© metamorworks | Shutterstock.com

UNECE WP.29 minimiert Bedrohungen für Cybersecurity

Gesetzliches Rahmenwerk

Heutige Fahrzeuge integrieren Fahrerassistenzfunktionen entweder als serienmäßigen Bestandteil oder als optionale Aufrüstung. Das bringt nicht nur Vorteile, sondern erhöht mit zunehmender Komplexität der vernetzten, automatisierten und später autonomen Fahrzeuge die Gefahr potenzieller Cyberangriffe massiv.

Riccardo Camacho

Automobilhersteller setzen moderne Hardware ein mit Funktionen zur Fahrerassistenz, wie automatisches Lenken, Bremsen, adaptive Geschwindigkeitsregelung, automatisches Einparken, Kollisionsvermeidung, Unterstützung beim Spurwechsel und vieles mehr. Einige dieser Fahrassistenzsysteme sind serienmäßig im Fahrzeug integriert. Andere wiederum werden als externe Geräte angeboten, die man direkt an den On-Board-Diagnose-II-Anschluss (OBD-II) des Fahrzeugs anschließen kann, um auf den Fahrzeugcomputer zuzugreifen und automatisiertes Fahren nach Level 2 zu erleben.

ADAS stützt sich auf mehrere Echtzeit-Datenquellen, die von der äußeren Umgebung des Fahrzeugs gesammelt werden, um die Funktionen sicher und zuverlässig auszuführen. Dazu zählen u. a. visuelle Daten von Kameras, Bildgebung von Lidar, Radar zur Abstandsmessung, Telemetriedaten wie Geschwindigkeit, Standort und Ortung sowie Fahrzeug-zu-Fahrzeug-Kommunikation. Zusammenarbeit und Kommunikation müssen auch zwischen Telematik, Gateways, Infotainment-Systemen und anderen Steuergeräten zur Unterstützung von ADAS stattfinden und über ein CAN-Bus erfolgen. Zum Einsatz kommen dabei verschiedene Technologien wie Bluetooth, Hochgeschwindigkeits-Breitband- oder Mobilfunknetze wie LTE und 5G, über die man die Autotüren ver-/entriegeln, den Motor starten und den Status des Fahrzeugs oder den Ort, an dem man es geparkt hat, abrufen kann – all das problemlos über eine Telefon-App mit PIN. Eine geheime vierstellige PIN ist zwar angenehm und bequem, reicht aber nicht aus, um die Cybersicherheit des Fahrzeugs zu gewährleisten.

ECE WP.29 Fahrzeug-Cybersicherheit

Nach langer Vorbereitung hat die Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) am 23. Juni 2020 regulatorische Anforderungen veröffentlicht, die die Automobilhersteller in ihre Unternehmen und Fahrzeuge einbauen müssen. Das betrifft nicht nur die Automobilhersteller, sondern auch

die Soft- und Hardware-Komponenten von Tier 1 und Tier 2 sowie mobile Dienste. Die neue Regelung UNECE WP.29 Cybersecurity and Cybersecurity Management Systems (CSMS) gilt für 54 Länder. Danach sind Fahrzeughersteller verpflichtet, einen risikobasierten Managementrahmen für das Aufspüren, die Analyse und den Schutz vor relevanten Bedrohungen, Schwachstellen und Cyberangriffen in ihre Unternehmensstruktur einzubauen. Dies lässt sich zweifellos in ein bestehendes Qualitätsmanagementsystem (QMS) und Prozesse integrieren, wie es die ISO 26262–2 zur Gewährleistung von Qualität und Sicherheit verlangt.

Zusätzlich gibt es ECE-WP.29-Anforderungen für den Fahrzeugtyp (Kategorie M und N, einschließlich der Kategorien L6 und L7 bei Ausstattung mit Funktionen für automatisiertes Fahren ab Stufe 3), zu denen das Prüfen der Implementierung der Cybersicherheitskontrollen und das erfolgreiche Absolvieren der Prüfung gehören. Erfüllt der Hersteller die organisatorischen und fahrzeugbezogenen ECE-WP.29-Schlüsselanforderungen korrekt, erhält er von einer Genehmigungsbehörde eine Konformitätsbescheinigung. Neufahrzeuge ohne diese Bescheinigung dürfen in der EU ab Juni 2022 nicht mehr verkauft werden.

