案例1

北京威努特技术有限公司

主标题：某水库自动化系统信息安全体系建设实践

副标题：基于工业控制系统白环境理念的纵深防御安全防护建设

引言：面对越来越严峻的信息安全形势，我国高度重视工业控制系统信息安全工作。随着 2017 年《国家网络安全法》颁布和 2021 年《关键信息基础设施安全保护条例》实施，其中明确提出“关键信息基础设施的运行安全”要在等级保护制度基础上，实行重点防护，而关键信息基础设施规定了水利等重要行业和领域的重要网络设施、信息系统等，说明工业控制系统安全在关键信息基础设施保障中的重要程度。

某水库工控系统建设较早，现有网络系统缺乏网络安全防护能力，存在较大的网络安全风险，不能满足政策法规技术要求，本项目结合生产控制系统的安全现状，帮助用户建立纵深防御防护体系，完善管理制度，强化网络安全技术保障能力，提高用户网络安全综合防护能力，确保水库工控网络系统能安全稳定运行。

一、项目概况

1. 项目背景

（1）城市运营保障责任重大

某水库是我国目前（2012 年）最大的江心水库，设计有效库容为 4.35 亿立方米。日供水规模 719 万立方米，占全市原水供应总规模的 50%以上，是重要的饮用水源地之一，承担着全市过半人口用水。

（2）工控整体安全形势不容乐观

工业控制系统越来越多地采用信息技术和通信技术，水库工控系统建设较早，前期工控系统整体网络设计只考虑了数据传输的稳定性和可靠性，未充分考虑安全防护能力；随着工业化和信息化的深度融合，，传统信息网络所面临的病毒、网络攻击等安全威胁也正在向工业控制系统扩散，工业控制系统面临着日益严峻的安全风险。例如，2015 年，河北省某污水处理厂 PLC 设备存在绕过权限修改寄存器值的漏洞，导致鼓风机设备不受操作员站控制，自行频繁启停，造成鼓风机全部烧毁；2016 年，河北省石家庄市某地表水厂受到恶意攻击，设置送水泵以最大频率运行，与此同时强制关闭泵后阀门，导致送水管道崩裂。

（3）国家法律政策驱动

面对越来越严峻的信息安全形势，我国高度重视工业控制系统信息安全工作。2016 年 10 月 17 日，工信部信软〔2016〕338 号《工业控制系统信息安全防护指南》正式颁布，指出工业控制系统应用企业应从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任十一个方面做好工控安全防护工作，切实提升工业控制系统信息安全防护水平，保障工业控制系统安全。2017 年 6 月 1 日起《中华人民共和国网络安全法》正式施行，其中明确提出“基础设施的运行安全”，要在等级保护的基础上实行重点防护。2021 年 9 月 1 日起《关键信息基础设施安全保护条例》正式实施，明确规定了关键信息基础设施包括水利等重要行业和领域的重要网络设施、信息系统等。

由于我国工业控制系统起步较晚，信息安全保障能力方面存在较大不足。面对复杂的工控安全形势，我国加强工业控制系统信息安全的保障工作迫在眉捷。

2. 项目简介

某水库整体工控系统涉及取水泵闸、下游水闸、输水泵站、输水闸井及控制中心等几个子系统，且由于水库工控系统建设较早，前期工控系统整体网络设计只考虑了数据传输的稳定性和可靠性，但工控网缺乏安全防护能力，一旦网络内某个子系统遭受攻击，很容易影响整个工控系统的正常运行，将会给自身以及城市的安全运营带来严重的影响。

同时，该水库现有工控系统不满足《中华人民共和国网络安全法》和 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》相关技术要求，需要对其整改建设，并通过三级等保测评。

3. 项目目标

通过对某水库进行调研和分析，并结合现有系统安全现状，存在的安全风险以及面临威胁，按照国家、行业相关标准，使之符合网络安全等级保护 2.0 要求，设计出基于工业控制系统白环境理念的纵深防御安全防护方案，建立起完善的技术防护体系，并在此基础上构建合规的管理制度体系，从而提高整某水库的整体综合防护能力。此次建设目标具体如下：

