**大型铝加工企业工业控制系统信息安全体系模型**

梁雨锋[[1]](#footnote-1)，汪萌[[2]](#footnote-2)

（1.中国铝业公司，北京 100082）

（2.中国铝业公司，北京 100082）

**摘 要：**工业控制系统信息安全面临越来越严峻的考验。结合大型铝加工行业生产特点，分析工业控制系统信息安全风险，参照国家信息安全等级保护相关要求，提出工业控制系统分层分区、纵深防御的信息安全防范思路和对策。

**关键词：**工业控制安全；铝加工企业；等级保护；信息安全

**Model of Industrial Control Systems Security in Large Aluminum Processing Enterprise**

Liang Yufeng, Wang Meng

（1.Aluminum Corporation of China ,Beijing,100082）

（2. Aluminum Corporation of China ,Beijing,100082）

**Abstract:** Industrial Control Systems Security is facing increasingly severe test. The information security risk of industrial control systems can be analysied by combining with the characteristics of production of the large aluminum processing industry. And referring to the national level of security protection requirements, ideas and measures of hierarchical partitioning and defensing in depth for information security of industrial control systems have been proposed.

**Keywords:** Industrial Control Security; Aluminum Processing Companies; Level Protection; Information Security

1. **工业控制系统信息安全现状**

现代工业控制系统 (ICS)包括数据采集系统 (SCADA)，分布式控制系统(DCS)，程序逻辑控制(PLC)以及其他控制系统等，目前已应用于金属冶炼、电力、水力、石化、医药、食品以及汽车、航天等工业领域，成为国家关键基础设施的重要组成部分，关系到国家的战略安全。

与传统基于 TCP/IP 协议的网络与信息系统的安全相比，我国 ICS 的安全保护水平明显偏低，长期以来没有得到关注。大多数ICS 在开发时，受限于计算资源有限，在设计时只考虑到效率和实时性等特性，并未将安全作为一个主要的指标考虑。随着信息化的推动和工业化进程的加速， 越来越多的计算机和网络技术应用于工业控制系统， 在为工业生产带来极大推动作用的同时，也带来了ICS的安全问题，如木马、病毒、网络攻击造成信息泄露和控制指令篡改等。 ICS 系统的安全事件会导致:(1)系统性能下降，影响系统可用性；(2)关键控制数据被篡改或丧失；(3)失去控制；(4)严重的经济损失；(5)环境灾难；(6)人员伤亡；(7) 破坏基础设施；(8)危及公众安全及国家安全。

据工业控制系统应急响应小组(ICS-CERT)通过工业控制系统相关的安全事故监控、分析执行漏洞和恶意代码、现场支持为事故响应和取证，发现工业控制系统相关的安全事件正在呈快速增长的趋势(如图1所示)。由图中可知，ICS-CERT 在2013 年上半年统计到的安全事件数已经超过了2012年全年的安全事件数。2013年上半年这 200多起工业控制系统安全事件，其中主要集中在能源、关键制造业、交通、通信、水利、核能等领域。

