© Etas

„Die Security muss gewährleistet sein und zugleich das modulare Nfz-Ökosystem unterstützt werden“

Die Systementwicklung im Softwarebereich ist untrennbar mit dem Aspekt Security verbunden. Dies gilt sowohl für den Pkw- als auch Nutzfahrzeugbereich. Dabei unterscheidet sich der Bereich Nfz durch größere Modularität und mehr übergreifende Zusammenarbeit zwischen Herstellern und Zulieferern: Bei diesem und anderen Aspekten könnte sich das Pkw-Segment eine Scheibe abschneiden, meint Dr. Jan Holle von Etas.

ATZelektronik _ Gibt es Besonderheiten, die die Software-Entwicklung im Nfz-Bereich unterscheidet von der für Pkws?
HOLLE _ Auf diese Frage gibt es sicherlich keine Antwort, die für alle Nutzfahrzeughersteller gleichermaßen zutreffend ist. In unseren Security-Softwareprojekten freuen wir uns aber über einen ausgeprägten Pragmatismus. Wir sehen den Wunsch der Hersteller, sehr stark auf Standardkomponenten mit einer entsprechend hohen Wiederverwendbarkeit und den damit einhergehenden ökonomischen Vorteilen zu setzen und erleben sehr kooperative Zusammenarbeitsmodelle, bis hin zu einer gemeinschaftlichen Entwicklung von Anforderungen und entsprechenden Softwarekomponenten.

Welchen Anforderungen muss die Software-Entwicklung für Nutzfahrzeuge genügen?
Im Bereich der nicht funktionalen Anforderungen, der Qualität und Prozesse wie MISRA, ASPICE etc. sehen wir kaum

gravierende Unterschiede zwischen der Software-Entwicklung im Nutzfahrzeug- und der im Pkw-Bereich. Die größten Unterschiede liegen darin, wie man gemeinsam Software entwickelt und die richtigen Softwarepakete spezifiziert und auswählt, denke ich. Durch die vergleichsweise geringen Stückzahlen sind die Nfz-Hersteller deutlich sensibler im Hinblick auf einmalige Software-Entwicklungs- und auch potenzielle Pflege- und Anpassungskosten. Darüber hinaus sehen wir gerade aus Security-Sicht spannende, spezielle Anwendungsfälle, wie beispielsweise Platooning.

© Etas

Dr. Jan Holle ist Product Field Manager Intrusion Detection & Prevention Solution (IDPS) bei Escrypt, einer Marke von Etas, in Stuttgart. Holle hat ein Diplom in Informatik und eine Promotion in Elektrotechnik. Er ist seit 2013 bei Escrypt tätig, zunächst als Security Engineer in den Bereichen IoT-Security und sichere EE-Architekturen und vor seiner heutigen Position als Produktmanager für In-Vehicle Network Security Solutions.

Ist agile Software-Entwicklung auch hier ein Thema oder läuft das klassischer ab, weil die Zyklen langsamer sind?
Hier gibt es genau wie im Pkw-Bereich eine sehr hohe Heterogenität, einige der Nutzfahrzeughersteller haben bereits agile Software-Entwicklungsmethoden im Einsatz oder sind zumindest bereit, sich auf die von uns eingesetzten agilen Methoden wie zum Beispiel SAFe, also Scaled Agile Framework, einzulassen. Aber natürlich gibt es auch Hersteller, die noch eher klassisch orientiert sind. Wir sehen bei einigen Nutzfahrzeugherstellern auch eine Agilität, die wir im Pkw-Bereich eher bei den Startups erleben; möglicherweise ein Ergebnis der vergleichsweise geringen Unternehmensgrößen und einfacheren Organisationsstrukturen. Es geht also nicht zwingend langsamer zu, auch wenn die Produktzyklen möglicherweise länger sind. Die angesprochene Heterogenität sehen wir übrigens ebenfalls beim Reifegrad der Organisationen hinsichtlich Security. Hier erfordert die Heterogenität individuelle Antworten, um den Reifegrad zu erreichen, welcher beispielsweise in der UN R155 gefordert wird.

