escrypt
SECURITY. TRUST. SUCCESS.

Whitepaper

Typgenehmigungsfähige Entwicklung
und Nachrüstung von E/E-Architekturen

Mit AUTOSAR zu UNECE-konformer Cybersicherheit

Schon bald wird der Nachweis einer adäquaten Absicherung des Fahrzeugs gegen Cyberangriffe zur Voraussetzung für die Typgenehmigung. Notwendige Bedingung dafür ist der Nachweis eines angemessenen Security-Levels auf Basis eines zertifizierten Cybersecurity-Managementsystems (CSMS). Bereits während der Entwicklung des Fahrzeugtyps müssen kritische Elemente identifiziert und angemessene Schutzmaßnahmen implementiert werden. Gleiches gilt für Bestandsarchitekturen; auch diese müssen bis 2024 gemäß den Vorgaben der UNECE WP.29 typgenehmigungsfähig nachgerüstet werden.

Auf dem Weg dorthin kann AUTOSAR zu einem wichtigen Schwungrad werden. Denn bereits heute bieten AUTOSAR Classic und Adaptive eine Reihe nutzbringender Security-Bausteine. Das Whitepaper zeigt auf, wo genau und in welchem Maße sich die AUTOSAR-Security-Bausteine konkret für die Umsetzung der in Annex 5 der in UN-Regulierung 155 geforderten Mitigationen einsetzen lassen.

Inhaltsübersicht

Enger Zeitrahmen verlangt praktikable Umsetzungsstrategie

Mit der Verabschiedung der UN-Regelungen 155 und 156 durch die WP.29 im Juni 2020 ist das Thema Produktsicherheit zur Schlüsseltechnologie für die Digitalisierungsstrategien der Automobilhersteller und -zulieferer geworden. Um weiterhin Zulassungen für ihre Fahrzeugtypen in der EU, Japan und weiteren wichtigen Märkten zu erhalten, müssen OEMs ein zertifiziertes Cybersecurity-Managementsystem (CSMS) betreiben und ein angemessenes IT-Sicherheitslevel ihrer E/E-Architekturen nachweisen.

Die EU beabsichtigt, diese Vorgaben für die Genehmigung neuer Fahrzeugtypen bis Juli 2022 verpflichtend zu machen und bis Juli 2024 auf ältere Architekturen auszuweiten. Japan hat ähnliche Zeitvorgaben (Abb. 1). Dementsprechend stehen die Automobilhersteller weltweit – unter Einbeziehung ihrer Zulieferer – vor der Aufgabe, entsprechende Schutzmaßnahmen für ihre Fahrzeuge zu konzipieren, umzusetzen und zu verifizieren [1, 2].

Abb. 1: Terminierung der UN-Regulierung 155 (UN R155): Angemessene Cybersicherheit wird ab Juli 2022 für neue Fahrzeugtypen und ab Juli 2024 für Bestandsarchitekturen verpflichtend für die Typgenehmigung.

Entwicklung und Nachrüstung im Lichte angemessener, verifizierbarer Cybersicherheit

Gemäß UN R 155 erfordert die zukünftige Typgenehmigung die Anwendung des CSMS des OEMs während der Entwicklung. Auch wenn das CSMS während der Entwicklung noch nicht in Betrieb war (vor Juli 2024), muss der OEM eine angemessene Sicherheit des Fahrzeugtyps nachweisen: Er muss die kritischen Elemente des Fahrzeugtyps identifizieren und diese durch geeignete Sicherheitsmaßnahmen vor zuvor definierten Bedrohungen schützen. Annex 5 der UN R 155 dient hier als Richtschnur: Aufgelistet finden sich dort sowohl die Schwachstellen und Bedrohungen, die berücksichtigt werden müssen (Teil A), als auch technische Maßnahmen zu deren Mitigation (Teile B, C). Dementsprechend verfolgen OEMs idealerweise einen umfassenden, nachvollziehbaren IT-Sicherheitsansatz für die Typgenehmigung, der mindestens die folgenden Fragen beantwortet [1]:

1. Sind alle notwendigen Artefakte vorhanden, um nachzuweisen, dass die Entwicklung des Fahrzeugtyps gemäß des CSMS/ adäquater Sicherheit erfolgt ist?

