钢铁行业工业互联网安全解决方案

上海宝信软件股份有限公司

网络行业应用篇/工业互联网安全

1 概述

1.1 背景

伴随着互联网信息技术、工业自动化技术的革命性突破和全球经济一体化的发展，工业互联网应运而生，并迅速成为热门技术，已经成为钢铁行业不断研究和持续探索的热点课题。经过近几年的发展，钢铁工业互联网的推广普及已经成为工业经济发展提供了更多的内驱力。为更好地激发工业互联网的技术潜能，引领工业互联网技术实现技术应用开发。钢铁工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

网络体系是实现连接钢铁行业工业系统、全价值链、全产业链的基础，包括网络互连、标识解析、应用支撑三大体系。数据包括“采集交换-集成处理-建模分析-决策与控制”，形成优化闭环，驱动工业智能化。安全是钢铁行业工业互联网各个领域和环境的安全保障，包括设备安全、控制安全、网络安全、应用安全和数据安全等。为加速提升工业互联网的应用质量与效果，为

我国的经济结构调整、动能转换贡献力量，全面推进“中国制造2025”和“互联网+”行动计划，有必要围绕国家网络安全法和网络安全等级保护制度加强对钢铁行业工业互联网信息安全领域解决方案的研究。

1.2 适用范围

钢铁行业工业互联网。

1.3 在工业互联网网络体系架构中的位置

本解决方案在下图中所处的位置为⑦。

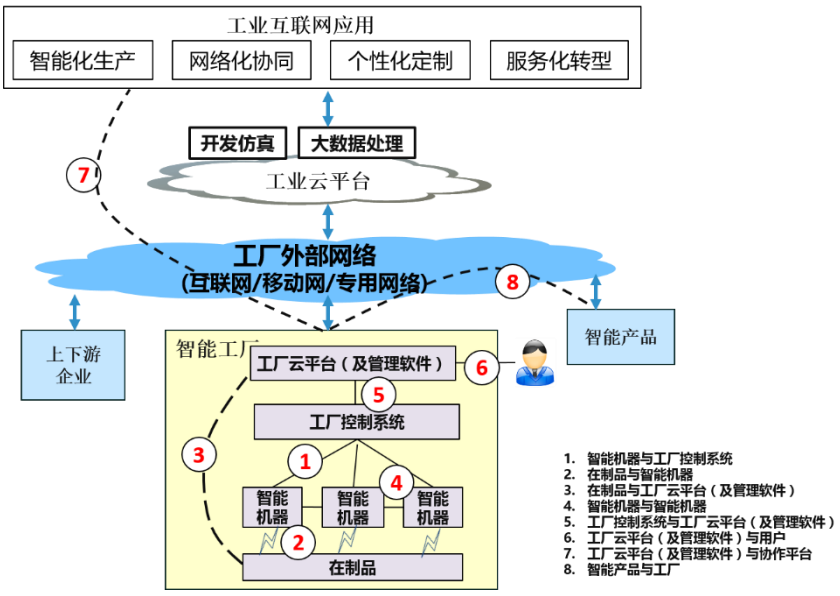

图 1 工业互联网互联示意图

2 需求分析

2.1 钢铁行业工业互联网脆弱性分析

2.1.1 操作系统漏洞

PC 与 Windows 的技术架构现已成为控制系统上位机的主流。而在控制网络中，上位机是实现与 MES 通信的主要网络结点，因此其操作系统的漏洞就成为了整个控制网络信息安全中的一个

短板。操作系统漏洞频繁出现，安全事故时有发生。以 Windows XP 版本为例，就曾被发现了大量漏洞，典型的如输入法漏洞、IPC$漏洞、RPC 漏洞、Unicode 漏洞、IDA&IDQ 缓冲区溢出漏洞、Printer 溢出漏洞、Cookie 漏洞等等。这些漏洞大部分危害巨大，恶意代码通过这些漏洞，可以获得 Windows XP 操作站的完全控制权，甚至为所欲为。

