DOI: 10.19666/j.rlfd.202409205

电力专用横向单向隔离装置安全加固中间件设计及应用

马瑞瑞，何　清，杨国栋，王大鹏，王　毅，杜保华
（西安热工研究院有限公司，陕西　西安　710054）

［摘　　要］为了提高电力监控系统的网络安全防护能力，设计了一种电力专用横向单向隔离装置安全加固中间件。该中间件集成了兼容性适配、文件格式矫正、加密认证、负载均衡及权限控制等功能，在业务系统所在管理信息大区和生产控制大区间构建了一道坚实的安全屏障，解决了隔离装置在升级加固过程中面临的业务系统兼容性、硬件故障及明文通信等安全问题，强化了电力监控系统数据传输通道的安全管控，实现了隔离装置的“高效无感知”和“标准化”安全升级加固。该中间件已成功应用于中国华能集团所有火电、水电和新能源电站，提升了电力监控关键信息基础设施网络安全边界防护能力，保障了电力生产的信息安全。

［关　键　词］隔离装置；安全加固；中间件；电力监控系统

［引用本文格式］马瑞瑞，何清，杨国栋，等. 电力专用横向单向隔离装置安全加固中间件设计及应用[J]. 热力发电，2025，54(5): 156-162.　MA Ruirui, HE Qing, YANG Guodong, et al. Design and application of security reinforcement middleware for interal unidirectional safety isolating device for electric power[J]. Thermal Power Generation, 2025, 54(5): 156-162.

Design and application of security reinforcement middleware for interal unidirectional safety isolating device for electric power

MA Ruirui, HE Qing, YANG Guodong, WANG Dapeng, WANG Yi, DU Baohua
(Xi’an Thermal Power Research Institute Co., Ltd., Xi’an 710054, China)

Abstract: To enhance the cybersecurity protection capabilities of power monitoring systems, a security reinforcement middleware for interal unidirectional safety isolating device for electric power has been designed. This middleware integrates compatibility adaptation, file format correction, encryption authentication, load balancing, and access control functions, addressing the security issues such as business system compatibility, hardware failures, and plaintext communication faced by isolation devices during the upgrading and reinforcement process. It enhances the security control of data transmission channels in power monitoring systems and achieves an “efficient and unobtrusive” and “standardized” security upgrade and reinforcement of the isolation devices. This middleware has been successfully applied to all thermal power, hydropower, and new energy power stations of Huaneng Group, strengthening the cybersecurity boundary protection capabilities of critical information infrastructure in power monitoring and ensuring the information security of power production.
Key words: isolation device; security reinforcement; middleware; power monitoring system

为筑牢电力监控系统边界防护，切实保证“安全分区、网络专用、横向隔离、纵向认证”的综合防护要求，电厂工控大区边界必须使用电力专用横向单向安全隔离装置[1-2]（隔离装置）。隔离装置分

收 稿 日 期：2024-09-04　网络首发日期：2025-04-18
基 金 项 目：中国华能集团有限公司总部科技项目（HNKJ24-H28, HNKJ24-H57）；陕西省科技计划项目（2024GX-YBXM-156）
Supported by: Science and Technology Project of China Huaneng Group Co., Ltd. (HNKJ24-H28, HNKJ24-H57); Shaanxi Provincial Science and Technology Plan Project (2024GX-YBXM-156)
第一作者简介：马瑞瑞（1982），女，硕士，高级工程师，主要研究方向为电站信息技术及其应用，maruirui@tpri.com.cn。

为正向型和反向型。正向隔离装置[3]用于生产控制大区到管理信息大区的非网络方式的单向数据传输，反向隔离装置[4-5]用于从管理信息大区到生产控制大区的非网络方式的单向数据传输，是管理信息大区到生产控制大区的唯一数据传输途径[6]。

