Funktionale Cybersicherheit

Sicherheitsmechanismen zur Absicherung von IT-Komponenten und Netzwerken in Fahrzeugen

Marius Golombeck

Fachhochschule Dortmund University of Applied Sciences and Arts, Dortmund, Germany
magol003@stud.fh-dortmund.de

Abstract. Moderne Fahrzeuge bieten dem Fahrer und den Fahrzeuginsassen eine Vielzahl an Funktionen. Von modernen Fahrassistenzsystemen, bis hin zu komplexen Infotainmentsystemen mit Smartphone-Integration sind moderne Fahrzeuge längst mehr als nur mechanische Fortbewegungsmittel. Die Hochtechnologie-Transformation des Automobils bietet zahlreiche Vorzüge sowie neue Möglichkeiten für Angriffe auf die Fahrzeuginfrastruktur. Durch die Integration der Fahrzeugsysteme entsteht ein komplexes Hard- und Softwarenetz mit Zugriffsmöglichkeiten auf z.T. hochanfällige und sicherheitskritische Komponenten. Durch den Einsatz grundlegender Konzepte zur Risikominimierung, sicherheitszuträglicher Systemarchitekturen sowie den Sicherheitsmodulen und -funktionen aus modernen Softwareplattformen kann die Sicherheit im gesamten Entwicklungsprozess gewährleistet und für das Endprodukt maximiert werden. Aktuelle Standards zur funktionalen Cybersicherheit, wie z.B. ISO/SAE 21434, können durch die Bildung einer gemeinsamen Basis innerhalb der Automobilindustrie zu einer erheblichen zur Verbesserung des Sicherheitsniveaus beitragen. Eine Absicherung hochintegrierter eingebetteter Systeme ist essenziell, um die Fahrzeugsicherheit auch zukünftig zu gewährleisten.

Keywords: Automotive Security, Network Security, Embedded Systems Security

DOI: 10.13140/RG.2.2.13195.92961

1 Funktionale Cybersicherheit

Die funktionale Sicherheit beschreibt Prozesse zur Durchführung von Sicherheitsaktivitäten für alle Phasen des Sicherheitslebenszyklus - und damit des Produktlebenszyklus. Für die Entwicklung von Fahrzeugen existiert eine Vielzahl an allgemein anerkannten Standards und Leitlinien. Diese werden in der Regel in Arbeitsgruppen und Kommissionen erarbeitet, die sich aus Experten der Automobilindustrie, Zulieferern, Herstellern und Domänenexperten zusammensetzt. So soll garantiert werden, dass alle Interessen vertreten und aktuelle sicherheitsrelevante Themen angesprochen werden. Außerdem werden in diesen Diskussionen auch aktuelle Ansätze der Forschung und neu entwickelte Komponenten in Fahrzeugen diskutiert und bewertet.

1.1 Standards der funktionalen Cybersicherheit

Im Bereich der funktionalen Cybersicherheit, also den Maßnahmen zur Verteidigung gegenüber maliziösen Angriffen, existieren jedoch nur wenige allgemein anerkannte Standards. Im Folgenden werden drei aktuell internationalen verbreitete Standards zur funktionalen Cybersicherheit von Fahrzeugen vorgestellt:

- ISO [1]26262 - „Road vehicles – Functional safety“
- SAE [2]J3061 - „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems“
- ISO/SAE 21434 - „Road vehicles - Cybersecurity engineering“

1.1.1 ISO 26262

Die Norm ISO 26262 bezieht sich auf die Cybersicherheit elektrischer und elektronischer Systeme innerhalb eines Fahrzeugs (PKW bis 3.5t zulässigem Gesamtgewicht). Sie behandelt mögliche Gefahren durch Fehlverhalten sicherheitsrelevanter Systeme, einschließlich der Interaktion dieser Systeme [1]. Die Entwicklung in internationalen Arbeitsgruppen beginnt 2005 und dauert 10 Jahre bis zur finalen Publikation im Jahr 2015. Die neuste Fassung wurde 2018 veröffentlicht. ISO 26262 adaptiert die Norm für Elektrik und Elektronische Systeme IEC 61508 speziell auf die funktionale Cybersicherheit von Automobilen.

Durch den Einsatz des ISO 26262 Standards soll die Systemsicherheit durch eine Reihe von Sicherheitsmaßnahmen erreicht werden, die in einer Vielzahl von Technologien implementiert und auf den verschiedenen Ebenen des Entwicklungsprozesses angewendet werden. Obwohl sich ISO 26262 primär mit der funktionalen Cybersicherheit von E/E-Systemen befasst, beinhaltet sie weitere angeschlossene

[1] International Organization for Standardization
[2] Society for Automotive Safety Engineers

Tätigkeiten, insbesondere während der Entwicklung, um bereits früh sicherheitsorientierte Produktstandards zu gewährleisten [2]. Hierzu zählen in erster Linie:

- Planung, Kontrolle und Anpassung des automobilen Sicherheitslebenszyklus (Management, Entwicklung, Produktion, Betrieb, Wartung)
- Das Automotive Safety Integrity Level (ASIL) Schema zur Risikobewertung und Klassifikation von Funktionen und Systemen
- Anforderungen und Validierungsmaßnahmen binnen eines begleitenden Anforderungsmanagements anhand der o.g. ASIL-Klassifikation (sowohl unternehmensintern wie auch für Stakeholder, z.B. Zulieferer)

Die Domäne der funktionalen Cybersicherheit umfasst insbesondere Bereich der Fahrerassistenzsysteme, des Antriebs, der Fahrdynamikregelung und/oder in aktive und passive Sicherheitssysteme. Mit dem Trend zunehmender technologischer Komplexität, Softwareinhalte und mechatronischer Umsetzung steigen die Risiken durch systematische Ausfälle und technisch bedingte Hardwareausfälle [1]. Der Standard ISO 26262 enthält vielfältige Anleitungen zur Vermeidung dieser Risiken und bietet entsprechende Methoden des Anforderungsmanagements und Prozessvorlagen (siehe Abbildung 1).

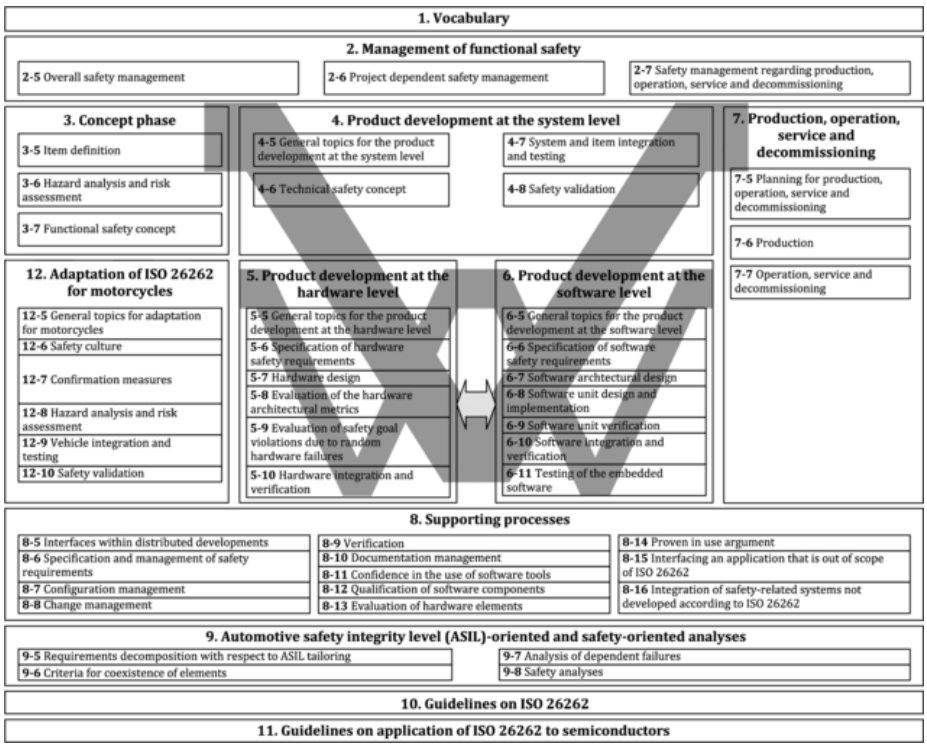

Abbildung 1 - Übersicht über den ISO 26262 Standard [2]

Hierzu ist die Norm im Kern in zehn Kapitel unterteilt. Kapitel 11 bezieht sich auf die Anwendung in der Halbleiterfertigung und Kapitel 12 (in Abbildung 1 nicht aufgeführt) betrifft Motorräder. Sie werden in dieser Arbeit nicht behandelt [2]:

- Kapitel 1 - „Vocabulary“ ist ein Metakapitel und enthält die Sprachelemente von ISO 26262, also Terminologien, Abkürzungen und Begriffserklärungen [2].
- Kapitel 2 - „Management of functional safety“ bezieht sich auf das Management von Cybersicherheitsanforderungen, sowohl aus einer organisatorischen wie auch aus einer projekt- und prozessorientierten Sichtweise [2].
- Kapitel 3 - „Concept phase“ betrachtet die initiale Projektdefinition und begründet detaillierte Cybersicherheitsanforderungen und -kriterien für das Projekt und initiiert damit den Sicherheitslebenszyklus [2].
- Kapitel 4 - “Product development at the system level” bezieht sich auf die Softwareentwicklung auf Systemebene. Es umfasst detaillierte Anforderungsanalysen, Systemkonzeption, funktionale und logische Einteilung sowie deren Evaluierung, Validierung und Verifikation [2].
- Kapitel 5 - “Product development at the hardware level” behandelt das hardwareseitige Systemdesign und dessen -implementierung [2].
- Kapitel 6 - “Product development at the software level” behandelt das softwareseitige Systemdesign und dessen -implementierung [2].
- Kapitel 7 - “Production and operation” spezifiziert die Anforderungen für die Systemproduktion, -operation, -installation, -wartung und -stilllegung [2].
- Kapitel 8 - “Supporting processes” definiert Unterstützungsprozesse der Entwicklung Prozessanforderungen. Außerdem werden hier die Bereiche Change-Management, Standards in der Dokumentation, Tool Qualifikationen, Verifikation und Validierung behandelt [2].
- Kapitel 9 - “Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses” definiert ASIL als Schema zur Risikobewertung und Klassifikation von Funktionen und Systemen anhand von vier Kategorien (ASIL A - D) je nach Integritätsgrad der Anforderung [2, 3].
- Kapitel 10 - “Guideline on ISO 26262” als informative Übersicht über ISO 26262 mit weiterführenden Erläuterungen zum Verständnis der vorgehenden Kapitel 2-9 [2].

Der Standard ISO 26262 ist ein vollständig strukturierter Leitfaden zur Entwicklung von sicherheitsrelevanten E/E-Systemen und -Funktionen in Fahrzeugen. Trotz starker Standardisierung innerhalb einer hochkomplexen Domäne bietet die Vorgehensweise nach ISO 26262 ausreichend Flexibilität zur Anpassung auf konkrete Nutzerszenarien und Anwendungsfälle. Durch die Adaption des allgemeinen IEC 61508 Standards werden bewährte Szenarien aus dem Bereich der Elektrik und Elektronik genutzt und für den Einsatz im Fahrzeug spezifiziert [3, 4].

Der Ausschluss bzw. die Vernachlässigung von systematischem Versagen bei der Risikoprognostizierung können zu einer impliziten Unterschätzung des Risikos führen. So besteht selbst bei minutiöser Detailarbeit im Rahmen des Standards keine Garantie,

dass Konstruktionsfehler auch nach Abschluss der Vorphase weiter verborgen bleiben. Durch den Ansatz der produktlebenszyklusbegleitenden Entwicklung können diese Fehler jedoch auch nach kommerzieller Einführung eines Fahrzeugs korrigiert werden.

Die Verwendung von ISO 26262 stellt einen bedeutenden Schritt in der cybersicherheitsorientierten Fahrzeugsoftwareentwicklung dar. Der Paradigmenwechsel, von einer schwarz-weißen Risikobetrachtung hin zu einer detaillierten und probabilistischen Einschätzung, führt schlussendlich zu präziseren Anforderungen und einer effizienteren Entwicklung [4].

1.1.2 SAE J3061

Der SAE J3061 Standard definiert einen Prozessrahmen für den Sicherheitslebenszyklus in verteilten E/E-Systemen. Er wurde 2016 veröffentlicht und bietet auf hoher Ebene eine Vielzahl an Anleitungen, Methoden und Best-Practice-Werkzeugen für sicherheitsrelevante Entwicklungsprozesse [5]. Die originären Ziele bei der Entwicklung von SAE J3061 sind die Entwicklung eines global harmonisierten Ansatzes zur Bestimmung von ASIL Klassifikationen (siehe Kapitel 1.1.1) sowie die Festlegung von standardisierten Metriken [5].
Die Motivation dahinter ist, in erster Linie das Thema der funktionalen Cybersicherheit in Fahrzeugen auf abstrakter Ebene, strukturiert zu adressieren. Durch die Vielzahl an involvierten Stakeholdern bei der Fahrzeugentwicklung sei ein integrierter, branchenübergreifender Ansatz die Lösung, um nachhaltige Cybersicherheit zu garantieren [5]. Als Basis nutzt SAE J3061 das Rahmengerüst von ISO 26262, verfolgt jedoch einen pragmatischeren, flexibleren und stärker adaptierbaren Ansatz zur Steigerung der funktionalen Sicherheit von E/E-Komponenten [6]. Wie bei ISO 26262 deckt SAE J3061 den gesamten Produktlebenszyklus ab [6]. Organisationen besitzen die Möglichkeit SAE J3061 separat oder in Verbindung mit einem weiteren Sicherheitsprozess (z.B. ISO 26262, siehe Kapitel 1.1.1) anzuwenden.

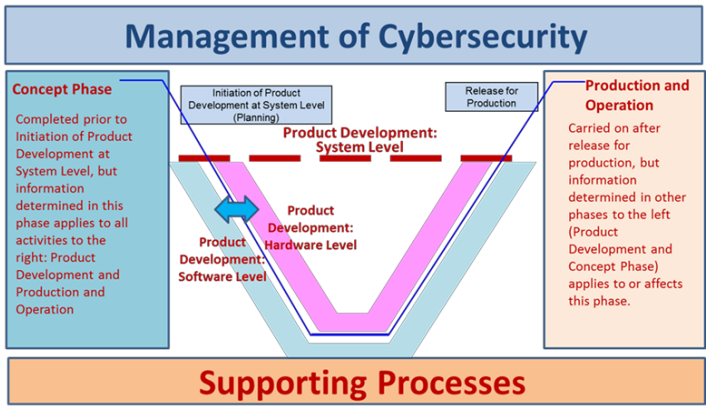

Abbildung 2 - Überblick über SAE J3061 [6]

Wie in Abbildung 2 zu erkennen teilt sich SAE J3061 in zwei Phasen auf. Die Konzeptphase sowie die Produktions- und Betriebsphase. Phasenübergreifend werden sie von Managementprozessen gesteuert und durch Unterstützungsprozesse assistiert. Im Kern steht die Produktentwicklung. Dort unterscheidet SAE J3061 zwischen Systemebene sowie Hard- und Softwareebene [6].

Die Konzeptphase besteht aus sieben Schritten und wird, wie in Abbildung 3 dargestellt, durch ein Flussdiagramm beschrieben. Das Ziel der Konzeptphase ist die Definition von Cybersicherheitszielen und -strategien der funktionalen Cybersicherheit auf hohem Sicherheitsniveau. Die Ziele und die Strategie werden dann verfeinert, um technische Details in die Produktentwicklungsphase einzubeziehen [6].

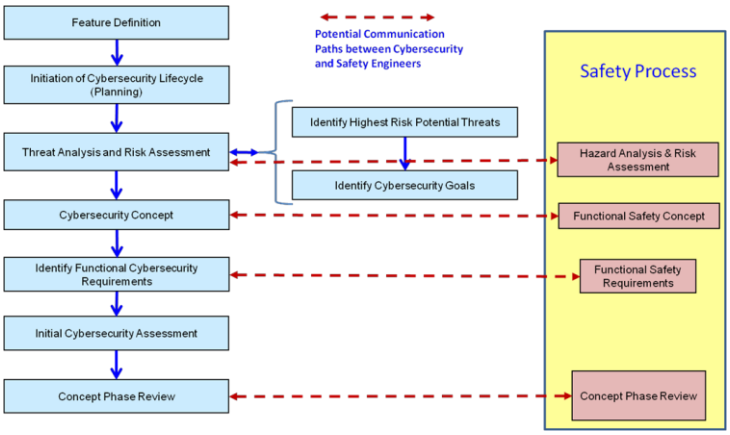

Abbildung 3 - SAE J3061 Konzeptphase Flussdiagramm mit Kommunikationswegen zu angeschlossenem Sicherheitsprozess [6]

Die Konzeptphase (1) beginnt mit der Definition von Merkmalen und Grenzen des Systems sowie dem Umfang der zu leistenden Arbeit. In der Initiierungsphase (2) wird das Projekt geplant und im Hinblick auf den Produktlebenszyklus dokumentiert. Die Hauptaktivität in der Konzeptphase ist die Bedrohungsanalyse und Risikobewertung (TARA[3], 3). Ihr Ziel ist die Identifizierung potenzieller Bedrohungen sowie die Beurteilung und Bewertung der Risiken im Zusammenhang mit ihren Bedrohungen. Anschließend erfolgt die Konzeptfestlegung auf Systemebene (4), welche im Rahmen der späteren Produktionsentwicklungsphase zu einer technischen Strategie verfeinert wird. Darauf folgt die Ermittlung funktionaler Cybersicherheitsanforderungen (5), die aus der Sicherheitsstrategie abgeleitet werden, um den Sicherheitszielen gerecht zu werden. Die Strategie wird somit, basierend auf den Ergebnissen der identifizierten Bedrohungen und Risiken durch das TARA, aus den allgemeinen Zielen abgeleitet. Die letzten beiden Schritte der Konzeptphase sind eine erste Bewertung der Sicherheit (6) und eine Überprüfung der gesamten Konzeptphase (7) im Sinne einer Qualitätskontrolle [5].

