石化行业工控安全解决方案

龙国东

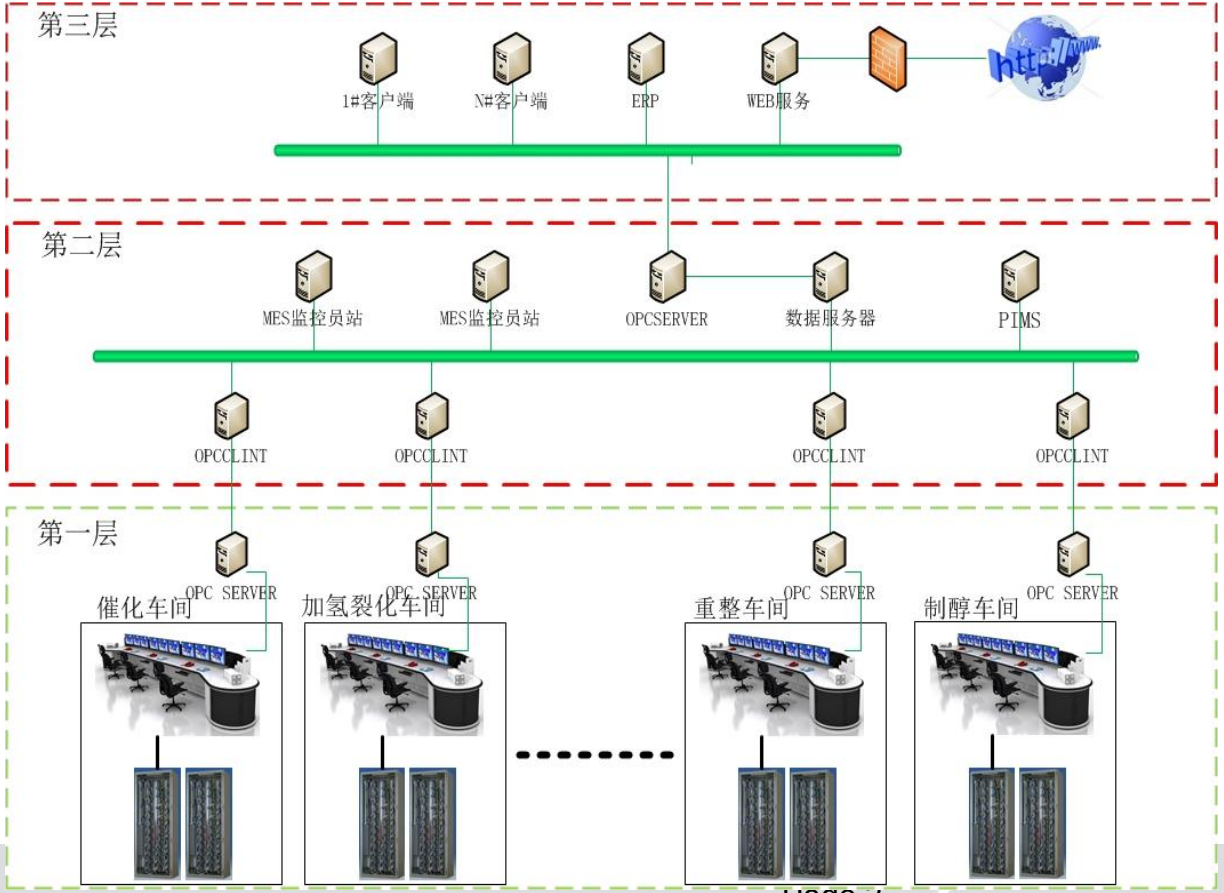
石油石化中工业信息化网络的应用

石油和化工企业的信息化分为三层结构：

第一层以PCS(Process Control System，过程控制系统)为代表的生产过程基础自动化层。；

第二层以MES(Manufacturing Execution System，制造执行系统)为代表的生产过程运行优化层；

第三层以ERP(Enterprise Resource Planning，企业资源计划)为代表的生产过程经营优化层。



“信息化带动工业化，工业化促进信息化”是中国的国策。

工业信息化网络面临的挑战

企业控制网络系统复杂多样，缺乏必要的安全边界及区域功能划分及防护；

交换机备用端口几乎无管理，可通过备用端口访问到系统中任何一台设备。

售后服务、运维服务人员被动服务，缺乏更新的指导策略及预防方法；

工程师、操作员站中专用软件和通用操作系统兼容性问题且缺少必要的防护手段；

网络中交换机某一端口发生异常只能查看交换机历史日志，缺少实时报警手段；

缺少专业的工控安全应急队伍，现有网络维护人员，无法及时、快速响应安全威胁和事件；

计算机U口只采用行政手段进行管理，可进行优化采用技术手段进行管理；

网络缺少必要的监测与审计手段，致使不能及时发现并相应网络威胁，不能追根溯源！

个别运行系统发现异常、疑似病毒文件；

石油石化行业工控网络的安全问题与风险

生产控制网络缺乏自身全面的安全性设计

我国石油石化行业生产控制系统安全防护滞后于系统的建设速度，生产控制系统缺乏自身的安全性设计。在信息安全意识、策略、机制、法规标准等方面都存在不少问题。

工控网络存在一定的脆弱性

（1）已建项目主要软硬件多为进口，可能存有后门

（2）油气开采、管道储运广泛使用无线通信，易被野外搭线监听、窃密和干扰

（3）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

工控网络面临着现实和潜在的威胁

