冶金工控系统主动防御技术体系白皮书

WHITE PAPER **2023**

SECURITY OF METALLURGICAL INDUSTRY CONTROL SYSTEM

2023.07

主编

程鹏、张镇勇

编写组成员

孟捷、汪京培、邓瑞龙、孙铭阳、王竟亦、赵成成、王东霞、车欣、张恒、方崇荣、王鑫、杨泽域、曾兰婷、彭莎、沈艺高、潘洁、施伟、郝怿、徐子东

顾问专家

尹怡欣、田有亮、孙彦广、刘杰、张海峰、张文安、陈铁明、郑驰、姜思鸿、焦四海、魏强、刘军、杨晓勇、谢永芳、陈阿莲

主编单位

浙江大学、贵州大学

指导单位

中国自动化学会、中国科学技术协会、钢铁研究总院、北京科技大学、浙江国利网安科技有限公司、柳钢东信科技有限公司、宝钢中央研究院、大唐高鸿数据网络技术股份有限公司、浙江工业大学、工信部电子五所、杭州安恒信息技术股份有限公司、360政企安全、中国人民解放军战略支援部队信息工程大学、中国自动化学会工控系统信息安全专业委员会、金川集团、贵州磷化(集团)有限责任公司、山东大学、中南大学

支持项目

科技部重点研发课题《工控系统安全主动防御机制及体系研究》，项目编号：2018YFB0803501；中国科协决策咨询项目《工业控制系统安全国家战略研究》，项目编号：20220615ZZ08010017

前言

PREFACE

随着工业化与信息化的深度融合，数字化、网络化、智能化成为冶金工业转型升级的典型特征，原本独立、封闭的冶金工控系统逐渐与互联网广泛互连，在加强生产管控、提升运作效率、促进节能减排等方面发挥了积极作用。然而，随着越来越多的工业设备接入互联网，木马、蠕虫、后门漏洞等各类网络安全威胁也随之涌入冶金生产流程，为冶金场景工控安全带来了新的挑战。

目前，冶金工控系统普遍存在生产设备老旧、边界防护不足、安全管理薄弱、控制器存在安全漏洞等问题，易受外部入侵者或内部不法人员攻击，导致敏感数据丢失、关键设备损坏，甚至引发重大安全事故。

近年来，工控领域频繁爆发的恶意攻击事件，说明冶金行业面临的网络安全威胁并非空穴来风[1]。2010年，震网病毒感染伊朗核设施控制系统，使得离心机大面积损毁，导致伊朗核计划被迫延迟[2]；2015年，乌克兰电力公司遭到“黑暗能量”病毒的攻击，导致乌克兰东部地区大面积停电；2017年[3]，中东一处石油和天然气石化设施因受

前言

PREFACE

到TRITON病毒攻击而被迫关闭[4]；2022年，伊朗Khouzestan钢铁厂遭受高级持续性威胁(ATP）攻击[5]，攻击者使用恶意软件、弱密码攻击和社会工程等手段，逐步获得钢厂生产网络的控制权进而对钢厂发动攻击，导致一台重型机械回转台出现故障引发了大火，最终钢厂被迫停产，遭受重大损失。

为保障工控系统的安全稳定运行，各国相继出台相关政策以应对潜在的攻击威胁。美国连续发布《端点安全最佳实践》[6]、《安全成熟度模型：描述和预期效果》[7]等白皮书，构建工业互联网安全框架；德国发布《工业4.0实施战略》，明确了工业4.0的关键技术演进方向、标准化路径及相关安全问题[8]；为切实维护工控系统网络安全，我国相关部门发布了《工控系统信息安全防护指南》[9]、《中国工业互联网安全态势报告(2018年）》[10]、《工业信息安全标准化白皮书(2019版）》[11]等相关文件。

在这种背景下，国内冶金行业企业迅速开展了工控安全防护工作，相关行业协会、工控厂商、

前言

PREFACE

信息安全企业也提供了技术支持。当前，冶金工控系统主要采用以边界防护为主的被动防御方案，将防火墙、网闸、网关、病毒防护软件、入侵检测设备部署在工控网络中。然而，由于攻防信息不对称性、不可避免的认知逻辑缺陷、防护方案与工控可用性需求的冲突等问题，被动防护难以为冶金场景提供全面有效的保护。主动防御技术具备动态可靠、适用性强、多维防御的特点，被认为是解决工控安全问题的潜在方案。主动防御技术包括拟态防御、可信防护、内生安全策略等，协调“识别、加固、检测、响应”等各种技术，实现全生命周期一体化的协同防御。

本白皮书针对冶金行业典型场景下工控系统的设备、协议、业务层面的脆弱性进行分析，并评估现有安全防护措施的有效性，明确在冶金行业背景下工控系统的安全防护需求，基于识别(Identification）-保护(Protection）-检测(Detection）-响应(Response)等方面的理论技术，提出一套冶金工控系统的主动防御技术参考体系，提升冶金工控系统应对各类安全威胁的防御能力。

前言

PREFACE

本白皮书的意义在于构建冶金行业典型场景工控系统的主动防御技术体系，为工控系统的主动防护技术的应用提供模板。同时，基于主动防御技术体系，为自主可控的产品开发和集成、行业的示范应用提供参考。

目录

01

冶金工控网络及其安全风险

1.1 冶金行业背景

近年来，我国冶金行业呈现出快速发展的趋势。我国拥有数量庞大的钢产量和常用有色金属产量，冶金产业发展水平居世界首位，未来我国冶金产品的实际需求将持续增长[12]。冶金消费品种也将发生变化，汽车、造船、建筑等领域为冶金行业的发展增添了动力[13]，如图1所示，机械行业、轻工业和汽车行业等需求占比将持续上升。

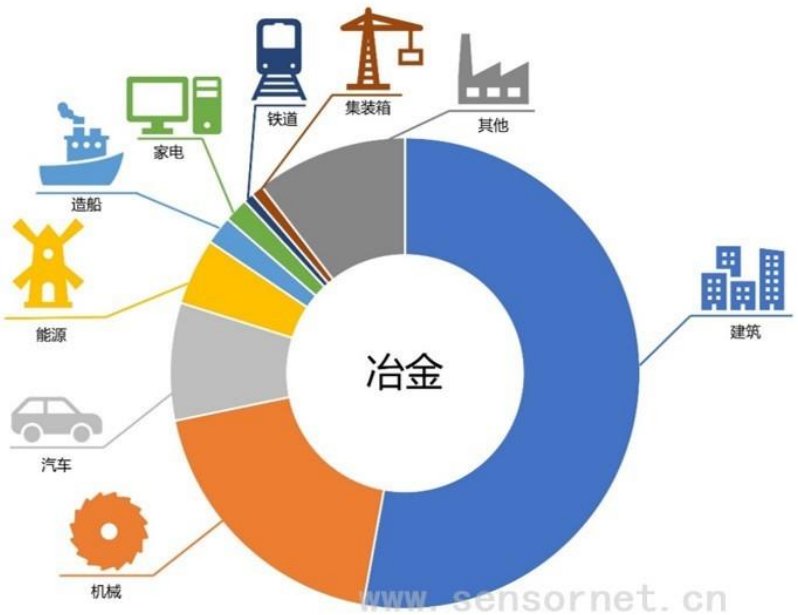

图 1 冶金行业与其他产业之间的关系

冶金行业作为典型的流程控制行业，其生产过程具有多工序连续生产、区域间强耦合、各影响因素非线性等特点，其生产数据表现出高吞吐、强交织、时变多态、异构多源的特征[14]，如何保证工艺流程安全高效生产是冶金行业面临的重大难题。工业信息技术的发展和应用为解决该难题提供了契机。利用工业互联网平台实现控制技术变革，设计符合冶金行业特点的控制网络构架，实现智能交互、最优控制和智能决策，最终解决异构设备接入、多源数据集成、数据建模分析、知识积累迭代等一系列问题，为解决冶金企业自动化和智能化提供新思路和新方法[15]。

我国冶金行业在经历了部门级信息化(MIS)和企业级信息化(ERP)之后，已经基本完成基础信息化。多数冶金企业构建了由一级PLC(可编程逻辑控制器)、二级PCS(过程控制系统)、三级MES(制造执行系统)、四级ERP(企业资源规划)、五级EIP(企业信息门户)为主线的五级信息系统架构[16]，如图2所示，82%的企业建设了车间级制造执行管理系统，87%企业全部或部分实现了磅秤计量数据自动采集[17]。冶金行业实现了基础数据的标准化、基本业务的流程优化、生产-业务系统的集成化。

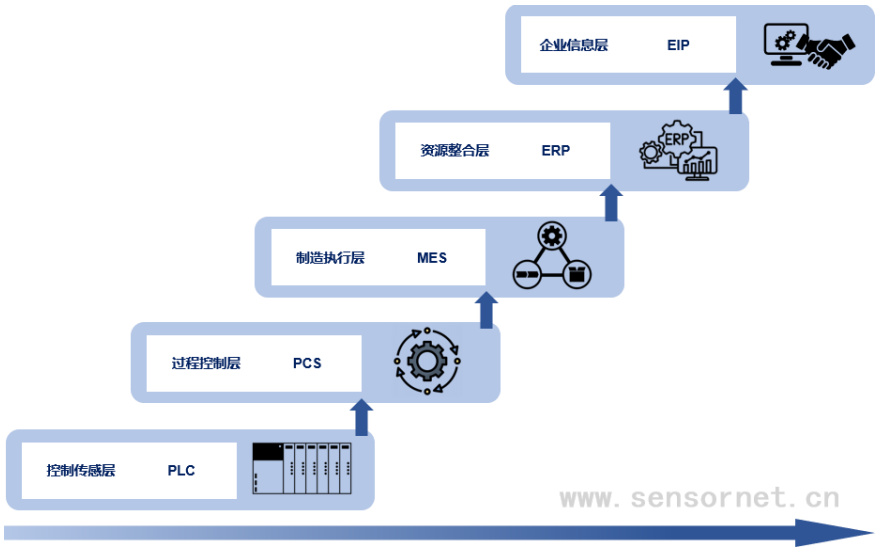

图 2 冶金行业的信息化

近年来，随着工业化与信息化的深度融合，数字化、网络化、智能化成为工业转型升级的典型特征，扩展到包括冶金在内的主流工控行业，例如冶金行业的一大子类钢铁企业。原本独立、封闭的工控系统与互联网广泛互联，对于提高钢铁企业的生产管控、运作效率、节能减排发挥了积极作用。2018 年钢铁行业两化融合指数达到 51.2，关键工序数控化率达到 68.7%，应用电子商务的企业比例超过 50%[18]。与此同时，工业互联网产业联盟联合中国钢铁工业协会、中国金属学会于2021年11月联合发布《工业互联网与钢铁行业融合应用参考指南》[19]，为钢铁企业工业互联网建设规划和融合应用进一步提供实施方法与路径参考，并指出随着5G技术的发展，冶金场景中数据采集、信息传输、生产控制等方面的需求有望通过“5G+工业互联网”的应用得到有效解决。

1.2 冶金工控网络

以钢铁冶金工艺为例，其流程复杂、任务繁多，包括冶炼、精炼、连铸、轧制等过程[20]，首先进行冶炼工艺，将原材料加热，分离出所需的金属或合金，再对金属进行精炼，以去除杂质并提高纯度，然后通过连铸将液态金属直接铸造成坯料，最后对金属坯料进行一系列塑性变形和加工的轧制工艺，以获得所需形态的金属产品。在这个生产过程中需要监测流场、温度场、应力场等多项现场数据。金属组织性能的控制，制造过程中的成分与板型控制、工艺技术优化等部分，也需要部署大量测控设备进行控制与监测[21]。为了方便对监测仪表、控制设备等部件进行自动化管理，冶金场景通常会构建符合现场要求的工控系统。由于各生产环节的需求不同，对应的控制系统特点也不一样，下面以高炉本体控制系统和冷轧控制系统为例进行

介绍。

炼钢过程的高炉是自动化程度和生产过程自动化要求最高的场景和关键的环节，生产全过程均采用自动化技术进行严格的控制和管理，具有大型化、连续化、自动化、高速化等特点[22]。高炉本体的数据监测和过程控制主要包括：炉内状态测量、高炉运行控制、高炉本体及人员保护等。高炉本体控制系统能够实现高炉本体的工艺数据采集和工序过程控制，由检测仪表、控制器(PLC)和上位机构成。其控制过程首先由检测仪表采集到温度、压力、流量等现场数据后，经由控制器将数据传输到上位机，上位机将当前的实时数据和历史趋势走向显示在控制画面中，供操作人员查看、分析当前高炉运行状况。高炉本体通过PLC编程实现风温、风压等物理量的PID自动调节与控制，工程师对PID参数进行设置，控制混风阀装置调节，并在上位机画面上显示相关数据[23]。

冷轧控制系统与高炉控制系统有较大差别,以国内某钢场冷轧带钢生产线为例，轧机和收卷机驱动电机采用直流电机，采用全数字直流调速装置，并配置一台PLC及其附属从站进行控制。辅助设备由稀油站、润滑站、液压站组成，各控制器、传动装置之间通过Profibus-DP网络等方式通信，实现集中控制。在操作台及主控室设置人机界面，以“Client-Server(C/S)”结构与PLC进行通信[24]。

