¿Cómo implementar una administración de seguridad eficiente en el Desarrollo del Producto?

Realizado por Wolfgang Reinelt y Michel Bonnet

Resumen Ejecutivo

Un aspecto vital en el desarrollo del producto es demostrar que dicho producto, solución o servicios está seguro antes de comercializarse. La manera en que se manejan las consideraciones de seguridad, afecta en gran parte a la eficiencia, el programa y el costo del proyecto. Este ensayo proporciona un enfoque lógico de administración para la seguridad en el desarrollo del producto. Se discuten los métodos para organizar los argumentos y la evidencia relacionada con la seguridad. Se proporciona un ejemplo para saber como presentar un caso de seguridad por medio de Goal Structure Notation (GSN).

998-2095-06-16-15AR0

Schneider Electric

Introducción

¿Cómo es que los fabricantes dentro de las industrias ferroviaria, automotriz y aeronáutica demuestran que un determinado producto, parte, solución o servicio es seguro? Es necesario construir un "caso" de seguridad alrededor de la evidencia de tal manera que los reguladores y/o certificadores estén convencidos de la validez de cualquier exigencia de seguridad. De igual manera, la evidencia necesita estar plasmada no sólo en papel, sino que tambien necesita aplicarse a situaciones de la vida real.

La certificación es un parteaguas importante que debe alcanzar cualquier fabricante que espera comercializar su producto eventualmente. Si los fabricantes o certificadores no pueden garantizar la seguridad del producto, ésto puede resultar en la pérdida de la vida y la pérdida de ingresos (por acciones legales y pérdida de confianza del cliente).

En lo que respecta a la administración de la seguridad, la evaluación mediante valoración independiente, es uno de los requisitos centrales de la práctica de seguridad funcional. Con el fin de ayudar a preparar a los accionistas para llevar a cabo una administración de seguridad apropiada, este ensayo describe una metodología llamada Goal Structure Notation (GSN), y abarca también los lineamientos de seguridad que se enfatizaron en las especificaciones IEC61508.

Cuando se aplican las normas IEC61508, los fabricantes necesitan mostrar que se ha valorado el riesgo, que se han definido y cumplido los requisitos y que se han planeado y llevado a cabo las actividades para la administración de seguridad. Es necesario que estas tareas hayan sido realizadas por personas con las competencias y la experiencia apropiada. Es tambien necesario presentar la evidencia al asesor independiente durante el curso del desarrollo de un producto, con el fin de asegurarle al que el producto o sistema que se está desarrollando es aceptablemente seguro. Al final del proyecto, cuando todos o cualquiera de los puntos indicados por el asesor hayan sido abordados, se emitirá un informe por parte del mismo, con el fin de presentar los resultados de la valoración independiente.

La construcción de este " caso de seguridad" es progresiva, a medida que el desarrollo del producto vaya avanzando a lo largo de las diferentes etapas del proyecto al proporcionar pruebas en cada una de las etapas de que los riesgos de seguridad se han reducido a un nivel aceptable. El caso de seguridad recopila momentos, al presentar evidencias de los aspectos cualitativos y cuantitativos de la seguridad funcional. Este enfoque se centra no sólo en los aspectos tecnológicos del producto en cuestión, sino también en el proceso, en el método y en el cumplimiento de las prácticas que incluye la oferta (ver Figura 1).

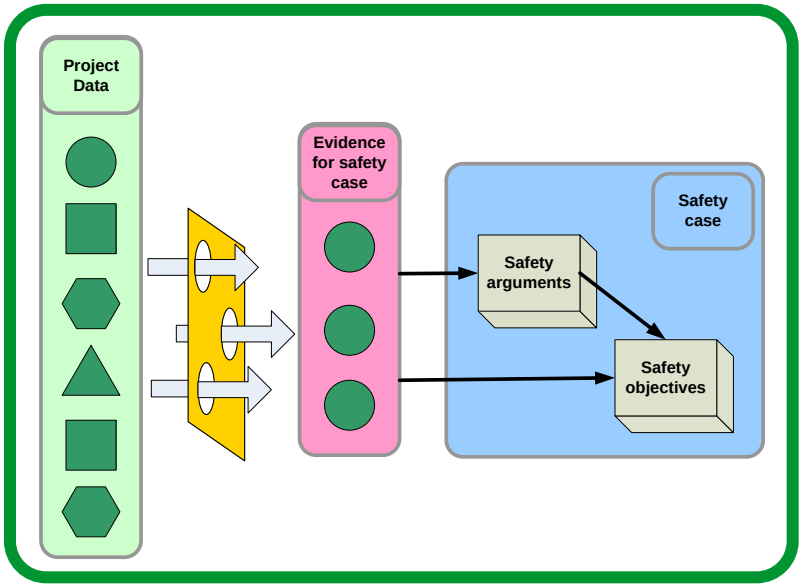

Figura 1
El cuerpo de la evidencia para un caso de seguridad se obtiene de los datos del proyecto.