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段

潜在威胁：攻击石油石化行业工控系统技术门槛越来越低，易被信息战攻击

工控网络安全防护体系尚未形成

（1）关键资产底数不清楚

（2）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）两化融合加速了网络安全风险的暴露

石油石化行业生产控制系统信息安全主要目标

保护工控系统免受病毒等恶意代码的侵袭。

避免工控系统遭受人为恶意或者无意的违规操作。

防范外部、内部的网络攻击。

在不利条件下维护生产系统功能。

安全事件发生后能迅速定位找出问题根源。

构筑工控网络安全“白环境”监控防护体系

运用**白名单**的思想，通过对工控网络流量、工作站软件运行状态等进行监控，运用大数据技术收集并分析流量数据及工作站状态，建立工控系统及网络正常工作的安全模型，进而构筑工业控制系统的网络 “**安全白环境**”。

核心理念

1. 只有可信任的 设备，才允许接入控制网络；
2. 只有可信任的 命令，才能在网络上传输；
3. 只有可信任的 软件，才能在主机上执行；

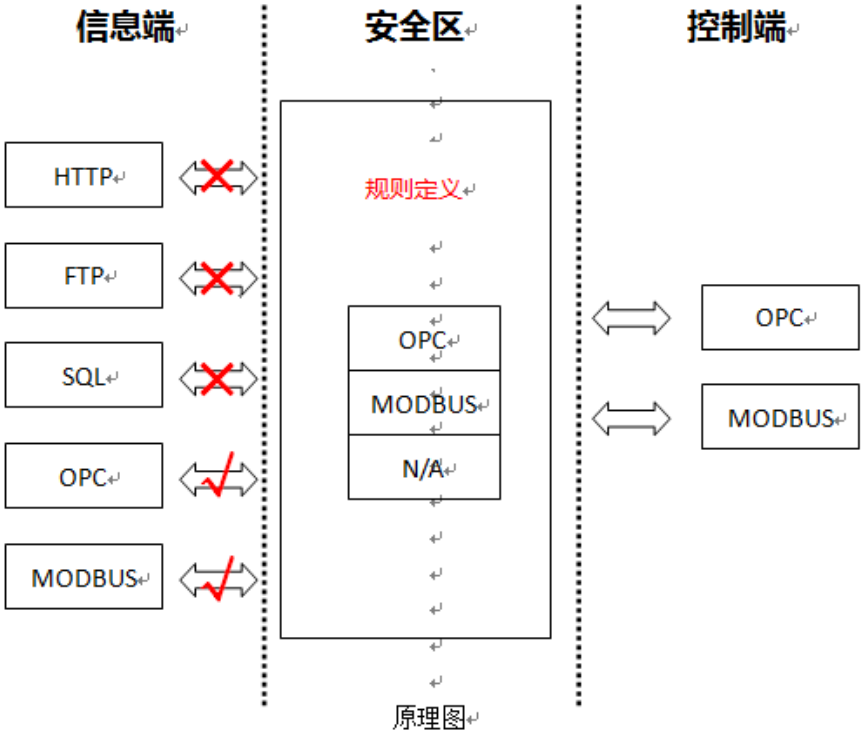
核心技术

1. 创新的“**软可信**”计算技术，降低方案成本，提高实用性；
2. 机器自学习“白环境”**智能建模**技术，降低维护成本，提高易用性；
3. 高速工控协议**深度包解析技术**，具备高安全性，低时延影响；

白名单机制

“白名单”主动防御技术是通过提前计划好的协议规则来限制网络数据的交换，在控制网到信息网之间进行动态行为判断。通过对约定协议的特征分析和端口限制的方法，从根源上节制未知恶意软件的运行和传播。

“白名单”安全机制是一种安全管理规范，不仅应用于防火墙软件的设置规则，也是在实际管理中要遵循的原则，例如在对设备和计算机进行实际操作时，需要使用指定的笔记本、U盘等，管理人员只信任可识别的身份，未经授权的行为将被拒绝。



