SECURITY VON BEGINN AN IM DESIGN-PROZESS VERANKERN

Mehr **Sicherheit** für vernetzte Fahrzeuge

Angesichts der Zunahme von künstlicher Intelligenz und autonomen Systemen, die Entscheidungen auf der Grundlage von in Echtzeit erfassten Daten treffen und der Tatsache, dass die meisten kritischen Systeme im Fahrzeug als Signal übertragen werden, ist es unerlässlich, die Elektronik im Auto von Anfang an auf Security & Safety zu trimmen. Security lässt sich nicht nachträglich in den Entwicklungsprozess einpflegen.

© Ar_TH | Adobestock

Im Wettbewerb, den Nutzern immer anspruchsvollere Erfahrungen zu bieten, entwickeln Fahrzeughersteller und Zulieferer immer komplexere Software für das Auto. Dieses verfügt nun über mehrere Kommunikationsschnittstellen mit den Insassen, dem OEM und der Verkehrsinfrastruktur – von Musik und Video bis über Over-the-Air-Software-Updates und V2X-Kommunikation (Bild 1). Alle diese Schnittstellen können das Risiko eines Cyberangriffs bergen, der die gesamte Produktion des Modelljahres betrifft. Die Fahrzeughersteller sind sich des Risikos bewusst, und es gibt Schwachstellen. Wie lässt sich jedoch das richtige Verfahren für Cybersicherheit, Risikobewertung und -analyse durchführen? Was soll unternommen werden, wenn jemand eine Schwachstelle findet? Wie lassen sich die Auswirkungen auf die Sicherheit der Kunden und auf die Marke minimieren?

Sicherheitsbedenken im Automotive-Bereich

In den letzten zehn Jahren wurden viele schwerwiegende Schwachstellen mit sicherheitskritischen Folgen aufgedeckt. Ein Angriff auf das System über anfällige Kommunikationsschnittstellen wie Bluetooth, Wi-Fi (WLAN) und LTE ist die Standardmethode, um Zugang zu den kritischen Systemen zu erhalten, die intern miteinander vernetzt sind.