OEMs müssen eine lückenlose Verfolgung aller Dokumente gewährleisten, die die Anwendung des CSMS während der Entwicklung nachweisen, z. B. Risikoanalysen, IT-Sicherheitskonzepte, Security-Testspezifikationen und entsprechende Testberichte. Viele dieser Aktivitäten sind in der Automobilindustrie längst zum Standard geworden. Die Herausforderung indes besteht darin, eine vollständige Dokumentation über die für die Cybersicherheit des Fahrzeugtyps ergriffenen Maßnahmen vorweisen zu können.

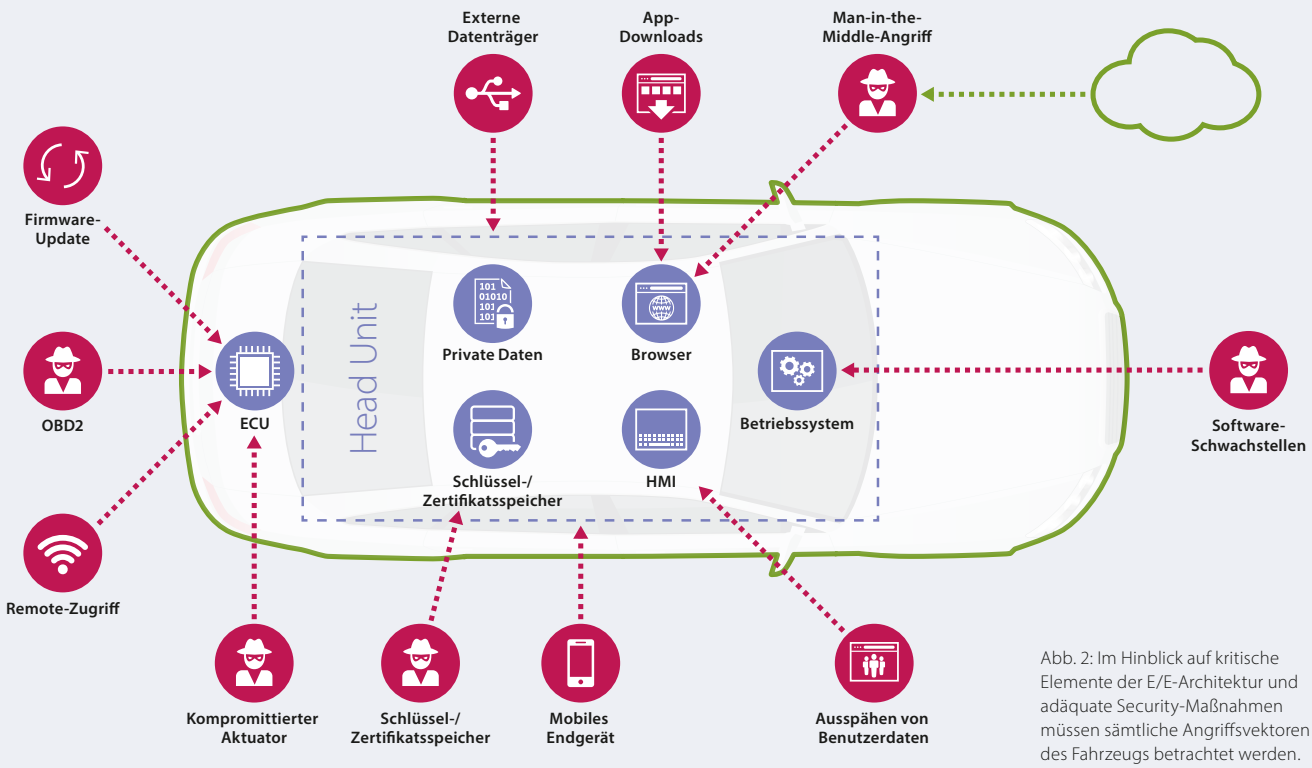

Abb. 2: Im Hinblick auf kritische Elemente der E/E-Architektur und adäquate Security-Maßnahmen müssen sämtliche Angriffsvektoren des Fahrzeugs betrachtet werden.

Für entlang eines CSMS entwickelte Fahrzeugtypen ergeben sich Nachweis und Dokumentation hier unmittelbar aus dem Cybersecurity-Managementsystem. Jedoch stellt sich ab Juli 2024 die gleiche Aufgabe auch für Legacy-Systeme: Hier gilt es ggf. in die Zeit vor Einführung eines CSMS mit definiertem Security-Engineering-Prozess zurückzugehen.

