

CÓMO ASEGURAR LA CIBERSEGURIDAD. LA IMPORTANCIA DE LA CERTIFICACIÓN Y DE LA CORRECTA DEFINICIÓN DE REQUISITOS DE CIBERSEGURIDAD PARA ASEGURAR UN ENTORNO CIBERSEGURO

Marta Castro, Saioa Bilbao, Libertad Moro, Mikel Vergara

⁽¹⁾ TECNALIA, Parque Científico y Tecnológico de Bizkaia Astondo Bidea, Edificio 700 E-48160 Derio, Bizkaia (Spain)

⁽²⁾ +34 667 17 89 14, marta.castro@tecnalia.com

RESUMEN: Los sistemas AMI (Infraestructura de Medición Avanzada) han evolucionado hacia sistemas más complejos. Esta evolución permite incluir comunicaciones e intercambio de datos. Esta inteligencia y comunicaciones permite una gestión más eficiente de la red, sin embargo, el hecho de tener múltiples puntos de acceso a los equipos de la red incrementa el riesgo y aumenta la exposición ante ciberataques.

Los contadores contienen información de carácter confidencial de millones de usuarios y es importante asegurar la confidencialidad de los datos, así como la integridad del remitente de las peticiones.

La ciberseguridad y la interoperabilidad de las soluciones de diferentes fabricantes es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI y, en consecuencia, resulta prioritario definir una metodología que asegure la calidad de los equipos desplegados. Esta metodología parte de la correcta definición de requisitos, hasta la certificación final de los productos.

1. INTRODUCCIÓN

Los sistemas AMI han evolucionado hacia sistemas complejos que incluyen comunicaciones e intercambio de datos. Esta inteligencia adicional e inclusión de comunicaciones permite una mayor flexibilidad y una gestión más eficiente de la red, así como tener una mayor información de las incidencias, eventos, alarmas y hábitos de consumo. Es decir, la digitalización de las Smart Grids, incluyendo comunicaciones, permiten una gestión más eficiente de la red ofreciendo mayor calidad de servicio a los clientes y servicios de valor añadido. Sin embargo, como consecuencia de esta mayor inteligencia y comunicaciones en los sistemas, se incrementan considerablemente los puntos de acceso a los equipos de la red, implicando que exista un mayor riesgo y una mayor exposición ante ciberataques.

Los contadores contienen información de carácter confidencial de millones de usuarios, por lo que resulta sumamente importante el aseguramiento la confidencialidad y la integridad de los datos y remitentes de las peticiones, tanto para evitar acceso a dicha información, como para bloquear una potencial suplantación de identidad y ataques a mayor escala. No obstante, es preciso llegar a un compromiso entre el nivel de seguridad y la combinación de velocidad-disponibilidad de los datos requeridos para cada caso de uso. Es por tanto, muy importante analizar las diferentes casuísticas y funcionalidades que existen en la red y los diferentes niveles de seguridad con los que se puede securizar los equipos y los sistemas.

La ciberseguridad y la interoperabilidad de las soluciones de diferentes fabricantes es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI, de forma que es muy importante definir una metodología que asegure la calidad de los equipos desplegados. Esta metodología parte de la correcta definición de requisitos, hasta la certificación final de los productos.

2. DESARROLLO/DESCRIPCIÓN

Asegurar la ciberseguridad de las soluciones de diferentes fabricantes es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI, por este motivo es muy importante definir una metodología que asegure la calidad de los equipos desplegados. Esta metodología parte de la correcta definición de requisitos, hasta la certificación final de los productos.

2.1. Estado del arte

La automatización de las Smart Grids y los sistemas AMI permite una mejor gestión, mayor eficiencia y calidad de servicio. Sin embargo, requiere de sistemas de protección específicos para evitar ciberataques.

En los últimos años, se ha pasado de una red eléctrica tradicional donde apenas existían comunicaciones, siendo necesaria la presencia física de personal técnico para el mantenimiento, análisis de fallos, lectura de eventos y alarmas o lectura de consumos para tarificar... a una red eléctrica y un sistema AMI inteligente donde las comunicaciones, los datos y la tecnología, posibilitan la gestión centralizada y reducen el factor humano en tareas de menor valor añadido.

