DOI:10.20040/j.cnki.1000-7709.2023.20222657

抽水蓄能电站计算机监控系统可信应用研究

蔡 杰[1],吴正义[1],张 鑫[2],赵毅锋[3],李小鹏[4],刘梦初[1]

(1. 南瑞集团(国网电力科学研究院)有限公司,江苏 南京 211106;2. 国网新源控股有限公司,北京 100052; 3. 国网新源控股有限公司抽水蓄能技术经济研究院,北京 100053; 4. 国网四川省电力公司电力科学研究院,四川 成都 610041)

摘要:针对近年来网络安全形势日益严峻、新型攻击手段不断涌现的问题,分析抽水蓄能电站计算机监控系统应用的可信计算功能需求,以可信硬件平台与操作系统为基础,提出抽蓄电站计算机监控系统可信应用体系架构,并讨论了可信分布式服务、业务行为可信分析等关键技术。结果表明,该设计实现了计算机监控系统的应用可信,为抽水蓄能电站控制系统提供了有效的主动防御机制,适应未来抽水蓄能电站监控业务的发展。

关键词:抽水蓄能电站;监控系统;分布式应用;可信计算

中图分类号:TV743;TM76 **文献标志码**:A **文章编号**:1000-7709(2023)10-0220-04

1 引言

1980年代起,我国抽水蓄能电站(简称抽蓄电站)逐渐进入建设高峰,建成一批总装机容量超过1 000 MW的大型抽水蓄能电站[1]。伴随近年来网络技术的发展,黑客入侵手段不断变化,传统被动防御策略疲于应对,抽蓄电站的网络安全风险日益加剧,亟需建立主动防御机制,在不影响系统实时性的前提下,降低电站运行管理过程中的安全风险[2]。在电网调度方面,我国科研人员应用了基于可信根的计算机系统与操作系统[3];在配电网方面,研究了主站与终端通信的机密性与完整性技术[4];在电力物联网方面,提出了软件行为评估方法[5];在现地控制技术方面,构建了可信PLC控制系统[6]。这些研究主要聚焦于计算机、操作系统、现地设备及采集通讯的可信计算技术,对于分布式应用可信计算研究较少。由于可信的基本理论要求从可信根开始逐级建立信任链,最终推广到整个系统,加之抽蓄电站监控系统普遍采用分布式架构[7],因此实现抽蓄电站计算机监控系统的整体可信,必须实现可信的分布式应用。本文以可信硬件与操作系统为基础,分析了抽蓄电站计算机监控系统可信应用的功能需求,提出监控系统可信应用体系架构,建立满足抽蓄电站运行管理要求的可信分布式服务与应用,为抽蓄电站控制系统提供有效的主动防御机制,满足系统在安全性、可靠性与实时性等方面的要求。

2 体系架构

2.1 需求分析

抽蓄电站计算机监控系统采用分布式架构,以实时数据总线、控制数据总线、历史数据总线为基础,通过不同应用节点中部署的功能与服务,实现电站各类生产设备的实时数据采集、信息交互与自动控制功能[8],见图1。

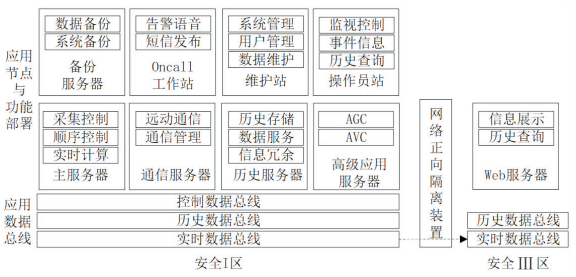

图1 监控系统功能与数据架构

Fig. 1 Functional and data architecture of SCADA

应充分考虑抽蓄电站运行管理要求与分布式应用特点,采取技术手段提升应用的主动防御能力,同时确保系统的稳定性、可靠性与实时性,其核心需求在于:①可认证性。应具备人员与节点

收稿日期:2022-12-29,**修回日期**:2023-01-11

基金项目:国家电网有限公司科技项目(5419-202243074A-1-1-ZN)

