© lesterman | Adobestock

HARMONISIERUNG VON CYBERSECURITY MIT SAFETY AND SYSTEM ENGINEERING

Hand in **Hand**

V2X-Kommunikation ermöglicht autonomes Fahren, mehr Sicherheit im Straßenverkehr, Energieeinsparungen und eine angenehme User Experience. Sie bringt aber auch neue Herausforderungen und Bedrohungen für die persönliche Sicherheit und den Schutz der Privatsphäre mit sich.

Die UNECE WP.29-Verordnung R155 für Cybersecurity-Managementsysteme (CSMS) ist in der Europäischen Union verpflichtend. R155 empfiehlt, die Anforderungen an das CSMS anhand von Normen wie der kürzlich veröffentlichten ISO/SAE 21434 umzusetzen. Es gibt weitere verbindliche oder empfohlene Normen und bewährte Verfahren zur Gewährleistung der Cybersecurity in der Automobilindustrie, beispielsweise ASPICE.

Ein systematischer Prozess und Methoden für die Entwicklung einer Automobilplattform und von Steuergeräten tragen dazu bei, die gesetzlichen Anforderungen zu erfüllen, die verschiedenen Sicherheitsstandards im Automobilbereich einzuhalten und die angestrebten Sicherheitsstufen für die Cybersecurity zu erreichen.

Dabei wird dem klassischen V-Engineering-Modell gefolgt und der ASPICE-Security-Engineering-Prozess und -Gruppen integriert. Für den Nachweis und die Bewertung der kritischen Phasen des CSMS werden Arbeitsergebnisse gemäß ISO/SAE 21434 erstellt. Eine Reihe von Cybersecurity-Aktivitäten, die über die Serienproduktion hinausgehen, werden durchgeführt, um neu entdeckte Schwachstellen zu erkennen und zu beheben. Als Teil des Vorgehensmodells wird die Integration des Security-Prozesses in den Safety-Prozess skizziert, um die Wahrscheinlichkeit von fehlenden Themen zu Beginn der Entwicklung zu reduzieren.

Die Durchführung einer Bedrohungs- und Risikoanalyse (Threat Analysis and Risk Analysis, TARA) ist ein iterativer Prozess, und sollte erst beendet werden, wenn die Anlagen ausreichend gegen Bedrohungen und gegen elektrische oder elektronische Komponenten geschützt sind. Mit dem Prozessmodell kann die iterative TARA nahtlos mit anderen Prozessmodellen integriert werden.

Verschiedene Themen wie autonomes Fahren, V2X-Konnektivität, Elektrifizierung und Shared Mobility wirken sich auf die Fahrzeugsicherheit aus. UNECE-Bestimmungen, Standards wie ISO/SAE 21434, ASPICE und andere bestehende Standards für die Cybersicherheit im Automobilbereich regulieren und leiten die Entwicklung und Sicherung von Fahrzeugen.

Die gesamte Wertschöpfungskette, einschließlich der Automobilhersteller (OEMs) und der -Zulieferer auf allen Ebenen, muss die Vorschriften der UNECE R155 und R156 einhalten. OEMs sind juristische Personen, die sich für CSMS- und SUMS-Audits registrieren lassen müssen. OEMs müssen sicherstellen, dass ihre Partner in der Wertschöpfungskette Cybersicherheitspraktiken befolgen und umsetzen.

Trotzdem wird dringend empfohlen, ISO/SAE 21434 und ISO 27001 für Cybersicherheit und ISO/CD 24089 für Software-Update-Engineering zu befolgen. Auf welche Weise können Cybersecurity-Engineering-Aktivitäten in ASPICE-basierte Entwicklungszyklen integriert werden? In den folgenden Abschnitten wird ein ganzheitlicher Ansatz für die Cybersecurity in der Automobilindustrie skizziert.