为便于与制造执行系统、企业管理系统互联互通，提高监控能力，冶金工控系统通常采用管理层、监控层、控制层、现场层四层控制网络结构，自上而下统一管理。冶金工控系统的网络结构如图3所示。

- 现场层

现场层主要由传感器和执行器构成，对物理对象的运行状态进行实时监测和在线操作。

- 控制层

该层主要负责收集现场层数据，并控制执行器进行材料的加工处理，一般位于冶金生产车间的现场，通过工业交换机与上层进行信息交互。其主要由PLC、上位机、人机交互界面(HMI)、数据采集卡件等设备构成。可以在本地实现连续控制调节、设备检测、系统测试与自诊断、过程数据采集、信号转换与协议转换等功能。

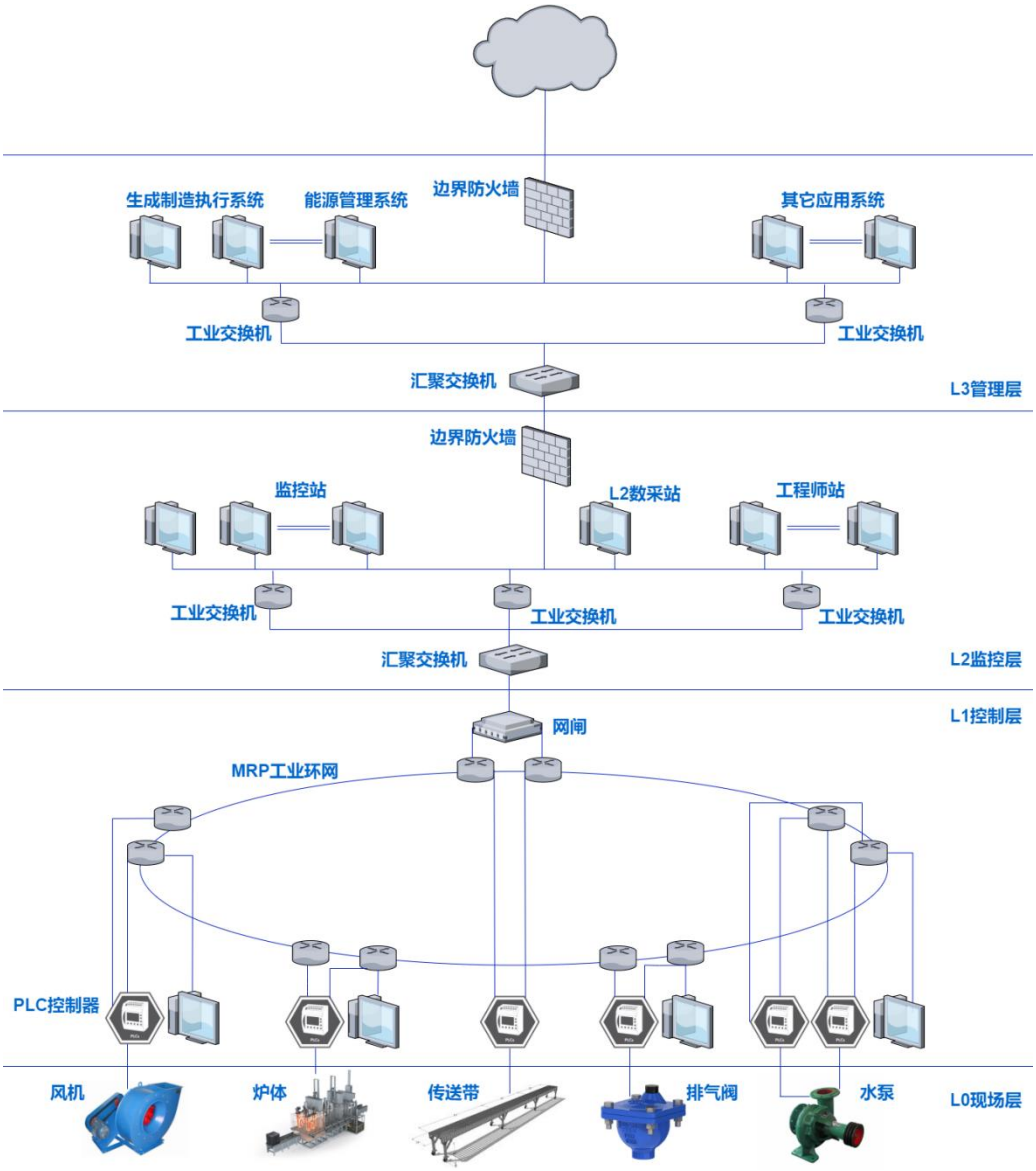

图 3 冶金工控网络

- 监控层

该层包含各个分装置的工程师站及操作员站，可以实现对生产过程的监控和系统组态的维护，并通过交换机汇聚各分区控制系统。通过设置全局工程师站对分区内所有装置的组态进行维护，查看网络内各装置的监控画面、趋势和报警。从数据流向的角度来看，现场层数据由传感器采集后传输至控制层，控制器以工控报文或

其他数据格式将现场数据向上传输，经过防火墙过滤送达至监控层的操作员站，操作员站对数据进行简单分析处理，将结果发送给管理层数据库。事实上，由控制层和生产监控层就能进行正常生产，但在冶金行业中，为实现生产管理信息化和智能化，通常要设置管理层及以上的网络。

- 调度管理层

调度管理层是将生产过程控制层的数据进行自动采集并建立大型实时数据库和关系数据库，并针对冶金行业实际需求和特点，利用数据处理和分析对生产过程进行管理和优化。

上述架构通过局域网实现数据的层级交互，基本满足了冶金生产过程中的控制要求。但是，由于冶金行业的连续生产需求，产线寿命往往超过十年，考虑到对生产流程的影响，大部分现场设备不会进行更新换代或版本升级，无法针对漏洞进行补丁，同时各层级、各设备间缺乏有效的安全隔离，给攻击者带来了可乘之机。

1.3 安全风险分析

近年来，工控领域频繁爆发的网络攻击事件，说明网络安全威胁并非空穴来风[25]。2010年震网病毒感染伊朗核设施控制系统，使得离心机大面积损毁，导致伊朗核计划延迟[2]；2014年底，德国一家钢铁厂遭受到高级持续性威胁(APT)攻击[26]。攻击者使用鱼叉式钓鱼邮件和社会工程手段，获得钢厂办公网络的访问权。之后攻击者利用该网络，渗透到钢铁厂的生产网络并发动攻击。攻击者的行为导致该钢铁厂工控系统的控制组件和整个生产线被迫停止运转，由于不是正常的关闭炼钢炉，从而给钢厂带来了严重破坏。2020年3月，钢铁制造商EVRAZ公司在北美分支机构，

包括加拿大和美国的钢铁生产厂均遭受了勒索软件Ryuk攻击，导致其在北美的分支机构瘫痪，大多数工厂停止生产[25]。2022年，伊朗Khouzestan钢铁厂遭受到高级持续性威胁(ATP)攻击[5]。攻击者使用恶意软件、弱密码攻击和社会工程等手段，逐步获得钢厂办公生产网络的控制访问权进而对钢厂发动攻击，导致一台重型机械回转台出现故障引发了大火，最终钢厂被迫停产，遭受重大损失。这一系列针对工控系统的攻击事件说明工控系统网络安全问题非常严重。

工控设备、协议和业务的安全漏洞使得冶金控制系统面临内外部威胁，工控系统网络安全风险呈现出攻击来源复杂化、攻击目的多样化以及攻击过程持续化的特征[27]。随着工业互联网的兴起，越来越多的工业设备接入网络，工业孤岛不再封闭，攻击者可以通过网络途径侵入冶金生产现场，利用先进的攻击手段，针对控制器、工控协议、业务流程发起攻击，进而影响正常生产过程甚至造成安全事故。经过分析，冶金行业可能面临的安全风险如下。

- 设备自身存在安全漏洞，系统安全风险大

当前主流的冶金工控系统普遍存在安全漏洞，部分严重威胁类漏洞能够远程执行，甚至在冶金场景中潜伏、传播。常见漏洞可分为不当输入认证、访问控制漏洞、凭证管理、配套软件漏洞等。

冶金工控系统存在各类输入形式，部分控制设备对输入内容及形式缺乏有效验证，攻击者可构造特殊的攻击载荷以触发漏洞，修改设备数据甚至获得设备控制权限。在访问控制方面，部分设备的访问控制策略不完善，甚至在设计时缺少访问控制功能，并且不对访问行为做任何身份认证，部分设备访问凭证结构过于简单，可

被直接爆破，凭证保护程度不足则可能导致凭证泄露等问题，攻击者可利用此类漏洞获取敏感信息或执行危险操作。

与工控设备配套的上位机软件用于设备组态及配置，其安全漏洞将直接威胁控制器安全。部分上位机软件未设置读取保护，攻击者可通过逆向技术分析上位机配置原理及通信流程，寻找潜在脆弱性；部分工控设备的认证过程在上位机处进行，攻击者可篡改上位机软件代码跳过凭证验证部分，突破认证防护。

- 网络安全边界模糊且防护措施薄弱，存在很大安全隐患

工控网络内部缺少纵向安全防护措施，各层级之间防御能力不足。控制器及HMI主机设备直接接入控制环网，缺乏隔离保护；典型冶金装置中控制层和监控层网络安全边界模糊，存在被病毒攻击及非法接入等风险[28]；同一装置内的PLC之间具有强关联性，高度依赖控制网络，其中一台设备被病毒感染，可能对整个控制网络的正常运行造成严重威胁。

同时，工控网络缺乏访问控制功能，没有在相应网络边界部署访问控制设备，不能对进出网络的信息内容进行审查和过滤，缺乏检查、定位和阻断非授权设备访问内部网络的能力；不同网段之间缺乏可靠的技术隔离手段，各网段间的信息交互缺少有效的安全保护措施，难以阻止恶意攻击传播；缺少监控网络异常流量的技术手段，无法实现安全审计。

- 工控系统缺少自动化周期数据备份和容灾方案

工控系统的容灾备份主要包括组态数据、工艺代码的备份，工控系统工程师站、操作员站的系统备份等。若发生系统崩溃、勒索病毒感染等紧急情况，导致业务中

断、数据丢失、重要文件无法恢复等状况时，难以迅速、有效地恢复系统至故障发生前的稳定状态。所以要加强工控系统备份和恢复能力，在发生安全事故时，具有快速恢复生产运行的能力。

- 工控系统协议存在脆弱性

常用的工控协议在设计之初只考虑了可用性，忽略了保密性、完整性需求。当前，常用公有协议如Modbus、私有协议如S7Comm等均存在明文传输的问题，包括寄存器地址、数值、变量类型等敏感数据在传输过程中未经加密处理，一旦攻击者进入网络监听，可以直接读取这些信息。工控协议需具备完整性，保证数据包中的内容在传输过程中不会被恶意篡改。但部分工控协议如S7Comm、OMRON FINS缺少完整性验证机制，攻击者截获通信流量后，修改敏感参数或执行代码，再重新发送给目标设备，影响设备正常工作。

- 缺乏外部入侵、违规操作的检测响应能力

随着工业互联网在冶金行业的应用，攻击者可以利用网络对冶金场景中的关键设备发起远程入侵，同时，内部不法分子也可能利用身份便利执行违规操作，对正常生产造成影响。当前冶金场景普遍缺少针对内外部威胁的检测、响应能力，管理者也缺乏相应的安全意识。

- 安全网络统一管理缺失

在冶金行业中，各类控制站、工作站和服务器规模数量庞大，一个典型钢铁厂中的控制站、工作站和服务器规模可达3000-4000台，管理任务重大且艰巨。目前大部分冶金企业在企业网络资产管理、安全策略管理、账户管理、配置管理、日志管

理、日常操作等方面缺乏统一的技术手段和管理方法，也无法对日志、监测和报警数据等进行分析和统计。

缺少安全策略、管理制度，管理者、操作人员安全意识淡薄，部分企业注重产能效益，对可能造成重大事故损失的安全威胁重视不足。管理者认为工业场景与网络环境的天然隔离保护依然存在，对潜在安全问题视而不见。操作人员安全意识不足，仍保留可能带来安全风险的行为习惯。企业缺乏针对工控系统安全的管理政策和监管制度，为病毒传播、外部入侵等风险保留了理想的土壤。

综上所述，冶金工控系统设备数量种类众多、系统结构复杂、业务流程长、管理难度大，其自身存在设备、协议、隔离、管理等各个层面的安全漏洞。在工业互联网普及的趋势下，工控系统的孤岛保护不复存在，面对各类针对工控设备的安全威胁，冶金工控系统需要部署全面完善的防御体系，才能应对各类安全挑战，为冶金生产的正常运作保驾护航。

