Dominar la complejidad: proceso de seguridad integrado para sistemas vehiculares modernos

03/12/2025 La seguridad funcional y la seguridad de la funcionalidad prevista son pilares esenciales para desarrollar sistemas vehiculares modernos y seguros. Con sistemas de asistencia cada vez más complejos y la conducción autónoma, la seguridad funcional cobra mayor importancia. Los expertos de Porsche Engineering aplican su experiencia de muchos años ayudando a los clientes a desarrollar sistemas modernos y conformes con la seguridad, desde el concepto inicial hasta la liberación.

La relación entre la seguridad funcional (FuSa) y la seguridad de la funcionalidad prevista (SOTIF) puede entenderse como dos caras de la misma moneda: juntas forman un todo valioso. Ambas desempeñan un papel decisivo en los modernos sistemas de asistencia al conductor, o ADAS (sistemas avanzados de asistencia al conductor), así como en la conducción autónoma (AD). FuSa aborda la pregunta clásica: ¿Qué sucede si falla un componente de software o hardware?

La seguridad funcional garantiza que el sistema no cause un riesgo inaceptable ante fallas internas,

como una falla del sensor o un error de software. Se basa en un proceso de análisis estructurado donde se examinan y evalúan todos los errores relevantes de software y hardware según sus efectos. Los efectos críticos para la seguridad se mitigan mediante medidas técnicas y procedimentales. Los métodos de seguridad funcional se aplican de manera consistente durante la fase de concepto y la implementación en serie. SOTIF aborda otra pregunta igualmente importante: ¿Qué sucede si el sistema opera sin fallas pero no logra dominar una situación operativa real? Esto concierne a los riesgos que surgen de las limitaciones de la función misma—por ejemplo, cuando la cámara de un vehículo es cegada por el sol o un algoritmo no detecta a un ciclista en una escena de conducción compleja.

SOTIF es un proceso de descubrimiento exploratorio donde las iteraciones son la herramienta central para mejorar gradualmente el diseño de la función y generar conocimiento. Para lograr la seguridad general del sistema, FuSa y SOTIF están interconectados sistémicamente y se complementan.

"FuSa garantiza que el hardware y el software funcionen de manera confiable. SOTIF garantiza que las capacidades de estos componentes confiables estén suficientemente especificadas y comprobadas para operar de manera segura en el mundo real", explica Marek Hudec, Gerente Senior de Seguridad de Sistemas en Porsche Engineering. "Un sistema puede ser seguro desde el punto de vista tradicional de FuSa, pero aún no ser suficientemente seguro desde el punto de vista de SOTIF debido a limitaciones de rendimiento".

Enfoque iterativo para SOTIF

A pesar de la similitud, existen diferencias en los pasos del proceso entre FuSa y SOTIF. Generalmente se prefiere un enfoque iterativo con análisis exploratorios y métodos de prueba para lograr SOTIF (ver recuadro en la página 38). "Los desarrolladores especifican, prueban y revisan el diseño del sistema hasta alcanzar un riesgo residual aceptable", informa Dennis Müller, Ingeniero de Desarrollo en Porsche Engineering. Porsche Engineering ofrece a sus clientes un portafolio de soluciones integral que incluye ambos métodos de seguridad—SOTIF y FuSa—para gestionar el complejo desarrollo y verificar y validar los sistemas de asistencia al conductor y las funciones de conducción autónoma.

"Apoyamos a nuestros clientes en la aplicación de las normas relevantes como ISO 26262 (FuSa) e ISO 21448 (SOTIF). Esto incluye su implementación en los procesos de desarrollo existentes, la ejecución de análisis de peligros y riesgos, la elaboración de conceptos de seguridad y el apoyo durante todo el ciclo de vida de seguridad", explica Müller. "En Porsche Engineering, aseguramos el desarrollo conforme a la seguridad mediante procesos integrados claramente definidos con responsabilidades dedicadas. Esto garantiza la conformidad con las normas y proporciona trazabilidad".