随着网络技术的快速发展，电力系统面临的网络安全威胁日益严峻。隔离装置作为电力系统中的重要安全设备，其性能和安全性直接关系整个系统的稳定运行。电力系统部分在运隔离装置存在若干亟待解决的安全问题。首先，部分设备老化且缺乏必要的权威安全认证，存在安全防护的风险隐患。多数设备未能满足网络安全等级保护 3.0 标准的核心要求，如三权分立管理、强口令机制、IP/MAC 绑定及全面的日志审计等，为系统安全埋下了隐患。其次，正向隔离装置在数据单向流动控制方面存在不足，未能全面遵循单比特应答策略，可能导致数据逆向泄露，危及生产控制大区网络的安全。此外，反向隔离装置缺乏对非 E 文本文件传输的有效限制[7-8]。E 文件使用电力行业专用数据描述语言，具有严格的格式定义和校验规则。缺乏此类控制可能导致恶意软件或非法数据绕过安全屏障，对关键生产控制区域构成直接威胁。

为了全面贯彻落实总体国家安全观，进一步提升电力监控系统网络边界安全防护能力，《国家能源局综合司关于印发 2021 年电力安全监管重点任务的通知》明确提出了推进隔离装置整改的工作要求，据此需要对各发电企业工控大区边界正向、反向隔离装置开展安全加固工作。

本文设计了一种电力专用横向单向隔离装置安全加固中间件（安全加固中间件），该中间件作为业务系统与隔离装置之间的桥梁，集成了兼容性适配、文件格式矫正、加密认证、负载均衡及权限控制等核心功能，旨在确保业务连续性与数据安全性的同时，实现在运隔离装置“高效无感知”和“标准化”安全升级加固，提升电力监控系统网络边界的安全防护能力。

1 安全加固中间件设计

现有业务系统与隔离装置之间的复杂交互关系，决定了隔离装置安全加固不能直接采取粗暴的硬件更换或升级策略。

首先，部分正向隔离的业务系统因不满足单比特数据通信安全审计策略，若直接升级硬件，将导致数据通信中断和业务程序异常，需依赖业务系统开发商进行系统层面的适应性改造；其次，反向隔离的业务系统中普遍存在非 E 文本文件传输模式，构成了隔离装置加固升级过程中的另一大障碍。隔离装置硬件设备加固升级后，此类非标准传输模式将面临通信阻断的风险，业务系统需要同步升级以确保数据传输机制与隔离装置加固策略相兼容；最后，从通信安全与效率的角度出发，现有业务系统中明文通信及非压缩数据传输方式不仅降低了数据安全性，还造成了隔离装置带宽资源的浪费。因此，在硬件升级的同时，需要开展通信协议的优化与改进，使业务数据传输满足隔离装置新的传输规则，同时提升数据传输的安全性与效率，最大化利用隔离装置的性能潜力。

鉴于业务系统全面升级改造的高成本、时间不确定性和厂商支持等因素，本文认为探索并实施一种更为高效、安全且成本效益显著的解决方案至关重要。这种方案需综合考虑业务连续性、安全性与成本控制的平衡，为隔离装置的安全加固提供切实可行的路径。

1.1 设计思路

中间件是一种独立的系统软件服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算资源和网络通信，同时标准化不同操作系统提供的应用程序接口，实现协议的统一化，屏蔽具体操作细节。中间件技术为隔离装置的安全加固提供了新的思路和实践路径。

本文设计的安全加固中间件属于安全增强型中间件，专注于提升电力监控系统的安全性，特别是在涉及数据隔离、加密通信、权限控制等关键安全领域。通过在业务系统与隔离装置之间插入一层安全逻辑，解决了业务系统兼容性、硬件故障、明文通信等风险。

1.2 软件架构

针对正向数据传输和反向文件传输 2 种不同的应用场景，本文分别设计并开发了正向隔离装置安全加固中间件和反向隔离装置安全加固中间件，以灵活应对不同场景下的安全挑战。

正向隔离装置加固中间件为第三方厂商业务系统建立安全稳定的数据传输通道，适配正向隔离装置单比特应答要求。反向隔离装置安全加固中间件则更专注于实现文件的安全回传与验证，支持多种类型文件与 E 文本文件的相互转换，确保文件符