原理图

纵深防御解决方案

1、网络分层分区，边界访问控制，避免无授权设备对区域的访问。

2、自学习建立工控系统及网络正常工作的安全模型 （安全白环境）和安全基线。

3. 基于通信“白环境”边界和区域的攻击防御和过滤

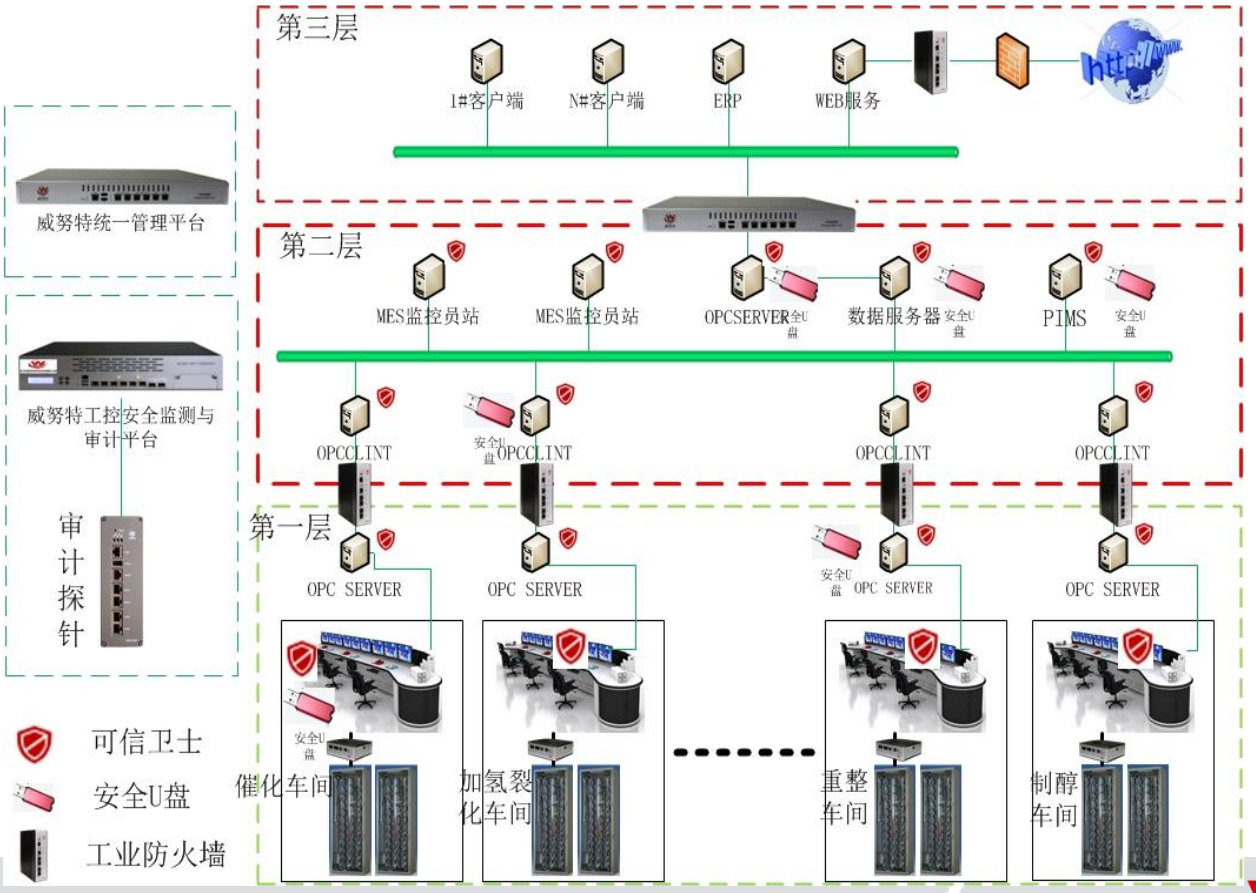
4. 基于通信“白环境”建立全网异常检测体系，实时检测恶意网络攻击，蠕虫扩散等

5. 终端安全：包括主机安全和DCS等工控设备安全

6. 统一安全管理和审计：响应异常，分析、审计攻击事件

7、动态安全：新攻击手段、防护方案、兼容性和影响进行验证。

8. 符合国际电工委员会（IEC）制定的工控安全防护62443标准



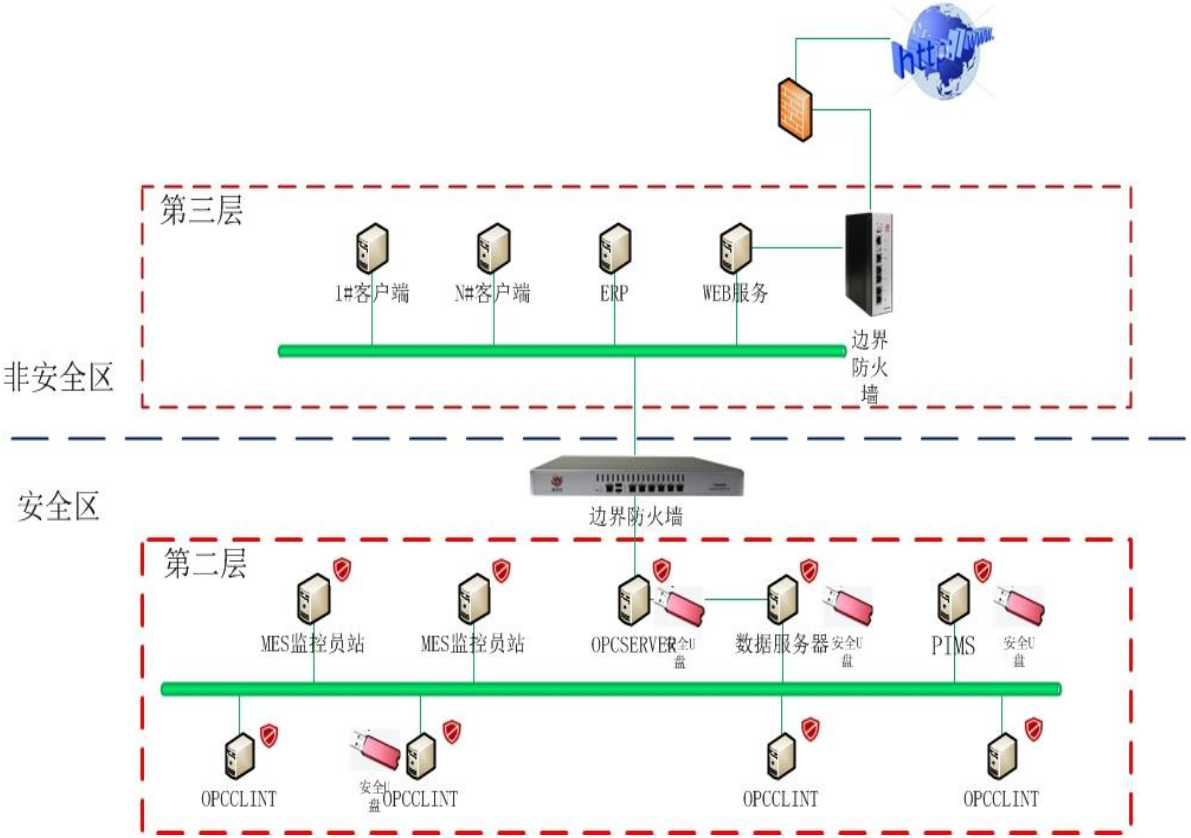
边界防护

1、安全分区：建立功能分区，划分安全区与非安全区

2、边界访问控制：工业边界防火墙通过对工业专有协议的深度解析，智能学习工控操作指令和参数建立网络和通讯“白环境”，阻止来自3、2、等层之间的越权访问，病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行。