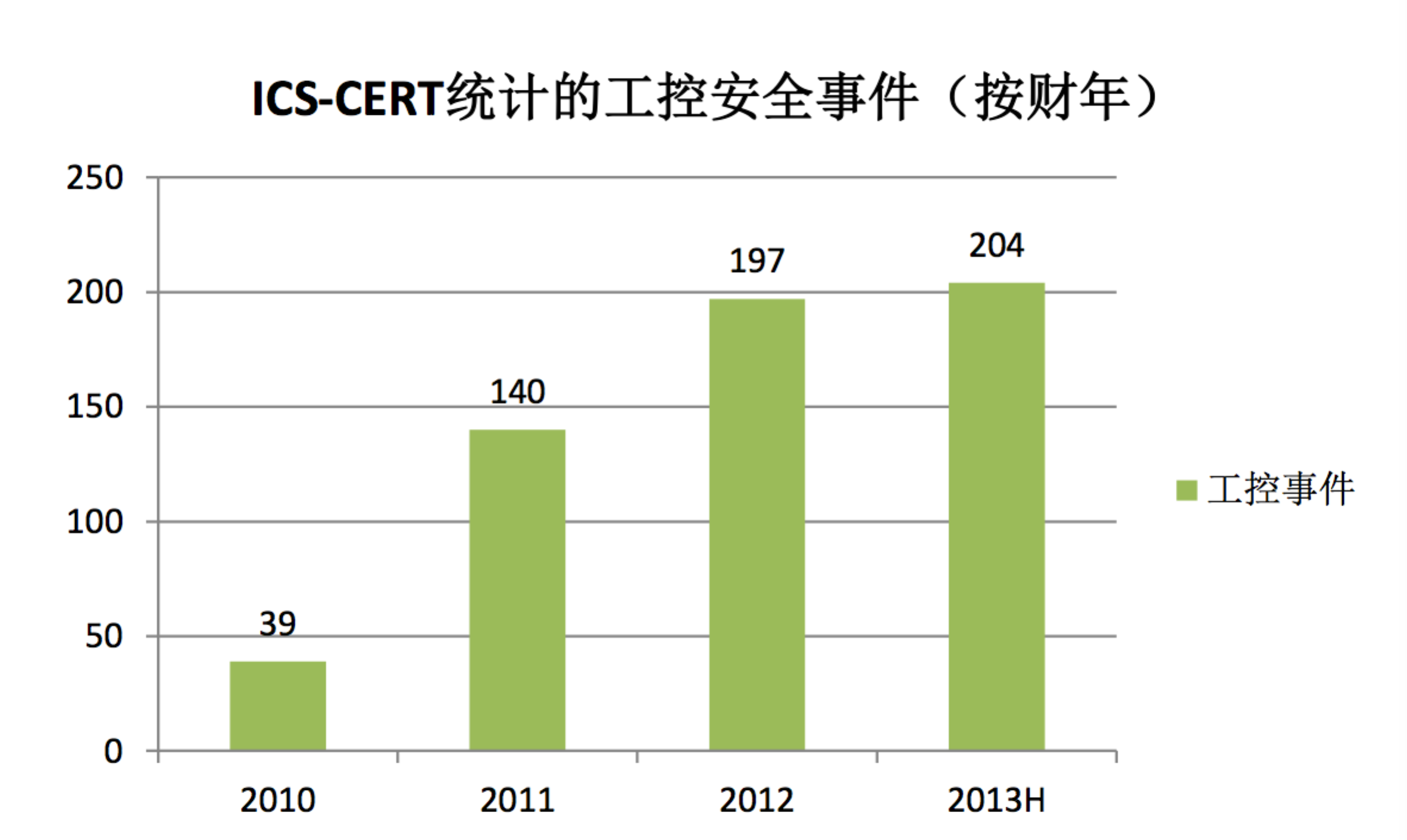


图1 ICS-CERT统计的工控安全事件

Figure 1 Industrial safety incidents statisticsed by ICS-CERT

1. **铝加工企业生产控制系统特点及信息安全分析**
   1. **铝加工行业生产控制系统特点**

铝加工企业主要生产板材、带材、箔材、管材、棒材、型材、线材和锻件（自由锻件、模锻件）等铝材料，产品广泛应用于航空航天、建筑、运输、电气、化工、包装和日用品工业等行业。生产控制系统以PLC为主，生产工艺有：

熔铸工序：熔炼→铸造→锯棒→铝棒均匀化→冷却、洗棒→进仓

挤压工艺流程：压前准备→挤压→拉伸矫直→锯切成品→装框修口。

板带连轧加工工艺流程：加热炉→粗轧→精轧→卷取。

以板带热轧生产为例，典型的工业控制网络如图2所示，HMI和过程机采用多CPU的高性能计算机，控制系统多采用PLC、Device-Net、FLEX I/O、现场执行设备及传动系统等。PLC采用西门子、施耐德、AB等品牌。

