输电线路边缘计算终端固件安全检测与加固技术

刘彦昌
北京吉北电力工程咨询有限公司　北京市　102600

摘　要：边缘计算融入输电线路智能监测，终端固件安全至关重要。本文基于输电线路野外场景，解析固件安全检测技术逻辑，阐述静态分析中的反汇编、符号执行等策略，动态调试里的硬件仿真、模糊测试方法，以及漏洞挖掘风险量化模型。构建多层级加固体系，涵盖可信启动、内存安全防护、加密通信、固件更新校验等。结合特高压输电线路案例，说明技术实施路径。通过集成硬件安全模块等手段，实现固件全生命周期管控，为输电线路边缘计算终端可靠运行提供技术支撑与实践范式。

关键词：边缘计算；输电线路；固件安全检测；安全加固；可信启动

输电线路是电能传输核心，其精准感知与稳定控制对电网安全意义重大。边缘计算应用于输电线路监测，实现风险实时捕捉与处置。但输电线路边缘终端多在野外，面临物理接触、通信干扰、固件升级等多重安全威胁。固件漏洞可能导致设备异常、数据篡改甚至输电中断。现有安全检测技术对输电终端特性考虑不足，加固方案存在兼容性与实用性矛盾。因此，开展适配输电场景的固件安全检测与加固技术研究，对推动输电线路智能化升级、保障电网安全十分必要。

1 固件安全检测技术

1.1 静态分析技术

静态分析技术通过对固件二进制文件的非执行式解析，挖掘潜在安全漏洞，其核心优势在于无需搭建完整运行环境，可快速定位代码层面的安全隐患，适配输电终端固件的嵌入式特性[1]。反汇编与控制流分析是静态检测的基础环节，需通过固件提取工具获取二进制镜像文件，针对ARM、MIPS架构采用IDA Pro配置对应内核指令集，或通过Ghidra插件完成解析。解析过程中重点构建函数调用关系图与控制流图，遍历关键路径识别缓冲区溢出、整数溢出等漏洞，优先核查传感器数据采集、控制指令下发模块的输入参数长度校验逻辑。

符号执行与约束求解技术通过数学建模模拟固件执行路径，基于KLEE或Angr框架构建约束条件库，针对传感器数据范围设置参数减少无效遍历，生成边界值测试用例验证固件对极端数据的处理能力，避免控制逻辑紊乱。敏感API调用检测需构建危险函数特征库，通过正则匹配与上下文分析判断调用安全性，利用Ghidra脚本批量扫描未校验参数的敏感函数，重点检测Modbus、IEC 61850协议解析相关的API调用，保障数据传输参数处理安全。

1.2 动态调试技术

动态调试技术监测固件运行行为捕捉隐性漏洞，核心是构建贴近实际的调试场景。硬件仿真调试针对ARM Cortex-A系列芯片，通过QEMU配置单板机镜像，采用GDB远程调试在关键节点设置断点监测寄存器与内存变化。支持JTAG接口的终端可通过OpenOCD直接连接硬件实现在线监控。模糊测试需结合接口类型设计用例，串口、网口采用AFL-Fuzz生成协议合规变异数据，工业协议基于帧格式修改关键参数构建测试模板，实时捕捉设备崩溃、内存泄漏等异常并定位漏洞根源。侧信道攻击分析通过专业设备采集功耗、电磁辐射数据，利用差分功耗分析、相关电磁分析算法提取密钥特征，重点测试低功耗模式下的侧信道安全性，避免功耗优化弱化防护能力。

1.3 漏洞挖掘与风险评估

漏洞挖掘与风险评估需建立科学的量化体系，结合输电线路的安全需求，实现对漏洞危害程度的精准判定与防护优先级排序。CVSS评分系统的应用需结合输电场景的特殊性进行指标调整，在“攻击向量”指标中重点考虑物理攻击的易实施性，在“影响范围”指标中纳入对输电调度、设备控制的潜在影响。对于远程代码执行、固件篡改等高危漏洞，需结合终端的部署位置（如跨越重要交通枢纽、生态保护区的输电线路）进一步提升风险等级。

攻击路径建模采用攻击树分析法，以“固件安全失效导致输电中断”为根节点，分解出物理攻击、网络攻击、固件更新攻击等二级节点，进一步细化为调试端口未关闭、签名验证失效、加密算法破解等三级节点。通过计算各节点的发生概率与影响程度，识别关键攻击面。实践中需重点关注固件更新接口、远程调试端口、物理存储介质等易被突破的环节。

2 固件安全加固技术

2.1 可信启动与安全启动链

可信启动技术以硬件级信任根为基础，构建从终端上电到应用运行的全流程安全验证体系，其核心在于确保固件的完整性与合法性，抵御篡改攻击。安全启动链的构建需遵循“自下而上、逐级验证”的原则，终端上电后首先由硬件信任根（如 TPM 2.0 芯片、TEE 可信执行环境）验证 Bootloader 的数字签名，验证通过后加载 Bootloader，再由 Bootloader 验证内核镜像的完整性，最后由内核验证应用程序的合法性。针对输电终端的国产化需求，可采用 SM2 非对称加密算法生成签名密钥，SM3 哈希算法计算固件的摘要值，确保签名验证的安全性与合规性 [2]。

