Firmware para Microarquitecturas de Algoritmia Embebida con Resiliencia

KK-2025/00047

Entregable E3.1

Informe de las necesidades de seguridad de arquitecturas embebidas con pocas prestaciones

<Versión 0.1>

31/12/2025

Proyecto subvencionado por el Departamento de Industria, Transición Energética y Sostenibilidad del Gobierno Vasco (Programa ELKARTEK 2025)
Eusko Jaurlaritzaren Industria, Trantsizio Energetiko eta Jasangarritasun Saila (ELKARTEK 2025 Programa) finantziatutako proiektua
Project funded by the Department of Industry, Energy Transition and Sustainability of the Basque Government (ELKARTEK 2025 Programme)

Resumen ejecutivo

Los dispositivos con recursos limitados (RCD) son componentes esenciales en la operación del sector eléctrico, desempeñando funciones críticas como la monitorización, el control y la protección de la red. Sin embargo, estas arquitecturas presentan importantes restricciones en cuanto a capacidad de procesamiento, memoria, consumo energético y conectividad, lo que dificulta la implementación de medidas de ciberseguridad robustas. En un contexto de creciente digitalización y conectividad, estas limitaciones convierten a los RCD en objetivos especialmente vulnerables frente a ciberataques, con potencial impacto en la estabilidad y seguridad de infraestructuras críticas.

En este entregable, correspondiente al PT3 del proyecto FIRMAR, se analizan los requisitos normativos y técnicos aplicables a los RCD, se identifican los principales retos para su cumplimiento y se proponen soluciones adaptadas que permitan garantizar la ciberresiliencia en entornos eléctricos. El análisis se centra fundamentalmente en el Reglamento Europeo *Cyber Resilience Act* (CRA), que establece requisitos para todos los productos con elementos digitales, así como en normas internacionales como IEC 62443 e IEC 62351, ampliamente adoptadas en entornos industriales y eléctricos.

El CRA, en vigor desde diciembre de 2024 y de aplicación completa en diciembre de 2027, introduce un cambio estructural en la forma en que los fabricantes deben abordar la ciberseguridad. Entre sus exigencias destacan el diseño seguro por defecto y por diseño, la gestión activa de vulnerabilidades, la provisión de actualizaciones seguras durante todo el ciclo de vida y la obligación de emitir declaraciones de conformidad acompañadas del marcado CE. Estas obligaciones se complementan con los requisitos definidos en la serie IEC 62443, que establece controles específicos para sistemas industriales, y en la IEC 62351, que regula la protección de protocolos críticos en redes eléctricas.

Cumplir con estas normativas en dispositivos RCD supone un desafío considerable. Las limitaciones de hardware, la ausencia de módulos seguros (TPM, HSM), la escasa memoria y la conectividad restringida dificultan la implementación de mecanismos como cifrado robusto, autenticación multifactor, monitorización continua o segmentación interna. Además, el ciclo de vida prolongado de estos dispositivos y su operación en entornos extremos añaden complejidad a la gestión de actualizaciones y a la protección frente vulnerabilidades emergentes.

El análisis realizado además identifica amenazas que pueden comprometer gravemente la disponibilidad, integridad y confidencialidad de los sistemas eléctricos. Entre ellas destacan los ataques de denegación de servicio (DoS/DDoS), la manipulación de datos críticos, la interceptación de comunicaciones (MITM), la explotación de vulnerabilidades de firmware y los ataques a la cadena de suministro. Estas amenazas pueden derivar en interrupciones operativas, pérdidas financieras, riesgos para la seguridad física y sanciones regulatorias, además de un impacto reputacional significativo.

La probabilidad y el impacto de estas amenazas son elevados en entornos donde los RCD carecen de mecanismos avanzados de protección. Por ejemplo, la explotación de firmware vulnerable puede permitir la instalación de malware persistente, mientras que la ausencia de cifrado en protocolos industriales facilita ataques MITM que comprometen comandos críticos. La falta de segmentación y control de interfaces incrementa la superficie de ataque, favoreciendo movimientos laterales dentro del dispositivo y la red.

Para mitigar estos riesgos, se propone un conjunto de estrategias adaptadas a las limitaciones de los RCD. Entre ellas se incluyen el uso de criptografía ligera (algoritmos optimizados como ASCON o PRESENT), la implementación de *Secure Boot* simplificado mediante raíces de confianza mínimas (ROM, e-Fuses), y la adopción de actualizaciones diferenciales que reduzcan el consumo de memoria y energía. Asimismo, se recomienda aplicar técnicas como el hash encadenado para garantizar la integridad de registros sin necesidad de bases de datos complejas, y mecanismos de segmentación funcional mediante *namespaces*, cgroups o entornos seguros (TEEs).

Por otro lado, es fundamental integrar los RCD en redes segmentadas, aplicar políticas de puerto cerrado por defecto y controlar el acceso a interfaces físicas y lógicas. La autenticación ligera

basada en HMAC puede ser una alternativa viable cuando no sea posible implementar certificados o PKI. Además, se aconseja delegar la gestión de identidades y roles en sistemas externos (IAM), reduciendo la carga sobre dispositivos con recursos limitados.

La evolución hacia modelos como Zero Trust, la actualización de los equipos mediante parches, y el uso de inteligencia artificial para la detección de anomalías, marcarán el futuro de la ciberseguridad en entornos OT. La virtualización ligera mediante contenedores seguros (por ejemplo, tecnologías basadas en WebAssembly) permitirá aislar funciones críticas sin comprometer la estabilidad del sistema. Asimismo, la preparación para la criptografía post-cuántica, aunque aún incipiente, será clave para anticipar amenazas futuras.

Como conclusión, la ciberseguridad en dispositivos con recursos limitados no es opcional, constituye un requisito estratégico para garantizar la continuidad del servicio eléctrico y la protección de infraestructuras críticas. Cumplir con el CRA y con estándares internacionales como IEC 62443 e IEC 62351 exige soluciones innovadoras que equilibren seguridad y rendimiento, apoyadas en diseño seguro, segmentación, criptografía optimizada y gestión eficiente de vulnerabilidades. Solo mediante un enfoque integral y proactivo será posible alcanzar la resiliencia operativa que demanda el sector eléctrico en un entorno cada vez más digital y conectado.