[3] Threat analysis and risk assessment

Der begleitende Managementprozesses zielt vor allem darauf ab, eine Sicherheitskultur zu bilden, welche ein effektives Sicherheitsmanagement innerhalb einer Organisation ermöglichen soll. Hierzu sind u.a. die folgenden Schritte angedacht [6]:

- Messung der Konformität eines Sicherheitsprozess
- Identifikation und Einrichtung von Kommunikationskanälen
- Entwicklung und Durchführung von Schulungen und Mentoring
- Betrieb und Wartungstätigkeiten (Incident Management, Monitoring im Betrieb)

Die Produktentwicklung wird, wie in der automobilen Softwareentwicklung typisch, als V-Modell skizziert. Es erfolgt, wie eingangs beschrieben, eine Gliederung in System- sowie Hard- und Softwareebene (siehe Abbildung 4).

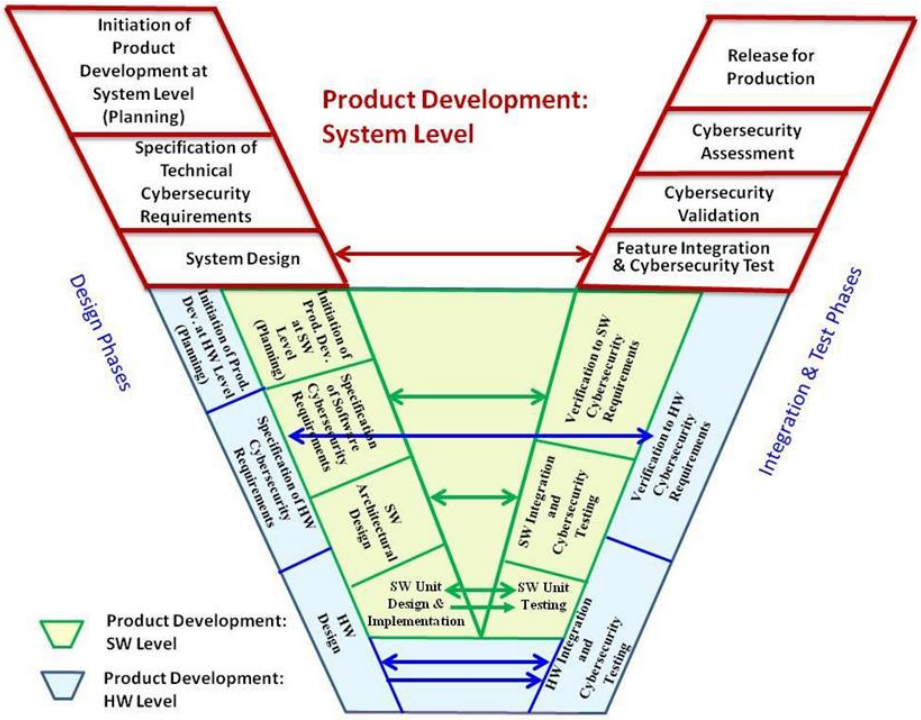

Abbildung 4 - SAE J3061 V Modell - Beziehungen zwischen Entwicklungsaktivitäten

Weiterhin enthält J3061 eine Reihe von Anhängen, die auf andere Sicherheits-Standards und -Richtlinien, Sicherheitsanalysetechniken, Sicherheits- und Datenschutzkontrollen, Schwachstellen-Datenbanken und in der Branche verwendete Klassifizierungsschemata verweisen [6].

J3061 ist eine der wenigen umfassenden Implementierungsrichtlinien für funktionale Sicherheit in der Automobilindustrie. Er wurde speziell mit Blick auf die funktionale

Cybersicherheit (und insbesondere auf ISO 26262) entwickelt [6]. Die von der SAE in dieser Hinsicht geleistete Arbeit wird nicht nur von der Automobilindustrie, sondern auch von anderen Normungsorganisationen anerkannt (z.B. ISO, siehe 1.1.3) und bildet die Grundlage für den kommenden Standard ISO/SAE 21434.

1.1.3 ISO/SAE 21434

ISO/SAE 21434 ist der erste von der ISO und der SAE gemeinsam entwickelte Standard zur funktionalen Cybersicherheit in Fahrzeugen. In Anerkennung des wachsenden Cybersicherheitsbedarfs wurde der Standard im Zusammenschluss aus mehr als 80 Unternehmen und Organisationen erarbeitet, welche mit der Automobilindustrie verbunden sind [7]. Die Norm beschreibt wie eine Kultur der Cybersicherheit etabliert werden kann, um mit den technologischen Veränderungen und Angriffen Schritt zu halten. Hierbei konzentriert sie sich auf die Schnittstelle zwischen funktionaler Sicherheit und Cybersicherheit - also den sicherheitsrelevanten, aber nicht unbedingt sicherheitskritischen, Funktionen und Systemen [7]. Es wird erkannt, dass es notwendig ist, die automobile Entwicklung klar vor dem Hintergrund von Cybersicherheit auszurichten. Ein solcher domänenspezifischer Cybersicherheits-Engineering-Standard soll nicht nur dem aktuellen Stand der Technik gehorchen, sondern auch die Zusammenarbeit zwischen Partnern in der Automobilindustrie unterstützen. Dies soll durch klare Terminologie und risikobasierte Managementansätze sowie durch die Definition klarer Schnittstellen zwischen den Unternehmen erfolgen [7]. Die Entwicklung beginnt im Oktober 2016. Die aktuelle Konzeptvorlage datiert auf Februar 2020. Die finale Veröffentlichung ist für Dezember 2020 geplant [8].

Die Entwicklung von ISO/SAE 21434 wird auf oberster Ebene in vier Kapitel[4] (PG1 - PG4) eingeteilt, dessen Inhalte von sog. Joint Working Groups erarbeitet und verwaltet werden. PG1 umfasst das Risikomanagement, PG2 die Systementwicklung, PG3 den Betrieb, Wartung und andere zugehörige Prozesse und PG4 bietet eine Prozess- und Interdependenzübersicht (siehe Abbildung 5).

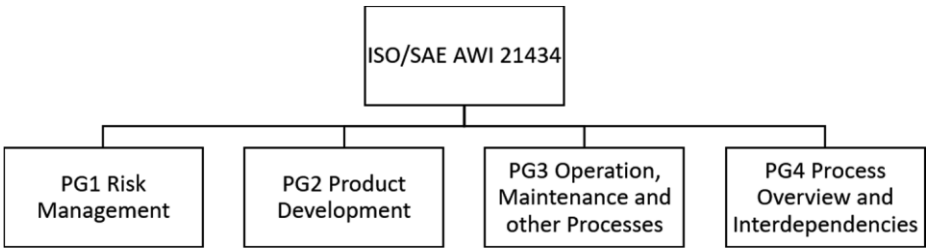

Abbildung 5 - ISO/SAE 21434 Joint Working Group Struktur [7]

[4] Sog. Project Groups

Die Phase des Risikomanagements (PG1) ist eine der Kernaktivitäten in der Sicherheitstechnik. Das Endziel des Risikomanagements ist die Sicherstellung der Parameterkonformität innerhalb von akzeptablen Risikoaußengrenzen. Hierbei werden vier aufeinanderfolgende Kernaktivitäten durchgeführt (siehe Abbildung 6) [7].

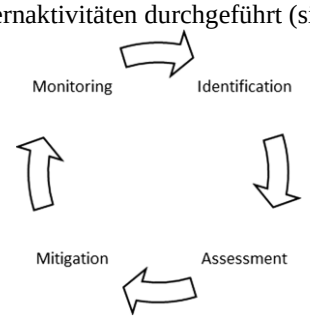

Abbildung 6 - Risikomanagement (PG1) in ISO/SAE 21434 [7]

Das Risikomanagement ist ein fortlaufender Prozess während des gesamten Sicherheitslebenszyklus. Daher ist eine wichtige Eigenschaft des Konzepts von PG1, Methoden und Ansätze bereitzustellen, die auch in anderen Abschnitten des Sicherheitslebenszyklus eingesetzt werden können. Eine der ersten bereitgestellten Methoden ist die Bewertung der Cybersicherheitsrelevanz. Wenn eine der Fragen in Tabelle 1 mit „Ja“ beantwortet wird, fällt das System in den Geltungsbereich von ISO/SAE 21434 [7].

