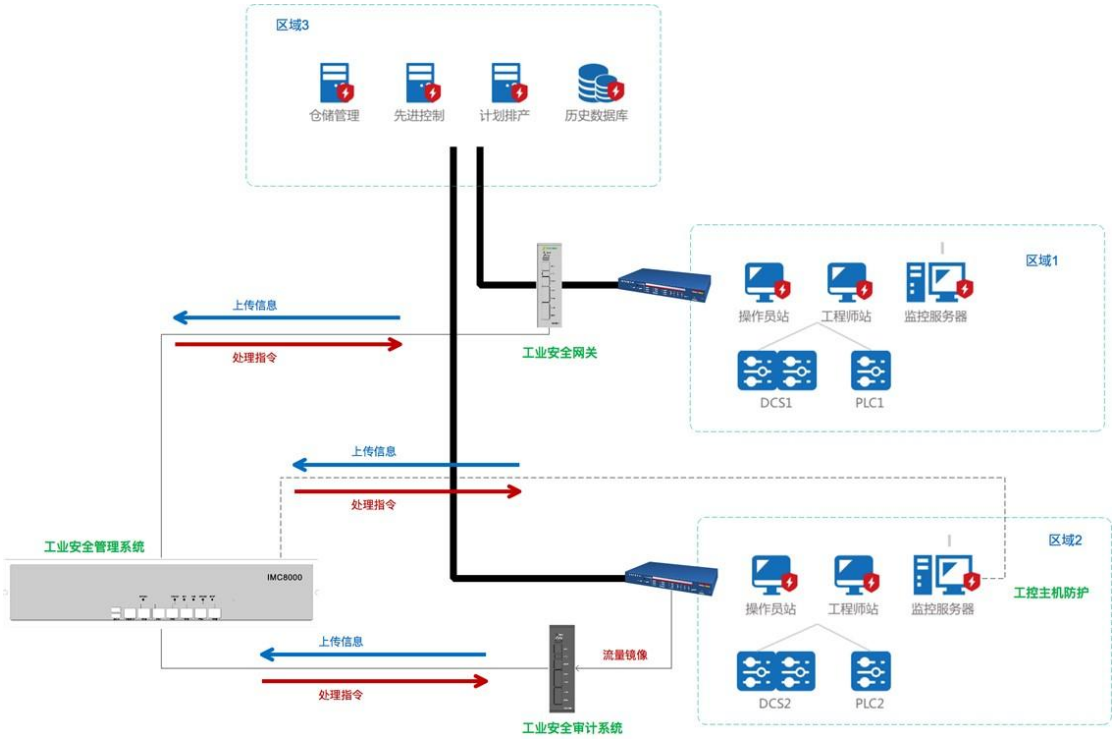


图 18　工业企业网络安全统一管理平台

### （3）工业企业网络安全威胁预警及态势感知平台

安全态势感知与威胁预警平台的整体架构分为：用户端、数据采集层、数据存储分析层、基础应用层、安全中心功能层。 并具备工控系统在线监测探针、工控系统攻击诱捕探针、工控威胁动态分析沙箱、恶意代码检测系统、威胁情报收集系统、IP 画像溯源系统、大数据流实时处理平台、大数据存储与检测平台等功能或模块。

图 19　安全威胁预警及态势感知平台

### （4）管理体系方案

- **工控安全制度管理**

根据工控安全制度管理的基本要求制定各类管理规定、管理办法和暂行规定。从工控安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

工控信息安全领导小组负责定期组织相关部门和相关人员对工控安全管理制度体系的合理性和适用性进行审定，定期或不定期对工控安全管理制度进行评审和修订，修订不足及进行改进。

- **工控安全机构管理**

根据基本要求设置工控安全管理机构的组织形式和运作方

式，明确岗位职责；

设置工控安全管理岗位，设立工控系统管理员、工控网络管理员、工控安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理工控信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确工控安全管理机构各个部门和岗位的职责、分工和技能要求。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

- **人员安全管理**

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。

一般单位都有统一的人事管理部门负责人员管理，这里的人员安全管理主要指对关键岗位人员进行的以工控安全为核心的管理，例如对关键岗位的人员采取在录用或上岗前进行全面、严格的安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统帐户和相关权限等措施。

只有注重对工控安全管理人员的培养，提高其工控安全防范意识，才能做到对工控安全有效的防范，因此需要对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。培训的内容包括单位的信工控息安全方针、工控信息安全方面的基础知识、工控安全技术、工控安全标准、岗位操作规程、最新的工作流程、

相关的安全责任要求、法律责任和惩戒措施等。

- **工控系统建设管理**

工控系统建设管理的重点是与工控系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方、测评方、安全服务方等完成，运营使用单位人员的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等活动的管理责任部门、具体的管理内容和控制方法，并按照管理制度落实各项管理措施，完整保存相关的管理记录和过程文档。

- **工控系统运维管理**

**1）环境和资产安全管理制度**

环境包括工程师站、工控机房以及设置有工控网络终端的生产环境，明确环境安全管理的责任部门或责任人，加强对人员出入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。对生产环境设置围挡等物理手段，或使用视频监控等措施。

资产包括介质、设备、设施、数据、软件、文档等，资产管理不等同于设备物资管理，而是从安全和信息系统角度对资产进行管理，将资产作为工控系统的组成部分，按其在工控系统中的作用进行管理。应明确资产安全管理的责任部门或责任人，对资产进行分类、标识，编制与工控系统相关的软件资产、硬件资产等资产清单。

**2）设备和介质安全管理制度**

明确配套设施、各类软硬件和工业控制器等设备管理、维护的责任部门或责任人，对工控系统的各种软硬件、工业控制器等设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面作出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。

**3）日常运行维护制度**

明确工控系统网络、工业控制系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理；制订工业控制器等设备操作管理、业务应用操作管理、变更控制和重用管理、信息交换管理相应的管理制度；制定与工控系统安全管理相配套的规范和操作规程并落实执行；正确实施为工控系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施，对运行安全进行监督检查。

**4）事件处置与应急响应制度**

按照国家有关标准规定，确定工控信息安全事件的等级。结合信息系统安全保护等级相关指南，制定工控系统安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。

**5）灾难备份制度**

识别需要定期备份的重要工控系统、系统数据及生产数据等，

制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度。

6）工控安全监测制度

开展工控系统实时安全监测，实现对物理环境（如视频监控等技术）、工程师站和生产车间等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，以便及时对工控安全事件进行响应与处置。

2、 拓扑建设

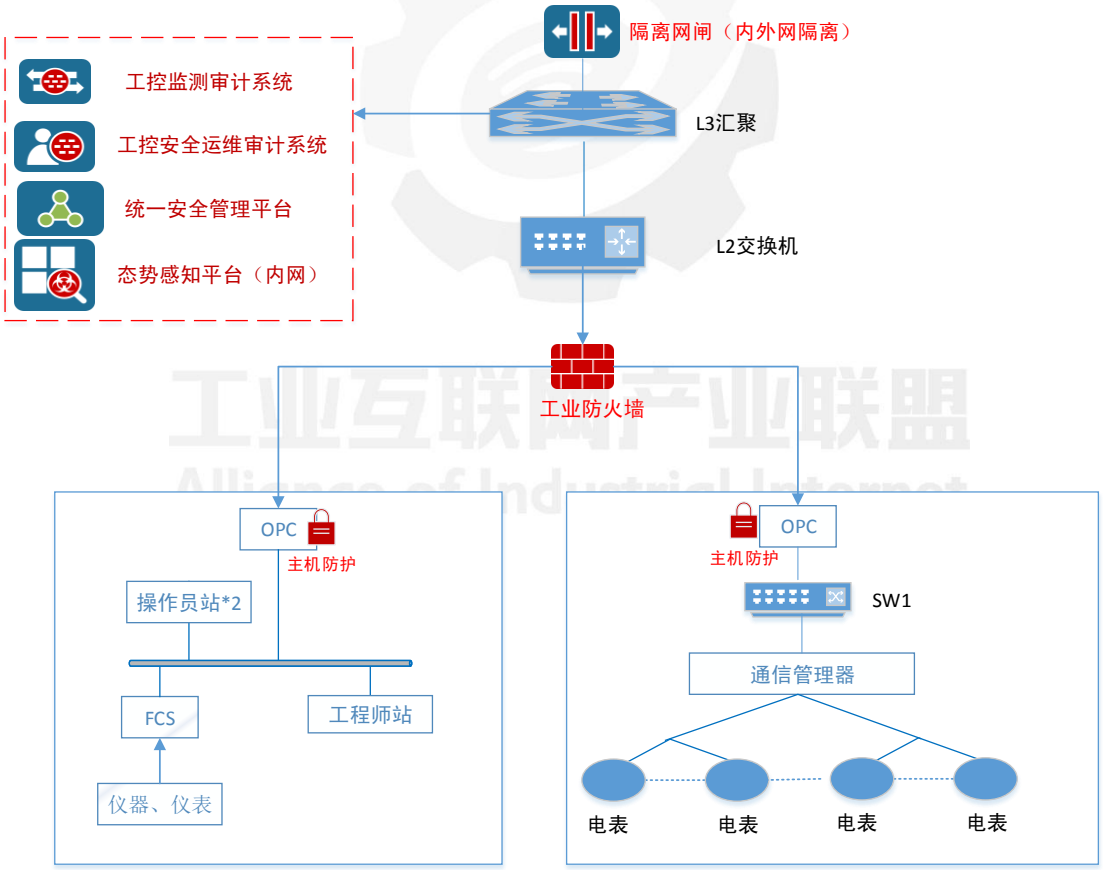


图 20　安全态势感知与威胁预警平台

2.3.4 小结

1、 完全自主的知产权

工业防火墙、工控安全监测与审计系统、工控主机防护系统、

统一安全管理平台具有完全自主的知识产权，已经申请到多项发明专利，江苏亨通工控安全研究院公司的安全产品能够帮助涉密单位、关系国计民生的大型工控企业对工控网络、网络内工作站、服务器进行安全防护和安全加固，杜绝安全后门隐患。

**2、 安全设备的统一管理**

统一安全管理平台将工控网络中的所有安全设备和系统统一集中管理，减少管理人员的工作量，降低企业人力资源的投入。

统一安全管理平台具有丰富的管理功能，友好的用户界面，人性化的统计报表，极大的提高企业工控安全管理的效率。

**3、 化繁为简的安全防护体系**

统一安全管理平台可以通过对工控网络内全部安全产品进行集中管理、全网安全信息的可视化展示、安全设备的统一配置等功能，简化工业控制网络内信息安全的防护工作流程，提升工控安全防护工作效率。

**4、 全面体系化的方案**

覆盖工业网络边界、主机、PLC 及 DCS 工控设备、工控组态软件等全方位安全的纵深防护体系，覆盖检测、防护、响应、审计的全过程，不留安全死角。

**5、 高度适配工控系统**

方案实施无需改造现有工业网络和频繁升级工控系统；无需频繁升级安全特征库；安全设备符合工控环境标准，可靠实用。

**6、 深度理解工控协议和操作行为**

深度理解工控系统广泛使用的 Modbus、 DNP3、IEC104、

Profinet、OPC 等数十种应用通信协议，智能学习各类操作行为和参数，更好的识别攻击行为。

**2.3.5 单位基本信息**

江苏亨通工控安全研究院有限公司（简称亨通工控安全）是亨通光电与国家信息安全工程技术研究中心江苏分中心合资共建企业；是国家中小型科技企业，江苏省双软企业、江苏省民营科技企业、江苏省高新技术企业，入选工信部工业互联网创新发展项目，被认定为江苏省工信厅工业信息安全服务支撑机构、江苏省通信管理局网络安全技术支撑单位（工业互联网安全方向）、苏州市委网信办苏州市网络安全技术支撑单位、苏州市网络安全信息咨询单位、江苏省工信厅工业控制系统信息安全三年行动计划支撑单位，是长三角 G60 科创走廊和江苏省工业互联网专业服务商；是国家高技能人才培训基地、苏州市职业大学"双师型"教师培养培训基地、苏州市职业大学高技能人才实训基地；是工业互联网联盟会员单位、工业信息安全产业发展联盟会员单位、江苏省网络安全协会常务理事单位、江苏省网络与信息安全产业联盟副理事长单位、江苏省信创联盟成员单位；认定为江苏省院士企业研究院、江苏省院士工作站、苏州市新型研发机构；组织承办苏州市政府技能状元赛、江苏省人社厅工业信息安全技能大赛、江苏省工信厅工业信息安全应急演练、长三角一体化发展示范区网络安全大赛；工业防火墙系统、工控监测审计系统、工业网闸、工控主机防护系统、安全运维审计系统以及抗拒绝服务系统获得公安部销售许可证，工业防火墙系统获得电科院产品检测

报告、行业第一个获得泰尔实验室检测报告；信息安全、网络安全业务已入围移动、电信、联通运营商供应商名录；自主研发的工控安全产品已在智慧水务、智慧燃气、智能制造、石油化工和电力行业应用。

## 2.4 案例四：鲁布革水电厂工业互联网电力监控系统综合安全防护解决方案

### 2.4.1 方案概述

**1、 行业现状**

为全面提升我国电力监控系统安全防护能力，进一步完善电力企业生产安全保障建设体系，国家能源局组织开展了电力监控系统安全防护的专项检查工作，并发布了《电力监控系统安全防护专项监管报告（2016）》。根据国家监管要求，南方电网公司和调峰调频发电公司制定并颁发《南方电网电力监控系统安全防护提升工作方案》（南方电网系统[2016]26 号文）、《调峰调频发电公司监控系统安全防护提升工作方案》（调峰调频设备[2016]18 号文）。

**2、 发展前景**

电力行业是我国重要的工业领域之一，发展工业互联网是电力行业数字化转型的必然过程，根据工信部印发的《工业互联网创新发展行动计划（2021-2023 年）》的相关内容要求，电力行业将进一步加快工业互联网创新发展步伐，持续推动工业数字化转型。

**3、 技术现状**

随着工业互联网领域的安全事件频发，工业领域网络安全态势日趋严峻。当前，根据上级监管要求，电厂进行了电力生产监控网络的相关安全建设，部署了安全访问隔离和纵向认证加密装置等设备，并没有从合规性和安全能力等方面进行系统规划和体系建设，导致电厂电力生产监控网络的防护水平低、防护效果差。

**4、 发展趋势**

根据《工业互联网创新发展行动计划（2021-2023 年）》中提出的实施企业网络安全能力贯标计划，明确企业设备、控制、网络、平台、应用和数据等的安全防护基本要求，强化企业自身防护，鼓励支持重点企业建设集中化安全态势感知和综合防护系统，提升网络和数据安全技术能力，开展对 PLC、SCADA 等重要系统的安全监测评估工作。安全是工业互联网发展的关键保障，电力生产监控网络安全又是工业互联网安全发展的重要组成部分。因此，电厂电力生产监控网络安全建设将是未来电力行业发展工业互联网、智慧电力的必然趋势。

**5、 安全风险和挑战**

云计算、人工智能、大数据、量子通信等数字技术的变革与发展，推动了网络攻防技术的快速更新迭代。勒索病毒、零日漏洞、数据泄露、社会工程已成为工业领域最为突出的攻击方式。当下，我国电力行业的电力生产监控网络安全防护水平普遍较弱，将无法应对外部和内部的数字安全风险。

### 2.4.2 典型安全问题

鲁布革水电厂电力生产监控网络和管理信息网络存在以下

主要安全问题:

**1、 生产控制区**

● 工作站未采取有效的主机防病毒措施，无法对病毒、木马和蠕虫等恶意

代码攻击进行技术防护和处理;

● 在安全访问控制方面，尚未根据分区分域原则设计部署有效的安全防护设备，

缺乏更有针对性的安全防护策略和安全机制;

● 缺乏对安全威胁和风险的入侵检测能力，无法对端口扫描、后门注入、DDoS、

缓冲区溢出等攻击行为进行及时检测与告警;

● 缺乏针对电力监控生产网络中网络流量和工控协议的安全审计能力，无法监

测工控网络攻击行为、异常流量并感知安全异常事件;

● 在上下级调度机构控制系统与电力调度数据网之间没有部署纵向加密设备，

无法保证生产环境数据在传输过程中的机密性、完整性和可用性;

● 没有有效的身份认证以及账号权限管理措施，无法对运维人员的操作行为进

行权限控制和操作行为审计，易造成账号密码泄露，带来安全隐患;

● 未对电力监控生产网络进行集中的安全管理，不能对网

络状况进行集中的监

控和对网络设备进行统一的管理。缺乏对安全事件识别、监测、分析、处置、响应的一体化运维能力，无法保障生产环境的业务可持续性运行，使得安全运维管理成本高、运维工作效率低。

**2、 管理信息区**

● 办公主机未采取有效的主机防病毒措施、无法对病毒、木马和蠕虫等恶意代

码攻击行为进行技术防护和处理;

● 缺乏对 USB 移动设备进行有效管控的技术手段，容易造成 USB 移动设备摆

渡之后造成的病毒、木马的传播扩散。

**2.4.3 安全解决方案**

1、 **主要解决的问题**

本方案涉及范围包括厂房监控系统和罗平集中控制系统，主要包括主机安全防护软件、工业防火墙、纵向加密、工控入侵检测、工控安全审计、运维安全审计、工控漏洞扫描、工业网络安全监测预警平台及附属等设备系统，并分别对厂房监控系统和罗平集中控制系统进行安全防护能力建设。

**（1）区域隔离与防护**

在监控系统的测量单元与工作站之间部署工业防火墙。通过部署工业防火墙，实现阻止来自区域之间的越权访问、入侵攻击和非法访问等，保护控制系统安全运行。实现横向逻辑隔离，将安全威胁和风险控制在有限范围内。

**（2）纵向加密认证**

在生产控制区与调度数据网的纵向连接处部署电力专用纵向加密认证网关或加密认证装置，为上下级调度机构或主站与子站端的控制系统之间的调度数据网通信提供双向身份认证、数据加密和访问控制服务。

**（3）网络入侵检测和恶意代码防范**

在生产控制区边界处旁路部署入侵检测设备，实时监控各种数据报文及来自网络外部或内部的多种攻击行为。在第一时间发现并阻止攻击和恶意破坏行为，同时形成日志报表，便于用户调查取证。入侵检测系统能够帮助安全管理人员及时发现威胁，扩展了管理人员的安全管理能力，可提高信息安全基础结构的完整性。通过在交换机上部署网络入侵检测系统，对关键的网络进行监控。

**（4）资产识别与漏洞闭环管理**

在生产控制区部署漏洞检测设备，能够及时发现上位机、服务器、控制设备、网络协议等的安全漏洞，及早发现潜在的安全隐患，并提供修补改进建议。漏洞检测系统能够帮助安全管理人员及时了解整个系统自身存在的脆弱性，便于及时采取相应的防护和应急响应手段。

**（5）主机安全防护**

在生产控制区上位机及服务器与管理信息区的主机上安装主机防护软件，监控分析应用程序和人工操作的行为特征，生成白名单。通过“白名单”阻止所有非法软件的执行，在没有杀毒

软件或杀毒软件更新不及时的环境下，病毒、蠕虫、木马等恶意程序依然无法执行。

**（6）网络安全审计**

在生产控制区的区域边界旁路部署工控网络监测与审计设备，收集全网工控设备流量，向工控安全管理平台集中汇报。统一收集网络日志，通过建模分析当前网络安全状态，为管理员提供可视化的操作行为、异常波动、告警信息等。

**（7）运维安全审计**

在管理信息区旁路部署堡垒机，接管数据库、网络等设备的登录，运维人员、第三方人员统一在堡垒机上操作。通过堡垒机进行权限分配、操作审计、进行合规性管理，对风险行为进行告警。

**（8）统一安全管理**

在生产控制区分别部署统一的安全管理平台，配合相关安全产品形成工控系统纵深防御体系。建立从网络边界到工业主机的立体式纵深防御体系，一是多处设防，避免单点被外部攻击后出现重大安全事件；二是集中管理，对全网安全策略和攻击事件进行统一管理。

**2、 技术架构与部署架构**

**（1）技术架构**

方案采用“平台+探针”的分层式技术架构。

**（2）部署架构**

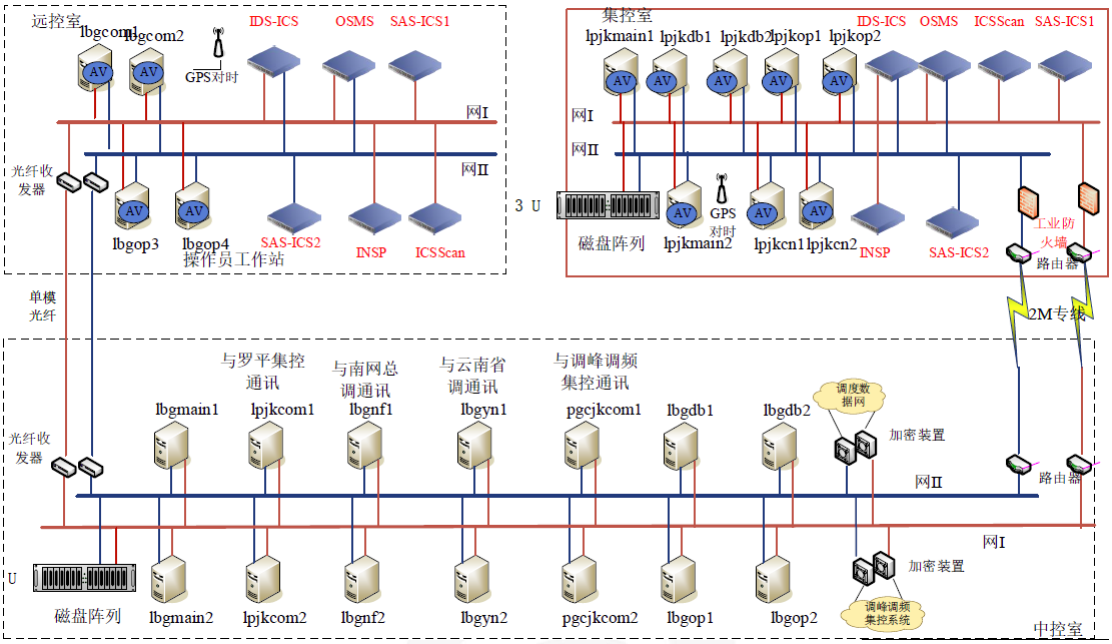


图 21　安全防护设计方案网络拓扑

（3）关键组件/模块、核心功能

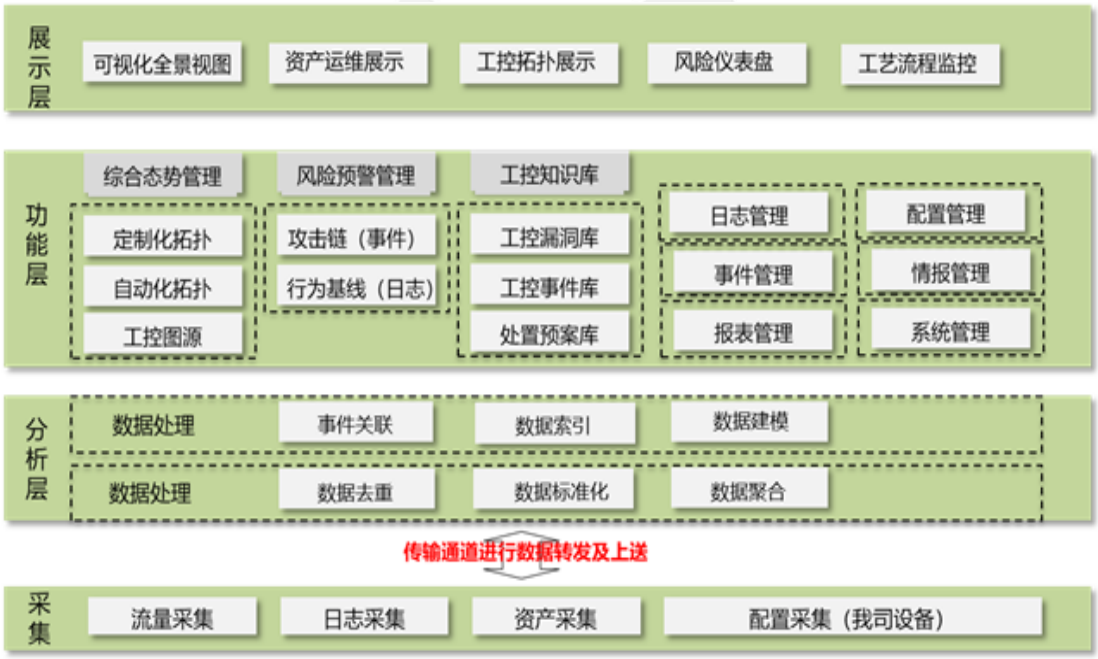


图 22　工业网络安全监测预警平台系统架构

● **数据采集层**：提供多种数据格式的接口，如 syslog、snmp 等协议格式，收集

工业网络中各类上位机服务器、工控终端、网络交换设备、

工控安全设备的日志信息和配置信息。

- **数据分析层**：对采集后的来自不同类型设备的日志、事件、配置信息进行集

中分析和处理。

- **系统功能层**：实现系统的应用功能的实现。包括基于工控网络拓扑的综合态

势管理、基于攻击链和业务行为基线的风险预警管理、基于工控事件库和处置预案库的工控知识库以及其他核心功能模块。

- **可视化展示层**：实现可视化的交互展示，包括工业网络风险全景视图，资产

运维监视视图，工控拓扑图，风险仪表盘等可视化模块。

**（4）方案的创新点、先进性、实用性、效益**

- **创新点**

**1）强大的分析引擎**

平台中预制关联分析引擎，对专项分析提供基础能力支撑，如风险分析、脆弱性分析、态势分析、资产分析、攻击链条分析等。分析引擎采用分布式设计，能够进行横向扩展，面对工业网络数据量时能够实现按需扩展，将分析引擎分散到其他更多的机器中，实现按需进行计算资源扩展。

**2）独有的数据强化技术**

提供一套简洁有效的日志统一分类机制，使用独有的技术将日志快速标准化，并基于安全分析需要进行数据的过滤和强化，丢弃无法用的噪音信息，提升日志查询和分析效率。

**3）“组态化”的配置模板**

提供基于组态的配置模板，针对客户的业务场景可以利用模板进行场景化配置，方便现场的操作人员对规则进行配置和使用，使用上贴合现场操作人员对工控系统的使用习惯。通过预制的设备类型和应用场景，用户无需关注具体的规则设备，只需要配置场景就可以实现在应用场景内的规则配置和应用。

**4）智能协议识别和辅助规则生成**

智能协议识别采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，通过对协议分布和流量信息的匹配，形成“网络流量行为基线”，帮助用户以最捷的方式了解和掌握网络中的业务通信状态，发现网络潜在的安全。智能化的流量自学习规则，还可以辅助系统自动生成相关的异常检测规则，对现有的规则进行调优等。

工业互联网产业联盟
Alliance of Industrial Internet

- **先进性**

**1）成熟的安全架构**

方案借鉴国际通用的 NIST CSF 安全能力框架，为用户构建从风险识别、安全防护、持续监测、安全响应和安全恢复的安全闭环能力。

**2）领先的安全理念**

打破传统的被动、静态式的边界安全防御理念，为客户重构主动、自适应的纵深安全防御体系，打造风险可视化、防御动态化和运行自动化的一体化安全能力。

**3）创新的安全技术**

方案中采用了较多的创新安全技术，例如人工智能算法、大数据分析模型、SOAR、威胁知识图谱、攻击链分析等技术，对攻击溯源分析和安全事件自动化处置提供了重要的技术基础。

- **实用性**

方案中涉及的核心产品均为绿盟自主设计研发，具有良好的自主可控性。在应用前全部通过严格的安全性测试和质量检测，以确保产品的高可靠性。为更好地满足客户场景化的安全建设需求，前期通过对电力生产监控环境的调研和分析，并对解决方案在该场景下的可用性、可靠性、安全性进行了充分的测试和验证。在实际的电力生产过程中，安全防护系统为电力生产监控网络提供了良好的安全保障作用，方案具有良好的实用性。

- **效益**

提升电力生产监控网络的安全运营能力，优化安全运维效率，降低安全运维成本，有效保障了电厂的可持续安全业务生产效益。

**（5）适用场景和对平台/软硬件的要求**

- **适用场景**

该方案非常成熟，可适用于离散、流程型工业领域的工业互联网厂内电力生产监控网络安全防护场景，包括电力、石油石化、智能制造、烟草制造、水务、机械加工等行业。

- **对平台/软硬件的要求**

平台软件系统可灵活适配于 X86 架构的服务器，其他探针类安全产品需满足工业生产环境要求。

### 2.4.4 小结

**1、 主要价值体现**

为电厂电力生产监控网络和管理信息网络建立集风险可视化、防御主动化、运行自动化的一体化安全能力，建立安全威胁感知和预警机制，完善纵深安全防御体系建设，提升安全运维效率。