La situación actual implica un aumento de la inteligencia en la red, que a su vez provoca que el sistema esté más expuesto ante ciberataques. Además, existen otros factores tales como el incremento de puntos de acceso a equipos, la falta de definición de exigencias regulatorias, el incremento y aparición de nuevas tecnologías y protocolos de comunicaciones no maduros en el mercado, que provocan incertidumbres en el entorno y mayores riesgos de vulnerabilidad.

Adicionalmente, a diferencia de otros sectores industriales, el sector eléctrico tiene ciertas condiciones y requisitos de operación que implican el desarrollo de soluciones novedosas y específicas en el campo de la ciberseguridad, por ejemplo:

- Necesidad de mantenimiento de servicio en activo, a pesar de encontrarse en situaciones de ataque.
- Elevada exigencia a los equipos en lo que respecta a tiempos de respuesta.
- Dispersión geográfica y de equipos.

Ante esta situación, los fabricantes, compañías eléctricas y distribuidoras se plantean qué requisitos o estándares de ciberseguridad deben cumplir los equipos, qué requisitos de ciberseguridad se deben pedir a los fabricantes de equipos, y posteriormente, cómo asegurar la verificación del correcto cumplimiento de dichos requisitos en los equipos.

Ante esta situación de incertidumbre para fabricantes, distribuidoras y clientes, resulta de vital importancia proporcionar una solución metodológica que responda a todas las incógnitas, permitiendo abordar de forma exitosa el desarrollo de producto y el despliegue ordenado en campo, asegurando la calidad de los equipos y entornos.

2.2. Problemáticas y necesidades del sector

Las problemáticas del sector eléctrico se dividen en tres grandes grupos:

- Regulatorios

Cualquier equipo que se instale en campo tiene que cumplir la normativa y directivas existentes. Sin embargo, a día de hoy, existe una falta de estandarización y nivel de detalle adecuado de la actual normativa. Además, resulta complejo el cumplimiento en paralelo tanto de las normativas genéricas, como los requisitos particulares definidos por los prescriptores, normalmente compañías eléctricas.

- Capacitación del personal

La capacitación del personal es clave en el camino hacia la ciberseguridad. Todas las personas de la empresa han de ser partícipes de este cambio y sentirse uno más del proceso de cambio. Sin embargo, actualmente existe un gran desconocimiento y el conocimiento está segmentado entre las áreas OT (Tecnologías de Operación) e IT (Tecnologías de la Información). Resulta de vital importancia la integración de OT y IT para definir un sistema ciberseguro y robusto ante ataques.

Por otro lado, es importante destacar que las soluciones del mundo IT no siempre son aplicables al mundo OT y, por tanto, hay que realizar un estudio previo sobre los parámetros y requisitos que se deben priorizar; Disponibilidad vs. Confidencialidad, Tiempos de respuesta mucho más exigentes y Dispersión geográfica y de equipos...

Por último, resulta conveniente destacar la tendencia hacia la transición de soluciones tecnológicas cloud. Si bien es cierto que disponen de características interesantes que permiten reducir costes, incrementar flexibilidad y ubicuidad, potenciar el análisis de datos y fomentar la colaboración entre diferentes actores, no hay que perder de vista que añade nuevos desafíos en ciberseguridad, siendo todavía más necesario la adquisición de conocimientos relacionados por los equipos de desarrollo de las compañías.

- Mantenimiento y despliegue

La transición hacia la red eléctrica inteligente no es algo inmediato ni sencillo. En la mayoría de ocasiones no se realiza un despliegue partiendo de cero, sino que se trata de redes ya desplegadas, siendo necesario realizar una migración paulatina en la que convivirán equipos tradicionales con otros actualizados, y será necesario analizar la viabilidad de las soluciones teniendo en cuenta la interoperabilidad entre equipos.

Además, la transición hacia sistemas AMI implica cambios relevantes en lo que respecta a la gestión de los ciclos de vida de los activos. Estos ciclos de vida se ven acortados, y resulta necesario abordar y definir un nuevo modelo de gestión de riesgos, actualizaciones, parches y procesos de resolución de incidencias, que tenga en cuenta las nuevas funcionalidades digitales de los equipos, con especial hincapié en el mantenimiento de los más altos estándares de ciberseguridad.

2.3. Soluciones ante las necesidades del sector

Las necesidades y problemáticas del sector obligan a abordar soluciones específicas para cada uno de los tres grandes bloques identificados.