动态信任链扩展需在固件运行过程中持续监测关键模块的完整性，通过在终端内核中植入完整性监测进程，定期对核心函数、配置文件的哈希值进行校验，校验周期可根据终端的业务负载动态调整。针对输电终端的实时性要求，可采用增量校验机制，仅对发生变化的模块进行完整性验证，减少对设备运行性能的影响。当监测到模块被篡改时，立即启动应急响应机制，隔离受感染的进程，同时向云端管理平台发送告警信息，便于运维人员及时处置。

2.2 内存安全防护

内存安全防护针对栈溢出、代码注入等常见攻击手段，从硬件配置与软件优化两个层面构建防护体系，确保固件运行时的内存数据安全。数据执行防护（DEP）的实现需结合终端的处理器架构进行配置，在 x86 架构终端中可通过操作系统开启 NX 位功能，标记数据内存区域为不可执行。在 ARM 架构终端中，通过配置 MPU 内存保护单元的权限寄存器，将数据区设置为只读或只写属性，禁止执行指令。

地址空间布局随机化（ASLR）需在固件编译阶段进行配置，通过修改链接脚本，使代码段、数据段、堆区、栈区的加载地址在每次启动时随机偏移。偏移量的生成可基于硬件随机数生成器，确保随机性与不可预测性。针对嵌入式系统内存空间有限的特点，可采用分区随机化策略，重点对核心功能模块的地址进行随机化处理，在保障安全的同时降低系统开销。

栈保护机制通过在函数栈帧中插入金丝雀值实现对栈溢出的检测，金丝雀值可采用动态生成的随机数，存储在栈帧的返回地址与局部变量之间。当发生栈溢出时，金丝雀值会被篡改，固件通过校验金丝雀值的完整性，触发异常中断并终止程序运行。实践中可结合硬件寄存器存储金丝雀值的备份，避免攻击者通过内存读取获取金丝雀值。

2.3 加密通信与数据保护

加密通信与数据保护技术旨在保障边缘终端与云端、终端与终端之间的数据传输安全，以及本地存储数据的机密性，适配输电线路复杂的通信环境与物理安全需求。国密算法的集成需遵循《电力行业信息安全等级保护测评要求》，在数据传输中采用 SM4 对称加密算法对敏感数据（如监测数据、控制指令）进行加密，密钥通过 SM9 非对称加密算法进行协商分发。针对输电终端的低带宽特性，可优化 SM4 算法的加密模式，采用 CTR 模式减少加密延迟，提升数据传输效率。

安全传输协议的优化需结合输电线路的通信场景，针对有线通信采用 TLS 1.3 协议构建加密通道，通过精简握手流程、复用会话密钥，降低连接建立时间。针对无线通信（如 5G、LoRa）采用 DTLS 协议，解决无线链路不稳定导致的重传问题。协议配置中需禁用弱加密套件，优先选择基于国密算法的加密组合，同时开启证书吊销列表校验，避免使用失效证书引发安全风险。

数据存储加密需针对终端的存储介质（如 eMMC、NAND Flash）采用分层加密策略，对设备密钥、数字证书等核心数据采用硬件加密方式，通过 HSM 硬件安全模块存储加密密钥。对监测日志、配置文件等普通数据采用软件加密方式，通过 SM4 算法进行全盘加密。同时设置密钥备份与恢复机制，定期将密钥备份至云端安全服务器，避免因终端物理损坏导致的数据丢失。

2.4 固件更新安全机制

固件更新安全机制需构建“可信分发、严格校验、可靠升级”的全流程防护体系，确保漏洞修复与功能升级过程的安全性，避免恶意固件植入。双分区更新策略将终端存储

区划分为活动分区与备份分区，活动分区存储当前运行的固件，备份分区用于存储待更新的固件。更新流程分为四个步骤：终端从云端获取加密的更新包，验证更新包的数字签名与完整性。将更新包解压后写入备份分区。对备份分区的固件进行完整性校验。校验通过后，通过修改分区表切换活动分区与备份分区，完成固件更新。更新过程中若发生断电、网络中断等异常情况，终端可从活动分区启动，保障设备正常运行[3]。

数字签名验证是固件更新的关键环节，更新包需由设备厂商通过私钥进行签名，终端通过预存的公钥验证签名有效性。公钥的存储需采用硬件保护方式，存储在 TPM 芯片或安全元件中，避免被篡改。针对输电终端的远程更新需求，可采用分级签名机制，省级电网公司对辖区内的终端更新包进行二次签名，确保更新包的来源可信。