3、纵向边界深度攻击防护：工业通信协议白名单，通信关系模型；

4. 可以解决：非授权访问；蠕虫病毒网络间扫描、传播；工业病毒针对DCS的定向攻击（利用漏洞，协议）



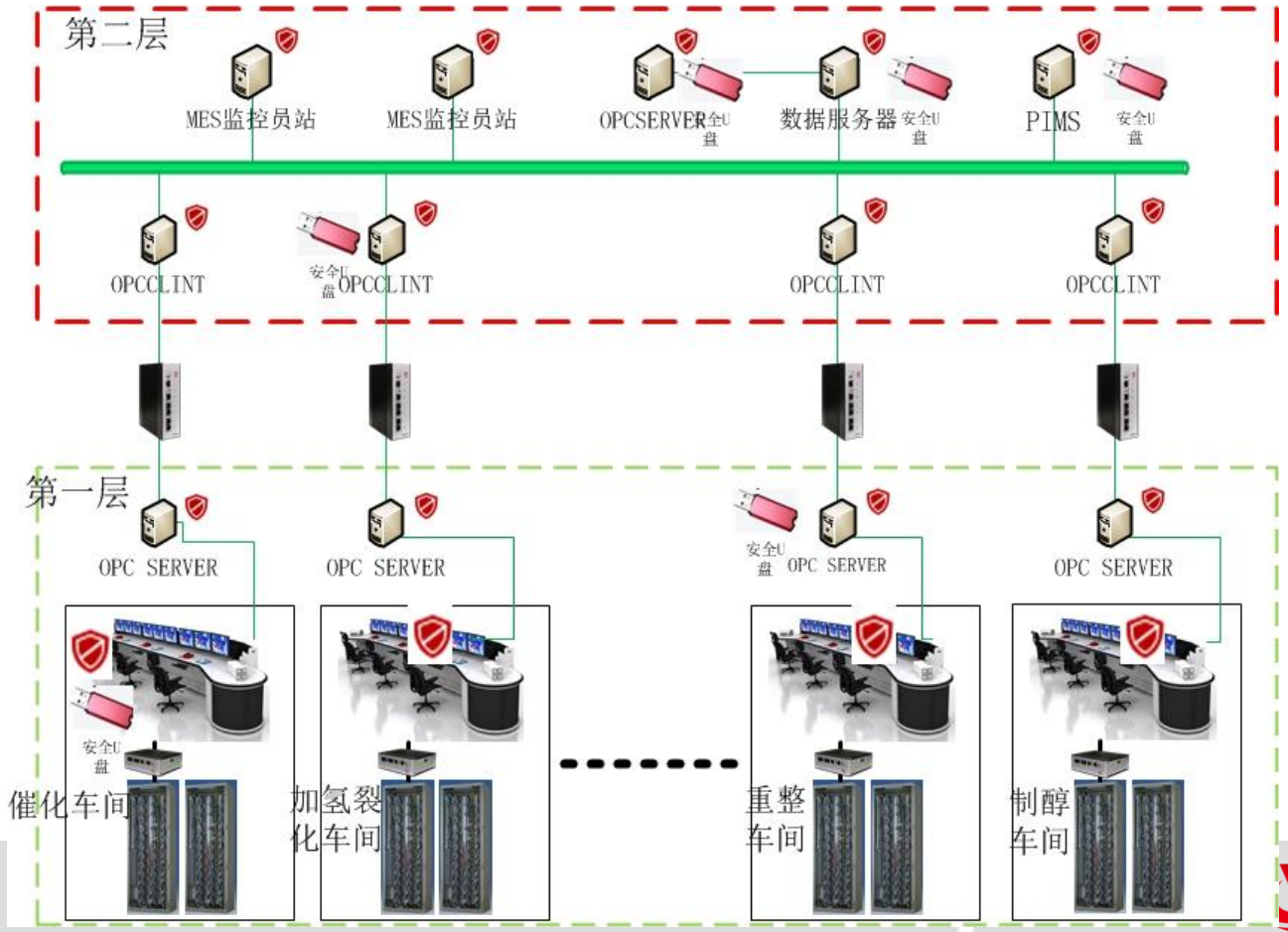
区域防护

1、区域划分：控制系统复杂多样，但依据生产车间或装置可进行功能分区

2、区域访问控制；工业防火墙通过对工业专有协议的深度解析，智能学习工控操作指令和参数建立网络和通讯“白环境”，阻止来自区域之间的越权访问，病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行。实现横向逻辑隔离，将危险源控制在有限范围内。