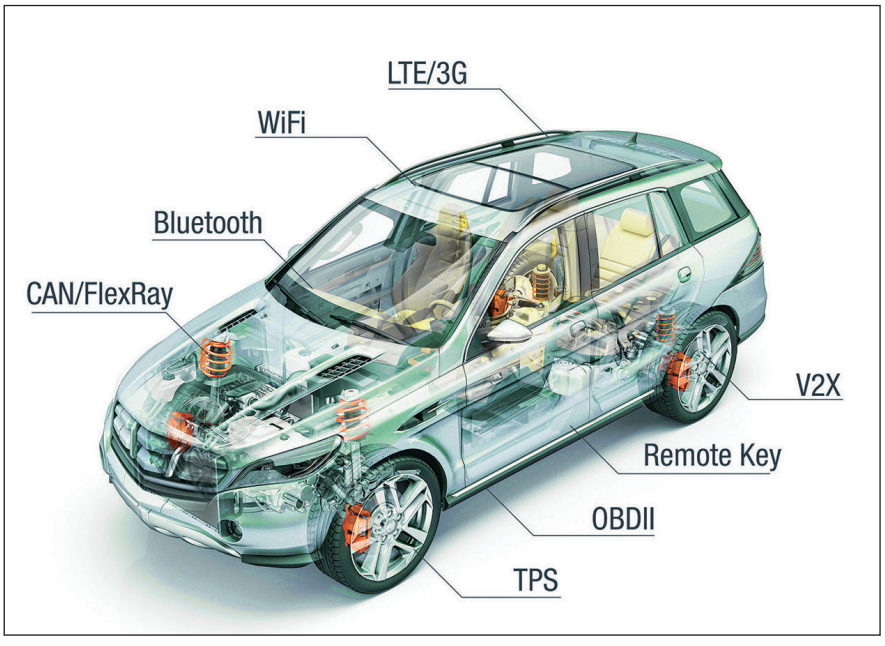

Bild 1: Gefährdete Schnittstellen im Fahrzeug © Green Hills Software

Angreifer nutzen meist eine der Schwachstellen in der Informations-Hub, weil auf dem Infotainment-System häufig ein Allzweck-Betriebssystem wie Linux oder Android ausgeführt wird. Nachdem sie sich Zugang auf das System verschafft haben, wird eine Schad-Software aufgespielt, die versucht, auf den CAN-Bus oder ein ähnliches Busprotokoll wie FlexRay oder LIN zuzugreifen. Weil der CAN-Bus ein Standard-Automotive-Protokoll ist und definiert wurde, bevor die Cybersicherheit des Fahrzeugs überhaupt von Bedeutung war, kann er sicherheitskritische Module wie Motorsensoren, Bremse und Getriebe umfassen. Hat man Zugriff auf ein Fahrzeug, kann der CAN-Bus ausgespäht und das Protokoll analysiert werden. Ein typischer Angriff besteht aus zwei Teilen (Bild 2). Im ersten Schritt wird das Infotainment-System angegriffen; im zweiten der Fahrzeugbus-Prozessor. Automobilhersteller setzen Firewalls und Isolation zwischen den Systemen ein, um die Sicherheit des Systems zu erhöhen – dies muss jedoch richtig konzipiert und bewertet werden.

ISO 21434

Wie können Entwickler bei der Vielzahl komplexer Software-Module im Fahrzeug, die auch von Drittanbietern und Open Source wie Linux/Android stammen, kritische Systemausfälle minimieren? Ein korrekter Software-Entwurf und -Entwicklungsprozess kann Schwachstellen verhindern. Entwickler müssen dabei jede Komponente bewerten und den Code sowie die Interaktionen mit anderen Komponenten verfolgen.

In der Vergangenheit gab es keine Standards für die Cybersicherheit in der Automotive-Branche und Unternehmen entwickelten ihren eigenen Verfahren, um Cybersecurity genüge zu tragen. Wird eine Schwachstelle aufgedeckt, müssen Kunden und andere Beteiligte informiert und ein Patch erstellt und bereitgestellt werden. Andere mögliche Schwachstellen müssen angegangen werden, um die wichtigsten und kritischsten Module vor weiteren Angriffen zu schützen.

Die ISO 26262 ist ein etablierter Standard für funktionale Sicherheit, der die Bewertung von Software-Komponenten vorschreibt. Sie berücksichtigt jedoch nicht den Software-Lebenszyklus wie OTA-Updates und wurde nicht als Norm für Security entwickelt.

Im Gegensatz dazu ist die ISO 21434 ein Rahmenwerk, das sich direkt auf die Cybersicherheit im Automotive-Bereich bezieht. Sie ist einer der Sicherheitsstandards, die vom Echtzeit-Betriebssystem (Real-time Operating System, RTOS) Integrity von Green Hills Software unterstützt werden. Die ISO 21434 gewinnt zunehmend an Bedeutung, weil verschiedene Regionen weltweit die Anforderungen des UNECE WP.29 Automotive Cybersecurity Management Systems (CSMS) in ihre Gesetzgebung übernehmen. Sie ist ein relevanter Standard für die Umset-

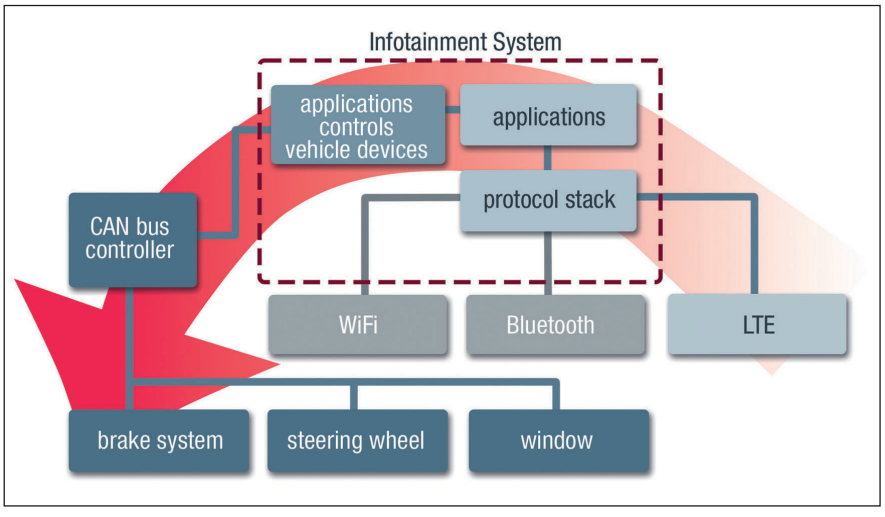

Bild 2: Typischer Angriffsweg eines Hackers © Green Hills Software

zung der UNECE-WP.29-CSMS-Anforderungen in die Praxis.