**2、 方案的特点和优劣势**

**（1）合规性**

不仅满足等保 2.0 合规性和上级单位监管要求，同时也很好地开展、落实并践行了《工业互联网发展行动计划（2018-2020 年）》。

**（2）适用性**

方案不仅适用于电力生产监控网络场景下的安全防护体系建设，同时还可广泛应用到其它离散和流程工业领域。

**（3）创新性**

在《工业互联网创新发展行动计划（2021-2023 年）》中提倡的利用人工智能、大数据技术等创新能力强化网络安全技术保障能力方面，绿盟采用独特的人工智能算法、大数据分析模型、UEBA 和安全编排、自动化响应处置等关键创新技术，帮助电厂构建弹性可扩展、动态自适应的安全防护体系。

### 2.4.5 单位基本信息

绿盟科技是我国最早从事工控网络安全业务的企业之一，主要业务范围覆盖运营商、金融、政府、能源、交通、教育医疗等

垂直行业，产品主要覆盖网络安全、云安全、工业互联网安全、5G 安全、数据安全、零信任安全、威胁情报、安全态势感知等领域。

基于多年的安全研究，绿盟科技为用户提供检测防御类、安全评估类、安全平台类、安全 SaaS 服务、安全运营服务等 40 多款高品质安全产品。近二十年的发展历程中，抗拒绝服务攻击系统、漏洞扫描器、网络入侵防护系统、远程安全评估系统、Web 应用防火墙等多款产品，进入国际权威咨询机构报告，并连续多年位居细分市场第一。

在 2020 年，绿盟科技入选工信部 2020 年网络安全技术应用试点示范项目，同时获得工信部 2020 年网络安全威胁认定先进单位，2020 年度工业信息安全应急服务优秀支撑单位，工业信息安全监测预警网络建设 CICS-CERT 支撑单位，2020 年度国家工业信息安全漏洞库优秀成员单位，2020 年工业信息安全优秀应用案例，工业信息安全产业联盟 2020 年度优秀成员单位等荣誉。

## 2.5 案例五：智慧矿山工业互联网安全纵深防御体系建设

### 2.5.1 方案概述

近年来，随着“数字矿山”、“智慧矿山”等先进生产技术和生产模式的发展，煤炭行业与工业互联网的融合及促进已势不可挡。国家高度重视智慧矿山发展工作，2020 年 3 月，国家发展改革委，国家能源局等八部门联合印发《关于加快煤矿智能化发展的指导意见》，促进煤炭产业转型升级。

黄陵矿业集团有限责任公司（以下简称“黄陵矿业”）是陕西煤业化工集团所属大型现代化核心企业，位于陕西省延安市黄陵县店头镇，是国家“八五”重点建设项目，20 项兴陕工程之一。为了紧随国家战略，黄陵矿业进行自动化、智能化建设。随着建设的逐步开展，工业生产网络从封闭逐步走向开放，生产网、管理网、互联网越来越多地相互联通，网络的互通互联造成了生产网络规模越来越复杂，网络威胁和安全风险也在不断增加，发生网络安全事故造成的损失也越来越大。

奇安信集团依托自身强大的工业安全研发能力和多年的煤炭行业经验积累，帮助黄陵矿业构建外部威胁可控、内部风险可知的纵深安全防御体系，切实提高煤矿关键信息基础设施的网络安全防御能力。

### 2.5.2 典型安全问题

建设黄陵矿业工业控制系统安全运营中心，建成以一号煤矿、煤矸石电厂为试点的煤炭工控安全体系化、细粒度的集煤炭生产工控安全监控、安全管理、安全运营为一体的工业网络安全中心，全面感知黄陵矿业煤炭生产网络中工业安全风险、工控资产、网络漏洞、安全威胁、异常行为等安全状况，从网络安全风险管理的角度出发，将煤炭生产控制网络中的信息资产、网络设备、安全事件、威胁监控、应急响应等环节打通，形成了以“综合安全态势、工业安全态势、网络资产态势、资产漏洞态势、工业威胁态势、异常行为态势、网络监控态势”等 7 大态势模块实时安全监控和底层多类安全设备协同防御的纵深防御的网络安全体系。

该项目目标符合工业互联网创新发展行动计划（2021-2023 年）第 42 条要求:强化网络安全技术保障能力,强化企业自身防护,鼓励支持重点企业建设集中化安全态势感知和综合防护系统,提升网络和数据安全技术能力。

但是由于黄陵矿业网络互联互通、网络规模大、复杂程度高,它所面临的安全威胁是多层面、复杂多样的,主要安全威胁如下:

1、 **控制系统边界不清晰**: 生产控制系统类型较多，生产控制网络边界不清晰，缺乏边界隔离。

2、 **工业主机缺乏安全防护:** 重要工业主机系统陈旧，无法抵御病毒木马攻击。

3、 **移动介质缺乏有效管理:** 工业主机运维过程易出现移动介质病毒感染，缺乏有效管控工具和措施。

4、 **工控系统关键设备缺乏审计**: 缺乏针对工控系统违规操作、越权行为等审计能力。

根据黄陵矿业工业控制系统现阶段的安全现状,结合整体安全整改的必要性，设计智慧矿山工业互联网安全解决方案，实现边界防护、主机安全、监测审计、统一管理的目标。

### 2.5.3 安全解决方案

通过前期调研了解到，应对黄陵矿业进行边界防护、主机安全、监测审计、统一管理的安全防护，通过奇安信工业安全监测系统(ISD)、工业安全主机防护系统(IEP)、工业防火墙(ISG)、工业网闸（ISS）、工业安全态势感知平台（IMAS）等软、硬件组合方式，可以及时发现内部、外部、恶意代码、ATP 等攻击，

将安全风险降低到可控范围内，减少网络安全事件的发生，保护煤矿企业工控系统高效、稳定运行。

**1、 项目总体架构**

划分工控网络安全域，隔绝企业资源层、生产管理层、生产监控层的网络攻击；充分考虑网络审计和入侵检测技术对工控网络的重要性，实时监测工控网络内的异常流量及异常行为；对工业主机进行必要的安全防护工作，防止病毒和恶意攻击引起工业主机蓝屏宕机。具体方案如下：

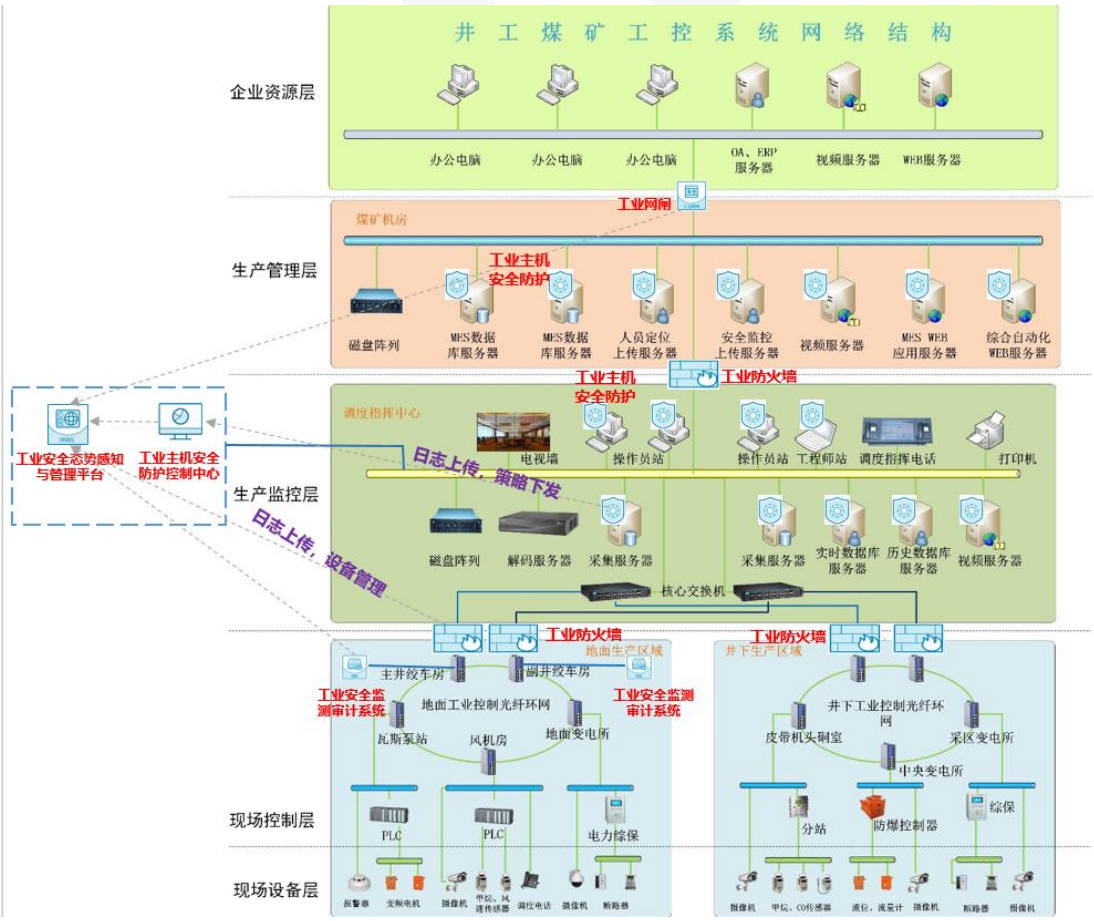


图 23　井工煤矿工控系统网络安全防护拓扑

（1）**物理隔离：**在黄陵矿业的生产网与办公网之间通过工业网闸实现物理隔离，采用“2+1”双主机+专用隔离模块的标准

网闸结构以及工业应用协议隔离技术实现企业网络和工业网络两个安全域之间访问控制、协议转换、内容过滤和信息交换;

**（2）主机防护+白名单：**针对煤炭控制系统主机，采用兼容工业应用软件的工业主机安全防护系统，利用白名单技术阻止控制系统遭到病毒木马和恶意攻击的威胁，确认无误后再接入控制网络。通过工业主机防护控制中心对工业主机终端进行集中策略配置、安全风险管控、终端版本推送、授权管理、以及终端单点维护和功能定制化;

**（3）安全隔离：**对井工煤矿工控系统的不同区域的边界采用工业防火墙进行安全隔离。通过深度解析多种工控协议，运用“白名单+智能学习”技术建立煤矿工控网络安全通信模型，阻断一切非法访问，仅允许可信的流量在网络上传输，达到对重要控制系统的安全保护目的;

**（4）安全监控与审计：**对工业环境的资产、异常行为、非法访问等通过工业安全监测系统进行集中监控和安全审计，实现区域内控制网络安全状况实时反馈，对外部入侵的行为进行告警，同时生成当前生产网络的行为日志和运行日志，便于安全事件的追溯和分析。

**（5）可视化呈现：**将工业环境的网络安全状态通过工业安全态势感知与管理平台进行“可视化”的呈现，全面提高该煤炭企业的工业安全防护的整体水平。

该防御体系的建立是采用工业网络安全领域的先进大数据分析技术、可视化技术、人工智能分析技术、态势感知技术等国

内领先的技术和手段，深入煤炭生产的实际业务场景，结合“智慧矿山”的技术发展路线进行业务安全场景的研究与应用，依靠现有的装备和技术升级促进煤炭生产方式根本性变革，为快速推进煤炭开采智能化、现场作业自动化、固定设施无人化、运营管理信息化提供重要的工业信息安全保障，为陕煤集团推进“智慧矿山”的最佳实践及国家工业互联网“新基建”建设提供重要的实践经验。

**2、 核心功能和技术指标**

本项目在智慧矿山行业背景下实现以下安全功能和技术指标:

**（1）一体化防护能力。**“关卡式”病毒拦截：可从入口进行外设管控、病毒防护、“永恒之蓝”漏洞防御，在运行时进行白名单管控和主机加固，病毒扩散时进行网络防护，从而进行一体化全方面安全防护。

**（2）资产分析管理能力。**“自助式”资产登记：进行硬件自动识别和编号、用户信息等资产自助登记，构建基于组织架构的资产风险管控体系，进行全局资产分析和安全管理。

**（3）集中运维管理能力。**“集中式” 运维管理：配置策略集中管理和日志、风险集中展示和分析，可以进行单机版、网络版、级联部署灵活部署，针对每个客户端可进行灵活的模块配置、权限配置、页面配置、扫描时间配置，满足工业主机现场定制化安全策略需求。

**（4）工业协议深度识别。**支持对 OPC、S7、Modbus、IEC104、

DNP3、FINS、BACNet 等多种工业协议报文深度达值域级解析，支持 100 种工业协议识别，支持工业协议合规性和畸形包检查。

**（5）白名单防护机制。**四重白名单防护体系，构建安全白环境；三段式运行模式，稳妥渐进实现安全防护；安全防护白名单自动生成、自动校验；白名单告警一键追加。

**（6）IT+OT 一体化防护更适应工业互联网。**具备 IT 防火墙网络层防护和应用层防护能力，具备完整的 AV、IPS 防护能力，且支持 HA、VPN 功能。

**（7）自动资产发现。**基于被动流量发现资产，支持多种厂商型号控制器，包括西门子，施耐德，罗克韦尔等。通过自动学习建立工控通信模型，形成资产白名单，监测非法设备接入。支持资产管理，可管理厂商名称、设备类型、设备型号、IP 地址、MAC 地址、使用协议、重要性等。

**（8）无损漏洞识别。**对识别后的资产进行脆弱性检查，包括资产所对应的漏洞信息、开放的端口和不安全的协议。其中漏洞识别支持 3 大漏洞库 CVE，CNVD，CNNVD，覆盖 220+厂商，3300+条漏洞。由于是被动的流量识别，相对于主动漏洞扫描的方式安全无损。

**（9）网络威胁检测。**系统内嵌 IDS 入侵检测引擎和 AV 反病毒引擎，实时检测工控系统网络中的威胁行为。IDS 引擎支持缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等。AV 引擎支持对传统 IT 协议中传输的文本、附件内容进行解析提取。对提取后的数据进行病毒扫描，支持的协议包括 HTTP、

FTP、SMTP、POP3、IMAP、SMB 等。

**（10）动态大屏展示。**为用户提供了大屏展示模块和仪表盘功能，提供全面实时的信息展示。从资产、协议流量、网络威胁等多个视角，结合实时曲线、动态占比、动态排行等显示模块，对工控系统网络安全状况进行直观展示。

**3、 项目先进性及创新点**

**（1）工业资产风险分析，提高运维效率。**工业主机安全防护系统能够基于工业资产进行全面梳理和安全防护，对生产网中主机进行安全风险分析和配置策略下发和集中管理，提升工业生产网安全运维便捷性，保证管理员对于工业主机安全风险第一时间进行处置和响应。

**（2）IT、OT 一体化防护。**针对工控网络中 IT、OT 流量进行全方位安全防护，通过应用识别、深度数据包解析以及一体化安全策略进行安全过滤，结合白名单、入侵防御、病毒检测等技术进行安全威胁检测和防护，保障工控网络安全。

**（3）以资产为中心。**工业安全监测系统通过资产自动识别、资产管理、资产网络关系图绘制，提供了以资产为中心的安全管理视角。工业生产流程比较固定，相较于以告警事件为中心的威胁分析方案，以资产为中心的漏洞发现与风险分析更符合工业环境管理习惯。级联无损部署方式，不影响生产。

**（4）多功能合一。**工业安全监测系统集流量审计、AV 检测、IDS 检测、白名单监测、工控关键操作监测引擎于一体，全面检测工业网络的病毒传播、入侵行为。兼备传统 IT 网络与工控网

络安全检测能力，适合 IT/OT 混合网络环境。同时满足合规要求和安全监测的要求。

通过基于工业主机防护、工业边界防护、工业安全监测、安全管理等安全机制，建立该矿业公司井工矿工业网络安全管理及态势感知的整体安全体系，能够有效监控该矿业公司工业系统的运行状态，实时监测和发现工业网络环境中的安全威胁，从而降低该企业工业安全风险。

该纵深防御解决方案基于典型的工业控制系统普渡模型进行设计，适用于工业互联网生产网企业内的安全建设，可形成智慧矿山场景的整体解决方案，符合工业互联网创新发展行动计划（2021-2023 年）第 34 条要求：培育领先企业。大力培育工业互联网技术创新企业，带动工业互联网关键技术和前沿创新能力整体提升。培育一批工业互联网系统解决方案供应商，面向重点行业与典型场景打造整体解决方案和集成技术产品。

**4、 下一步实施计划**

本方案的设计结合现行的国家政策法律法规、安全标准规范和该矿业公司的实际业务需求对安全集成工作进行细化和深化，同时综合未来 3-5 年安全规划的设计思路和保障体系框架编制而成，能够指导下一步安全建设工作。

该方案符合国家等级保护政策的思路和基本要求，并结合该矿业公司的实际情况，下一步计划为该企业工控系统信息安全项目建设、安全产品集成实施、安全管理体系文件编制和安全服务工作。

### 2.5.4 小结

奇安信为黄陵矿业建设的智慧矿山工业互联网安全纵深防御体系，能够有效监控黄陵煤矿集团工业系统的运行状态，实时监测和发现工业网络环境中的安全风险，提高安全防护能力，避免因工业网络安全攻击造成的损失，促进煤炭行业高质量发展。

该纵深安全防御体系的成功应用是新技术、新业态、新模式的最佳实践，为煤矿企业工业互联网安全建设树立行业标杆，具有良好的示范作用。

### 2.5.5 单位基本信息

奇安信科技集团股份有限公司（以下简称奇安信，股票代码688561）成立于2014年，专注于网络空间安全市场，为向政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，奇安信是2022年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商；此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

## 2.6 案例六：智慧水务典型安全解决方案

### 2.6.1 方案概述

某市级水务集团现拥有现代化水厂 8 座，实际最高日供水120万立方米，持续保障市区的用水需求。随着水务投资规模的增加，目前处于向智慧水务方向拓展的阶段。该水务集团公司开展了智慧水务建设项目，将其管辖的8家自来水厂实现统一的运

营管理、生产调度、状态监测、安全管理等功能。水厂网络与集团网络实现更高效的互联互通，随之，安全问题更加突出。为保障智慧水务安全稳定开展，水务集团启动“工业互联网信息安全防护”项目，针对下辖的所有水厂进行工业控制系统安全建设，保障关键信息基础设施的安全运行，完成工控系统网络安全备案、整改建设以及等级保护测评工作。

同时在信息化、智慧化建设的过程中，将网络安全建设与其业务场景结合，达成满足合规以及获得实际防护能力与安全管理能力的目标。北京启明星辰信息安全技术有限公司面向智慧水务场景下的安全需求，辅助用户将业务运行与安全防护有机融合。

### 2.6.2 典型安全问题

2020 年 4 月，以色列供水系统的网络攻击事件引起各国对供水设施遭受攻击和入侵的重视，美国国土安全部的统计显示：早在 2015 年，针对供水系统的网络攻击事件，就已经排入前三名，仅次于关键制造和能源行业。由此可见网络威胁已经向城市供水系统领域渗透，把水务工业控制系统作为攻击目标，为城市供水系统敲响了安全警钟。

该水务集团下的工业控制系统不仅用于监控水源、监控水处理过程、控制管道中的压力和流量以及供应成品的水，而且执行数据记录、报警和诊断功能，保障大型、复杂的水务过程系统的持续运营。现有的工业自动化控制系统在设计、研发中没有充分考虑安全问题，在部署、运维中又缺乏安全意识、管理、流程、策略与相关专业技术的支撑，导致供水、排水系统存在着诸多安

全问题，一旦被无意或恶意利用就会造成各种信息安全事件。供水、排水调度工业自动化控制系统的安全直接关系到“生命线”安全。

该水务集团股份有限公司建设面临的工业信息安全风险主要有以下 3 个方面：

**（1）安全防护水平相对落后**

下辖各个公司的供水调度、排水工业控制系统普遍存在安全漏洞，缺乏有效的安全配置策略，外网边界易被突破；企业内网边界访问控制管理薄弱，安全防护设备严重缺乏；工控设备开启高风险远程访问服务现象普遍，存在高危风险隐患；工控系统主机安全防护措施较弱，控制权限易被远程获取，会引起病毒感染与扩散、生产中断等风险。

**（2）网络攻击风险持续加剧**

供水调度、排水工业控制系统采用大量的 IT 技术，互联性逐步加强，工业控制信息安全日益进入黑客的研究范围，国内外大型的信息安全交流会议已经把工业控制信息安全作为一个重要的讨论议题。随着黑客的攻击技术不断进步，攻击的手段日趋多样，入侵到某个系统，成功破坏其完整性成为可能；工业控制系统普遍缺乏网络准入和控制机制，上位机与下位机通讯缺乏身份鉴别和认证机制，只要能够从协议层面跟下位机建立连接，既可以对下位机进行修改，普遍缺乏限制系统最高权限的限制，高权限账号往往掌握着数据库和业务系统的命脉，任何一个操作都可能导致数据的修改和泄露。

**（3）安全管理机制尚待健全**

工作人员对工业控制系统信息安全的重视不够，工控安全责任意识、风险意识不足，管理制度不健全，相关标准规范缺失，技术防护措施不到位，安全防护能力和应急处置能力不高，需要形成常态的安全运营机制，定期进行事件分析、安全运维、安全培训等。

### 2.6.3 安全解决方案

本解决方案中的智慧水务业务场景包含智慧水务平台、自来水厂生产系统两大部分。安全建设也依据其业务场景进行设计实施，解决方案总体框架如下图所示：

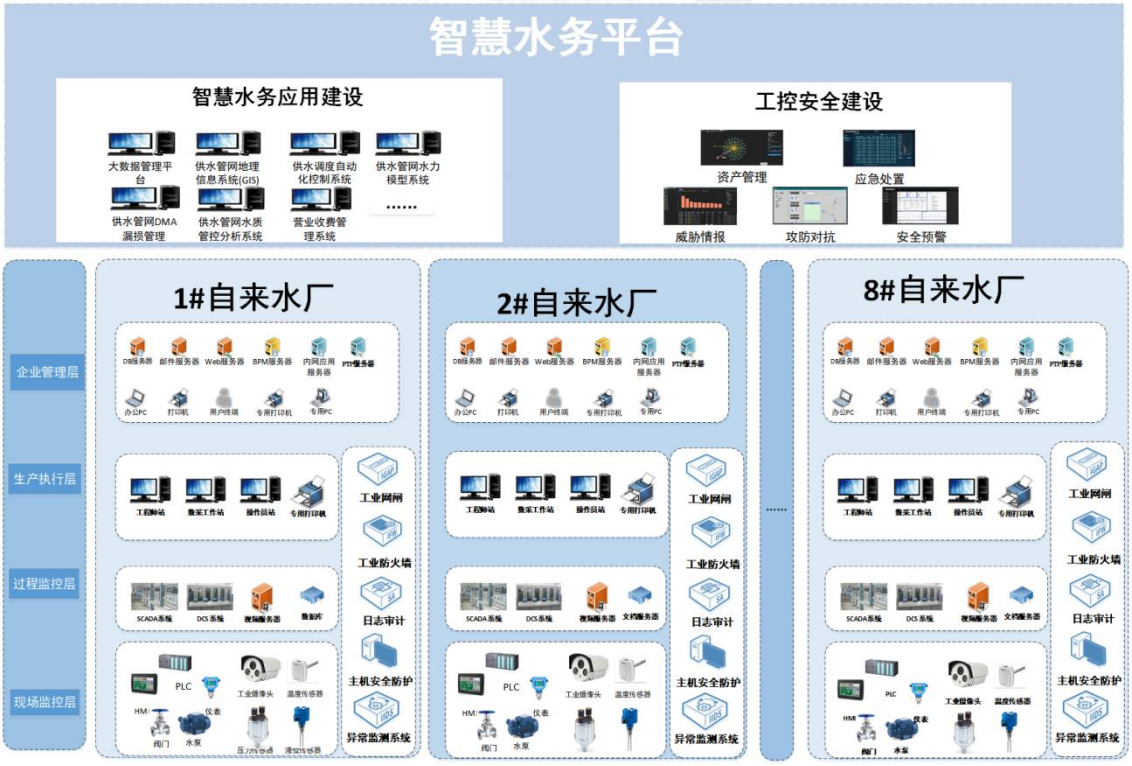


图 24　智慧水务总体框架示意图

智慧水务平台是依托云架构的物联网水务平台，平台包含大数据管理平台、供水管网地理信息系统(GIS)、供水调度自动化

控制系统(SCADA)、供水管网水力模型系统、供水管网 DMA 漏损管理、供水管网水质管控分析系统、营业收费管理系统。可对 8 个自来水厂实现云端管控、任务处理、数据存用、任务下发、业务监测等功能。

集团下辖 8 个自来水厂的工艺流程基本相同，从智慧水务工业控制系统的环境特点、技术特点、协议特点角度分析，大型自来水厂多数采用的处理工艺一般是常规处理加深度处理，工艺复杂，设备先进。常规处理包括：混合、反应、沉淀、过滤及消毒几个过程。深度水处理工艺在常规水处理工艺的基础上添加了臭氧处理和碳过滤或投加高锰酸钾和粉末活性炭等工艺流程。如下图 2 为臭氧处理加碳过滤的深度处理工艺流程。

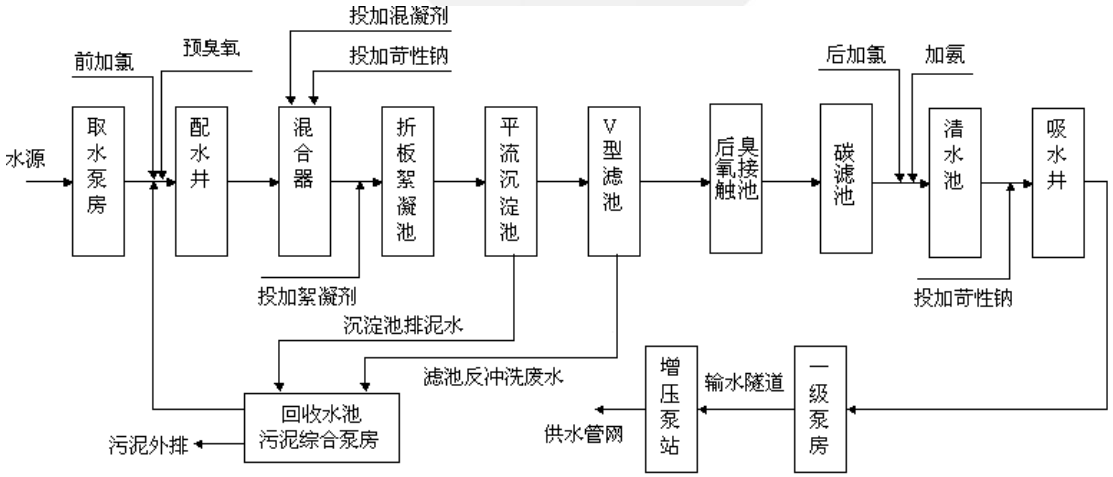


**图 25　自来水厂深度处理工艺流程图**

从现场调研的工艺流程分析来看，整个大型自来水厂工艺流程包含的现场控制层设备分为机械设备和控制设备，机械设备一般有几十种，例如鼓风机、提升泵、刮泥机、加压泵、臭氧制备机、回流泵、加药泵、搅拌机等。这些设备都是工艺处理环节中

的关键设备。控制设备比如现场控制层的 PLC，仪器仪表，RTU 等，监控层有上位机组态软件、工业数据库、网络摄像头等。

生产系统由企业管理层、生产执行层、过程监控层、现场监控层组成，分别承担以下任务:

- **企业管理层:** 负责监控各个水厂工艺流程的实时监控、生产调度、数据分析

等功能，涉及水管网地理信息系统(GIS)、供水调度自动化控制系统(SCADA)、供水管网水质管控分析系统等系统，设备类型以传统服务器以及传统信息系统为主，企业管理层同时承担为水务集团总部传送业务数据的功能，实现上下级平台联动。

- **生产执行层:** 负责对各工艺流程的具体生产活动下发执行指令，其中包括操

作员站、数采工作站、上位机等设备，以工作站设备为主。

- **过程监控层:** 负责对自来水生产流程以及厂区环境数据进行监控以及数据采

集。主要包括 SCADA 系统、DCS 系统、视频监控服务器等。

- **现场监控层:** 负责执行具体生产指令以及收集数据。具体设备包括 PLC、温

度传感器、压力传感器、液位传感器、工业摄像头等终端设备。

水厂的生产数据包含流量，液位，压力，浊度等，生产数据均汇聚到水务集团办公网的集中控制中心的智慧水务平台进行分析处理。经过对客户的业务场景梳理、分析，本方案针对边缘