3.工业协议的安全检查。

3.机架式防火墙适于工业机柜内安装，硬件设计符合工业环境。



主机应用白名单防护

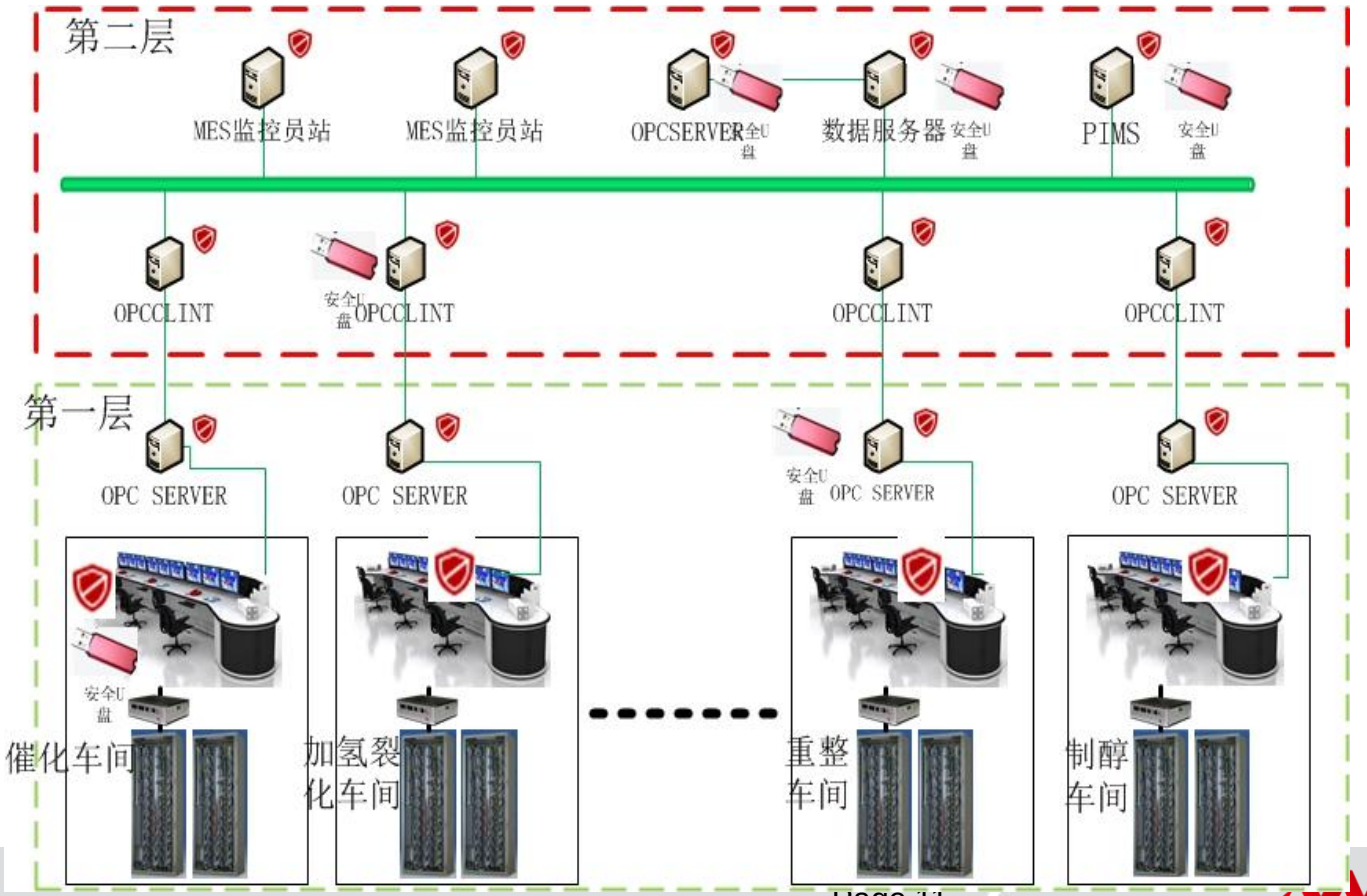
1、学习建立系统软件和工业软件白名单基线

2. 主机加固：通用操作系统完整性；注册表文件；配置文件；专用工程软件