2. Was sind die kritischen Elemente der E/E-Architektur?

Die Klärung dieser Frage rückt die Entwicklung und eventuelle Nachrüstung von Fahrzeugtypen in den Fokus, denn hier lassen sich Budget- und Engineering-Engpässe vermeiden, wenn der Juli-2024-Termin näher rückt. Je früher im Entwicklungszyklus die Frage nach den Security-kritischen Elementen beantwortet wird, desto weniger Nacharbeit ist nötig. Ein Readiness-Check vor Beginn jeder Entwicklungs-/Nachrüstaktivität ermöglicht hier intelligente Entscheidungen: Mit den richtigen Maßnahmen auf der E/E-Ebene (z.B. durch Nutzung der AUTOSAR Security-Bausteine) kann der Aufwand im Vergleich zu einer rein komponentenzentrierten Betrachtung reduziert werden.

Die VTA-Readiness-Bewertung durch ESCRYPT identifiziert potenziell kritische Elemente auf systematische Weise und stützt sich dabei auf Musterbeispiele aus dem offiziellen Interpretationspapier der UN R 155, auf Feedback technischer Dienste und auf über ein Jahrzehnt Erfahrung in Analyse und Design sicherer Fahrzeugarchitekturen (Abb. 2). Zentraler Bestandteil der Readiness-Bewertung ist die Identifizierung technischer Sicherheitslücken; das wiederum gestattet erste Budgetschätzungen, relevante IT-Sicherheitsprüfungen und eine Priorisierung der Aufgaben auf dem Weg zur Typgenehmigung.

3. Welche technischen Cybersecurity-Maßnahmen, sowohl auf Steuergeräte- als auch auf E/E-Ebene, sind implementiert und warum sind sie – insbesondere im Hinblick auf Annex 5 – angemessen?

Dritter entscheidender Schritt zur Typgenehmigung ist die Definition und Umsetzung technischer Schutzmaßnahmen, um eine angemessene Cybersicherheit für das Fahrzeug herzustellen. Die Absätze 7.3.3 und 7.3.4 der UN R 155 fordern vom Fahrzeughersteller:

- eine Risikobewertung des Fahrzeugtyps der verschiedenen Fahrzeugsysteme sowie deren Zusammenwirken untereinander und mit externen Systemen vorzunehmen und
- den Nachweis zu erbringen, welche geeigneten Schutzmaßnahmen zur Mitigierung der identifizierten Risiken (angesichts Annex 5, Part B und C, und erforderlichenfalls darüber hinaus) getroffen wurden.

Das bedeutet, dass der OEM während der Entwicklung des Fahrzeugtyps diejenigen Security-Komponenten und -Mechanismen implementieren muss, die gewährleisten, dass die E/E-Architektur sowohl in ihren einzelnen Systemen als auch in deren Kommunikation untereinander und in ihrer Kommunikation nach außen zum Zeitpunkt der Typgenehmigung ausreichend abgesichert ist.

Dieser dritte Aspekt, die Implemetierung adäquater Security-Maßnahmen angesichts Annex 5, stellt für Bestandsarchitekturen, die auf ihre Genehmigungspflichtigkeit ab Juli 2024 ausgerichtet werden müssen, eine besondere Herausforderung dar. Denn für sie ist eine potenzielle Nachrüstung von Legacy-Hardware- und Software-Komponenten vonnöten. Hier kann es sich als großer Vorteil erweisen, wenn die Komponenten AUTOSAR-Security-Bausteine beinhalten; denn die können als Hebel genutzt werden, um den Zeit- und Kostenaufwand für Nachrüstungen zu minimieren.

AUTOSAR als Fixpunkt bei der Absicherung von E/E-Architekturen

Angesichts immer neuer Bedrohungsszenarien und der wachsenden Zahl von Angriffvektoren bei vernetzten Fahrzeugen macht die UNECE WP.29 die Typgenehmigung davon abhängig, ob die in Annex 5 der Verordnung aufgeführten Bedrohungen und Security-Maßnahmen nachweislich bei der Entwicklung des Fahrzeugs berücksichtigt wurden. Allein schon in technischer Hinsicht ist das eine anspruchsvolle Aufgabe. Erst recht aber, wenn der Zeithorizont derart eng gesetzt ist: Denn während die Fahrzeughersteller noch dabei sind, die notwendigen organisatorischen und prozessualen Voraussetzungen in Form eines CSMS zu schaffen, müssen sie bei neuen Fahrzeugtypen, die in weniger als zwei Jahren genehmigungsreif sein werden, bereits die erforderlichen mitigierenden IT-Sicherheitsmechanismen in der E/E-Architektur umsetzen.