作者简介:蔡杰(1983-),男,高级工程师,研究方向为水电厂及新能源控制系统自动化、实时数据库、历史数据库、网络通信、模型管理、数据分析与挖掘,E-mail:caijie@sgepri.sgcc.com.cn

的身份鉴别能力,避免非法登录与操作,识别非法节点访问并拒绝其连接;②机密性。分布式节点间信息通信应具备机密性,避免关键信息泄露,增加通信报文伪造难度;③完整性。确保通信报文与应用程序的完整性,避免恶意植入等手段影响系统运行;④有效性。结合抽蓄电站运行管理要求,建立行为分析机制,拒绝非正常的控制要求并记录日志;⑤实时性。避免对监控系统的正常运行造成影响,确保实时数据与控制命令的实时性;⑥可用性。在系统发生局部故障的情况下保持系统功能的正常运行。

2.2　可信应用体系架构

以可信硬件与操作系统为基础,采用节点认证、加密通信等技术,建立抽蓄电站监控系统可信应用功能架构,主要分为如下层次(图 2):①硬件层。实现可信硬件支撑,建立可信根。②系统层。驱动可信硬件,实现基础系统软件支撑,将信任扩大到操作系统。③应用层。采用满足可信要求的实时数据总线、历史数据总线与控制数据总线,建立可信分布式服务,实现分布式节点间的可信网络通信;以可信分布式服务为基础,建立可信分布式应用,将信任扩展到整个监控系统。

图 2　监控系统可信计算体系架构

Fig. 2　Architecture of trusted distributed application in SCADA

3　关键技术

3.1　可信分布式服务

由于监控系统不存在动态接入需求,采用管理员人工分发密钥方式,减少非必要的操作环节。采用国产 SM2 加密算法,利用每个分布式节点的可信模块生成公钥与私钥。私钥存储在可信模块内,公钥由管理员汇总后根据需要分发到其他节点,加密存储在受保护空间内防止窃取与篡改。

3.1.1　历史数据与控制数据总线

历史数据与控制数据总线基于 TCP 协议实现,支持冗余网络设计。客户端发起并建立连接后,采用 f_{SM2PIK} 算法利用私钥对本地存储的可信度量信息与摘要进行签名:

$$S_{\mathrm{ClientPCR}} = f_{\mathrm{SM2PIK}}(E_{\mathrm{ClientPCR}}) \tag{1}$$

$$S_{\mathrm{M}} = f_{\mathrm{SM2PIK}}(D_{\mathrm{M}}) \tag{2}$$

式中,$S_{\mathrm{ClientPCR}}$ 为加密的可信度量信息;$E_{\mathrm{ClientPCR}}$ 为客户端节点可信度量信息;S_{M} 为加密后摘要;D_{M} 为信息摘要。

客户端将 $S_{\mathrm{ClientPCR}}$ 与 S_{M} 同时发送至服务端,服务端采用 f_{SM2Pub} 算法利用客户端公钥进行验签:

$$E'_{\mathrm{ClientPCR}} = f_{\mathrm{SM2Pub}}(S_{\mathrm{ClientPCR}}) \tag{3}$$

$$D'_{\mathrm{M}} = f_{\mathrm{SM2Pub}}(S_{\mathrm{M}}) \tag{4}$$

式中,$E'_{\mathrm{ClientPCR}}$、D'_{M} 分别为服务端解密后的可信度量信息、摘要信息。

此时服务端应用需对客户端进行节点可信检查。首先对 $E'_{\mathrm{ClientPCR}}$ 进行摘要计算,将结果与 D'_{M} 对比。其次检查 $E'_{\mathrm{ClientPCR}}$ 确认客户端可信度量满足可信条件。最后检查该客户端是否存在于访问白名单中。这些条件满足,说明完成客户端的身份认证与可信检查,否则返回错误断开连接。在分布式应用中信任是双向的,客户端也需对服务端身份进行认证。随后进入业务数据交互阶段,客户端使用 f_{merg} 函数合并命令与可信度量信息,并对结果进行摘要与加密:

$$D_{\mathrm{ClientMessage}} = f_{\mathrm{merg}}(E_{\mathrm{ClientPCR}}, D_{\mathrm{ClientCMD}}) \tag{5}$$