Das Rahmenwerk deckt das Cybersicherheitsmanagement vom Konzept über die Fertigung bis zum Betrieb ab und definiert eine gemeinsame Sprache für Cybersicherheit. Der Standard hilft zu verstehen, was falsch laufen könnte, wie Unternehmen die Abteilung für Cybersicherheit organisieren können, was sie überprüfen sollten und wie man Probleme handhabt. Es definiert Begriffe, die im Zusammenhang mit Cybersicherheitsrisiken verwendet werden. Das ist wichtig, weil die Verwendung derselben Terminologie für die klare Kommunikation zwischen Organisationen und Unternehmen unerlässlich ist.

Die ISO 21434 bezieht sich eher auf das Lebenszyklusmanagement als auf eine bestimmte Technik, Methode oder ein System. Das traditionelle Sicherheitsmanagement geht nicht weit über die Serienfertigung hinaus. Sobald die Entwicklung abgeschlossen und zertifiziert ist, wird der Code eingefroren. Das Lebenszyklusmanagement deckt einen größeren Bereich ab, der auch den Betrieb und die Wartung umfasst. Die ISO 21434 beschreibt auch, wie Risikobewertungen rund um die Cybersicherheit in jedem Teil des Lebenszyklus angewendet werden können.

Der Standard dient als Leitfaden, um schützenswerte Assets, Bedrohungsszenarien und Risiken zu identifizieren und zu bewerten: Welche Möglichkeiten gibt es, in das Fahrzeugnetz einzudringen? Kann das aus der Ferne erfolgen oder muss sich der Angreifer in der Nähe des Fahrzeugs befinden? Müssen sich Angreifer physisch Zugang zum Fahrzeug verschaffen?

Einige Assets stehen in direktem Zusammenhang mit der Sicherheit, andere nicht. Der Diebstahl persönlicher Daten ist ein Problem, aber kein sicherheitskritisches Ereignis. Wenn jedoch das Bremssystem nicht mehr funktioniert, kann das schwerwiegende Folgen haben. Der Standard hilft bei der Risikobewertung und bietet Hilfsmittel zur Bewertung verschiedener Auswirkungen.

Sicherheitszertifiziertes RTOS ist unerlässlich

Die richtigen Tools und Prozesse erleichtern die Verwaltung des Produktlebenszyklus. Ein sicherheitszertifiziertes Echtzeit-Betriebssystem ist unerlässlich, um undurchdringbare Module im Fahrzeug zu verbauen. Ein solches RTOS (oder Separation Kernel) verwendet Hardware-Speicherschutz, um Treiber, Software von Drittanbietern, Kommunikation, Embedded-Anwendungen zu isolieren und zu schützen sowie eine oder mehrere Instanzen von Android oder Linux zu hosten. Sichere Partitionen garantieren die Trennung von Benutzeraufgaben und sind robuster als sie normalerweise in Universal-Betriebssystemen wie Linux zu finden sind. Der Heap wird beispielsweise getrennt, sodass ein Speicherleck in einer Anwendung keine Auswirkungen auf andere Adressräume hat. Die minimierte Störanfälligkeit zwischen den Anwendungen macht die Risikobewertung überschaubarer und bietet mehr Möglichkeiten, das Risiko zu mindern und zu priorisieren.

Die zuverlässige Echtzeit-Trennungs-Partitionsarchitektur führt neben kritischen Echtzeit-Software-Funktionen mehrere beliebige Gastbetriebssysteme aus (Bild 3). Anwendungen und Gastbetriebssysteme werden effizient auf einen oder mehrere Cores verteilt und können gemäß einem strengen Zugriffskontrollmodell effizient miteinander kommunizieren und Systemperipherie wie die GPU oder Ethernet gemeinsam nutzen. Durch die getrennte Architektur kann das RTOS eine klare Trennung zwischen den Partitionen gewährleisten. Wenn nur eine Anzahl begrenzter Module mit der Fahrzeugbusschnittstelle kommunizieren kann, erhöht das die Systemtrennung und Sicherheit.