02

冶金工控安全防护需求及挑战

2.1 安全防护现状

2.1.1 已有防护措施

为弥补安全漏洞，降低安全隐患影响，根据工业企业的安全实践和相关政策标准，在冶金场景中常通过以下防护措施对工控系统进行保护。

- 控制设备冗余防护

在重要的冶金控制场景(如高炉炼铁、轧钢等)中，对关键控制设备进行冗余配置，可以在主要组件发生故障时接管工作，避免因主控制器宕机影响生产过程。

- 生产节点网段隔离

冶金流程任务复杂，需要控制的设备众多。根据生产功能不同，可将具有相同生产任务的设备、传感器、控制器划为一个节点集合，不同节点处在不同的网段，通过采用物理隔离措施，防止传播性较强的病毒跨网段传播。

- 防火墙

如图4所示，在冶金控制网-管理网以及管理网-外网之间采用边界隔离防火墙，禁止系统集成商、设备供应商、第三方运维服务商等其他外部企业通过互联网远程扫描工控资产、连接控制网内的系统或设备。

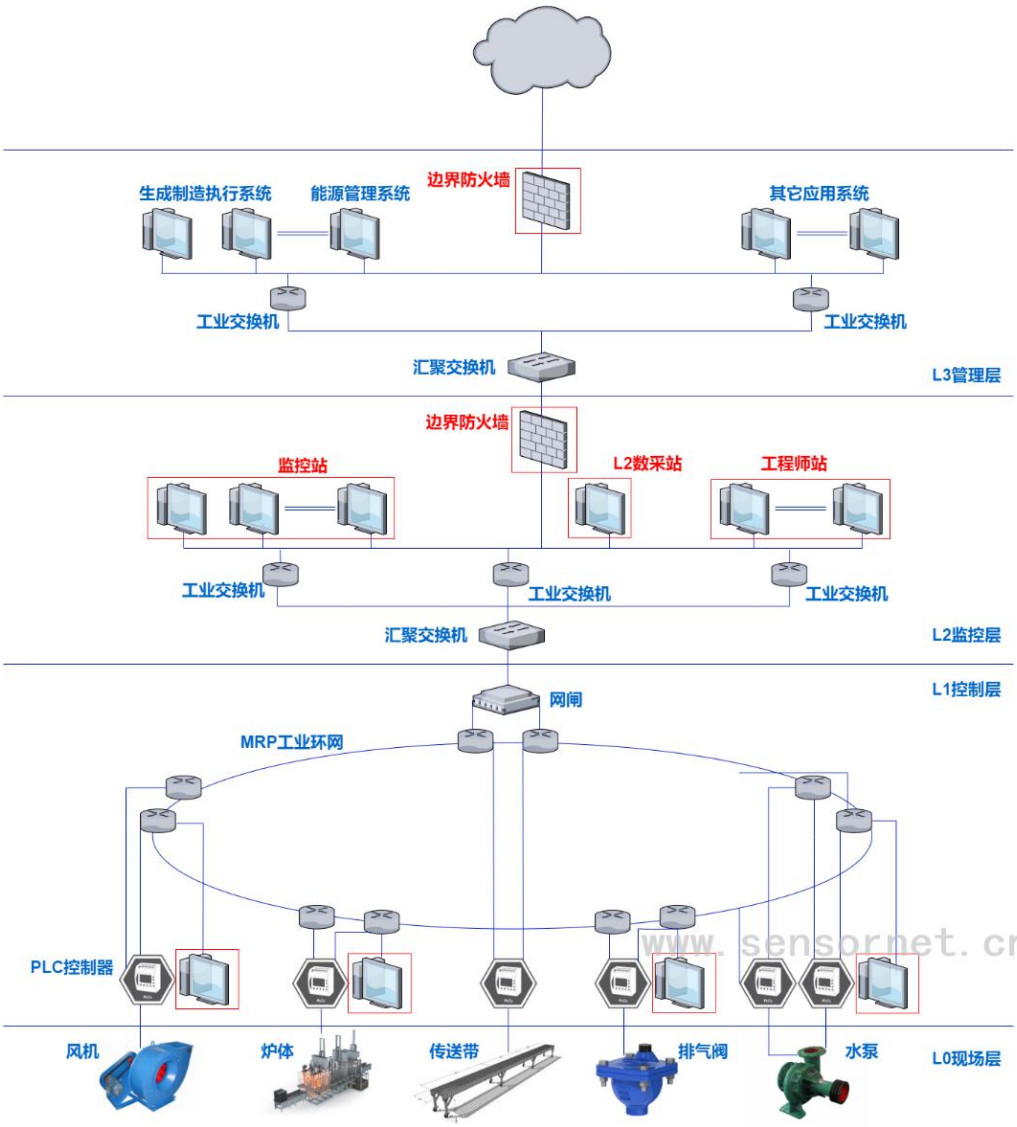

图 4 现有安全防护手段

- 网闸隔离

在冶金工控系统的管理层、控制层之间设置具有特定导向规律的网闸，过滤不符合规定的流量，阻断网络的直接连接，只完成特定的工业应用数据交换。

- 操作系统防护

在管理层/监控层办公电脑上安装安全卫士、杀毒工具等防御软件，实时监测操

作系统安全状态，查找并杀灭常见操作系统病毒。

- 人员培训

冶金企业对现场工作人员进行安全培训。除了常规的生产操作之外，工作人员还需遵守相关的安全规定，如不使用非工作U盘传输文件、不设置弱口令、定期检测作业日志等。

- 定期安全测试

冶金企业会定期进行安全测试，或邀请第三方机构开展等保测试，对易受攻击的工作站、控制器、服务器等设备进行漏洞排查

2.1.2 现有防护不足

现有防护措施在一定程度上能够减轻冶金工控系统安全漏洞带来的影响，但其安全防护覆盖面有限，具体体现在以下方面：

- 未解决设备自身安全性问题

通过冗余的方式能够缓解设备异常造成的影响，但无法解决设备自身存在的安全问题。如果攻击者利用冗余机制设计隐蔽性强的攻击手段，现有的防护机制将无法检测并抵御此类攻击[29]。同时现有冶金场景中的控制器绝大多数是外国厂商生产，其系统结构及通信协议已被深入研究，有大量公开的设备脆弱性资料可供攻击者参考；与控制器配套的组态软件也存在大量的安全漏洞，易成为攻击者的潜在攻击对象；监控层、管理层的上位机多使用Windows操作系统，其自身漏洞也可能被攻击者利用，仅通过安全卫士和杀毒软件难以满足冶金场景下的安全防护需求。

- 边界防护不够彻底

没有在控制层－监控层之间采取有效的防御措施，安全边界仍然模糊；各类工控设备及HMI主机设备均就近接入控制环网，没有网关保护；控制网络中部署的多数是无法识别解析工控协议的通用网关、防火墙[30]，无法识别特有的工控流量，也无法分辨出针对工控设备的特有攻击行为。

- 缺少漏洞扫描设备

冶金行业工控网络规模较大、节点众多，工控资产的安全管理困难，现有的防护体系中缺少对设备的脆弱性检测，无法及时识别设备中存在的安全漏洞，缺乏必要的补丁、升级。

- 缺少入侵检测及安全审计系统

现有防御方案缺少入侵检测机制，无法及时发现针对工控系统的入侵行为，只能等待设备出现故障造成损失后对攻击做出反应。同时，冶金行业的控制对象数量种类众多、流量数据大，需要安全审计网络中的协议流量，对用户行为进行精细化识别和审查，及时发现异常并告警。

- 缺少自动化周期数据备份和容灾方案

一旦攻击者突破防御、攻击成功，将对冶金生产造成严重影响。现有防护措施缺少自动化周期数据备份，也没有攻击后的快速恢复方案。遭受攻击后，恢复难度很大。

- 缺乏综合安全管理

现有防护策略在企业网络资产管理、安全策略管理、账户管理、配置管理、日志管理、日常操作等方面缺乏统一的技术手段和管理方法，也无法对日志、监测和报警数据等历史数据进行综合分析统计，各项防御措施分散独立，难以形成一体化的安全防御技术体系。

2.2 安全防护需求

针对当前冶金行业存在的脆弱性问题及现有防护措施的不足[31]，需要一套成熟的一体化工控安全主动防御技术体系来解决冶金场景下工控设备面临的安全问题。该主动防御体系应满足如下防护要求：

识别能力。具备风险识别能力，能够依靠主动/被动探测方式对全场景设备进行管理、安全分析，能融合攻击模式、威胁影响度量、脆弱性关联分析等关键理论和技术，识别设备本体的安全漏洞并构建漏洞数据库；针对主流的工控协议进行深度分析，包括数据包检查、流量审计、协议逆向等，提取攻击行为特征并构建攻击指纹数据库，支持与CVE[32]、CNVD[33]与CNNVD[34]漏洞库的关联，识别典型的操作业务流程的攻击方式，并建立相应的脆弱性知识库。

加固能力。针对风险识别结果对设备本体及相应编译器、组态软件进行安全加固，如，部署基于可信计算的工控本体操作系统，实现工控安全协议加固技术；部署能够深度解析工控协议的工业安全防火墙、安全网关等网络接入设备，提升协议安全性；协同部署安全卫士、访问控制模块、防火墙等设备，实现本体、组态软件、边界和网络的安全；并能够针对工控场景特有的安全威胁设置安全策略，同时能够应对未知威胁。

检测能力。基于当前流量、业务运行情况、故障日志、传感控制数据等实时监测生产流程状况，基于攻击行为指纹库侦测并识别可疑行为，实现威胁位置及传播路径的跟踪溯源；利用入侵检测系统和安全审计系统，对冶金系统通信内容进行识别审查，实时监控工控通信过程，甄别针对工控系统的入侵行为，发现异常及时告警。

响应能力。具备应急响应能力及后置恢复能力，面对不同程度的攻击威胁实施相应的响应策略，支持自动化周期数据备份，制定攻击后的快速恢复方案，最小化损失并对攻击行为进行反制。

2.3 安全防护规范

2.3.1 等保2.0防护需求

参照等保2.0相关规定[35]，冶金行业的主动防御技术体系应满足以下要求：

- 网络架构

工控系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段；工控系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；涉及实时控制和数据传输的工控系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离。

- 通信传输

在工控系统内使用广域网进行控制指令或生产数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据保密传输；应采用校验技术或密码技术保证通

信过程中数据完整性。

- 边界防护

应保证跨越边界的访问数据流通过边界设备提供的受控接口进行通信；应能够对非授权设备私自连接到内部网络的行为进行检查或限制；应能够对内部用户非授权连接到外部网络的行为进行检查或限制。

- 访问控制

应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；应对进出网络的数据流实现基于应用协议和应用内容的访问控制；应在工控系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；应在工控系统内安全域和外安全域之间的边界防护机制失效时，及时进行报警。

- 入侵防范

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间。

- 安全审计

应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的

用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

2.3.2 防护政策与标准

- 政策要求

《中华人民共和国网络安全法》

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》 (国发〔2012〕23)

《关于加强工控系统信息安全管理的通知》(工信部〔2011〕451 号)

《国务院关于深化制造业与互联网融合发展的指导意见》(国发〔2016〕28号)

《信息化和工业化融合发展规划(2016-2020 年)》

《工控系统信息安全防护指南》

- 标准及规范

GB/T30976.1-2014《工控系统信息安全第1 部分：评估规范》

GB/T30976.2-2014《工控系统信息安全第2 部分：验收规范》

GB/T32919-2016《信息安全技术工控系统安全应用指南》

GB/T33007-2016《工业通信网络网络和系统安全建立工业自动化和控制系统安全程序》

GB/T33008.1-2016《工业自动化和控制系统网络安全可编程序控制器(PLC)》

GB/T33009.1-2016 《工业自动化和控制系统网络安全集散控制系统(DCS)第1部分：防护要求》

GB/T33009.2-2016 《工业自动化和控制系统网络安全集散控制系统(DCS)第2部分：管理要求》

GB/T33009.3-2016 《工业自动化和控制系统网络安全集散控制系统(DCS)第3部分：评估指南》

GB/T33009.4-2016 《工业自动化和控制系统网络安全集散控制系统(DCS)第4部分：风险与脆弱性检测要求》

GA/T695-2007《信息安全技术-网络通讯安全审计-数据留存功能要求》及《安全审计工控协议加测内容》

网络安全等级保护定级指南(GB/T 22240-2020)

网络安全等级保护实施指南(GB/T 25058-2019)

网络安全等级保护测评指南(GB/T 28449-2018)

网络安全等级保护基本要求(GB/T 22239-2019)

网络安全等级保护设计技术要求(GB/T 25070-2019)

2.3.3 安全防护原则

对于冶金行业工控系统信息安全建设，应当以适度风险为核心，以重点保护为原则，从业务的角度出发，重点保护重要的业务系统，在方案设计中应当遵循以下的原则：

- 适度保护原则

冶金工控系统设备种类众多，系统结构复杂，流程工艺连续多样，安全漏洞存在于方方面面。同时，随着信息技术的发展和攻击者能力的增强，各类新的漏洞也层出不穷，任何一套防御策略都无法完全覆盖冶金场景的全部安全脆弱点。选择和部署防御策略时需要在防御效果与部署成本之间平衡折中，在保证生产效益的同时寻求高效的防护方法。另外，冶金工控系统的可用性、功能安全性、生产安全性仍然是该行业首要考虑的因素，因此，在考虑网络安全问题时，不能破坏上述三个基本要素，适度防护是可行之策。