$$S_{\mathrm{ClientMessage}} = f_{\mathrm{SM2PIK}}(D_{\mathrm{ClientMessage}}) \tag{6}$$

$$S_{\mathrm{M}} = f_{\mathrm{SM2PIK}}(D_{\mathrm{M}}) \tag{7}$$

式中,$D_{\mathrm{ClientCMD}}$ 为原始控制信息;$D_{\mathrm{ClientMessage}}$ 为 $E_{\mathrm{ClientPCR}}$ 与 $D_{\mathrm{ClientCMD}}$ 合并后的信息内容;$S_{\mathrm{ClientMessage}}$ 为加密后报文;S_{M} 为加密后摘要;D_{M} 为 $D_{\mathrm{ClientMessage}}$ 信息摘要。

客户端将 $S_{\mathrm{ClientMessage}}$ 与 S_{M} 同时发送至服务端,服务端使用客户端公钥进行解密:

$$D'_{\mathrm{ClientMessage}} = f_{\mathrm{SM2Pub}}(S_{\mathrm{ClientMessage}}) \tag{8}$$

$$D'_{\mathrm{M}} = f_{\mathrm{SM2Pub}}(S_{\mathrm{M}}) \tag{9}$$

式中,$D'_{\mathrm{ClientMessage}}$ 为服务端解密后的信息;D'_{M} 为解密后的摘要。

服务端对 $D'_{\mathrm{ClientMessage}}$ 进行摘要计算,并将结果与 D'_{M} 对比,验证信息完整性。随后使用拆分函数 f_{unmerg} 获取 $E_{\mathrm{ClientPCR}}$ 与 $D_{\mathrm{ClientCMD}}$,并对客户端可信度量进行检查,确认客户端满足可信条件。检查完成后,服务端执行命令。

图 3 为历史数据与控制数据总线交互过程。

3.1.2　实时数据总线

为实现跨安全区的网络部署架构,实时数据总线采用组播协议实现,支持冗余通道设计。由于使用不可靠连接建立总线,单纯采用节点身份

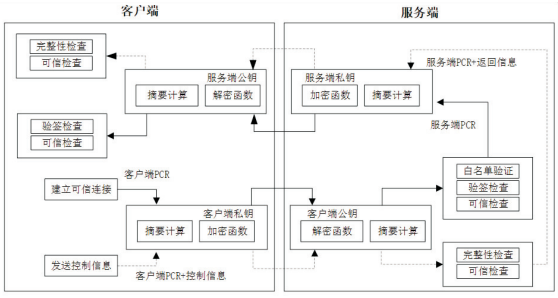

图 3 历史数据与控制数据总线交互过程

Fig. 3 Interaction process of historical data and control data bus

认证机制无法杜绝恶意复制报文并在不恰当时机发送报文、干扰系统数据正确性的行为。需在认证节点身份的同时，对信息实时性进行校验。首先发送端采用 f_{merg} 函数对发送端 PCR 信息、实时数据与时间进行信息合并，使用发送端私钥对其结果进行摘要与加密：

$$D_{\text{Message}} = f_{\text{merg}}(E_{\text{PCR}}, D_{\text{Data}}, D_{\text{Time}}) \tag{10}$$

$$S_{\text{Message}} = f_{\text{SM2PIK}}(D_{\text{Message}}) \tag{11}$$

$$S_{\text{M}} = f_{\text{SM2PIK}}(D_{\text{M}}) \tag{12}$$

式中，E_{PCR} 为发送端 PCR 信息；D_{Data} 为实时数据；D_{Time} 为信息的当前时间；S_{Message} 为加密后的内容；D_{Message} 为合并后的信息内容；S_{M} 为摘要的加密结果；D_{M} 为 D_{Message} 的摘要。

