中国科学院软件研究所学术年会'2022
暨计算机科学国家重点实验室开放周

工具系统

# 嵌入式可信防护系统

冯伟 李为 秦宇

冯伟 18810678038 fengwei2009@iscas.ac.cn

## 具体内容介绍

### 1. 系统简介

嵌入式可信防护系统是基于国产安全芯片、国密算法与可信计算机制实现的一套主动防护系统，面向智能装置与嵌入式设备提供主动识别、主动控制、主动报警等安全功能。该系统基于软硬件协同设计思想，使用可信引导、完整性度量、白名单管控、知识库收集、主动报警等技术，实现了一套贯穿硬件层、内核层和应用层的嵌入式系统整体安全加固方案。我们在QEMU模拟器、嵌入式开发板以及5款不同国产电力装置上完成了系统的集成与测试。系统安全功能开销在毫秒级别，对嵌入式应用本身的运行不造成影响。

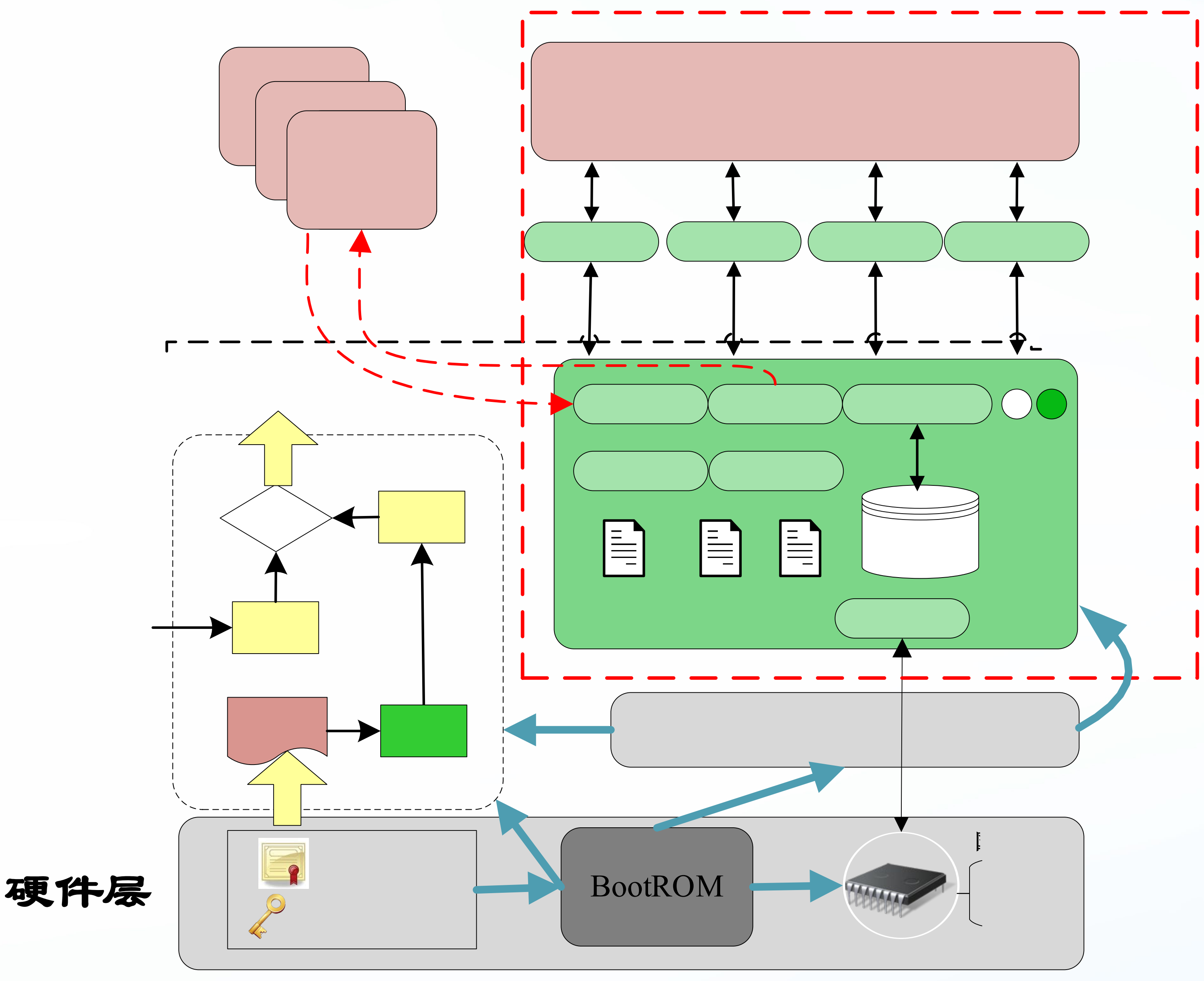

图1 系统架构

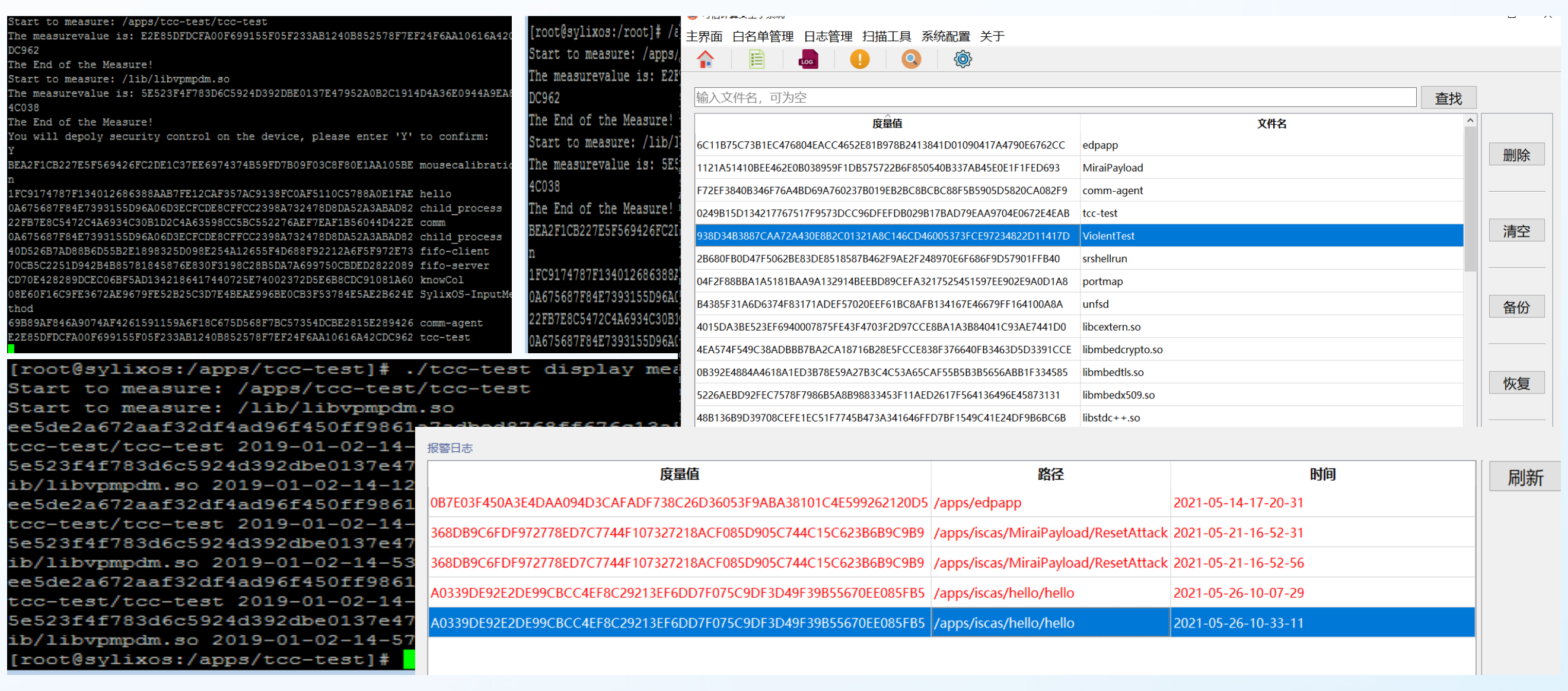

图2 系统运行与界面

### 2. 技术思路

① **初始配置**：设备出厂进行初始化白名单安全策略配置

② **可信引导**：一级度量一级，建立启动过程的信任链

③ **设备运行**：可信防护系统对设备运行的所有可执行代码进行度量与管控，只允许合法嵌入式应用运行；自动识别其他未知或者恶意程序，并进行阻断与主动报警；无人值守