- Regulatorios

En el ámbito de la regulación y la estandarización es importante elaborar un análisis de vulnerabilidades del sistema y del equipo. además, es crítico el estudio de los diferentes protocolos, estándares, normativas, requisitos genéricos y requisitos particulares con el objetivo de elaborar una especificación particular que recoja todos los requisitos adaptados a las necesidades del cliente.

- Capacitación del personal.

La formación del personal tanto en los aspectos regulatorios como en la especificación particular que resuma los requisitos particulares del cliente es clave para asegurar que todas las personas de la empresa son conscientes de la importancia y necesidad de la ciberseguridad.

- Mantenimiento y despliegue.

De cara a asegurar el correcto mantenimiento y despliegue de las soluciones y de los equipos es necesario elaborar y definir unos procedimientos de ensayos que recojan de forma detallada los pasos a realizar para comprobar y verificar cada uno de los requisitos de la especificación dando lugar a la certificación del producto.

Sin embargo, y aunque las soluciones puedan parecer sencillas es importante plantearlas cómo parte de una metodología global, en la se defina y acompañe al cliente desde la idea hasta el correcto despliegue de las soluciones en campo. Este procedimiento ayudará a asegurar que las soluciones, productos y sistemas cumplen con la calidad suficiente para dar un servicio óptimo a los usuarios, asegurando también la ciberseguridad de los datos y la interoperabilidad de las soluciones.

3. RESULTADOS Y DISCUSIÓN

Asegurar la ciberseguridad y la interoperabilidad de las soluciones de diferentes fabricantes es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI, de forma que es importante definir una metodología que minimice y reduzca los problemas derivados del sector, asegurando al mismo tiempo la calidad de los equipos desplegados. Esta metodología (Figura 1) parte de la correcta definición de requisitos, hasta la certificación final de los productos.

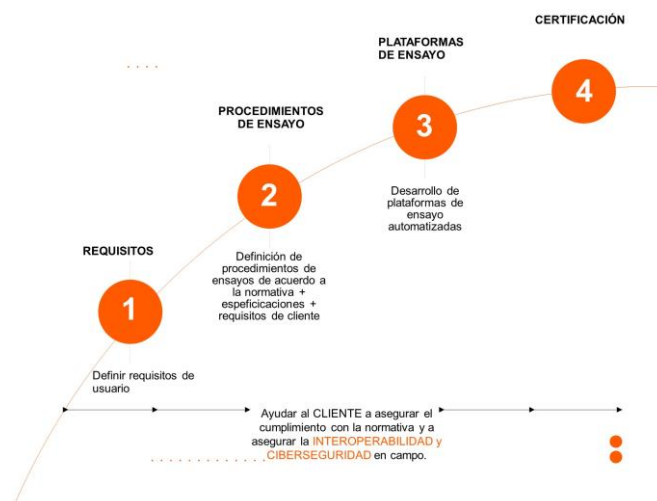


Figura 1

3.1. Definición de Requisitos

La definición de requisitos es el primer paso para asegurar la calidad de las soluciones. Como se ha comentado en los apartados anteriores, una de las problemáticas que existen actualmente es la falta de regulación y la existencia de requisitos genéricos y poco precisos. De forma que, es clave una correcta definición de requisitos aplicables a cada cliente, producto y caso de uso.

Una definición detallada de requisitos implicará, analizar la normativa aplicable y las especificaciones de producto, así como el entorno en el que se va a instalar el producto o sistema. Además, de analizar los requisitos específicos que deben cumplir de acuerdo con las características particulares del cliente, con el objetivo de definir un documento de requisitos adaptado a las necesidades del cliente.

Los requisitos clave de ciberseguridad en los sistemas AMI se basan en:

- El control de acceso basado en roles: es necesario definir la información a la que van a tener acceso los diferentes roles y con qué nivel de permisos. Es decir, hay que detallar la lista de objetos y sus derechos de acceso.
- La encriptación para garantizar la confidencialidad.
- La autenticación para verificar el origen y la integridad de los mensajes.
- La gestión de las claves de ciberseguridad.
- Registros de eventos de seguridad.
- Medidas y registros ante fraudes y ataques de ciberseguridad.

3.2. Definición de procedimiento de ensayos

A continuación, y como segundo paso, hay que definir un procedimiento de ensayos donde se indique de forma detallada cómo se va a verificar cada uno de los requisitos o aquellos que aseguren al menos la funcionalidad mínima requerida.