合反向隔离装置的传输要求。正向/反向隔离装置加固中间件都可对数据进行加密、压缩处理，提高数据传输效率，增加传输数据安全性。

安全加固中间件采用分层体系架构，由基础服务层、通用功能层、应用层组成，其架构如图 1 所示。

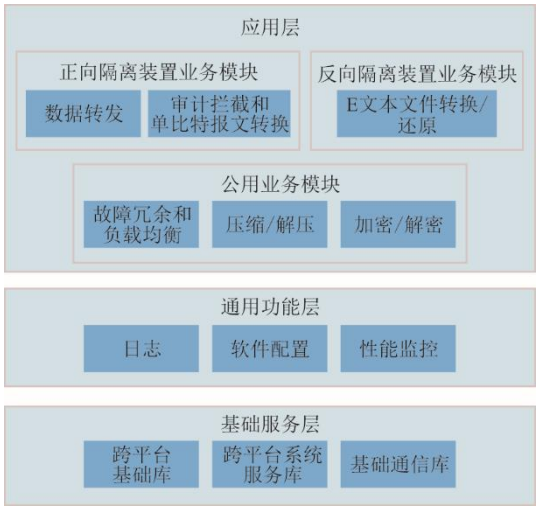

图 1 安全加固中间件软件架构

Fig.1 Software architecture diagram of isolation device security reinforcement middleware

基础服务层包括跨平台基础库、跨平台系统服务库、基础通信库。跨平台基础库为 Windows、Linux 操作系统提供一致的标准函数、类型、线程和锁使用接口。跨平台系统服务库为 Windows、Linux 操作系统提供一致的服务程序编程框架及接口。基础通信库提供 TCP 通信的封装，包括常见 Socket 编程接口的封装。

通用功能层主要是为提高软件的易用性以及方便监视软件的性能。包括日志、软件配置、性能监控模块。日志模块支持本地日志及日志按模块分仓存储处理。软件配置模块对软件提供运行参数的配置，如正向隔离装置加固中间件 TCP 通信 IP、端口，反向隔离装置加固中间件 E 文件转换、还原路径等参数的配置。性能监控模块方便分析隔离装置加固中间件的运行状态，包含 CPU 使用率、内存占用、网络流量分析。

应用层是隔离加固中间件的核心业务层，集成了公用业务、正向隔离装置业务及反向隔离装置业务 3 大模块。公用业务模块涵盖故障冗余与负载均衡、数据压缩/解压及加密/解密功能，确保系统高可用、提升传输效率并保障数据安全。正向隔离装置业务模块应用于正向隔离装置安全加固中间件，专注于数据透明转发、审计拦截及单比特报文转换，有效管理内外网间数据流动，增强通信安全性。反向隔离装置业务模块应用于反向隔离装置安全加固中间件，通过 E 文本文件的高效安全转换/还原功能，支持灵活的文件转换需求。整体而言，应用层实现了业务功能的全面覆盖与高效协同。

2 关键技术介绍

2.1 单比特安全审计策略适配技术

通过正向隔离装置发送数据和返回数据逻辑如图 2 所示。正向隔离装置单比特数据通信安全审计策略对内网客户端向外网服务器发送数据不做限制，对外网服务端返回内网客户端的每个报文，只允许为 1 bit 数据，其值只能是“0x00”或者“0xff”，通常用于确认已经收到客户端的数据，表明处理成功或失败。单比特应答审计策略确保了数据只能从高安全级别区域向低安全级别区域单向流动，防止了潜在的反向数据流动，从而保护生产控制大区网络不受外部威胁。

为满足上述审计策略，实现业务系统与正向隔离装置兼容适配，正向隔离装置安全加固中间件对内网业务系统客户端发往外网业务系统服务端的数据包进行透明转发，对外网业务系统服务端返回内网业务系统客户端的数据包（响应报文）进行审计拦截或单比特报文转换。

针对拦截部分返回数据包不影响业务系统正常通信的场景，加固中间件将对不满足单比特数据通信安全审计策略的数据包进行拦截。针对拦截部分返回数据包会引起业务系统通信中断的场景，加固中间件通过报文协议转换配置，实现返回数据包的单比特报文转换。