（1）以改造某水库生产控制系统网络为基础，帮助用户建设纵深防护防御体系，提高用户生产网安全防护能力，避免用户生产网遭受到网络入侵等攻击行为而给用户造成巨大经济损失。

（2）结合用户现有管理制度，以 GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》为基准；协助用户建立完善的管理制度流程，从而完善用户网络方面管理制度。

（3）开展合规分析工作，整合工信部的《工业控制系统信息安全应用指南》（GB/T 32919-2016）、GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》、《关键信息基础设施安全保护条例》进行合规分析，通过后期培训和材料预准备，使得用户能够在今后的贯标检查过程中，顺利达标。

二、项目实施概况

依据目前某水库生产网络的安全现状，为满足安全防护效果能够满足国家政策法规及各级主管单位的相关要求，具体安全需求如下：

主机安全加固技术需求

现场根据调研，工控机操作系统以 Windows server 2012、Win7 操作系统为主，现场工控主机无任何恶意代码防范措施，USB 外设管控未做任何管控措施，现场存在移动介质内外网滥用等安全问题，极容易遭受 U 盘摆渡攻击，从而造成生产业务的中断。

内外网网络边界防护需求

目前外部边界生产管理层和上级企业资源层之间缺乏外网的边界隔离技术措施，无法对经过的数据流量进行过滤，由一些非法人员可以从上级部门侧入侵到工控网，存在一定的安全隐患。

内网生产管理层与过程控制层之间缺乏有效的防护措施，容易发生针对生产控制网络内的逻辑控制器（PLC）的非法访问及攻击行为。

入侵检测防范及网络审计技术需求

现有工控网络内缺少入侵检测及网络检测审计措施，无法及时发现内网的一些恶意流量攻击，一旦出现内网的恶意网络攻击事件，无法进行发现和回溯。

日志统一存储需求

工控网缺乏日志集中存储技术措施，无法对网络内服务器日志、操作员日志、交换机日志、安全设备日志等进行统一的收集存储，在不满足网络安全法和等级保护制度要求的同时，也无法对工控网的网络运维日志进行有效的大数据分析。

集中管控技术需求

现有工控网缺乏统一管理技术手段，在后续安全运维时，会消耗较多的运维时间，同时缺乏对第三方运维审计管控，存在较大安全隐患。

系统漏洞管理需求

工控网目前缺乏有效的系统漏洞及时发现技术，一旦系统厂商发布高危漏洞，用户没有及时发现或更新，那么黑客人员很容易利用漏洞对工控网的主机或 PLC 发起攻击，一旦攻击成功，那么用户会面临较大的经济损失和企业影响。

1.方案整体概述

（1）方案整体设计

某水库生产控制系统安全建设依据“安全分区、纵深防护、统一监控”的原则进行建设。

“安全分区”：根据生产过程，将生产相关配套工业控制系统按照板块进行安全分区。板块内部再根据不同控制系统进行安全分域。根据划分的安全区、安

全域制定区间、域间防护措施。

“纵深防护”：结合安全区、安全域划分结果，在制定区、域边界防护措施的同时，也要在安全区、安全域内部部署异常行为、恶意代码的检测和防护措施。

“统一监控”：针对各安全区、安全域的防护措施、监测及审计措施建立统一的、分级的监控系统，统一监控业务板块的工业控制系统的安全状况。将各业务板块的工业控制系统安全风险进行集中的展示，以风险等级的方式给出不同工业控制系统的安全风险级别，全面了解并掌握系统动态。