Doch die Herausforderung reicht noch weiter. Denn neue Fahrzeugtypen lassen sich immerhin so entwickeln, dass sie von vornherein nach den UNECE-Anforderungen und dem CSMS zugelassen werden können. Hingegen müssen bestehende Architekturen, für die ursprünglich keine IT-Sicherheitsprozesse unter UNECE WP.29 vorgesehen waren, für die Typgenehmigung ab 2024 modernisiert werden. Genau das jedoch, nämlich retrospektiv für diese Bestandsarchitekturen eine State of the Art Security zu implementieren, ist mitunter schwierig.

AUTOSAR-Security-Bausteine

Eine naheliegende Lösung ist, dabei vor allem auf bekannte Technologien und Standards zu setzen. Als weithin verbreitete, bewährte Software-Plattform zur Entwicklung von E/E-Architekturen ist AUTOSAR hier das natürliche Mittel zum Zweck – und zwar sowohl für die Entwicklung neuer als auch für die Nachrüstung bestehender Architekturen. Denn die standardisierten Spezifikationen in AUTOSAR haben die IT-Security längst mit im Blick. Sowohl AUTOSAR Classic als auch AUTOSAR Adaptive verfügen heute bereits über eine Reihe von IT-Sicherheitsbausteinen. Diese wiederum lassen sich in unmittelbar in funktionale Security innerhalb der Bordnetzarchitektur übersetzen und können – im Sinne von „Security-by-Design" – gezielt für die Umsetzung etlicher der von der UNECE.WP29 vorgeschriebenen Mitigationen eingesetzt werden [1, 3, 4]:

- **Krypto-Stack**
  Die gezielte Bereitstellung von kryptographischen Primitiven, Schlüsseln und Zertifikaten wird in AUTOSAR durch den Krypto-Stack (Krypto-API) realisiert. Die Applikationen greifen unabhängig von der Krypto-Implementierung nur auf die vom Krypto-Stack bereitgestellten Schnittstellen zu, was die Portabilität von Anwendungen auf verschiedene Steuergeräte erhöht.

- **Sichere Kommunikation**
  Mit SecOC (Secure Onboard Communication) bietet AUTOSAR ein Kommunikationsprotokoll, das den Datenverkehr auf klassischen Fahrzeugbussen wie CAN schützt und eine granulare Anpassung der Sicherheitsstufen erlaubt. AUTOSAR Adaptive unterstützt außerdem die TCP/IP-Kommunikation via Ethernet mittels TLS und IPSec und ermöglicht so den einfachen Aufbau sicherer Verbindungen nicht nur innerhalb des Fahrzeugs, sondern auch mit externen Instanzen, etwa dem OEM-Backend.

- **Sichere Diagnose / Logging**
  AUTOSAR wacht über den autorisierten Zugriff auf sensible Daten im Fahrzeugnetzwerk mittels der UDS-Dienste 0x27 (Security Access) und 0x29 (Authentication). Der Diagnosetester beispielsweise erhält erst dann Zugriff auf solche Daten, wenn er zuvor eine Challenge-Response-Kommunikation durchgeführt oder sich per Zertifikat authentifiziert hat. Daneben unterstützt AUTOSAR das Logging von sicherheitsrelevanten Ereignissen im Security Event Memory.

- **Identity- und Access-Management**
  Das AUTOSAR-Modul Identity- und Access-Management sorgt dafür, dass nur autorisierte Applikationen auf bestimmte kritische Systemressourcen (z.B. sensible Daten im persistenten Speicher, Kommunikationskanäle, kryptografische Schlüssel) Zugriff erhalten. Diese Zugriffsrechte können in AUTOSAR Adaptive bedarfsgerecht konfiguriert und jederzeit upgedatet werden.

- **Angriffserkennung**
  Wichtiger Bestandteil wirksamen Security-Managements über den gesamten Fahrzeuglebenszyklus ist ein Intrusion Detection System (IDS), das Angriffe auf das Fahrzeug erkennt und an ein Backend meldet. Aus diesem Grund ist der IDS-Manager (IdsM) als maßgebliche Schaltstelle eines verteilten IDS seit dem Releases R20-11 in AUTOSAR integriert [5].

- **Sichere Updates**
  Die Secure-Update-Funktion in AUTOSAR Adaptive hilft in der Folge die erkannten Schwachstellen zu beheben, indem sie Security-Updates für einzelne Applikationen oder sogar für die gesamte Plattform empfängt und verarbeitet. Die einzelnen Update-Blobs werden dabei vom Backend signiert, so dass nur Updates aus vertrauenswürdiger Quelle ausgeführt werden.