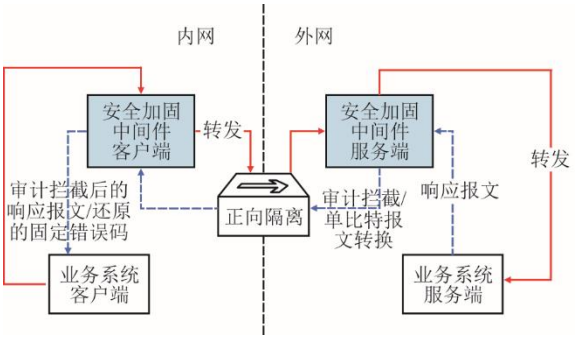

图 2 通过正向隔离装置发送数据和返回数据逻辑

Fig.2 Logical diagram for sending and returning data through forward isolation device

例如：某电厂业务系统服务端从外网返回错误码到内网客户端，错误码由 8 个“0x00”或“0xff”

单比特包组成。内网业务系统客户端需要收到所有单比特包，否则业务将被中断。安全加固中间件服务器端将所有返回非零的错误码（非 8 个“0x00”）转换为 1 个单比特包“0xff”，将连续 8 个“0x00”转换为 1 个单比特包“0x00”进行处理并传输。穿隔离装置单比特传输后，安全加固中间件客户端将接收到的“0x00”还原为 8 个连续“0x00”（对应二进制为“00000000”，表示成功），将“0xff”还原为“0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff”（对应二进制为“00000001”，该错误码可被业务系统识别并处理）并发送至业务系统客户端，系统正常运行。该示例中错误码配置转换见表 1。

表 1 单比特错误码配置转换
Tab.1 Single-bit error code configuration conversion table

业务系统服务端发送响应报文	加固中间件服务端转换	加固中间件客户端转换	业务系统客户端接收响应报文
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00	0x00	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff	0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff
xff,0x00,0x00,0x00,0x00,0x00,0x00,0x00, 0x00	0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff
0xff,0xff,0x00,0x00,0x00,0x00,0x00,0x00,0x00	0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff
.....	0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff	0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff

这种报文转换策略将所有非零的错误码使用业务系统可处理的某个错误码代替，虽然牺牲了错误码的准确性，但确保了业务系统的稳定运行并符合新的安全审计要求。

2.2 数据压缩和加密

针对现有部分早期的业务系统使用明文通信，并且通信数据未采用压缩传输，造成数据安全性低、隔离装置带宽资源利用率不高的问题，通过在加固中间件中引入可配置的数据压缩及加密模块[9-10]，在现有业务系统不做任何改动的情况下，实现数据的压缩和加密传输。

当大量数据穿隔离装置传输时，会造成隔离装置负载过高、数据传输链路不稳定。此时加固中间件客户端可根据用户配置对数据进行压缩处理，通过减小隔离装置带宽占用，达到提高隔离装置传输效率和业务系统稳定性的目的。通过隔离装置后，由加固中间件服务端进行数据解压，并将解压后的数据发送至业务系统服务端。加固中间件默认使用 LZ4 压缩算法[11-12]，该压缩算法具有压缩和解压速度快的特点，同时可配置使用 Zstandard 压缩算法[13-14]。该压缩算法以其高压缩比而闻名，但压缩和解压速度方面则 LZ4 更优。对某电厂的业务系统真实传输数据实测表明，默认配置下，Zstandard 压缩算法与 LZ4 压缩算法比较，前者压缩速度约为后者的 75%，解压速度约为后者的的 50%，但压缩率较后者提高了约 13%。使用 Zstandard 压缩，带宽占用约为未开启压缩带宽占用的 43%，使用 LZ4 压缩，带宽占用约为未开启压缩带宽占用的 56%。用户可根据现场业务系统需要选择更快压缩/解压速度的 LZ4 压缩算法，或更高压缩率的 Zstandard 压缩算法。