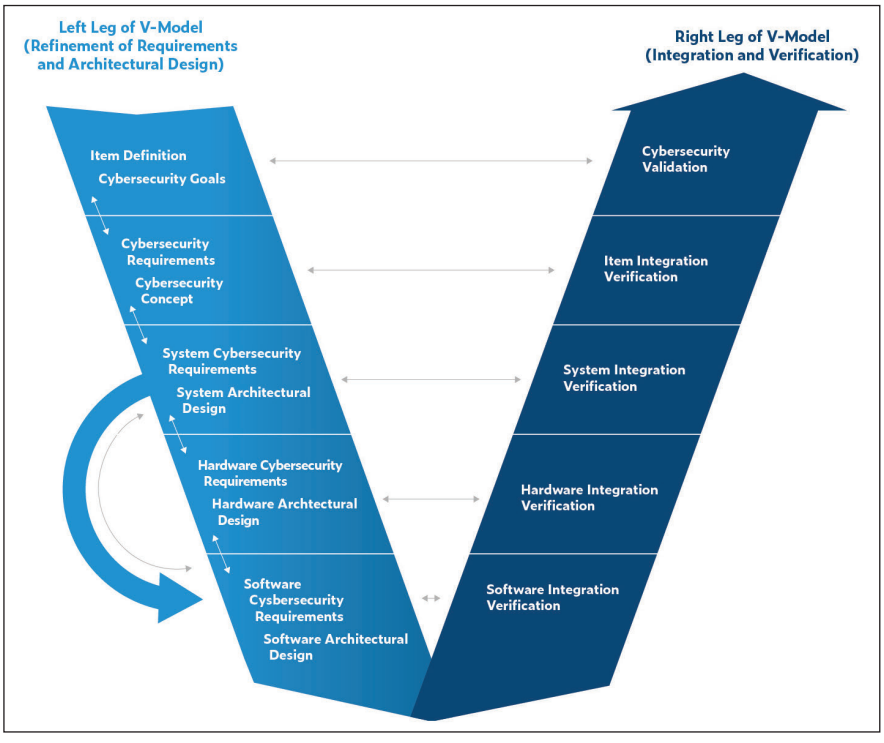

Bild 1: Das V-Modell zeigt den Ansatz für eine formale Verifizierung und Validierung, den die Entwicklung sicherheitskritischer Software verwendet. © Parasoft

Eine kleine Beispielliste mit Bedrohungen und entsprechenden Abhilfemaßnahmen aus ECE/TRANS/WP.29/2020/79 Anhang 5 Tabelle B1 (**Tabelle 1**) aufgeführt. Diese konzentriert sich auf Gefährdungen und Entschärfungsmaßnahmen im Zusammenhang mit den Kommunikationskanälen des Fahrzeugs. Wichtig dabei ist, dass die ‚Shall / MUSS'-Aussagen verpflichtende Anforderungen darstellen, während die ‚Should / SOLLTE'-Aussagen für das Bemühen um die Abschwächung der Bedrohung stehen.