2.1.2 工业控制系统漏洞

由于早期的钢铁行业工业控制系统都是在相对独立的网络环境下运行，在产品设计和网络部署时，只考虑了功能性和稳定性，对安全性考虑不足。随着钢铁行业工业控制系统网络之间互联互通的不断推进，以及工控系统和工业设备接入互联网的数量越来越多，通过互联网对工业控制系统实施攻击的可能性越来越高，而每年新发现的 SCADA、DCS、PLC 漏洞数量也不断增加，这些都为钢铁行业工业互联网带来巨大的安全隐患。

2.1.3 工业网络漏洞

钢铁工业控制网络的设备分布于厂区各处，由于网络基础设施的局限性，经常需要无线网络、卫星、GPRS/CDMA 等通用传输手段来实现与调度中心的连接和数据交换。这些传输手段没有足够的安全保护和加密措施，很容易出现网络窃听、数据劫持、第三人攻击等安全问题，而且攻击者还可以利用不安全传输方式作为攻击工业控制网络的入口，实现对于整个工业控制网络的渗透和控制。

2.1.4 工业云平台安全问题

在钢铁行业工业云平台中，作为底层支撑技术的虚拟化技术在带来效率提升和开销降低的同时，也带来了一系列由于物理的共享与逻辑隔离的冲突而导致的数据安全问题。在钢铁行业公有云环境下，不同机构之间物理隔离的网络被由网络虚拟化技术构建的虚拟网络取代。这种网络资源复用模式虽然实现了网络资源的高效利用、网络流量的集中分发，但也带来了诸多安全问题。

2.2 钢铁行业工业互联网安全威胁分析

2.2.1 来自外部网络的渗透

钢铁行业工业互联网会有较多的开放服务，攻击者可以通过扫描发现开放服务，并利用开放服务中的漏洞和缺陷登录到网络服务器获取企业关键资料，同进还可以利用办公网络作为跳板，逐步渗透到控制网络中。通过对于办公网络和控制网络一系列的渗透和攻击，最终获取企业重要的生产资料、关键配方，严重的是随意更改控制仪表的开关状态，恶意修改其控制量，造成重大的生产事故。

2.2.2 帐号口令破解

由于企业有对外开放的应用系统（如邮件系统），在登录开放应用系统的时候需要进行身份认证，攻击都通过弱口令扫描、Sniffer 密码嗅探、暴力破解、信任人打探套取或社工比较合成口令等手段来获取用户的口令，这样直接获得系统或应用权限。获取了用户权限就可以调取相关资料，恶意更改相关控制设施。

2.2.3 利用移动介质攻击

当带有恶意程序的移动介质连接到工程师站或操作员站时，移动介质病毒会利用移动介质自运行功能，自动启动对控制设备进行恶意攻击或恶意指令下置。一方面造成网络病毒在企业各个网络层面自动传播和感染，靠成业务系统和控制系统性能的下降，从而影响企业监测、统筹、决策能力。另一方面会针对特定控制系统或设备进行恶意更改其实际控制量，造成生成事故。

2.2.4 PLC 程序病毒的威胁

通过对工程师站及编程服务器的控制，感染（替换）其相关程序，当 PLC 程序的下发时，恶意程序一起被下发到 PLC 控制设备上。恶意程序一方面篡改 PLC 的实际控制流，另一方面将运算好的虚假数据发给 PLC 的输出，防止报警。通过这种方式造成现场设备的压力、温度、液位失控，但监测系统不能及时发现，造成重大的安全事故。

2.2.5 利用工业通信协议的缺陷

Modbus、DNP3、OPC 等传统工业协议缺乏身份认证、授权以及加密等安全机制，利用中间人攻击捕获和篡改数据，给设备下达恶意指令，影响生产调度，造成生产失控。

2.2.6 利用无线网络入侵

控制网络通过 DTU 无线设备通过 802.11b 协议连接到管理区的网络，通过对网络无线信息的收集，侦测 WEP 安全协议漏洞，破解无线存取设备与客户之间的通讯，分析出接入密码，从而成

功接入控制网络，控制现场设备，获取机要信息，更改控制系统及设备的控制状态，造成重大影响。

3 解决方案

3.1 设计思路

钢铁行业工业互联网安全框架设计是在充分借鉴传统网络安全框架和国外工业互联网安全相关框架的基础上，结合我国钢铁行业工业互联网的特点研究并提出的，旨在指导钢铁行业工业互联网开展安全防护体系建设，提升安全防护能力。