回滚保护机制通过记录固件的版本信息与安全状态，限制终端回退至存在高危漏洞的旧版本固件。终端存储当前固件的版本号与安全等级，更新新固件后将版本信息写入不可修改的存储区域。当检测到回滚操作时，终端验证目标版本的安全等级，若低于当前版本则拒绝回滚。若因特殊需求必须回滚，需通过云端管理平台的授权验证，确保回滚操作的合法性。

3 输电场景下的安全加固实践

3.1 硬件安全模块集成

硬件安全模块集成针对输电终端野外部署的物理安全风险，通过专用安全芯片与防篡改设计，构建硬件级的安全防护屏障。安全元件（SE）的应用需选择符合 ISO 7816 标准的嵌入式安全芯片，该芯片具备独立的处理器、内存与加密引擎，可实现密钥生成、加密运算、证书存储等安全操作。在输电终端中，SE 芯片与主控芯片通过 SPI 接口通信，所有敏感操作均在 SE 内部完成，避免密钥在软件层的暴露。

物理防篡改设计需结合输电终端的部署环境，采用多重防护措施。在终端外壳安装光敏传感器与振动传感器，当检测到外壳被开启或剧烈振动时，立即触发篡改告警，同时通过 SE 芯片擦除存储的敏感数据。外壳材质采用高强度合金，表面进行防拆卸处理，增加物理拆解的难度。此外，终端的接口防护也需强化，对未使用的串口、JTAG 接口进行物理封堵，防止攻击者通过接口接入设备。

3.2 安全启动验证优化

安全启动验证优化需要平衡输电终端的安全需求与恶劣环境下的运行效率，通过动态调整验证策略，实现安全性与实用性的统一。快速启动模式的设计需根据终端的工作场景动态切换验证级别，在日常巡检等非关键场景下，采用精简验证流程，仅验证 Bootloader 与内核的签名，缩短启动时间。在故障处置、数据上传等安全敏感场景下，启用完整验证链，对所有模块进行完整性校验。验证策略的切换可通过云端指令或本地环境监测自动触发，例如当终端检测到网络连接异常时，自动启用完整验证模式。

远程验证支持通过构建云端验证服务器集群，实现对终端固件的实时可信度评估。终端启动时计算固件的哈希值，通过加密通道发送至云端服务器，服务器将该哈希值与预存的合法哈希值进行比对，返回验证结果。若验证失败，服务器向终端发送隔离指令，禁止终端接入电网通信网络。针对野外终端的网络不稳定问题，采用哈希值分片传输与断点续传技术，确保验证数据的可靠传输。

3.3 侧信道攻击防护

侧信道攻击防护针对输电终端的物理特征泄露风险，通过电磁屏蔽与功耗平衡设计，降低攻击成功率，保障固件的密钥安全与逻辑安全。电磁屏蔽设计需采用多层次防护方案，终端外壳内层铺设铜箔导电涂层，关键电路板采用屏蔽罩封装，减少电磁辐射泄露。同时优化电路板的布线设计，将加密模块与其他模块的线路分离，避免电磁耦合导致的信息泄露。屏蔽材料的选择需兼顾防护效果与散热性能，采用透气型导电材料，确保终端在高温环境下的正常散热[4]。

功耗平衡技术通过优化固件执行时序与电源管理策略，使终端的功耗曲线趋于平稳，掩盖密钥运算等关键操作的功耗特征。采用动态电压频率调节（DVFS）技术，根据终端的工作负载调整处理器频率，避免因高频运算导致的功耗突变。在加密算法执行过程中，插入伪操作指令，使功耗曲线保持稳定。同时采用基于硬件噪声的真随机数生成器（TRNG），为加密运算提供高质量的随机数，进一步提升功耗分析的难度。

4 结论

输电线路边缘计算终端固件安全是电网智能化建设关键。本文构建的技术体系，通过静态与动态分析精准挖掘固件漏洞、量化风险，以多层级加固策略构建全生命周期防护

屏障。实践应用显示，集成硬件安全模块、优化安全启动、强化侧信道攻击防护等措施，可提升终端抗攻击能力，降低安全事件发生率。随着新技术发展，固件安全面临新挑战，后续需深化技术与场景融合，优化检测与加固方案，推动技术迭代升级，为智能输电网络提供有力支撑。

参考文献：

[1] 王霞 . 基于双目立体视觉的输电线路导线覆冰厚度检测方法 [J]. 工业控制计算机 ,2025,38(8):60–62.

[2] 康宇昊 . 边缘计算在输电线路监测通信组网中的应用分析 [J]. 技术与市场 ,2024,31(11):50–5360.

[3] 姜岚 , 程若恒 , 唐波 , 智李 . 基于图像边缘识别的输电线路拉线塔拉线张力测试方法 [J]. 高电压技术 ,2022,48(11):4469–4477.

[4] 张姝 , 王昊天 , 董骁翀 , 李玉容 , 李烨 , 王新迎 , 孙英云 . 基于深度学习的输电线路螺栓检测技术 [J]. 电网技术 ,2021,45(7):2821–2828.

作者简介：刘彦昌（1985—），男，汉族，山东金乡，工程师，大学本科，研究方向电力工程。