④ **策略更新**：更新嵌入式应用，知识库扫描搜集

⑤ **攻防验证**：对Mirai恶意载体与攻击的防护验证

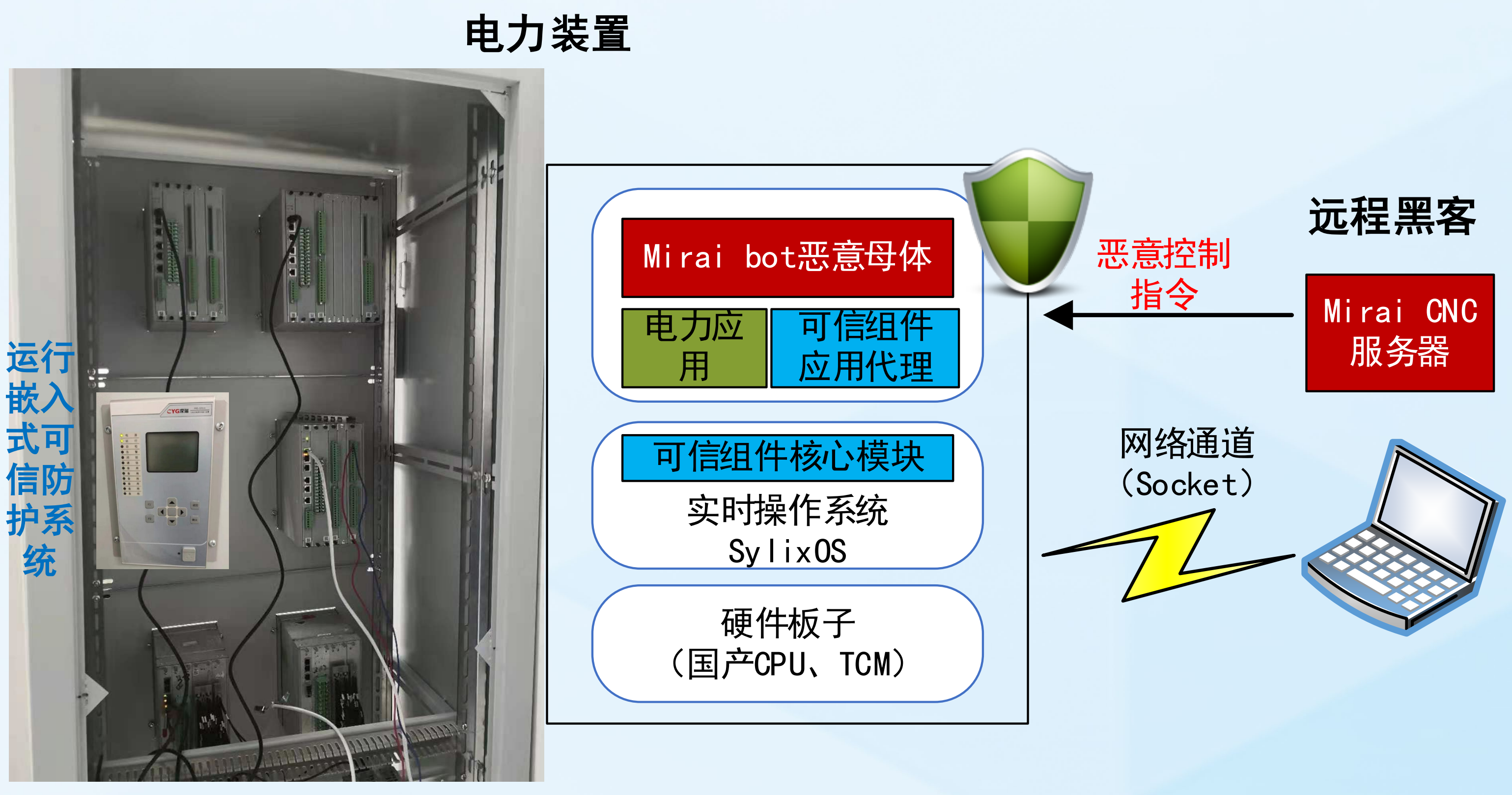