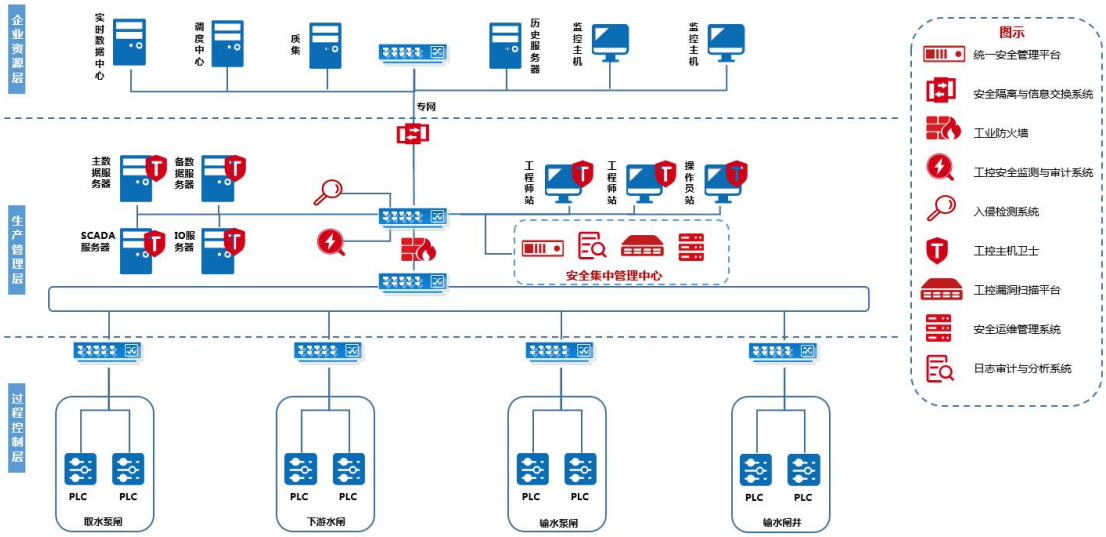

图 1 某水库网络拓扑图

（2）边界安全防护安全设计

在生产管理层到企业资源层之间部署工业网闸，通过工业网闸实现生产管理层和企业资源层的物理隔离，工业网闸分别由内、外网处理单元与数据交换单元（专用隔离芯片）三部分组成。内、外网处理单元是一台专有的网络安全计算机设备，分别连接于内外网络。内、外网处理单元之间通过专用的隔离芯片进行数据的摆渡传输，其过程类似 U 盘拷贝。当专用隔离芯片与内网联通时与外网电路是断开的，当隔离部件与外网联通时，与内网是断开的，在确保网络隔离的前提下实现适度的数据交换，因此能够最大程度的保证某水库生产网的外网边界与企业资源层相互访问通信安全。

在工程师站和 PLC 之间串联部署工业防火墙实现对现场工业控制指令的检测和管控，通过工业防火墙对工业协议深度解析，保护 PLC 免遭工业病毒的恶意攻击，目前某水库生产网系统工业协议采用的是 CIP、S7 等工业协议，工业

防火墙能够对现场应用层 CIP、S7 等工业协议进行深度解析，发现上位机对 PLC 下发的指令不符合白名单的安全测量时，防火墙及时的对数据进行拦截并告警，从而及时有效的避免中间人和一些不法人员的入侵攻击行为。

（3）网络安全审计安全设计

在某水库生产系统网络中通过交换机的端口镜像功能旁路部署安装工控安全监测与审计系统，对工控网络中的控制系统进行审计，以保证触发审计系统的事件存储在审计系统内，能够根据存储的记录和操作者的权限进行查询、统计、管理、维护等操作，能够在必要时从记录中抽取所需要的资料。工控安全监测与审计系统的部署为控制系统网络提供事前监控、事中记录、事后审计。

1) 工控安全监测与审计系统能够解决以下问题：

- 基于正常通信模型，对工控指令攻击、控制参数的篡改、病毒和蠕虫等恶意代码攻击行为等进行实时监测和告警。
- 实时监测设备流量，当发现其在一段时间内没有收发流量，则进行实时报警。
- 实现对工控协议报文不符合其规约规定的格式进行检测并告警。
- 对工程师站组态变更、操控指令变更、PLC 下装、负载变更等操作行为进行记录和存储， 便于安全事件的事后审计。
- 对各类安全日志进行记录和存储，便于安全事件的调查取证。

（4）网络入侵防范安全设计

目前某水库工控网络内部缺乏对异常的攻击检测措施，无法通过技术手段来实现基于攻击检测告警，因此在控制网管理层核心交换机上部署入侵检测设备对工控网络内部的网络攻击进行检测。同时入侵检测也是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。