La ejecución de una metodología de un caso de seguridad presenta ventajas múltiples:

- La argumentación y la documentación se organiza y estructura para que el accionista pueda tener acceso a la información rápida y fácilmente. Dicha estructura también facilita la revisión y los retos de otros.
- El proceso invita a que haya debates y se aclaren las suposiciones.
- El enfoque va más allá de la tecnología,al introducir un análisis del proceso, los métodos y el cumplimiento.
- Además, formaliza la aprobación de la empresa y el proceso de evaluación independiente.
- Funge como base para la administración de cualquier cambio.

Caso de seguridad vs certificación

Dentro del campo de los productos, la **certificación** es el proceso de declaración por medio del cual se cumplen los requisitos especificados para un producto.[1] La certificación se lleva a cabo por los individuos u organizaciones de terceros que no proveen y no consumen el producto. Un certificado es el entregable (o resultado) de este proceso. A menudo, la certificación se lleva a cabo en tres etapas:

1. El proveedor del producto expide un informe de revisión que contiene evidencia de seguridad y lo entrega al certificador.
2. Un informe técnico que detalla los requisitos cumplidos por el producto que aborda las preguntas de cómo y por qué dichos requisitos cumplidos también se entregan.
3. La emisión de un certificado que está disponible para clientes o consumidores del producto. A menudo, un certificado consiste en una sola página que enlista los requisitos que se han cumplido de acuerdo con las normas internacionales.

Tabla 1
Elementos que se presentan en un documento típico de caso de seguridad.

Los elementos de un caso de seguridad	
Resumen ejecutivo	Arreglos de emergencia y contingencia
Definición del sistema y resumen de descripción	Información operacional**
Suposiciones	Informe de evaluación de seguridad independiente
Progreso contra el programa designado de seguridad	Conclusiones y recomendaciones
Conformidad con los requisitos de seguridad*	Referencias

* Consiste en los requisitos de seguridad, metas y objetivos; resumen del argumento y evidencia que muestre cómo han sido/serán cumplidos todos los requisitos que son poco probables de cumplir con acciones correctivas; acciones sobresalientes para la administración de riesgo; riesgos residuales, aprobación regulatoria y restricciones asociadas; arreglos de retroalimentación para defectos y deficiencias; problemas de interfaz con otros sistemas.

** Alcance operacional, limitaciones y capacidad operacional; así como principales áreas de riesgo.

Las **evaluaciones funcionales de seguridad** son diferentes a los certificados, en el aspecto de que dan mayor énfasis a los niveles de integridad y consecuencias de la seguridad. Así como la certificación, se busca que una persona, departamento u organización lleve a cabo una evaluación. Sin embargo, esta "organización diferente" no es necesariamente un

[1] Tal como definió la IEC dentro del Vocabulario Electrotécnico Internacional (IEV, por sus siglas en inglés) en la página http://www.electropedia.org/

tercero en el mismo sentido que una certificación, ya que la evaluación de la seguridad funcional sólo decreta que el evaluador es "distinto y aparte, por la administración y otros recursos" (IEC61508-43.813). Por ejemplo, en el caso de una evaluación de seguridad funcional, un cliente puede estar evaluando a un proveedor.
A pesar de que la actividad de la evaluación puede ser la misma, está no califica como una certificación.

Un **caso de seguridad** (vea la **Tabla 1**) es más un argumento estructurado, respaldado por un órgano de evidencia que proporciona un caso persuasivo, comprensible y válido acerca de que un sistema es seguro para una aplicación y entornos determinados. Un informe del caso de seguridad es un entregable que resume un momento en particular. El informe del caso de seguridad enfatiza áreas de riesgo del proyecto relacionadas con la seguridad, la cuales requieren la atención de la gerencia y ofrecen la visión y el estatus del caso de seguridad a los accionistas.