安全防护场景、企业安全防护场景和企业安全综合管理平台三个安全场景提供解决措施。分别针对不同安全需求和风险，部署安全措施：

智慧水务平台侧通过应用威胁情报分析、异常流量监测、资产安全威胁预警、网络攻击预测等技术实现智能化、智慧化的安全管理，保障智慧水务系统安全稳定运行。

自来水厂工控系统通过实施分层分域安全策略，部署工业防火墙、工业主机防护系统、工业入侵防御系统等，从终端管控、主机防护、平台管理、跨网跨域防护等角度保障设备安全，控制安全和边缘测的网络安全。

本解决方案依据工业互联网体系架构 2.0 的思路与方法，从业务视图、功能架构、实施框架及技术体系四个维度解决现阶段面临的最主要的安全问题，同时结合水务行业工业系统的环境特点及最新的工业安全标准与技术，方案设计拓扑如下图所示：

工业互联网产业联盟
Alliance of Industrial Internet

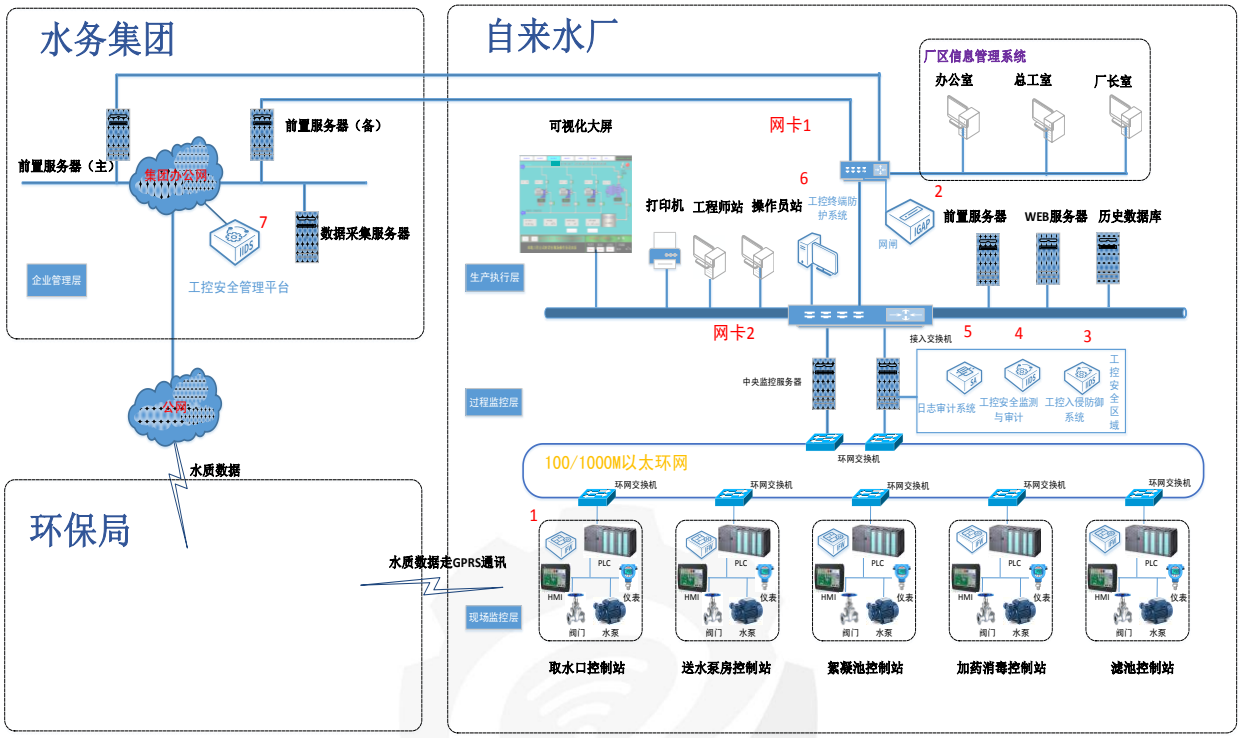


图 26　水厂等级保护建设规划拓扑

本解决方案在智慧水务项目建设背景下实现以下场景化防护效果:

**1、 基于生产控制系统安全稳定运行场景效果**

按照工艺流程以工控子系统为防护对象，分成取水口控制站、送水泵房控制

站、絮凝池控制站、加药消毒控制站、滤池控制站等安全域，以“域间隔离，统一监测”为防护策略，采取安全措施如下:

**（1）边界防护：**在厂区安全域之间采用适用于工业环境的专用防火墙以逻

辑串接的方式进行部署，对安全域边界进行监视，识别边界上的入侵行为并进行有效阻断。通过工业协议的深度识别与过滤，实现了从边界、区域到终端的完整防护，降低了网络被入侵及安全威胁迁移扩散的风险。

**（2）入侵防护+安全策略：**在工控环网与生产执行层的接口处部署入侵防御系统，结合行业定制化安全策略，提供工控信息安全特色场景化的防护。通过对设备固件进行安全增强，识别并阻断该高危端口扩散，预防攻击传播风险。例如：从水务集团下辖的某自来水厂服务器在运作过程中发现异常，不断向外部发送大量的 445 端口数据包，且在枚举内网及互联网 IP 地址，并发起攻击传播行为，从此现象出发为防范水务集团之前遭遇恶意攻击的问题再次出现，采用规避技术手段防止扩散、及时止损，现采用水务行业工控信息安全特色场景化的入侵防御系统，已经识别并阻断该高危端口扩散，阻断 5 万多次攻击。

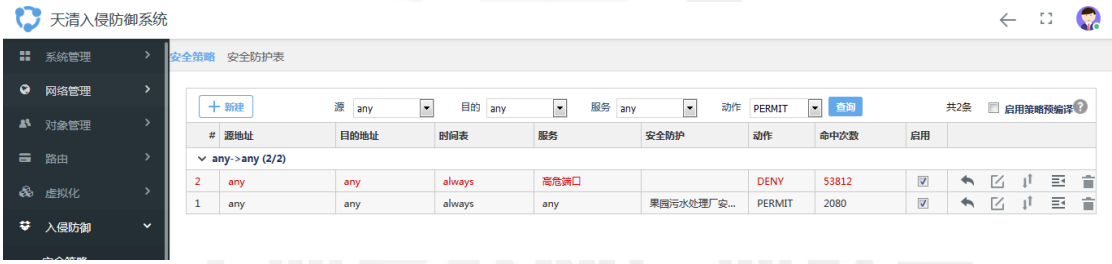


图 27　入侵防御系统阻断 5 万多次攻击

**（3）异常监测+安全审计：**在工控环网与生产执行层的接口处部署异常监测与审计系统，对工控网络敏感指令数据进行记录和异常检测。可检测工控网络中发生的入侵攻击，实时监测工控网络中的敏感操控，实现故障与异常的预警。

**（4）保障工控系统日志集中管理：**通过旁路部署日志审计系统，将网络中存在的网络设备、操作系统、数据库系统、安全设备等产生的日志信息统一存储、分析、告警。解决水务集团现有工控系统中日志存储分散，不利于统一管理，同时对于数据存储时间、维度没有进行统一管理的问题。

**2、 基于集团网络与水厂网络安全互联场景效果**

自来水厂生产数据安全可靠上传，避免形成安全风险暴露点，影响水厂工控系统和智慧水务平台的安全稳定运行。采取如下措施：

**（1）主机防护+白名单：**在设备层和边缘层上部署主机防护系统，制定白

名单安全策略，从源头上遏制了恶意代码的运行，消除病毒或恶意代码通过终端外设进入工控终端及工控生产网络的可能性。从操作系统内核、协议栈等方面进行安全增强，并力争实现对于设备固件的自主可控。

**（2）边界防护：**在集团办公网与下属水厂边界部署工业加固型网闸，对两

网间的数据交换进行安全防护，同时对 OPC、Modbus/TCP 等工业协议进行深度解析和指令级的控制，保证只允许合法的指令和访问通过。

**3、 基于智慧水务的安全管理平台场景效果**

采用智慧水务安全管理平台对系统运行状态进行监控，对安全日志集中存储。可对网络中所有的工作站，服务器，工业设备，网络设备，安全设备进行资产管理，拓扑管理，性能管理，日志管理等，满足等级保护三级中统一管理，集中存储的相关要求。为用户提供了大屏展示，提供全面实时的信息展示。从资产、协议流量、网络威胁等多个维度进行直观展示。从数据的采集、数据存储到数据分析展现都应用了大量的大数据处理分析技术。可

以应对不同用户环境对海量安全信息数据的高速处理场景，并通过分析结果和可视化效果向用户呈现全网的态势感知。

智慧水务安全管理平台以业务信息系统安全为保障目标，从监控、审计、风险、运维四个维度对全网的整体安全进行集中化的管理与运维，为用户建立起了一个可视、可查、可度量与可持续的安全管理新平台。

**图 28　四维一体的智慧水务安全管理与运维**

工业互联网产业联盟
Alliance of Industrial Internet

借助智慧水务安全管理平台，可获得对网络安全的可视化，洞悉业务信息系统的运行状况与安全状况；可以对网络的安全事件进行综合分析与审计，识别和定位外部攻击、内部违规；可以进行业务系统的安全风险度量、安全态势度量和安全管理建设水平度量；可以进行持续的安全巡检、应急响应与知识积累，不断提升安全管理的能力。应用效果如下图所示：

图 29　工控安全管理平台大屏展示

### 2.6.4 小结

本解决方案从智慧水务下关键基础设施面临的安全挑战入手，给出了针对性的场景化安全防护应对措施。实现水务集团内部工控网络安全风险细粒度管控，健全了企业工控网络安全管理体系，提高了企业内部威胁监测能力，打造出以水务行业专属入侵监测系统为核心的特色安全框架，为智慧水务工控信息安全赋能。该解决方案以启明星辰安全厂商做技术支撑，充分利用该水务集团股份有限公司工业控制系统的特点不断动态调整防护的重点和优先级，迈出了水务行业工控安全建设的第一步。

### 2.6.5 单位基本信息

启明星辰信息技术集团股份有限公司成立于 1996 年，是国内极具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。目前，启明星辰已对网御星云、杭州合众、书生电子、赛博兴安进行了全资收购，自此，集团成功实现了对网络安全、数据安全、应用

业务安全等多领域的覆盖，形成了信息安全产业生态圈。集团总部位于北京市中关村软件园启明星辰大厦，在全国各省市、自治区设立分、子公司及办事处三十多个。

启明星辰集团在 2013 年就启动工控安全研究，参与包括等保 2.0 在内的工业互联网相关国家标准、行业标准近 20 个，2015 年发布工业互联网安全产品体系。近年来通过先进制造、石油石化、电力、冶金等行业建设实践，已有超千个工业互联网安全行业应用案例，在 2019 年工业互联网安全营业额达 2 个亿。

## 2.7 案例七：工业 5G 边缘计算平台安全解决方案

### 2.7.1 方案概述

中国移动工业 5G 边缘计算平台是集宏量异构工业设备接入、海量数据实施处理、多态智能计算和多行业应用平行扩展特征的综合性系统平台。为保证平台整体安全的完备性、广泛的可移植性和适用性，采用的安全方案设计原则是：保持与研发生命期同步，基于复杂系统的功能有机分解而有序分析风险，采用标准化的安全协议、安全基线或普遍应用的最佳实践。平台融合的安全体系或架构主要包括 5G 网络安全、虚拟化平台安全、容器安全、外部通信安全、内部服务调用安全、系统或组件级的原生安全和高可用架构等。

### 2.7.2 典型安全问题

经过对平台资产识别、运行逻辑分析和威胁分析后，得出如下的平台安全风险：

# 表 1　平台安全风险信息表

| 序号 | 风险 | 危害 | 等级 | 控制策略 |
|---|---|---|---|---|
| 1 | 边缘侧与服务侧通信消息被非法篡改 | 边缘侧发送、接收的消息用于一切业务关联的计算和设备驱动，此风险破坏数据完整性和真实性，导致服务侧的业务能力失效或设备驱动失效。 | 高 | 1、边缘侧网关与服务侧网关内集成 SSL 协议，保护上层消息的完整性；2、安全维护边缘侧与服务侧网关的安全。 |
| 2 | 边缘侧与服务侧通信消息被非法窃听 | 边缘侧发送的消息包含生产性秘密数据或用户隐私数据，此风险破坏数据的机密性，导致技术秘密或用户隐私泄漏，进而产生违规违法后果。 | 高 | 1、边缘侧网关与服务侧网关内集成 SSL 协议，保护上层消息的机密性；2、安全维护边缘侧与服务侧网关的安全。 |
| 3 | 对边缘侧、服务计算侧各系统的攻击性访问 | 非法访问边缘侧、服务计算侧并破坏系统的配置文件、软件模块等的机密性、完整性，进而导致系统不可用、业务能力失效。 | 高 | 1、对边缘侧、服务侧的各系统的管理访问经过统一访问点的认证和授权；2、与系统开发同步执行安全需求、安全设计、安全实施和安全测试和安全运维，其中特别关注系统访问控制模块和日志模块。 |
| 4 | 非法现场设备接入 5G 网传输虚假信令或数据 | 非法设备向边缘侧发送虚假数据、或信令洪范攻击，导致系统不可用、业务能力失效。 | 高 | 1、完全启用 5G 的订阅者隐私保护；2、完全启用 5G 的安全机制。 |
| 5 | 设备与边缘侧之间的通信消息被非法篡改 | 设备侧发送采集数据、接收驱动消息，此风险破坏数据完整性和真实性，导致最终服务侧的业务能力失效或设备驱动失效。 | 高 | 1、如果设备支持安全协议，则在设备与边缘网关内启用 SSL 协议，保护上层消息的完整性；如果设备不支持安全协议，则在设备和边缘网关内集成应用层安全协议保护消息内容；2、完全启用 5G 的安全机制。 |
| 6 | 设备与边缘侧之间的通信消息被非法窃听 | 设备侧发送采集数据、接收驱动消息，此风险破坏数据机密性，导致技术秘密或用户隐私泄漏，进而产生违规违法后果。 | 高 | 1、如果设备支持安全协议，则在设备与边缘网关内启用 SSL 协议，保护上层消息的机密性；如果设备不支持安全协议，则在设备和边缘网关内集成应用层安全协议保护消息内容；2、完全启用 5G 的安全机制。 |

| 序号 | 风险 | 危害 | 等级 | 控制策略 |
|---|---|---|---|---|
| 7 | 能力开放接口缺乏对访问主体的认证和授权 | 此风险会无条件接收服务请求并响应，导致错误发送或接收消息而破坏平台数据机密性或数据完整性，也可能成为更多网络攻击的通道。 | 高 | 1、设计平台能力的授权访问机制; 2、安全设计服务接口，拒绝对内部系统的直接访问。 |
| 8 | 边缘侧内各服务之间的调用缺乏鉴权 | 此风险会破坏边缘侧内部数据机密性或数据完整性，也可能成为更多内部系统攻击的通道。 | 中 | 1、设计内部服务的授权访问机制。 |
| 9 | 服务计算侧各服务之间的调用缺乏鉴权 | 此风险会破坏服务侧内部数据机密性或数据完整性，也可能成为更多内部系统攻击的通道。 | 中 | 1、设计内部服务的授权访问机制。 |
| 10 | 边缘侧数据处理容量低 | 设备侧可能发送高频度、大尺寸的实时数据，边缘侧不能及时处理可能导致数据丢失，而引发业务功能失效。 | 中 | 1、在边缘侧设计高容量、高性能的数据接收、存储、处理架构。 |
| 11 | 服务计算侧数据处理容量低 | 边缘侧可能发送高频度、大尺寸的实时数据，服务侧不能及时处理可能导致数据丢失，而引发业务功能失效。 | 中 | 1、在服务侧设计高容量、高性能的数据接收、存储、处理架构。 |

工业互联网产业联盟
Alliance of Industrial Internet

### 2.7.3 安全解决方案

#### 1、 平台逻辑架构

平台分为边缘网关、平台两大部分，边缘网关（网关服务系统）分为四层:设备服务层、核心服务层、支持服务层、输出服务层,还包括安全服务及管理服务,边缘侧主要实现数据的接入、处理、输出。平台侧主要包括设备监控模块、设备管理模块、数据管理模块、服务编排模块、应用管理、系统管理模块。

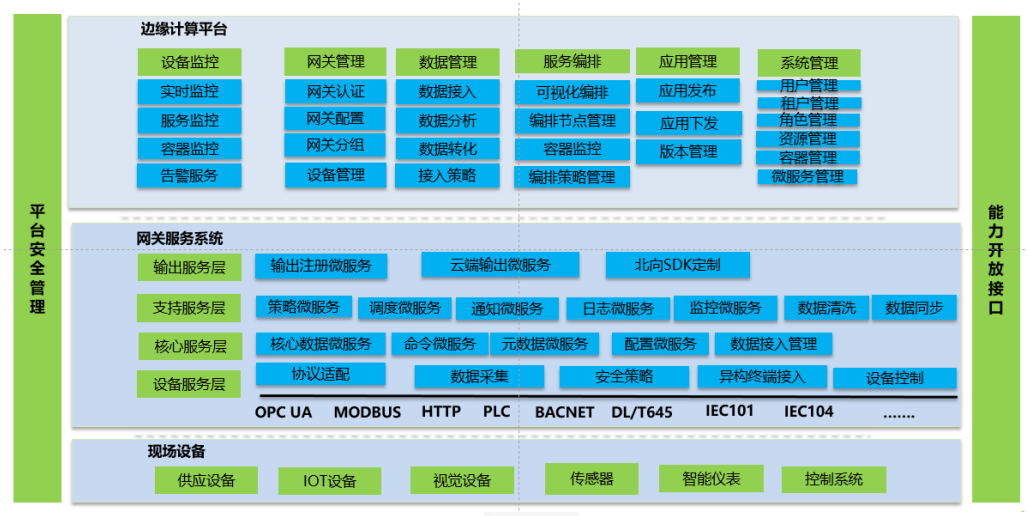


图 30　平台整体结构

网关接入平台需向平台发送接入认证消息及网关自身的信息，平台处理接收接入数据采用 mqtt 通讯方式，平台采用 mqtt server 集群进行数据接收，采用分布式接入服务集群进行数据处理与入库操作。

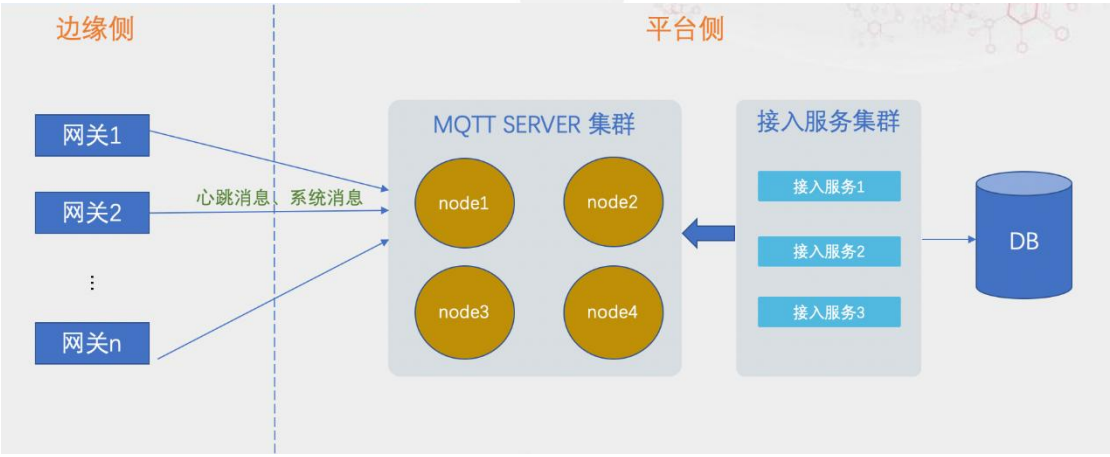


图 31　网关接入

- **平台已应用的项目**

东方电气 5G 风电数采项目：将发电机组 PLC 的数据通过边缘网关采集后，通过在边缘网关部署相应的算法，在边缘网关侧做本地边缘计算后，在本地直接进行机组参数调整，再将一些相

关的数据传回到中心。

**2、 风险控制方法与设计描述**

**（1）边缘侧与服务侧通信消息被非法篡改、边缘侧与服务侧通信消息被非法窃听的风险控制方法：**

在边缘侧和服务侧分别集成 SSL 网关（TLS 最新版本），在边缘侧和服务侧之间建立安全隧道。SSL 网关是 SSL 协议的终结点，对边缘侧和服务侧内部系统透明。SSL 协议基于预共享秘密执行握手认证建立安全连接，并协商会话密钥保护后续传输数据的机密性和完整性。

SSL 预共享密钥工程要求：128 比特，有效期 1 年，在 SSL 网管内安全存储。密钥生成工程选择：使用专门密码机生成；或利用算法 HASH256（rand，onetime-password）生成。

SSL 安全网关的工程选项：若边缘侧与服务侧集中部署于同一网段，且具备足够的物理安全和系统运维安全时，可取消 SSL 网关。

**（2）对边缘侧、服务计算侧各系统的攻击性访问的风险控制方法：**

- **平台内安全方案：**

1）各系统同步执行安全需求分析、系统级威胁建模，安全设计、安全实施和安全测试和安全运维，每一个系统必须集成访问控制模块和日志模块，其中访问控制模块：人机交互访问基于

角色控制，采用“口令+验证码”双因素认证，程序间的服务交互采用的统一接口结构是 ServiceNameRequest(token, other_parameters),其中 token 是平台统一采用的 OAuth2.0 令牌。

2）基于“业务运行恰当运行环境”原则配置每一个系统纵深各软件层的安全基线。

- **平台外安全方案：**部署 AAA 统一运维管理访问接口。

**（3)非法现场设备接入 5G 网传输虚假信令或数据的风险控制方法：**

- 针对 3GPP 接入的现场设备,采用集成归属网公钥的 SIM 卡，启用 SUCI 身

份保护;

- 针对 non-3GPP 接入的现场设备,由非 3GPP 接入网关(例如 CPE）启用可

用的设备接入认证;

- 无论是 3GPP 接入还是 non-3GPP 接入设备,均统一启用 5G 非接入层安全认

证，具体安全机制遵循中国移动 5G 网安全设置;

- 制定物理安全管理制度，保护现场设备和非 3GPP 接入网关的物理安全。

**（4）设备与边缘侧之间的通信消息被非法篡改、设备与边缘侧之间的通信消息被非法窃听的风险控制方法：**

- **非 5G 安全方案：**

1)如果设备支持安全协议，则在设备与边缘网关内启用 SSL 协议，保护上层消息的完整性； 在边缘侧和服务侧分别集成 SSL 网关（TLS 最新版本），在边缘侧和服务侧之间建立安全隧道。SSL 网关是 SSL 协议的终结点，对边缘侧和服务侧内部系统透明。SSL 协议基于预共享秘密执行握手认证建立安全连接，并协商会话密钥保护后续传输数据的机密性和完整性。SSL 预共享密钥工程要求：128 比特，有效期 1 年，在 SSL 网管内安全存储。密钥生成工程选择:使用专门密码机生成;或利用算法 HASH256(rand，onetime-password）生成。

2)如果设备不支持安全协议，则在设备和边缘网关内集成应用层安全协议（EAP-PSK）保护消息内容。具体加密逻辑如下:

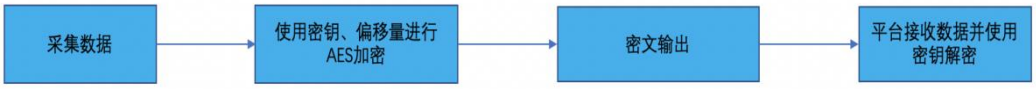


图 32　加密逻辑

- **5G 安全方案:**

无论是 3GPP 接入还是 non-3GPP 接入设备，均统一启用 5G 非接入层安全认证和密钥协商机制，利用生成的接入层密钥保护消息机密性和完整性。具体安全机制遵循中国移动 5G 网安全设置。

**5、能力开放接口缺乏对访问主体的认证和授权的风险控制方法:**

能力开放接口设计为整个平台对外服务的唯一通道，接口内集成相对独立的服务访问认证授权模块（EAP-PSK），认证过程协

商访问密钥，访问密钥构造访问令牌 token，token = (ID, service-name, HMAC(ID,service-name))，token 是服务访问的参数。EAP-PSK 的认证建立通信状态逻辑如下:

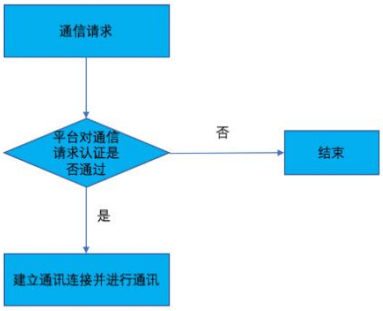


图 33　建立通信状态逻辑

**6、边缘侧内各服务之间的调用缺乏鉴权、服务计算侧各服务之间的调用缺乏鉴权的风险控制方法:**

服务调用采用的统一接口结构是 ServiceNameRequest(token, other_parameters),其中 token 是平台统一采用的 OAuth2.0 令牌。

**7、边缘侧数据处理容量低、服务计算侧数据处理容量低的风险控制方法:**

如下图所示，边缘侧采用多网关并行计算、结合高容量数据缓存保证边缘侧数据不丢失。模式通过协议适配采集边缘工业设备及传感器数据，平台采用 mqtt server 集群接收网关上报的采集数据，采用分布式数据接收服务集群处理 mqtt 数据后转发至 Kafka 集群，Clickhouse 集群接收 kafka 数据并存储。具体工程中有架构师设计详细的数据缓存和网关并发机制。

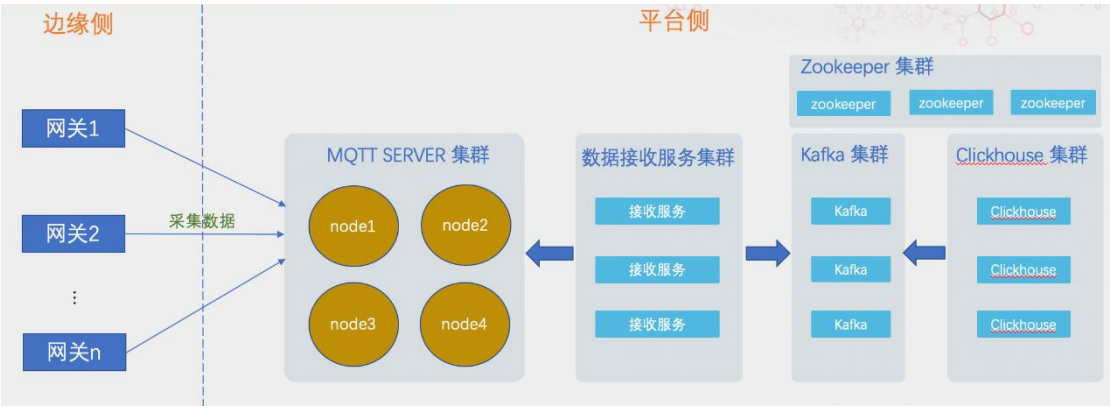


图 34　风险控制方法

### 2.7.4 小结

数据采集基础系统能够在靠近用户或数据源的位置提供网络、计算、存储服务，不仅能够实现流量的本地化处理，降低对传输网络和元断数据中心的流量冲击；而且能够提供低时延和高稳定的应用运行环境，有利于计算框架在终端和数据中心间的延展，有助于实现场景需求、算力分布和部署成本的最佳匹配。

在工业领域，数据采集基础系统能够帮助解决工业制造大融合下的分工，即 OICT 的融合；在智慧城市/交通/医疗等领域，数据采集基础系统解决了边缘层异构模型融合，实现了各类高效边缘智能化应用；在消费领域，数据采集基础系统通过网络，安全，边缘智能等手段渗入生产消费各个环节，将市场消费体系带入了新零售阶段。