钢铁行业工业互联网安全防护对象是明确工业互联网安全防护工作范围的基础，并为防护工作的实施指明方向。在传统网络安全框架与工业互联网安全相关框架中，都对其防护对象做了明确界定，钢铁行业工业互联网安全体系部分也从防护对象角度提出了工业互联网安全的五大重点方向，即安全保障、平台安全、网络安全、应用安全和工控安全。

3.2 安全建设目标

为确保钢铁行业工业互联网的正常运转和安全可信，应对工业互联网设定合理的安全目标，并根据相应的安全目标进行风险评估和安全策略的选择实施。工业互联网安全目标并非是单一的，需要结合工业互联网不同的安全需求进行明确。工业互联网安全包括保密性、完整性、可用性、可靠性、弹性和隐私六大目标，这些目标相互补充，共同构成了保障工业互联网安全的关键特性。

- 保密性：确保信息在存储、使用、传输过程中不会泄漏给

非授权用户或实体。

- 完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
- 可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。
- 可靠性：确保工业互联网系统在其寿命区间内以及在正常运行条件下能够正确执行指定功能。
- 弹性回复：确保工业互联网系统在受到攻击或破坏后恢复正常功能。
- 隐私安全：确保工业互联网系统内用户的隐私安全。

3.3 安全设计框架

钢铁行业工业互联网安全设计框架主要不同的防护对象部署相应的安全防护措施，根据实时监测结果发现网络中存在的或即将发生的安全问题并及时做出响应。同时加强防护管理，明确基于安全目标持续改进的管理方针，保障工业互联网的持续安全。钢铁工业互联网安全框架如下图所示。

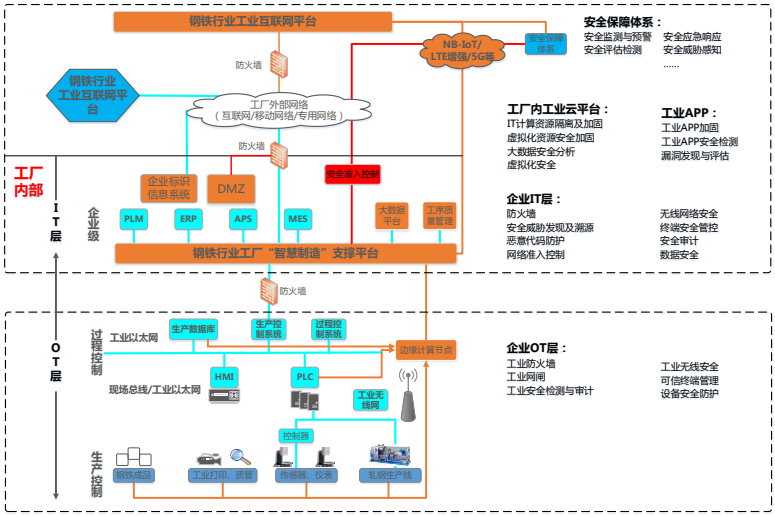

图 2 钢铁行业工业互联网安全整体架构图

钢铁行业工业互联网安全整体架构设计主要考虑钢铁行业以属地化生产业务为主，因此聚焦于工厂内网环境，主要分为 5 个方面内容组成，分别是安全保障体系、工业云平台、工业应用、网络安全和工业控制系统安全，其中钢铁行业 IT 层面关注于安全保障体系、工业云平台、工业应用和网络安全，OT 层面关注于工业控制系统安全。

3.4 钢铁行业 IT 层面安全建设方案

3.4.1 安全保障体系

3.4.1.1 安全评估

钢铁行业工业互联网必须以安全风险管控为切入点，必须定期对工业互联网系统的各安全要素进行风险评估。对应工业互联网整体安全目标，分析整个工业互联网系统的资产、脆弱性和威胁，评估安全隐患导致安全事件的可能性及影响，结合资产价值，明确风险的处置措施，包括预防、转移、接受、补偿、分散等，确保在工业互联网数据私密性、数据传输安全性、设备接入安全

性、平台访问控制安全性、平台攻击防范安全性等方面提供可信服务，并最终形成风险评估报告。

3.4.1.2 安全监测与预警

钢铁行业工业互联网要构建一个能覆盖安全业务全生命周期的，以安全事件为核心，实现对安全事件的“预警、检测、响应”动态防御体系。能够在攻击发生前进行有效的预警和防护，在攻击中进行有效的攻击检测，在攻击后能快速定位故障，进行有效响应，避免实质损失的发生。