Welche Rolle spielen Standardisierungen wie die J1939?
Interessanterweise sind der Umfang und die Art und Weise, wie die Standards und deren Möglichkeiten genutzt werden, ebenfalls eher heterogen und reichen von einer sehr umfangreichen Nutzung zur Implementierung eigener Funktionen bis hin zu minimalistischer Implementierung nur an den Schnittstellen, an denen eine Unterstützung des Standards dringend erforderlich ist. Der Standard hilft natürlich insbesondere dort, wo das Ökosystem im Nutzfahrzeugbereich die Kooperation mehrerer Hersteller erfordert, also zum Beispiel, wenn Chassis und Antrieb oder – natürlich noch relevanter – wenn Anbauteile und Aufbauten von unterschiedlichen Herstellern stammen. In diesem Fall spart man hohe Abstimmungsaufwände und ermöglicht flexible Nutzungs- und sogar Umnutzungsvarianten über den Fahrzeuglebenszyklus – von diesem Ansatz könnte man auch für die Entwicklung der zukünftigen, Software-definierten Pkws profitieren. J1939 hilft, die Entwicklung von verschiedenen Softwarekomponenten und der Komponenten insgesamt voneinander zu entkoppeln und vereinfacht dadurch ebenfalls die Entkopplung von Entwicklungszyklen und den Einsatz unterschiedlicher Entwicklungsmethoden.

Sehen Sie auch Nachteile durch Standards?
Wie bei jeder Standardentwicklung bedarf auch die Weiterentwicklung von J1939 eines entsprechenden Aufwandes und der nötigen Zeit für die industrieweite Abstimmung. Insofern erscheint es mir eine dauerhafte Herausforderung zu sein, den Standard schnell genug an neue Technologien und Marktanforderungen anzupassen.

Überwiegt der Vorteil eines gemeinsamen Ökosystems mit größerer Infrastruktur oder ist „one size fits all“ eher ein Nachteil in Sachen Differenzierung?
Das sind natürlich valide Bedenken, jedoch ermöglichen Standards und Standardkomponenten es den Herstellern auch, sich auf ihre Kernkompetenzen zu fokussieren. Sie können sich also konzentrieren auf die Produkt- oder Serviceeigenschaften, welche für den Kunden kaufentscheidend sind. Hinzu kommt, dass wir gerade im Nutzfahrzeugbereich die Notwendigkeit sehen, dass Fahrzeuge erst durch eine Kombination von Systemen verschiedener Hersteller die Anwendungszwecke des Kunden erfüllen können. Würde ein Fahrzeughersteller versuchen, alles aus einer Hand anzubieten, dann müsste er extrem viele Varianten inklusive des entsprechenden Domänenwissens unterstützen, was wirtschaftlich kaum sinnvoll darstellbar ist.

„Die größten Unterschiede liegen darin, wie man gemeinsam Software entwickelt und die richtigen Softwarepakete spezifiziert“

Kann für die Security ein Intrusion Detection System das Allheilmittel sein?
Auf keinen Fall! Ein Intrusion Detection System, also IDS, ist immer eine ergänzende Security-Lösung. Mir ist hier wichtig zu betonen, dass wir zuallererst die grundlegenden Security-Mechanismen im Fahrzeug etablieren müssen. Das sind Mechanismen, wie sichere Firmwareupdates, Secure Onboard-Kommunikation (da, wo sie angemessen ist) und natürlich abgesicherte Diagnosezugriffe, jeweils mit starker Kryptographie

© Etas

Bei einigen Nutzfahrzeugherstellern sehe man eine Agilität, die sich im Pkw-Bereich eher bei den Startups findet, und die möglicherweise ein Ergebnis der vergleichsweise geringen Unternehmensgrößen und einfacheren Organisationsstrukturen sei, meint Holle

beispielsweise unter Nutzung von Hardware-Security-Modulen mit etablierten Automotive-Security-Software-Stacks. Dabei muss stets auch sichere Software-Entwicklung praktiziert werden. Auch hier ist die Wiederverwendung von etablierten Security-Bibliotheken zu empfehlen. Dann erst kann sinnvoll ein Intrusion Detection System, kurz IDS, im Fahrzeug realisiert werden, das vornehmlich die Aufgabe hat, noch nicht bekannte Bedrohungen zu erkennen. Das heißt: Gegen Bedrohungen, die bereits zum Entwicklungszeitpunkt des Fahrzeugs bekannt sind, sollten geeignete Security-Maßnahmen implementiert werden. Ein IDS ist dann eine ergänzende Lösung, um auch für zukünftige, noch unbekannte Bedrohungen gewappnet zu sein.

Wie viele Nfz-OEMs setzen bereits heute IDS ein oder planen deren Verwendung?
Das unterscheidet sich regional sehr stark, am verbreitesten sind IDS in Europa, aber auch die Nfz-Hersteller in Asien (hier insbesondere China) und Nordamerika ziehen gerade stark nach. Der Hauptgrund für die unterschiedliche Einführungsgeschwindigkeit liegt dabei in den regional unterschiedlichen Regulierungen und wird gerade in Europa durch die Security-Anforderungen aus der UN R155 im Rahmen der Typengenehmigung motiviert. In China entstehen gerade umfangreiche Standards und Regulierungen zur Cybersecurity, die in Umfang und Tiefe sogar noch einmal deutlich über die Anforderungen der UN R155 hinausgehen.