（5）主机安全加固安全设计

根据某水库生产系统现状，操作员站等主机使用的是微软的 Windows 7 等操作系统，且现场操作系统未做过任何的系统补丁更新，同时这些现场主机需要经常采用 U 盘进行数据拷贝，很容易将外网病毒木马带入工作系统终端上，然后通过终端散播到网络的各个区域，最终致使整体生产网络瘫痪。

此次在某水库服务器和主机上部署工控主机卫士软件，保护这些设备的主机安全。工控主机卫士采用“白名单”管理技术，通过对数据采集和分析，其内置智能学习模块会自动生成工业控制软件正常行为的白名单，与现网中的实时传输数据进行比较、匹配、判断。如果发现其用户节点的行为不符合白名单中的行为特征，其主机安全防护系统将会对此行为进行阻断或告警，以此避免主机网络受到未知漏洞威胁，同时还可以有效的阻止操作人员异常操作带来的危害。

2. 安全集中管理中心建设

（1）安全集中管理中心建设总体设计

在生产管理层核心交换机上搭建一套安全集中管理中心，通过安全集中管理中心对生产网的安全设备、网络设备、安全软件进行集中管理和日志集中存储分析，并通过安全集中管理中心的漏洞扫描设备定期的对生产控制系统的服务器和主机进行漏洞扫描，及时发现工控系统内部的系统漏洞并进行修复。

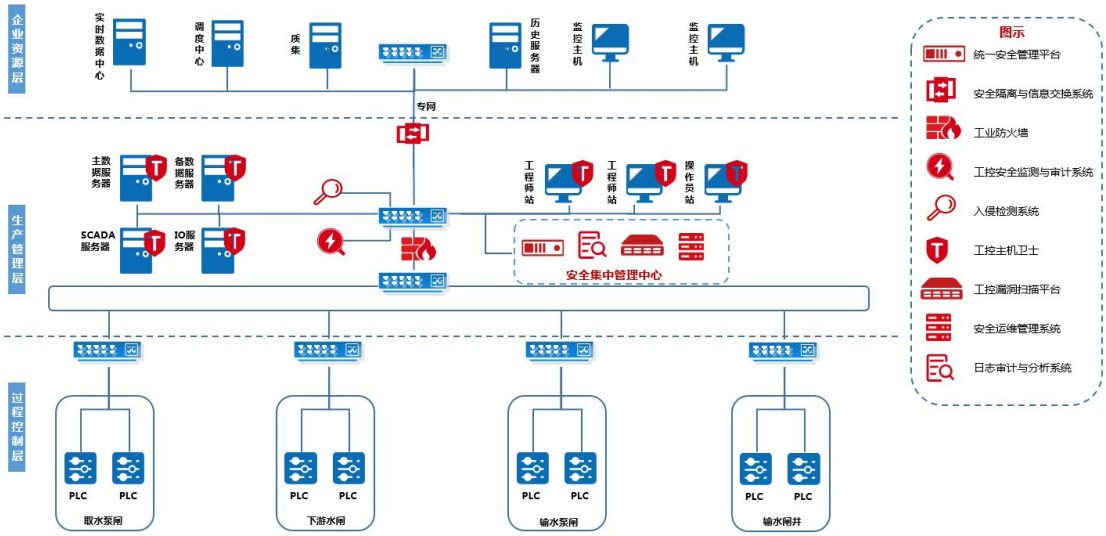

图 2　安全集中管理中心建设拓扑图

（2）日志审计集中存储设计

目前某水库生产网没有统一的日志存储服务器，无法生产网安全设备、服务器、交换机、操作员站等日志进行统一存储，同时《中华人民共和国网络安全法》的出台及信息系统安全等级保护的要求，明确要求对关键信息基础设施和二级以上的信息系统必须对网络、主机和应用进行安全审计。

综上所述，用户需要一个全面的、面向网络资源的、集中的安全日志审计平

台及其系统，这个系统能够收集来自客户网络资源中各种设备和应用的安全日志，并进行存储、监控、审计、分析、报警、响应和报告。

此次在生产网内部安全集中管理中心部署一台日志审计与分析系统实现对安全设备及网络设备的日志存储，以便满足相关法律法规的政策要求。

（3）安全运维审计设计

目前某水库网络当中缺乏安全运维管控，用户无法对生产网的运维进行详细技术管控，因此此次在生产网当中部署一台安全运维堡垒机，对生产网的后期运维进行统一管理，通过堡垒机对不同对象的运维人员下发不同的管理权限，并对管理权限进行划分，其次通过运维堡垒机能够追溯运维人员在运维过程中做的运维操作，以便在发生安全事件时，能够通过运维堡垒机进行事件追溯。