安全策略中描述了工业互联网总体的安全考虑，并定义了保证工业互联网日常正常运行的指导方针及安全模型。通过结合安全目标以及风险评估结果，明确当前工业互联网各方面的安全策略，包括对设备、控制、网络、应用、数据等防护对象应采取的防护措施，以及监测响应及处置恢复措施等。同时，为打造持续安全的工业互联网，面对不断出现的新的威胁，需不断完善安全策略。

3.4.1.3 安全威胁感知

钢铁行业工业互联网安全威胁监测感知是部署相应的安全监测措施，主动来自系统内外部的安全风险，具体措施包括数据采集、收集汇聚、特征提取、关联分析、状态感知等。数据采集指对工业现场网络及工业互联网平台中各类数据进行采集，为网络异常分析、设备预测性维护等提供数据来源。对于数据的收集汇聚主要分为两个方面。一是对 SCADA、MES、ERP 等工业控制系

统及应用系统所产生的关键工业互联网数据进行汇聚，包括产品全生命周期的各类数据的同步采集、管理、存储及查询，为后续过程提供数据来源。二是对全网流量进行监听，并将监听过程中采集到的数据进行汇聚。特征提取是指对数据特征进行提取、筛选、分类、优先级排序、可读等处理，从而实现从数据到信息的转化过程，该过程主要是针对单个设备或单个网络的纵向数据分析。信息主要包括内容和情景两方面，内容指工业互联网中的设备信号处理结果、监控传输特性、性能曲线、健康状况、报警信息、DNC 及 SCADA 网络流量等；情景指设备的运行工况、维护保养记录、人员操作指令、人员访问状态、生产任务目标、行业销售机理等。关联分析过程通过将运行机理、运行环境、操作内容、外部威胁情报等有机结合，基于大数据进行横向大数据分析和多维分析，利用群体经验预测单个设备的安全情况，或根据历史状况和当前状态的差异发现网络及系统异常。状态感知基于关联分析过程，实现对企业工业互联网运行规律、异常情况、安全目标、安全态势、业务背景等的认知，确定安全基线，结合大数据分析技术，发现潜在威胁、预测黑客攻击。

3.4.2 工业云平台安全

对于钢铁行业工业互联网平台是业务生产稳定运行的基础保障，可采取的安全措施包括安全审计、认证授权、大数据安全分析等。并对平台公开漏洞和后门并加以修补；对恶意行为进行实时监测，以发现可疑行为并进行异常阻止，从而降低未

公开漏洞产生的危害。

1）安全审计

安全审计主要是指对平台中与安全有关的活动的相关信息进行识别、记录、存储和分析。平台建设过程中应考虑具备一定的安全审计功能，将平台与安全有关的信息进行有效识别、充分记录、长时间的存储和自动分析。能对平台的安全状况做到持续、动态、实时的有依据的安全审计，并向用户提供安全审计的标准和结果。

2）认证授权

工业互联网平台用户分属不同企业，需要采取严格的认证授权机制保证不同用户能够访问不同的数据资产。同时，认证授权需要采用更加灵活的方式，确保用户间可以通过多种方式将数据资产分模块分享给不同的合作伙伴。

3）安全隔离

平台不同用户之间应当采取必要的措施实现充分隔离，防止蠕虫病毒等安全威胁通过平台向不同用户扩散。平台不同应用之间也要采用严格的隔离措施，防止单个应用的漏洞影响其他应用甚至整个平台的安全。

4）大数据安全监测

基于大数据安全监测技术，对平台实施集中、实时的安全监测，监测内容包括各种物理和虚拟资源的运行状态等。通过对系统运行参数（如网络流量、主机资源和存储等）以及各类

日志进行分析，确保工业互联网平台提供商可执行故障管理、性能管理和自动检修管理，从而实现平台运行状态的实时监测。

5）补丁升级

钢铁行业工业互联网平台搭建在众多底层软件和组件基础之上。由于工业生产对于运行连续性的要求较高，中断平台运行进行补丁升级的代价较大。因此平台在设计之初就应当充分考虑如何对平台进行补丁升级的问题。