- **Trusted Platform**
  Auch die Anwendungen auf Steuergeräten, Domänencontrollern und Vehicle-Computern im Fahrzueg bedürfen regelmäßiger Überprüfung. Diese Aufgabe übernimmt Secure Boot beziehungsweise die Trusted-Platform-Funktion in AUTOSAR Adaptive. Sie verifiziert als Fortführung der Secure-Boot-Vertrauenskette die Integrität aller Anwendungen und der Plattform. So ist sichergestellt, dass nur vertrauenswürdige Software ausgeführt wird.

Die meisten der aufgeführten AUTOSAR-Security-Bausteine sind für beiden Plattformen, Classic und Adaptive, verfügbar, einige jedoch werden nur für AUTOSAR Adaptive unterstützt (Abb. 3). Das AUTOSAR-Konsortium treibt die Entwicklung hier jedoch bedarfsorientiert voran. So ist beispielswesie geplant, die Secure-Update-Funktion auf AUTOSAR Classic auszuweiten.

	AUTOSAR Classic R20-11	AUTOSAR Adaptive R20-11
Krypto-Stack	✔	✔
Sichere Kommunikation	✔	✔
Sichere Diagnose / Logging	✔	✔
Identity- und Access-Management	✖	✔
Angriffserkennung	✔	✔
Sichere Updates	✖	✔
Trusted Platform	✖	✔

Abb. 3: Security-Bausteine in AUTOSAR Classic und Adaptive (Stand November 2020).

Nachrüstung von Legacy-Systemen mittels AUTOSAR

AUTOSAR ist also durchaus ein Mittel der Wahl, wenn es darum geht, Lücken in Bestandsarchitekturen zu schließen und die Legacy-Systeme durch Umsetzung und Nachweis geeigneter Security-Maßnahmen fitzumachen für die die Typgenehmigung. So ist zum Beispiel in vielen AUTOSAR-Classic-basierten Steuergeräten das SecOC-Modul entweder bereits vorhanden oder kann mit geringem Aufwand nachgerüstet werden. Die sichere Onboard-Kommunikation in Bestandsarchitekturen lässt sich demnach vergleichsweise unproblematisch implementieren, und diese Architekturen können in ihrer revidierten Form weiterhin eine Zulassung erhalten.

Gleichwohl funktioniert die Nachrüstung bestehender E/E-Architekturen mittels AUTOSAR nicht in allen Fällen: Im Gegensatz etwa zu SecOC, das als seit langem fester Bestandteil von AUTOSAR in den meisten ECUs vorhanden ist, lassen sich neuere Security-Features wie IDS (Angriffserkennung per Intrusion Detection System) oder Sichere Updates nicht so leicht nachrüsten, da sie nicht mit früheren AUTOSAR-Versionen kompatibel sind. Nichtsdestotrotz gilt: Dort wo ein Upgrade bestehendender Fahrzeugsysteme möglich ist, und mehr noch für die Entwicklung neuer E/E-Architekturen stellt AUTOSAR einen nützlichen Eckpfeiler für die Umsetzung UNECE-konformer Security-Maßnahmen [1].

Mit AUTOSAR-Security-Bausteinen zu UNECE-konformer Mitigation

Bleibt die Frage, an welcher Stelle und inwieweit sich die einzelnen Anforderungen der UNECE WP.29 an die Cybersicherheit des Fahrzeugtyps und Mitigation fahrzeugspezifischer Bedrohungen (gemäß Annex 5, Part B) mit Hilfe der Security Features, die AUTOSAR bietet, konkret erfüllen lassen. Denn tatsächlich lassen sich die vorhandenen AUTOSAR-Security-Bausteine auf unterschiedliche Weise und in unterschiedliche starken Maße auf die spezifischen Weisungen des Regelwerks bezüglich möglicher Schwachstellen anwenden.

Insofern ist es zweckmäßig, ein qualitatives Rating vorzunehmen, das differenziert aufzeigt, inwieweit die einzelnen AUTOSAR-Security-Bausteine auf die einzelnen in Annex 5 der UNECE-Regularien aufgeführten Mitigationen Anwendung finden können (siehe Abb. 4 auf Seite 10., AUTOSAR-UNECE-Security-Matrix). Je nachdem lässt sich hier unterscheiden zwischen

- ● Komplementärer Security-Baustein: Der AUTOSAR-Security-Baustein stellt Funktionen zur Verfügung, die die Mitigation im Rahmen eines umfassenderen Konzepts unterstützen.
- ●● Konstitutiver Security Baustein: Der AUTOSAR-Security-Baustein stellt Features bereit, die die Mitigation in hohem Maße erfüllen.

