市政水务

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

市政水务是事关民生的重要公共服务设施，水务设施已广泛应用自动化系统，实现水处理过程各个环节的监测与控制。当前市政水务设施大量使用西门子、施耐德等国外软硬件系统，漏洞多，缺乏防护手段。在安全建设中，应依托等保2.0“一个中心，三重防护”的防御思路，结合水务公司的实际需求，通过分期分步建设，构建安全运维体系，完善积极防御与闭环管理能力，全方位保障水务集团网络安全。

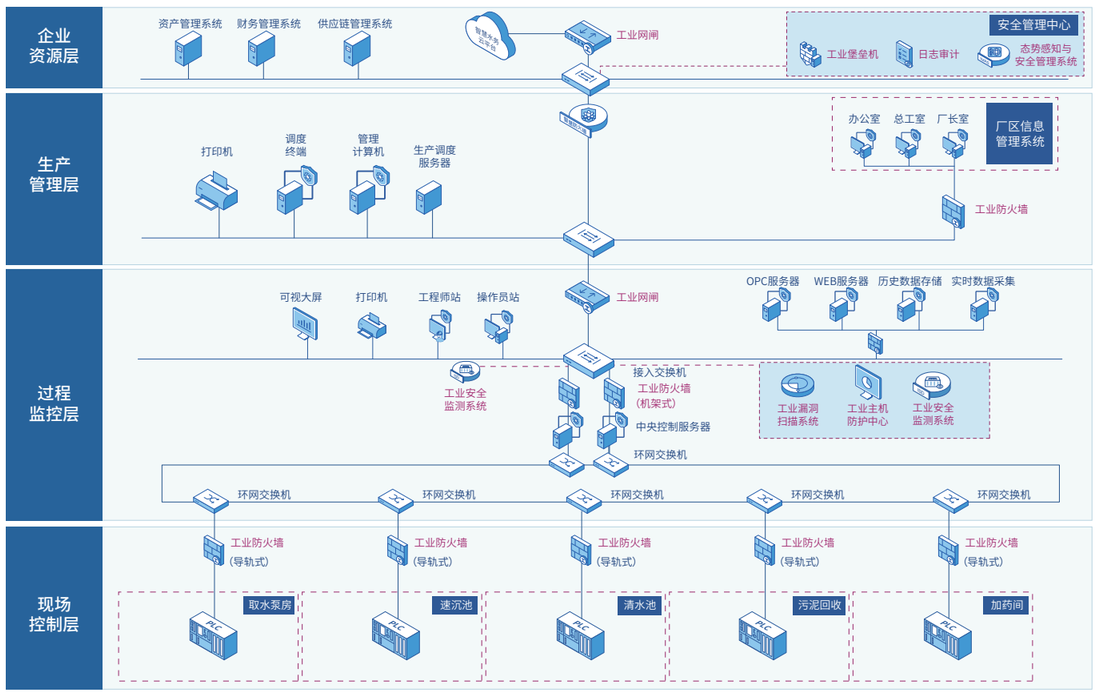
解决方案 SOLUTION

生产网边界隔离防护：水厂生产网与办公网的边界部署工业网闸，通过访问控制、协议转换、内容过滤和信息交换等功能，实现单向数据隔离。在生产网内部，中控室和工控环网之间，中心机房重点业务服务器到核心交换机之间，各个工艺段（粗格栅、生化池等）之间部署工业防火墙，实现区域间的逻辑隔离和访问控制，保障区域边界安全及数据安全。

工业主机安全加固：在中控室、现场阀室的工程师站、操作员站、各个工控业务服务器安装白名单防护软件，通过对应用程序白名单管理，对USB等外设统一管控，有效抵御病毒木马、恶意软件以及非法入侵，保障业务安全稳定。

关键流量节点审计：部署工业安全管理与态势感知系统，通过收集生产网内流量、日志等安全数据，结合威胁情报数据，基于关联分析引擎、异常行为分析模型，从工控资产、资产漏洞、网络威胁、操作行为等多个维度进行大数据分析，以组态化的形式将工业网络的安全态势进行可视化大屏呈现，对网络威胁及时进行应急响应，为企业安全建设升级优化提供实践依据。

建设安全管理中心：集团及水务公司侧划分专门区域建立安全管理中心，部署工业安全态势感知与管理平台，进行设备集中管控及安全态势展示；部署工业堡垒机，提供单点登陆位置；部署工业日志审计，实现网内各类系统的日志、事件、告警统一收集与监控。