在设计安全加固中间件时，加密传输技术是确保数据安全的关键环节。生产控制大区与管理信息大区之间使用正向/反向隔离装置传输数据时，使用明文进行数据传输存在较大安全隐患。此时可通过加固中间件客户端对跨域传输的数据进行加密处理，增加系统安全性。数据加密算法使用 SM4 对称国密算法[15-16]。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构设计，大大增加了破解难度，具有高效性和高安全性的特点。

该解决方案多次在国家网络安全防护演练中成功应对网络攻击并为企业解决了老旧业务系统难以通过数据安全性检测的问题，确保了数据流转过程的完整性与机密性。

2.3 E 文本文件自适应转换技术

针对反向隔离装置升级加固后将禁止非 E 文本文件数据通信问题，本文提出了反向隔离装置 E 文本文件自适应转换技术[17]。该技术支持任意文件格式和标准 E 文本文件格式高效安全互转换，实现了现有业务系统无需任何修改，即可满足升级加固后的反向隔离装置强制 E 文件传输的安全要求，提高了反向隔离装置升级加固后业务系统的兼容性和安全性。

该技术包括反向隔离装置加固中间件客户端和服务端 2 个部分的处理。

第 1 步，加固中间件客户端将非 E 文件转换为 E 文件。加固中间件客户端加载非 E 文件，对文件数据进行 CRC 校验[18]计算，根据用户配置对文件数据进行压缩和加密[19]处理，然后将处理后的二进制数据转换为 16 进制字符，并按照 E 语言格式组

织，再次进行 CRC 校验。

第 2 步，加固中间件服务端将转换后的 E 文件还原为原始文件格式。加固中间件服务端接收到 E 文本文件后，首先验证转换标识和头部信息，然后对文本进行 CRC 校验，确保数据未被篡改或损坏。确认无误后，将 16 进制文本还原为二进制数据，并根据需要进行解压或解密，最终恢复为原始文件格式。

该技术通过确保所有非 E 格式文件在通过反向隔离装置前转换为遵循严格标准的 E 文本文件，有效防止了恶意软件或非法数据未经校验直接渗透至生产控制大区。转换过程中集成的数据校验机制及加密压缩处理，进一步加固了数据的安全性，确保数据的完整性和机密性不被破坏，不仅增强了系统的防御能力，还提高了对潜在安全威胁的识别和应对能力。

2.4 隔离装置多路冗余和负载均衡

针对单路隔离网络架构不具备数据链路冗余能力，设备故障或数据通信量大时，会造成业务中断或数据丢失的问题，本文设计了隔离装置中间件多路冗余架构和负载均衡算法，实现了隔离装置数据传输通道高可用和带宽扩展的功能，可满足对数据传输带宽和稳定性具有更高要求的应用场景。图 3 为隔离装置多路冗余和负载均衡软硬件拓扑。

如图 3 所示，安全加固中间件客户端可连接并管理多路正向隔离装置，实现数据传输链路多路冗余[10-21]和负载均衡。当各路隔离装置运行正常时，加固中间件客户端根据网络负载情况对数据进行多路分发，可提高数据链路的带宽。当某路隔离装置故障时，加固中间件客户端检测到连接断开，则不再给该数据链路分发数据。该方式虽然整体网络带宽被降低，但不影响业务系统数据传输；当加固中间件客户端检测到隔离装置故障恢复重连后，该隔离装置会被及时并入正常数据链路中，参与负载均衡数据传输。

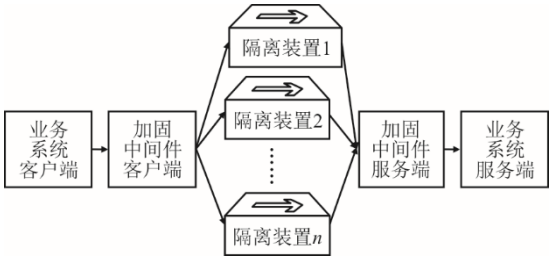

图 3 隔离装置多路冗余和负载均衡软硬件拓扑

Fig.3 Isolation device multi-channel redundancy and load balancing software and hardware topology