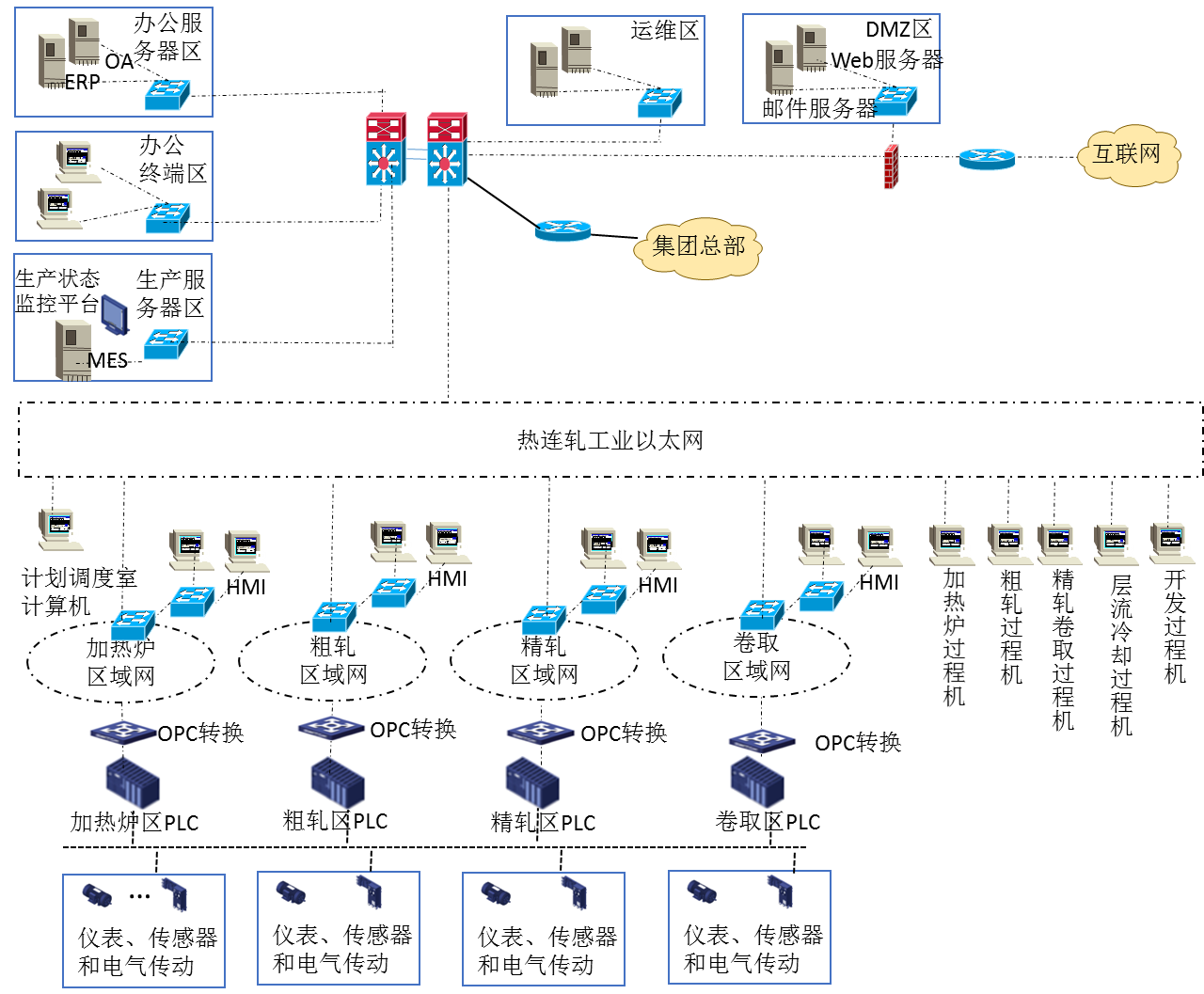


图2 热轧生产线工业控制系统架构

Figure 2 Industrial control system architecture of hot rolling production line diagram

* 1. **工业控制系统面临的信息安全问题分析**
     1. **威胁源分类**

随着两化融合的深入，工控系统不再是封闭的系统，而是与办公网、互联网有千丝万缕的联系，因此，威胁的来源也更加广泛，主要威胁如下表所示。

表1 工业控制系统威胁源分类

Table 1 Classification of threats source of industrial control systems

|  |  |
| --- | --- |
| **威胁源** | **描述** |
| **境外机构** | 在空间安全（Cyber security）和信息战的思维下，境外机构发展其对我国国家基础设施进行信息窃取、状态干扰和攻击的能力，其后果可能对我国工业基础设施产生严重影响，甚至可能危及人民生命 |
| **内部人员** | 由于利益或者不满情绪的驱使，利用其对工业控制系统环境相关系统的了解，将在不具备大量计算机入侵知识的前提下造成系统损坏或者信息失窃；同时人员误操作也可能造成一定程度上的风险 |
| **境内外**  **恐怖分子** | 恐怖分子尝试通过对工业控制系统的干扰、破坏从而威胁国家关键基础设施的安全 |
| **工业间谍** | 获取工业控制网络的相关核心技术和敏感信息 |