Überblick über den Prozess

Im Folgenden wird ein integriertes Prozessübersichtsdiagramm für die Entwicklung eines sicheren Kfz-Steuergeräts dargestellt. Die Aufnahme von Cybersicherheitsaktivitäten für ein Projekt erfordert ein etabliertes Cybersecurity-Managementsystem (CSMS) gemäß ISO/SAE 21434, Absatz 05, und ein Software-Update-Managementsystem (SUMS) gemäß ISO/CD 24089. Das CSMS muss Cybersecurity-Richtlinien, Regeln, Kompetenzmanagement für Ressourcen, kontinuierliches Management, Toolmanagement und Prozesse definieren. Das SUMS muss auch den notwendigen Prozess spezifizieren, um Rückverfolgbarkeit, Konsistenz, einen eindeutigen Identifikator, Interdependenz und Kompatibilität während des Software-Aktualisierungsprozesses sicherzustellen (Bild 1).

Für die Entwicklung und Produktion von Automotive-Steuergeräten müssen eine Hochsicherheitseinrichtung zum Schutz sensibler Daten sowie eine Infrastruktur und Verfahren eingerichtet werden. Das lässt sich als Teil eines CSMS auf Organisationsebene handhaben.

Die nachfolgenden Abschnitte behandeln projektspezifische Cybersecurity-Aktivitäten, die parallel zu anderen Produktentwicklungsaktivitäten durchgeführt werden müssen, um die gesetzlichen Anforderungen zu erfüllen, die Industriestandards für die Sicherheit in der Automobilindustrie einzuhalten und

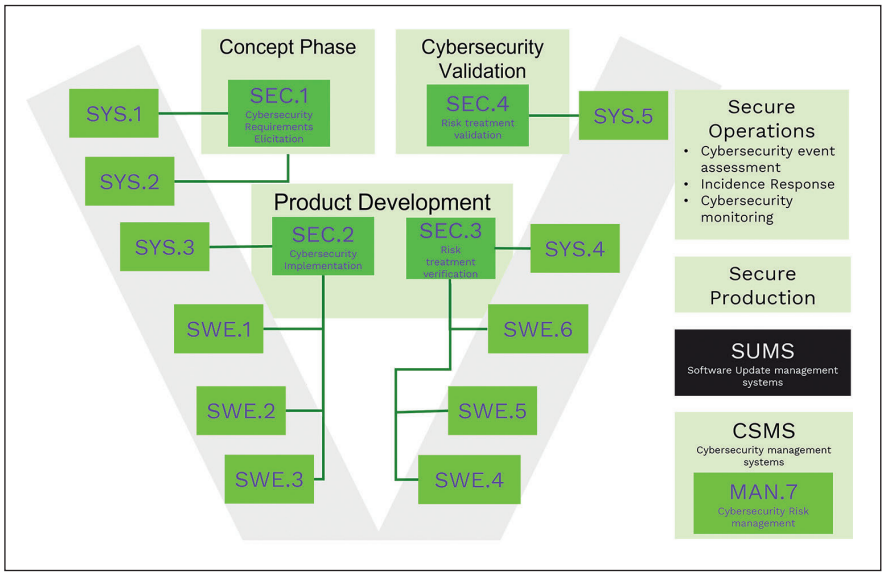
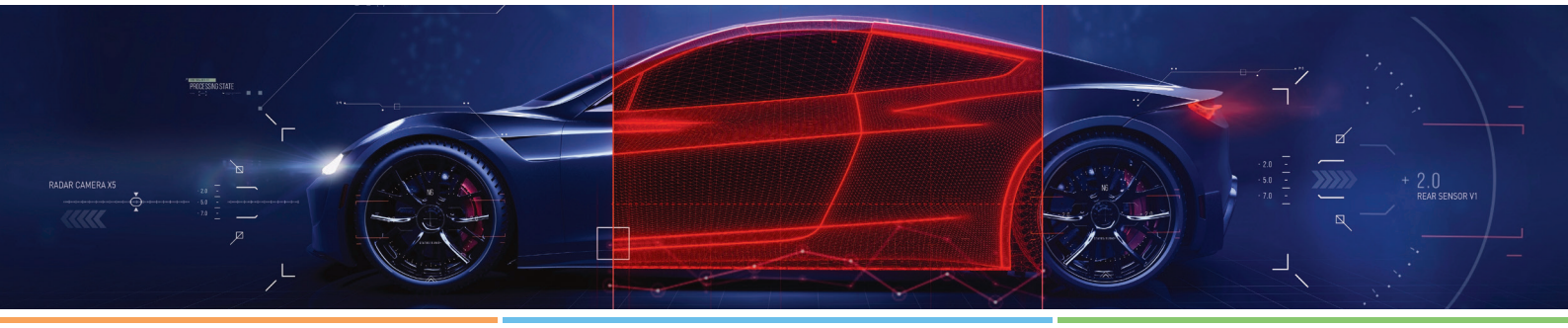