Referenztabelle A1	Bedrohungen für Fahrzeugkommunikationskanäle	Ref	Minderungsmaßnahme
4.1	Spoofing von Nachrichten (z. B. 802.11p V2X beim Platooning, GSM-Nachrichten usw.) durch Identitätswechsel	M10	Das Fahrzeug **muss** die Authentizität und Integrität der empfangenen Nachriten überprüfen.
5.1	Kommunikationskanäle ermöglichen Code-Injektionen in Fahrzeugdaten/-code, z. B. können manipulierte Softwarebinärdateien in den Kommunikationsstrom injiziert werden	M10 M6	Das Fahrzeug **muss** die Authentizität und Integrität der empfangenen Nachrichten überprüfen. Bereits bei der Konzeption der Systeme **müssen** Sicherheitsvorkehrungen vorgesehen werden, um Risiken zu minimieren.
6.1	Akzeptieren von Informationen aus einer unzuverlässigen oder nicht vertrauenswürdigen Quelle	M10	Das Fahrzeug **muss** die Authentizität und Integrität der empfangenen Nachrichten überprüfen.
7.2	Erlangen von unbefugtem Zugriff auf Dateien oder Daten	M8	Das Systemdesign und die Zugangskontrolle **müssen** so ausgelegt sein, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können. Beispiele für Sicherheitsmaßnahmen bietet das OWASP.
11.1	Schädliche interne Nachrichten (z. B. CAN-Nachrichten)	M15	Maßnahmen zur Erkennung schädlicher interner Nachrichten oder Aktivitäten **sind zu erwägen.**

Tabelle 1: Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Fahrzeugkommunikationskanälen © UNECE | Parasoft

WP.29 Abschnitt 7.3.3 betont, dass der Fahrzeughersteller eine umfassende „Risikobewertung" durchführen muss. Es wird allerdings keine Aussage dazu getroffen, wie diese durchzuführen ist. Jedoch wird in Abschnitt 5.3.1(a) auf verschiedene Normen zur Risikobewertung verwiesen; eine davon ist die Automobil-Cybersicherheitsnorm ISO/SAE 21434 – Road Vehicles – Cybersecurity Engineering.

ISO/SAE 21434 Straßenfahrzeuge-Cybersecurity Engineering

Eine gemeinsame Arbeitsgruppe der ISO- und SAE-Organisationen hat im Mai 2020 einen Entwurf der ISO/SAE 21434 für Fahrzeughersteller und Zulieferer veröffentlicht, der im August 2021 freigegeben wurde. Die Norm soll sicherstellen, dass:

- Cybersecurity-Risiken erfolgreich gehandhabt werden.
- Cybersecurity-Richtlinien und -Prozesse definiert werden.

Auswirkung	Angriffsvektor			
	Physisch	Lokal	Angrenzend	Netzwerk
Vernachlässigbar	-	-	-	-
Mäßig	CAL 1	CAL 1	CAL 2	CAL 3
Schwerwiegend	CAL 1	CAL 2	CAL 3	CAL 4
Gravierend	CAL 2	CAL 3	CAL 4	CAL 4

Tabelle 2: Risikobewertung auf Grundlage von Parametern für Auswirkungen und Angriffsvektoren © UNECE | Parasoft

Themen	CAL			
	1	2	3	4
Analyse der Anforderungen	□	□	□	□
Generierung und Analyse von Äquivalenzklassen			□	□
Grenzwertanalyse			□	□
Fehlerraten				

Tabelle 3: Methoden zur Ableitung von Testfällen © UNECE | Parasoft

- Eine Cybersecurity-Kultur gefördert wird.

Die Norm ist in verschiedene Kapitel untergliedert. Eine davon betrifft die „Risikobewertungsmethoden", bei denen Bedrohungs- und Schadensszenarien berücksichtigt werden müssen. Dazu zählt beispielsweise ein Angriffsweg, bei dem CAN-Botschaften an das Steuergerät des Antriebsstrangs gefälscht werden, was zum Verlust der Kontrolle und zu möglichen Schäden führen kann. Da Angriffe über verschiedene Medien wie Bluetooth, LTE, USB oder physischen Zugang (ISO/SAE 21434) erfolgen können, wurden die Bedrohungen nach der Durchführbarkeit der Angriffe kategorisiert in:

- hoch
- mittel
- niedrig
- sehr niedrig

Ein „Defense-in-Depth"-Ansatz, bei dem mehrere Schichten von Cybersicherheitsmaßnahmen zum Einsatz kommen für den Fall, dass der Angriff eine Schicht durchdringen kann, muss dokumentiert und durchgeführt werden. Für die Auswirkungen auf die Sicherheit gilt die ISO 26262 für Straßenfahrzeuge – Funktionale Sicherheit.