Muy a menudo, los casos de seguridad son producidos por los contratistas o por los proveedores del producto y, por lo general, utilizan la redacción que se utiliza en las certificaciones. Sin embargo, como no son interpretados por un tercero, no pueden fungir como una certificación, pero sí pueden facilitar la certificación, al proporcionar los argumentos necesarios para obtenerla. Un caso de seguridad puede fungir como la base para la aprobación de una empresa y/o una evaluación independiente. Note que un informe de evaluación de seguridad (funcional) independiente, tal como se define con anterioridad, es un subgrupo del informe del caso de seguridad.

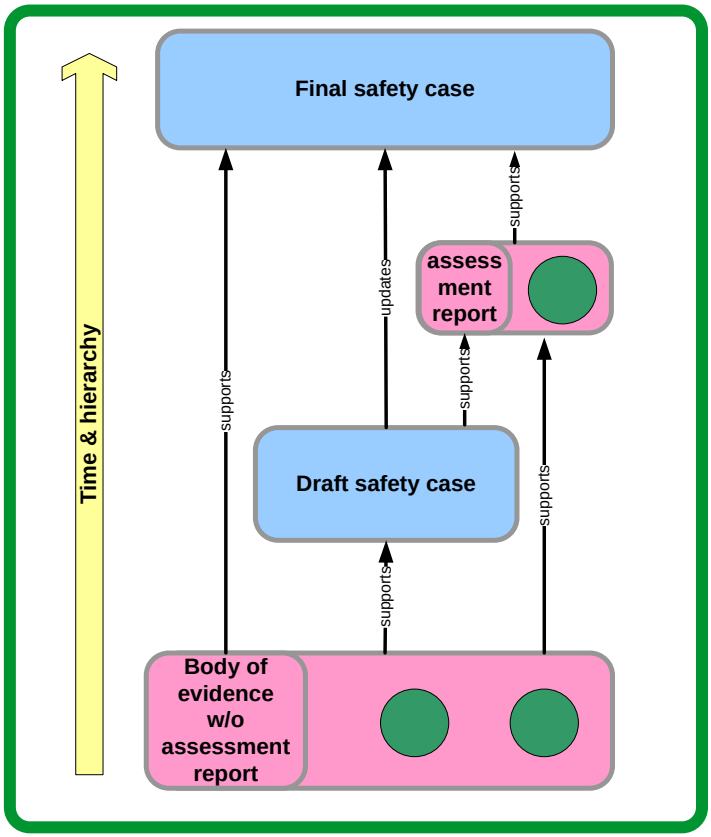

Figura 2
Etapas de integración del caso de seguridad y los resultados del informe de evaluación

Construir el caso de seguridad

El trabajo para armar un caso de seguridad consiste en seleccionar y recopilar las evidencias de seguridad apropiadas que comprobarán que todos los requisitos de seguridad han sido cumplidos. Estos requisitos de seguridad pueden clasificarse en las dos categorías siguientes:

- **Requisitos técnicos** - Aún si la norma IEC 61508 requiere una investigación profunda, las evidencias de seguridad serán proporcionadas por los entregables sobre el ciclo de vida útil del desarrollo del proyecto, incluyendo especificaciones, diseño y resultados de las pruebas.
- **Requisitos de proceso** - La norma IEC 61508 proporciona varias tablas que pueden utilizarse para seleccionar las medidas adecuadas para el nivel de integridad de la seguridad que pretende alcanzarse. Una vez que se seleccionó el grupo de técnicas y métodos, estos deben ejecutarse durante las fases del ciclo de vida útil del proyecto. La gestión de calidad del proyecto y los entregables del mismo, entonces, ayudarán a mostrar que todas las mediciones planeadas han sido aplicadas de manera exitosa.

Dependiendo del tamaño del producto, la complejidad o la novedad, las evidencias de seguridad pueden recopilarse a partir de diferentes contribuyentes y pueden variar en formato y cantidad. Como resultado, los argumentos y las consideraciones de seguridad son discutidos entre los diferentes contribuyentes y el equipo de administración de seguridad funcional o el equipo de certificación (en caso que un fabricante o proveedor se encuentre en la fase de obtener una certificación requerida por un tercero).

Se organiza y estructura un buen informe de caso de seguridad, de manera que presente consideraciones, argumento y evidencia. Un buen informe responde claramente a la pregunta "¿por qué su producto es seguro?" Al involucrar tanto a los accionistas como a los diseñadores de productos en proceso de casos de seguridad, los diseñadores se fuerzan de manera predeterminada con el fin de aprender cómo y por qué sus productos son aceptablemente seguros (o no seguros). Esto los invitará a tener más cuidado con la seguridad en sus diseños actuales y futuros. De igual manera, la administración obtendrá el conocimiento claro de los riesgos y las responsabilidades que involucra el traer un producto al mercado.