3. 阻止恶意软件执行

4. 避免人员未授权随意安装软件

5. 管理U盘的使用： 安全U盘，和普通U盘的读写控制



实时监测

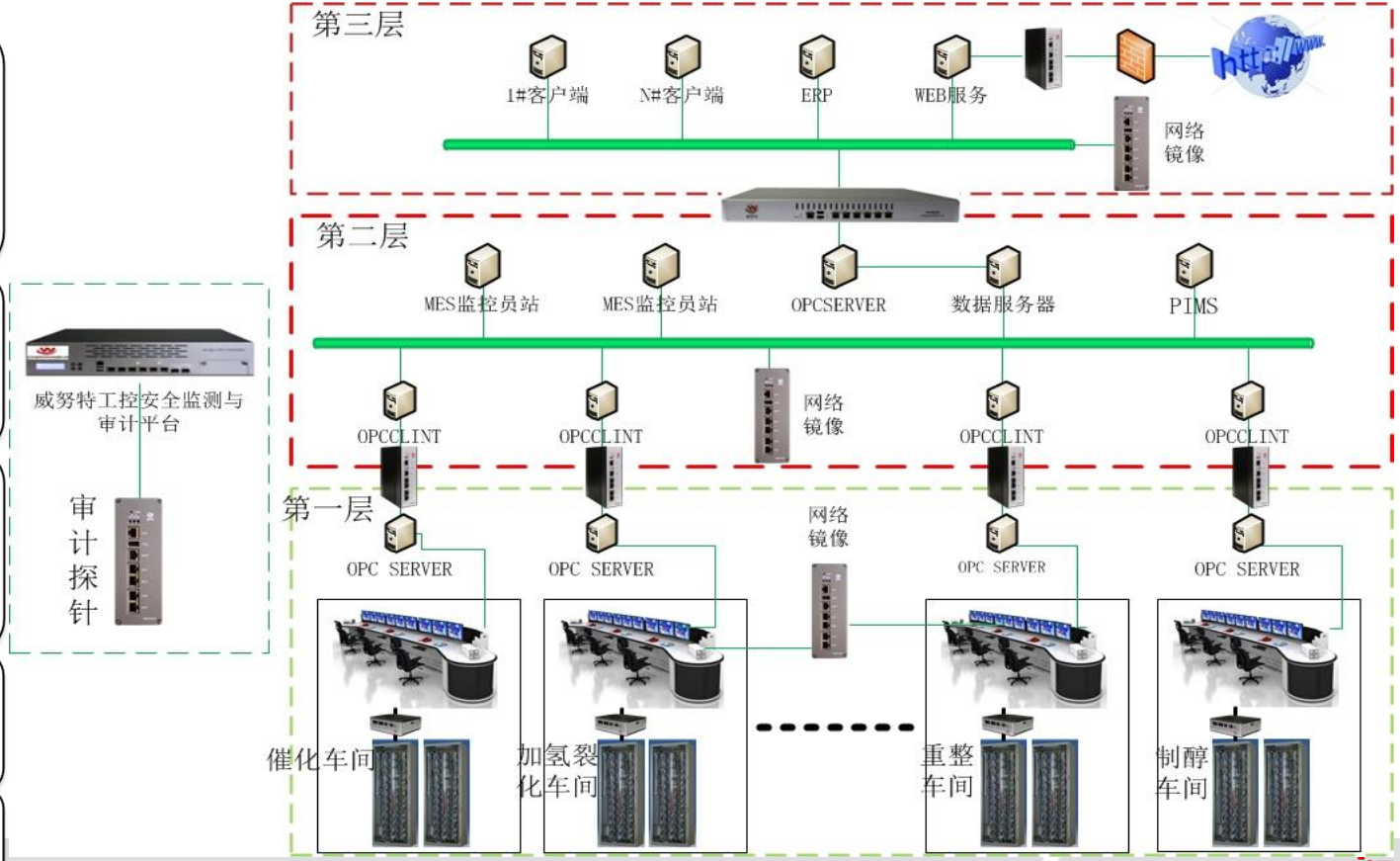
1、网络异常检测：忠实记录工控协议通信记录，自学习建立正常通信行为基线模型，对偏离基线异常操作行为进行告警上报；