Physische oder drahtlose Verbindung zu einem beliebigen Element der internen Fahrzeugkommunikation	Ja / Nein
Physische oder drahtlose Verbindung zu einem beliebigen Element der externen Fahrzeugkommunikation	Ja / Nein
Indirekte Verbindung zu einem beliebigen Element des Fahrzeugkommunikationsnetzwerks	Ja / Nein
Enthält elektronische / optronische Geräte oder Hardware	Ja / Nein
Enthält Software	Ja / Nein
Enthält Sensoren	Ja / Nein

Tabelle 1 - Bestimmung der Cybersicherheitsrelevanz [7]

Das Ziel dieser Cybersicherheitsrelevanz Bewertung ist es, ein schnelles, unkompliziertes Werkzeug bereitzustellen, das verwendet werden kann, um festzustellen, ob die Cybersicherheit bei der Entwicklung berücksichtigt werden sollte [7].

In der Phase der Systementwicklung (PG2) richtet sich ISO/SAE 21434 wie bereits ISO 26262 und SAE J3061 (siehe 1.1.1, 1.1.2) am V-Modell aus. Abbildung 7 zeigt einen Überblick über die Phasen der Systementwicklung. In der Konzeptphase wird der Gegenstand der Entwicklung definiert und es werden unter Verwendung der Bedrohungsanalyse und Risikobewertung (TARA, siehe Kapitel 1.1.2)

Cybersicherheitsziele definiert. Während der Systemspezifikation werden die Anforderungen verfeinert und den Bereichen Software und Hardware zugeordnet. Folglich wird eine Schwachstellenanalyse und Risikobewertung durchgeführt, um sicherzustellen, dass keine zusätzlichen Bedrohungen eingeführt werden und das Restrisiko akzeptabel ist. Für die sichere Softwareentwicklung existieren Anleitungen, insbesondere mit dem Fokus auf sichere kooperative Soft- und Hardware-Entwicklung. Nach den Design- und Development-Phasen schließen Systemverifikation und Validierungstests die Entwicklung ab [7].

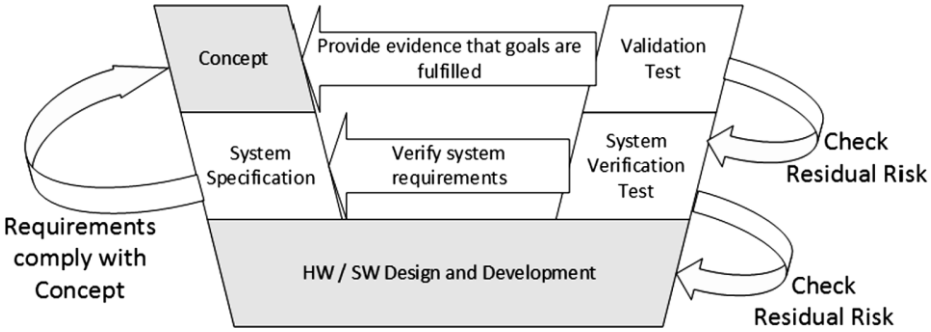

Abbildung 7 - ISO/SAE 21434 V-Modell der Systementwicklung [7]

Die Phase PG3 bezieht sich auf die Produktion und den Betrieb der Soft- und Hardware, um auch hier eine vollständige Abdeckung des Lebenszyklus zu gewährleisten. Der Fokus liegt in der Produktion auf einem sicheren Transfer von der Entwicklung in ein Produktivsystem sowie auf dem Schutz von Produktionsartefakten. Weiterhin konzentrieren sich die Tätigkeiten im Betrieb auf Monitoring, Incident Response und das ausrollen von Updates [7].

In Phase PG3 werden initial Anforderungen angegeben, welche sicherstellen sollen, dass keine unautorisierten Änderungen durchgeführt werden kann - in der Lieferkette oder während der Produktion. Schwerpunkt ist der Schutz der Produktivsetzung und sämtlicher Informationen, vom Entwurf bis zur Produktion. Die vorgestellten Methoden reichen von klassischen Cybersicherheitsmethoden, über kryptographische Hashes bis zur Kontrolle und Beschränkung des physischen Zugangs. Bei der Produktivsetzung von Software wird zur Installation und Konfiguration sowie zur Verteilung von kryptographischen Schlüsseln ein uneingeschränkter Zugang benötigt. Während dieser Phase ist das System anfällig und der Zugang zu Werkzeugen und Systemen muss streng kontrolliert werden. Weiterhin muss sichergestellt werden, dass Produktionsschnittstellen deaktiviert und geschützt werden, sofern sie im Produktivbetrieb nicht mehr benötigt werden [7].

Um die Cybersicherheit während des Betriebs zu gewährleisten, ist es notwendig, nicht nur Vorfälle zu überwachen, sondern auch für eventuelle Schwachstellen vorbereitet zu sein, die entweder während der Entwicklung unbemerkt bleiben oder durch neu angeschlossene Hard- oder Software entstehen. Somit werden an dieser Stelle

Richtlinien und Verfahren für die Reaktion auf potenzielle Schwachstellen und die Reaktion auf Vorfälle definiert.
Abschließend wird in PG3 die sicherheitskonforme Systemaktualisierung thematisiert. So soll gewährleistet werden, dass Systemaktualisierungen korrekt durchgeführt werden können, während die benötigte Funktionalität dafür höchsten Sicherheitsstandards genügt. Alle cybersicherheitsbezogenen Systeme die prinzipiell die Cybersicherheit des Systems beeinflussen können, sollen Update-Fähigkeiten besitzen. Darüber hinaus darf keine Systemkomponente in einen unvorhergesehenen Fehlerzustand verfallen und das System muss in der Lage sein, sich bei einem (teilweisen) Systemausfall korrekt zurückzusetzen. Außerdem muss ein Update stets verifiziert werden, um die Einschleusung maliziösen Programmcodes zu unterbinden [8]. Es ist also erforderlich ein Gleichgewicht zwischen Verfügbarkeit, der Wiederherstellung des ursprünglichen Zustands und der Sicherheit zu gewährleisten [7].

Die Prozess- und Interdependenzübersicht (PG4) behandelt Aktivitäten, die nicht in direktem Zusammenhang mit konkreten Cybersicherheitsaktivitäten stehen, die aber dennoch für die Erreichung der gesamthaften Cybersicherheit notwendig sind. Hierzu gehören u.a. die Entwicklung einer Cybersicherheitskultur und das Management der Cybersicherheit in der gesamten Organisation [7]. Ziel dabei ist es die Anforderungen und Richtlinien so zu definieren, dass Cybersicherheit als Priorität und Qualitätsmerkmal akzeptiert wird – und nicht als Hindernis bei der Produktentwicklung durch höheren Prozessaufwand. Hier werden z.B. Incident Response Levels zur Cybersicherheit festgelegt sowie dazu konkrete Beispiele für eine adäquate Cybersicherheitskultur gegeben [7].

Weiterhin ist in PG4 das Konzept des Development Interface Agreement (DIA) aus ISO 26262 in einer erweiterten Version enthalten [7]. Diese Vereinbarung dient zur Dokumentation von Verantwortlichkeiten, zum Informationsaustausch und zur Arbeitsteilung zwischen Zulieferern und OEMs. Mit Vorlagen zur Strukturierung und Zuteilung von Verantwortlichkeiten versucht mehr Formalismus einzuführen. Hiermit können zwischen OEMs und Zulieferern zusätzliche Schnittstellenvereinbarungen zur Wartung oder für Incident Management Aktivitäten getroffen werden [7].

Abbildung 8 zeigt den vollen Umfang von ISO/SAE 21434 von insgesamt 15 Kapiteln und detailliert ihren Inhalt.