数据采集基础系统包含网关服务系统和数据采集系统管理平台，分别部署于网关和云端，提供业务场景的全方位服务支持。

### 2.7.5 单位基本信息

中移(上海)信息通信科技有限公司(中移上海产业研究院，简称中移上研院)是中国移动通信集团落实央地融合，在沪设立

的全资子公司，是中国移动 5G 应用创新中心，是中国移动面向智慧交通、工业能源、金融科技等行业提供产品和解决方案的研发运营支撑一体化的科创公司。公司以 5G 发展为契机，结合新一代信息技术以及中国移动各方面优势，依托上海“五个中心”建设，发挥长三角地区经济发展和信息通信产业优势，辐射全国，通过 5G 赋能行业实现协同发展、融合创新、生态共建。

## 2.8 案例八：大型排水集团生产控制系统安全解决方案

### 2.8.1 方案概述

水是人类生命的源泉，科学用水和排水是人类社会发展史上最重要的社会活动和生产活动内容之一，特别是现代，随着城市化进程的加快，给水排水工程已经发展成为城市建设和工业生产的重要基础设施，成为人类健康安全和工农业科技与生产发展的基础保障，城市给水排水系统的安全运行，对于保障城市安全运营至关重要，是城市、国家安全的重要组成部分。

某大型排水集团（以下简称“排水集团”）承担着所在城市防汛、污水处理、再生水生产利用以及污泥处理的重大责任，下属有多个再生水厂、多个分公司管理近百个泵站生产控制系统，当前排水集团下属再生水厂及分公司生产控制系统存在较大的安全风险，具体表现为：区域边界未采用专用安全系统进行边界隔离，承载业务系统的工控主机未进行安全防护以及核心控制设备在无任何防护措施的情况下运行，这些安全风险一旦被利用，直接影响排水集团关键业务系统的正常运行，将会给企业自身以及城市的安全运营带来严重的影响。

### 2.8.2 典型安全问题

经过前期的调研发现，排水集团生产控制系统存在以下安全风险：

**1、 安全区域边界风险**

排水集团生产控制系统及下属再生水厂、分公司网络边界未采取任何安全防护措施，一旦局部网络节点发生病毒感染，将会直接影响整个排水集团生产控制系统；下属再生水场、分公司内部未进行安全域划分，存在多个网络攻击途径；

**2、 安全通信网络风险**

对核心控制设备由外部和内部发起的误操作甚至恶意操作行为无任何感知和防御措施；

**3、 安全计算环境风险**

下属再生水厂及分公司的生产控制系统中的工程师站/操作员站/服务器等均

为 windows 平台，考虑到业务的连续性、稳定性等因素，工控主机操作系统均未及时的更新补丁，存在较多安全漏洞；工控主机未安装恶意代码防范软件，存在带病运行的情况；

**4、 安全管理风险**

企业网络安全意识薄弱，无论是企业管理人员还是技术人员，普遍缺乏工业

控制网络安全防护所需的专业知识，缺少有效的安全防护管理机制。

### 2.8.3 安全解决方案

#### 1、 建设目标

排水集团生产控制系统高度依赖工业控制系统来实现自动化作业，生产控制系统信息安全问题日益突出，安全建设任务更加紧迫，由于行业的特殊性，必须设计并建设一套技术先进、安全高效、可靠可控的生产控制系统，确保排水生产控制系统的安全运行，通过本方案安全建设实现以下目标:

**（1）提高生产控制系统基础设施安全防护能力**

通过强化生产控制系统中基础设施的安全防护，建立基于“动态行为白名单”的工业互联网端点安全防护技术体系，使得生产控制系统的基础设施能够抵抗从外部、内部发起的网络攻击，确保生产控制系统安全运行。

**（2）建立一套基于业务的整体综合保障体系**

立足于生产控制系统业务流程，利用先进的安全防护技术手段，从管理机构、

管理制度、安全运维、应急处置、安全教育等方面出发，建立一套排水集团整体安全保障体系，一旦发生任何安全事件，能够更及时、准确、有效的解决安全事件，将安全事件带来的影响降到最低。

**（3）提高生产控制系统综合防护能力**

通过集中整合、分析排水集团内部厂区的设备资产、网络流量、安全漏洞、

安全配置、安全日志、设备运行状态、业务故障日志等信息，

实现集团工业互联网安全的可视化展示、安全预警及知识库管理，同集团专家团队有机结合，提高集团生产控制系统综合防护能力。

## 2、 方案总体架构和主要内容

本项目结合排水集团下属再生水厂、分公司的实际地理位置和业务属性划分不同的网络区域，按照 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中的“一个中心、三重防护”要求，强化再生水厂、分公司生产控制系统的安全防护。

基于再生水厂和分公司生产控制系统的安全防护建设，采用“一个中心、三重发现”的建设理念，建立集团级工业互联网安全态势感知平台和综合防护系统。总体架构如下图所示：

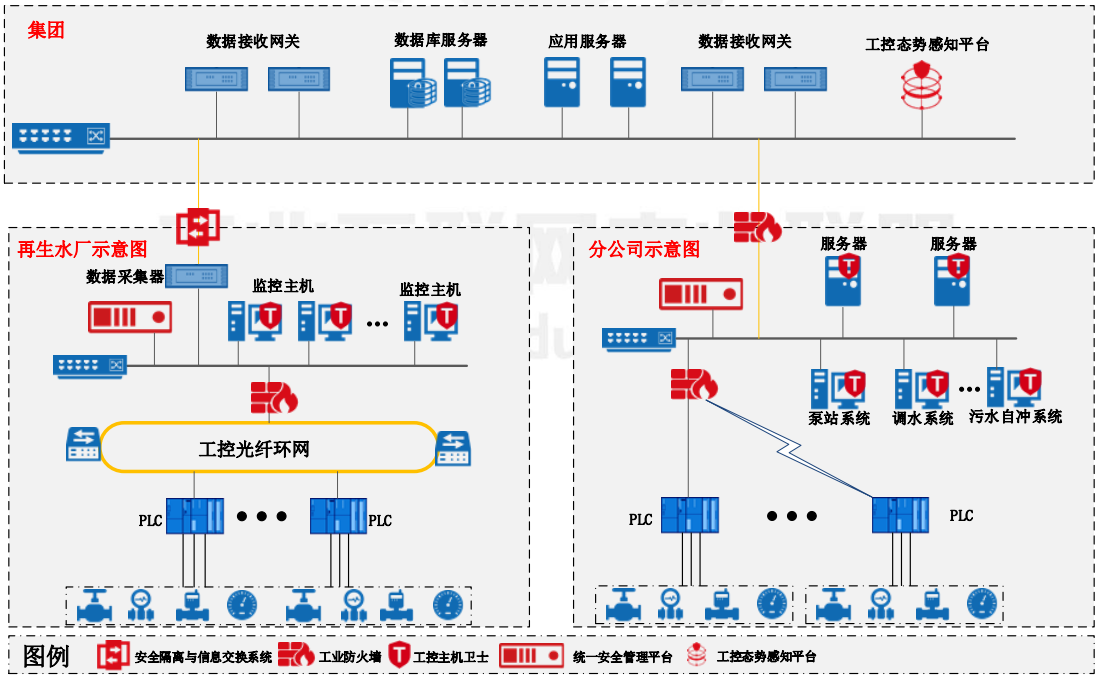


图 35　某大型排水集团安全防护总体架构

### （1）强化关键基础设备安全防护能力

排水集团生产业务高度依赖工业控制系统来实现自动化作业，自动化的核心主要依靠具有逻辑控制功能的 PLC 和上位机来

实现，因此对于整个生产控制系统而言，PLC 和上位机属于关键基础设施，必须加强关键基础设施的安全防护。具体防护措施如下图所示：

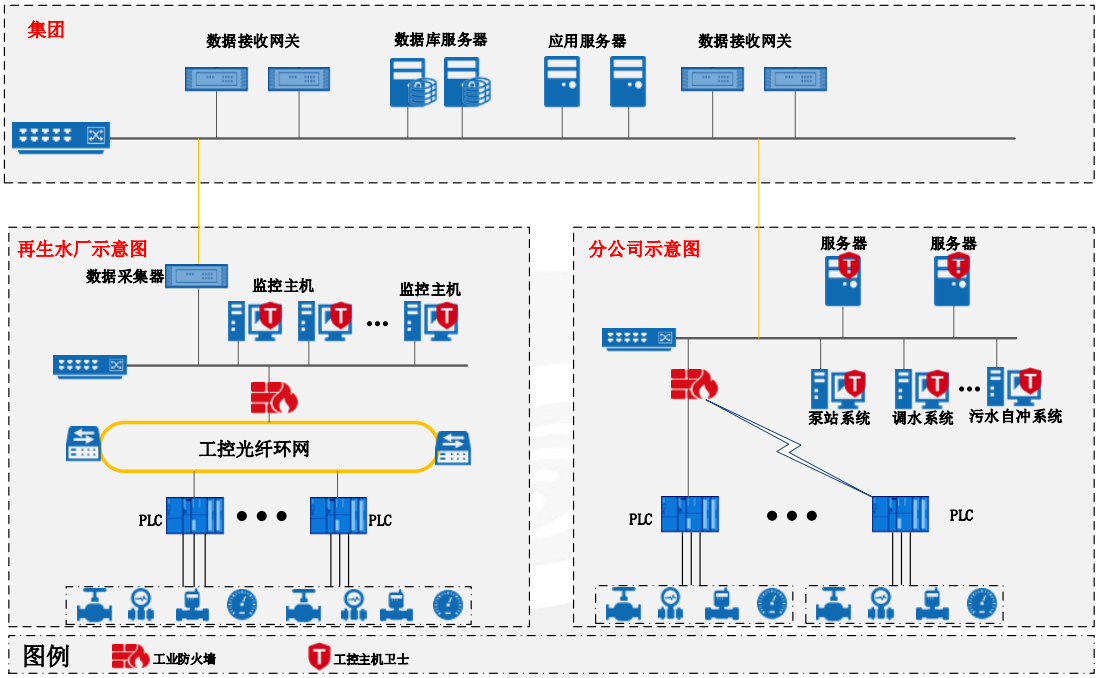


图 36　排水集团关键基础设备安全防护

- **提升关键 PLC 安全防护能力**

在再生水厂和分公司泵站关键 PLC 前端串联部署工业防火墙，基于工业协议深度解析技术，智能学习建立业务系统安全通信模型，形成业务白名单，防止非法指令下达至关键 PLC 控制设备，确保生产控制系统的安全。

工业防火墙基于对工控协议的通信报文进行采集与深度解析，利用人工智能算法自学习建立工控通信模型基线，对当前工控协议通信行为与工控通信模型基线进行对比分析，对不符合与工控通信模型基线的异常行为进行告警和阻断，如异常指令操作、新出现的设备（IP 地址）、异常连接行为、异常通信地址、异

常通信端口等告警。工业防火墙的白名单防御模式有三种，结合业务实际需求可调整至不同的安全应用模式，具体如下：

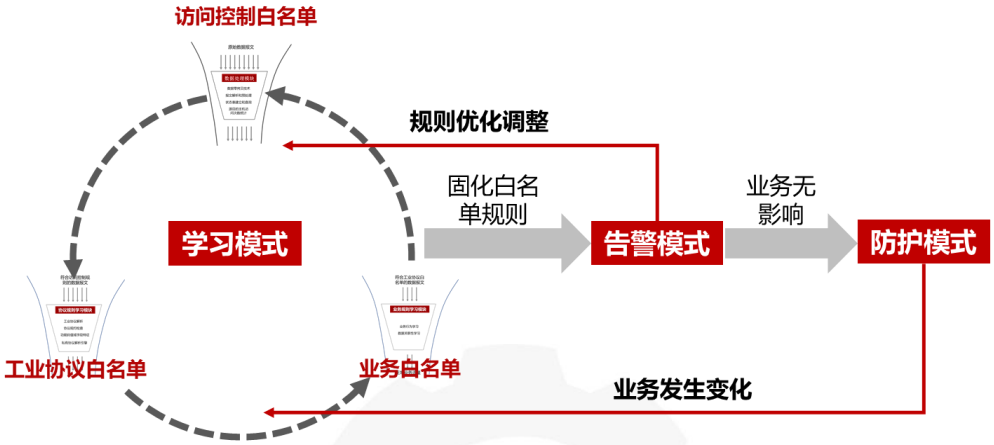


图 37　工业防火墙安全防护模型

1）**学习模式：**工业防火墙初次接入工控系统网络时，默认安全应用模式为学习模式，处于该模式下可通过 AI 智能学习建立 3 类白名单（访问控制白名单、工业协议白名单以及业务白名单），实现访问控制白名单固化、工业协议白名单固化、业务白名单固化（简称三重固化）。学习模式下的安全防护设备只具备学习功能，无告警及防护功能。

2）**告警模式：**告警模式下可针对违法白名单异常操作行为实时告警，同时安全运维人员可针对异常告警行为进行识别、结合实际业务情况对白名单防护规则进行优化调整；

3）**防护模式：**经过学习模式、告警模式后，进入防护模式。处于防护模式下的安全防护设备可对违法白名单异常操作进行实时阻断并产生告警，从而保障业务的高效、稳定运行。

- **提升上位机安全防护能力**

对排水集团再生水场及分公司生产控制系统中的工控主机

（操作员站、工程师站、服务器）部署工控主机卫士安全防护软件，通过工控主机卫士的程序白名单、网络白名单、访问控制、外设管控、非法外联、双因子认证以及安全基线一键配置功能实现工控主机的安全防护。

图 38　工控主机卫士七大功能

**（2）提升网络边界安全防护能力**

排水集团下属再生水厂、分公司分布在不同的地理区域，承担着不同区域的防汛工作、污水处理等工作。为了避免因局部生产控制系统安全事件影响全局生产系统的安全运营，对不同再生水厂和分公司划分独立的网络区域，在网络区域边界部署安全隔离与信息交换系统（网闸）、工业防火墙进行边界隔离，根据实际业务需求设置严格的访问控制策略；有效的防止外部区域对内部区域的非法访问、网络攻击以及数据外泄。

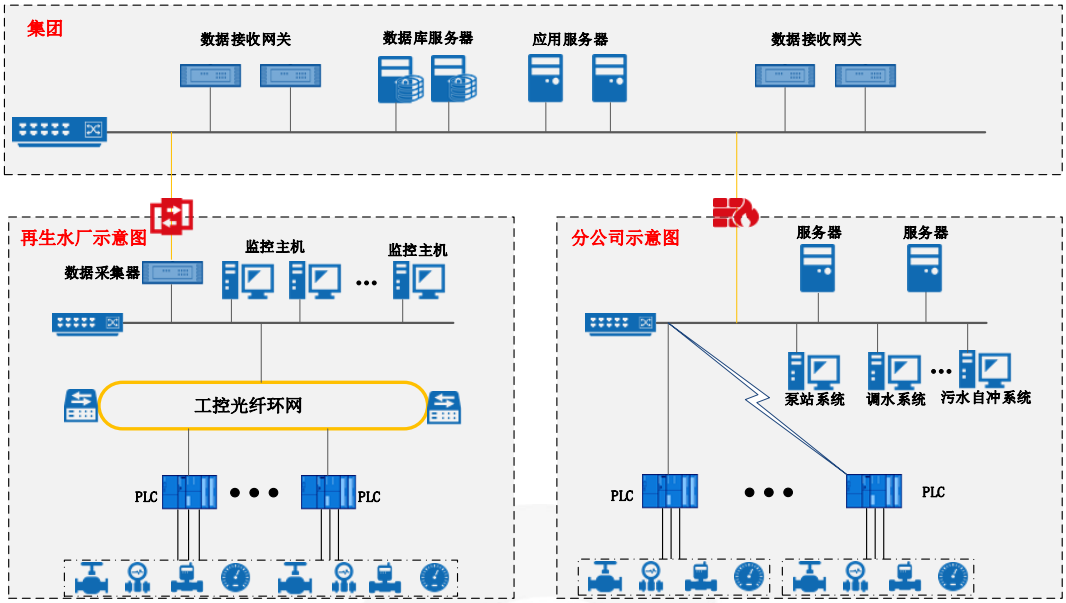


图 39　排水集团下属再生水场、分公司网络边界防护

### （3）提高集中管理能力

在各再生水厂、分公司建立安全管理中心，通过统一安全管理平台实现企业资产的集中管理、安全策略的集中管控、安全事件的集中分析，解决再生水厂、分公司资产和安全运营可视的难题。

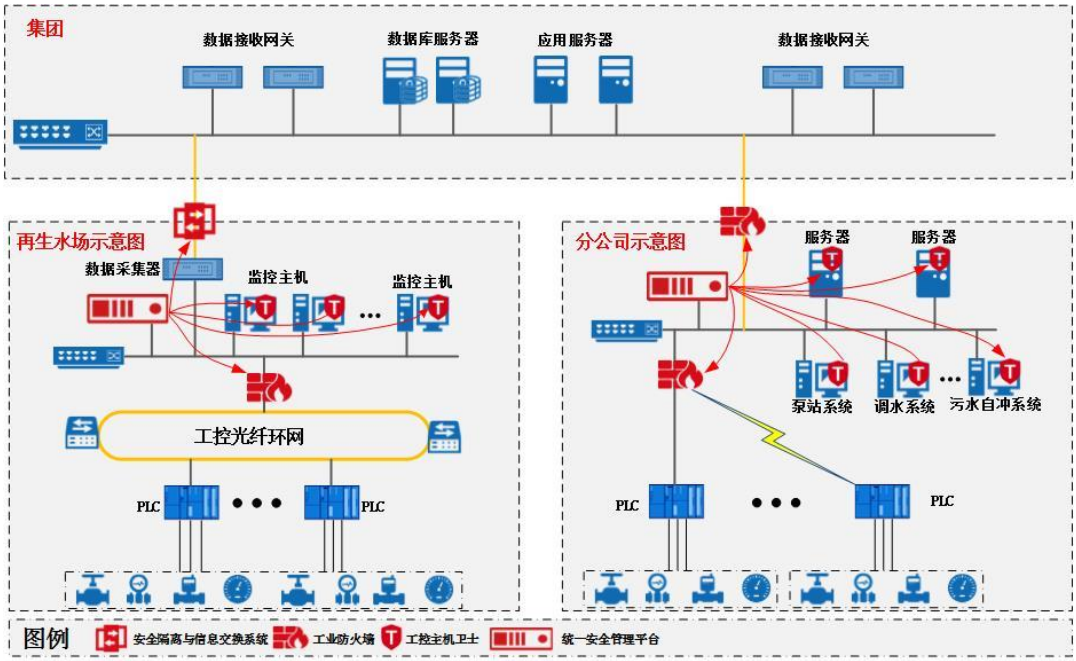


图 40　统一安全管理平台的集中管控

### （4）建立集团工业互联网安全态势感知平台

在排水集团侧建立工业互联网安全态势感知平台，整合各再生水厂和分公司的设备资产、网络流量、安全漏洞、安全配置、安全日志、设备运行状态、业务故障日志等信息，通过智能关联分析获取集团的安全风险和态势，结合集团专家团队支撑，指导安全告警的事件处置工作。

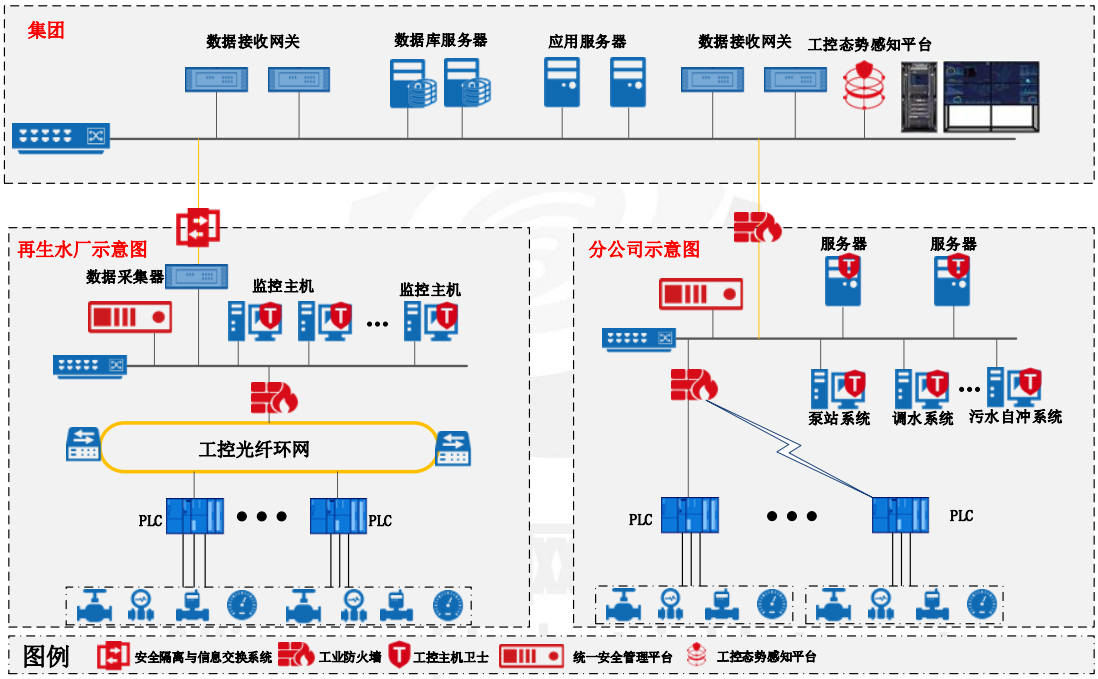


图 41　集团工业互联网态势感知平台部署

工业互联网安全态势感知平台借鉴“一个中心、三重防护”的纵深防御模型。采用“一个中心、三重发现”的建设理念，其中一个中心是指集团级工业互联网安全态势感知平台，三重发现是指发现工控网络区域边界、网络通信、计算环境安全问题的能力。集团级工业互联网安全态势感知平台通过报警反馈给厂侧，对厂侧安全防护进行监督。

通过建设集团工业互联网安全态势感知平台，提升排水集团

生产控制系统整体态势感知能力，同集团专家团队有机结合，提高集团生产控制系统综合防护能力，具体体现在以下方面：

- **整体安全态势分析：**通过将各厂区的健康指数和地域地图中的厂区相结合，

可以实现集团的安全态势可视化。

- **厂区安全态势分析：**将厂区的安全态势量化分析；通过将安全告警和网络拓

扑中的设备资产相结合，可以实现厂区的安全态势可视化。

- **资产动态分析：**自动识别出高风险的资产，通过资产存在的漏洞和关联的安

全事件告警，可以计算出资产的风险评分；通过资产的合规检查，获得资产的安全配置不合规项，可以计算出资产的合规评分。

- **脆弱性态势分析：**平台自动识别出每个厂区的高、中、低危漏洞的数量，漏

洞级别的分布，漏洞类型的统计，漏洞的设备类型排名，漏洞的设备厂商排名，以及资产的漏洞数量排名。

- **安全事件态势分析：**平台自动识别紧急、重要、一般的安全事件的变化趋势，

获取安全事件的类型统计结果；通过对源 IP 的安全事件数量分析，可以迅速识别攻击的发起源头、受害者、核心攻击事件。

- **攻击路径溯源分析：**通过采集 IP 对应的漏洞、开放端口、安全事件，基于

人工智能的知识图谱技术进行关联分析，获取攻击路径和攻击时间轴，最终可以对攻击路径进行溯源分析。

- **工控网络合规评估：**平台记录每个厂区的合规指数和其变化趋势、采集主机

终端的合规指数、分析写合规评估调查问卷，最终形成整个企业的合规指数。

**3、 方案先进性及创新点**

**（1）基于软件服务器的进程白名单更新技术**

通过软件服务器的进程白名单更新技术，在企业部署环境中只需要更新软件服务器计算机上的进程白名单列表便能使全网相同操作系统的电脑都能共享这一更新的白名单，从而不需再对每台计算机进行重复操作，有效减少安全运维工作量，更有益于积累全网软件的白名单库。

**（2）基于一种程序白名单知识库更新技术**

通过建立安装程序的进程父子关系树及临时程序白名单列表；在业务系统升级过程中自动判断，将属于进程父子关系的可执行文件一键加入白名单库，无需要过多的人工干预，实现系统的平滑升级。

**（3）基于“行为白名单”建立的面向工控 PLC 设备的行为模型固化技术**

采用了基于“行为白名单”的“三重固化”技术。针对工控设备的属性及行为进行描述，通过分析和抽象工控设备自身属性、行为及与其它设备的交互特征，构建工控设备行为模型描述框架，

实现行为白名单的识别与固化；通过分析和抽象工控协议的状态机及交互特征，构建工控协议行为特征解码引擎，实现协议白名单的识别与固化，创建并实现访问控制白名单的固化。

### （4）基于工控网络安全健康指数评估的技术

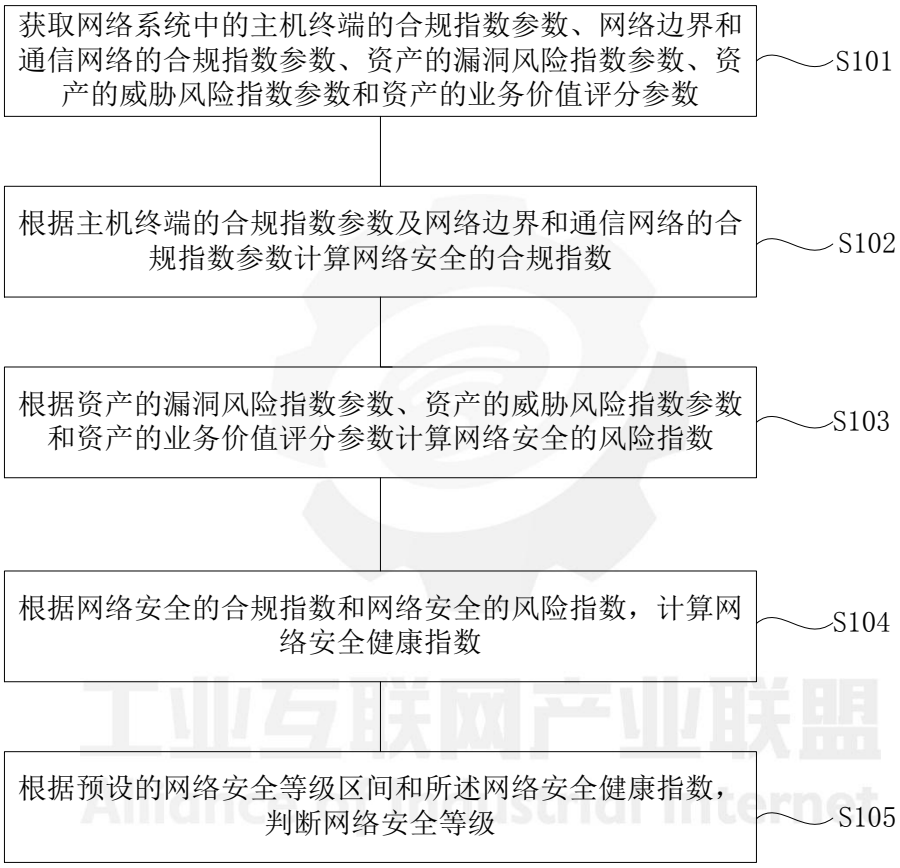


**图 42　工控网络安全健康指数的计算流程**

针对工控安全态势的分等级评估的问题，本方案采用了工控网络安全健康指数评估技术，该方法包括：获取网络系统中的主机终端的合规指数参数、网络边界和通信网络的合规指数参数、资产的漏洞风险指数参数、资产的威胁风险指数参数和资产的业务价值评分参数；根据主机终端的合规指数参数及网络边界和通信网络的合规指数参数计算网络安全的合规指数；根据资产的漏洞风险指数参数、资产的威胁风险指数参数和资产的业务价值评

分参数计算网络安全的风险指数；根据网络安全的合规指数和网络安全的风险指数，计算网络安全健康指数；根据预设的网络安全等级区间和网络安全健康指数，判断网络安全等级。

**4、 方案使用场景**

基于“动态行为白名单”的工业互联网端点安全防护技术体系适用于业务流程较为固定、运行环境相对稳定固化、系统更新频率较低的工业互联网端点类系统，通过“动态行为白名单”机制实现异常操作指令、用户误操作行为、网络入侵行为、恶意代码等主动防御，广泛应用于市政水务、石油石化、电力、轨道交通、烟草、智能制造、冶金及军工等国家重点工控行业。

**2.8.4 小结**

**1、 方案价值体现**

通过北京威努特技术有限公司对排水集团下属的再生水厂、分公司进行摸底调研和分析，并结合排水集团生产控制系统的安全现状、存在的安全风险以及面临的威胁，按照国家、行业相关要求，整合内部各再生水厂和分公司的设备资产、网络流量、安全漏洞、安全配置、安全日志、设备运行状态、业务故障日志等信息，设计出基于“动态行为白名单”的工业互联网端点安全防护技术，实现智能关联分析建立排水集团工业互联网集中化安全态势感知和综合防护系统，为排水集团工业互联网建设打下坚实基础。

**2、 方案特点**

**（1）合规性：**方案整体规划建设符合国家相关政策和标准

要求，有效避免了来自信息网的安全隐患对生产网带来的威胁，满足合规文件要求;

**（2）防护能力：**方案采用“动态行为白名单”机制建立纵深防御安全技术体系，确保基础设施的安全；建设集团工业互联网态势感知平台，全面提高集团的态势感知能力和综合防护能力。

**（3）安全保障：**利用先进的安全防护技术，结合健全的安全管理制度，通过运维人员及安全防护体系的有机结合，提高排水集团生产控制系统的保证能力。

**（4）经营效益：**通过对关键业务系统整体安全防护，大大降低了因网络安全事件带来的经济损失。

**3、 案例提供方**

本案例由北京威努特技术有限公司提供，北京威努特技术有限公司参与本案例前期调研、安全咨询、方案设计、安全建设及安全运维。

工业互联网产业联盟
Alliance of Industrial Internet

**2.8.5 单位基本信息**

北京威努特技术有限公司（以下简称“威努特”），是国内工控网络安全领军企业、全球六家荣获国际自动化协会安全合规学会 ISASecure CRT Tool 认证企业之一和亚太地区唯一国际自动化学会（ISA）全球网络安全联盟(GCA)创始成员。

威努特作为国家高新技术企业，以创新的“白环境”整体解决方案为核心，自主研发了 5 大类 30 款全系列网络安全专用产品，拥有 66 项发明专利、67 项软件著作权、77 项原创漏洞证明等核心知识产权。积极牵头和参与工控网络安全领域国家、行业

标准制定，受邀出色完成新中国 70 周年庆典、中共十九大、全国两会等重大活动的网络安保任务，被授予“国家重大活动网络安保技术支持单位”，得到了中央网信办、公安部、工信部等国家政府部门的高度认可。迄今已成功为市政、电力、轨道交通、石油石化、军工、烟草、智能制造、冶金等国家重要行业 1000 多家工业企业提供了全面有效的安全保障。

威努特始终以“专注工控，捍卫安全”为使命，致力于为我国基础设施网络空间安全保驾护航!