* + 1. **工业控制系统的脆弱性分析**

工业控制系统脆弱性分为管理和技术两方面，经分析主要存在策略和程序上的脆弱性，以及平台自身的脆弱性和网络脆弱性。

下表描述了工业控制系统中可能存在的脆弱性：

表2 工业控制系统脆弱性

Table 2 Fragility of industrial control systems

|  |  |  |
| --- | --- | --- |
| **脆弱性分类** | | **描述** |
| **策略和程序脆弱性** | | 缺乏针对工业网络的特定安全策略 |
| 无针对工业控制网络的培训和意识教育 |
| 缺乏安全架构和设计 |
| 没有针对安全策略形成安全工作流程 |
| 缺乏安全审计 |
| 缺乏工业控制网业务连续性计划或者灾难恢复计划 |
| 缺少口令重复登录的次数限制和口令定期更换机制 |
| 缺乏工业控制网络特定的变更管理 |
| **系统脆弱性** | **系统配置脆弱性** | 操作系统以及软件打补丁不及时，并且未经过测试 |
| 使用默认配置 |
| 关键配置未存储或者备份 |
| 移动设备数据缺乏保护 |
| 缺乏适当的密码策略 |
| 不恰当的访问控制 |
| **硬件脆弱性** | 针对关键系统缺乏物理防护 |
| 未授权人员对设备的物理访问 |
| 不安全的远程访问 |
| 资产登记不完备 |
| 缺乏备用能源 |
| 易受网络负载的影响，环境控制缺失 |
| 缺乏无线电频率和电磁脉冲防护能力 |
| 缺乏关键组件的冗余 |
| **软件脆弱性** | 存在缓冲区溢出漏洞 |
| 安全功能未默认开启 |
| 针对OPC的RPC/DCOM攻击 |
| 使用不安全的工业领域通讯协议 |
| 使用明文 |
| 运行不必要的服务 |
| 不适当的针对配置和编程软件的访问控制 |
| 未采用入侵检测/防御工具 |
| 未留存日志 |
| 未监控安全事件 |
| **恶意代码保护脆弱性** | 未安装恶意代码防护软件 |
| 恶意代码防护软件更新不及时 |
| 恶意代码软件部署前未测试 |
| **网络脆弱性** | **网络配置脆弱性** | 网络架构存在脆弱性 |
| 未对数据流进行限制 |
| 网络设备配置脆弱性 |
| 网络设备配置未存储和备份 |
| 敏感信息如口令等传输未加密 |
| **网络硬件脆弱性** | 不恰当的物理保护和环境控制 |
| 不安全的物理端口 |
| 未必要人员对网络设备和链接线缆的访问 |
| 关键网络缺乏冗余 |
| **网络边界脆弱性** | 未定义安全边界 |
| 未部署防火墙或者配置不当 |
| 控制网络内部存在其他不相关的流量 |
| 控制网络依赖非控制网络的服务 |
| **网络监控/日志脆弱性** | 不恰当的防火墙和路由器日志配置 |
| 控制网络无监控 |
| **无线网络脆弱性** | 无线客户端和接入点的认证措施不足 |
| 无线客户端和接入点之间的数据传输保护措施不足 |
| **通信脆弱性** | 通信缺乏完整性校验 |
| 通信未进行用户和设备的认证 |
| 采用公开明文协议 |
| 关键监控和控制路径未识别 |

工业控制系统漏洞日益增多，攻击手段更为复杂化，对工业控制系统的安全防护日趋重要，必须从整体安全防护角度出发。

1. **工业控制信息安全体系模型**
   1. **思路**

参照IEC62443《工业过程测量、控制和自动化 网络与系统信息安全》对网络进行分区分域，分析工业控制系统面临的威胁，依据《工业控制系统安全指南》（NIST SP800-82)、《信息系统安全等级保护基本要求 （GB/T 22239-2008）》等相关要求进行建设，重点加强纵深防御。

* 1. **体系模型**

参照IEC62443工业控制系统模型和IATF框架，对企业工业控制网进行分区分域，如下图所示。

企业经营管理（业务规划和物流）

生产管理

监督控制

基本控制

安全和保护

过程（受控设备）

第4层 企业经营管理层

第3层 生产管理层

第2层 监督控制层

第1层 现场控制层

第0层 现场设备层

工业自动化

与控制系统

图3 工业控制系统分层架构

Figure 3 Layered architecture of industrial control systems

第4层企业经营管理层，包括企业财务系统、办公系统、以及一个地点的下属工厂或所属企业进行生产计划、运营管理和维护等相关系统。

第3层企业生产管理层，包括分派生产任务，详细生产调度，可靠性保障的贯彻执行和本地的控制优化等。

第2层监督控制层，包括监督和控制实际生产过程的功能。包括人机界面HMI，操作员站，负责组态的工程师站等。报警服务器及报警处理。监督控制功能。实时数据收集与历史数据库，用于连接的服务器客户机等。