（4）工控漏洞扫描安全设计

此次在生产当中部署一台漏洞扫描设备，它可以帮助用户管理人员随时掌握当前系统中漏洞情况，通过扫描生产网当中的网络及工控设备从而评估你的网络的安全级别，并生成评估报告，提供相应的整改措施。

（5）统一集中管理平台安全设计

在生产网网设置安全管理区域，在生产网的核心交换机旁路部署统一安全管理平台，方便管理人员的日常管理与维护

3. 具体应用场景和应用模式

通过在某水库的控制中心搭建一套完善的安全集中管理中心实现对取水泵站、下游水闸、输水泵闸、输水闸井的网络会话日志、设备运行日志及设备的告警日志进行集中收集并分析，实时掌握各个子系统的网络安全态势，一旦某个子系统网络出现异常情况，配合安全集中管理中心的统一安全管理平台对安全设备的策略进行动态化的调整，达到对某水库工控系统进行实时监控和精准防护。

4. 安全及可靠性

在许多情况下，设备的不可靠会导致系统的不安全。当设备发生故障时，不仅会影响用户的正常业务运行，而且可能会因设备出现故障而导致安全防护体系失效，从而使系统受到网络攻击，因此此次项目在方案设计时从技术层面和管理

层面入手，来整体提高设备的安全性和可靠性，具体如下：

基于技术层面：首先从技术层面入手，此次需要串联在系统中的设备分别是工业防火墙和工控网闸，其它设备因旁路部署，即使出现故障也不会影响现有的业务正常运行，方案的可靠性和安全性只涉及到串联的安全设备。工业防火墙是串联生产管理层和过程控制层之间，一旦防火墙出现故障会导致水库整个工控系统业务瘫痪，因此本次采用工控专用防火墙来实现管理层和控制层之间的安全防护，工控专用防火墙业务接口具备 Bypass 功能；工业防火墙通过接口的 Bypass 功能保护网络间的应急通讯。保证物理硬件在出现问题时工控网络的正常通讯。

在生产管理层和企业管理层之间部署工业网闸实现某水库和原水公司之间的边界防护，目前某水库只需要把本地的生产数据通过网闸上传到原水公司即可，现场的水泵控制还是由生产管理层实现，因此对现场数据传输的实时性要求不高，同时某水库本地有一台数据服务器来实时的存储生产数据，由数据服务器把数据同步给上级原水公司，一旦网闸设备出现故障，导致某水库和原水公司链路中断，数据服务器会进行本地缓存，当后续链路恢复通信时，数据服务器会把本地缓存的数据同时上传到原水公司，从而提高数据传输的可靠性。

基于管理制度：“三分技术，七分管理”是网络安全领域的一句至理名言，因此现场网络是否能够安全稳定的运行还需要结合安全管理制度，此次在项目完成建设后，协助用户制定完善的安全运维管理制度和安全巡检管理制度，每天由现场工作人员登录到各个设备上查看设备的运行日志和告警日志，并生成巡检报告，一旦发现设备出现故障，及时的启动应急预案，恢复网络，提高设备系统的可靠性。

5. 其他亮点

（1）本方案以主动防护为核心，白名单防护技术为基础，帮助用户建立纵深防御防护体系，提高用户网络安全防护能力，确保水库工控网络系统能安全稳定运行；

（2）根据客户现场管理组织架构，帮助客户完善管理制度，提高企业网络运行的标准化和规范化，从而协助用户实现网络运维管理“一切按照制度办事”的目标；

（3）顺利通过三级等级保护测评，为后续水务集团构建集团级态势感知监测预警平台奠定坚实的基础。

三、下一步实施计划

在原水公司完成多个厂区的工控安全建设后，后续由水务公司牵头，定制研发水务集团级态势感知监测预警平台，首先由每个厂区统一安全管理平台把安全设备的运行状态，对安全事件、资产脆弱性、安全规则配置、设备可用性与安全相关的数据进行统一采集、集中分析，发现事件或安全风险时可实时触发告警。后续由统一安全管理平台把相关的数据发送到集团级态势感知监测平台实现联动，从而实现对整体水务工控系统安全设备的集中管控和展示。