发送端将 S_{Message} 与 S_{M} 同时发送至数据总线。总线上的任意接收节点，根据报文中地址信息判断数据源节点，然后使用该节点公钥对接收的 S_{Message} 与 S_{M} 进行解密：

$$D'_{\text{Message}} = f_{\text{SM2Pub}}(S_{\text{Message}}) \tag{13}$$

$$D'_{\text{M}} = f_{\text{SM2Pub}}(S_{\text{M}}) \tag{14}$$

式中，D'_{Message} 为接收端解密后的信息；D'_{M} 为解密后的摘要。

服务端对 D'_{Message} 进行摘要计算，并将结果与 D'_{M} 对比，认证信息源节点身份，验证信息完整性。随后使用拆分函数 f_{unmerg} 获取 E_{PCR}、D_{Data}、D_{Time}，完成下列检查：①检查数据源可信度量，确认客户端满足可信条件；②检查信息发布时间，与系统当前时间对比，确保信息及时有效；③检查信息源白名单，确认来自有效数据源。检查完成后，接收端更新本地实时库，否则丢弃。

图 4 为实时数据总线交互过程。

3.2 业务行为可信分析

信息化应用的业务行为分析主要聚焦于控制流完整性、信息流行为模型的研究。但在控制系统中，用户更关心系统控制操作的合理性与实时性，需根据抽蓄电站的业务特点建立行为可信分

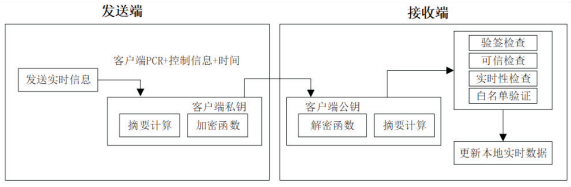

图 4 实时数据总线交互过程

Fig. 4 Interaction process of real data bus

析与闭锁机制，避免因入侵等原因产生的非法设备操作造成人身或财产损失。主要包含如下方面：①设备工况依赖性检查。检查违反必要工况条件的控制行为，如非低转速加闸等；②工况转换规范性检查。抽蓄机组相对常规机组有更多的稳态与暂态工况，各工况间的转换应严格满足可逆式抽水蓄能机组工况转换导则要求，如与发电工况机组使用相同引水管道的机组应闭锁抽水控制令等；③控制信息实时性检查。如果系统中某个控制命令存在较长时间，应标记为可疑操作行为；④调节范围有效性检查。根据设备特性与管理要求，控制调节应限制在一定的步长范围内，如闸门开度调整等。

当控制命令通过检查后应用才能转发，否则应闭锁控制并记录日志。业务行为的分析结果作为分布式应用的可信度量信息，应扩展到节点的 PCR 中，作为节点可信的判断依据。

图 5 为业务行为可信判断流程。

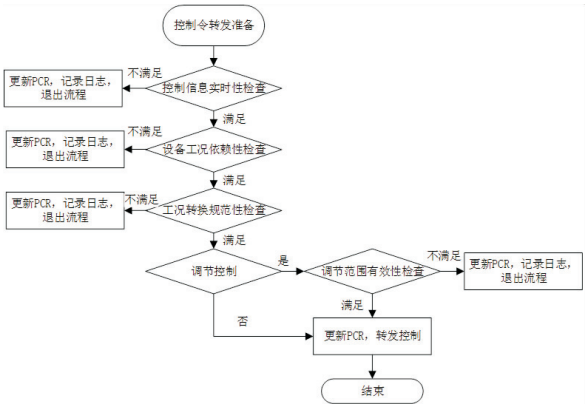

图 5 业务行为可信判断流程

Fig. 5 Process of judgement on trusted behavior

3.3 可信应用支撑环境

除了可信硬件平台与操作系统，仍需采用技术手段，建立可信应用的支撑环境。具体包括：①应用完整性。依托可信操作系统，建立应用程序的校验与加固机制，对应用程序进行数字签名，杜绝应用程序被蓄意破坏或无意更改的情况；②用户真实性。采用多因子身份认证技术，建立完整的用户登录验证机制，避免身份盗用后造成的核心数据泄漏或蓄意破坏行为；③日志有效性。建

立日志审计机制,及时收集和归档日志,确保可信应用运行过程中产生的日志信息安全有效;④系统安全性。建立漏洞扫查机制,提前发现操作系统的不安全因素,从而有针对性地修补缺陷,防范于未然。