## 2.9 案例九：5G+智慧轨道交通安全解决方案

### 2.9.1 方案概述

中国城轨在“量”上已经全球领先，据维基百科统计，中国城市轨道交通协会 2018 年统计数据显示:在地铁里程全球 Top10 城市中国占 5 个，南京以 394.3KM 通车里程位居全球第 6，城轨短缺问题已经解决。

习总书记在十九大报告中提出要建设“交通强国”，城轨交通行业要向数字化、智慧化方向发展。中国城市轨道交通协会在 2020 年 3 月发布了《智慧城轨建设纲要》，明确在智能技术装备体系中，5G 技术和物联网是智能通信系统装备的重要落地方向。

当前全国各地铁公司先后与各电信运营商展开 5G 创新合作，如广州地铁利用互联网的思维和技术对传统轨道交通进行重构和再造;上海地铁发布建设智慧地铁,不断加快互联网、物联网、大数据、云计算、人工智能等先进技术在地铁运营全过程的应用，

深圳、重庆地铁也先后发声要在智慧城轨领域发力。重点破解地铁现网运行几大难题:

1、 **LTE-M 带宽能力不足:** 当前地铁车地 LTE-M 系统无法满足实时传送要求,部分业务(大数据)只能通过折中的手段获取。

2、 **现有系统管道差异化能力不足:** 无法提供稳定可靠、业务宽带、具有 QoS 保障和实时性要求的车地无线数据业务承载。

3、 **信息孤岛严重:** 无法实现数据互通和共享,无法挖掘跨专业领域的数据关联关系。

4、 **多云异构对运维提出挑战:** 不同云平台采用不同的技术架构，运维技能要求高，运维成本高。

5、 **缺专业运维能力:** 云计算和大数据对 IT 要求高，需建立专业的云计算规划和运维团队，保障系统可控、可持续演进。

以上种种不足对城轨建设、运营带来下影响:

对建设公司而言: 对传输带宽的需求，部分系统的网络带宽远远达不到业务需求，导致部分业务只能通过折中的手段获取。

通号设备处: 对高带宽的需求，列车运维数据无法实时回传至轨旁，辅助运营维护和故障分析。LTE 网络带宽不足，单列车运维数据传输速度需达到 1G 以上。对高带宽的迫切需求，信号系统要求综合无线通信系统 LTE 车地无线系统能够在高速移动状态下，提供稳定可靠、业务宽带、具有 QoS 保障和实时性要求的车地无线数据业务承载。

通信系统建设的网络带宽分配各专业使用,主要分配给视频监控使用，剩余带宽不足以满足新业务系统上线需求，现有的传

输网络在建设初期规划不足，导致很多新建系统无法承载。例如：1 号线、2 号线建设的传输带宽 2.5GB，实际可用带宽 768MB，在运营其他线路带宽理论值 10G，在建的 7 号线带宽理论值 40G；承载众多系统数据传输任务，各系统分配带宽极少。若需扩容则需要重新铺管布线，对于在营线路，施工难度较大，成本较高。

运维系统上线受传输网络带宽限制，如：供电分公司对于蓄电池的日常维护，需要对它的电压、温度等指标进行监控，以保证它的工况良好，目前受通信系统带宽不足的限制，蓄电池监控功能无法实现，可以考虑 5G 网络加 5G 模组的方式，实现对蓄电池数据采集、监控。

城市轨道交通信号系统从最初的基于固定闭塞信号系统，到基于 2.4GHz 无线局域网车地通信系统的移动闭塞信号系统。以及最近几年开始应用的基于 LTE-M 的蜂窝移动网络的车地通信系统的移动闭塞信号系统，都是得益于通信技术的发展，特别是无线通信技术的发展。基于无线通信的 CTBC 信号系统用通信网络来实现列车和地面设备的双向通信，用实时汇报的列车位置和计算移动授权的移动闭塞来代替固定的轨道区段闭塞实现列车运行控制。但是，从固定闭塞信号系统到移动闭塞信号系统，改变的仅仅是车地之间的通信。还有数据传输量大，对传输要求高轨旁联锁设备，自动列车防护系统设备，自动列车监控系统设备等都是依靠传统的有线网络进行通信。车站 ECC(元件控制)设备与轨旁的信号机，转辙机等设备也都采用有线通信，存在中间的通信设备多、故障风险大、光/电缆的维护和检修耗时耗力等等

诸多弊端。

基于上述提到的问题，目前城市轨道交通行业内的各方开始普遍思考如何改进目前主流的 CBTC 技术以适应未来的市场。而随着蜂窝移动通信系统的长足发展，5G 通信时代的到来，特别是 eMBB 和 uRLLC 的应用将打破带宽与时延的边界，为整个信号系统的 “无线化”以及“云化” 提供了可能。5G 定义了 eMMB、uRLLC 和 mMTC 三大场景，eMMB 指高速率连接，URLLC 指超低时延超可靠连接，mMTC 指超大规模连接，在工业领域这三大场景将广泛应用到。5G 强化了物与物之间的链接，扩大移动网络在各垂直行业的物联网应用。目前，轨道交通的发展对通信连接有着严苛的要求，要在复杂多变的作业环境下具有短时延、大带宽、高可靠性等通信连接要求。

随着 5G 发展越来越成熟，在地铁运营和维护，经营管理等方面，出现了越来越多的智能应用。一是在列车运行过程中，车地通信和信号运行大数据传输对通信网络有着严格的要求，尤其是大数据传输传统的 4G 网络很难达到预期要求，数据的实时数据无法共享；二是随着技术不断发展，信号系统的下一个发展趋势必然也是信号系统转入云端部署，信号系统应用软件转入云端部署，可以大大提高系统的经济效益，并减少了系统的脆弱性。而 5G 网络的到来使上述设想成为现实。

项目应用目标主要包括超高清视频等大流量移动通信宽带业务、与运营维护相关的大规模物联网业务平台业务等需要低时延、高可靠连接的场景，项目研究方向分为列车车地通讯、车载

运行大数据和轨旁器件控制等方面，通过 5G、MEC 等技术有效提升感知，实现信号控制系统升级，解决行业难题。

项目应用信息安全目标主要是结合项目应用目标，通过对项目应用网络架构进行安全需求分析从而对新型网络架构进行网络安全规划设计，确保通过相应的信息安全建设，助力 5G+MEC 智慧轨道交通更安全。

### 2.9.2 典型安全问题

地铁信号系统是列车运行控制的核心，5G+MEC 实现了列控的超低时延转发，平均转发时延达 7ms，而当前 LTE-M 在 20ms 以上。同样，列车大数据系统即 TGMT 大数据分析系统 TBDS 使用 5G 取代 WIFI 和 LTE-M 通信模式，由原来列车回库后进行数据回传转变为原系统需驻车后下载，5G 实现了大数据系统的实时回传，提高故障预测精度。

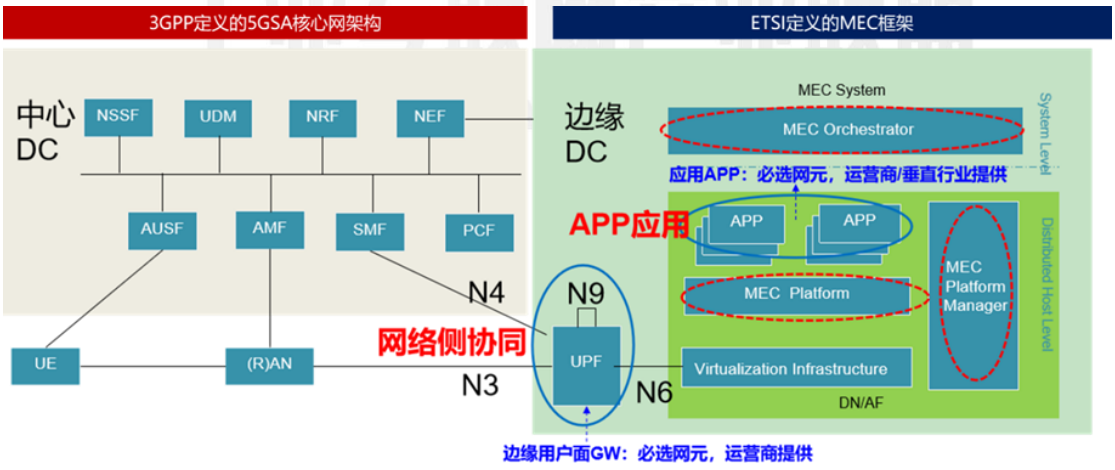


图 43　MEC 和 SA 架构融合

项目使用的 5G+MEC 网络架构平台如图 1 所示，网络安全问题具体表现为以下几个方面：

**1、 未进行安全域划分，区域间未设置访问控制措施。**

地铁信号系统的集成化越来越高，与各系统有着紧密的联系，但是仅在应用层面进行访问控制，系统底层没有访问控制措施，很容易绕过应用层的控制措施，直接对变电站/所的供电系统进操作，对环控系统的 PLC 控制器进行操作。

与互联系统间通过通信处理机 FEP 进行接口通信，仅考虑功能实现，未对通信处理机上的通用操作系统进行安全加固，导致通信处理机容易成为攻击靶标并沦陷为网络攻击的跳板。

**2、 缺少网络监控手段，不能及时发现网络安全问题，**

地铁信号系统网络上缺少网络安全监测机制，不能发现网络入侵、病毒、网络访问异常、网络拥塞等问题。更不能发生隐藏的问题，威胁潜伏越久，累积的潜在损失就越大。

**3、 缺少网络审计手，出现问题后靠人员经验排查。**

地铁信号系统网络上缺少网络安全审计，一旦发生问题基本靠人工经验排查，不能及时确定问题所在，及时排查到故障点，排查过程耗费大量人力成本、时间成本。没有审计记录难以找到问题根源，解决问题往往治标不治本，相同的问题反复发生，严重降低生产效率。

**4、 系统运行后，操作站和服务器很少打补丁，存在系统漏洞，系统安全配置较薄弱，防病毒软件安装不全面。**

地铁信号系统的工作站一般采用 Windows 系统，上线后基本不会对操作系统进行升级，而操作系统在使用期间不断曝出漏洞，导致操作站和服务器暴露在风险中。在系统上线前没有关闭掉多余的系统服务，以及系统的密码策略等进行安全加固等问题。另

外，运维人员调试过程中可以对操作站和服务器安装软件。为了方便调试，会开启操作系统远程服务功能，上线后通常不会屏蔽这个功能，安全配置薄弱，容易遭受攻击。

防病毒软件的安装不全面，即使安装后也不及时更新防恶意代码软件版本和恶意代码库。

**5、 存在使用移动存储介质不规范问题，易引入病毒以及黑客攻击程序。**

在地铁信号系统运维和使用过程中，存在随意使用 U 盘、光盘、移动硬盘等移动存储介质现象，有可能传染病毒、木马等威胁进生产系统。

**6、 上线前未进行网络安全测试。**

地铁信号系统在上线前未进行安全性测试，系统在上线后存在大量安全风险漏洞，安全配置薄弱，系统带病工作。

因此，通过 5G+智慧轨道交通安全解决方案，可以实现以下安全要求:

**（1）解决 5G 网络接入终端的安全问题**

**（2）解决 MEC 机房及服务器的安全问题**

**（3）解决 UPF 应用分发的流量风险识别问题**

**（4）实现新型网络架构下一体化网络监测手段**

最终实现:

**（1）数据不出场、网络高可靠、确定性 SLA（服务等级协议）、安全管控、极简部署与运维;**

**（2）边缘覆盖广、分流灵活开放、差异化 QoS（服务质量）、**

0 时延切换、灵活订阅与开通。

### 2.9.3 安全解决方案

本项目信息安全主要针对由基于 LTE-M 的蜂窝移动网络升级至 5G 网络而进行量身定做。针对升级后的 5G 网络安全风险点进行逐一网络安全加固，信息安全设计覆盖服务器安全、5G 基站与 UPF 核心流量安全检测和通过 5G CPE 模块接入 5G 网络的终端设备安全。

南京联通与南京地铁联合完成全国首个基于 5GSA 架构的 MEC 部署，实现城轨三大业务流在 MEC 节点完成业务流转发，实现流量本地化，使系统具备实时、高效、可靠安全转发与处理。项目主要通过 5G 网络并结合 MEC 实现地铁专网功能，同时通过 5G 实现地铁信号系统云化，提升轨道交通领域系统效能，解决行业难题。项目总体架构方案如图 2 所示。

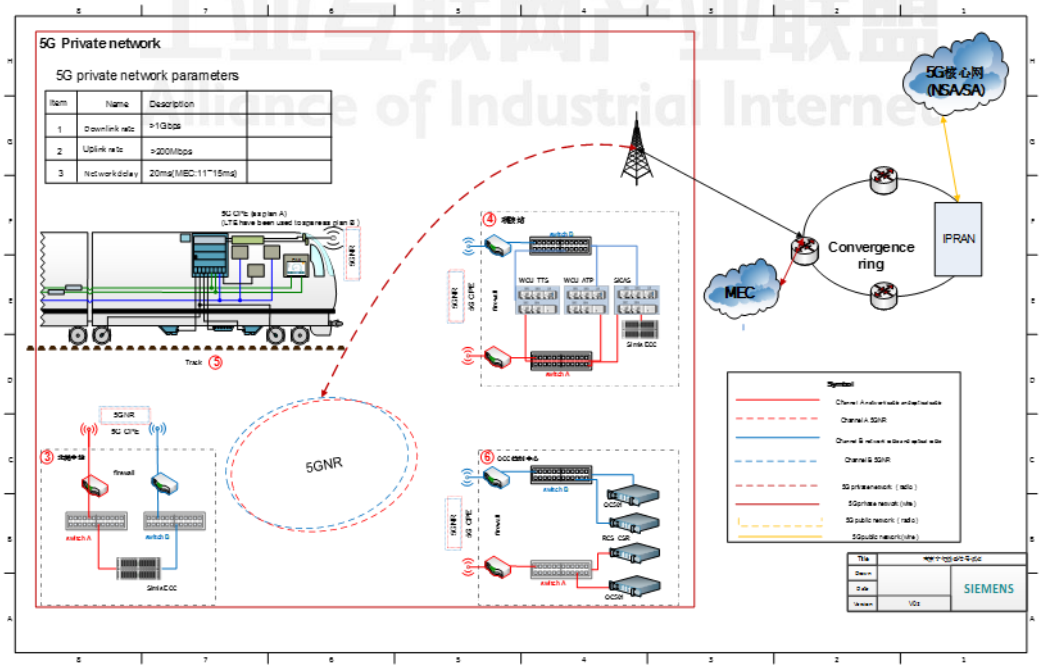


图 44　系统架构

在马群基地试车线设备室布放 MEC 对接各业务测试平台，实现 5G+MEC 轨道交通领域行业应用。MEC 组网方案图如所示。

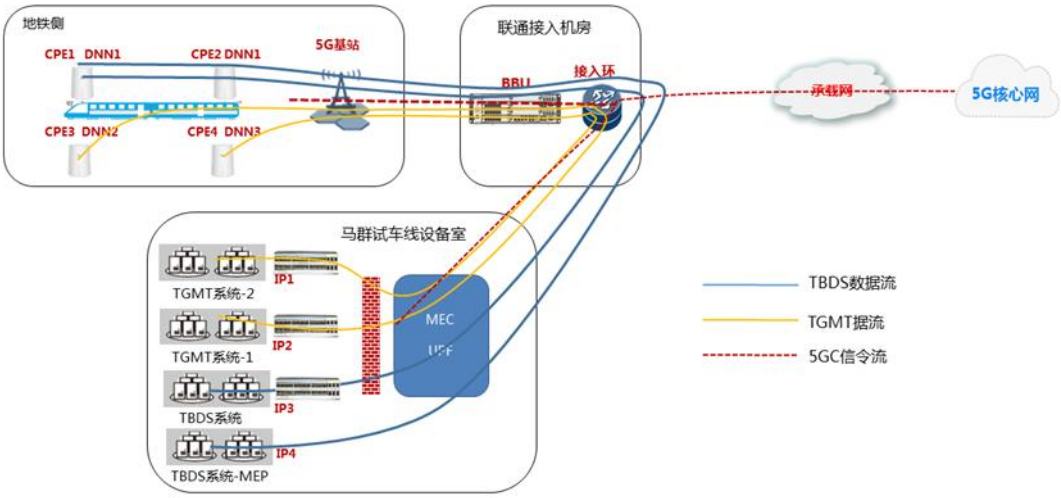


图 45　MEC 方案图图

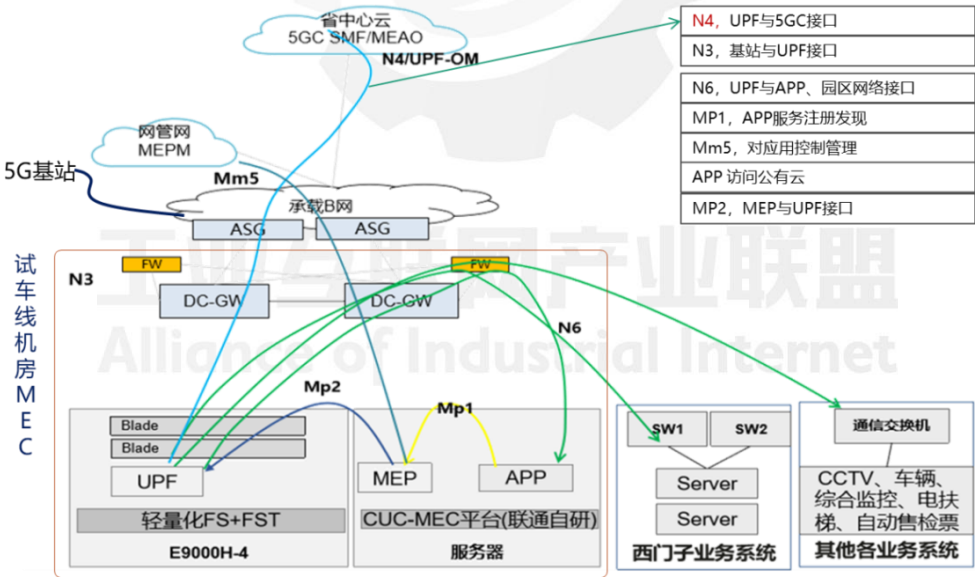


图 46　未加安全防护的业务架构图

用户访问西门子车地系统平台：终端->基站->ASG->DC-GW->UPF->DC-GW->FW->西门子交换机->西门子平台

用户访问西门子大数据系统平台：终端->基站->ASG->DC-GW->UPF->DC-GW->FW->MEP 服务器

## 1、扁平化支撑体系

- 数据在马群本地流转
- 业务流全部经由 UPF 转发
- TBDS 系统部署在联通 MEP 服务器

**2、 低时延/高安全**

西门子实测显示，车载数据流经 MEC 转发，用户侧延时低至 3~4ms，业务流不经核心网，叠加隧道保护，高安全。

**3、 MEC 节点能力开放**

MEC 平台虚拟资源池的开放性得到验证：西门子大数据诊断（TBDS）系统解耦后成功部署在 MEP 服务器上。

江苏启明星辰针对本场景潜在的信息安全设计覆盖服务器安全、5G 基站与 UPF 核心流量安全检测和通过 5G CPE 模块接入 5G 网络的终端设备安全三个层面的风险，提出以下框架方案。

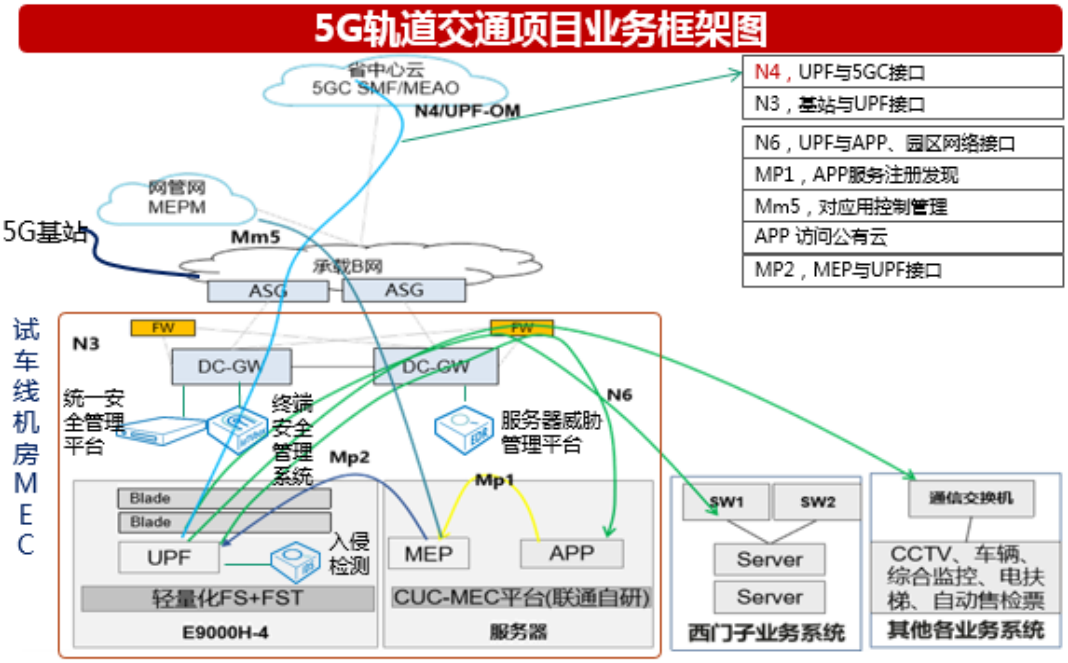


图 47　轨道交通项目业务框架图

**4、 网络安全设计**

**（1）服务器和终端安全**

- 部署服务器安全威胁管理平台
- 在各服务器中部署轻量级客户端
- 服务器实威胁全视角、全过程溯源

天珣终端高级威胁检测与响应系统是启明星辰集团推出的一款扎根现在且面向未来的终端 EDR 安全产品。天珣终端高级威胁检测与响应系统的客户端轻量且具有高端侧覆盖的特性，能为安装 Windows 、Linux 以及国产操作系统的终端保驾护航。天珣终端高级威胁检测与响应系统具有强大的数据采集能力，能够详尽的采集终端的静态和动态信息，如软硬件资产信息、安全合规信息及运行信息等。以数据为抓手，天珣终端高级威胁检测与响应系统实现了对已知和未知威胁的防护和分析。

天珣终端高级威胁检测与响应系统的网络、进程和外设三大白名单功能，仅需四步即能简单、智能、快速地对终端进行安全运行防护。

第一步：信息一键提取。服务器端发起网络、进程、外设采集策略，可采集当前运行、历史运行信息。

第二步：威胁情报 IOC 碰撞。所有采集到的信息均与内置威胁情报进行 IOC 碰撞，辅助研判信息安全性。

第三步：人员复核调整。人工对于机器判别出的有威胁信息进行二次校验。

第四步：一键将复核后信息转换成安全策略并执行安全防护。

未知威胁检测是 EDR 产品核心安全能力的体现，天珣终端高

级威胁检测与响应系统有强大的未知威胁检测手段，覆盖 9 大 APT 攻击步骤。能够以主动防御的方式寻找攻击早起的预警指标，通过攻击行为建模，根据上下文、序列事件来识别未知威胁，并形成 APT 攻击链条对攻击进行溯源。

EDR 系统采用标准的 C/S 架构逻辑，对于内网所有的终端电脑进行安全，让安全防护不在受操作系统限制，并且突破性采用极轻量级客户端设计理念，终端只做基础的信息采集以及简单的控制响应功能，降低对于终端的运维工作量，所有检测与分析能力交付 EDR 分析中心进行检测，良好的设计理念赋予了分析中心可对外扩散能力，在自身安全威胁分析能力不足或无法准确研判时，可联动外界平台来增强自身对于安全威胁的分析能力。

**（2）5G 基站与 UPF 流量安全**

对通过 5G 基站接入 UPF 的流量进行安全检测，具备对各类攻击行为等威胁具有高精度的检测能力。

启明星辰工控入侵检测系统是面向工业企业领域推出的针对工业控制系统的专用网络安全检测系统。

产品实现了对工业控制系统中的工控语言的专项解读，提供特有的工控网络安全检测策略，并可针对工控网络敏感指令数据进行记录和异常检测。不仅可检测工控网络中发生的入侵攻击，还可实时监测工控网络中的敏感操控，实现故障与异常的预警。

系统采用特征检测技术、工控异常行为检测技术、黑白名单技术、基线技术等，通过对网络流量的深度包解析和流解析，实现了病毒、木马、蠕虫、僵尸网络等各种威胁的全面有效检测。

系统通过内置特征库、病毒库、异常行为模型库实现对工控网络的威胁的自动检测。系统支持基于黑白名单的检测，用户可以通过定义黑白名单实现对违规业务和未知业务的检测。

系统基于自主研发的、灵活的规则描述语言技术，提供了一个开放式的自定义检测规则的用户接口，可以满足更加贴合用户业务的异常检测要求，例如通过自定义检测规则，可以实现异常时间、异常 IP、多 IP 登录等异常登录行为、恶意业务订购、高频业务访问、业务绕行等业务异常行为。

产品开放其灵活、强大的定制检测能力，针对客户环境中重点/敏感操控指令进行专门监测并记录。通过对工控语言的解读，研究其中各种入侵途径，从而形成了特有的工控网络检测策略。支持 Modbus 协议、IEC-60870-104 协议、Profinet 协议、Siemens S7 协议等工控协议的深度解析。

**（3）终端安全**

通过白名单加流量学习方式建立通过 5G 接入的终端的行为基线，对接入终端进行全局管理和安全监测。

启明星辰 IoT-VBox 主要解决 2B（企业端）场景下的物联网安全防护需求。产品实现了一种无代理的安全防护方法，也就是说无须改造物联网设备，即可有效地帮助解决大型、动态和多样性等复杂企业网络环境下的物联网终端可见性和安全控制的挑战。IoT-VBox 可以发现企业网络中的电脑、智能手机、物联网设备、操作技术系统、外围设备、网络基础设施组件和流氓设备等，并精确分类，然后进行设备指纹基线、网络基线（按需通断）