Bild 1: Überblick über den Prozess © KPIT Technologies



dsPIC33C DSC für robuste Automotive-Designs

Hohe Zuverlässigkeit und Robustheit in rauen Umgebungen

Die Digital Signal Controller (DSCs) dsPIC33C sind für extreme Betriebsbedingungen ausgelegt und bieten Echtzeitreaktion und hohe Zuverlässigkeit bei extremen Temperaturen.

Sie bieten den richtigen Mix von Funktionen für viele allgemeine Automotive-Anwendungen.

- AEC-Q100-Grade-0-qualifizierte Bausteine (150 °C) für robuste Leistungsfähigkeit unter extremen Bedingungen
- Hochleistungs-Core mit DSP Engine bietet deterministische Reaktion für Steuerungen
- Analog-Integration auf hohem Niveau sorgt für optimale Signalaufbereitung und -messung und reduziert die Kosten für die Stückliste
- Robuste Kommunikationsperipherie wie CAN FD, LIN und SENT
- dsPIC33C DSCs und TrustAnchor TA100 sorgen für robuste Sicherheit
- MCAL-Treiber, ein vollständiges Ökosystem aus Bibliotheken, Entwicklungs- und Konfigurations-Tools
- Skalierbare Serien mit kleinem bis großem Speicher für Anwendungen mit oder ohne AUTOSAR
- DSCs sind ausgelegt für funktionale Sicherheit und helfen, die Richtlinien ISO 26262 ASIL B oder ASIL C zu erzielen

MICROCHIP

microchip.com/dsPIC33C

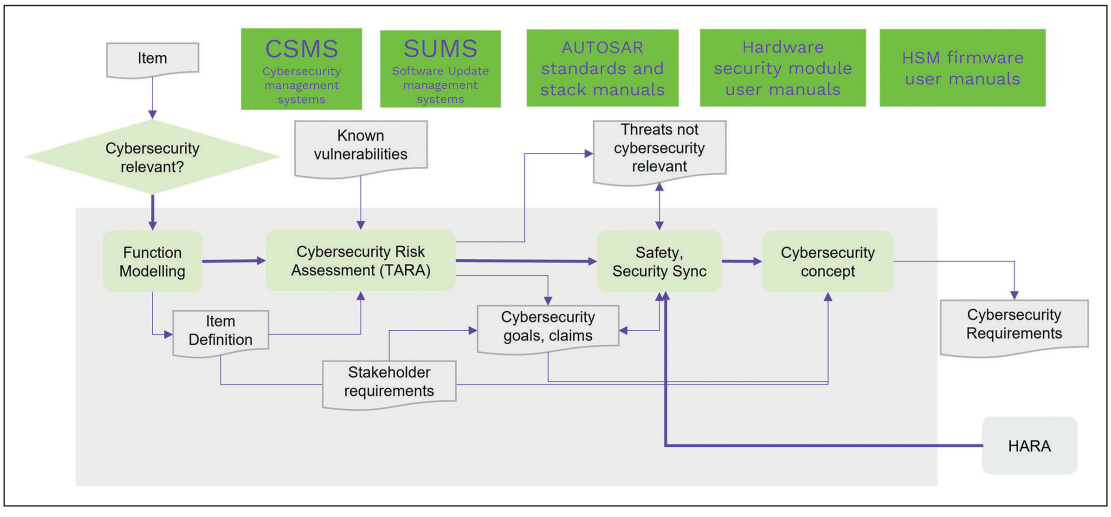


Bild 2: Konzeptphase © KPIT Technologies

das angestrebte Sicherheitsniveau für die Cybersecurity zu erreichen.