第1层现场控制层，主要是PLC,该层是对来自第0层的传感器所采集的数据进行操作，执行控制算法，输出到执行器（如控制阀门等）执行，该层通过现场总线与第0层的传感器和执行器形成控制回路。设备包括但不限于如下所示：

第0层现场设备层，该层是对生产设施的现场设备进行数据采集和输出操作的功能，包括了所有连在现场总线的传感器（模拟量和开关量输入）和执行器（模拟量和开关量输出）等控制对象。

* 1. **控制系统信息安全对策**

工业控制系统的信息安全按照分层分区、纵深防御思路进行设计。以大型铝加工企业为例，其工业控制系统层次和区域划分如下：

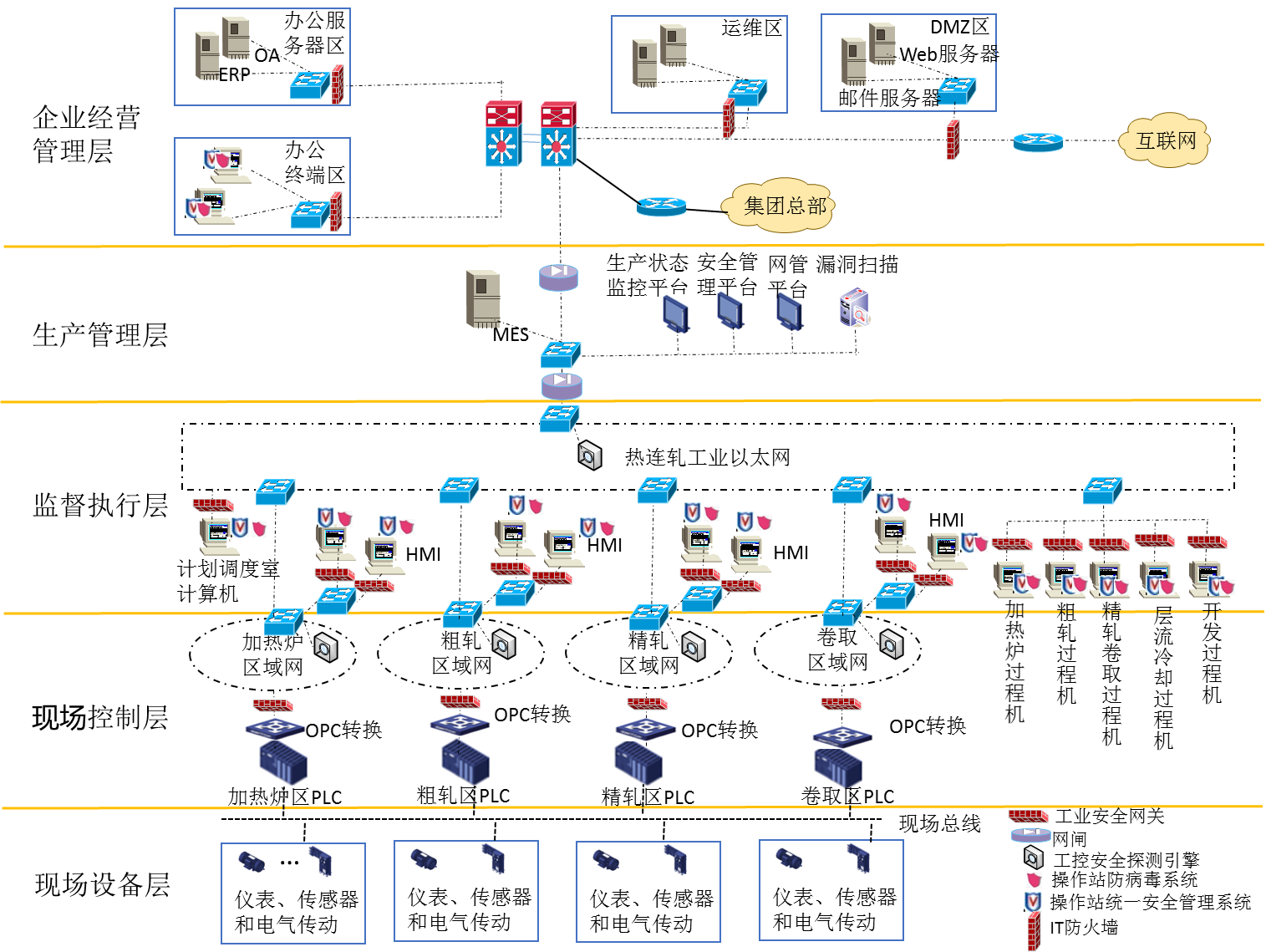


图4 某铝加工企业工业控制网络分层分区模型

Figure 4 Hierarchical partitioning model of industrial control network in an Aluminum processing enterprise