Porsche Engineering cuenta con experiencia de muchos años en toda la cadena de desarrollo. Desde la elaboración de requisitos hasta la simulación y prueba de vehículos reales, utiliza métodos de vanguardia para desarrollar funciones de advertencia, sistemas de estacionamiento y funciones de conducción (parcialmente) autónomas. Un ejemplo es el componente de software modular "Guardian", diseñado para facilitar la transición de sistemas avanzados de Nivel 2 a la conducción altamente

automatizada de Nivel 3. Ofrece una solución robusta, segura y conforme a las normas para implementar componentes de seguridad en sistemas de conducción autónoma. Mediante el análisis de datos de conducción reales, se identifican de manera exploratoria situaciones potencialmente críticas y casos especiales—denominados corner cases y edge cases—que se utilizan para generar escenarios basados en datos. A medida que aumenta la responsabilidad del sistema, los desafíos también crecen. En seguridad funcional, estos desafíos consisten principalmente en que los conceptos de degradación y advertencia ya no pueden depender únicamente del conductor, quien tiene la responsabilidad exclusiva de todas las maniobras durante la conducción asistida (Nivel 1) y semiautomatizada (Nivel 2).

Esto cambia a partir del Nivel 3. En este caso, los sistemas deben manejar fallas de forma autónoma, ya que el conductor ya no tiene un deber constante de atención. Solo cuando los sistemas alcanzan sus límites debe ser posible intervenir después de un período de advertencia apropiado. En principio, la operabilidad segura debe garantizarse cuando ocurren fallas, al menos durante cierto tiempo—esto hace que el salto del Nivel 2 al Nivel 3 sea desafiante. Como resultado, el número de redundancias en la electrónica del vehículo aumenta rápidamente, junto con la carga de trabajo de desarrollo y los costos asociados. Con respecto a SOTIF, el desafío radica en la profundidad y amplitud del conjunto de todos los escenarios operativos posibles que la función necesita dominar.

"Estos incluyen el entorno vehicular en constante cambio, el comportamiento de los usuarios de la carretera y eventos imprevisibles, denominados escenarios inseguros desconocidos", dice Hudec. Para hacer frente a esta complejidad, los sistemas se diseñan inicialmente para un dominio de diseño operativo definido (ODD). Los escenarios que deben dominarse de manera segura se restringen a un espacio derivado sistemáticamente, que se divide en escenarios individuales discretos mediante un portafolio de escenarios. El sistema debe garantizar que el acercamiento al límite de este espacio se detecte en una etapa temprana para que el control pueda transferirse al conductor o el vehículo pueda detenerse de manera segura dentro de los límites del ODD. "Este enfoque es extremadamente importante para el desarrollo de asistencia al conductor: cuanta más responsabilidad asume un sistema para la conducción real, más crítico se vuelve considerar los aspectos de seguridad de FuSa y SOTIF", explica Müller.

Mejora de la seguridad mediante redundancia

Un ejemplo práctico que ilustra los enfoques diferentes pero complementarios de FuSa y SOTIF es una situación de Nivel 3 de SAE para la conducción automatizada en autopista donde el conductor renuncia completamente a la responsabilidad. Para gestionar fallas de hardware o software se requiere FuSa: supongamos que el sensor de radar que mide la distancia al vehículo de adelante tiene un defecto de hardware y ya no proporciona datos. Esta falla podría hacer que la función dependa de datos de sensores desactualizados o no válidos y posiblemente corra el riesgo de una colisión trasera. Por eso los expertos de Porsche Engineering utilizan análisis de seguridad deductivos e inductivos para identificar tales fallas, que deben verificarse mediante mecanismos de seguridad. En este caso específico, por ejemplo, la redundancia sería útil para evitar que esta falla individual local conduzca a la "no disponibilidad global" de los datos del sensor, al menos hasta que el conductor vuelva a asumir la

responsabilidad de conducir.