AUTOSAR-Module anforderungsgerecht einsetzen – Zwei Beispiele

Die umseitig Tabelle (Abb. 4, AUTOSAR-UNECE-Security-Matrix) liefert konkrete Hinweise, für welche potenziellen Angriffsvektoren und in welchem Maße AUTOSAR-Security zielführend für eine typzulassungskonforme Absicherung der E/E-Architektur eingesetzt werden kann. Die Lesart der Übersicht in Bezug auf Zuordnung und Einstufung der AUTOSAR-Security-Bausteine verdeutlichen hier folgende zwei Beispiele (postulierte Mitigationen aus Annex 5, Part B) [2]:

- **M10 – Das Fahrzeug muss die Authentizität und Integrität der Nachrichten, die es empfängt, überprüfen.**
  Die Authentizität und Integrität der fahrzeuginternen Kommunikation kann durch Verwendung der von AUTOSAR angebotenen sicheren Kommunikationsprotokolle überprüft werden. Diese Protokolle können quasi „out-of-the-box" verwendet werden (●●), wenngleich natürlich eine korrekte Konfiguration erforderlich ist [6]. Zusätzlich ist die sichere Kommunikation auf kryptographische Schlüssel und Primitive angewiesen. Beides wird vom AUTOSAR-Krypto-Stack bereitgestellt, der diesen Anwendungsfall damit ergänzend unterstützt (●).
- **M18 – Es sind Maßnahmen zur Definition und Kontrolle der Benutzerrollen und Zugriffsrechte auf der Grundlage des Prinzips der geringsten Rechte zu ergreifen.**
  Benutzerauthentifizierung und -autorisierung können mit AUTOSAR auf zwei verschiedenen Ebenen realisiert werden: Das AUTOSAR-Modul für Sichere Diagnose kann verwendet werden, um den Zugriff über den Diagnosetester zu authentifizieren (●). Der Baustein Identity & Access Management indes schränkt den Zugriff Benutzer-exponierter Applikationen auf kritische Ressourcen ein (●). Allerdings decken die beiden AUTOSAR-Bausteine hier nur Teilaspekte ab, und gewährleisten keineswegs die Kontrolle aller möglichen und denkbaren Benutzerzugriffe auf das Fahrzeug.
  Sie erfüllen also die Anforderung nicht umfassend, sind aber geeignet die Mitigation mit zu unterstützen.

AUTOSAR-Security als Teil der Lösung

In diesem Zusammenhang ist wichtig, sich noch einmal vor Augen zu halten: Als Middleware stellt AUTOSAR Services zur Verfügung, die von verschiedensten Applikationen genutzt werden können. Das heißt im Umkehrschluss, dass AUTOSAR-Features in der Fahrzeugarchitektur zwar vielfältig einsetzbar sind, aber dabei nicht immer auf den exakt erforderlichen Anwendungsfall einer spezifischen Anforderung abzielen. Gleichwohl lassen sich für die AUTOSAR-Security-Bausteine – mit Blick auf die Tabelle (Bild 4) – zwei wichtige Erkenntnisse formulieren:

- Für fast jede gemäß der UN R155 zu berücksichtigende Mitigation stellt AUTOSAR ein oder mehrere Module bereit, die die jeweilige technische Lösung unterstützen können.
- Für eine ganze Reihe dieser Mitigationen bietet AUTOSAR sogar Funktionen, mit denen sich die Anforderungen weitgehend erfüllen lassen.

Kurzum: AUTOSAR löst sein Versprechen ein, und seine vielfältigen Security-Bausteinen sind grundsätzlich geeignet, alle von der UNECE geforderten Mitigationen zu adressieren. In welchem Ausmaß – ob nur teilweise oder vollständig – sie zur Erfüllung der UNECE-Cybersicherheitsanforderungen als Bedingung für die Typzulassung beitragen, bedarf einer differenzierten Betrachtung. AUTOSAR kann hier also zum wichtigen Teil der Lösung werden, ist aber nicht die alleinige Antwort. Denn um das Fahrzeug ganzheitlich abzusichern, müssen Security-Konzepte für alle Mitigationen entwickelt werden, die sowohl AUTOSAR-Module als auch zusätzliche Security-Systeme, wie z.B. Hardware-Security-Module (HSM), mit einschließen.