和行为基线的学习建立，在基线的基础上，当发生设备仿冒入侵、非法连接以及非法行为时，设备就会进行报警、阻断。

相较于传统的准入类产品，IoT-VBox 无须安装客户端，无须改造物联网和 BYOD 设备，更具备普适性和灵活性； IoT-VBox 的安全管控技术是面向物联网设备全生命周期的防护，会持续的收集、关联和分析设备信息，网络流量，进而以评估和持续监控安全态势，并实时做出管控动作；企业网络中的物联网设备种类众多，IoT-VBox 的设备指纹、行为学习等安全功能均不基于预置库，现场学习，无须针对碎片化的物联网设备进行定制开发，提高了产品的普适性；使用预置特征、厂商标识库和强大的自定义规则库来自动对设备进行分类；IoT-Vbox 采用主被动技术结合并且开关独立，对一些高优先级的设备（如工控设备）可提供被动无扰的监控功能；IoT-Vbox 具有设备冒用的实时检测能力，算法与企业网络中的物联网设备的数量中无关，当设备被仿冒时，可实时检测发现并报警、阻断；面向物联网设备行为相对规定的特点，IoT-VBox 可在线学习物联网设备的行为，自动生成行为基线，当行为发生异常时可报警、阻断。

**（4）一体化安全**

从监控、审计、风险和运维四个维度建立起来的一套可度量的统一业务支撑平台。启明星辰工控信息安全管理系统就相当于工控信息安全的指挥部，产品以设备资产管理为主线，以安全信息集中管理为手段，以威胁发现和处置为核心，目的是帮助用户构建一个威胁监控以及威胁处置的统一安全管理中心。

面向工控信息网络的安全防护，集中采集工控环境中各类设备的运行信息及安全设备的监控信息。通过工控风格的展现界面和多维可视化视图高效呈现安全监控信息，帮助用户实时洞察工控威胁与异常。

通过统一的漏洞、事件、状态管理，从工控业务操作的视角进行各工业控制操作流程的健康性评估与风险定位，结合强大的关联分析技术综合分析海量监控信息，深度发现危害业务的可疑攻击以及违规操作。

在集中安全信息与威胁展现的基础中，提供全网统一的告警响应能力，将异常及故障及时通报用户，并且提供安全事件规范化处理的技术支撑，使安全事件流程化、快速化处理，提升运维的能力与效率。

本项目方案深度贴合地铁轨道交通需求，本着实用为先的原则，建成后能大幅提升地铁车地通信及运行效率，并能节约投资。技术上紧贴 5G 三大特性，且较为成熟，可推广程度高。地铁轨道交通内 5G 应用场景，综合分析看来，主要包括超高清视频等大流量移动通信宽带业务、与运营维护相关的大规模物联网业务平台业务等需要低时延、高可靠连接的场景。

**5、 项目的创新性主要表现在以下方面:**

**（1）5G 创新技术**

通过 5G 网络切片及 MEC 边缘计算实现地铁专网网络覆盖需求，同时采用 5G 冗余设计保证网络的可靠性。项目分为列车车地通讯、车载运行大数据和轨旁器件控制三个方面，很好的贴合

了 5G 大带宽、低时延、多连接的特性，能通过 5G 技术有效提升感知，解决行业难题。采用了如下的技术实现方式。

**1）5G 专网：**与 LTE-M 网络设计结构类似，5G 网络作为车地综合通信系统的网络，对接核心机房实现冗余备份，计划采用两套 5G 设备组建 A、B 专网使用不同频段，每个网络均包括了核心网、基带处理单元、射频拉远单元、车载无线终端 ，大大提升网络安全性。

**2）频谱资源预留：**针对项目提出的 5G 专网应用需求，采用频谱资源预留解决方案，同时部署不同频段的两套 5G 硬件设备，作为热备。

**3）高带宽高可靠：**利用 5G 网络拥有的 eMBB（超大带宽），uRLLC（超高可靠性，超低时延）和 mMTC（超大连接）三大特性为承载地铁 CBTC、PIC、CCTV 等多业务信号提供了可能，相比 4G 时代网络性能有了明显提升，5G 网络兼顾高带宽和高可靠性，可有效替代传统的无线传输网络。

**4）边缘计算能力：**项目采用 SA +MEC 边缘计算的能力，推进在轨道交通领域创新技术应用的落地。

**（2）信号系统云化**

**1）本地控制单元下沉的优势：**一是节省集中站设备房的占地面积，机柜数量以及减少值班人员数量，节省投资成本和运营成本；二是使用无线与联锁通信，节约了光、电缆成本以及电缆敷设，以及长期维护的人员和耗材成本，节省运营成本，提高经济效益；三是大大降低了设备故障的影响面；四是单个本地控制

单元的故障仅仅影响到一个轨道元素。

**2)核心控制部分的上升优势:**一是核心控制部分上移集中，节省了联锁站设备房的占地面积，机柜数量以及减少值班人员数量，节省投资成本和运营成本；二是使用无线与联锁通信，节约了光、电缆成本以及电缆敷设，以及长期维护的人员和耗材成本，节省运营成本，提高经济效益；三是上移集中至中央控制中心，方便设备管理和维护方便，增强系统故障的响应速度和处理效率；四是核心控制部分功能“软件化”，“开放化”，采用普通商用服务器，使硬件设备类型更加统一，而且容易形成规模化，降低库存量，提高经济效益。

**3）5G 无线空口技术优势:** 早期的 CBTC 系统车地通信，采用 2.4GHz 无线局域网。由于属于免授权无线信道，接入不受限制且频宽有限。随着社会的发展，大量用户采用无线接入，使频道选择困难，且经常受到大功率信号的干扰。车地之间采用 5G 通信将会使车地通信更加稳定，高效。引入 5G 通信系统后，5G 优秀的无线空口技术无论在时延还是带宽，以及移动性上面将比目前的轨道无线通信标准 LTE-M 网络的表现更为优秀。

项目验证了城轨交通全新 5G 框架下，终端产品、网络、边缘云和城轨业务系统之间的全线贯通，为 5G 智慧轨道交通项目的深化合作和应用延展创造了条件，5G 大带宽、低时延、广连接特性验证有效，5G 有能力构建智慧城轨底层网。

信息安全设计覆盖到了由于网络升级而带来的各个安全风险点，从服务器安全、5G 基站与 UPF 核心流量安全检测和通过

5G CPE 模块接入 5G 网络的终端设备安全最后到统一安全管理。

项目通过5G+MEC+切片与轨道交通的技术融合解决城轨关键难题，开创运营商+地铁实现多云融合、双网保障、多维数据挖掘等地铁建设与运营新模式，解决行业难题，快速极大提升轨道交通的运营效率。打造全国首个轨道交通全场景、全门类、全业务测试和认证基地，加速新产品、新方案的研发、生产、测试和迭代，加速产业聚集，孵化独角兽，推进轨道交通产业数字化、智慧化进程。

关键软硬件及系统的技术来源如下图所示，包含软硬件的型号及提供商。

**表 2　设备来源**

| 序号 | 设备及型号 | 提供商 |
|---|---|---|
| 1 | 边缘云 DC-GW | 南京联通 |
| 2 | UPF | 南京联通 |
| 3 | 防火墙 | 南京联通 |
| 4 | 统一安全管理平台 | 江苏启明星辰 |
| 5 | 服务器安全管理系统 | 江苏启明星辰 |
| 6 | 入侵检测系统 | 江苏启明星辰 |
| 7 | 物联网终端安全接入与防护系统 | 江苏启明星辰 |

### 2.9.4 小结

项目验证了 5G 框架下，构建智慧城轨底层网的可行性和先进性，解决 5G 终端与网络协议匹配问题、解决系统反向控制问题、优化 5G 漏缆覆盖不及预期问题以及解决全国首个 5G 网络 3.5GHz 无线信号的合路问题，建立了由点到面的一体化信息安全解决方案，并在服务器安全层面依托全量信息采集能力，实现

对威胁全视角、全过程溯源。

为 5G+MEC 智慧城轨实施一体化安全措施，通过统一安全管理平台，对各个网络设备的威胁日志进行收集和分析，除此之外，统一安全管理平台系统内置业务建模工具，用户可以构建业务拓扑，反映业务支撑系统的资产构成，并自动构建业务健康指标体系，从业务的性能与可用性、业务的脆弱性和业务的威胁三个维度计算业务的健康度，协助用户从业务的角度去分析业务可用性、业务安全事件和业务告警。

在服务器安全层面：采用业内成熟的 EDR 产品，该产品使用极致轻量级客户端（最小 500k）作为服务器信息采集和安全响应点，配合高性能管理平台对采集的原始数据进行清洗、聚合、威胁检测、行为分析，对项目中所涉及到的所有服务器威胁进行全面安全响应，依托全量信息采集能力，实现对威胁全视角、全过程溯源。

基于本项目已实施的安全防护产品，根据智慧城轨业务的特点，进一步梳理业务安全风险，并深入探索 5G 自身技术实现而带来的安全风险，完善信息安全防护体系，为 5G+MEC 智慧城轨项目的复制推广提供专属信息安全解决方案。

**2.9.5 单位基本信息**

中国联合网络通信有限公司是中国分别在纽约、香港、上海三地上市的综合性电信运营企业。公司在国内 31 个省（自治区、直辖市）和境外多个国家和地区设有分支机构。2019 年 4 月 24 日，中国联通正式部署“7+33+n”5G 战略，中国联通南京市分

公司作为 7 个 5G 连续覆盖的城市之一，抢抓 5G 战略机遇，致力于推动科技创新、赋能行业，不遗余力推进、孵化 5G 应用落地。目前已取得多项成果，为南京创新名城战略做出了积极贡献。

南京地铁集团有限公司成立于 2012 年 6 月 18 日，主要承担南京市地铁工程的规划、设计、筹资、建设、运营及与地铁相关的物业开发等。南京地铁采取“职能部门+子公司”的集团化管控模式，建设、运营、资源开发“三位一体”协同发展。集团通过建立和完善公司治理机制、业务管控机制和财务监管机制等七大机制，协同好与建设、运营、资源开发、小镇开发四个公司的关系，共同打造更好南京地铁。

江苏启明星辰信息安全技术有限公司是北京启明星辰的全资子公司。北京启明星辰是信息安全行业的领军企业，参与包括等保 2.0 在内的工业互联网安全相关国家标准、行业标准近 20 个，已获得国家专项课题 20 个。依托北京启明星辰 24 年的行业积累，江苏启明星辰致力于打造本地化专业人才队伍及产品体系。

## 2.10 案例十：某 5G+智慧轨道交通安全解决方案

### 2.10.1 方案概述

2017 年 6 月 1 日，《中华人民共和国网络安全法》（以下简称“网络安全法”）正式施行。网络安全法是网络安全的基础性法律。网络安全法第 31 条明确规定“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”。城市轨道交通作为关键基础设施，是否能够持续安全运行，直接关系到广大乘客的生命安全，一旦遭到破坏，会对国家秩序造成重大隐患。

2021 年 1 月 13 日，工信部印发《工业互联网创新发展行动计划（2021-2023 年）》，2021-2023 年是我国工业互联网的快速成长期，要推动工业化和信息化在更广范围、更深程度、更高水平上融合发展，文件明确提出安全保障强化行动，要依法落实企业网络安全主体责任，明确企业安全责任要求和标准规范，城市轨道交通企业作为高频应用的城市基础设施的直接管理者，必须在用户隐私保护、业务数据安全隔离、端到到数据安全等方面肩负起最重要的责任，也保障“5G+工业互联网”融合应用的持续推进。

5G 网络的高带宽、低时延、海量连接等特性为轨道交通提供基础网络，大幅提升了轨道交通的信息化水平，催生更多的智能化数字化产品用于轨道交通，5G 及安全技术可实现多网合一，节省自建网络的成本和运营成本，提高系统融合管理效率。

面对 5G 网络的新发展趋势，尤其是 5G 新业务、新架构、新技术，都会对安全和用户隐私保护提出新的挑战。5G 安全机制除了要满足基本通信安全，还需要为不同业务场景提供差异化安全服务，能够适应多种网络接入方式及新型网络架构，保护用户隐私，并支持提供开放的安全能力。5G 网络必须能够提供不低于传统专网的安全性与可靠性，才能够胜任高价值资产的承载，充分灵活地应用 5G 基础设施以及围绕 5G 网络的创新所带来的新

技术与新能力，使 5G 网络与轨道交通的安全充分受益。

### 2.10.2 典型安全问题

5G 网络的引入，打破了原有相对封闭的网络环境，轨道交通业务及管理数据与运营商的网络数据汇聚在 MEC 上，MEC 将承载重要轨道交通业务数据流量，同时作为边缘云还会承担相关的轨道交通业务以及开放网络能力，例如室内高精度定位业务，5G+智慧轨道交通数据将从传统的少量、单一、单向数据逐步发展为大量、多维、双向数据，5G+智慧轨道交通用户多样化、设备多样化、业务多样化、平台多样化的网络发展趋势，使得轨道交通业务数据在用户、设备、业务、平台之间持续流动，导致数据的安全风险增加。

1、 轨道交通数据中心需要同时处理 5G 接入的轨道交通用户数据和公众用户的互联网访问的数据，改变了内外网隔离的边界，同时数据中心内部的大量交互，导致网络边界变得更加模糊和复杂，这些因素使得攻击的途径和手段更加多样化，轨道交通数据更容易被窃取，增加了数据的安全风险。

2、 5G 网络同时承载了公众用户以及轨道交通用户，但是网络资源有限，当网络高峰期时会影响到轨道交通业务应用的带宽、时延等可用性要求，导致业务受阻，严重影响业务正常运行。如果网络边界隔离不够，攻击者可能利用公众网络来攻击轨道交通网络。同时轨道交通不同类型业务有不同的业务性能指标要求，需要通过隔离来满足不同业务需求。

所以基于数据安全的考虑，除了要求数据进行隔离，同时还

需要实现不同类型业务之间的隔离，满足业务端到端超低延时和高可靠性要求以及数据安全保护。

### 2.10.3 安全解决方案

5G+智慧轨道交通安全解决方案通过基于业务优先调度、多层次网络切片隔离安全、多元化边缘计算（MEC）安全、端到端数据安全保护，实现敏感数据不出轨道交通、超低时延及超高带宽，实现轨道交通信息高速传输、互联互通、智能应用，提升智能调度成效，为市民提供高效便捷的信息交互和乘车体验，有效提升轨道交通服务管理水平。

**1、 PRB 硬隔离切片方案**

5G 网络切片是基于无线接入网、承载网与核心网基础设施，以及网络虚拟化技术构建的一个面向不同业务特征的逻辑网络，是上层的服务对网络质量的需求和底层的基础设施之间的桥梁。切片的目的是整合底层的资源，编排端到端的网络来满足服务对网络质量的需求。将切片技术应用于轨道交通业务，每个切片承载着特定的轨道交通应用，彼此相互隔离，可在网络层面实现精细化管理。首先通过细分基础网络，构建不同粒度的切片域，显著缩小被保护目标的攻击面；其次能够按照切片实施更细粒度、更严格的安全策略和更有针对性的管理手段，按需提供不同等级的安全服务；最后切片之间采用严格的隔离措施，一方面能够防范威胁向其他切片扩散，控制威胁的影响范围，另一方面也能够控制故障和异常的影响范围。

5G SA 环境的无线 PRB（Physical Resource Block，物理资

源块)硬隔离切片方案，解决方案涵盖了 5G 商用终端、5G 基站、承载及 5G 核心网，构建了端到端的 5G 轨道交通切片，标志着 5G 切片专网技术正式在轨道交通领域展开应用。

终端层面，普通切片和轨道交通切片采用不同的用户终端，根据接入控制各自接入到相应的切片中进行物理隔离；无线层面，采用 PRB 硬隔离为轨道交通切片预留了相关空口资源，实现轨道交通业务优先保障；传输层面，通过 VPN 方式对两种切片进行逻辑隔离；核心网层面，将各个子切片端到端拉通，普通切片和轨道交通切片采用 UPF 独享，实现用户数据隔离；应用层面，轨道交通用户专线接入轨道交通数据中心，实现物理隔离。

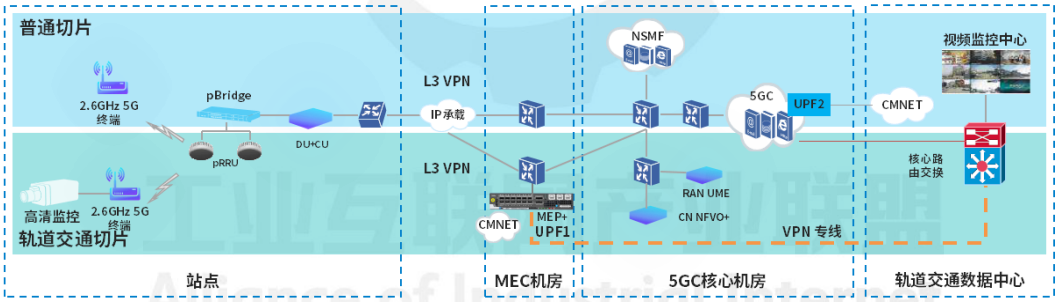


**图 48　普通切片和轨道交通切片**

无线空口侧资源从时、频、空域维度划分为不同的物理资源块（PRB），不同切片的数据（DRB）承载映射到不同的物理资源块（PRB），实现物理安全隔离，互不影响。各切片所需的 PRB 可按频域或总资源百分比进行切分和预留，颗粒度 1%，对应的调度方式可分为共 5 种模式，独占资源部分即专享的空口资源。另外还有优先、正常、禁止调度区域，丰富的模式可以适配各种业务的差异化需求。

轨道交通业务切片使用基于 PRB 预留的无线子切片，独享部分公网无线空口资源，提供类似于专用无线频谱资源的硬隔离，在网络隔离能力、确定性上有明显提升。

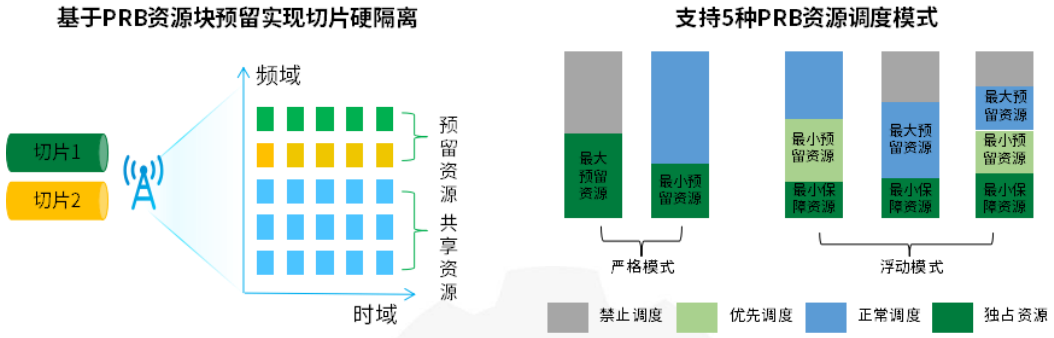


图 49　PRB 硬隔离切片

## 2、 端到端数据安全保护

MEC 本地分流实现数据不出轨道交通，保证数据端到端安全主要有三个方面，第一个接入认证，包括主认证和切片二次认证，保证用户合法接入，同时双向认证保证用户和网络之间的相互可信；第二个数据访问控制，防止接入用户的非授权访问网络切片；第三个是轨道交通数据走 VPN 专线不出虚拟专网，不出轨道交通，对轨道交通高价值资产数据，在空口、UE 和 MEC 之间还可以使用 IPSec/TLS 等安全传输方式，对需要保护的信息进行机密性和完整性保护，同时 MEC 内部边界做安全隔离。

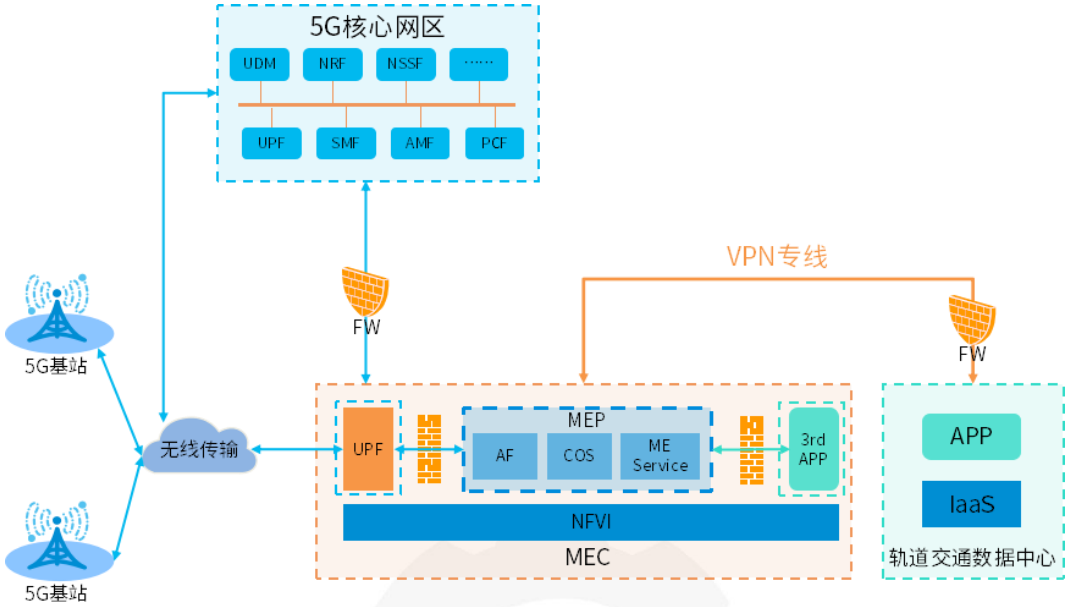


图 50　端到端数据保护

### (1) 多种终端类型双向接入认证

通过 5G 网络实现了对轨道交通各类应用的各种终端类型接入，包括各类传感器、CCTV、X 光安检机、电子引导屏、边门和综合安检等。为具备不同安全能力的终端提供统一接入认证，根据安全等级的不同配置接入认证，保证接入网络的用户的合法性。并提供双向认证机制，保证用户和网络之间的相互可信，才能防止轨道交通业务数据泄露或被篡改。

- **统一网络认证框架**

基于统一的认证框架提供用户和网络之间的双向认证，屏蔽接入差异，并支持 3GPP 和非 3GPP 接入，在非 3GPP 接入时，使用“EAP-5G”的特定于供应商的 EAP 方法，利用“扩展”EAP 类型用于封装 NAS 消息。

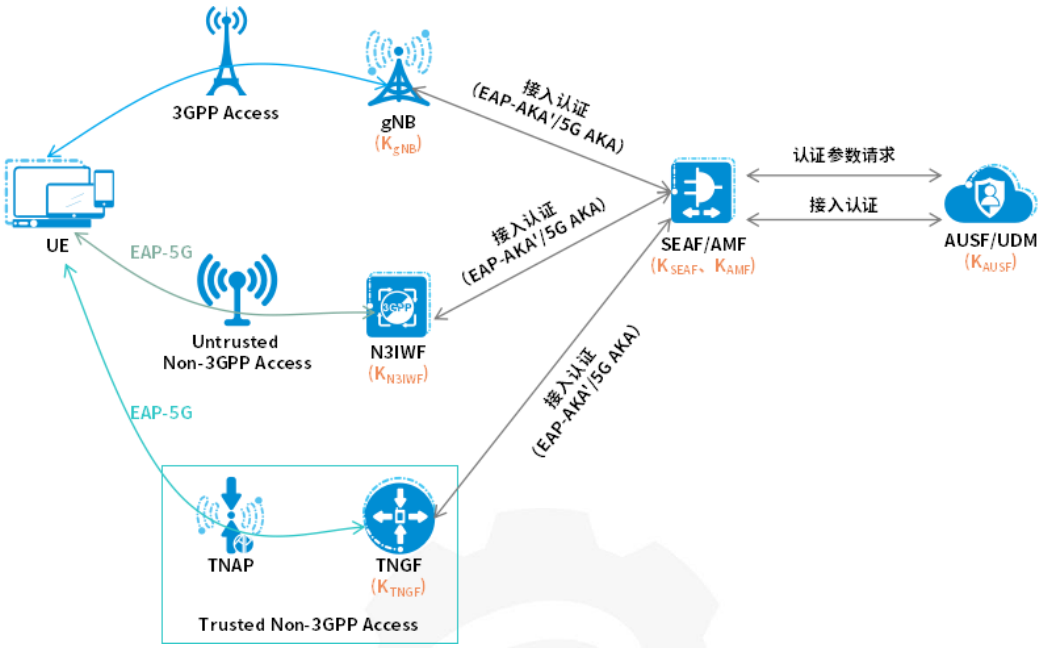


图 51　统一网络认证框架

- **切片特殊认证和 DN-AAA 二次认证**

主认证之后，根据策略触发切片特殊认证，和第三方的 AAA 进行对接认证，在创建 PDU 会话时，还可以进行轨道交通 DN-AAA 的二次认证，认证通过后才能访问切片数据网络。

1）**主认证：**正常网络认证，AMF 作为 Authenticator。

2）**切片特殊认证：**根据策略触发切片特殊认证，AMF 作为 Authenticator。

3）**轨道交通 DN-AAA 二次认证：**SMF 作为 Authenticator，在 USIM/ME 和 DN-AAA 间传达认证请求和响应。如果轨道交通 DN-AAA 认证不通过，则终止 PDU 创建流程。

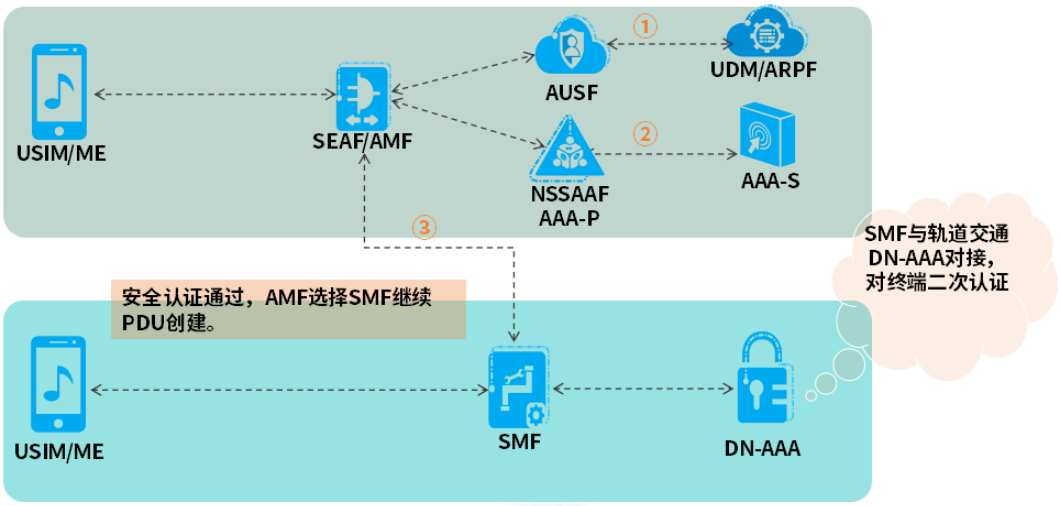


图 52　切片特殊认证和 DN-AAA 二次认证

- **双向认证**

双向认证，保证用户和网络之间的相互可信，5G 鉴权过程增强了归属网的控制，防止拜访网中可能存在的欺诈，除了鉴权机制，还关联鉴权与后续登记过程实现进一步的防欺诈防护。

**(2) 访问控制安全**

- **网络纵深防御**

部署 WAF、防病毒、数据库安全网关和数据防泄露系统等相关安全设备来实现检测网络中的异常活动并进行纵深防御。

- **安全访问策略**

在用户接入切片时，进行切片认证，以验证用户接入切片的权限，并严格定义数据访问权限，防止非授权用户接入网络切片，窃取信息或破坏切片正常运行。

**(3) 数据传输安全**

通过MEC 内部边界安全隔离，在MEC 部署、业务运行过程中，对 MEC 应用可能涉及的数据进行识别，包括用户的标识、接入位

置等。在数据产生和处理过程中，根据数据的敏感度进行分类，建立不同安全域间的加密传输链路。对轨道交通高价值资产数据，在空口、UE 和 MEC 之间使用 IPSec/TLS 等安全传输方式，对需要保护的信息进行机密性和完整性保护，避免传输过程中数据泄露或被篡改，并通过 VPN 专线实现数据不出轨道交通网络。

**(4) 数据存储安全**

对安全要求高的数据采用加密方式存储。根据不同的安全级别采用差异化的数据安全技术，对数据使用方进行授权和验证，保证数据使用的目的和范围符合安全策略。建立数据备份恢复机制，根据数据冗余强一致性、弱一致性等控制策略与规范，实现不同一致性水平需求的数据副本多样性、多变性和多种压缩策略存储管理，定期测试数据恢复程序。