6）虚拟化安全

虚拟化是边缘计算和云计算为基础，为避免虚拟化出现安全问题影响上层平台安全，在平台安全防护中要充分考虑虚拟化安全。虚拟化安全的核心是实现不同层次及不同用户的有效隔离，其安全增强可以通过采用虚拟化加固等防护措施来实现，并增加恶意代码检测及防病毒安全体系。

3.4.3 工业应用安全

钢铁行业工业应用软件是推进智能化生产、网络化协同、个性化定制、服务化延伸等方面的重要载体。对工业应用程序而言，最大的风险来自安全漏洞，包括开发过程中编码不符合安全规范而导致的软件本身的漏洞以及由于使用不安全的第三方组件而引起的漏洞等。

1）代码审计

代码审计指检查源代码中的缺点和错误信息，分析并找到这

些问题引发的安全漏洞，并提供代码修订措施和建议。开发过程中应该进行必要的代码审计，发现代码中存在的安全缺陷并给出相应的修补建议。企业应对工业应用程序开发者进行软件源代码安全培训，包括：了解应用程序安全开发生命周期（SDL）的每个环节，如何对应用程序进行安全架构设计，具备所使用编程语言的安全编码常识，了解常见源代码安全漏洞的产生机理、导致后果及防范措施，熟悉安全开发标准，指导开发人员进行安全开发，减少开发者引入的漏洞和缺陷等，从而提高工业应用程序安全水平。

2）漏洞发现

漏洞发现是指基于漏洞数据库，通过扫描等手段对指定工业应用程序的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。在应用程序上线前和运行过程中，要定期对其进行漏洞发现，及时发现漏洞并采取补救措施。

3）审核测试

对工业应用程序进行审核测试是为了发现功能和逻辑上的问题。在上线前对其进行必要的审核测试，有效避免信息泄漏、资源浪费或其他影响应用程序可用性的安全隐患。

4）行为监测和异常阻止

对工业应用程序进行实时的行为监测，通过静态行为规则匹配或者机器学习的方法，发现异常行为，发出警告或者阻止高危行为，从而降低影响。

5) 防篡改及身份授权

工业互联网中的控制软件可归纳为数据采集软件、组态软件、过程监督与控制软件、单元监控软件、过程仿真软件、过程优化软件、专家系统、人工智能软件等类型。增加工业软件防篡改功能，保障控制软件安全的重要环节，对于控制软件应采取恶意代码检测、预防和恢复的控制措施。

3.4.4 网络安全

钢铁行业工业互联网的发展使得工厂内部网络呈现出 IP 化、无线化、组网方式灵活化与全局化的特点，工厂外网呈现出信息网络与控制网络逐渐融合、企业专网与互联网逐渐融合以及产品服务日益互联网化的特点，是造成传统互联网中的网络安全问题开始向工业互联网蔓延，钢铁行业应用过程中主要表现为以下几个方面：工业互联协议由专有协议向以太网/IP 协议转变，导致攻击门槛极大降低；工厂现有 10M/100M 工业以太网交换机性能较低；工厂网络互联、生产、运营逐渐由静态转变为动态，安全策略面临严峻挑战等。随着工厂业务的拓展和新技术的不断应用，今后还会面临 5G/SDN 等新技术引入、工厂内外网互联互通进一步深化等带来的安全风险。

工业互联网网络安全防护应面向工厂内部网络、外部网络及标识解析系统等方面，具体包括融合网络结构优化、边界安全防护、接入认证、通信内容防护、通信设备防护、安全监测审计等多种防护措施，构筑立体化的网络安全防护体系。

1）优化网络架构

在网络规划阶段，需设计合理的网络结构。一方面通过在关键网络节点和标识解析节点采用双机热备和负载均衡等技术，应对业务高峰时期突发的大数据流量和意外故障引发的业务连续性问题，确保网络长期稳定可靠运行。另一方面通过合理的网络结构和设置提高网络的灵活性和可扩展性，为后续网络扩容做好准备。