Planung

Der projektabhängige Plan für Cybersecurity-Aktivitäten und die Verantwortlichkeiten müssen gemäß ISO/SAE 21434, Abschnitt 06, festgelegt werden. Die Kontrolle und der Plan müssen sicherstellen, dass der Lieferant alle Vorschriften und Normen zur verteilten Entwicklung einhält. Innerhalb des projektspezifischen CSMS müssen Cybersecurity-Fälle eröffnet werden, um die Arbeitsergebnisse zu verfolgen, zu aktualisieren, während des Projekts zu überprüfen und mit einem Bewertungsbericht abzuschließen, bevor die Produktion freigegeben wird. Der in ASPICE definierte Prozess des Cybersecurity-Risikomanagements kann als Teil des CSMS betrachtet werden. Das CSMS muss Aktivitäten im Zusammenhang mit der Produktions- und Betriebssicherheit begrenzen. Für Software-Updates muss SUMS befolgt werden.

Konzeptphase

Die Entwicklung von Cybersecurity beginnt mit der Konzeptphase, in der die Sicherheitsanforderungen (Bild 2) ermittelt werden. Die Aktivitäten müssen gemäß ISO/SAE 21434, Abschnitt 09, durchgeführt werden und sind dem in ASPICE definierten SEC.1-Prozess ähnlich. In der Konzeptphase wird die Bedrohungsanalyse für ein Element, ein Bauteil oder ein Set durchgeführt, das eine Funktion auf Fahrzeugebene implementiert. Er lässt sich zusammen mit dem SYS.1-Prozess ausführen. Danach können die Prozesse SYS.2 und SYS.3 folgen. Der ASPICE-SYS.3-Prozess kann zum Einsatz kommen, um die Architektur für Cybersecurity-Systemelemente auf Grundlage der Systemanforderungen zu bestimmen.

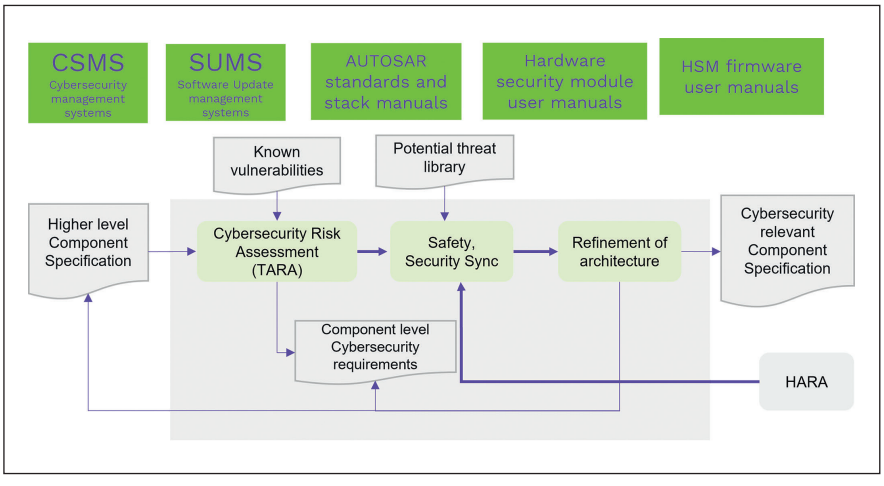


Bild 3: Architektur- und Design-Verfeinerung © KPIT Technologies

Die Risikobewertung für Cybersecurity (TARA) lässt sich mit verschiedenen Methoden durchführen. Ein EVITA- oder STRIDE-Modell (E-Safety Vehicle Intrusion Protected Applications) kann zur Bewertung der Sicherheit in der Konzeptphase zum Einsatz kommen. Die Modellierung und Bewertung kann mit dem Microsoft Thread Modeling Tool mit einer auf die Automobilindustrie zugeschnittenen Vorlage durchgeführt werden.