### 2.10.4 小结

基于 5G 的 MEC 技术，采用了多元化的安全防护，实现乘客的精准定位，从而实现客流分布、客流预测和客流引导等多种业务，基于 5G 的网络切片技术，通过预留一定比例的 PRB 资源，保障轨道交通专网的最小带宽和最大可调用带宽，实现轨道交通专网和公网的安全隔离，从而保障轨道交通安全稳定。端到端数据安全保护，保证轨道交通业务数据分类分级加密传输存储，不出轨道交通园区。整体方案提高了系统的响应性能、运作能力和安全性，进一步支撑轨道交通数字化转型的发展。

### 2.10.5 单位基本信息

中兴通讯是全球领先的综合通信信息解决方案提供商。公司

成立于1985年，是在香港和深圳两地上市的大型通信设备公司。公司通过为全球 160 多个国家和地区的电信运营商和政企客户提供创新技术与产品解决方案，让全世界用户享有语音、数据、多媒体、无线宽带等全方位沟通。

中兴通讯拥有通信业界完整的、端到端的产品线和融合解决方案，通过全系列的无线、有线、业务、终端产品和专业通信服务，灵活满足全球不同运营商和政企客户的差异化需求以及快速创新的追求。目前，中兴通讯已全面服务于全球主流运营商及政企客户。

中兴通讯坚持以持续技术创新为客户不断创造价值，在美国、瑞典、中国等地设立全球研发机构，同时进一步强化自主创新力度，保持在 5G 无线、核心网、承载、接入、芯片等核心领域的研发投入，研发投入连续多年保持在营业收入 10%以上。中兴通讯拥有全球专利申请量 7.6 万件，已授权专利超过 3.6 万件，连续 9 年稳居 PCT 国际专利申请全球前五。同时，中兴通讯是全球 5G 技术研究和标准制定的主要参与者和贡献者。根据 IPlytics 2020 年 2 月的报告，中兴通讯向 ETSI 披露了 5G 标准必要专利 2,561 族，位列全球前三。

中兴通讯在 5G+工业互联网内生安全领域主要研究 5G 端到端安全、零信任网络、态势感知和 APT 监测和防护。中兴通讯从 2017年开始零信任网络技术的研究，对零信任网络的应用场景、技术框架、标准进展、关键技术等都进行了深入的研究，结合对通信网络的理解，提出了基于零信任和移动目标防御技术的

FlashGate（闪门），能够在兼容现网终端、现网业务的情况下实现业务授权和基于身份的访问控制。

中兴通讯致力于构建 5G 时代自主创新核心竞争力，将凭借领先的 5G 端到端全系列产品与解决方案，加速推进全球 5G 商用规模部署。

## 2.11 案例十一：青岛海尔 5G 智慧工厂安全防护应用案例

### 2.11.1 方案概述

中国移动与海尔集团于 2019 年启动 5G 智慧园区项目，一期针对 5G MEC+机器视觉、5G+AR 远程运维指导、5G+AR 巡检及行为检测等 7 个业务场景进行应用创新试点。

一期项目在位于青岛市黄岛区中德工业园的海尔冰箱互联工厂、中央空调互联工厂完成 5G 基站部署，同时在海尔崂山园区创牌中心下沉部署 MEC，中德园区内所有业务数据均在 MEC 内，控制面由中国移动大区核心网提供网络切片承载。

海尔在智慧工厂内新的生产场景如 AR/VR、高清工业相机质检等均需要较高的网络带宽和网络时延，当前的网络环境无法满足。而 5G 网络相比以前的有线网络、WIFI 或 4G 网络具备了更多优势，例如更高的移动性、灵活性，更简单的网络管理以及更低的构建成本。

作为新一代无线通信技术，5G 网络的迅猛发展切合了传统制造企业在智能制造转型过程中对无线网络的应用需求。在网络安全方面，按照国务院、工业和信息化部、中国移动 5G 网络安全防护最新要求以及安全三同步实施要求，海尔 5G 网络致力于

打造出满足端到端多级安全防护体系的网络架构。

本项目以“智能制造”为目标，结合企业当前网络痛点和创新技术应用，运用 5G、MEC 边缘计算、网络切片及安全防护、AR、机器视觉等新技术能力为客户提供定制、交互、安全、柔性的产品+服务。

同时，本项目可以在家电制造行业及更多的制造企业进行快速复制和推广，推进制造业的网络化、数字化和智能化转型，以柔性化、定制化和智能化生产模式满足更广阔市场需求。

### 2.11.2 典型安全问题

按照工业和信息化部、中国移动 5G 网络安全防护最新要求，遵循安全三同步实施要求，在海尔 5G 智慧工厂项目规划、建设、运行阶段同步进行安全相关工作，确保 5G 安全工作贯穿全过程。

从 5G 终端安全接入认证、MEC 业务隔离与数据安全防护、5G 网络切片业务隔离与网络通道安全保障技术、业务边界防护与数据安全防护等方面入手，构建基于“端-边-管-云”安全架构的端到端多级安全防护体系。

项目网络拓扑如下图所示。

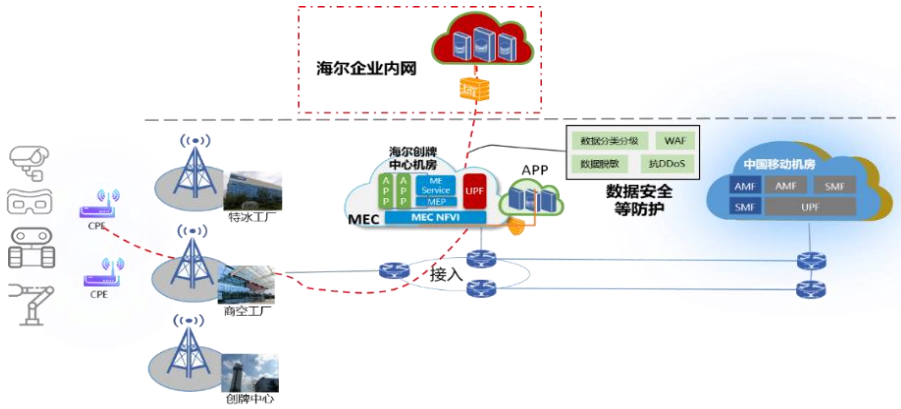


图 53 海尔项目网络拓扑

项目典型安全痛点如下:

**1、 行业监管要求**

（1）2017 年提升工业互联网安全防护能力，建立数据安全保护体系，推动安全技术手段建设;

（2）2019 年加快构建工业互联网安全保障体系，提升工业互联网安全保障能力。

**2、 海尔自身需求**

（1）异构、多协议终端统一认证接入;

（2）生产数据安全性和私密性数据隔离;

（3）不同业务场景安全、可靠性要求不同;

（4）行业网络切片的隔离性。

### 2.11.3 安全解决方案

基于“端-边-管-云”安全架构的端到端多级安全防护体系，解耦 5G 安全能力，通过划分不同层次安全域、部署安全防护设备、建设安全系统，针对海尔不同业务场景户对安全的需求提供端到端灵活的安全策略。

**1、 总体安全防护方案架构**

总体安全方案架构如下图所示。

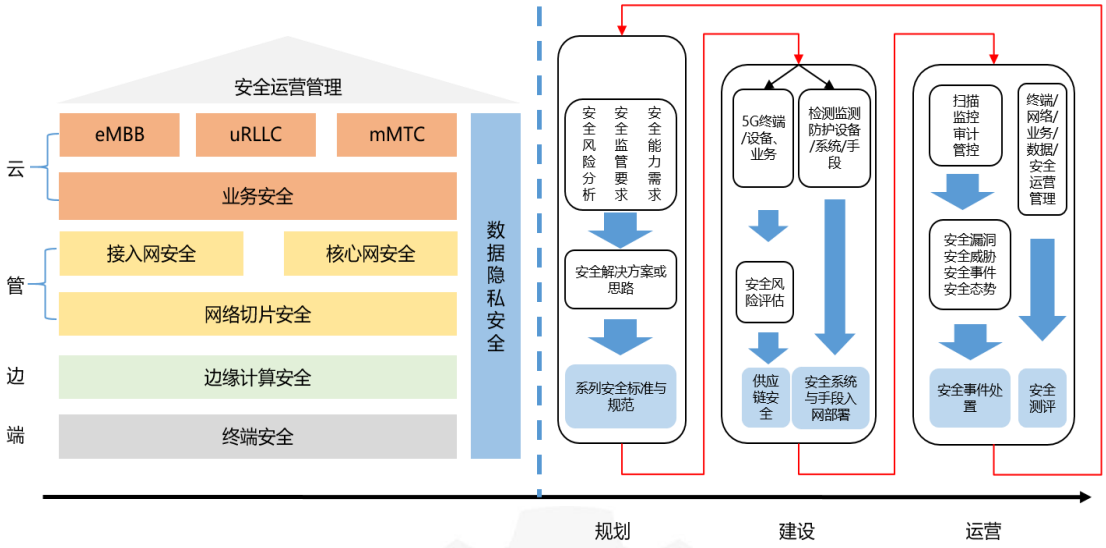


图 54　海尔 5G 智慧工厂安全防护框架图

**（1）5G 安全工作“三同步”**

在海尔 5G 智慧工厂前期讨论、规划阶段，安全团队针对业务场景、5G 技术使用、落地网络架构，并根据安全监管需求，进行安全风险分析与安全能力需求分析。同时结合中国移动 5G 网络和业务系统建设要求，提出安全解决方案或思路。

在业务试点建设阶段，同步建设安全保障手段，对海尔的 AR、机器视觉新业务上线前，严格做好 5G 终端、设备、业务的安全风险评估，并根据评估结果进行整改复核，需满足安全监管要求，并做好供应链整体安全。

AR、机器视觉等业务在 2019 年上线运行后，为保证安全能力持续符合国家及公司内部安全管理要求，山东公司开展周期性风险扫描、监控、审计和管控，及时发现安全漏洞、威胁、事件等，并对安全事件进行处置。

**（2）“端-边-管-云”的安全防护方案**

海尔 5G 智慧工厂应用场景丰富，多类业务分别对 5G 提出了

eMBB、uRLLC 业务需求，各类业务对网络能力需求不同，业务接入方式和网络服务方式存在较大差异，在安全方面需求差异性也非常明显。这需要运营商能针对 5G 智慧工厂各类业务安全需求，明确新业务安全需求差异性，定义多级的 5G 网络安全机制，保障 5G 智慧工厂业务健康发展。

中国移动 5G 行业虚拟专网支持定制化的安全，引入用户接入安全、数据传输安全、网络切片安全、服务化架构信令安全、边缘计算安全、数字证书、网络设备安全保证等方式为行业用户提供覆盖网络的通用安全，通过制定组网安全域划分、部署安全防护设备、建设安全管控系统、搭建网络与业务系统间的安全通道、提供业务技术安全等多方面，针对 5G 智慧工厂对安全的需求提供端到端灵活的安全策略。

**2、 安全方案技术概述**

**（1）端侧防护**

针对 5G 智慧工厂中的 CPE、嵌入式通信模块两类终端，在终端安全方面规划了如下安全防护措施:

- 接入 5G 的终端应支持 5G-AKA 或 EAP-AKA’认证，5G 可实现对 CPE、

通信模组终端的双向鉴权认证;

- 5G 可提供灵活的二次认证和密钥管理，用于终端与业务系统之间的业

务认证以及相关密钥管理功能;

- 5G 可为含通信模组终端、CPE 开启针对控制面、用户面

数据的加密传

输方式，保证数据机密性。

**（2）边缘计算侧防护**

为了满足海尔 5G 智慧工厂对低时延业务、数据不出园区的需求，本试点业务中可将 MEC 部署在海尔创牌中心园区。由于部署的物理位置、网络边界和承载主体等方面的特殊性，MEC 应从平台层、网络层和业务管理层等多个方面在物理安全、认证授权、数据传输/存储/处理、边界防护等方面进行安全防护。在边缘计算侧规划了如下安全防护措施:

- 边界防护: 部署在创牌中心园区内的 MEP、UPF 与核心网间部署防火

墙、IPS 进行边界防护，UPF 与海尔企业内网间也部署防火墙进行边界防护;

- APP 防护: APP 上线前，采用身份验证、安全合规检查和审核等手段

对应用镜像和代码进行扫描和审计。APP 上线后，进行安全加固和风险评估。APP 下线后，注销 APP 的相关访问权限，擦除相关的敏感数据;

- 数据安全: APP 与 MEC 平台等进行通信时，5G 可提供身份认证，并

对传输的数据进行机密性和完整性保护。

**（3）“管”道网络防护**

海尔 5G 智慧工厂终端通过 CPE、RAN 接入 5G，5G 可提供接

入双向认证、统一认证框架满足异构工厂内终端安全接入 5G。

- 针对 5G 无线接入、传输网、核心网网元加强安全防护;
- 切片接入认证：5G 可为终端或用户提供接入切片的认证;
- 切片数据保护：终端与基站间、基站与 AMF 网元间、基站与 UPF 间、

UPF 与业务系统间开启 IPsec 加密机制;

- 切片隔离：实施切片间隔离、切片网络与用户隔离等方式，提供网络专

用、定制化以及专属接入的能力。

**（4）“云”端业务防护**

针对海尔的业务系统，一阶段规划了如下云端业务安全措施:

- 针对海尔的业务平台加强认证授权、数据防泄漏、边界防护;
- 针对 eMBB、uRLLC 业务进行分级安全防护。

**3、 先进性及创新点**

**（1）分级安全防护体系**

针对海尔 5G 智慧工厂的不同业务场景的技术应用特点、差异化安全需求，提供分级安全防护体系来满足差异化需求，采用合适的安全防护手段。为支持不同业务的端到端安全保护，需要灵活的安全架构，由中国移动向海尔提供不同等级安全保护的网络切片。

**表 3　分级安全防护体系**

| 分级防护 | 端 | 边 | 管 | 云 |
|---|---|---|---|---|
| 1 级 | 基础安全 | 基础 MEC 防护 | 3GPP 基础鉴权、基础隐私保护、信令完整性保护 | 边界防护 |
| 2 级 | 3GPP 基础鉴权、CPE 白名单控制等 | 全流程数据加密传输等 | 3GPP 基础鉴权、基础隐私保护、信令完整性保护、用户面机密性、切片接入认证等 | 边界防护、eMBB 业务防护、数据防泄漏 |
| 3 级 | 3GPP 基础鉴权、CPE 白名单控制、二次认证等 | 全流程数据加密传输、基于安全资源池安全服务 | 3GPP 基础鉴权、基础隐私保护、信令完整性保护、用户面机密/完保、切片接入认证、二次认证、SBA 安全等 | 边界防护、eMBB 增强业务防护、uRLLC 业务防护、数据防泄漏、安全服务等 |

### （2）基于 MEC 的数据安全防护

《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》中要求提升工业互联网安全防护能力，建立数据安全保护体系，推动安全技术手段建设。

针对海尔对业务数据不出园区的安全要求，提供基于 MEC 的从终端到业务系统的端到端数据安全防护手段，确保仅合法终端接入，建立数据传输安全机制，提供 APP 关键数据防护手段，保障 MEP 自身数据安全。

**图 55　基于 MEC 的数据安全防护**

**4、 实施效果**

海尔 5G 智慧工厂丰富的业务场景代表了国内大多数制造业对 5G 网络、安全的需求，目前已完成并通过验收的 AR 远程指导、机器视觉等 3 个业务场景中采用的安全技术方案具备了规模推广的理论基础、技术基础、实践基础。

**（1）助力产业建立数据安全手段：** 5G MEC 边缘计算提供无线虚拟专网，

大带宽、低时延、高计算的平台，通过在 UPF 与企业内网间新增数据安全防护手段，助力行业建立数据安全防护能力，保证数据不出园区，满足行业监管要求。

**（2）提升安全防护水平：** 运营商提供的 5G 增强内生安全服务，联合

专业常识提供的通用安全服务将提高企业的安全专业水平，提升企业安全防护水平。

**（3）可定制的安全防护服务：** 针对不同业务场景的差异化安全需求，

运营商提供可定制的安全防护服务，减少统一的网络策略和安全机制难于满足各垂直行业不同的安全需求。

**（4）降低安全建设成本：** 由运营商提供端到端多级的 5G 增强安全内生服务、通用安全防护服务，减少企业安全设备采购数量，降低企业安全建设成本。

**2.11.4 小结**

此方案解决了海尔数据不出园区，数据传输安全问题，并且

提供分级安全防护措施合理的适配各业务场景安全需求，提升了海尔特冰工厂、中央空调工厂的检测、测量效率，圆满完成既定目标的相关任务，在实践、理论和技术等层面可以进行大规模复制推广。

**1、 大规模推广实践基础**

基于“端-边-管-云”的端到端多级安全防护方案，实施企业网络安全分类分级管理制度。一期工程中 5G+机器视觉、5G+AR 远程中应用的安全方案已完成交付并通过了中国移动、海尔验收，能很好满足海尔智慧工厂的安全需求。

**2、 大规模推广理论基础**

针对各业务场景的安全需求，定制个性化、合适的安全防护方案，大幅度提高安全防护手段的建设速度。

**3、 大规模推广技术基础**

5G 网络内生安全能力基于 3GPP 标准定义，由运营商来建设、提供标准 5G 网络内生安全能力；建设安全态势感知系统，提升网络和数据安全技术能力；通用安全能力采用业内成熟的安全产品或系统，其稳定性、可靠性均具备满足电信级业务的需求。

### 2.11.5 单位基本信息

中国移动研究院成立于 2001 年，是中国移动通信集团公司直属单位。研究院以做“中国移动技术创新的引擎”为愿景，落实国家创新驱动发展战略和构建公司“力量大厦”战略，致力于成为公司权威的战略智库，深入开展技术产业引领、现网运营支撑、新型产品和重大平台研发。

安全技术研究所是研究院内专职安全方向新技术研究、安全服务的智库，目前拥有 4 项国家级安全资质、74 项个人资质，2 个国家重点实验室。

中国移动通信有限公司山东有限公司于 2008 年 12 月 09 日成立。在集团公司授权范围内从事国内、国际移动通信业务（包括移动电话业务、数据业务、多媒体业务）国际互联网接入业务；IP 电话业务以及其他电信与信息业务等。

## 2.12 案例十二：面向钢铁行业一体化平台安全解决方案

本项目中新赛克联合南京钢铁集团有限公司和江苏省互联网行业管理服务中心，旨在围绕钢铁行业工控网络安全监测与防护需求，明确安全责任要求和标准规范，落实主体责任，建设工业企业网络安全综合防护平台。针对南钢 PLC、数据采集与监视控制系统（SCADA）等核心领域，利用机器学习、大数据技术强化安全态势分析技术，打造基于主机防护、监测预警、数据保护、统一管理、全面可视化等多层次一体化防御体系，提升网络和数据安全技术能力，强化南钢自身防护，通过网络安全可视化打造运行高效的安全保障体系。同时与监管侧平台对接进行信息共享、数据联动、协同防御。

### 2.12.1 方案概述

随着钢铁冶金行业信息化的持续推进，能源管理中心的投入运行，使原本相对独立的 DCS、PLC、仪器仪表、SCADA 等控制系统通过网络和信息系统连为一体。由于长期缺乏安全需求的推动，对 OT 网络环境的安全威胁缺乏充分的认识，现有的工业自动化

控制系统在设计、研发中没有充分考虑安全问题，在部署、运维中缺乏安全意识、管理、流程、策略与相关专业技术的支撑，导致许多工业自动化控制系统中存在着或多或少的安全问题。随着两化融合的推进，IT/OT（信息技术和操作技术）一体化的逐步推进，工业自动控制系统正在面临前所未有的信息安全威胁。

国家相关主管部门发布《关于加强工业互联网安全工作的指导意见（征求意见稿）》及工业互联网创新发展三年行动计划（2021-2023 年）等政策文件，要求依法落实企业网络安全主体责任，加强网络安全供给创新突破，促进网络安全产业发展壮大，强化网络安全技术保障能力，尽快推动并落实工业互联网安全发展。

当前行业应用客户有意愿通过部署相关安全产品和方案解决其生产制造过程中的网络安全问题，但网络安全厂商提供的解决方案与产品满足不了其要求，究其原因是工业领域行业壁垒明显，安全厂商不了解各个行业的典型生产制造流程、工艺特性等，在没有深入了解客户业务属性的基础上，无法设计出结合不同行业业务属性的安全解决方案。

随着钢铁冶金行业信息化的持续推进，能源管理中心的投入运行，使原本相对独立的 DCS、PLC、仪器仪表、SCADA 等控制系统通过网络和信息系统连为一体。同时依托计算机系统对能源生产、能源管理、能源调度进行扁平的一体化管理，不断提高劳动生产率和生产管理水平，使生产管理由事后的、粗放管理模式向事前的、精细化管理模式转变，形成了适用于钢铁企业的能源在

线监测、能效分析平台和企业级能源优化系统，对于强化钢铁企业生产管控水平、规范内部管理、提高运作效率、节能减排、增产降耗发挥了巨大的作用。但由于大量信息系统和网络技术的应用，也给钢铁冶金企业生产控制系统带来了新的安全风险及挑战。

### 2.12.2 典型安全问题

随着美国“再工业化、先进制造”，德国“工业 4.0”，我国“制造强国，网络强国”等国家战略的推出，以及物联网、云计算、大数据等新一代信息技术的大规模应用，工业体系由自动化向数字化、网络化、智能化方向发展。新一轮产业变革为经济转型带来新机遇的同时，也加速了网络安全风险向工业领域全面渗透，工业信息安全问题日益凸显。

钢铁冶金行业信息化持续推进，能源管理中心投入运行，使原本相对独立的 DCS、PLC、仪器仪表、SCADA 等控制系统通过网络和信息系统连为一体。由于大量信息系统和网络技术的应用，给钢铁冶金企业生产控制系统带来了安全威胁，如图所示：

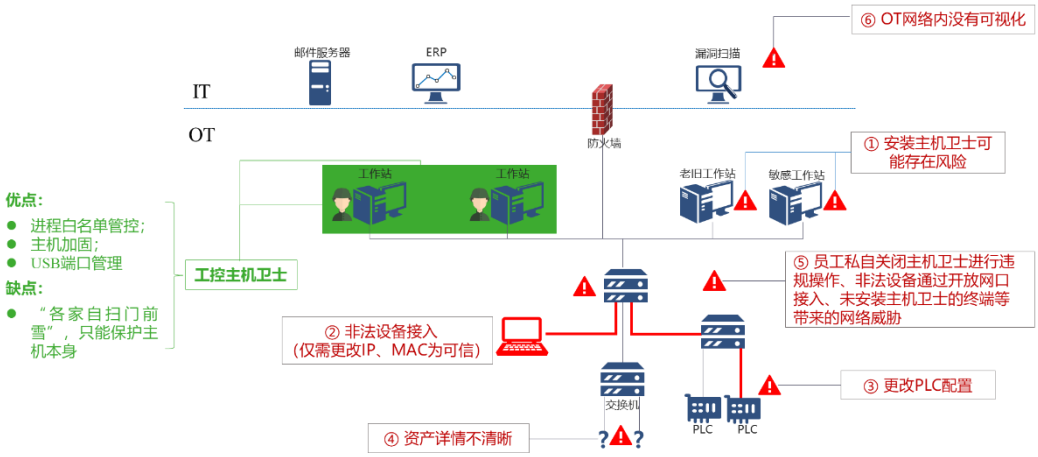


图 56　工业网络安全面临的威胁情况

1、 **老旧系统计算资源紧缺：**某些老旧操作系统计算资源比

较紧缺：安装主机卫士后，某些进程可能导致资源占用过大，影响工业软件的正常运行；

2、 **存在未授权软件：**许多国外的控制系统对于在主机上安装其他未经其授权的软件比较敏感，一旦发生安全事故，无法厘清相互之间的责任；

3、 **缺乏外联设备接入检测能力：**对于未经授权的 PC 设备（或其他主机）仅需更改 IP 和 MAC 即可顺利进入工业网络内部，当前系统缺乏对该类非法外联设备的接入检测；

4、 **缺少对行为实时检测手段：**非法外联设备进入工业网络内部之后，对 PLC 等控制系统的指令操作、配置更改等涉及业务安全的行为无法实时有效监测；

5、 **资产信息不清晰：**对工业资产的具体数量、漏洞情况、安全状态等信息不清晰；

**6、终端风险：**员工私自关闭主机卫士进行违规操作、非法设备通过开放网口接入、未安装主机卫士的终端等带来的病毒、木马等网络威胁；

**7、OT 网络缺少可视化能力：**OT 网络内没有可视化。工业网络内部资产情况、网络威胁情况、安全事件告警情况、其他网络安全设备数据关联情况等缺乏统一的管理平台进行可视化呈现和集中管控。

因此，需针对钢铁行业工业网络的特点，加强工业资产发现与管理、网络威胁事件监测、业务安全行为监测及 OT 网络安全可视化建设。

### 2.12.3 安全解决方案

通过与南钢相关人员的交流沟通，钢铁制造现场的参观与实践，深度了解钢铁生产制造流程与相关工艺，梳理钢铁制造生产流程与工艺（如图所示）。

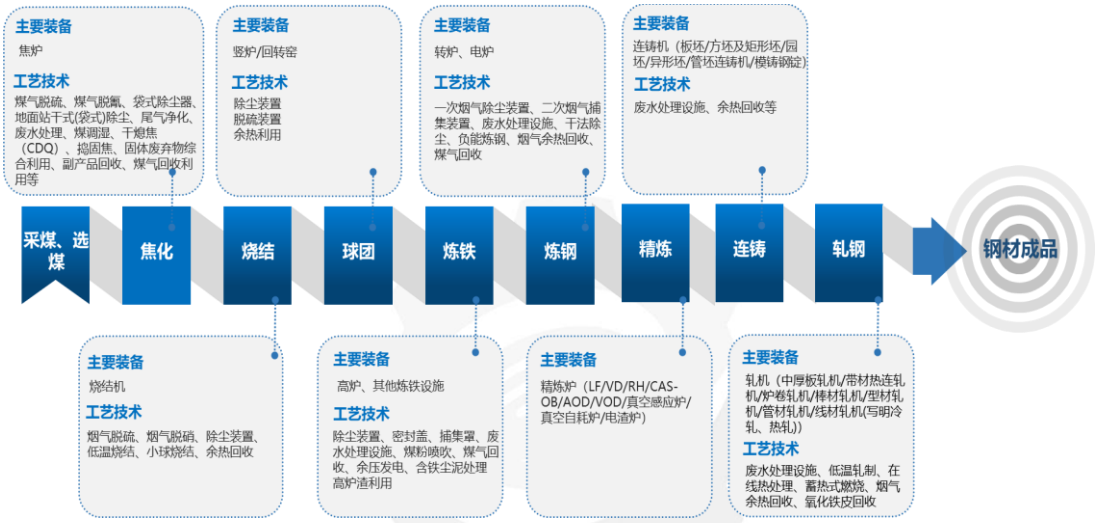


图 57　钢铁生产制造流程图

通过深度调研了解客户面临的安全问题，梳理出了钢铁行业当前面临的典型安全问题与迫切需求：

- 缺少对违规操作、非法接入设备等非法行为的安全监测手段；
- 当前安全产品没有结合钢铁制造业务与工艺流程；
- 缺少 OT 网络安全可视化体系；
- 缺少统一的安全设备管理平台。

#### 1、 总体方案

本方案已在南京钢铁有限公司等多个省份的行业客户落地应用实施，得到了客户的一致认可，其典型部署方案如图所示：

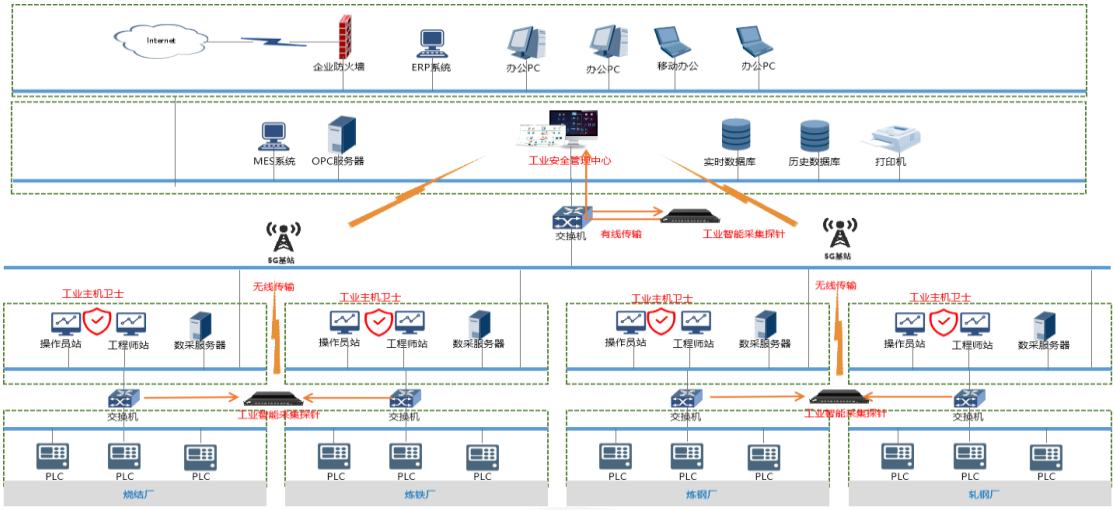


**图 58　典型部署方案图**

工业智能采集探针部署在工控网络各层流量汇聚节点的交换机旁，通过端口镜像的方式实现工控网络数据的全量采集，并基于边缘计算对采集的数据进行深度报文解析，剔除无效脏数据后生成安全日志，通过有线或者 5G 无线的方式加密传输给工业安全管理中心。