- 技术管理并重原则

目前大部分冶金行业中的工作者更追求企业的生产效益，容易忽视生产过程中的安全防范问题，企业内部也缺少相关的安全政策与管理制度。单纯依靠安全技术来改善冶金行业的安全现状是片面的，不改变管理观念与管理制度，仅通过部署安全产品很难完全覆盖冶金行业工控系统所有的信息安全问题。另一方面，目前冶金场景中运用到的安全技术不足，难以形成有效的保护。在部署防御策略时，需要将安全技术与管理制度结合推进，切实有效地保障冶金场景安全性。更重要的是，安全策略更需要有效监管，专业有效的管理才能充分发挥安全技术在增强冶金工控系统安全方面的作用。

- 分层分区原则

冶金工控系统一般分为五层，每层的功能和特点不同，需要针对每层的特点和需求有针对性地部署安全策略。同时，在每一层内根据功能和需求划分安全区域，

不同区域间设置交互策略和安全保护措施，方便集中管理的同时，也可以遏制嵌入网络的病毒、蠕虫等在整个系统内传播。

- 动态调整原则

防御策略需要根据保护对象和内外部威胁的变化进行动态调整。随着工业互联网的引入，冶金场景将产生较大变化，且该变化还会根据技术的革新不断演变，同时冶金场景所面临的内外部威胁也在不断改变，冶金企业的组织架构、管理策略等因素也会实时影响冶金工控系统的防御需求。因此，要求防御策略需要具备动态调整的能力。

2.4 安全防护挑战

为实现对冶金工控系统的主动安全防护，需解决控制设备、通信协议、关键业务等方面存在的安全问题。由于冶金工控系统广泛分布攻击面，面向信息安全和功能安全构建主动防御技术体系存在极大挑战。冶金工控系统的安全漏洞如图5。

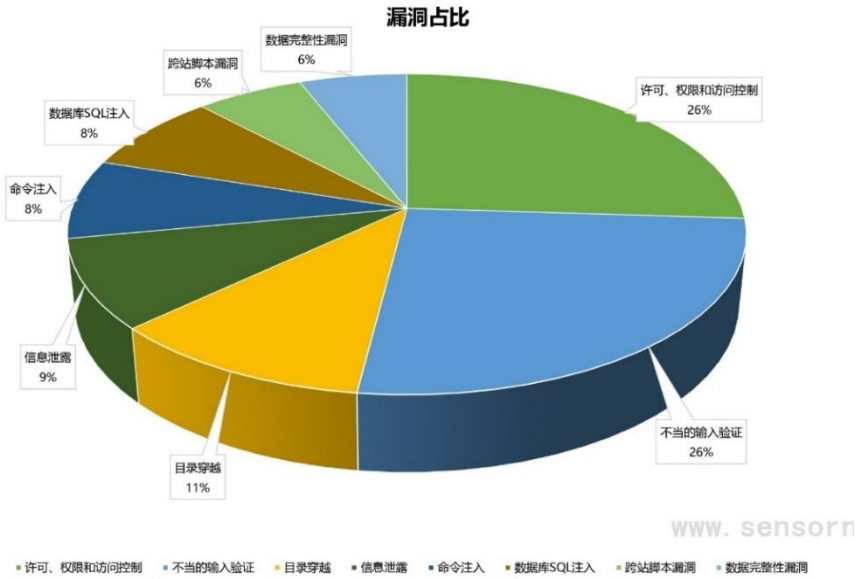

图 5 冶金工控系统不同漏洞类型的占比

2.4.1 控制设备的安全问题

冶金工控系统常用的控制器是可编程逻辑控制器PLC[36]，主要包括西门子S7系列、施耐德[37][38]、欧姆龙[39]等。这些PLC的安全性逐渐成为工控系统软肋，根据公开的漏洞数据库CVE显示，冶金场景中常用的PLC型号施耐德M340漏洞数达85个，西门子S7-300达19个，罗克韦尔Micrologix 1400达47个。另一方面，由于业务生产需求，PLC难以经常停机维护或更新，这导致大部分设备难以对漏洞进行及时补丁，严重威胁控制器安全。据统计，主流控制器存在的漏洞数量如图6所示。

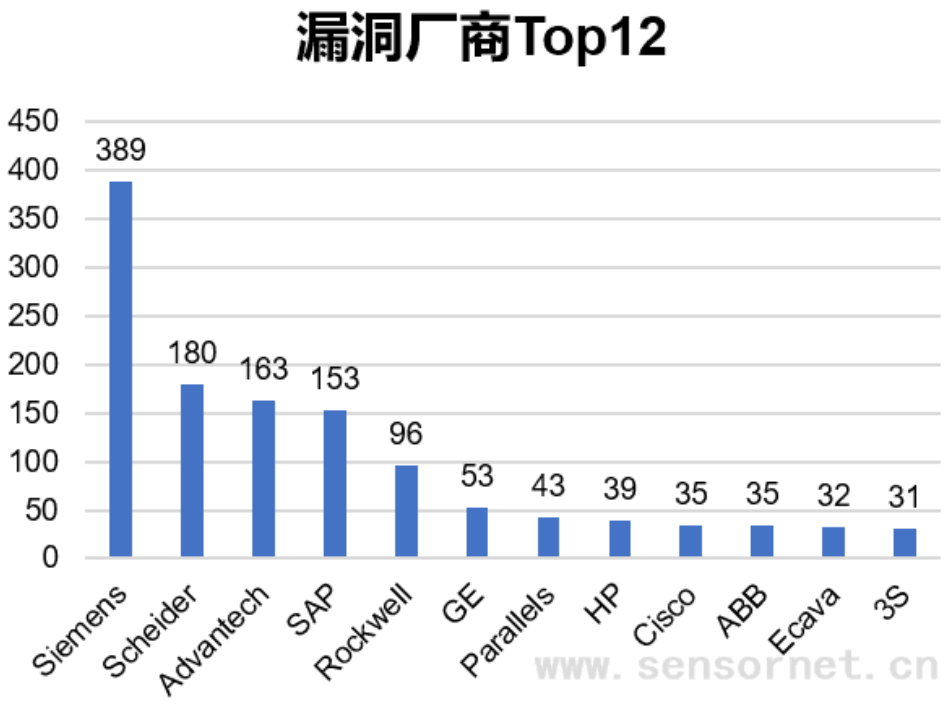

图 6 主流控制器存在的漏洞数量

- 西门子S7系列PLC

由德国西门子公司生产，在冶金的各个环节中广泛应用。S7系列可编程逻辑控制器分为微型 (如S7-200)、小型(如S7-300)和中、高性能要求的PLC(如S7-400)[40]。

S7-200适合256点以下的控制对象，能够完成多种场合下的自动检测、监测及控制功能；S7-300能满足中等性能要求的应用，采用模块化结构，具备高速(0.6~0.1μs)指令处理能力，可进行浮点数运算。在冶金场景中较为常见的是S7-200和S7-300。

- 施耐德PLC

施耐德电器公司有多款适用于过程控制场景的控制器，如Modicon M580、M340、Premium等，适用于各类生产场景。Modicon自动化控制平台拥有全系列完整的处理器，适用于复杂的控制过程。支持5种IEC编程语言(FBD、LD、SFC、ST、IL)，适用于高性能多任务系统，具有11M集成存储空间，集成优异的通讯功能和诊断功能，前面板有多个内置端口(USB、Ethernet TCP/IP、Modbus Plus、以及至少一个 Modbus端口)。具有涂层保护模块，适用于高温等恶劣环境，无需停机即可安装新模块，能较好地契合冶金场景的控制需求。

- 欧姆龙PLC

欧姆龙PLC根据IO点数与功能不同，可分为微型、小型、中型、大型、运动控制五种类型，其中中型PLC如CJ1、CS1等系列常用于过程控制任务。CJ1G-CPU4引入新型回路控制，CPU单元内置控制模拟量(如温度、压力、流速)的引擎，可与执行顺序控制的引擎一起为单个单元提供高速顺序控制以及高速的高级模拟量控制。具备高速执行速率，可在10ms内执行20个回路的PID操作，结构化的编程让程序更标准与简化。

除了上述在冶金场景中常见的控制器品牌，AB、三菱、GE等厂商生产的PLC也在冶金行业中有所应用。工业控制器依照生产需求，结合现场传感器采集的数据，

按照内部代码逻辑控制执行单元完成相应动作，并及时将设备及生产状态以工控协议规定的流量格式发送给上位机，作为整个生产系统的大脑在冶金场景中起到至关重要的作用。这也要求控制器必须能够长期稳定、可靠地运行，控制协议能够满足实时性、准确性的要求。因此，生产商在设计控制器时将实用性与可靠性作为最重要的生产标准，而在一定程度上忽略了安全性。同时早期工控设备与外网隔离，拥有天然的保护屏障，不存在遭受网络攻击的问题，其安全性更容易被忽略，这导致工业控制器中普遍存在威胁性较高的安全漏洞。冶金场景下常用控制设备存在的漏洞举例[32]如表1所示。

表 1 控制器漏洞

CVE-ID	漏洞描述	受影响产品型号	漏洞评分	漏洞类型
CVE-2018-18997	设备允许未经身份验证的攻击者使用管理 Web 界面将 HTML / Javascript 有效负载插入任何设备属性，这可能使攻击者可以显示/执行访问者浏览器中的有效负载。	Gate-e1 Firmware Gate-e2 Firmware	4.5	web
CVE-2011-5007	3S CoDeSys 3.4 SP4 Patch 2 和更早版本的 CmpWebServer 组件中基于堆栈的缓冲区溢出，如 ABB AC500 PLC 和可能的其他产品所使用的那样，使远程攻击者可以通过长 URI 到 TCP 端口 8080 执行任意代码。	Codesys3.4 ABB AC500 PLC	10	Buffer Overflow
CVE-2015-3938	MELSEC FX3G PLC 设备上的 HTTP 应用程序允许远程攻击者通过长参数导致拒绝服务(设备中断)。	Melsec Fx3g	7.8	DoS
CVE-2019-6535	远程攻击者可以通过端口 5007 发送特定字	Some Firmwares of Q03，04，06，10，13，20，26，		DoS

	节，这将导致以太网堆栈崩溃。	50udecpu		
CVE-2019-13533	攻击者可能会监视 PLC 与控制器之间的流量并重播可能导致工业阀门打开和关闭的请求。	Omron PLC CJ series, all versions Omron PLC CS series, all versions	8.1	AC
CVE-2019-18269	软件会正确检查是否存在锁，但是该锁可由外部控制或受预期控制范围之外的参与者影响。	Omron PLC CJ series, all versions Omron PLC CS series, all versions	9.8	AC
CVE-2019-10955	一个开放的重定向漏洞可能允许未经身份验证的远程攻击者输入恶意链接，以将用户重定向到可以在用户计算机上运行或下载任意恶意软件的恶意站点。	Compactlogix 5370 L1\L2\L3FirmwareV30.014 Micrologix 1100 FirmwareV14.00 Micrologix 1400 A Firmware Micrologix 1400 B FirmwareV15.002	5.8	AC
CVE-2018-17924	罗克韦尔自动化 MicroLogix 1400 控制器和 1756 ControlLogix 通信模块未经身份验证的远程威胁参与者可以向受影响的设备发送 CIP 连接请求，并且即使连接了系统中的控制器，连接成功后仍可以向受影响的设备发送新的 IP 配置进入硬运行模式。当受影响的设备接受此新 IP 配置时，由于系统流量仍试图通过覆盖的 IP 地址与该设备进行通信，因此该设备与系统的其余部分之间会发生通信丢失。	1756-en2f、en2t、en2tr、en3tr Series A ,B ,C Firmware 1756-enbt Firmware 1756-eweb Series A,B Firmware Micrologix 1400 Firmware	7.8	AC
CVE-2017-6030	受影响的产品生成的随机 TCP 初始序列号不够充分，这可能使攻击者可以根据先前的值预测该数字。这可能会使攻击者欺骗或破坏 TCP 连接。	Modicon M221 Firmware1.1.1.5 Modicon M241 Firmware4.0.3.20 Modicon M251 Firmware4.0.3.20	6.4	insecure Protocol

CVE-2019-6820	ATV IMC 中收到特定的以太网帧时，存在缺少关键功能的身份验证漏洞，该漏洞可能导致设备 IP 配置(IP 地址，网络掩码和网关 IP 地址)的修改。	Modicon M100 Firmware Modicon M200 Firmware Modicon M221 Firmware Modicon M241 Firmware Modicon M251 Firmware Modicon M258 Firmware	6.4	AC
CVE-2017-2680	产品可能会受到特制 PROFINET DCP 广播(第 2 层-以太网)数据包引起的拒绝服务条件的影响。	Dk Standard Ethernet Controller Firmware4.1.1 Simatic S7-200 Smart Firmware Simatic S7-300 Firmware Simatic S7-400 Firmware Simatic S7-1200 Firmware Simatic S7-1500 Firmware	6.1	DoS
CVE-2016-9158	发送到端口 80 / tcp 的特制数据包可能导致受影响的设备进入缺陷模式。 需要冷重启才能恢复系统。	Simatic S7-300 Cpu Firmware Simatic S7-400 Cpu Firmware	7.8	DoS
CVE-2017-2680	产品可能会受到特制 PROFINET DCP 广播(第 2 层-以太网)数据包引起的拒绝服务条件的影响。	Dk Standard Ethernet Controller Firmware4.1.1 Simatic S7-200 Smart Firmware Simatic S7-300 Firmware Simatic S7-400 Firmware Simatic S7-1200 Firmware Simatic S7-1500 Firmware	6.1	DoS
CVE-2016-9158	发送到端口 80 / tcp 的特制数据包可能导致受影响的设备进入缺陷模式。 需要冷重启才能恢复系统。	Simatic S7-300 Cpu Firmware Simatic S7-400 Cpu Firmware	7.8	DoS