SOTIF entra en juego al dominar los límites de rendimiento para la conducción automatizada en autopista. Por ejemplo, la detección de vehículos debe diseñarse para que todos los demás vehículos alrededor o que se acercan, incluidas todas las motocicletas, sean detectados. Sin embargo, debido a los límites de rendimiento técnicamente inherentes de los sensores utilizados, el vehículo puede no detectar correctamente ciertas siluetas estrechas y trayectorias de aproximación bajo condiciones de luz o clima desfavorables. Aunque el hardware y el software funcionan perfectamente, esto podría hacer que la función inicie un cambio de carril que resulte en riesgo de colisión con una motocicleta que adelanta. En este caso, los procesos SOTIF estipulan que el diseño debe analizarse y validarse en todos los escenarios operativos y que las debilidades identificadas se corrijan con la siguiente iteración del diseño (actualización de especificación seguida de actualización de implementación). Por ejemplo, se podrían instalar cámaras adicionales y sensores lidar en la sección trasera o se podrían optimizar los algoritmos de fusión de sensores.

"El mayor desafío ya no está solo en el sistema mismo, sino en la complejidad casi infinita de la realidad. No es posible probar todos los escenarios concebibles por adelantado, pero es necesario lograr una cobertura suficiente del rango de operación. El proceso de desarrollo es tan complejo como cabría esperar. SOTIF proporciona el marco para comprender los límites del sistema y diseñarlos de manera segura incluso cuando todos los componentes funcionan perfectamente", explica Müller.

Proporcionar evidencia cualitativa y cuantitativa de que un sistema es seguro requiere grandes cantidades de datos de prueba, una cantidad considerable generada a través de simulaciones. El mayor desafío es lidiar con escenarios inseguros desconocidos—situaciones peligrosas que no se tuvieron en cuenta durante el desarrollo debido a especificaciones insuficientes o que podrían ocurrir por cambios en las condiciones operativas. Descubrir y minimizar estos es el objetivo central de SOTIF y representa un gran desafío al desarrollar los sistemas. "En Porsche Engineering, ofrecemos a nuestros clientes no solo servicios de prueba individuales, sino también una cooperación cercana y a largo plazo para cumplir con las enormes demandas del desarrollo de ADAS/AD y poner en circulación funciones seguras, robustas y confiables", promete Hudec.

Métodos como el reconocimiento de corner cases basado en IA o modelos de IA especialmente entrenados proporcionarán cada vez más apoyo a los desarrolladores en el futuro. Ya está claro que el uso de IA en sistemas críticos para la seguridad requerirá procedimientos de verificación aún más complejos. Este tema es abordado por el nuevo borrador de norma internacional ISO/PAS 880, que trata sobre la seguridad de la IA cuando forma parte del producto final. Otra innovación es el borrador de norma internacional ISO/TS 5083, que se centra específicamente en la seguridad de las funciones de conducción autónoma del vehículo y tiene en cuenta no solo los componentes a bordo, sino también los componentes externos y su efecto en la seguridad general. Esto se conoce como seguridad holística. La comunicación V2X orientada a la seguridad entre vehículos y con la infraestructura trae nuevas posibilidades de mejora de la seguridad, pero también nuevas fuentes potenciales de fallas y nuevas dependencias. Estas también deben salvaguardarse con la misma consistencia—un proceso exigente al que los expertos de Porsche Engineering se dedican a diario.

Resumen

Los requisitos de la seguridad funcional de los vehículos se deben en gran medida al uso generalizado de sistemas de asistencia. El rendimiento del sistema correctamente implementado en corner cases es el enfoque principal de SOTIF. Porsche Engineering utiliza métodos basados en datos e IA para dominar la complejidad y poner en circulación sistemas confiables.

Info

Texto publicado por primera vez en Porsche Engineering Magazine, edición 1/2025.

Texto: Ralf Bielefeldt

Copyright: Todas las imágenes, videos y archivos de audio publicados en este artículo están sujetos a derechos de autor. La reproducción total o parcial no está permitida sin el consentimiento por escrito de Dr. Ing. h.c. F. Porsche AG. Por favor, contacte a magazin@porsche-engineering.de para obtener más información.

MEDIA ENQUIRIES

Elizabeth Solís

Public Relations and Press
Porsche Latin America
+1 (770) 290 8305
elizabeth.solis@porschelatinamerica.com

Link Collection

Link to this article
https://newsroom.porsche.com/es/2025/innovacion/pla-porsche-engineering-functional-safety-deleoping-modern-vehicle-systems-41267.html