2、网络攻击检测：识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测；

3、关键事件检测：例对工程师站组态并更、操控指令变更、PLC程序下装以及负载变更等关键事件告警：

4、工业网络可视化：提供多维度网络流量视图，统计视图；

5、为售后服务、运维服务提供指导



统一管理

1、集中管理安全设备：如工业防火墙、可信卫士、工控安全检测与审计系统，实现工控网络的拓扑管理、安全配置及安全策略管理、设备状态监控、告警日志等。

2、全局安全防护管理；

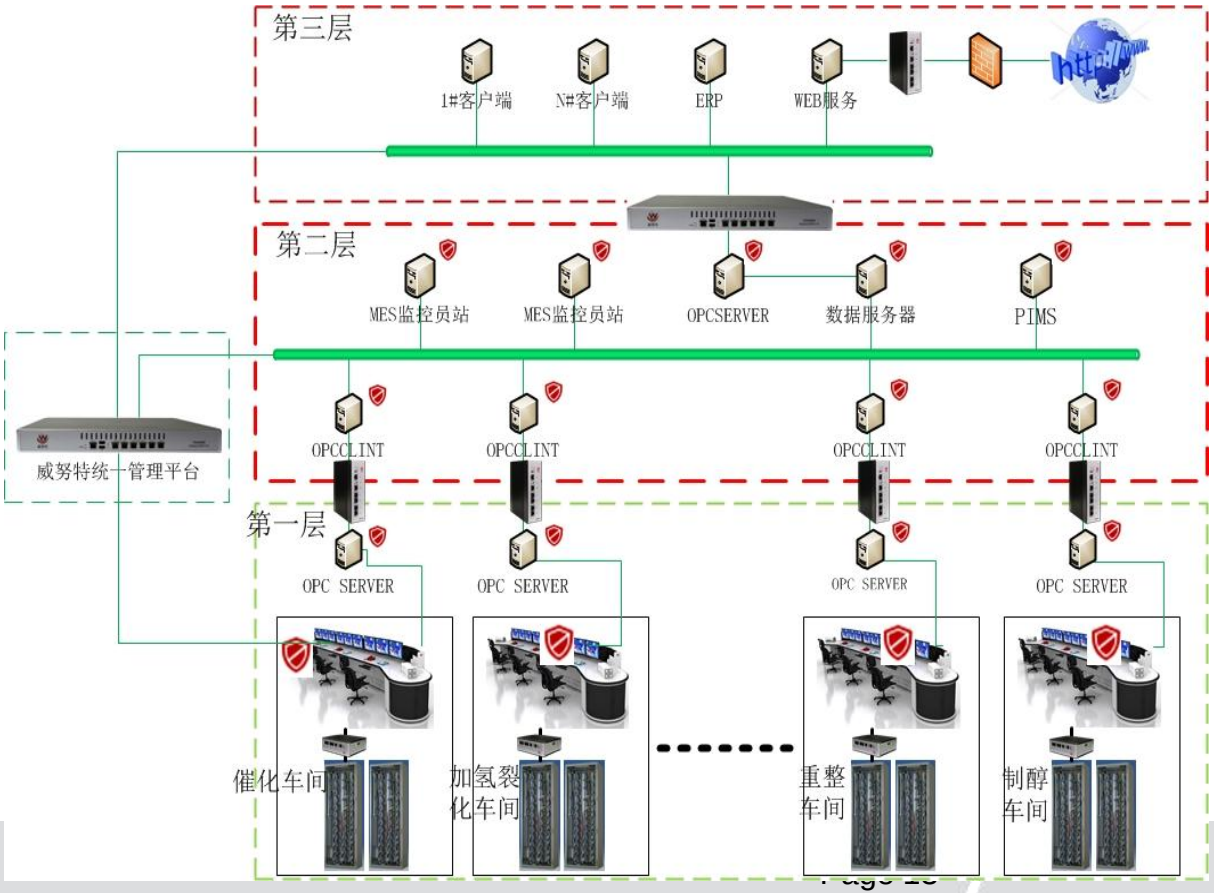