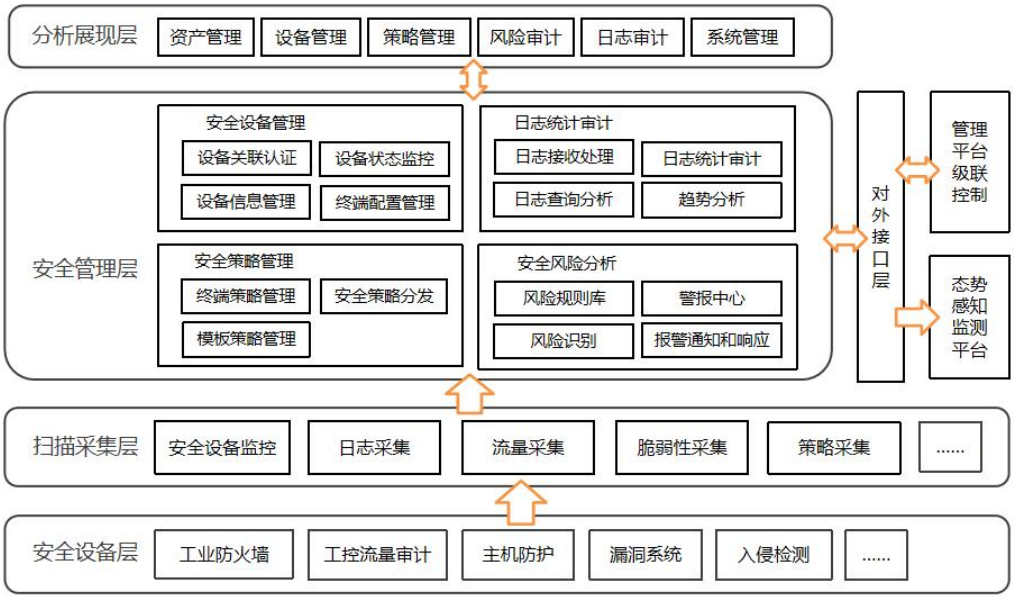

图 3　安全集中管理中心建设拓扑图

四、项目创新点和实施效果

1. 项目先进性及创新点

本次基于工业白环境理念的纵深防御安全防护建设项目涉及多处原创性、创新性技术应用两点，总结归纳为如下：

（1）基于软件服务器的进程白名单更新技术

通过软件服务器的进程白名单更新技术，在企业部署环境中只需要更新软件服务器计算机上的进程白名单列表便能使全网相同操作系统的电脑都能共享这一更新的白名单，从而不需再对每台计算机进行重复操作，有效减少安全运维工作量，更有益于积累全网软件的白名单库。

（2）一种基于工业网络异常中断的检测方法

通过创新的采用技术检测手段，以达到针对工业网络中的异常网络中断情况进行告警，及时提醒用户进行应急管理。

（3）一种工控网络文件强制访问控制策略配置的方法

采用针对工控网络文件特别设计的强制访问控制技术，以实现在特殊环境下具备针对相关文件的访问策略的控制和配置，以达到合规要求。

（4）一种工控协议解码规则的表述及优化解码方法

用于在工业场景下针对不同的工控协议数据流进行解码和识别，该方法设计优化了其解码的方法，提高效率和准确率。

2. 实施效果

（1）本方案以主动防护为核心，白名单防护技术为基础，帮助用户建立纵深防御防护体系，提高用户网络安全防护能力，确保水库工控网络系统能安全稳定运行；

（2）根据客户现场管理组织架构，帮助客户完善管理制度，提高企业网络运行的标准化和规范化，从而协助用户实现网络运维管理“一切按照制度办事”的目标；

（3）顺利通过三级等级保护测评，为后续水务集团构建集团级态势感知监测预警平台奠定坚实的基础。