2.4.2 常用协议的安全性问题

在冶金场景中，控制器与其他设备通信时采用工控协议进行数据传输。冶金工控系统中常用的工控协议及其脆弱性分析如下：

- S7Comm、S7Comm-Plus

S7Comm(S7 Communication)是西门子公司开发的私有协议，属于S7通讯协议簇里的一种，其TCP/IP实现依赖于面向块的ISO传输服务。S7协议被封装在TPKT和ISO-COTP协议中，其报文结构如图7所示。S7Comm协议用于编程、在PLC之间交换数据、从SCADA(监控和数据采集系统)中访问PLC数据和安全诊断的目的[41]。目前使用该协议的有S7-300、S7-400系列PLC。

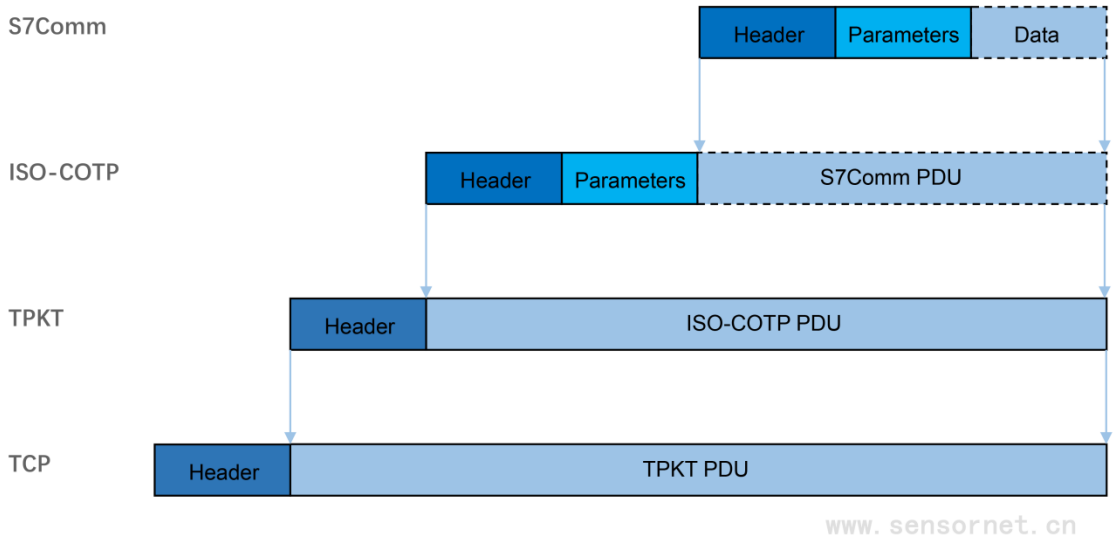

图 7　S7Comm协议格式

S7Comm协议使用明文传输信息，协议格式已经被解析的非常清楚，一旦流量

被捕获或监听，攻击者能够轻易地从流量中提取出敏感数据，获取设备信息。S7Comm协议不具备会话认证机制及完整性校验机制，攻击者可以通过中间人攻击、重放攻击等手段篡改控制器数据，甚至直接命令控制器执行危险操作，破坏正常生产过程甚至造成严重的安全事故。

S7Comm-Plus目前是S7通讯协议簇中安全性最高的协议，在S7Comm协议基础上添加了会话认证、程序加密等安全机制，建立通信前进行四次握手确定会话加密密钥，利用复杂的加密算法对交互内容进行保护，该协议部署于S7-1200/1500系列PLC之上。与S7Comm相比，S7Comm-Plus的安全性大大提升，显著降低了西门子PLC被攻击的可能性。但是，目前已有安全研究员对S7Comm-Plus协议进行了深度解析，利用其通信原理设计伪装上位机对PLC进行攻击，控制PLC的运行状态，甚至发动更为隐蔽的伪装攻击。

- Modbus

Modbus协议是Modicon公司推出的全球第一个真正用于工业现场的总线协议。与其他工控协议相比，Modbus协议具有公开发表且无著作权要求、易于部署和维护、修改本地字节更容易的特点，因此，在工业控制领域有非常广泛的应用。Modbus协议采用主-从结构，客户机使用不同的功能码请求服务器执行不同的操作[42]。服务器执行功能码定义的操作并向客户机发送响应，或者在操作中检测到差错时发送异常响应。

Modbus/TCP在冶金行业中应用广泛，其存在的安全问题不容忽视。Modbus协议通信过程缺乏必要的认证步骤，攻击者寻找一个合法地址，合理使用功能码就能建

立Modbus通信会话，达到扰乱正常通信过程的目的。Modbus协议目前没有较为全面的访问控制机制，导致用户可以进行任意操作，获取数据或攻击设备。同时，该协议所有的数据均通过明文进行传输，包括寄存器的地址、数值、变量类型等敏感数据，一旦攻击者进入网络监听，可以直接读取这些信息。

Modbus TLS协议以Modbus协议为基础，在传输层引入TLS协议以解决传输流程中的数据完整性、保密性和可用性问题。TLS协议即安全传输层协议，在OSI模型中通常被放置在第六层，在TCP/IP模型中则位于应用层和传输层之间，而它本身则可以被细分为两个层和五个子协议。TLS的特性在于定义了一组可以在两个通信对等体之间共享的安全加密参数，将其与Modbus/TCP相结合，可以保证数据传输在通过TSL握手建立的安全通道中，而TSL所要求的身份认证来源于服务器生成的包括版本号、用户名、有效性、签名算法和公钥的安全证书，这种保护方式有效的克止了重放攻击的发生。

但是，Modbus TLS提供了更高的安全性的同时，也增加了通信的复杂度，配置和部署的难度，虽然在[43]一文中对Modbus TLS方案的请求/响应事件进行了验证，但是考虑到采用的验证设备在工业控制系统中不具备普适性，且工业控制系统的更新能力有限，因此Modbus TLS协议的部署情况并不广泛。此外，由于TLS协议堆叠在TCP协议之上，因此不具有解决某些TCP漏洞的能力，如TCP SYN Flood和TCP RST Flood仍可能导致系统资源的耗尽，这些问题仍由其他普遍解决方法来预防。

- OPC协议

OPC(Object Linking and Embedding for Process Control)是微软公司的对象连接和

嵌入技术在过程控制方面的应用[44]。OPC规范从OLE/COM/DCOM的技术基础上发展而来，并以C/S模式为面向对象的工业自动化软件的开发建立了统一标准，该标准定义了在基于PC的客户机之间进行自动化数据实时交换的方法。

根据卡巴斯基实验室2018年的安全报告显示，OPC协议存在可被利用发起远程代码执行和DoS攻击的漏洞，并将这些漏洞归在两个漏洞编号下：CVE-2017-17433和 CVE-2017-12069，后者影响西门子自动化系统和配电产品的安全性。攻击者识别使用开放OPC服务的设备后，可利用漏洞向该设备发送Payload以触发DoS条件或远程代码执行攻击。攻击者可利用远程代码执行漏洞在网络中横向移动，控制工业流程并隐藏自身。

除此之外，Ethernet/IP、BACnet等公有协议以及MELSEC-Q、Omron FINS等私有协议也在冶金场景有所应用。这些工控协议在设计时并未考虑工控系统与外界网络的交互，因此安全机制薄弱。由于工控系统的开放性增强，工控内部网络正面临着前所未有的巨大考验。来自外部网络的攻击者可以利用工控协议的脆弱性对工控系统发起攻击，造成无法挽回的后果。

表 2 工控协议漏洞

协议名称	脆弱性	攻击风险
Modbus	缺乏认证机制、缺乏权限区分、数据明文传输、缺乏广播抑制(串行 Modbus)	敏感信息识别、信息欺骗、洪泛攻击、重放攻击
Ethernet/IP	加密、认证机制缺陷、完整性验证缺陷	伪造数据攻击、中间人攻击
OPC	过时授权服务、RPC 漏洞、多余端口服务	拒绝服务攻击、远程代码执行
DNP3	数据帧完整性、授权机制不足	中间人、重放、窃听、数据篡改、拒绝服务、缓冲区溢出
Profinet	授权、加密、认证缺陷	控制进程数据、读取设备状态

2.4.3 工控业务的安全问题

保证业务的持续性是对工控系统的基本要求。一个工控系统由多个业务组成，每个业务可以分为多个功能模块，每个功能模块由多个软件、硬件实现。工控系统的业务包括生产业务、通信业务、控制业务、调度业务、管理业务等。为了实现不同的业务，需使用不同的专有功能模块，而这些功能模块由主机、控制器、通信网络、应用软件、服务器等软硬件设备组成。由于系统软件漏洞、应用软件漏洞、控制器漏洞、通信协议漏洞的存在，使得业务不可避免的存在脆弱性，可能导致业务在受到外部攻击的情况下被中断。下面介绍面向业务的威胁源及威胁影响。

- 面向业务的威胁源

根据其造成损失的来源是否存在人为因素，冶金行业业务面临的威胁可分为两种类型：人为威胁和非人为威胁。其中，人为威胁根据业务所受破坏的意图分为恶意攻击威胁和非恶意攻击威胁；非人为威胁根据系统所受破坏的方式分为外在环境威胁和内在系统威胁。具体威胁源分类与详细描述见表3。

表 3 内外部威胁对工控系统业务的影响

威胁源类型	具体分类	示例说明
非人为威胁	外在环境威胁	断电、静电、灰尘、潮湿、温度、电磁干扰、洪水、火灾、地震、意外事故等环境危害或自然灾害。
	内在系统威胁	硬件老化、资源耗竭等带来的硬件威胁； 工业应用软件、APP 等设计缺陷带来的软件威胁；通信协议设计缺陷带来的网络威胁。
人为威胁	非恶意攻击威胁	内部工作人员的违规操作； 外部运维人员、产品供应商的隐私信息泄露等。
	恶意攻击威胁	利用病毒、木马、僵尸程序、逻辑炸弹程序、流氓软件、勒索软件等进行恶意代码传播的威胁； 通过网络服务或应用攻击，口令破解、字典攻击，散列认证规避，中间人攻击，拒绝服务攻击，权限提升，ARP 重定向、投毒，协议攻击，TCP 会话劫持等进行的虚假身份认证威胁； 利用过程控制的特点和缺陷设计对应的攻击手段，获取非法的操作权限，伪造合法的工控指令等形成的功

		能安全破坏威胁； 通过社会工程学攻击，采用非技术手段如插 U 盘、钓鱼手段、水坑攻击、物理破坏、社交媒体攻击等造成的管理威胁； 内部人员出于某种目的，利用本身的访问权限，物理接触系统、掌握系统的关键信息进行有意的破坏或数据信息泄露等造成的内部间谍威胁。

- 面向业务的攻击影响

通过梳理现有的安全事件，网络攻击对业务可能产生的影响包括：生产与经济损失、拒绝查看、拒绝控制、安全损失、视图丧失、操纵控制、操作视图、操作信息窃取，如表4所示。

表 4 业务脆弱性及其说明

影响	说明
生产与经济损失	黑客可能会通过中断甚至破坏控制系统操作、设备和控制过程的可用性和完整性而导致生产力和收入损失。此技术可以是针对物理系统攻击引起的直接影响，也可能是针对信息系统攻击产生的间接影响。
拒绝控制	攻击者会采用拒绝控制的方式以暂时阻止操作员或工程师与过程控制进行交互。攻击者可以通过拒绝过程控制访问实现与控制装置的暂时通信中断或阻止操作员调整过程控制。受影响的过程在失去控制期间可能仍在运行，但不一定处于期望的状态。
拒绝查看	攻击者会使用拒绝查看以试图破坏和阻止操作员对信息环境状态的监测，具体可表现为设备与其控制器之间的临时通信故障。在这种情况下，干扰一旦停止接口将恢复并可用。另外，攻击者可能通过阻止操作员接收状态和报告消息来实现拒绝查看，其目的是阻止操作员注意到状态的变化或异常行为。
安全损失	安全损失可以描述物理影响和威胁，或控制系统环境、设备或过程中发生不安全条件和活动的可能性。例如，攻击者会发出命令或影响，并可能抑制安全机制，从而导致人员伤亡。
视图丧失	当物理侧设备需要本地操作人员干预时，攻击者可能会造成持续或永久性视图丧失。通过造成持续的上报消息可见性丧失，攻击者可以有效地隐藏当前的操作状态。这种视图丧失不会影响物理过程本身。
操纵控制	攻击者可以在工业环境中操纵物理过程控制，操纵控制的方法包括对设定值、标记或其他参数的更改。攻击者可操纵控制系统设备或己方的设备，实现对物理过程的通信和控制。
操作视图	攻击者可能试图操纵上报给操作员或控制器的信息。这种操纵可能是短期的，也可能是持续的。在这段时间内，物理过程本身可能处于与所报告的状态截然不同的状态。如果视图被篡改，操作员可能会被欺骗去做一

