intellicar.de
autonomous, shared & connected mobility

Tests & Research >

15.07.2021 - 10:38

Fortiss veröffentlicht umfangreiches Whitepaper zu ISO 21434

fortiss

Die Cybersicherheits-Anforderungen in der Fahrzeugentwicklung nehmen ständig zu. Der Standard ISO 21434 liefert wesentliche Aspekte zur Verbesserung der Fahrzeugsicherheit. Das Landesforschungsinstitut des Freistaats Bayern für softwareintensive Systeme (Fortiss) publiziert ein Whitepaper, das bei der Umsetzung von ISO 21434 in konkreten Entwicklungsprojekten unterstützen soll.

Beim Blick über den Tellerrand wird klar: Trotz Stolpersteinen rückt die Vision des autonomen Fahrens immer näher. Im besten Falle verspricht man sich neben großen wirtschaftlichen Erfolgen auch eine Erhöhung der Verkehrssicherheit. Da selbstfahrende Fahrzeuge jedoch zum großen Teil auf digital vernetzten Systemen basieren, müssen sich die OEMs immer mehr der Herausforderung stellen, mit der sich die traditionelle IT schon lange auseinandersetzen muss: Cyberangriffe.

Der Standard ISO 21434 definiert, wohin die Reise zu mehr Sicherheit in Zukunft gehen wird. Das Landesforschungsinstitut des Freistaats Bayern für softwareintensive Systeme (Fortiss) hat mit dem vorliegenden Whitepaper „Security Engineering for ISO 21434“ erstmalig einen praxisnahen Umsetzungsleitfaden für Ingenieure in der Automobilindustrie bereitgestellt. Fortiss ist in der Rechtsform einer gemeinnützigen GmbH organisiert. Die Gesellschafter sind zu zwei Drittel der Freistaat Bayern und zu einem Drittel die Fraunhofer-Gesellschaft.

Der Standard ISO 21434 ist demnach ein wesentlicher Schritt zur Verbesserung der Fahrzeugsicherheit, da er einige der wichtigsten Herausforderungen adressiert, die mit dem zunehmenden Einsatz von Informations- und Kommunikationstechnologien in Fahrzeugen einhergehen. Mit Blick auf die OEMs gilt es diese Anforderungen nun umzusetzen und die damit verbundenen Komplexitäten greifbar zu machen. Zukünftig müssen in Fahrzeugen spezifische Cyber-Security-Managementsysteme (CSMS) implementiert werden. Was bedeutet dies heute schon für die EntwicklerInnen und IngenieurInnen? Betroffen sind übrigens nicht nur die Autobauer selbst, sondern auch die Entwicklungsabteilungen der Erstausrüster, Zulieferer und zahlreiche Entwicklungsdienstleister. Für all diese Zielgruppen ist Cybersecurity im vernetzten Auto ein Pflichtthema und es wird zu einer zukünftigen Daueraufgabe, die mit Auslieferung des Fahrzeugs an die NutzerInnen keineswegs beendet ist.

Der von Fortiss bereitgestellte Umsetzungsleitfaden „Security Engineering for ISO 21434“ (PDF zum Download hinterlegt) soll genau an dieser Stelle ansetzen. Er erklärt zunächst den Standard und dessen

Bestandteile und unterstützt somit bestenfalls bei einer möglichst effizienten Umsetzung.

Fahrzeuglebenszyklus

Der Industriestandard ISO 21434 basiert auf Anforderungen zu Vorgehen und Methoden zur Bewertung des Sicherheitsrisikos. Auf dieser Grundlage werden Sicherheitsargumente erstellt, die die Fahrzeugsicherheit gewährleisten sollen. Doch angesichts der Komplexität vernetzter Fahrzeuge und eng getakteter Produktionsfristen ist es ohne Automatisierung nicht möglich, alle vorgeschriebenen Aktivitäten auszuführen und alle Artefakte zu verstehen. Darüber hinaus ist Cybersicherheit eine kontinuierliche Aufgabe, da viele neue Schwachstellen und Angriffe erst nach der Fahrzeugproduktion entdeckt werden, und diese dann erneute Gegenmaßnahmen und Analysen erfordern.

Um den Cybersicherheits-Anforderungen in der Fahrzeugentwicklung umfassend und von Anfang an gerecht zu werden, schlagen die WissenschaftlerInnen von Fortiss einen Security-Engineering-Ansatz vor. Dieser beinhaltet angemessene, automatisierte Methoden, mit deren Hilfe vermieden werden kann, dass (implizite) Annahmen übersehen oder notwendige Abwägungen zwischen Cybersecurity und funktionaler Sicherheit nicht berücksichtigt werden. Durch praktische Anwendungsbeispiele veranschaulicht das Whitepaper, dass der vorgeschlagene Ansatz die Effizienz bei der Erstellung von Artefakten erheblich steigern und eine kontinuierliche Sicherheitsbewertung ermöglichen kann. Im Anschluss zeigt das Papier noch weitere wichtige Forschungsansätze auf, um den vorgeschlagenen Ansatz möglichst automatisiert zu realisieren.

Herausforderungen

Die Zielgruppe dieses Whitepapers sind alle Cybersecurity-IngenieurInnen in der Automobilbranche, die vor der aktuellen Herausforderung stehen, die ISO 21434 in konkreten Entwicklungsprojekten umzusetzen. Sie sollen in die Lage versetzt werden, sich ein klareres Bild von der ISO 21434 zu machen, insbesondere von den Aktivitäten, die während der Risikobewertung durchgeführt werden. Und sie werden verstehen, dass Teile der ISO 21434 durch geeignete Techniken automatisiert werden können. Auf diese Weise erhalten sie eine klare Perspektive, wie eine kontinuierliche Sicherheitsanalyse für Kraftfahrzeuge unter Verwendung eines inkrementellen Ansatzes umgesetzt werden kann.schluss zeigt das Papier noch weitere wichtige Forschungsansätzeuf, um den vorgeschlagenen Ansatz möglichst automatisiert zu realisieren.

Autor: jst

Beitrag teilen