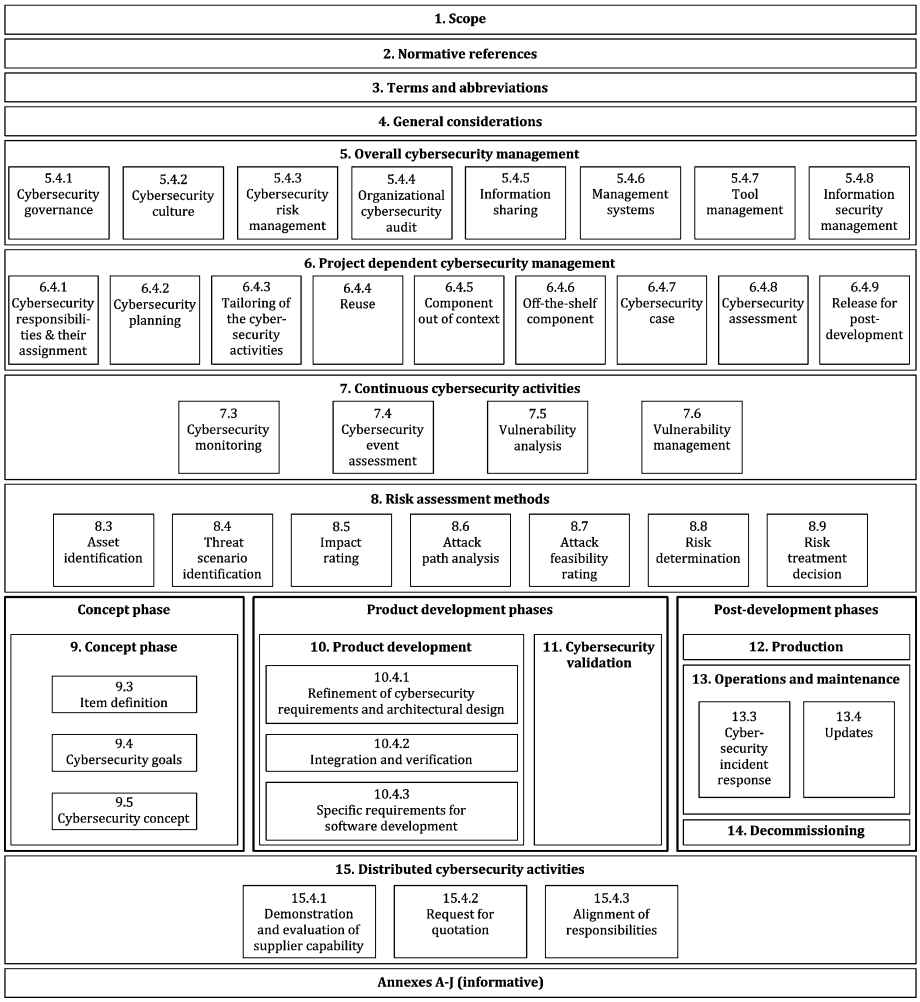

Abbildung 8 - Übersicht über den ISO/SAE 21434 Standard [9]

Die strukturelle Ausrichtung an ISO 26262 (siehe Abbildung 1) ist zu erkennen. Einige Themen, wie Datenschutz und Privatsphäre sowie die Interaktion zwischen Sicherheit und Schutz sind momentan noch nicht ausreichend abgedeckt, werden ISO/SAE 21434 allerdings zukünftig ergänzen [7, 9]. Dies ist insbesondere dem Zeitdruck bei der Entwicklung geschuldet [7, 9].

Insbesondere ISO/SAE 21434 besitzt das Potenzial, eine gemeinsame Basis innerhalb der Automobilindustrie zu schaffen, indem es die Vorteile aus den Standards ISO 21262 und SAE J3061 vereint und den Fokus auf die funktionale Cybersicherheit legt.

1.2 Konzepte zur Risikominimierung

Die Konzepte zur Risikominimierung der in Kapitel 1 vorgestellten Standards finden bereits in zahlreichen Fahrzeugkomponenten Verwendung [10]. In diesem Kapitel wird auf Basis der Konzepte zur Risikominimierung aus ISO 26262 (siehe Kapitel 1.1.1) ein Einblick in ausgesuchte Konzepte gegeben, welche anhand von Beispielen praxisorientiert erläutert werden.

1.2.1 Plausibilitätskontrollen

Eine Plausibilitätskontrolle stellt meist das letzte Hindernis dar, bevor ein Fehlerzustand erzeugt wird. Es handelt sich hierbei um einfache Prüfungen, durch die festgestellt wird, ob alle Voraussetzungen für die sichere Ausführung einer Funktion gewährleistet sind [11]. Um eine geforderte Systemintegrität zu gewährleisten, müssen die Systeme fehlertolerant, zuverlässig und sicher sein. Ein fehlertolerantes System muss also in der Lage sein, Fehler korrekt und schnell zu erkennen (siehe Abbildung 9) [12].

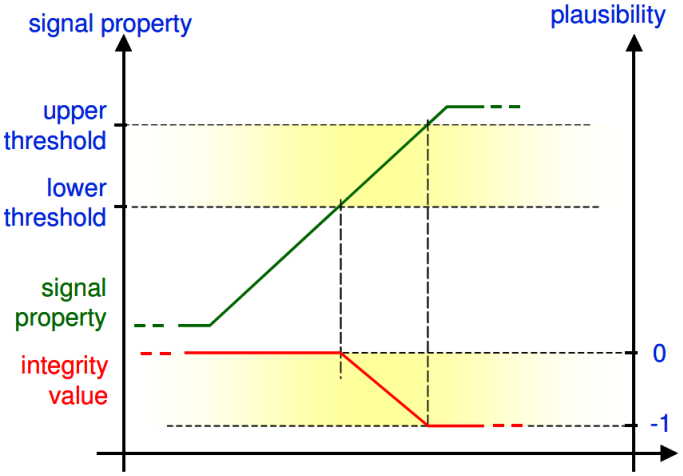

Abbildung 9 - Plausibilitätskontrolle eines Einzelsignals mittels Werteintegrität [12]

Abgebildet ist ein einzelnes Sensorsignal mit festgelegten Ober- und Untergrenzen sowie dem Integritätswert minus eins. Solange das Signal sich zwischen den erlaubten Grenzen bewegt, werden die Sensorwerte als plausibel erachtet. Mit dem Überschreiten des oberen Schwellenwerts, degradiert[5] der Signalwert zum Integritätswert und erreicht seinen definierten Mindestwert von minus eins. Das System ist so eingerichtet, dass alle berechneten Plausibilitätswerte auf den Wertebereich von null bis eins normalisiert werden. Dies garantiert die Vergleichbarkeit der berechneten Plausibilitätswerte im gesamten System [12].

[5] Funktionseinbuße oder -Verlust nach Fehlereintritt

1.2.2 Fehlererkennung

Zur Erkennung von Fehlern werden zumeist Plausibilitätskontrollen verwendet (siehe Kapitel 1.2.1). Ein Mechanismus zur einfachen Fehlererkennung ist die Beschränkung von physikalischen Steuergrößen auf einen erlaubten Wertebereich. Wenn ein Sensor einen erlaubten Wertebereich von 0,5 V bis 1,8 V besitzt und dieser unter- oder überschritten wird (z.B. 0 V), wird ein Fehler erzeugt. Dieses Prinzip kann durch redundante Sensorlegung (siehe Kapitel 1.2.6) verstärkt werden. So kann ein Fehler erkannt und trotzdem ein korrektes Sensorsignal verarbeitet werden [13].

1.2.3 Fehlerbehandlung

Auftretende Fehler werden dem zentralen Fehlermanagement gemeldet und in einem Ereignisspeicher abgelegt. Zu jedem erkennbaren Fehler gibt es eine vorher definierte Sicherheitsbetrachtung [13]. Diese legt fest, wie betroffene Steuergeräte beim Eintreten des jeweiligen Fehlers reagieren. Beispielsweise werden bei einem Fehler der Innenraumbeleuchtung nicht auch die Schweinwerfer abgeschaltet. Hier ist ein Kompromiss aus Sicherheit und Verfügbarkeit zu treffen [13]. Die Strategie zur Fehlerbehandlung ist komponentenindividuell und lässt sich nicht allgemein beantworten [13]. Dies macht eine ausführliche individuelle Betrachtung der Risiken im Vorfeld der Entwicklung umso wichtiger, um burschikose Strategien zur Fehlerbehandlung zu auszuarbeiten [4, 13].

1.2.4 Abgestufte Funktionseinschränkungen

Zur Aufrechterhaltung der Hauptfunktionalität eines Systems können weniger kritische Komponenten abgeschaltet werden. Ein modulares Systemdesign stellt hierfür die Basis dar. Stets muss hierbei der Betriebszustand des Fahrzeugs berücksichtigt werden. Eine Systemkomponente die während dem Stand keinerlei Kritikalität aufweist, kann z.B. während der Fahrt höchstkritisch für die Sicherheit der Fahrzeuginsassen sein. Als Beispiel sei die Abschaltung sämtlicher Kommunikationsfunktionen ausgehend der zentralen Steuereinheit bei einem OTA-Update genannt, welches nur im Stand bzw. im Wartungsmodus durchgeführt werden kann. So kann gewährleistet werden, dass das Fahrzeug erst dann wieder in den Betriebszustand überführt wird, wenn das Update erfolgreich eingespielt und verifiziert wurde. Auf elementarer Ebene, beim Ausfall oder Fehlerzustand von Sensoren, kann durch eine bei der Entwicklung korrekt definierte Parameterlogik sichergestellt werden, dass fehlerhafte Messwerte nicht zu weitreichenden Fehlzuständen führen [13]. Als Beispiel kann ein Getriebesensor genannt werden, der im Fehlerzustand falsche Werte zurückliefert und somit der ECU übermittelt, dass ein zurückschalten in den Rückwärtsgang möglich ist, obwohl sich das Fahrzeug in voller Vorwärtsfahrt befindet, was zu einem Totalschaden des Getriebes führen würde. Dies kann z.B. durch Nutzung noch vorhandener Messwerte und korrekte Parametrisierung während der Systemkonfiguration umgangen werden [13].