	些对系统有害的事情，例如操作员可能会发出错误的控制指令，导致系统发生灾难性的后果。
操作信息窃取	为了谋取个人经济利益或者为将来的攻击行为做准备，攻击者可能把窃取生产环境中的操作信息作为任务目标。这些操作信息可能包括设计文档、生产计划、运行数据或提供操作细节的类似工件文件。

03

冶金工控系统主动防御技术体系

3.1 信息系统安全防御技术体系

PDR防御技术体系是最早体现主动防御思想的一种网络安全模型[45]。PDR模型是建立在基于时间的安全理论基础之上的，包括protection(保护)、detection(检测)、response(响应)三个过程，是一个可量化、可数学证明的安全模型。由于信息安全相关的所有活动，无论是攻击行为、防护行为、检测行为还是响应行为，都要消耗时间，因而可以用时间尺度来衡量一个体系的能力和安全性。在PDR模型的基础上，美国国际互联网安全系统公司ISS将其优化为循环式PDR模型，即P2DR模型，也称可适应网络安全模型。该模型包含4个主要部分：policy(安全策略)、protection(防护)、detection(检测)和response(响应)。在整体安全策略的指导下，通过部署安全防护措施对风险进行及时处置，并对处置过程中的经验进行总结，从而保证防护、检测和响应组成了动态安全循环。

之后在P2DR模型的基础上，进一步将恢复环节提升到与防护、检测和响应等环节同等重要的程度，提出了PPDRR模型[46]，也称为P2DR2模型。该模型是在整体安全策略的控制和指导下，综合运用防护工具和检测工具的同时，通过适当的响应策略将系统调整到“最安全”和“风险最低”的状态。该模型能够被用来解决业务连续性要求很高的系统安全防护问题。

APPDRR模型进一步贯彻了主动防御思想[47]，它认为网络安全模型的第一个重

要环节是风险评估，通过风险评估，掌握网络安全面临的风险信息，进而采取必要的处置措施，使得网络安全水平呈现动态螺旋上升的趋势。第二个重要环节是安全策略，一方面，安全策略应当随着风险评估的结果和安全需求的变化做相应的更新；另一方面，安全策略在整个网络安全工作中处于原则性的指导地位，其后的检测、响应诸环节都应在安全策略的基础上展开。系统防护是安全模型中的第三个环节，体现了网络安全的静态防护措施。接下来是动态检测、实时响应、灾难恢复三环节，体现了安全动态防护和安全入侵、安全威胁“短兵相接”的对抗性特征。

3.2 面向冶金工控系统的IPDR一体化安全主动防御模型

与传统信息系统相比，工控系统的保护对象不同，防护侧重点也不同，其主要区别如表5所示。在设备层面，由于工艺生产要求，工控设备需要保持长周期运行，导致系统和软件实时更新困难，传统防病毒和检测手段难以保障安全；在协议层面，工业协议私有化程度高，为满足功能性、实时性要求导致基础功能不完善，技术兼容性差；在业务方面，嵌入式计算环境实时性要求高，但计算、存储资源有限，传统安全技术将导致较高的系统负荷。

从威胁源头来看，工控系统不仅面临来自信息侧的威胁，还面临物理域与信息域手段的叠加作用，因此防范难度更大。从现实案例来看，这种融合也表现为阶段连续性的信息物理融合，通过信息侧发起威胁，引发关键信息基础设施内部信息域的局部扰动，再运用这种扰动构造跨越效应，引起信息域或者物理域更大尺度的暂态变化，并结合物理侧手段进一步迟滞或者破坏其他域的正常工作进程。

表 5　信息系统与工控系统安全防御区别

	工控系统安全	信息系统安全
设备层面	长周期运行、实时更新困难、技术兼容性差	可灵活更新、常规防病毒和检测手段有效
协议层面	高度私有化、基础功能不完善、兼容性差	标准化协议、完善的基础功能、良好的兼容性
业务层面	实时性要求高、计算、存储资源有限	实时性要求相对较低、计算、存储资源充足
威胁源头	信息侧威胁和物理域威胁叠加	主要面临来自信息侧的威胁

面对信息物理融合带来的各类威胁，防御人员需要深入探究工控系统安全内涵和安全体系构建原则，综合考虑功能安全和信息安全，构建面向工控系统全生命周期的一体化安全防护体系。根据冶金场景中工控系统防护的脆弱性，遵循现有的工控系统安全防护要求，本白皮书提出“识别(**I**dentification)-保护(**P**rotection)-检测(**D**etection)-响应(**R**esponse)”一体化工控安全主动防御模型**IPDR**，如图8所示，基于威胁识别与安全保护的系统安全加固方法以及基于信息网络与物理系统数据融合、安全联动的系统实时检测与响应机制，制定冶金工控系统主动防御技术体系。

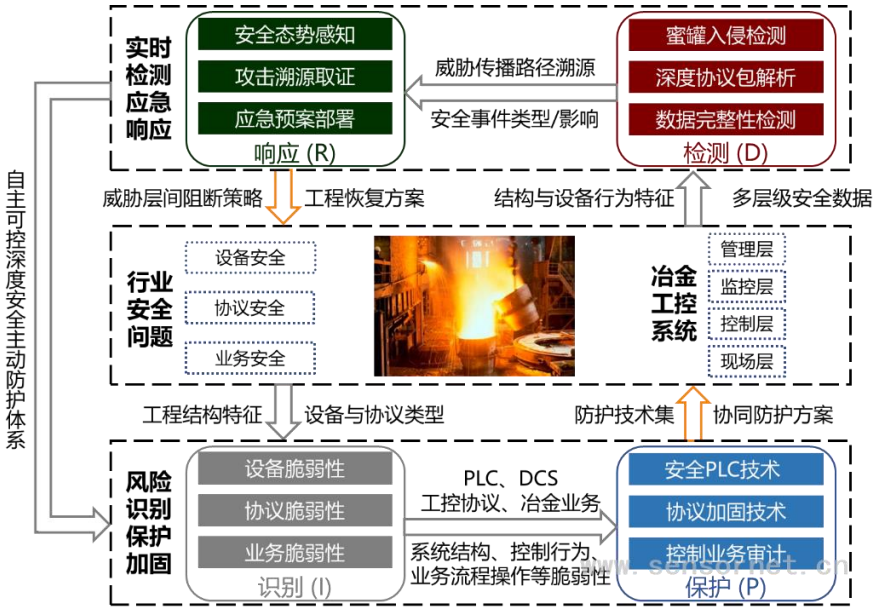

图 8 冶金行业主动防御技术体系**IPDR**

IPDR模型包括识别、保护、检测、响应四大安全模块，彼此之间协同配合，形成三大安全控制回路，实现具有自演化能力的工控系统威胁识别、安全保护、异常检测和实时响应的一体化联动和持续提升的安全防御技术体系。具体地，系统安全加固回路基于控制工程设计架构、运行机理、历史记录等信息的分析，识别工控系统安全脆弱点，针对性地提出系统设备、控制行为和业务流程的安全加固方案；威胁实时防护回路协同采集工控系统各层级安全数据，创新性地结合系统物理动态运行特征，综合分析系统状态，研究多层级威胁跟踪溯源机制并针对性地提出系统实时应急响应策略；以“实时检测应急响应”结果持续更新系统“风险识别保护加固”能力，“风险识别保护加固”的执行将进一步提高系统异常检测和防御能力，通过该动态演化机制，持续动态地增强工控系统应对威胁的防护能力。

- 识别

全面识别冶金工控系统在设计、运行、服务等全生命周期中组件、协议、设备等关键功能节点的自身脆弱性并进行脆弱性关联分析；从刻画威胁行为模式及其影响的角度，识别并总结控制工程全生命周期各阶段中的核心控制设备破坏、恶意代码注入等威胁的行为特征，以此制定识别策略应对潜在威胁。

- 保护

基于识别环节所得到的脆弱性分析结果，利用安全加密、多重访问控制、设备可信保护等技术对工控系统本体进行加固;同时根据工控系统本体在控制工程设计、运行、服务等阶段的全生命周期中的交互行为，对编译器、控制器、操作系统及通信系统进行安全优化。

- 检测

关联系统内部功能结构与外部威胁信息，分析工控系统功能、信息、操作等安全的相互依赖关系，根据系统自身结构与物理域的动态行为特征，关联管理、监控、控制与部件等层级的安全数据进行静态威胁特征匹配与动态异常检测机制，实现工控系统运行、服务等时期的异常实时检测；基于攻击源指纹信息、系统设备状态、工控系统各层数据流信息，结合工控系统拓扑结构、系统动态行为特征，实现威胁位置及传播路径的跟踪溯源。

- 响应

基于工控系统脆弱性与威胁事件关联关系，结合网络安全防御技术与物理系统安全保障机制(功能安全与操作安全)，构建结合功能、信息、操作等安全的前置防御响应策略库；结合专家知识与行业安全事件处置规则，构建基于特征匹配的应急响应方案科学决策机制。

3.2 冶金工控系统IPDR关键技术

- 主动防御技术总览

图 9 主动防御技术总览

- 威胁识别技术

(1) 控制器脆弱性分析技术

当前冶金工控系统中的控制器存在诸多安全漏洞，主要可归纳为不当的输入认证、许可权限和访问控制不足、缺乏完整性校验、组态软件漏洞等，可通过以下方法进行脆弱性分析。

固件逆向分析方法。通过提取嵌入式系统的固件文件，利用逆向工程技术进行解析，分析固件中各代码模块的调用关系及代码内容，从而发现嵌入式系统中可能存在的漏洞及后门。固件可通过官网下载、硬件接口获取等方式获得。常用的固件分析方法包括动态分析和静态分析。通过静态分析技术可以了解到后门密码、服务端口、配置文件等情况，但静态分析也存在不足之处，例如，法提供实际运行环境，无法获得固件在真实系统中的行为和交互、无法获取固件动态生成的代码、无法提

供固件运行时的变量值、寄存器状态等运行时信息，对于异常情况的认知和解析能力都十分受限。总言之静态分析能够提供的分析数据相对动态分析更为有限，因此需要将动态分析方法和静态分析相结合，对固件进行全方面的评估，可以通过qemu、gdbserver等工具进行动态调试以弥补静态调试的不足。

软件逆向技术利用逆向工程技术对控制器配套使用的上位机软件进行分析，通过静态调试或动态调试的方法测试软件功能，推演软件与控制器的交互过程，寻找其在数据传输、身份认证、逻辑更改等方面的脆弱性。

流量分析技术通过数据包分析软件获取控制器同上位机或其他控制器通信过程中的流量数据，配合上位机软件调试控制器功能，寻找两者在交互过程中可能出现的漏洞。

(2) 协议脆弱性分析技术

目前业界使用的工控协议均为二进制协议，运行在基于TCP/IP模型的工业以太网之上。相对于传统互联网协议，工控协议具有私有性、封闭性、场景性的特点，这使得对于工控协议的脆弱性检测更特殊[48]。早期的工控设备与外网隔离，不存在遭受网络攻击的风险，在设计工控协议时并未考虑到安全因素。随着工控系统的开放性增强，控制设备暴露在开放环境中的可能性越来越大，协议漏洞带来的风险日益升高[49]，对工控协议进行脆弱性分析，提升冶金场景通信安全性势在必行。常用的协议脆弱性分析方法如下

基于网络流量的协议分析方法。该方法需要采集大量工控协议报文数据，构建报文数据集，依据报文间变化规律和相似性提取特征字节，恢复报文格式。在传输

相同类型功能的报文时，报文的部分特征字段及格式具备较强相似性。执行相同功能时，报文的时序基本保持固定，有较强的规律性。常通过序列比对技术对上述特性进行分析，从而得到协议语法、语义、时序等要素。

基于程序分析的协议分析方法则以协议的上位机软件作为分析对象。上位机软件接收到报文之后，利用不同的程序段处理报文中的各项内容，因此报文的各部分内容与软件中的不同程序段具有潜在的对应关系，由此可以从程序运行记录中获取协议信息。动态污点分析技术是目前主流的程序分析方法。

模糊测试是一种“黑盒测试方法”，通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞。在工控协议分析中，模糊测试方法采用变异策略，向目标输入畸形的数据包，分析异常结果，常用工具包括Peach、SIPIKE、Sulley等。相较于逆向分析方法，模糊测试分析自动化程度高，可脱离源代码进行操作，但对于一些专有工控协议效果不佳，常用于对协议栈的分析。

(3) 业务脆弱性分析技术

工控系统的核心是保障控制业务的正常执行。通过感知现场层的物理过程状态，对业务进行有效控制和优化管理是工控系统的关键。然而，攻击者的最终目的往往都是破坏或阻断控制业务，造成设备损坏甚至人员伤亡。对于业务脆弱性一般可采用如下方法分析。