反向隔离装置的数据传输链路多路冗余和负载均衡处理方法和正向隔离装置类似，区别在于负载均衡分发时，加固中间件客户端通过反向隔离装置的文件摆渡目录中现存未摆渡文件的大小来进行负载均衡权重计算。现存未摆渡文件越小，表示负载越小，则优先进行文件分发。当加固中间件客户端检测到某路反向隔离装置故障时，则将该反向隔离装置负责摆渡的文件快速分发到其他路反向隔离装置，确保文件摆渡不中断。

3 应用情况

3.1 总体应用情况

截至 2024 年 6 月，安全加固中间件在华能集团 32 个产业公司及区域公司下属的 900 多家燃煤、燃气、水电、风电、光伏企业或场站实施推广，近千台在运隔离装置完成升级加固，其中完成约 70%正向隔离装置、30%反向隔离装置的“高效无感知”和“标准化”安全升级加固。

3.2 典型应用案例

北方联合电力有限责任公司（北方公司）是中国华能集团的区域子公司，是内蒙古自治区最大的发电供热企业。2021 年底至 2023 年期间，北方公司全面采用安全加固中间件对所属 18 家单位部署在生产控制大区与管理信息大区边界的在运隔离装置进行升级加固，涵盖 17 家火电厂、1 家新能源公司（风电总部及公司各场站），共部署安全加固中间件 36 套。

隔离装置硬件设备延用原厂商进行升级加固工作，对于原厂家设备不能满足安全加固工作要求的，替换为满足国网电科院认证的隔离装置。在运隔离装置完成硬件升级加固工作的同时，同步完成安全加固中间件的部署及调试。

针对正向数据传输的场景，在内网业务系统与正向隔离装置之间，以及正向隔离装置与外网业务系统之间，分别部署正向隔离装置安全加固中间件客户端和服务端，具体如图 4 所示。

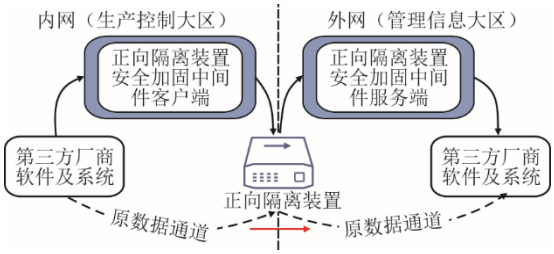

图 4 正向隔离装置安全加固中间件部署方式

Fig.4 Deployment method of forward isolation device security reinforcement middleware

针对反向文件传输的场景，在原“文件发送目录”和反向隔离装置之间部署反向隔离装置安全加固中间件客户端和新“文件发送目录”，在反向隔离装置和原文件接收目录之间部署新文件接收目录和反向隔离装置安全加固中间件服务端，具体如图 5 所示。

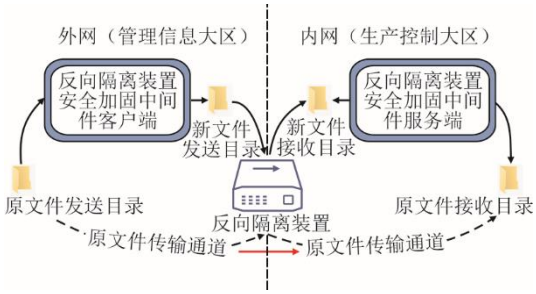

图 5 反向隔离装置安全加固中间件部署方式
Fig.5 Deployment method of backward isolation device security reinforcement middleware

经现场检验测试，隔离装置升级加固后，数据通信和应用数据刷新均达到预期效果。安全加固中间件的引入，有效隔离了第三方厂家软件与生产控制大区之间的直接通信，降低了外部攻击或非法数据渗透的风险，提升了系统的整体安全防护水平。