Abgestufte Funktionseinschränkungen lassen sich meist während der Systemkonzeption definieren [13]. Standards in Normen unterstützen hier insbesondere bei der Händelbarkeit der Komplexität eines Systems. Informationen aus einer vorgelagerten Risikomanagementphase können zur Bewertung genutzt werden [10].

1.2.5 Diversitäre Programmierung

Die diversitäre Programmierung beschreibt die Entwicklung der gleichen Aufgabe durch unterschiedliche Herangehensweisen (z.B. durch unterschiedliche Entwickler, andere Programmiersprachen, Compiler oder Toolketten) [13, 14]. Die Fehlertoleranz gegenüber Entwicklungsfehlern wird durch die Vermeidung eines Single-Point-of-Failure erhöht. In diesem Sinne darf auch ein Entwickler nie seine eigene Software testen und freigeben [13]. Zur Sicherstellung einer diversitären Entwicklung erfolgen alle Freigaben nach Reviews im Mehraugenprinzip [13]. Dies stellt mitunter einen erheblichen Mehraufwand dar und sollte daher nur gezielt eingesetzt werden um einen effizienten Entwicklungsprozess zu garantieren [14].

1.2.6 Redundanz

Eine redundante Auslegung von Sensoren, Rechnern bzw. deren Komponenten oder ganzen Systemen erhöht die Verfügbarkeit eines Systems und führt somit zur Verbesserung der Sicherheit [15]. Beim Ausfall einer Komponente kann eine redundante Komponente die Funktionalität übernehmen. Ein ideales Redundanzkonzept stellt eine vollständige Fehlertoleranz, mit uneingeschränktem Weiterbetrieb nach Fehlereintritt, ohne zusätzlichen Platzbedarf im Automobil dar. Dies ist jedoch meist nicht realistisch, sodass meist eine teilweise Fehlertoleranz mit etwaiger Degradation bei höherem Platzbedarf erreicht wird. Grundsätzlich stehen bei der Frage nach einer redundanten Auslegung stets Kosten und Nutzen gegenüber.

1.3 AUTOSAR Security Module und Funktionen

AUTOSAR umfasst bereits verschiedene IT-Sicherheitsanwendungen zur Absicherung der Kommunikation im Fahrzeug und zum Schutz von Daten [16]. Die AUTOSAR Adaptive Plattform wird speziell im Hinblick auf hochvernetzte und autonome Fahrzeuge entwickelt und ist die aktuellste Softwareplattform von AUTOSAR. Die Erstveröffentlichung datiert auf den 31.03.2017. Die wichtigsten Treiber für die Entwicklungsinitiative sind Anwendungsfälle wie hochautomatisiertes Fahren, Car-2-X Anwendungen, Cloud Computing und erhöhte Konnektivität. Weiterhin liegt der Fokus auf Echtzeitanwendungen und Sicherheit.

Nachfolgend werden die wichtigsten Sicherheitsmodule aus AUTOSAR Classic und AUTOSAR Adaptive sowie ausgewählte Sicherheitsfunktionen vorgestellt und ein möglicher Entwicklungsprozess in Kapitel 1.3.7 durch ein Beispiel erläutert.

1.3.1 Crypto Stack

Der Crypto Stack in AUTOSAR Adaptive enthält die kryptographischen Verfahren und implementiert benötigte Keystores sowie stellt diese über einheitliche Schnittstellen zur Verfügung [17, 18]. So kann ein kontrollierter Zugriff über wohldefinierte Schnittstellen garantiert werden, unabhängig von ihren Implementierungen [18]. Außerdem wird so die Portabilität für verschiedene ECUs gewährleistet [17].

1.3.2 SecOC

Die fahrzeuginterne Kommunikation besitzt bisher mit nur wenigen Ausnahmen keine Sicherheitsmerkmale. Gegenwärtig verfügt CAN nur über CRC-Funktionen oder Checksummen, die keine effektive Sicherheit bieten [19, 20]. Der Grund dafür ist das kurze Format von CAN Nachrichten und die eingeschränkten. Neuere Bussysteme wie CAN FD[6], ermöglichen dies jedoch. Hier setzt das AUTOSAR Classic Modul SecOC[7] zur Absicherung der CAN-Kommunikation auf [21]. Es gewährleistet Authentizität und Integrität der Botschaften während der Übertragung, sichert jedoch nicht ihre Vertraulichkeit [22]. SecOC spezifiziert die Authentizität elementarer Nachrichten, und überprüft sie auf Spoofing oder Manipulation Angriffe und kann somit Replay Attacks erkennen [19]. Wie durch Miller und Valasek [23] gezeigt, verfügt ein Angreifer über den Zugriff auf sämtliche an den CAN Bus angeschlossene Funktionen, sobald er sich im CAN Netzwerk manifestiert. SecOC verhindert dies durch Hinzufügen eines Message Authentication Codes (MAC) [19]. Während beim klassischen CAN Bus nur 8 Byte verarbeitet werden, kann bei CAN FD auf 64 Byte eines Datenframes zurückgegriffen werden [19]. Dies ermöglicht die vollständige Überprüfung des MAC - anstelle einer partiellen Überprüfung aufgrund von Größenlimitierungen [19].

Während die sichere Kommunikation in klassischen CAN Netzwerken auf eine Nutzlast von 8 Byte beschränkt ist, erlaubt die Kommunikation auf 64 Byte mittels CAN FD einen Einsatz des SecOC Moduls zur Absicherung. Jedoch steigt damit auch die Netzwerkkomplexität, sodass sich für die Topologie insbesondere in puncto Geschwindigkeit und Effizienz weitreichende Anpassungen ergeben können [19]. Ansätze dazu finden sich in ISO/SAE 21434 (siehe Kapitel 1.1.3) sowie in AUTOSAR Adaptive [24].

1.3.3 TLS

Während SecOS ausschließlich die interne Fahrzeugkommunikation absichert, zielt der Einsatz des kryptographischen TLS-Protokolls[8] auch auf die Absicherung der Kommunikation zu externen Diensten ab [25]. Beide Standards steigern die Authentizität und begünstigen vertrauensvolle Kommunikation. TLS ermöglicht die

[6] Controlled Area Network Flexible Data-Rate
[7] Secure Onboard Communication
[8] Transport Layer Security

Kommunikation zwischen Client/Server-Anwendungen, über das TCP-Protokoll, in einer Weise die Manipulation und Nachrichtenfälschung sowie Lauschangriffe verhindern soll [26]. Der TLS-Handschlag authentifiziert beide Kommunikationsparteien anhand von digitalen Zertifikaten, führt einen Schlüsselaustausch durch und handelt die verwendeten Verfahren für Verschlüsselung und Authentifizierung der Applikationsdaten aus [27]. Allerdings unterstützt TLS nur Unicast Nachrichten [26]. TLS[9] ist sowohl in AUTOSAR Classic wie auch in AUTOSAR Adaptive seit Ende 2018 nutzbar [28]. Bei der Implementierung können durch den zusätzlichen Zeitaufwand beim Einsatz von TLS nur zeitunkritische Anwendungen abgesichert werden [17]. Der allgemeine Einsatz eignet sich jedoch problemlos [25].

1.3.4 IPsec

Das Netzwerk-Layer-Protokollpaket IPsec[10] sichert Netzwerkverbindungen durch Verschlüsselung und Authentifizierung von IP-Paketen ab. Es stellt einen Teil des IP Protokollpakets dar und besteht aus den folgenden drei elementaren Komponenten [29]:

- Internet Key Exchange (Schlüsselverwaltung)
- Authentifizierungs-Header (Sicherstellung von Integrität)
- Kapselung der Sicherheitsnutzlast (Sicherstellung von Integrität und Vertraulichkeit)

Es handelt sich um einen offenen Netzwerkstandard, der seit 1995 von der IETF[11] gepflegt und allgemein verwendet wird [29]. Er kommt weit verbreitet in Netzwerkausrüstung sowie Server- und Desktop-Betriebssystemen zum Einsatz [29]. Das Ziel der Implementierung des IPsec-Protokolls in AUTOSAR Adaptive Plattform ist die Bereitstellung sicherer Kommunikationskanäle im bordeigenen IP-Netzwerk [29]. Eine Implementierung von IPsec ist ausschließlich in der AUTOSAR Adaptive Plattform verfügbar [21]. Das Ziel ist die Absicherung der Kommunikation zwischen Netzwerkknoten und somit der Steigerung der Schutzziele Vertraulichkeit und Integrität. IPsec als Standard-Netzwerksicherheitsprotokoll bietet Mittel für eine sichere Kommunikation und unterstützt gleichzeitig die Interoperabilität von Stacks verschiedener Hersteller [29].