Cybersecurity-Risikobewertung

Weil Bedrohungspfade auch mit Schäden zusammenfallen, wurden folgende Schadensauswirkungsgrade definiert:

- Severe / Gravierend
- Major / Schwerwiegend
- Moderate / Mäßig
- Negligible / Vernachlässigbar

Basierend auf den Angriffs- und Schadensszenarien lässt sich eine Sicherheitsstufe für die Cybersicherheit (Cybersecurity Assurance Level, CAL) definieren. Die Stufe CAL 4 verlangt das höchste Maß an Sorgfalt bei Entwurf, Tests und Überprüfen der Cybersicherheit, während für CAL 1 ein niedriges Maß an Strenge ausreicht.

Beispiel für eine Risikobewertung

Eine einer Software- oder Hardware-Komponente zugewiesene CAL-Stufe (**Tabelle 2**) kann sich auf die für ihre Entwicklung und Prüfung eingesetzten Methoden auswirken. So gibt es beispielsweise empfohlene Verifikationsmethoden für die Integration, wie anforderungsbasierte Tests, Schnittstellentests, Evaluierung der Ressourcennutzung, Kontroll- und Datenfluss und statische Codeanalyse für Software. Auf der Ebene der Code-Einheiten wird möglicherweise eine Strukturabdeckung auf Anweisungs- oder Verzweigungsebene angeraten. **Tabelle 3** listet Methoden zur Ableitung von Testfällen; die Häkchen bedeuten Empfehlungen.

Cybersicherheit über den gesamten SDLC

Entwickler von Embedded Systemen wissen, dass die ISO/SAE 21434 den gesamten Lebenszyklus der Softwareentwicklung (Software Development Life Cycle, SDLC) umfasst – von den Anforderungen über den Entwurf, die Implementierung und Integration bis hin zu Verifizierung und Validierung (V&V, **Bild 1**). Daher sollte man sicherstellen, dass ein solides Application-Lifecycle-Management- oder Requirements-Management-Tool (ALM bzw. RM) zum Einsatz kommt. Zusätzlich zu den Anforderungen der jeweiligen Interessensgruppen und allen anderen Sicherheitsvorschriften müssen auch die Anforderungen der ECE WP.29 an die Cybersicherheit erfüllt werden. Hilfreich ist hier der Einsatz einer Rückverfolgbarkeitsmatrix, um sicherzustellen, dass man keine Cybersicherheitsanforderungen übersieht.

Normenkonformität und Testkonfigurationen

Die ISO/SAE 21434 empfiehlt für V&V-Testmethoden wie die statische Code-Analyse, Kontroll- und Datenflussüberprüfung, Grenzwertanalyse, strukturelle Codeabdeckung und mehr. Ein idealer Ausgangspunkt für die Umsetzung der Cybersicherheitsanforderungen ist der Einsatz von Programmierstandards wie SEI CERT, CWE, OWASP und MISRA C:2012. Diese und andere Standards können Sicherheitsschwachstellen bereits beim Schreiben des Codes und/oder als Teil der kontinuierlichen Integrationspipeline (CI) aufdecken.

Es ist sinnvoll, die von der Norm empfohlene Code-Abdeckung zu nutzen, um zu erfahren, welche Teile der Software noch nicht getestet wurden. Empfehlenswert ist auch die Berücksichtigung des evolutionären Wandels, der sich in der Automobilindustrie vollzieht, und wie er sich auf die Norm ISO/SAE 21434 und auch auf die eingesetzten Entwicklungswerkzeuge auswirken wird. Man sollte sich vergewissern, dass man diese Entwicklung problemlos mitmachen kann, beispielsweise mit einem vom TÜV für den Einsatz in sicherheitskritischen Systemen zertifizierten Tool. So ist man bereits gerüstet, wenn es soweit ist, dass das Tool auch für den Einsatz bei cybersicherheitskritischen Systemen zertifiziert werden muss. ■ (eck)

www.parasoft.com

Ricardo Camacho ist technischer Autor bei Parasoft. © Parasoft