Neben dem Betriebssystem sind nach ISO 26262 zertifizierte Entwick-

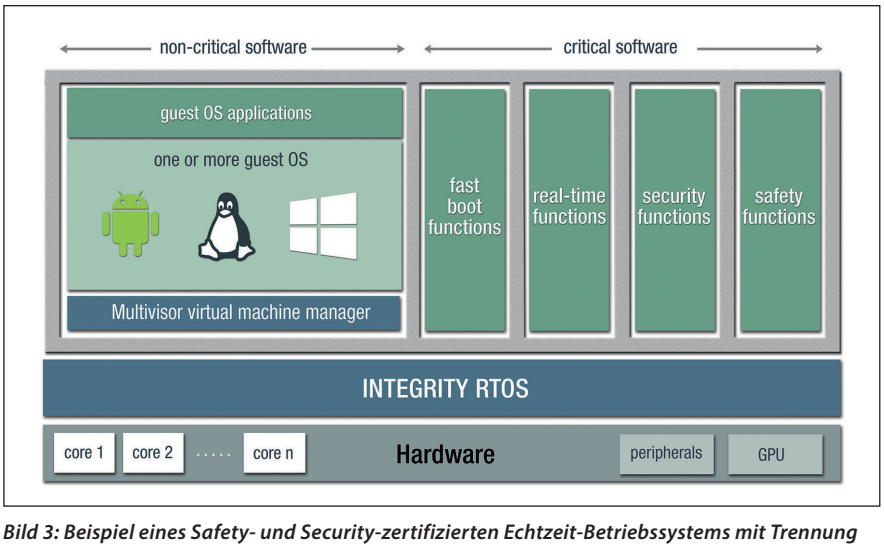

Bild 3: Beispiel eines Safety- und Security-zertifizierten Echtzeit-Betriebssystems mit Trennung
© Green Hills Software

lungswerkzeuge wichtige Komponenten für den Aufbau eines sicheren Systems für Cybersicherheit. Die ISO 21434 erwähnt einige Codierungsrichtlinien wie MISRA C, die zur Risikominderung beitragen. MISRA identifiziert Aspekte der C-Programmiersprache, die aufgrund ihrer Mehrdeutigkeit und Anfälligkeit für häufige Sprachfehler vermieden werden sollten. Zum Beispiel im folgenden Code:

if (flag && (total=num++))

Die ursprüngliche Absicht des Codes ist wohl *„total == num++;"* nicht *„total = num++;"*. Der Programmierer hat das zusätzliche Zeichen „=" übersehen. Daher wird der Code nicht wie erwartet ausgeführt. Selbst wenn der Fehler bemerkt und „=" in „==" geändert wird, wird „num" dann erhöht? Die Antwort lautet ja und nein, denn wenn das Flag falsch ist, wird „num" nicht erhöht. Die MISRA-Richtlinien helfen, diese Art von Fehlern zu vermeiden.

MISRA C ist ein Leitfaden für Software-Entwickler und keine Spezifikation für einen Compiler. Die manuelle Überprüfung des Codes wäre ein mühsamer Prozess. Daher ist es besser, einige dieser Schritte zu automatisieren, um eine einheitliche Durchsetzung zu gewährleisten. Aus diesem Grund kommt es auf die Wahl eines C-Compilers an, der MISRA C 1998, MISRA C:2004 und die neue Version MISRA C:2012 für die gängigsten Automotive-Systemprozessoren wie Arm, RH850, Power Architecture, MIPS und Intel unterstützt.

Hackern keine Angriffsfläche bieten

Mit einer wachsenden Zahl externer Kommunikationsschnittstellen und einer Vielzahl von Software-Anwendungen und Betriebssystemen bieten moderne Fahrzeuge eine große Angriffsfläche für Hacker. Selbst wenn Schwachstellen identifiziert und Gegenmaßnahmen eingeleitet werden, ist der Prozess der Aktualisierung von Systemen und sicheren Installation von Patches in großem Umfang äußerst kostspielig und schwierig. Der Standard ISO/SAE 21434, veröffentlicht im August 2021, bietet einen Rahmen, der speziell für die Cybersicherheit im Automotive-Bereich entwickelt wurde. Die ISO 21434 ist entscheidend für die Umsetzung der UNECE-WP.29-CSMS-Anforderungen (die jetzt weltweit übernommen werden) in die Praxis. Es ist daher unerlässlich, ein Safety- und Security-zertifiziertes RTOS wie Green Hills INTEGRITY zu verwenden, das die ISO 21434 unterstützt. Auch eine zertifizierte und kompatible Toolchain sollte zum Einsatz kommen, um die Sicherheit bei der Entwicklung von Embedded-Systemen für Anwendungen im Fahrzeug zu gewährleisten.

■ (eck)

www.ghs.com

Ryan Kojima ist Embedded Software Consultant, Advanced Products bei Green Hills Software. © Green Hills Software