"Un buen informe responde claramente a la pregunta ¿por qué su producto es seguro?"

Entre más estructurada esté la documentación y la argumentación, será más fácil manejar los cambios (tales como: la evolución de las normas de seguridad, los cambios en el diseño o las actualizaciones de las operaciones del producto) y llevar a cabo un análisis rápido del impacto de la seguridad.

En la práctica, las diferentes fases del análisis de seguridad, a menudo, son llevadas a cabo por diferentes equipos. Cada uno de los equipos busca la manera de mejorar la seguridad dentro de su propio dominio y cumple con los niveles de seguridad establecidos. Este documento del caso de seguridad funge como un catalista que conecta todas las partes y argumenta cómo cada una de las prácticas o actividades contribuye con los objetivos de seguridad. La generación del caso de seguridad puede actuar como una herramienta para administrar la complejidad. Las diversas tareas, tales como: los requisitos de ingeniería, el desarrollo de software y hardware y las pruebas, pueden armonizarse desde una perspectiva de seguridad. El caso de seguridad ayuda a conectar todas las partes y a enfocarlas todas al mismo grado. Durante el ejercicio de documentación, la debilidad se vuelve visible y puede ser abordada por el proyecto actual y compensada para cuando se realicen los proyectos futuros.

Sin embargo, el objetivo final es producir un caso de seguridad completo, que se resume en un informe de caso de seguridad. La información que se encuentra en el informe es sustentada por evidencias de seguridad que cumplen con los requisitos regulatorios y demuestran que el producto es aceptablemente seguro y está listo para comercializarse.

Reducción de riesgos

Aquellos que buscan un caso de seguridad deben estar conscientes de dos factores. En primer lugar, no todas las plantillas de los casos de seguridad se encuentran estandarizadas. Algunos departamentos dentro de las organizaciones pueden haber construido su propia plantilla que puede incluir especificaciones inconsistentes. En segundo lugar, las plantillas del informe del caso de seguridad, en ocasiones, puede enmascarar una cultura de "seguridad en el papel" que resulta a expensas de la "seguridad real".

Caso de seguridad incremental

Otro aspecto importante a considerar al momento de construir un caso de seguridad es el tiempo. A lo largo de los años, el desarrollo del caso de seguridad se dejó hasta el final del ciclo de desarrollo del producto. Como resultado, se perdieron oportunidades para detectar problemas de seguridad desde el principio, en algunos casos, esto llevó a una costosa renovación con el fin de cumplir los objetivos.

Con el fin de mitigar dichos riesgos del proyecto, deberá construir un plan de administración de seguridad para el proyecto, que incluya una etapa temprana de conceptualización, una verificación de la prueba y una estrategia de validación, durante las primeras etapas del ciclo de vida útil del desarrollo del producto. Esto autoriza la ejecución de una evaluación preliminar con el fin de obtener la confianza de que el producto se encuentra a punto de cumplir los objetivos de seguridad. Las organizaciones más desarrolladas buscan implementar un ciclo de vida útil del caso de seguridad completo, que incluye las auditorias del caso de seguridad incremental, las cuales se llevan a cabo a lo largo de las diversas etapas del proyecto de desarrollo del producto (ver la **Figura 3**).

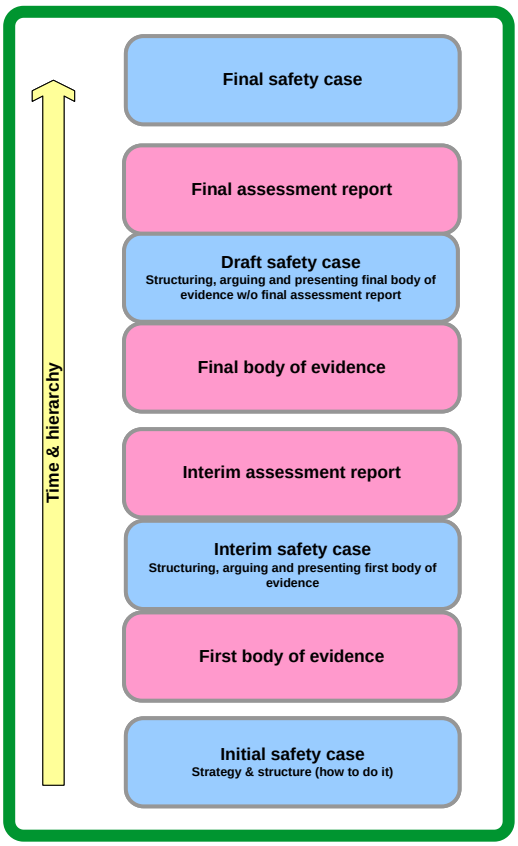

Figura 3
Ejemplo de este caso de seguridad desarrollado a lo largo del ciclo de vida útil del proyecto.