AUTOSAR-UNECE-Security-Matrix

Zu berücksichtigende Maßnahmen nach Annex 5 der UN-Regulierung 155	Krypto-Stack	Sichere Kommunikation	Sichere Diagnose/Logging	Identity & Access Mgmt.	Intrusion Detection System	Sichere Updates	Trusted Platform
M3 IT-Sicherheitskontrollen sind auf Backend-Systeme anzuwenden. Wenn Backend-Server für die Bereitstellung von Diensten kritisch sind, gibt es Wiederherstellungsmaßnahmen für den Fall eines Systemausfall.	Außerhalb des AUTOSAR-Anwendungsbereichs – Mindert Bedrohungen außerhalb des Fahrzeugs						
M6 Systeme müssen nach Security-by-Design entwickelt werden, um Risiken zu minimieren.	●	●	●	●	●	●	●
M7 Zum Schutz der Systemdaten / des Codes sind Zugangskontrolltechniken und -designs anzuwenden.			●	●			
M8 Systemdesign und Zugangskontrolle sollte es Unbefugten unmöglich machen, auf persönliche oder systemkritische Daten zuzugreifen.			●	●			
M9 Es sind Maßnahmen zur Verhinderung und Aufdeckung von unbefugtem Zugang anzuwenden.				●●	●		
M10 Das Fahrzeug muss die Authentizität und Integrität der Nachrichten, die es empfängt, überprüfen.	●	●●					
M11 Für die Speicherung kryptografischer Schlüssel sind IT-Sicherheitsmaßnahmen zu implementieren.	●						
M12 Vertrauliche Daten, die ans oder vom Fahrzeug übertragen werden, müssen geschützt werden.	●						
M13 Es sind Maßnahmen zu ergreifen zur Aufdeckung einer Denial-of-Service-Attacke und zur Wiederherstellung nach einem solchen Angriff.					●		
M14 Maßnahmen zum Schutz der Systeme gegen eingebettete Viren/Malware sind in Betracht zu ziehen.					●		●
M15 Maßnahmen zur Erkennung maliziöser interner Nachrichten oder Aktivitäten sind in Betracht zu ziehen.		●●		●	●		
M16 Es sind sichere Software-Update-Verfahren anzuwenden.	●					●●	
M18 Es sind Maßnahmen zur Definition und Kontrolle der Benutzerrollen und Zugriffsrechte auf der Grundlage des Least-Privilege-Prinzips zu ergreifen.			●	●			
M19 Organisationen müssen sicherstellen, dass IT-Sicherheitsverfahren definiert und befolgt werden, einschließlich der Protokollierung von Vorgängen und Zugriffen im Zusammenhang mit dem Management der IT-Sicherheitsfunktionen.			●	●	●		
M20 IT-Sicherheitsmaßnahmen sind auf Systeme anzuwenden, die Fernzugriff haben.	●			●			
M21 Software muss sicherheitsbewertet, authentifiziert und integritätsgeschützt sein. IT-Sicherheitsmaßnahmen müssen angewandt werden, um das Risiko durch Software Dritter, die voraussichtlich im Fahrzeug gehostet wird, zu minimieren.				●●			●●
M22 IT-Sicherheitsmaßnahmen sind auf externe Schnittstellen anzuwenden.	●	●	●●*				
M23 Cybersecurity-Best-Practices für Software- und Hardware-Entwicklung sind zu befolgen.	Aus Software-Sicht außerhalb des Anwendungsbereichs, aber AUTOSAR bietet Leitlinien zum Secure Coding						
M24 Bei der Speicherung personenbezogener Daten sind Best Practices zum Schutz der Datenintegrität und Vertraulichkeit zu befolgen.	●			(●)**			

* Gilt nur für Bedrohung „Threat T18.3" (Diagnoseschnittstellen)
** Rollen/Recht-Management über IAM geplant, aber noch nicht umgesetzt

Rating
● AUTOSAR stellt Features bereit, die im Rahmen eines größeren Konzepts verwendet werden können, um die Mitigation zu implementieren
●● AUTOSAR stellt Features bereit, die die Mitigation zu einem Großteil implementieren

Abb. 4: Mitigationen gemäß Annex 5 der UN-Regulierung 155 und deren Unterstützung durch AUTOSAR-Security-Bausteine.