2）网络边界安全

根据工业互联网中网络设备和业务系统的重要程度将整个网络划分成不同的安全域，形成纵深防御体系。安全域是一个逻辑区域，同一安全域中的设备资产具有相同或相近的安全属性，如安全级别、安全威胁、安全脆弱性等，同一安全域内的系统相互信任。在安全域之间采用网络边界控制设备，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。

3）网络接入认证

接入网络的设备与标识解析节点应该具有唯一性标识，网络应对接入的设备与标识解析节点进行身份认证，保证合法接入和合法连接，对非法设备与标识解析节点的接入行为进行阻断与告警，形成网络可信接入机制。网络接入认证可采用基于数字证书的身份认证等机制来实现。

4）通信和传输保护

通信和传输保护是指采用相关技术手段来保证通信过程中的机密性、完整性和有效性，防止数据在网络传输过程中被窃取或篡改，并保证合法用户对信息和资源的有效使用。通过加密等方式保证非法窃取的网络传输数据无法被非法用户识别和提取有效信息。增加网络传输的数据采取校验机制，确保被篡改的信息能够被接收方有效鉴别。应确保接收方能够接收到网络数据，并且能够被合法用户正常使用。

5）网络设备安全防护

为了提高网络设备与标识解析节点自身的安全性，保障其正常运行，网络设备与标识解析节点需要采取一系列安全防护措施，对登录网络设备与标识解析节点进行运维的用户进行身份鉴别，并确保身份鉴别信息不易被破解与冒用；对远程登录网络设备与标识解析节点的源地址进行限制；对网络设备与标识解析节点的登录过程采取完备的登录失败处理措施；启用安全的登录方式（如 SSH 或 HTTPS 等）。

6）安全监测审计

网络安全监测指通过漏洞扫描工具等方式探测网络设备与标识解析节点的漏洞情况，并及时提供预警信息。网络安全审计指通过镜像或代理等方式分析网络与标识解析系统中的流量，并记录网络与标识解析系统中的系统活动和用户活动等各类操作行为以及设备运行信息，发现系统中现有的和潜在的安全威胁，实时分析网络与标识解析系统中发生的安全事件并告警。同时记

录内部人员的错误操作和越权操作，并进行及时告警，减少内部非恶意操作导致的安全隐患。

7）数据安全

钢铁行业工业互联网相关的数据按照其属性或特征，可以分为四大类：设备数据、业务系统数据、知识库数据、用户个人数据。根据数据敏感程度的不同，可将工业互联网数据分为一般数据、重要数据和敏感数据三种。工业互联网数据涉及数据采集、传输、存储、处理等各个环节。随着工厂数据由少量、单一、单向向大量、多维、双向转变，工业互联网数据体量不断增大、种类不断增多、结构日趋复杂，并出现数据在工厂内部与外部网络之间的双向流动共享。由此带来的安全风险主要包括数据泄露、非授权分析、用户个人信息泄露等。对于钢铁行业工业互联网的数据安全防护，应采取明示用途、数据加密、访问控制、业务隔离、接入认证、数据脱敏等多种防护措施，覆盖包括数据收集、传输、存储、处理等在内的全生命周期的各个环节。

3.5 钢铁行业 OT 层面安全建设方案

随着钢铁行业信息化的推进，MES、EMS 的建设越来越多，原本相互独立 DCS、PLC、仪器仪表、SCADA 等控制子系统需要通过网络和信息系统连接在一起，这些子系统，负责完成对原料供配、焦化、烧结、炼铁、炼钢、除尘、连铸等控制任务，一旦受到恶性攻击、病毒感染，就会导致工控系统的控制组件和整个生产线被迫停止运转，甚至造成人员伤亡等严重后果。