Goal Structure Notation

Hasta este momento, este ensayo ha abordado el concepto del caso de seguridad y ha presentado sus ventajas y limitaciones. El informe del caso de seguridad ha sido descrito como un documento que resume los eventos que se han llevado a cabo con el fin de

asegurar la seguridad del producto. Como el caso de seguridad es un "argumento estructurado", el siguiente paso lógico es formalizar ambos, que la "estructura" y el "argumento" son partes del proceso. Un método llamado Goal Structure Notation (GSN) ha sido creado para sustentar este esfuerzo. GSN se define de la siguiente manera:

"La fijación de la argumentación gráfica puede utilizarse para documentar los elementos individuales de cualquier argumento (reclamaciones, evidencia e información contextual) y, quizás más significativamente, las relaciones que existen entre estos elementos (por ejemplo, cómo es que las reclamaciones se sustentan en otras reclamaciones y en última instancia en evidencias, y el contexto que se define por medio del argumento). Los argumentos documentados por medio del GSN pueden ayudar a asegurar las propiedades esenciales de los sistemas, servicios y organizaciones (tales como las propiedades de seguridad)".[2]

La **Figura 4** ilustra un ejemplo de cómo el Goal Structure Notation muestra los elementos de un argumento.

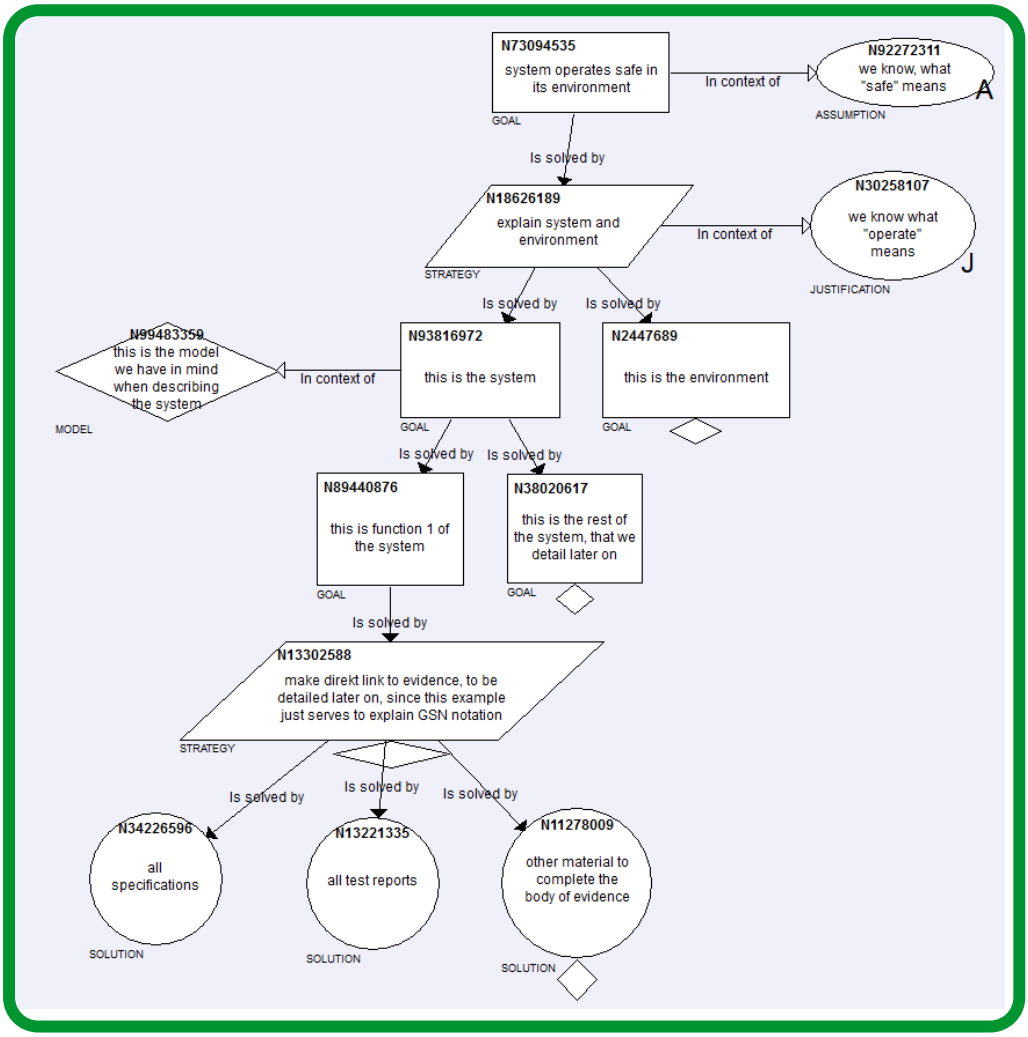

Figura 4
Ejemplo de GSN

En la Figura 4, la información fluye de arriba a abajo. Se relaciona un nuevo argumento a discusiones previas que ya han sido resueltas. Esto hace que el entender su razonamiento sea más fácil. La información se divide cuidadosamente en objetivos y sub-objetivos, suposiciones, justificaciones y referencias para modelos bajo consideración.

[2]Grupo de trabajo de GSN: GSN community standard versión 1 (2011).

Conclusión

Los informes de los casos de seguridad proporcionan un catalizador importante para fomentar una cultura de "primero la seguridad" entre las organizaciones que fabrican partes, productos y sistemas para industrias importantes, tales como: aéreas, aeroespaciales, ferroviarias y automotrices. Además, con el fin de documentar los argumentos para la seguridad de cualquier producto, los informes de casos de seguridad también generan los beneficios siguientes:

- **Proporciona una visión general de las modificaciones** - Una vez que un producto se comercialice, se le realizarán modificaciones al producto, como nuevas características. El registro proporcionado por el informe inicial del caso de seguridad puede fungir como una referencia que ayude a catalogar estos nuevos cambios y modificaciones desde una perspectiva de seguridad.