1.3.5 Identitäts- und Zugriffsmanagement

Das AUTOSAR Identitäts- und Zugriffsverwaltungsmodul (IAM)[12] verwaltet die Zugriffsrechte von Subjekten auf Objekte [21]. Das Ziel von IAM ist es eine fehlerhafte oder kompromittierte Anwendungen daran zu hindern, auf einen Dienst oder Ressourcen zuzugreifen, auf die keine Zugriffsrechte bestehen [30]. Die Zugriffsrechte

[9] Aktueller oder gleich Version 1.2
[10] Internet Protocol Security
[11] Internet Engineering Task Force
[12] AUTOSAR Identity and Access Management (IAM)

werden direkt aus den jeweiligen Modellen der Entwicklung abgeleitet. Während der Entwurfsphase einer Anwendung werden ihre Rechte definiert und vom IAM während des Einsatzes umgesetzt. Diese Zugriffsrechte sind in AUTOSAR mittels einer Access Control Matrix frei konfigurierbar und jederzeit aktualisierbar (siehe Abbildung 10).

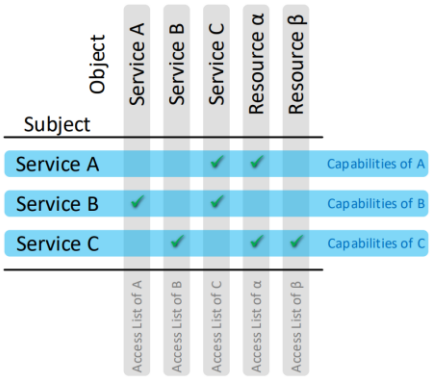

Abbildung 10 - AUTOSAR Identitäts- und Zugriffsmanagement - Access Control Matrix [30]

Die Zugriffsmatrix zeigt die Zugriffsrechte von Subjekten auf Objekte. Ein Objekt ist ein Artefakt, das den Zugang auf ein Objekt anfragt. Die Informationen über die Zugriffsrechte müssen dem System über ein Manifest zur Verfügung gestellt werden.
Als Beispiel für den praktischen Nutzen eines IAM kann durch Miller und Valasek gegeben werden. Sie nutzen das Infotainmentsystem dazu, Zugriff auf den CAN-Bus und damit auf die vollständige Fahrzeugsteuerung zu erhalten [31, 32]. Ihre Ausarbeitungen, zeigen warum Anwendung wie das Infotainmentsystem aus Sicherheitsgesichtspunkten keinen Zugriff auf Gas, Bremse oder Lenkung des Fahrzeugs besitzen sollte [23, 33, 34]. Der Einsatz eines Identitäts- und Zugriffsmanagementsystems, wie AUTOSAR IAM, ist eine rudimentäre Methode, um Zugriffsrechte festzulegen und zu sichern. So kann diese Art von Angriffen effektiv unterbunden werden.

1.3.6 Sicherheitsdiagnostik

AUTOSAR Classic und Adaptive unterstützten die Protokollierung sicherheitsrelevanter Ereignisse und stellt autorisierte Zugriffe sicher. Beispielsweise erhält so ein Diagnosetestapparat bei der Fahrzeugwartung nur Zugang zu protokollierten Sicherheitsvorfällen, wenn zuvor eine Challenge-Response-Kommunikation durchgeführt oder eine zertifikatsbasierte Authentifizierung erfolgt ist [17].

1.3.7 Entwicklungsprozess

Um einen Schutz zu bieten, müssen die in Kapitel 1.3.1 bis 1.3.6 beschriebenen AUTOSAR Module und Funktionen bereits bei der Risikoanalyse und

Anforderungsermittlung berücksichtigt werden sowie im Entwicklungsprozess wohlkonfiguriert und getestet werden [21]. Dies könnte bei Nutzung der Module SecOC, TLS und IPsec (siehe 1.3.2 bis 1.3.4) wie folgt aussehen [21]:

Während der Risikoanalyse und Anforderungsermittlung werden die Nachrichten identifiziert, welche vom ausgewählten Modul geschützt werden sollen. Falls eine Kombination aus Modulen verwendet wird, müssen diese korrekt spezifiziert und auf Interoperabilität geprüft werden [21].

Bei der Konfiguration werden die Module meist anhand der Risikobewertung und den Anforderungen unter der Hilfenahme der Funktionen aus dem Crypto Stack (siehe 1.3.1) eingerichtet. Eine Fehlkonfiguration besitzt mitunter weitreichende Folgen. So kann ein Fehler in der Konfiguration einer einzigen ECU zur Nicht-Verifikation gesicherter Nachrichten führen, die somit verworfen werden [21].

Nach der Implementierung und Prüfung werden mehrere Tests durchgeführt, bevor die ECU für die Produktion freigegeben werden kann. Jedenfalls sollte hier eine Code-Überprüfung der sicherheitskritischen Komponente, ein Penetrationstest der ECU und ein Funktionstest der jeweilig eingesetzten Module durchgeführt werden [21].

2 Fazit

Unter Fahrzeugsicherheit wird längst nicht mehr nur die rein funktionale Sicherheit verstanden. Diese beschreibt allgemein Prozesse zur Durchführung von Sicherheitsaktivitäten. Hier können zum Beispiel der Einsatz von z.B. Airbags, ABS und Traktionskontrolle zur Erhöhung der Insassensicherheit genannt werden.

Die Automobilbranche sieht sich einer stetig fortschreitenden Digitalisierung gegenüber, welche immer neue Technologien als auch Sicherheitsrisiken bereithält. Durch den Einsatz kommunikationsfähiger E/E-Komponenten werden neue Angriffsflächen geschaffen, welche eine Sicherheitsdefinition benötigen, die insbesondere die allgemeine IT-Sicherheit von Fahrzeugen abdeckt.

Im Bereich der funktionalen Cybersicherheit, also den Maßnahmen zur Verteidigung gegenüber maliziösen Angriffen, existieren jedoch nur wenige allgemein anerkannte Standards. Im Rahmen dieser Arbeit wurden drei aktuell international verbreitete Standards zur funktionalen Cybersicherheit von Fahrzeugen vorgestellt, ISO 26262, SAE J3061 und den aktuellsten Standard ISO/SAE 21434. Insbesondere ISO/SAE 21434 besitzt das Potenzial, eine gemeinsame Basis innerhalb der Automobilindustrie zu schaffen, indem es die Vorteile aus den Standards ISO 21262 und SAE J3061 vereint und den Fokus auf die funktionale Cybersicherheit legt.

Durch den Einsatz grundlegender Konzepte zur Risikominimierung, sicherheitszuträglicher Systemarchitekturen sowie den Sicherheitsmodulen und -funktionen aus modernen Softwareplattformen kann die Sicherheit im gesamten Entwicklungsprozess gewährleistet und für das Endprodukt maximiert werden.

3 Ausblick

Moderne Fahrzeuge sind ohne Frage hochkomplex und es erscheint unmöglich die Komplexität zu kontrollieren. Ein Umdenken der Fahrzeugentwicklung mit einem hohen Stellenwert der Sicherheit ist insbesondere vor Hintergrund aufkommender Technologien, wie dem autonomen Fahren und der stets steigenden Kommunikation (u.a. C2X, C2C, Autonomes Fahren, usw.), von oberster Bedeutung.

Die große Anzahl an Steuergeräten (wie z.B. 98 Stück in einem Range Rover [33]) kommen den Automobilunternehmen jedoch nicht entgegen, da sie die ohnehin unübersichtliche Fahrzeuginfrastruktur nur weiter verkomplizieren und damit eine sinnvolle Absicherung nicht zulassen. Man stelle sich vor, fast 100 elektronische Endgeräte mit völlig unterschiedlichen Technologien mit sich zu führen, welche alle separat abgesichert werden müssen.

Grundlagenangriffe, wie durch Charlie Miller und Chris Valasek [23, 31–35], betreffen prinzipiell eine Vielzahl an Fahrzeugen. Dies zeichnet ein Schreckensszenario ab, welches weiterhin unterschätzt wird. Trotz deutlichem Aufzeigen klaffender Sicherheitslücken, wurde ihnen in diesem Fall vom Hersteller bzw. Zulieferer lange keinerlei Beachtung geschenkt, sodass sie auch nach mehrfachen Anläufen nicht komplett geschlossen wurden [23, 34].

Die steigende Plattformdenke von Automobilunternehmen und -konzernen mit Hintergrund der Vereinheitlichung von Komponenten (siehe z.B. Volkswagen, Toyota, GM, PSA) ist beim Blick auf Kosteneinsparung durchaus sinnvoll. Hier wird jedoch der Preis für geteilte Topologien gezahlt. Durch Vereinheitlichung steigt schlichtweg die Auswirkung von Angriffen in der Breite. Historisch gewachsene, zum Teil Jahrzehnte alte Plattformen, erhöhen dieses Risiko zusätzlich. Eine Zusammenarbeit der Automobilhersteller, wie zum Beispiel im Bereich der Softwareplattformen, oder bei Standards und Normen (siehe ISO/SAE 21434, Kapitel 1.1.3) ist der Sicherheit nur dann zuträglich, wenn ihr bei der Entwicklung auch tatsächlich vorrangig Beachtung geschenkt wird.