3.5.1 技术保障体系

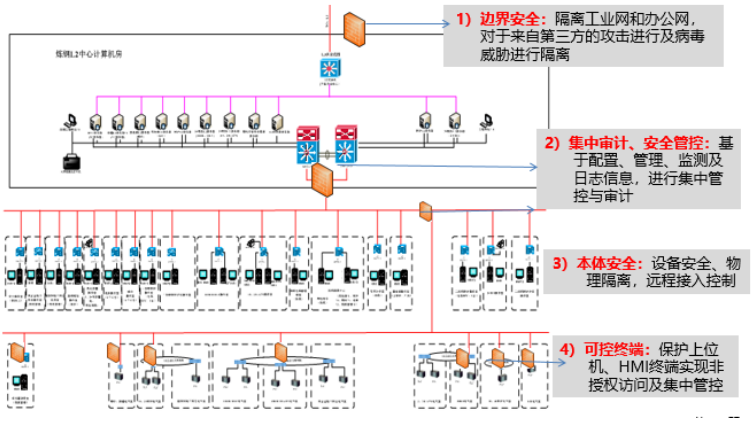

图 3 钢铁行业工业控制系统安全架构图

钢铁行业工业互联网安全主要采用分层隔离、纵深防御的模型设计，整体架构设计如上图所示。

钢铁行业工业控制系统分为五层结构，L5 是企业问的管理决策系统，L4 是面向整个企业内部管理和计划的 ERP 系统，L3 是面向生产和执行过程的 MES 系统，L2 是面向生产过程和控制的 PCS(过程控制)系统,L1 是生产设备控制系统。基于数据采集、设备控制的安全考虑，防护方案如下：

1）边界、区域及终端防护

在 L2 与 L1 之间、L1 内部部署工业控制防火墙及网络防毒墙进行边界和终端防护，通过工业协议的深度解析确保过程控制系统与现场控制设备之间、HMI 和现场控制设备之间通讯与控制的合法性；通过“黑”、“白”名单相结合的防护机制，有效阻止网络病毒、非法入侵、恶意控制等的威胁。

2）集中审计和安全管控

在 L2 层、L1 层部署工控监测审计终端，详细记录过程控制

系统和 HMI 对现场控制设备的操作过程，实现对关键参数配置实时监测与安全审计并进行及时的预警响应。

3）本体安全

基于工业控制系统相关设备对象，提供安全补丁升级及加固措施，对外部接入工业系统现场操作提供安全授权及访问控制措施。

4）可控终端

工业控制系统应用场景的特殊性，通用杀毒软件无法有效对各控制系统（DCS/SCADA/PLC/SIS 等）操作站及工程师站。可信终端可以有效识别和查杀异常威胁进程，解决了工控系统终端病毒感染、恶意代码进程启动、操作系统内核漏洞、USB 误用滥用等安全隐患，从根本上实现了对各种不安全因素的主动防御。

3.5.2 管理制度体系

依据工信部《工业控制系统安全防护指引》的要求，建立工控系统管理制度体系。

1）恶意代码管理机制

钢铁行业需要建立工业控制系统防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采用必要的安全预防措施。安全预防措施包括定期扫描病毒和恶意软件、定期更新病毒库、查杀临时接入设备（如临时接入 U 盘、移动终端等外设）等。

2）应急响应预案

钢铁行业需要自主或委托第三方工控安全服务单位制定工控安全事件应急响应预案。预案应包括应急计划的策略和规程、应急计划培训、应急计划测试与演练、应急处理流程、事件监控措施、应急事件报告流程、应急支持资源、应急响应计划等内容。

3）资产管理制度

钢铁行业应建设工业控制系统资产清单，明确资产责任人，以及资产使用及处置规则。完善工业控制系统资产清单，包括信息资产、软件资产、硬件资产等。明确资产责任人，建立资产使用及处置规则，定期对资产进行安全巡检，审计资产使用记录，并检查资产运行状态，及时发现风险。

4）工控安全管理机制

工业企业应建立健全工控安全管理机制，明确工控安全主体责任，成立由企业负责人牵头的，由信息化、生产管理、设备管理等相关部门组成的工业控制系统信息安全协调小组，负责工业控制系统全生命周期的安全防护体系建设和管理，制定工业控制系统安全管理制度，部署工控安全防护措施。

5）变更管理制度

为了工业控制系统安全稳定，设备或者程序升级变更必须确保任何变更都是可控的，有记录并定期接受审核的。

6）系统和软件升级制度

工控信息安全管理人员应定期关注工控系统相关设备或系统厂商安全问题公报以及国家漏洞库的公报，掌握补丁更新动态，

及早获取补丁更新程序。并进一步地针对补丁建立起部署前测试、更新时的应急、更新后的跟踪监控的安全机制。

7）定期安全培训

应定期对技术人员、管理人员、运行维护人员开展针对性的工控信息安全培训，提高工控信息安全技术技能，增强工控信息安全意识。