- **Explica las especificaciones del proyecto y las desviaciones que existieron a partir del plan de seguridad inicial** - A lo largo de un proyecto, el equipo del proyecto puede desviarse del plan original con la aprobación del comité de dirección. Por ejemplo, los miembros del equipo pueden cambiar, los métodos pueden reforzarse para incrementar el nivel de calidad y los requisitos del cliente también pueden cambiar. Por lo tanto, la planeación debe actualizarse, incluyendo aquellos aspecto de planeación que afectan al plan de seguridad. Finalmente, el plan de seguridad actúa como un registro de los cambios que se han llevado a cabo.

- **Aclara la dependencia que existe en los casos de seguridad** - Un caso de seguridad bien documentado puede fungir como el impulso necesario para realizar otros casos de seguridad que utilicen una línea de argumentación que haya sido exitosa para obtener las aprobaciones necesarias y comercializar el producto.

Para mayor información, consulte el ensayo de la conferencia "Safety Case and Certification" (Caso de seguridad y certificación) dada por Wolfgang Reinelt & Michel. Bonnet (Safe.tech 2015, Munich, Alemania).

Acerca de los

Wolfgang Reinelt es un experto en el grupo de exportación encargado de la seguridad funcional en Schneider Electric y es responsable de la administración de la seguridad funcional dentro del departamento de soluciones para las máquinas (Industria empresarial). Cuenta con un grado de Maestría en Matemáticas y un Doctorado en Ingeniería Eléctrica, ambos de Paderborn University, Alemania. Publicó numerosos ensayos de conferencias y artículos en diarios revisados por sus colegas y cuenta con patentes dentro del área de ingeniería de control, detección de fallas y seguridad. Antes de unirse a Schneider Electric en 2007, trabajó en la industria automotriz con temas similares.

Michel Bonnet es responsable de la administración de seguridad funcional dentro del departamento de automatización de energía de Schneider Electric (Departamento de energía). Desde el 2008, ha dirigido los proyectos de gestión de calidad y de administración de seguridad funcional con relación a los relevadores de protección. Es un experimentado ingeniero de aplicaciones y ha trabajado en la automatización de seguridad y subestaciones del proyecto del sistema de control digital. Cuenta con un grado en Ingeniería de ESIGELEC, en Rouen, Francia.