工业主机卫士部署在工控网络中的操作员站、工程师站、数控库服务器等终端设备上，通过监控主机的进程状态、网络端口状态、USB 端口状态，以白名单的技术方式，全方位地保护主机的资源使用，禁止非法进程的运行，禁止非法网络端口的打开与服务，禁止非法 USB 设备的接入，从而切断病毒和木马的传播与破坏路径。

工业安全管理中心对采集的日志信息进行关联分析，识别网络中内的所有资产，绘制资产拓扑图；监测生产现场异常操作、非法外联，非法接入等安全事件；对资产进行无损漏洞扫描，发现资产存在的漏洞；内置丰富的工控漏洞利用攻击模型库、以及工控木马病毒库，进行工控漏洞利用、工控木马病毒的监测。安

全管理中心可与第三方安全设备对接，进行安全日志的统一分析与审计，并通过高度可视化的界面给企业管理者带来直观的全网络一体化的安全态势详情。此外，工业安全管理中心可选择与省级工业互联网安全态势感知平台对接，一方面为省级平台提供深入到企业内部的数据支撑，解决省级平台在公网侧获取的数据源过于单一的问题；另一方面，企业可以从省级平台获取最新的漏洞、恶意 IP、安全事件等信息，完善企业的安全监测能力；从而实现监管侧与企业侧的数据联动，协同防御。

## 2、 技术路线

本项目依照先进性、可靠性、开放性的原则，为面向钢铁行业的工业互联网安全一体化平台设计了合理的技术路线，为技术研究、产品研制及方案应用提供扎实的理论基础，总体技术架构如图所示。

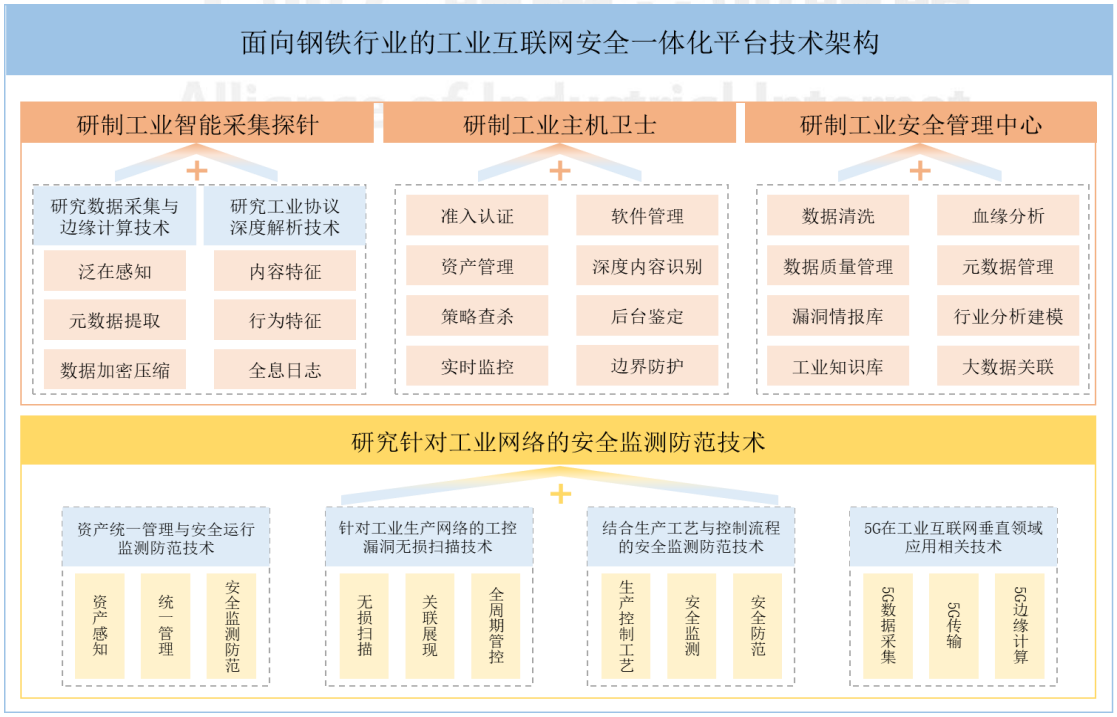


**图 59　面向钢铁行业的工业互联网安全一体化平台技术架构**

首先以工业互联网、网络安全、5G 及三者融合等相关技术为基础，展开针对资产统一管理与安全运行监测防范技术、工业生产网络的工控漏洞无损扫描技术、结合生产工艺与控制流程的安全监测防范技术、5G 在工业互联网垂直领域应用等方面展开技术研究，为后续产品研制提供坚实的理论基础。

开展面向工业互联网的泛在感知、元数据提取、数据加密压缩等工业数据采集与边缘计算技术，以及针对工业控制协议的特征提取、DPI 等深度解析技术的深度研究，并在此基础上研制工业智能采集探针设备，实现工业现场数据的全量、实时采集。

开展准入认证、策略查杀、资产管理、实时监控、软件管理、内容深度识别、后台鉴定、边界防护等安全防护技术，并在此基础上开发工业主机卫士产品，实现信息管理与信息安全防护。

开展数据接收、数据清洗、数据治理、数据分析等大数据技术，以及行业数据分析模型、行业基础信息库、工业知识库等信息库表的研究积累，并在此基础上开工业安全管理中心产品，实现工业数据的关联分析与结果呈现。

### 3、 功能架构

面向钢铁行业的工业互联网安全一体化平台整体功能架构如图所示。

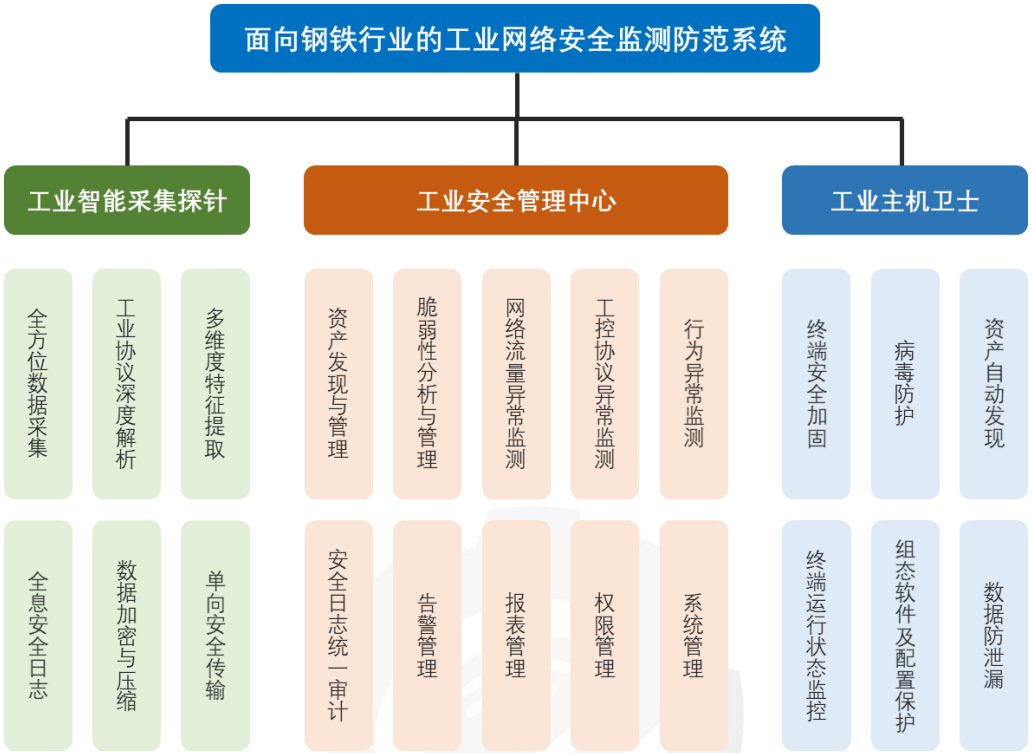


**图 60　面向钢铁行业的工业互联网安全一体化平台功能架构**

工业智能采集探针采用无害化方式旁路部署，在不影响正常生产的前提下实现工业现场数据全量采集，并凭借强大的 DPI 能力实现工业协议的深度解析，同时完成元数据提取及全息安全日志的加密传输；工业安全管理中心依靠丰富的数据分析模型对数据进行关联分析，完成精细化管理与安全监测；工业主机卫士能够帮助企业客户实现终端安全加固、终端运行状态监控、病毒防护、组态软件及配置保护、资产自动发现、数据防泄漏等安全防护功能，保障系统、网络安全。

### 4、 产品介绍

#### （1）工业互联网智能采集探针

工业智能采集探针是中新赛克研制的一款面向钢铁、石化、电力、智能制造等行业的具备工控网络数据采集和安全监测需求

的高端数据采集设备，以旁路方式部署在工控网络各层汇聚交换机侧，在不影响正常工业生产的前提下，实现对工业企业 OT 网络中的数据全量实时采集，支持设备运行状态数据采集、工业协议深度解析、多维度安全元数据提取、数据加密、格式化日志生成、单向安全传输等功能，具有工业级可靠性，满足工业网络安全相关标准要求，具备高端口密度、高性能和灵活部署能力。主要功能如下:

**1）全方位数据采集:** 工业智能采集探针通过采集工控网络各层汇聚节点交换机镜像的流量实现对工控网络所有通信数据的全量采集，实现对网络中通用主机、嵌入式主机、网络设备、安全设备、上位机、PLC 等设备的通信数据以及运行状态数据的采集。

**2）工业协议深度解析:** 工业智能采集探针支持数十种工业协议的识别与深度解析，可以解析到工业协议的种类、功能码、寄存器地址等，实现指令级的深度解析，并在进一步拓展中。目前支持的协议覆盖了多个行业的典型协议，包括常见的Modbus、Profinet、IEC104、DNP3、S7、BacNet、OPC 等。

**3）多维度特征提取:** 业智能采集探针支持多种类型的特征提取，为后端业务系统提供数据分析的业务数据支撑，主要支持以下特征的提取: 五元组特征提取、资产特征提取、工控漏洞特征提取、行为特征提取等。

**4）全息安全日志:** 工业智能采集探针在对数据预处理之后，可以将处理后的数据生成统一的日志格式，默认的数据格式为

TLV 日志格式，但可开启日志转换功能，生成 MQTT、Syslog 等友好的日志格式，从而可以很好的与第三方平台对接，如工业互联网平台等。

**5）数据加密与压缩：**工业智能采集探针在数据采集和传输的环节中，通过将处理完提取的全息日志采用国产加密算法的方式进行数据的安全防护，防止核心数据的泄露。此外，工业智能采集探针通过提取关键特征生成全息日志的方式进行高效的数据压缩，降低对工控网络传输资源的占用。

**6）单向安全传输：**工业智能采集探针提供了硬件增强的网络边界保护，确保所有的数据信息从 OT 网络到外部网络的单向传输和复制，从而阻止任何病毒，DOS 攻击，人为错误或其他任何网络攻击传播到受保护的网络中，保障部署后的高端安全可靠。

**（2）工业安全管理中心**

系秉承着丰富的大数据平台产品开发经验以及多年积累的工控网络安全监测研究基础，中新赛克为满足工控网络安全监测与统一管理的需求，研发了基于大数据平台的集多功能于一体的工业安全管理中心。工业安全管理中心内置丰富的工控安全知识库以及多种安全分析模块，基于工控网络萃取的各类安全数据，实现工业资产自动发现与网络拓扑可视化、资产漏洞扫描与管理以及工控网络异常威胁监测。同时其可对分布部署在网络中的安全设备进行统一配置管理，实现对企业安全防护产品的统一配置、全面监控、实时告警和联动处置。主要功能如下：

**1）资产发现与管理：**资产发现与管理是工业安全管理中心

的核心功能模块，其能够实现内网资产的扫描发现、手动管理、资产变更比对、资产全方位画像、资产安全监测以及可视化展示等功能。工业安全管理中心内置丰富的资产指纹库，通过指纹比对、SNMP 扫描等方式自动识别网络中的资产信息，包括服务器、路由器、主机等 IT 层资产以及上位机、PLC、控制器等工业现场资产，并结合流量深度分析为每个资产进行多维度画像，为每个资产打上品牌、型号、五元组、运行状态、通信、风险、责任人、责任部门等标签，从而实现资产的全方位监测。

**2）脆弱性分析管理：**工业安全管理中心通过多种威胁监测手段对工控网络进行威胁发现，威胁发现对象涵盖主流的网络主机、操作系统、数据库系统、组态软件以及 PLC 等，通过最新的威胁情报库、内网主机扫描结果、基线扫描结果、人工渗透测试结果等，将资产与威胁信息进行统一关联、展现和告警，使管理人员可以有效地跟踪威胁的全生命周期，清楚地掌握全网的安全健康状况，实现威胁的全生命周期的可视、可控和可管。

**3）网络流量异常监测：**工业安全管理中心可对网络中各个资产的网络流量模型进行统一的建模分析，建立符合当前资产以及网络流量的多种安全基准模型，如通信安全基线模型、网络流量基线模型等，针对不同的资产设置不同的网络流量阈值以及通信白名单等方式，对偏离于安全基线外的网络流量以及通信行为等进行实时的安全告警，从而发现非法外联、通信中断、流量突变等安全威胁。通过流量曲线图、柱状图和详尽的流量分布表等多种方式对整个控制网络总体流量监测结果进行展示。

**4）工控协议异常监测：**工业安全管理中心基于工业智能采集探针采集对工业协议的深度解析后的数据，可对工业协议实现指令级的异常监测，从而发现如下异常状况并进行实时报警。能够监测到的工控协议异常包括指令变更、阈值报警、组态变更、负载变更等。

**5）行为异常监测：**工业安全管理中心具备基于异常行为的事件关联分析功能，具备细粒度的动态周期性行为建模能力和基于多次指数平滑的行为预测能力。能对指定 IP 的事件行为特征（如错误比例、拒绝比例、频度、出现次数等）进行周期性建模，然后将实测值与建模值进行比较，判定异常；能根据指定 IP 的事件行为特征（如错误比例、拒绝比例、频度、出现次数等）的历史值通过预测算法预测出未来时间的取值区间，然后将实测值与预测值进行比较，判定异常。

**6）安全日志统一审计：**工业安全管理中心实时将网络中不同厂商的网络设备、安全设备、服务器、操作员站、数据库系统、工业智能采集探针的日志信息，进行统一地采集、范式化、分类、过滤和关联归并分析，实现分布式日志的统一采集和分析，帮助一线管理人员从海量日志中迅速、精准地识别安全事件，及时对安全事件进行追溯或干预，满足国家标准规范中关于日志审计的相关要求。

**7）告警管理：**工业安全管理中心告警管理模块可以向用户展示告警相关的统计视图，包括告警数量、告警类型分布、告警级别分布、告警状态统计、重点关注内容、告警趋势、待处置告

警列表、威胁情报命中排行、关联规则命中排行、最近告警列表等信息。

**8）报表管理：**工业安全管理中心可以提供灵活的报表管理功能，包括资产、安全事件、风险分析等，支持快速生成报表，实时的输出期望的报表内容，也可按照客户指定的周期自动生成报表以帮助用户周期回顾安全情况。同时系统提供了报表模板的灵活编辑，用户可以根据自身需求在多个预制报表模板中选择自身需要内容，调整顺序以形成自身需要的报表。

**9）权限管理：**工业安全管理中心可以针对不同的人员设置不同的权限，分别为超级管理员、系统管理员和日志审计员。超级管理员主要负责用户的创建、删除和功能证书的管理；系统管理员负责主要负责平台的业务配置和管理，包括规则的管理和报警的处理等；日志审计员可对安全日志进行审计。

**10）系统管理：**系统具有丰富的自身配置管理功能，包括自身配置、系统运行参数监控等。系统具有自身运行监控与告警、系统日志记录，存储，备份等功能。

**（3）工业主机卫士**

工业主机卫士是专门保护工控主机环境的一款安全软件，其部署在工控上位机等工控网络主机上，通过监控工控主机的进程状态、网络端口状态、USB 端口状态，以白名单的技术方式，全方位地保护主机的资源使用。根据白名单策略，工控主机安全产品会禁止非法进程的运行，禁止非法网络端口的打开与服务，禁止非法 USB 设备的接入，从而切断病毒和木马的传播与破坏路径。

主要功能如下:

1）**终端安全加固：**通过禁用系统 Autorun、终端的账号和共享的匿名枚举、终端的可匿名的共享、系统安全模式的功能、Windows 远程桌面、设置 Windows 账号策略和密码复杂度策略等，对终端操作系统进行安全加固，防止终端用户误操作，并有效预防蠕虫病毒和木马对计算机终端带来的攻击。

2）**终端运行状态监控：**通过海量工业环境终端软件白名单库，并结合管理员手工增加，工控终端只能运行指定的软件，在白名单之外的软件，都将被禁止。通过设置 MD5 码校验的方式检查进程名，防止用户对程序改名逃避安全检查。内置进程网络访问控制白名单，针对工控终端实现基于进程、端口或协议的双向访问的细粒度访问控制，确保工控终端的所有网络访问都是受到许可的，即使终端通过其他途径感染了病毒或恶意代码，也能切断其传播途径，减轻。

3）**病毒防护：**采用网络接入结束，确保只有受系统管理并且符合安全策略的终端才允许接入 OT 网络，否则将被隔离在工控网络之外，彻底消除蠕虫病毒、木马侵害的源头以及别有用心的偷窥和网络滥用。通过管理、控制和监控计算机终端外设使用情况，结合对未知设备进行自动检测和采样，实现对未知和新增设备的有效控制和管理，确保工控终端与外界的数据交换在可控的环境中进行，防止通过终端外设将病毒传入到工控终端，从而传播到整个工控网络。

4）**组态软件及配置保护：**通过操作系统内核技术，监控各

种程序对组态软件及其配置文件的访问和修改。确保组态软件不被修改、组态配置文件只能被组态软件读取和修改，杜绝第三方程序查看配置文件内容、阻止第三方程序修改组态软件及其配置文件，消除威胁安全生产的隐患，保证工业控制系统的安全。

**5）资产自动发现：**自动获取工业主机 CPU、内存、硬盘等基础信息，同时生成日志发送给管理中心，形成资产清单，实现资产属性的统一维护。

**6）数据防泄漏：**支持文件权限的设计、白名单等安全策略，防止数据的肆意拷贝和无授权的访问。

**5、 方案亮点**

该解决方案开发的硬件防护产品工业智能采集探针采用无铅化的设计标准，不仅给同行业相关企业试点示范的作用，也可推进国家相关强制标准规范的实施。无铅化的标准，一方面有利于生产工人的身体健康，另一方面有利于保护环境。从长远看，其具有良好的环境生态效益。

该产品是中新赛克自主研发创造，推进国家相关强制标准规范实施，加快网络安全产品国产化建设，让网络安全可信，避免采购外国品牌存在网络“后门”，减少关键信息基础设施内的脆弱点。

该解决方案依据工业互联网创新发展三年行动计划（2021-2023 年）顺利实施，将推动《关于加强工业互联网安全工作的指导意见（征求意见稿）》，落实提升企业工业互联网安全防护水平和强化工业互联网数据安全保护能力要求的发展，起

带头示范的作用，有助于更多安全公司和工业企业落实指导意见，有助于促进工业互联网信息安全产业发展。当前，我国传统信息安全厂商逐渐关注工业控制系统信息安全，针对工业控制系统实时性、可用性等特点设计了相关安全防护产品。但这些产品和解决方案的思路相对偏向信息网络的安全防护，大多集中在工业防火墙、网关等单点主动防护设备。本方案从更适用工控网络和客户真实需求安全监测的角度，设计工控网络安全解决方案，为即将进入及已经进入工控网络安全市场的友商，提供新的技术方向。

随着本项目的顺利实施和其带来的示范效应，将会有更多的工业企业重视公司的网络的安全，将企业的网络安全体系建设起来。从而可以有效的保障工业企业的网络安全，而保障工业企业的网络安全从侧面就是保障企业的资产安全、保障工业企业的安全生产，保障企业不因为网络安全攻击事件导致停产的问题，避免像台积电类似的事件再次发生，从而帮助企业创造更多的价值，避免经济损失。

工业互联网产业联盟
Alliance of Industrial Internet

### 6、 项目先进性及创新点

#### （1） 项目的先进性

随着我国工业互联网的飞速发展及工控安全市场的爆发，绝大多数传统信息安全厂商加入市场角逐，由于其在工控领域的积累不足，造成安全解决方案多样、不足、片面的情况普遍存在，并且方案缺少针对性、落地性。项目组结合工业现场、工业互联网、网络安全等相关技术展开研究，取得多项专利、软著等技术成果，在相关领域获得多项省部级荣誉奖项，其中：

**部级荣誉奖项**主要包括:

- 2019 年工业互联网试点示范项目（中新赛克）
- 2019 年工业互联网试点示范项目（南钢）
- 2018 年网络安全技术应用试点示范项目
- 2018 年制造业与互联网融合发展试点示范

**省级荣誉奖项**主要包括:

- 2019 年智慧江苏重点工程
- “腾云驾数”优秀产品
- “腾云驾数”优秀解决方案
- 江苏省工业互联网发展示范企业（平台类）
- 江苏省工业互联网示范工程（标杆工厂类）
- 江苏省工业互联网示范工程（企业上云类）

本项目基于对钢铁行业工业现场的深入调研和深刻理解，以保障生产、抵御威胁为目标，提出工业互联网安全监测解决方案，本项目中所使用的方案框架清洗、前瞻性强，产品集成度高、易用性强，处于国内领先水平，其先进性主要体现在如下几个方面:

- IT-OT 一体化安全监测
- 超高的可靠性与稳定性
- 无铅化设计提升产品的国际竞争力
- 自适应端口速率满足网络未来发展需求
- 支持多种日志格式
- 集多功能于一体的安全管理中心
- 丰富灵活的算子

- 全流程可视化大数据处理方式与业务呈现

**（2）项目的创新点**

基于对钢铁行业、及其他典型行业的深入调研，结合项目团队在工业互联网安全领域的技术与实践积累，本项目提出的工业互联网安全监测解决方案思路新颖，核心技术具有创新性，所使用的软硬件产品已在一定程度上实现自主可控，并制定国产化全面替代计划。本项目主要创新点包含以下几个方面：

- **技术创新：**结合生产工艺与控制流程的控制网络安全检测方法
- **技术创新：**基于多维度特征的工控协议深度解析
- **技术创新：**基于物理网与信息网深度融合的系统模型
- **方案创新：**基于钢铁行业工艺流程的自适应动态安全防护模型
- **方案创新：**边缘计算技术与安全监测方案的深度融合
- **方案创新：**数据采集设备“无害化”灵活部署
- **应用创新：**工业互联网安全监测方案行业应用的有益探索
- **自主可控：**产品自主可控程度高，国产化替代计划完备

**7、 实施效果**

**（1）项目应用效果**

该项目于 2019 年 11 月顺利推出后，首次落地应用是 12 月份在南京钢铁有限公司的高速线材厂部署实施，经过现场工勘、客户需求深度对接沟通后，部署了 16 套工业主机卫士、4 台工

业智能采集探针以及 1 套工业安全管理中心系统。系统上线之后，在很短的时间内帮助客户构建了整个工控网络的安全可视化体系，发现僵尸资产 12 台、查杀拦截病毒 53 次、监测违规操作 20 余次，避免重大安全事故 2 次。

**（2）实用性分析**

本项目提出的工业互联网安全额解决方案不仅在钢铁行业发挥了重要作用，还能够根据具体需求，协助提升多个典型行业工业互联网安全检测能力。在首个试点顺利应用后，该方案成功在全国多个钢铁企业推广应用。

### 2.12.4 小结

该解决方案面临巨大的市场需求和业务驱动，不仅可为公司带来显著的业务增长，还可从侧面推动整个产业链的发展，包括芯片厂商、安全服务厂商、测评机构、设备代工厂商、其他安全公司，为社会和国家带来巨大效益。

其次，该解决方案开发的硬件防护产品采用无铅化的设计标准，不仅给同行业相关企业试点示范的作用，也可推进国家相关强制标准规范的实施。无铅化的标准，一方面有利于生产工人的身体健康，另一方面有利于保护环境。从长远看，其具有良好的环境生态效益。

同时，该产品是中新赛克自主研发创造，推进国家相关强制标准规范实施，加快网络安全产品国产化建设，让网络安全可信，避免采购外国品牌存在网络“后门”，减少关键信息基础设施内的脆弱点。

除此之外，随着解决方案的顺利实施和其带来的示范效应，将会有更多工业企业重视公司网络安全，建设企业网络安全体系，从而有效保障工业企业的网络安全。保障工业企业的网络安全是保障企业的资产安全和工业企业的安全生产，保障企业不因网络安全攻击事件导致停产，避免类似台积电的事件再次发生，从而帮助企业创造更多价值，避免经济损失。

### 2.12.5 单位基本信息

1. 南京中新赛克科技有限责任公司

中新赛克成立于 2007 年，原为中兴通讯控股子公司。2012 年，由深圳市国资委下属的深圳市创新投资集团有限公司投资控股，并于 2017 年 11 月在深交所上市。

公司在工业互联网安全领域已入选工业互联网产业联盟成员单位、工业控制系统信息安全产业联盟理事单位、工业信息安全产业发展联盟成员单位、南京工业互联网产业联盟理事单位。公司具有一支实力雄厚的研发团队，核心成员均具有丰富网络安全、工控安全的从业经验，主持或参与多项国家级相关课题，取得多项专利和软著，团队参加过第一届护网杯、工业信息安全技能大赛、CTF 等多项工业互联网网络安全赛事，并取得优异成绩。

2. 江苏省互联网行业管理服务中心

江苏省互联网行业管理服务中心是省通信管理局下属全额拨款事业单位，承担我省互联网行业管理、三网融合网络信息安全管理的技术支撑和服务工作。

3. 南京钢铁有限公司

南京钢铁有限公司始建于1958年，于2000年9月在上海证券交易所上市，具备年产1000万吨钢的生产能力，以专用板材、优特钢长材为主导产品，打造“2+3+4”高端研发平台，建立“产销研用+服务”一体化的精益研发体系，打造钢铁新材料为核心的相互赋能、复合成长的产业链生态圈。

工业互联网产业联盟
Alliance of Industrial Internet

## 3. 结束语

当前工业互联网基础设施建设加快，云计算、5G、人工智能、大数据等新技术广泛应用，为工业企业制造、生产、运营带来极大的变革，同时也使得工业企业面临着更多的安全风险。

在工业和信息化部网络安全管理局指导和支持下，中国移动携手相关单位共同完成本报告的编写，以期为工业互联网的发展贡献一份力量。本报告从工业互联网安全的实践层面，响应国家的决策部署，着眼于新技术融合带来的安全问题以及固有的安全风险，汇编了业内优秀安全解决方案，为工业企业提供安全建设参考。

安全是工业互联网的保障。在未来，工业互联网这一新兴基础设施建设将向更广范围、更深程度、更高水平不断推进。面对新技术以及安全防护新形势，工业互联网安全生态将不断面临新的挑战，这需要安全行业与工业行业互相协作，深耕工业互联网安全，不断推出新的安全解决方案，提升各方应对安全风险的能力，协同打造安全的工业互联网，才能更好的赋能工业互联网，推动产业升级，促进工业互联网的繁荣与发展。

希望联盟持续致力于工业互联网安全生态的构建，为成员单位提供开放、共享的平台，与产业链合作伙伴互利共赢，实现商业价值的提升，推动工业互联网安全领域的持续发展。