成功案例 SUCCESSFUL CASE

- 北控水务集团
- 上海白龙港污水处理厂
- 苏州水务集团
- 深圳水务集团

燃气输配

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

燃气输配系统是城市的重要基础设施，普遍采用SCADA系统实现燃气场站数据的实时采集与设备的远程控制。目前燃气输配SCADA系统普遍采用Modbus TCP/OPC等低安全度的标准协议，并逐渐采用通用操作系统、数据库，这种设计在带来便利的同时也增加了安全风险。2021年 Colonial Pipeline 遭受名为“DarkSide”攻击团伙勒索攻击之后被迫关闭，为全世界燃气行业敲响了警钟。

解决方案 SOLUTION

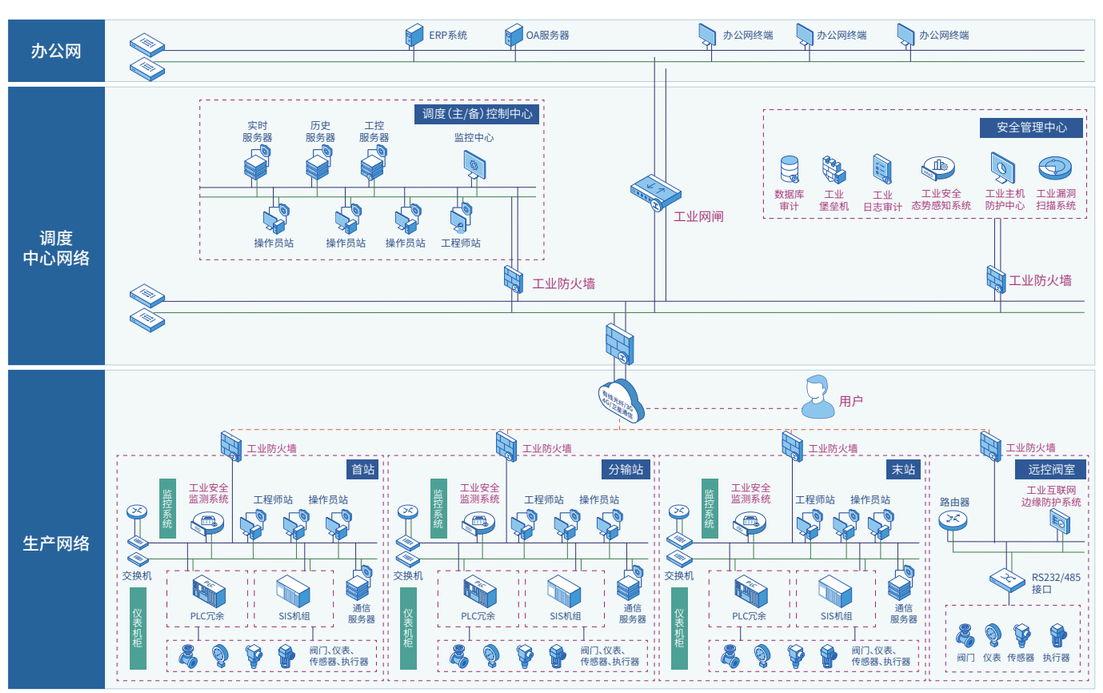
强化边界访问控制：在首末站、分输站以及远控制阀室的出口位置、进入调度中心和安全管理中心的边界位置部署工业防火墙，实现区域间的逻辑隔离和访问控制，保障区域边界安全及数据安全。

工业主机安全加固：在现场的工程师站、操作员站、各个工控业务服务器安装白名单防护软件，防止病毒、木马对主机的感染，保障各系统内工业主机安全。

审计追溯日志留存：在各个站点的核心交换机旁路部署工业安全监测审计，实现资产识别、威胁分析及漏洞检测，同时可作为安全管理中心侧主要探针，为态势感平台提供网络环境安全信息。

网络边缘准入控制：在无人职守的远控阀室部署工业边缘安全可信防护系统，通过资产发现、身份认证、准入控制，异常处置等功能，保障边缘网络接入安全。

建设安全管理中心：在调度中心或燃气公司专门建立安全管理中心区，部署工业安全态势感知与管理平台，实现设备集中管控及安全态势展示；部署工业堡垒机，提供统一身份认证接口，对资产及账号等进行集中化运维管控；部署工业漏扫，实现实时在线漏洞扫描；部署工业日志审计，实现网内各类系统、数据库的日志、事件、告警统一收集与监控。



成功案例 SUCCESSFUL CASE

- 重庆燃气集团
- 珠海燃气集团
- 新疆燃气集团
- 合肥燃气集团