1. 现场设备层

现场设备层是传输的模拟信号或数字信号，与过程控制层设备进行严密的、高速的数据交换。在建设阶段考察仪表、传感器和电气传动设备的自身的安全性，例如：高可靠性、设备标识与鉴别、身份认证等。

1. 过程控制层

按照工序不同分为加热炉区、粗轧区、精轧区和卷取区，每个区域是单独的一个工业以太网。各工序需要有数据交互，通过梳理传输协议、IP地址、端口、传输参数和指令等信息，建立白名单，用工业安全网关做访问控制。

在各区域环网交换机上做端口镜像，部署采集器，采集网络传输数据，并传给安全管理平台。

1. 生产执行层

生产执行层包括各工序PLC的HMI以及过程计算机，使用的是通用Windows系统，在计算机上安装防病毒系统和统一安全管理系统，进行防病毒，U盘使用管理、上网管理、软件白名单管理、进程管理等。

在HMI、各工序过程机前端部署工业安全网关，实现对HMI或过程机与PLC通讯的传输协议、IP地址、端口、传输参数和指令等信息控制。并在热连轧工业以太环网交换机做端口镜像，部署采集器采集网络传输数据，并传给安全管理平台。

1. 经营管理层

在MES与工业以太网之间部署双向隔离网闸，采用数据摆渡机制对生产计划、生产状态数据、采集的网络数据、设备安全日志等信息进行传输控制。

部署安全管理平台实现如下功能：

1. 自动发现和识别工业控制设备资产，并识别这些资产之间的连接关系或包含关系，以拓扑方式展示资产信息。
2. 对各种不同厂商的工业控制设备、信息安全设备、网络设备、服务器的安全性与可用性进行实时监控，可以对监控指标设置告警阈值，触发告警。
3. 进行网络根本故障源（Root Cause）诊断，协助管理员定位故障问题源。
4. 分析出工业控制系统信息安全态势。
5. 提供多种知识体系，包括案例库、漏洞库、事件库、文档库、字典库等。

部署漏洞扫描系统对HMI、工业交换机、过程机、PLC等进行漏洞发现。

1. 战略决策层

运维决策层参照等级保护要求建设，在运维区部署漏洞扫描系统、运维审计系统、安全管理系统、桌面安全管理系统服务端、桌面防病毒服务端、准入系统、网管系统。办公服务器区部署防火墙做端口级的访问控制策略。在DMZ区部署VPN，web安全网关，邮件系统前部署防垃圾邮件。在互联网区部署上网行为管理、入侵防御系统等。

1. **结束语**

本文参照信息安全等级保护系列标准和相关规范的设计思路，提出了铝加工企业工业控制系统信息安全防护方案。通过此方案的实施可带来如下收益：

1. 促进两化融合进程，进而提高生产效率。
2. 提高防范工业控制安全生产事件的能力。
3. 总结试点经验，建立集团工业控制安全技术规范，指导同类型企业工业控制安全建设。
4. **参考文献**

|  |  |
| --- | --- |
| 期刊 | [1]唐文. 工业自动化控制系统信息安全研究[J]. 计算机安全, 2012 (4): 2-7 |
| 期刊 | [2]张帅. 工业控制系统安全现状与风险分析——ICS 工业控制系统安全风险分析之一[J]. 计算机安全, 2012 (1): 15-19. |
| 期刊 | [3]张敏, 张五一, 韩桂芬. 工业控制系统信息安全防护体系研究[J]. 工业控制计算机, 2013, 26(10). |

1. 作者简介：作者1梁雨锋（1962 ），男，北京，教授级高级工程师，博士研究生，企业信息化，北京市西直门北大街62号，010-82298868，yf\_liang@chalco.com.cn;作者2汪萌（1983 ），男，北京，中级工程师，硕士研究生，企业信息安全，北京市西直门北大街62号，010-82298869，wm@chalco.com.cn [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)