4　测试情况

在抽水蓄能电站自主可控设备联合调试环境中搭建洪屏电站模拟环境,针对监控系统可信应用的实时性、稳定性与信息机密性进行测试,结果见表 1。由表 1 可知,采用节点认证与加密传输机制后,分布式应用间信息传递无法通过黑客手段进行窃取、伪造与干扰,信息机密性与完整性得到保障。控制操作受到行为分析功能的约束,确保业务行为的可信、有效。监控系统单点故障不会对系统功能造成影响,确保功能的可用性与稳定性。可信计算对系统正常业务功能无明显影响,满足大型抽水蓄能电站实时数据与控制的性能要求。

表 1　模拟环境测试结果

Tab. 1　Test result in simulated environment

条件	通信机密性	通信完整性	单点故障	控制行为有效性	实时数据发布与接收时长/ms	系统闭环控制周期/s
常规应用	不满足	不保证	不影响运行	不保证	<13	<1
可信应用	满足	保证	不影响运行	保证	<20	<1

5　结论

a. 本文设计并实现的抽蓄电站计算机监控系统可信应用体系架构,实现了高安全、高可靠、高实时的监控系统可信分布式服务与应用,填补了控制系统可信应用领域空白,为抽蓄电站控制系统建立从可信根到可信应用的主动防御体系,有效降低了抽蓄电站运行管理过程中的安全风险,对保障电网安全稳定运行具有重要意义。

b. 该架构经过了严格的安全性、可靠性与实时性测试,达到预期的设计目的,满足大型抽水蓄能电站的运行管理要求与信息安全要求。随着我国水电开发工作的不断深入,大型抽蓄电站建设、改造项目不断开展,该成果具有广泛的推广前景。

参考文献:

[1] 吴小锋, 李刚, 马聖恒,等. 抽水蓄能电站监控系统国产化改造方案研究[J]. 中国农村水利水电, 2022(6):202-206.

[2] 高昆仑, 辛耀中, 李钊,等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化, 2015, 39(1):48-52.

[3] 高昆仑, 王志皓, 安宁钰,等. 基于可信计算技术构建电力监测控制系统网络安全免疫系统[J]. 工程科学与技术, 2017,49(2):28-35.

[4] 亢超群, 李二霞, 李玉凌,等. 新一代配电主站主动防御架构设计方法[J]. 电力信息与通信技术, 2021,19(3):65-73.

[5] 杨维永, 刘苇, 崔恒志,等. SG-Edge:电力物联网可信边缘计算框架关键技术[J]. 软件学报, 2022, 33(2):641-663.

[6] 施一明, 高博, 王天林,等. PLC 控制系统可信架构及硬件技术研究[J]. 中国仪器仪表, 2022(4): 27-30,36.

[7] 李硕, 姜海军, 操俊磊,等. 深圳抽水蓄能电站计算机监控系统设计与应用[J]. 水力发电, 2021, 47(2):64-68.

[8] 施冲,朱辰,方辉钦,等. 水电厂计算机监控技术发展趋势分析[J]. 水电自动化与大坝监测, 2002, 26(6):1-4,17.

Research on Trusted Applications in SCADA for Pumped Storage Power Station

CAI Jie[1], WU Zheng-yi[1], ZHANG Xin[2], ZHAO Yi-feng[3], LI Xiao-peng[4], LIU Meng-chu[1]

(1. NARI Group (State Grid Electric Power Research Institute) Co., Ltd., Nanjing 211106, China; 2. State Grid Xinyuan Co., Ltd., Beijing 100052, China; 3. Pumped-storage Technology & Economic Research Institute of State Grid Xinyuan Co., Ltd., Beijing 100053, China; 4. State Grid Sichuan Electric Power Research Institute, Chengdu 610041, China)

Abstract: In respect to the network security situation and attacks of new types, the needs of trusted computing of applications in SCADA for pumped storage power station was analyzed. Based on the trusted hardware platform and operating system, a system structure of trusted applications in SCADA was proposed, and the key techniques such as trusted distributed services and trusted behavior analysis were discussed. The results show that the proposed design realizes the trusted applications in SCADA, and provides active defense mechanism for SCADA, and adapts to the development of prospective SCADA applications for pumped storage power station.

Key words: pumped storage power station; SCADA; distributed application; trusted computing