Die Ziele der Cybersecurity und der funktionalen Sicherheit können manchmal im Widerspruch stehen, zum Beispiel stellt das Cybersecurity-Ziel den Dienst sicher. Das Safety-Ziel besteht darin, ein System oder eine Funktion abzuschalten, wenn eine gefährliche Situation festgestellt wird. Daher ist eine Interaktion zwischen Cybersecurity und funktionaler Sicherheit erforderlich, und die von TARA und HARA ermittelten Risiken und Pläne zur Risikominderung müssen von dem gemeinsamen Team überprüft und entsprechend aktualisiert werden.

Produktentwicklung: Design

ISO/SAE 21434, Abschnitt 10, definiert die Produktentwicklung für Cybersecurity. Der Prozess kombiniert Aktivitäten und Umfang der ASPICE-Prozesse SEC.2 und SEC.3. Nach Abschluss der Konzeptphase und dem Beginn des System-Engineerings besteht der nächste Schritt in der Entwicklungsphase darin, die Risiken in den Systemelementen zu analysieren. Die Cybersecurity-Spezifikation für ein Systemelement, die Anforderungen und eine Architektur enthält, ist die primäre Eingabe. Der Prozess würde die Systemarchitektur aktualisie-

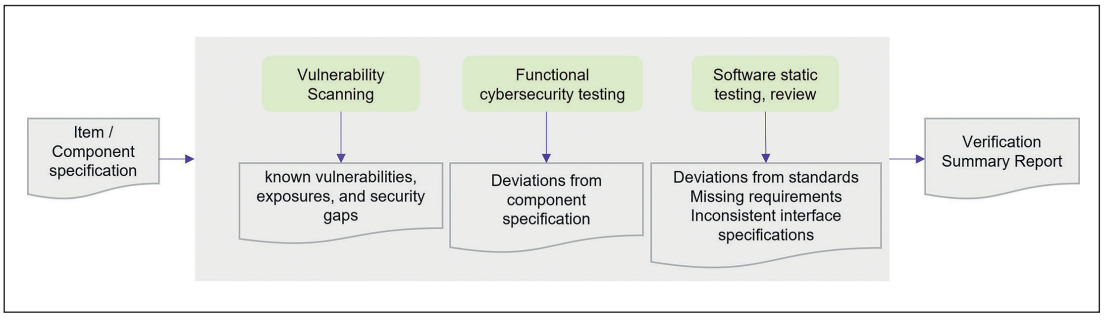


Bild 4: Überprüfung
© KPIT Technologies

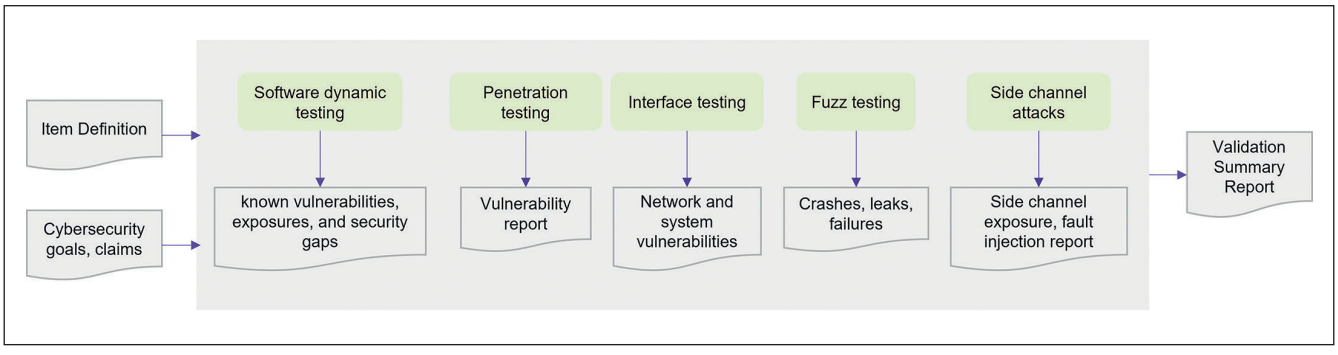


Bild 5: Validierung © KPIT Technologies

ren und verfeinern und die Spezifikationen für die nächste Stufe der Cybersecurity-Komponenten festlegen. Eine in der Konzeptionsphase gewählte Risikominderungsmaßnahme kann neue Werte einführen, die geschützt werden müssen. Daher ist eine Bedrohungsanalyse auf Grundlage von Stride oder einer ähnlichen Methode erforderlich, um Risiken in dem entwickelten System zu ermitteln.

Bild 3 zeigt ein Standardverfahren zur Ermittlung von Risiken und zur Entwicklung von Spezifikationen für Cybersecurity-Komponenten. Wenn die Produktentwicklung fortschreitet und Spezifikationen für Software- und Hardware-Komponenten entwickelt werden, ist eine Bedrohungsanalyse möglicherweise nicht mehr erforderlich, wohl aber eine Schwachstellenanalyse. Ebenso kann der Synchronisierungsprozess für die Sicherheit entfallen, wenn die Systemabstraktion auf der Ebene der Einheiten erfolgt.

Produktentwicklung: Verifizierung