3.3 应用效果

安全加固中间件在业务系统所在管理信息大区和生产控制大区间构建了一道坚实的安全屏障。加密传输确保了跨域传输数据的机密性，防止了敏感信息泄露，强化了电力监控系统数据传输通道的安全管控。同时，安全加固中间件的设计充分考虑了与现有业务系统的兼容性，避免了硬件更换和业务系统升级带来的高昂成本和时间风险。与直接硬件升级或修改业务系统代码等方案相比，安全加固中间件在保持业务连续性和提升系统安全性方面展现出了独特的优势，极大提升了交付效率，降低了运维成本，经济效益显著。

4 结　语

本文设计了一种电力专用横向单向隔离装置安全加固中间件，有效解决了隔离装置在安全加固过程中面临的业务系统兼容性、硬件故障及明文通信等安全风险。通过标准化、资源优化和增强的安全处理逻辑，为电力监控信息系统的安全稳定运行提供了有力保障。该安全加固中间件已成功应用于中国华能集团所有火电、水电和新能源电站，强化了电力监控关键信息基础设施网络安全边界防护能力，保障了电力生产的信息安全，促进了国内工业互联网的安全升级，取得了良好的社会效益。

未来，我们将继续探索更安全高效的加密算法、优化安全加固中间件的性能，并扩大其应用范围，以进一步提升电力系统的整体安全防护能力。

［参 考 文 献］

［1］ 杨鹏. 大型发电厂电力监控系统安全防护方案设计及工程实践[J]. 电工技术, 2023(12): 186-189.
YANG Peng. Design and engineering practice of security protection scheme for large plant power monitoring system[J]. Electric Engineering, 2023(12): 186-189.

［2］ 杨至元, 张仕鹏, 孙浩. 电力系统信息物理网络安全综合分析与风险研究[J]. 南方能源建设, 2020, 7(3): 6-22.
YANG Zhiyuan, ZHANG Shipeng, SUN Hao. Integrated cyber-physical contingency analysis and risk estimates[J]. Southern Energy Construction, 2020, 7(3): 6-22.

［3］ 曹翔, 张阳, 宋林川, 等. 基于深度报文检测和安全增强的正向隔离装置设计及实现[J]. 电力系统自动化, 2019, 43(2): 162-167.
CAO Xiang, ZHANG Yang, SONG Linchuan, et al. Design and implementation of a forward isolation device based on deep packet inspection and security enhancement[J]. Automation of Electric Power Systems, 2019, 43(2): 162-167.

［4］ 申永辉. 电力专用安全隔离装置的原理和应用[J]. 湖南电力, 2006(6): 31-33.
SHEN Yonghui. Principle and application of power specific safety isolation devices[J]. Hunan Electric Power, 2006(6): 31-33.

［5］ 郭仁超, 徐玉韬. 内外网数据安全交换技术在电网企业的应用研究[J]. 电力大数据, 2018, 21(2): 61-66.
GUO Renchao, XU Yutao. Research on the application of internal and external network data security exchange technology in power grid enterprises[J]. Power Big Data, 2018, 21(2): 61-66.

［6］ 可再生能源发电站电力监控系统网络安全防护技术规范[S]. 北京: 中国标准出版社, 2018: 1.
Technical specification for cyber security protection of electric power system supervision and control in renewable energy power station[S]. Beijing: China Standard Press, 2018: 1.

［7］ 杜鹏, 陶洪铸, 高保成, 等. 面向多应用的通用数据采集技术方案[J]. 电力系统自动化, 2015(1): 26-30.
DU Peng, TAO Hongzhu, GAO Baocheng, et al. A universal data collection technology solution for multiple applications[J]. Automation of Electric Power Systems, 2015(1): 26-30.

［8］ 李丽芬, 程晓荣, 吴克河. 计算机网络体系结构[M]. 北京: 中国电力出版社, 2006: 1.
LI Lifen, CHENG Xiaorong, WU Kehe. Computer network architecture[M]. Beijing: China Electric Power Press, 2006: 1.

［9］ 曹井万. 数据加密和单向网闸技术在流程行业的应用研究[J]. 信息记录材料, 2022, 23(6): 161-164.
CAO Jingwan. Research on the application of data encryption and unidirectional gateway technology in the process industry[J]. Information Recording Materials, 2022, 23(6): 161-164.