Mit Betrachtung auf potenzielle Folgen von vernachlässigten oder nicht (ausreichend) umgesetzten Sicherheitsmechanismen ist ein gemeinsamer Ausgangspunkt für OEMs und Zulieferer, wie ihn zum Beispiel der moderne Standard ISO/SAE 21434 bietet, umso essenzieller. Ohne Zweifel wird Cybersicherheit auch zukünftig ein Thema von grundlegender Bedeutung im gesamten Produktlebenszyklus des Automobils darstellen.

Literatur

[1] H.-L. Ross, „Funktionale Sicherheit im Automobil“.

[2] *ISO 26262-1:2018(en) - Road vehicles — Functional safety information and use case definition*.

[3] J. Cooling, „A quick guide to ISO 26262“. [Online]. Verfügbar unter: https://www.feabhas.com/sites/default/files/2016-06/A%20quick%20guide%20to%20ISO%2026262[1]_0_0.pdf. Zugriff am: 17. Juli 2020.

[4] P. Kafka, „The Automotive Standard ISO 26262, the Innovative Driver for Enhanced Safety Assessment & Technology for Motor Cars“, *Procedia Engineering*, Jg. 45, S. 2–10, 2012, doi: 10.1016/j.proeng.2012.08.112.

[5] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger und P. Puschner, „Using SAE J3061 for Automotive Security Requirement Engineering“ in *Computer Safety, Reliability, and Security*, 2016, S. 157–170.

[6] L. Boran, B. J. Czerny und D. Ward, „Overview of recommended practice - SAE J3061“. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Juni 2016. [Online]. Verfügbar unter: https://nmi.org.uk/wp-content/uploads/2016/06/4_SAE-J3061-and-friends-for-NMI-Jun-16.pdf

[7] C. Schmittner, G. Griessnig und Z. Ma, „Status of the Development of ISO/SAE 21434“ in *Communications in Computer and Information Science, Systems, Software and Services Process Improvement*, X. Larrucea, I. Santamaria, R. V. O'Connor und R. Messnarz, Hg., Cham: Springer International Publishing, 2018, S. 504–513, doi: 10.1007/978-3-319-97925-0_43.

[8] MathWorks, Hg., *Model-Based Engineering for Cybersecurity: Preparing for UN ECE Regulation and ISO/SAE 21434*, 2020. [Online]. Verfügbar unter: https://de.mathworks.com/content/dam/mathworks/mathworks-dot-com/company/events/conferences/automotive-conference-stuttgart/2020/model-based-engineering-for-cybersecurity-preparing-for-unece-regulation-and-iso-sae.pdf

[9] *ISO/SAE DIS 21434 - Road vehicles — Cybersecurity engineering*.

[10] H.-L. Ross, *Functional Safety for Road Vehicles*. Cham: Springer International Publishing, 2016.

[11] M. Ring und R. Kriesten, „Plausibility Checks in Automotive Electronic Control Units to Enhance Safety and Security: The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications : November 13-17, 2016, Barcelona, Spain“ in *VEHICULAR 2016: The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications : November 13-17, 2016, Barcelona, Spain*, 2016, S. 16–19. [Online]. Verfügbar unter: https://www.semanticscholar.org/paper/Plausibility-Checks-in-Automotive-Electronic-Units-Ring-Kriesten/4941657cfb5ec78caf0c003870217280334b0433

[12] H. Versmold und M. Saeger, „Plausibility Checking of Sensor Signals for Vehicle Dynamics Control Systems“, *Forschungsgesellschaft Kraftfahrwesen Aachen*, 2006. [Online]. Verfügbar unter: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.548.9617&rep=rep1&type=pdf
[13] F. Wolf, *Fahrzeuginformatik*. Wiesbaden: Springer Fachmedien Wiesbaden, 2018.
[14] Avizienis und Kelly, „Fault Tolerance by Design Diversity: Concepts and Experiments“, *Computer*, Jg. 17, Nr. 8, S. 67–80, 1984, doi: 10.1109/MC.1984.1659219.
[15] *Band G, Kapitel 7: Prinzipien*, 2013. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G7_HV-Prinzipien.pdf?__blob=publicationFile&v=1
[16] AUTOSAR, „AUTOSAR Introduction“, 2018. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/ABOUT/AUTOSAR_Introduction.pdf. Zugriff am: 1. November 2019.
[17] N. Fabritius, R. Jung und J. Holle, „Secure Ethernet – an opportunity for vehicle IT“, *Security Special 2017*, S. 5–7, 2017. [Online]. Verfügbar unter: https://www.etas.com/data/RealTimes_2017/rt_2017_1_05_en.pdf
[18] AUTOSAR, „Requirements on Crypto Stack: AUTOSAR CP Release 4.3.1“, Nr. 426, 2017. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SRS_CryptoStack.pdf
[19] T. Islinger, Y. Mori, J. Neumüller, M. Prisching und R. Schmidt, „Autosar SecOC for CAN FD“, *CAN Newsletter*, 1/2017, S. 44–45, 2017. [Online]. Verfügbar unter: https://can-newsletter.org/uploads/media/raw/d904c90ba599c668e9758ae558dcb845.pdf
[20] Robert Bosch GmbH, „CAN Specification“, 1991. [Online]. Verfügbar unter: http://esd.cs.ucr.edu/webres/can20.pdf
[21] A. Berthold und M. P. Schneider, „AUTOSAR security – Adaptive platform must focus on holistic vehicle protection“, *Security Special 2020*, S. 6–7, 2020. [Online]. Verfügbar unter: https://www.escrypt.com/sites/default/files/2019-12/ESCRYPT_Security-Special_2020_EN.pdf
[22] M. Ring, D. Frkat und M. Schmiedecker, „Cybersecurity Evaluation of Automotive E/E Architectures“ in *ACM Computer Science in Cars Symposium*, Kaiserslautern, Germany, 2018.
[23] C. Miller und C. Valasek, „Securing Self-Driving Cars (one company at a time)“, Aug. 2018.
[24] AUTOSAR, „Specification of Manifest: AUTOSAR AP Release 19-03“, 19-03, 2019. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/user_upload/standards/adaptive/17-03/AUTOSAR_TPS_ManifestSpecification.pdf
[25] D. Zelle, C. Krauß, H. Strauß und K. Schmidt, „On Using TLS to Secure In-Vehicle Networks“ in *ARES '17: International Conference on Availability,*

Reliability and Security, Reggio Calabria Italy, 2017, S. 1–10, doi: 10.1145/3098954.3105824.
[26] Internet Engineering Task Force, Hg., „The Transport Layer Security (TLS) Protocol Version 1.3“ ISSN: 2070-1721, Aug. 2018. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc8446. Zugriff am: 19. Juli 2020.
[27] J. Kreissl, „Absicherung der SOME/IP Kommunikation bei Adaptive AUTOSAR“. Masterarbeit, Universität Stuttgart, 2017. [Online]. Verfügbar unter: https://elib.uni-stuttgart.de/bitstream/11682/9482/1/ausarbeitung.pdf
[28] AUTOSAR, „Specification of TCP/IP Stack: AUTOSAR CP R19-11“, 19-11, 2019. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-1/AUTOSAR_SWS_TcpIp.pdf
[29] AUTOSAR, „Explanation of IPsec Implementation Guidelines: AUTOSAR AP R19-11“, 19-11, 2019. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/user_upload/standards/adaptive/19-11/AUTOSAR_EXP_IPsecImplementationGuidelines.pdf
[30] AUTOSAR, „Requirements on Identity and Access Management: AUTOSAR AP R19-11“, 19-11, 2019. [Online]. Verfügbar unter: https://www.autosar.org/fileadmin/user_upload/standards/adaptive/19-11/AUTOSAR_RS_IdentityAndAccessManagement.pdf
[31] C. Miller und C. Valasek, „Remote Exploitation of an Unaltered Passenger Vehicle“, 10. Aug. 2015. [Online]. Verfügbar unter: http://illmatics.com/Remote%20Car%20Hacking.pdf. Zugriff am: 1. November 2019.
[32] C. Miller und C. Valasek, „CAN Message Injection: OG Dynamite Edition“, 28. Juni 2016. [Online]. Verfügbar unter: http://illmatics.com/can%20message%20injection.pdf. Zugriff am: 1. Dezember 2019.
[33] C. Miller und C. Valasek, „A Survey of Remote Automotive Attack Surfaces“, 2014. [Online]. Verfügbar unter: http://illmatics.com/remote%20attack%20surfaces.pdf
[34] C. Miller und C. Valasek, „Adventures in Automotive Networks and Control Units“, 7. Aug. 2013. [Online]. Verfügbar unter: http://illmatics.com/car_hacking.pdf. Zugriff am: 1. Dezember 2019.
[35] C. Miller und C. Valasek, „Car Hacking: For Poories: a.k.a. Car Hacking Too: Electric Boogaloo“, 2014. [Online]. Verfügbar unter: http://illmatics.com/car_hacking_poories.pdf. Zugriff am: 1. Dezember 2019.