De esta forma, se asegura por un lado el cumplimiento de los requisitos del cliente, y por otro, el hecho de que todos los laboratorios ensayan y aplican las pruebas siguiendo el mismo procedimiento y se certifica con un entorno de pruebas y equipamiento de ensayos común a todos los laboratorios.

3.3. Creación de entornos de ensayos

El tercer paso en la metodología es crear el entorno de ensayos con el objetivo de aplicar el procedimiento de ensayos de una forma rigurosa que asegure la calidad del proceso de certificación. En este punto se puede proceder de dos formas diferentes:

- Certificación manual: el técnico de ensayos comprueba de forma manual cada uno de los requisitos. Esto implica dependencia 100% del conocimiento del técnico de ensayos, y pone en peligro la repetitividad de los ensayos.
- Certificación automatizada: Se crea una plataforma de ensayos automatizada, que controla todos los equipos auxiliares necesarios para la certificación de una forma automática, con lo que se consigue independencia del técnico de ensayos, repetitividad en los ensayos, reducir el tiempo de ensayos, ya que esto permite que sea la propia

plataforma de ensayos la que analice los logs y presente el resultado de cumplimiento o incumplimiento frente al requisito, con lo que se pueden dejar ensayos ejecutándose incluso sin técnico de ensayos presente. Adicionalmente, estas herramientas de ensayos almacenan gran cantidad de logs, evidencias e información que ayuda a la depuración del fallo en caso de que se produzca.

3.4. Certificación

La certificación de ciberseguridad es el único medio objetivo que permite valorar y acreditar la capacidad de un producto o sistema para manejar información de forma segura. Además, permite dar conformidad a requisitos de ciberseguridad según estándares europeos o internacionales o requisitos de cliente.

Para definir el esquema de certificación es necesario contar con un “Organismo Nacional de Acreditación”, rol desempeñado en España desempeña ENAC, organismo con potestad de acreditación a empresas como Entidades Evaluadoras (por ejemplo, Tecnalía).

Una vez resueltas las no conformidades durante las pruebas de ciberseguridad del proceso de certificación, en el caso de que las hubiera, la Entidad Evaluadora es la responsable de certificar la ciberseguridad del sistema AMI, de acuerdo con un proceso de evaluación y dando conformidad a unos requisitos de ciberseguridad basados en estándares europeos o internacionales. Para cerrar el proceso, la Entidad Evaluadora emite un informe de certificación donde se recoge el resultado de todas las pruebas, así como el entorno de ensayos y equipos auxiliares utilizados en el proceso de certificación.

Cabe destacar que, la certificación realizada por un laboratorio de ensayos se trata de una Certificación tipo, que asegura el cumplimiento de los requisitos de ciberseguridad para un modelo de equipo con versión software (SW) y hardware (HW) específica. De forma que, cualquier cambio de firmware (FW), SW o modificación HW requiere de la actualización de la certificación. Además, y derivado de esto, es importante definir unos ensayos mínimos que aseguren la calidad y la funcionalidad del equipo, de forma que facilite las recertificaciones y ante cualquier cambio de FW como mínimo se realicen esta batería reducida de pruebas que a su vez garantizan la calidad de los requisitos básicos.

4. CONCLUSIONES

La ciberseguridad es un aspecto crítico que ha de ser tenido en cuenta desde el inicio del desarrollo del producto, es decir, desde la concepción de la idea hasta el despliegue de la solución en campo. De forma que es importante definir una metodología o procedimiento que asegure que todos los aspectos relevantes que pueden poner en riesgo la ciberseguridad del sistema se han analizado y certificado.

Por otro lado, el sector eléctrico se trata de un sector diferencial con condiciones de operación exigentes, donde las medidas y requisitos a definir han de adaptarse a las necesidades de los tiempos de respuesta y la criticidad del sector.

Y por último, los contadores contienen información de carácter confidencial de millones de usuarios y es importante asegurar la confidencialidad de los datos, así como la integridad del remitente de las peticiones.

La ciberseguridad es algo crítico para el correcto despliegue y funcionamiento de los sistemas AMI, de forma que es muy importante definir una metodología que asegure la calidad de los equipos desplegados. Esta metodología parte de la correcta definición de requisitos, hasta la certificación final de los productos