[10] 陈志军, 洪莎莎. 跨网络信息安全交换平台建设方案研究[J]. 数字通信世界, 2021(5): 80-81.
CHEN Zhijun, HONG Shasha. Research on the construction plan of cross network information security exchange platform[J]. Digital Communication World, 2021(5): 80-81.
[11] 程裕博. 基于网络多路径和数据压缩的IPFS文件传输性能优化研究[D]. 重庆: 重庆理工大学, 2024: 1.
CHENG Yubo. Research on IPFS file transfer performance optimization based on network multipass and data compression[D]. Chongqing: Chongqing University of Technology, 2024: 1.
[12] 吴涛. 基于LZ4算法的无损压缩硬件设计与WIFI传输[D]. 南京: 东南大学, 2021: 1.
WU Tao. Hardware design of lossless compression based on LZ4 algorithm and WIFI transmission[D]. Nanjing: Southeast University, 2021: 1.
[13] 徐雪强. 基于自适应压缩算法的远程数据采集系统设计与应用[D]. 哈尔滨: 黑龙江大学, 2023: 1.
XU Xueqiang. Design and application of remote data acquisition system based on adaptive compression algorithm[D]. Harbin: Heilongjiang University, 2023: 1.
[14] 王炳耀. Zstd压缩算法的硬件设计与验证[D]. 西安: 西安电子科技大学, 2023: 1.
WANG Bingyao. Hardware design and verification of Zstd compression algorithm[D]. Xi'an: Xidian University, 2023: 1.
[15] 宋永立, 孙若尘, 贾娟, 等. 基于国密算法的CoAP安全协议研究与实现[J]. 计算机工程与设计, 2024, 45(7): 2066-2073.
SONG Yongli, SUN Ruochen, JIA Juan, et al. Research and implementation of CoAP security protocol based on domestic cryptographic algorithms[J]. Computer Engineering and Design, 2024, 45(7): 2066-2073.
[16] ABED S, JAFFAL R, MOHD B J, et al. Performance evaluation of the SM4 cipher based on field-programmable gate array implementation[J]. IET Circuits, Devices & Systems, 2021, 15(2): 121-135.
[17] 陈少立, 何清, 王奕飞, 等. 一种通过反向网闸同步非E文件的方法: CN202111299310.4[P]. 2024-02-23[2024-05-16].
CHEN Shaoli, HE Qing, WANG Yifei, et al. A method of synchronizing non E files through reverse gateway: CN202111299310.4[P]. 2024-02-23[2024-05-16].
[18] 罗长洲, 马梦宇, 李萌, 等. CRC校验码软件生成技术原理分析[J]. 计算机仿真, 2024, 41(3): 158-161.
LUO Changzhou, MA Mengyu, LI Meng, et al. Principle Analysis of CRC checksum software generation system[J]. Computer Simulation, 2024, 41(3): 158-161.
[19] 任晨, 刘立, 陈鹏, 等. 一种基于隔离网闸的大文件高效传输方案[J]. 信息化建设, 2021(2): 62-64.
REN Chen, LIU Li, CHEN Peng, et al. An efficient transmission scheme for large files based on isolation network gates[J]. Informatization Construction, 2021(2): 62-64.
[20] 白燕. 基于网闸的双机热备系统的设计与实现[D]. 北京: 北京理工大学, 2016: 1.
BAI Yan. Design and implementation of a dual machine hot backup system based on network gates[D]. Beijing: Beijing Institute of Technology, 2016: 1.
[21] 杨越, 王若冰, 刘瑞, 等. 基于多传输通道的单向传输技术研究[J]. 计算机应用与软件, 2017, 34(4): 135-141.
YANG Yue, WANG Ruobing, LIU Rui, et al. Research on unidirectional transmission technology based on multiple transmission channels[J]. Computer Application and Software, 2017, 34(4): 135-141.

（责任编辑　杜亚勤）

广告目次