分析法通过机理建模，给出控制业务的动态数学表达。根据系统模型的输入输出关系，分析潜在攻击对相关变量的篡改、延迟、阻断效果，建立不同手段、不同目的、不同层次的攻击模态及其组合形式，刻画控制业务的脆弱性。该方法从系统

层面抽象出攻击形态，可辅助分析攻击对系统运行造成的影响。

控制逻辑反演法是一种基于数据来反推控制逻辑的方法。由于控制器一旦部署，往往很少进行更新和硬件迭代。对于攻击者而言，控制器的使用时间越久，其可被利用的漏洞越多。而对于操作员而言，很多控制器的配置文件早已遗失，控制器就像个黑盒。控制逻辑反演可重新恢复控制器中的控制业务逻辑，并分析控制逻辑是否存在被篡改、插入恶意代码、执行异常等风险，从而发现控制业务中潜在的脆弱性。

- 安全保护技术

(1) 安全PLC技术

目前国内工业场景中大部分使用进口控制器，难以满足自主可控的要求。使用国密算法芯片和国产操作系统，参考目前PLC普遍暴露出的安全问题，重新设计安全PLC架构及功能，添加通信加密、访问认证等安全功能，可以弥补冶金场景中现有控制器的安全问题，应对各类攻击威胁。

(2) 协议加固技术

对现有协议进行加固，提升协议安全性能，是解决当前冶金场景中工控协议脆弱性的有效方法。常用的协议加固方法包括黑白名单技术、动态分级加密技术、完整性保护技术、可信代理技术。

黑白名单是指根据当前工控系统状态，建立协议、节点、流量之间的关系模型，建立包含内部可信设备及可信行为的白名单，只允许白名单中的可信设备按照要求

执行可信操作，拒绝名单之外的设备访问和操作行为，强化通信行为的规范性，弥补现有工控协议脆弱性带来的威胁。

动态分级加密技术将各类数据按照功能及敏感度进行划分，针对不同数据采用不同等级和成本的保护方案。加解密模块利用实时密钥对敏感数据进行加密，降低攻击者破解加密的可能性。

可信代理技术借由配置有白名单规则的代理服务器实现协议的轻量级安全加固，为不具有会话认证的协议提供保护。通过配置过滤规则检测流量的合法性，对接收的流量进行过滤，同时记录非法流量以便后续的威胁排查。通过可信代理服务器将工控协议交流双方隔离保护，降低了非法流量的威胁。

(3) 控制业务审计技术

通过业务审计技术对冶金工控系统开展安全审计，进而从业务层面对冶金系统进行保护。通过工控安全审计系统采集场景中产生的实时流量，识别通信双方身份及涉及的业务信息，构建冶金系统网络通信模型，从业务要求与业务逻辑的角度检测流量。同时可以通过独立于审计对象的审计师对冶金工控系统的业务场景进行审计评价，提出当前存在的问题和改进建议。

- 异常检测技术

(1) 蜜罐技术

工控蜜罐模仿真实的工控设备行为，迷惑攻击者向其发动攻击，收集攻击方法并以此制定相应的防御策略[50]。蜜罐捕获的数据都与攻击行为有较强的相关性，基

于蜜罐数据的入侵检测算法可以获得很低的误报率和漏报率，进而有更大的概率捕获新的攻击。由于蜜罐设计的目的就是为了被入侵，因此，部署在蜜罐之上的入侵检测系统总是能在第一时间发现入侵，从而触发网络报警、系统报警或数据报警。根据预置的蜜罐策略，可以及时限制攻击者对关键设备的访问。

(2) 协议深度包解析技术

如何结合工控系统的特性，并通过理解数据中隐含的语义信息来进行系统运行状态的异常检测一直是工控安全中的关键问题。深度包解析能够有效地获取系统可信信息并进行异常检测。通过拆解协议数据包，基于OSI七层模型分析各层次在数据包封装过程中实际的应用情况，根据层次结构解封采集到的数据包，并根据相应协议文档对各层信息进行逐层解码获取报文信息。

(3) 基于深度神经网络的异常检测技术

基于TCP/IP的工控协议在控制网络通信过程中有明确的交互机制，但很多数据包的动态序列会因为不同连接之间的相互干扰而呈现出一定的随机性。长短期记忆神经网络因为对历史序列具有选择性记忆功能，能够很好地解决噪声混入或因序列过长而造成梯度消失的问题。经过分析工控网络通信数据包序列的动态特征，根据与自然语言文本预测研究的相似性，选择具有记忆性的预测模型来设计入侵检测算法，能够有效提高攻击检测成功率。

(4) 对抗样本生成技术

基于机器学习算法的入侵检测系统是目前工控安全方向的研究热点，但机器学习算法易被攻击者精心设计的对抗样本所欺骗。因此，为了保证工控系统应用安全，

维护其算法的安全性和鲁棒性，需要设计一个针对工控入侵检测系统的对抗样本生成算法。通过主动生成对抗样本，可以进行工控系统相关的主动防御，进一步增强数据包异常检测性能。

(5) 数据完整性检测技术

冶金系统运行时会产生大量相关数据信息，这些数据在时间上具有关联性，易受到攻击者攻击篡改。可利用神经网络在行为与时间相关的特性构建数据完整性攻击模型，识别攻击者注入的虚假数据。还可以在控制系统中引入水印认证机制弥补防御信息不对等劣势，提升攻击检测性能。

(6) 业务检测技术

冶金工控业务涉及大量复杂的过程数据，在出现故障或攻击后，这些数据会发生异常波动。因此，可以应用RNN网络分析技术进行高效的质量预测、异常检测、能耗优化、生产优化、产品质量分析等。业务上还可以通过对社交媒体、新闻、论坛、微博等平台的数据进行监控和分析，冶金企业可以了解到相关舆论趋势，这有助于及时发现和应对可能产生的攻击。

- 应急响应技术

(1) 冶金系统安全态势感知技术

冶金环境中包含大量主机、控制器、路由器等设备，其产生的日志与告警之间有很强关联。态势感知技术通过多元数据融合技术识别外部攻击信息，利用其他信息进一步得到攻击对系统造成的影响，并根据当前影响趋势进行预测判断[51]。态势

感知技术可分为状态提取、态势评估、趋势预测三部分，通过融合多元数据对系统整体态势做出判断，并依据历史记录和当前情况进行预测，从而起到受到攻击后及时响应，提前补救的作用。

(2) 攻击溯源技术

系统遭受恶意攻击之后，应立刻对攻击行为进行溯源，找出攻击者真正意图，遏制攻击者进一步行动。攻击溯源技术主要包括网络溯源技术和恶意代码溯源技术。前者通过分组标记、设备日志、链路分析、IP定位等方式追踪攻击者身份、位置、攻击路径等信息，后者通过分析恶意代码内容、比对典型攻击代码特征及攻击套路溯源出代码的作者及所属类别。

(3) 攻击取证技术

系统受到攻击后，现场会遗留相关攻击信息。针对现场具体情况，采取特定手段保护攻击痕迹，之后通过残余数据获取、日志分析等方法获取攻击前后设备的运行状态及行为记录，经过分析鉴定，找到有价值的攻击证据及攻击信息，协助后续保护恢复工作，并向相关部门呈现规范形式下的保存结果。

(4) 安全应急预案部署

安全应急响应预案是针对内外部攻击者入侵的应急管理、指挥、紧急恢复等策略，是根据冶金场景特点，针对各级可能发生的安全事件制定的专项方案。没有一种安全防御策略能够提供绝对的保护。提前制定安全应急预案，能够帮助工作者在面对突发的攻击事件时有所准备，采取合理的处置措施及时应对，树立最后的安全屏障。

3.3 IPDR主动防御技术体系的优势

IPDR主动防御技术体系具有以下特点：

- 全面性

IPDR模型以“识别-保护-检测-响应”四个关键步骤，形成一套完整的一体化主动防御体系，安全保护范围覆盖了冶金场景中常被作为攻击目标的工业控制器、监控上位机及其他网络设备，全面保护了数据采集、指令控制、信息传输等工控行为。

- 系统性

IPDR模型各个环节间相互支持，构成完整的安全防护系统。三大回路闭环反馈，实现威胁识别、安全保护、异常检测和实时响应的一体化联动和持续提升，形成可自动演化的安全防护生态系统。

- 综合性

由于工控系统信息安全威胁与物理系统业务逻辑缺陷、设备随机故障等安全风险深度耦合，单一信息网络防御或物理系统保护难以为工控系统提供有效防护。通过识别、保护、检测、响应四项防护模块联动，统筹各项防御措施，确保冶金生产的信息安全、功能安全、操作安全，协同优化冶金工控系统防御能力，提升冶金场景的综合安全性。

04

冶金典型场景下的IPDR应用方案

4.1 IPDR主动防御技术体系

冶金行业面临着控制系统数量多、控制协议脆弱、控制软件升级滞后等问题。面向其设计防护系统的基本思路是围绕“识别(**I**dentification)-保护(**P**rotection)-检测(**D**etection)-响应(**R**esponse)”四个方面，形成一套完整的一体化**IPDR**主动防御技术体系。

- 识别

实现对控制器组态篡改、插入、删除等破坏行为的在线精确识别；对控制系统漏洞进行识别与扫描，扫描对象包括HMI、上位机、PLC、数据采集和存储服务器等；深入分析冶金系统网络结构、控制数据流特征等，建立网络安全基线检查标准和规范，协助网络安全管理人员及时识别网络安全风险。全面识别针对控制工程全生命周期各阶段的核心控制设备、协议和业务等攻击行为。

- 保护

按照冶金工控系统安全优先级或业务关键程度，对控制网络进行横向安全区域逻辑划分，实现基于逻辑安全区域的网络安全风险隔离。采用白名单技术，对上位机进行进程级防护，防止非法软件、程序或进程运行；设计工业主机安全防护系统，使其具有自主安全防护功能，防止非法卸载。基于识别环节所得到的设备脆弱性分

析结果，针对冶金场景下常用的工控设备存在的脆弱性，设计本体安全防护方案，利用安全加密、多重访问控制、设备可信保护等技术对工控系统本体进行加固；同时根据工控系统本体在控制工程设计、运行、服务等阶段的全生命周期中的交互行为，对编译器、控制器、操作系统及数据采集与监控系统进行安全增强和优化；关联CVE、CNVD等漏洞数据库，实时关注供应商发布的漏洞补丁、固件版本并及时更新；部署具备工控流量解析能力的安全网关、安全网闸、工业防火墙等网络防护设备。

- 检测

关联系统内部功能结构与外部威胁信息，分析工控系统功能、信息、操作等安全的相互依赖关系，根据系统自身结构与物理域的动态行为特征，关联管理、监控、控制与部件等层级的安全数据，设计静态威胁特征匹配与动态异常检测机制，实现工控系统运行、服务等阶段的异常实时检测。具体来讲，融合情报、规则关联、机器学习、统计行为等分析方法将检测发现的网络攻击数据、告警数据、运行分析数据、信息系统漏洞等多维度历史数据统一汇总分析后，结合本地数据回溯攻击过程。同时支持自动化漏洞扫描，支持入侵检测系统及时发现针对工控系统的入侵行为，支持审计系统对冶金系统通信内容进行识别审查，实时监控工控通信过程，发现异常及时告警、实时推送。

- 响应

构建基于网络安全管理平台分级部署协同管控的网络安全管理体系，实现工控系统脆弱性与主要攻击事件之间的关联关系，结合网络安全防御技术与物理系统安

全保障机制(功能安全与操作安全)，构建结合功能、信息、操作等安全的前置防御响应策略库；结合专家知识与行业安全事件处置规则，设计基于特征匹配的应急响应方案科学决策机制。

4.2 关键技术部署

根据冶金行业工控系统规模及业务数据流特点，遵循工控信息安全防护投入适度、技术管理并重、分层分区域建设、动态调整四大原则，制定如下工控系统安全防护方案。

控制层部署控制器监测和恢复模块，对控制器的程序运行状态进行实时监测，并能对被非法篡改的组态程序进行恢复。采用基于白名单技术管控所有工作站和服务器，在同一网段内应当能够实现集中管控或日志采集，防范未知病毒的运行及其对主机资源的利用。限制控制器的访问控制权限，使用经过安全论证的认证机制。增加异常检测模块，实时分析网络流量，深度解析工控协议数据包。

监控层采用态势感知平台，被动式的安全分析和漏洞分析，不产生主动流量干扰工控生产环境；自动生成网络拓扑，并支持基于网段的灵活查询分析。采用工控漏洞扫描系统，探测工控环境中的软硬件工控资产的漏洞存在情况，并支持与CVE、CNVD与CNNVD漏洞库的关联。采用工业入侵检测系统，工控入侵行为检测库涵盖针对工控系统的各类扫描、探测、远程连接、设备控制等行为。采用工业安全审计系统，用于工控网络内工业实时流量采集与审计，实现网络异常识别、非法入侵识别、非法设备接入识别等功能。

管理层采用工业信息单向导入系统，用于工控网络和信息网络或者工控网络内

的边界防护和单向物理隔离。采用融合双物理主机和专用单向隔离卡的安全物理架构，实现无协议数据单向摆渡。采用工业综合安全管理平台，用于对工控网络内所有网络安全设备上送数据进行统一处理和存储，基于数据分析进行风险评估和安全预警。