3、全网异常攻击检测和审计；

4、统一主机安全管理；

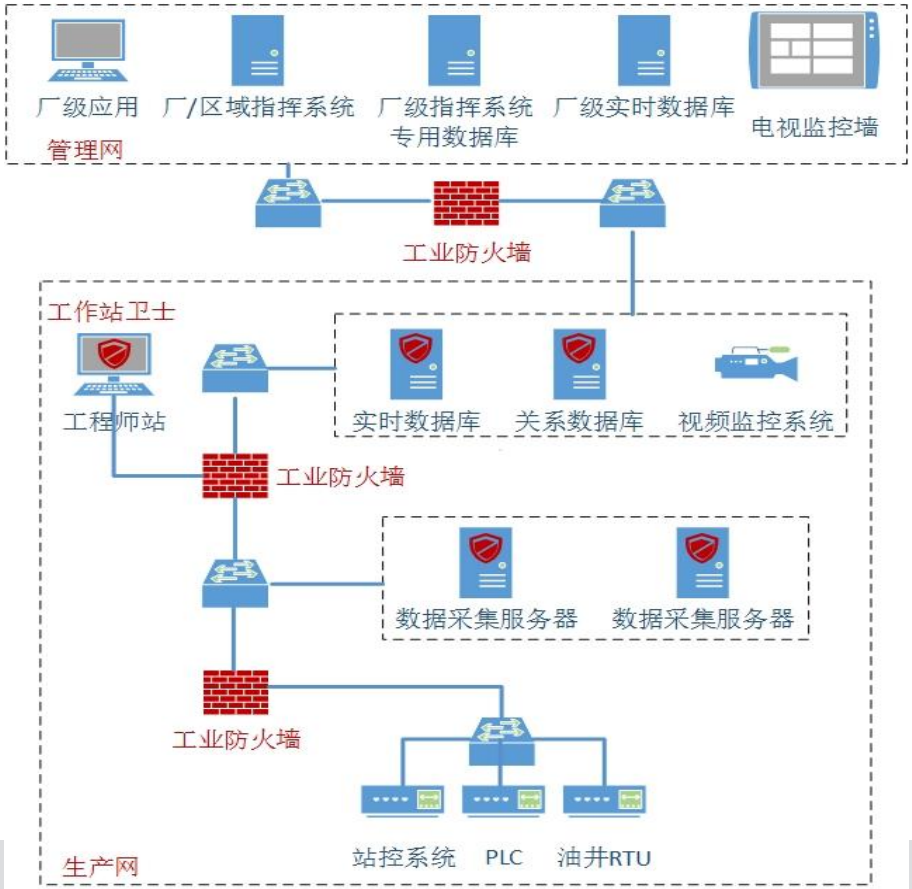
5、集中的安全日志审计；

6、工作站终端异常实时报警；

7、分级分权限管理；



行业案例—新疆XX油田



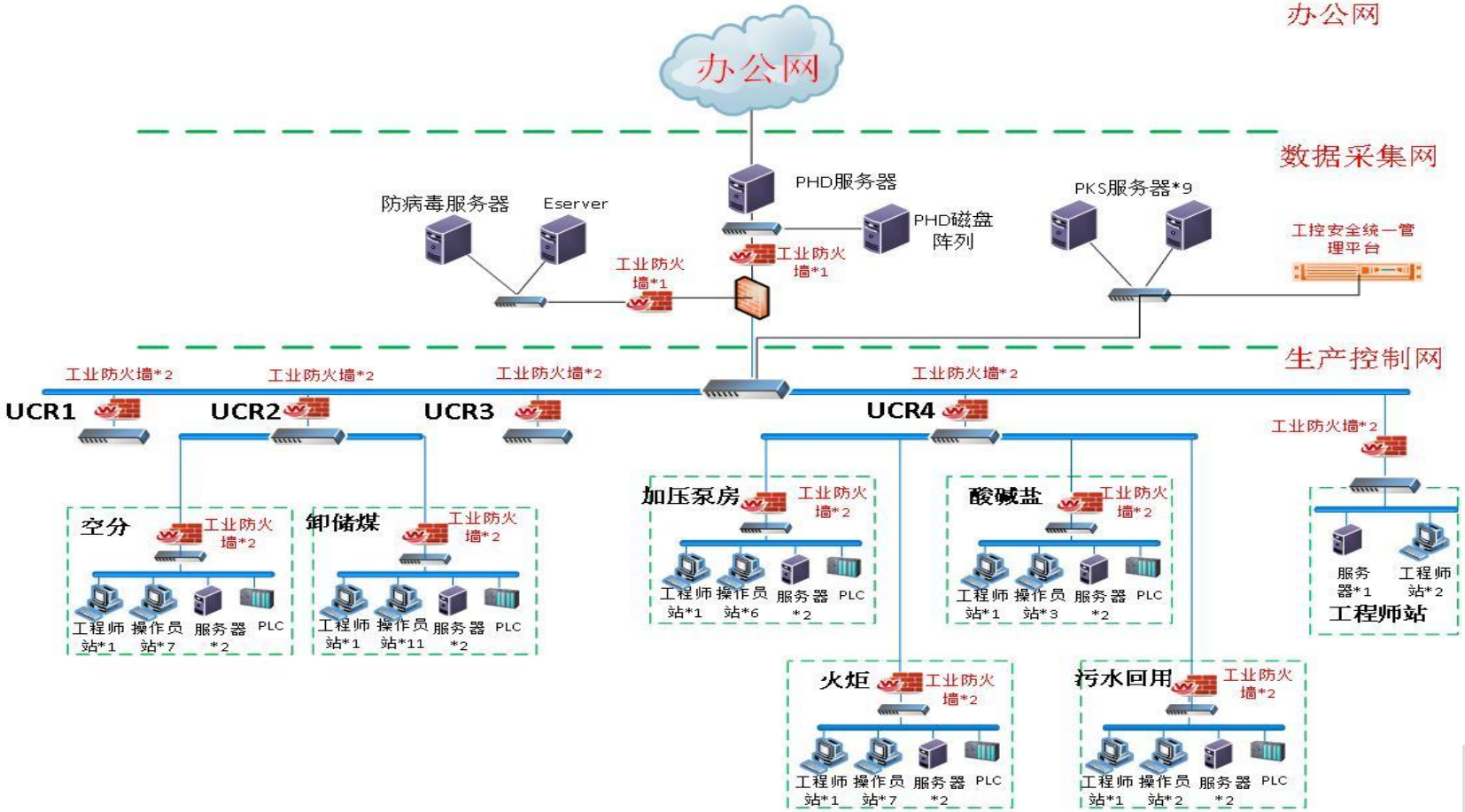
客户价值

✓工作站可信卫士保护工作站免受病毒侵袭

✓可信边界网关进行数采协议OPC的只读防护；

✓可信区域网关进行各采油井之间的网络隔离，访问控制以及专用工控协议的控制；

行业案例—陕西XX煤化工



工控安全 迫在眉睫！