Bild 4 zeigt verschiedene Verifizierungsaktivitäten, um zu bestätigen, dass die Implementierung und Integration der Komponenten den verfeinerten Cybersecurity-Anforderungen und dem Architektur-Design entspricht. Der Prozess und die Aktionen sind der ASPICE-SEC.3-Prozessdefinition ähnlich. Die Verifizierungsprozesse für Software-, Hardware-, System- und Objektintegration müssen eingehalten werden.

Validierung

Die Cybersecurity-Validierung nach ISO/SAE 21434 konzentriert sich auf die Elementebene. Die Prozessziele sind die gleichen wie bei ASPICE SEC.4. Es müssen eine Reihe von Validierungsmaßnahmen durchgeführt werden, um zu bestätigen, dass die Cybersecurity-Ziele und -Ansprüche erfüllt wurden. Wie in Bild 5 dargestellt, führt KPIT im Rahmen des Fahrzeugprojekts verschiedene Validierungsaktivitäten durch.

Produktion

Ein Cybersecurity-Fall und ein Bewertungsbericht müssen vor Beginn der Produktion fertig sein. Die Produktionskontrollpläne müssen gemäß ISO/SE 21434, Abschnitt 12, erstellt werden und Anweisungen zur Installation der Ausrüstung enthalten, damit keine unbefugten Änderungen vorgenommen werden können.

Sichere Abläufe

Cybersecurity ist auch außerhalb der Serienproduktion ein Thema. Neu aufgedeckte Schwachstellen müssen behoben werden. Für diese Stufe gilt ISO/SAE 21434, Abschnitt 13. Zu den Aktivitäten gehören die Aktualisierung der öffentlich zugänglichen Schwachstellendatenbank, der Abgleich neu entdeckter Schwachstellen mit der Produktfunktionalität / dem Produktdesign und gegebenenfalls eine Risikobewertung für alle Design-Änderungen oder neu entdeckten Schwachstellen. Es ist wichtig, interne und externe Quellen zu überwachen, nach definierten Auslösern zu sortieren und Cybersicherheitsereignisse zu analysieren.

Schlussfolgerung

Infolge der neuen Vorschriften ist Cybersecurity keine Option mehr. Sie ist wie die funktionale Sicherheit obligatorisch. Ein Prozessmodell für die Cybersicherheit kann in Übereinstimmung mit verschiedenen Normen und egulatorischen Anforderungen erstellt werden. Dieses fügt sich nahtlos in andere damit verbundene Entwicklungsaktivitäten ein und trägt dazu bei, Redundanz und Verwechslung zu vermeiden. ■ (eck)

www.kpit.com

Biju Sadasivan arbeitet als Associate Solution Architect bei der MicroFuzzy GmbH – Member of KPIT Group.
© KPIT Technologies