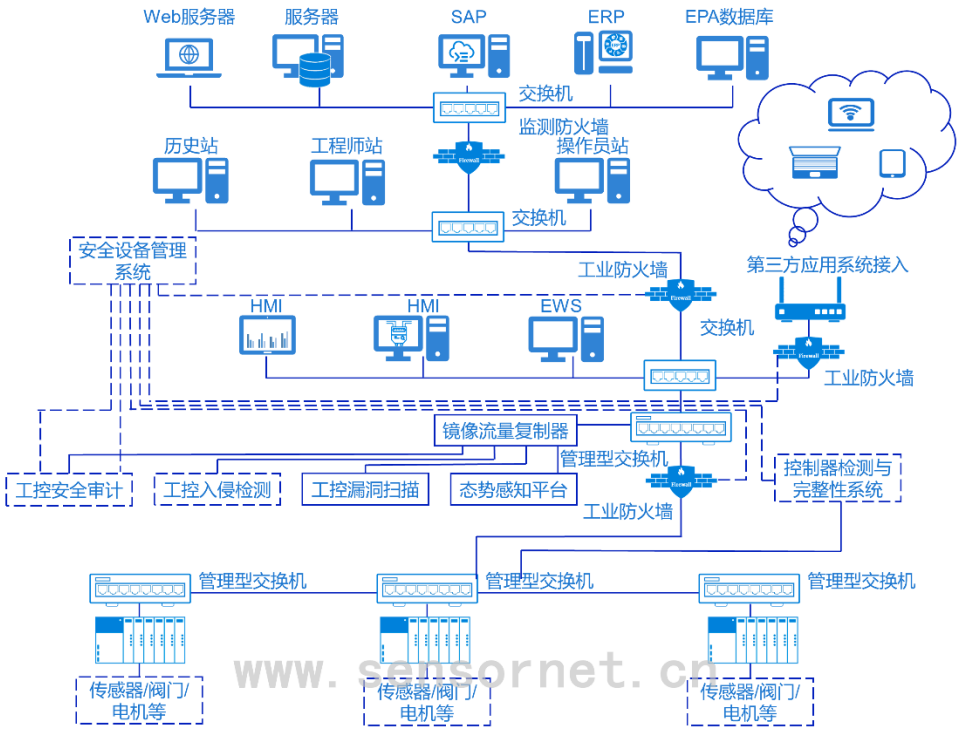

图 10 冶金场景工控系统主动防御技术部署图

4.3 主动防御关键技术及其功能

表 6 防御技术及其功能

控制器安全组态及其监视系统	实时监测控制器健康状态：对设备的运行状态、数据状态等进行实时监测
	备份控制器关键数据：备份控制器控制代码、硬件配置、原始参数等关键数据，在控制器遭受攻击导致数据和配置缺失后进行快速恢复
	控制器数据块级监测与恢复：支持控制器组态、篡改、插入、

	删除等破坏行为的在线精确识别与恢复
	一对多安全防护模式：可根据控制网络规模灵活配置，一台设备最多可同时支持十台控制器的数据监测与组态恢复
	硬件基础：产品采用工业级元器件、工业级设计，支持 1+1 冗余电源
	灵活的控制器安全防护模式：根据用户需求配置防护策略、防护模式，支持告警、恢复等多种防护模式
	丰富的设备与协议兼容性：支持西门子 S7-300、西门子 S7-400 控制器、AB5000 系列控制器、施耐德昆腾系列等控制器完整性监测与恢复。支持 Seimens S7、Seimens ISO、施耐德 Modbus/TCP 协议、RockWell CIP 等主流控制器厂商协议
工业主机安全防护系统	采用白名单技术，对上位机进行进程级防护，防止非法软件、程序或进程运行
	能够对移动介质进行管控，如光驱、软驱、USB 等
	能够限制文件夹读写权限
	告警及日志的管理
	自身安全防护，防止非法卸载
网络边界防护	基于白名单机制进行访问控制
	能够对所在网络工业协议进行深度包解析，并支持对标准的工控协议进行指令级解析
	支持数据流和协议自动分类和识别，辅助生成策略
	支持软件或硬件 bypass，异常情况下能够自动旁路
远程/外部终端接入防护	基于白名单机制进行访问控制
	能够对所在网络协议进行深度解析，并支持对公开的标准工业协议进行指令级解析
	支持实用的传统网络功能，和双机热备功能
	支持软件或硬件 bypass，异常状况下能够实现及时的自动旁路
网络行为监测和审计	工业协议深度解析
	工控资产扫描和登记
	工控安全基线管理

	实时监测流量异常和非法网络访问
未知威胁发现和跟踪溯源	未知私有协议逆向分析
	逻辑代码执行过程状态监测
	工控业务逻辑反演
安全策略和告警	对防火墙、网闸、上位机防护、工控审计、入侵检测进行安全统一管理
	独立于业务网络的安全管理专用网络
	安全管理网络采用加密方式传输
	包含安全策略统一管理，安全事件和日志统一采集
冶金态势感知系统	对防火墙、网闸、上位机防护、工控审计、入侵检测进行安全统一管理
	独立于业务网络的安全管理专用网络
	安全管理网络采用加密方式传输
	包含安全策略统一管理，安全事件和日志统一采集
工控网络漏洞识别和管理	通用漏洞扫描、工控软件扫描、工控设备扫描、自主工控漏洞扫描、数字化设计制造软件平台漏洞扫描、端口快速扫描、弱密码检测、定时扫描、扫描报表功能、管理员权限管理、AAA 认证、日志和告警、未知漏洞挖掘、资产管理等

参考文献

[1]. 李鸿培，忽朝俭，王晓鹏. 工控系统的安全研究与实践[R]. 北京：绿盟科技, 2014.
[2]. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Secur. Priv., vol. 9, no. 3, pp. 49-51.
[3]. M. Geiger, J. Bauer, M. Masuch and J. Franke, "An Analysis of Black Energy 3 Crashoverride and Trisis Three Malware Approaches Targeting Operational Technology Systems," IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, vol. 2020-Septe, pp. 1537-1543, 2020.
[4]. L. Zhao and W. Li, "Co-design of dual security control and communication for nonlinear CPS under DoS attack," IEEE Access, vol. 8, pp. 19271-19285, 2020.
[5]. 深度剖析：伊朗钢铁厂入侵路径推测及对钢企数字化安全转型启示[OL]. FreeBuf.COM, 2022. https://www.freebuf.com/articles/ics-articles/338273.html.
[6]. S. Hanna, S. Kumar and D. Weber, "IIC endpoint security best practices," IIC, USA, 2018. https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf.
[7]. S. Carielli et al., "IoT Security Maturity Model (SMM): Description and Intended Use," IIC, USA, 2020. https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf.
[8]. 刘晓曼，杜霖，杨冬梅. 2019 年工业互联网安全态势简析[J]. 保密科学技术, 2019(12):27-31.
[9]. 工业控制系统信息安全防护指南[R]. 工业和信息化部, 2016.
[10]. 中国工业互联网安全态势报告(2018 年)[R]. 中国信息安全, 2018.
[11]. 工业信息安全标准化白皮书(2019 版)[R]. 工业信息安全产业发展联盟, 2019.
[12]. 2020-2024 年中国冶金行业深度调研及投资前景预测报告[R]. 锐观产业研究院, 2019.
[13]. 冶金行业产业链及投资机会分析[OL]. 中国投资咨询网，2016. http://www.ocn.com.cn/chanye/201604/satdx12151318-2.shtml.
[14]. 冶金自动化．科技新进展：冶金工业互联网与大数据平台建设[OL]. 2020. https://www.sohu.com/a/408203956_465552.
[15]. 王彦姣. 智能自动化在金属冶炼中的应用研究[J]. 世界有色金属, 2020(12):15-16.
[16]. 于立业，薛向荣，张云贵等. 工控系统信息安全解决方案[J]. 冶金自动化, 2013, 37(1):5-11.
[17]. 李新创，施灿涛，赵峰. “工业 4.0”与中国钢铁工业[J]. 钢铁, 2015, 50(11):1-7.
[18]. 中国两化融合发展数据地图(2018)[R]. 国家工业信息安全发展研究中心, 2018.
[19]. 工业互联网与钢铁行业融合应用参考指南[R]. 工业互联网产业联盟，中国钢铁工业协会，中国金属学会, 2021.
[20]. 王伟哲. PLC 在钢铁冶金企业电气自动化控制中的应用[J]. 科技风, 2020(06):118.
[21]. 赵明珠. 钢铁冶金企业自动化仪表的有效运用[J]. 化工管理, 2020(08):159-160.
[22]. 张志远，刘竞，高棋兴. 工控网络安全设备在冶金行业(炼钢)高炉的应用[J]. 自动化博览, 2020, 37(02):32-34.
[23]. 王利山. 浅析炼铁高炉的自动控制系统[J]. 科技创新与应用, 2016(10):87.
[24]. 朱邦产. PLC 和计算机控制系统在冷轧带钢生产线中应用[J]. 科技资讯, 2010(23):50-51.
[25]. 夏侯振宇，杨华. 钢铁企业工业信息安全风险分析和防护对策探讨[J]. 江西科学, 2021, (2):374-380.
[26]. 信息安全与通信保密编辑部. 德国钢厂遭网络攻击造成巨大物理破坏[J]. 信息安全与通信保密, 2016(09):25.
[27]. 许海峰，靳静，丛力群. 冶金行业工业控制信息安全系统浅析[J]. 自动化仪表, 2015, 36(09)1-5.
[28]. 赵坤鹏，张成军，韩明，王义. 浅论冶金工业环境下网络病毒的防范与治理[J]. 自动化博览, 2020, 37(08):84-87.
[29]. K. Stouffer, V. Pillitteri, "Guide to Industrial Control Systems (ICS) Security," NIST, 2011. http://dx.doi.org/10.6028/NIST.SP.800-82r2.
[30]. 刘锋，冯全宝. 一种基于工业防火墙的序列攻击检测实现方法[P]. 北京市：CN111245780A, 2020-06-05.

[31]. 赖英旭, 刘静, 刘增辉, 张靖雯. 工控系统脆弱性分析及漏洞挖掘技术研究综述[J]. 北京工业大学学报, 2020, 46(06):571-582.
[32]. 国际 CVE 标准[OL]. http://www.cve.mitre.org.
[33]. 国家信息安全漏洞共享平台[OL]. https://www.cnvd.org.cn/.
[34]. 国家信息安全漏洞库[OL]. http://www.cnnvd.org.cn/.
[35]. 陈广勇, 祝国邦, 范春玲.《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)标准解读[J]. 信息网络安全, 2019(7):1-7.
[36]. 郇恩年. PLC 在用户行业中的调查报告[J]. 机电产品市场, 2004(07):20-22.
[37]. 陈明, 司鹏, 李红. 施耐德电气 Quantum PLC 在高炉上料系统中的应用[J]. 可编程控制器与工厂自动化, 2008(05):60-62+51.
[38]. 姚振爽. 施耐德昆腾 PLC 在高炉上料系统中的应用[J]. 中国科技信息, 2009(21):140-141.
[39]. 邱智豪, 韩建春, 罗丹. 基于欧姆龙 PLC 的自动送料装车控制系统设计与实现[J]. 数码世界, 2018(07):221-222.
[40]. 廖常初. S7-300/400 PLC 应用技术[M]. 机械工业出版社, 2012.
[41]. A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell and I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system," Int. J. Crit. Infrastruct. Prot., vol. 26, Sep. 2019.
[42]. 左卫, 程永新. Modbus 协议原理及安全性分析[J]. 通信技术, 2013, 46(12):66-69.
[43]. M. K. Ferst, H. F. M. de Figueiredo, G. Denardin and J. Lopes, "Implementation of secure communication with Modbus and transport layer security protocols," Proc. 13th IEEE Int. Conf. Ind. Appl. (INDUSCON), pp. 155-162, Nov. 2018.
[44]. 焦青松. OPC 技术及其在分布式远程监控系统中的研究与应用[D]. 华南理工大学, 2004.
[45]. W. Schwartau, "Time-based security explained: Provable security models and formulas for the practitioner and vendor," Computers & Security, vol. 17, no. 8, pp. 693-714, Jan. 1998.
[46]. C. Liu, Y. Zhang, and R. Chen, "Research on dynamic model for network security based on artificial immunity," Int. J. Knowl. Lang. Process, vol. 2, pp. 21-35, 2011.
[47]. 潘洁, 刘爱洁. 基于 APPDRR 模型的网络安全系统研究[J]. 电信工程技术与标准化, 2009, 22(07):27-30.
[48]. 冯涛, 鲁晔, 方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报, 2017, 38(S2):185-196.
[49]. 杨帅. 基于工业以太网的信息网络安全应用研究[J]. 信息与电脑(理论版), 2020, 32(13):212-214.
[50]. 胡海龙. 基于蜜罐技术的工业控制入侵捕获系统的设计与实现[D]. 郑州大学, 2017.
[51]. 李治霖. 工业控制网络安全态势感知的研究[D]. 长春工业大学, 2020.