图3 五款电力装置与系统攻防验证

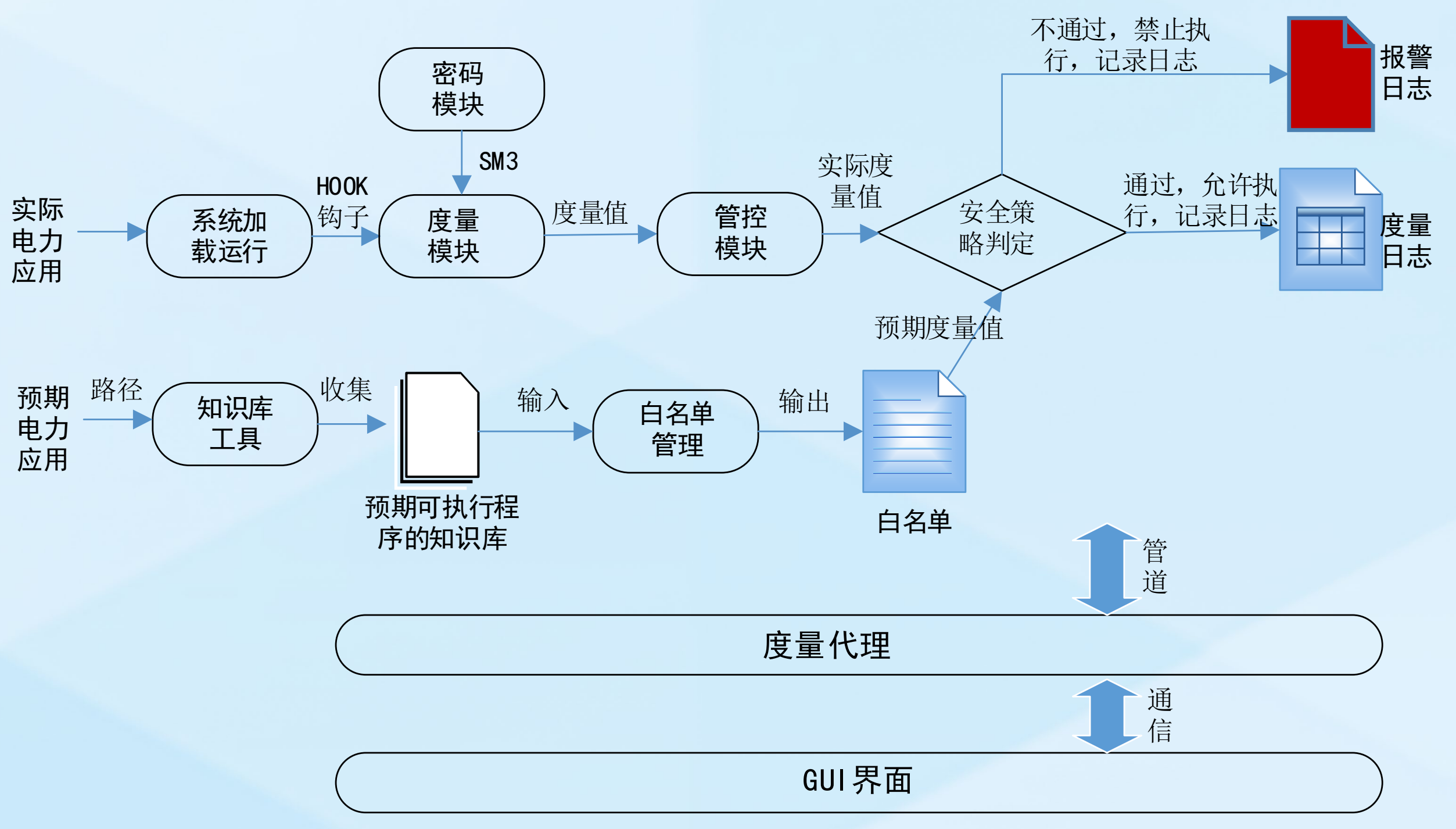

图4 度量管控