Fazit: AUTOSAR-Security-Potenziale für die Typgenehmigung erschließen

Sehr bald schon werden OEMs gemeinsam mit ihren Zulieferern für die Typgenehmigung Prozesse und Maßnahmen nachweisen müssen, die eine adäquate Security im Fahrzeug gewährleisten. Die Fahrzeughersteller sind daher verpflichtet, bei der Entwicklung des Fahrzeugtyps ein zertifiziertes Cybersecurity-Managementsystem (CSMS) zur Anwendung zu bringen. Zugleich müssen sie bereits jetzt, derweil sie ihr Cybersicherheitsmanagement aufbauen, die mitigierende Security-Mechanismen gemäß den UNECE-Anforderungen in die Entwicklung ihrer E/E-Architekturen einbeziehen.

Die UNECE-Vorgaben betreffen dabei nicht nur die Entwicklung neuer Fahrzeugtypen, sondern werden ab Mitte 2024 auch für Bestandsarchitekturen wirksam. Womöglich stellt die Nachrüstung von Legacy-Systemen hier sogar die größere Herausforderung dar. Doch egal, ob Neuentwicklung oder Nachrüstung – vollständige Dokumentation, die Identifizierung kritischer Elemente und die planvolle Implementierung von Security-Maßnahmen gemäß Annex 5 der UN-Regulierung 155 sind die zentralen Schritte hin zu adäquater Cybersicherheit im Sinne der Typgenehmigung.

In diesem Zusammnheng kann sich AUTOSAR als nützlicher, zielführender Anker und Hebel erweisen. Denn AUTOSAR bringt heute bereits eine ganze Reihe von Security-Bausteinen mit, die mehr oder minder umfänglich auf die spezifischen von der UN R155 zu berücksichtigenden Mitgationen einzahlen. Es gilt also, die AUTOSAR-Security-Bausteine explizit und an gegebener Stelle im Rahmen des CSMS zu betrachten und in die Verwirklichung UNECE-konformer Automotive Cybersecurity mit einzubeziehen. Gelingt es, das den vorhandenen AUTOSAR-Security-Bausteinen innewohnende Potenzial im Abgleich mit den von der UNECE benannten Bedrohungen und zu beachtenden Mitigationen abzurufen, lassen sich auf dem Weg hin zu einer typgenehmigungsfähig abgesicherten E/E-Architektur Zeit und Kosten sparen.

AUTOSAR wird so zu einem wichtigen Erfolgsfaktor bei der genehmigungspflichtigen Absicherung von Fahrzeugen. Wirksame holistische Automotive Security, wie sie die UNECE WP.29 einfordert, jedoch wird auch über AUTOSAR hinausreichen müssen – vom Hardware-Security-Modul (HSM) im Microcontroller über das fahrzeuginterne Netzwerk hinaus bis ins OEM-Backend oder Vehicle Security Operations Center (V-SOC) sowie über die gesamte Lieferkette und den kompletten Lebenszyklus des Fahrzeugs hinweg.

Quellen

[1] Moritz Minzlaff et al. UNECE-Wunsch trifft AUTOSAR-Wirklichkeit: Adäquate Cybersicherheit als Voraussetzung für die Typgenehmigung. Elektronik automotive, November 2020.

[2] UNECE World Forum for Harmonization of Vehicle Regulations: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Unter: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[3] Michael Schneider et al. AUTOSAR Adaptive: Cybersicherheit inklusive. Elektronik automotive, Dezember 2020.

[4] AUTOSAR Release R20-11. Aktuelle Informationen und Spezifikationen unter: https://www.autosar.org/standards/

[5] Jan Holle et al. Automotive Cybersecurity – Effizientes Risikomanagement für den gesamten Fahrzeuglebenszyklus. ATZelektronik, November 2020.

[6] Michael Schneider, Alexandre Berthold. AUTOSAR Security: A holistic approach. Whitepaper ESCRYPT, Oktober 2019.

Autoren & Kontakt

Dr. Moritz Minzlaff
Senior Manager Security Consulting
Moritz.Minzlaff@escrypt.com

Marcel Rücker, M.Sc.
Security Consultant
Marcel.Ruecker@escrypt.com

Dr. Michael Schneider
Project Manager AUTOSAR Security
MichaelPeter.Schneider@escrypt.com

ESCRYPT GmbH
Ullsteinstraße 128
12109 Berlin, Germany
Phone: +49-30-403-6919-00
info@escrypt.com

www.escrypt.com

Status: 08/2021