Schreiben die von Ihnen angesprochenen Regulierungen konkrete IDS-Technologien vor?
In China ist das in der Tat der Fall, dort sind die Anforderungen so klar formuliert, dass nur noch wenige technische Freiheitsgrade verbleiben. Die UN R155 hingegen verfolgt eher einen risikobasierten Ansatz mit mehr Freiheitsgraden für den OEM. Die Regelung gibt allerdings gerade im Anhang auch sehr konkrete Beispiele für typische Bedrohungen und potenziell geeignete Gegenmaßnahmen, beispielsweise die Erkennung von schädlichen Botschaften auf dem CAN-Bus. Meiner Meinung nach wird es schwerlich gelingen zu argumentieren, wie man diese und ähnliche Anforderungen ohne eine In-Fahrzeug-Überwachungslösung (IDS) verbunden mit einer Flottenüberwachung in Form eines Vehicle Security Operations Center, kurz VSOC, effizient und effektiv erfüllen kann. Auch die meisten OEMs zumindest in Europa haben sich daher unter anderem durch die Integration von IDS-Komponenten und den Aufbau von VSOCs auf die neuen Regulierungen vorbereitet oder bereiten sich aktuell darauf vor.

Hat die Modularität von Nfz-Systemen einen Einfluss auf die Security? Denn entwickelt wird ja eigentlich für sehr viele Märkte und Ausrüster.
In der Tat muss nicht nur im Bereich des IDS, sondern auch im Bereich der anderen Security-Maßnahmen – denken wir zum Beispiel an die notwendige Kryptographie für die Authentifikation bei Diagnoseanforderungen oder auch das Schlüsselmanagement für sichere Onboard-Kommu-

© Etas

In China entstünden gerade umfangreiche Standards und Regulierungen zur Cybersecurity, die in Umfang und Tiefe sogar noch einmal deutlich über die Anforderungen der UN R155 hinausgehen, erklärt Holle

nikation – bei Nutzfahrzeugen eine zusätzliche Herausforderung berücksichtigt werden. Bei jeder Systementwicklung gilt: Die Security muss gewährleistet sein und zugleich das modulare Nfz-Ökosystem unterstützt werden.

Gibt es eine Zusammenarbeit der Hersteller bei Security-Themen?
Die gibt es und wird auch durch uns unterstützt, beispielsweise durch Beteiligung beziehungsweise Beiträge im Rahmen relevanter Gremien. Zu Security-Themen bei Nutzfahrzeugen gibt es beispielsweise eine spezielle Interessensgruppe, die Commercial Vehicle Affinity Group, CAG, im Rahmen des Auto-Isac. Darüber hinaus findet Austausch und Zusammenarbeit natürlich auch in den entsprechenden Gremien von Standardisierungsorganisationen wie der SAE statt.

© Etas

Der vermehrte Einsatz von nicht differenzierenden, standardisierten Softwareplattformen könne viele Vorteile für Hersteller mit sich bringen. Die dadurch ermöglichte Wiederverwendbarkeit von Software sei ökonomisch sinnvoll, kommentiert Holle

„Ein IDS ist eine ergänzende Security-Lösung, um gegen zukünftige Bedrohungen gewappnet zu sein“

Wie sehen Sie OTA-Updates im Nutzfahrzeugbereich – ebenso einfach beherrschbar wie bei Pkws?
Im Hinblick auf Security sehe ich hier keine wesentlichen Unterschiede, aber natürlich haben wir das Thema der Modularität, also die Frage: Wie können Einzelkomponenten im Fahrzeug, ggf. Anbauteile und Aufbaukomponenten auch über die Luftschnittstelle aktualisiert werden und wie kann dennoch ein konsistenter Softwarezustand im Gesamtfahrzeug erreicht werden? Das ist aber zunächst keine Fragestellung, die in erster Linie die Security betrifft.

Die Aufteilung intelligente Zugmaschine – dummer Trailer: Wird sich das aus Ihrer Sicht ändern und was wäre wichtig dafür?
Ich denke, dass wir schon heute Anbauteile sehen, welche eine Eigenintelligenz besitzen und zum Teil werden auch bereits die dafür nötigen Schnittstellen zur Zugmaschine realisiert, denken wir beispielsweise an Sensorik, die aus physikalischen Gründen nicht in der Zugmaschine angeordnet werden kann. Dieser Trend wird sich in der Zukunft sicherlich noch verstärken. Was man aus Security-Sicht natürlich erreichen muss, ist, dass in einem solchen Verbund keine zusätzlichen Schwachstellen entstehen und mindestens das gleiche Sicherheitslevel erreicht wird wie für die eigentliche Zugmaschine. Hierzu stehen uns aber unter anderem gute kryptographische Mechanismen und Security-Konzepte zur Verfügung, um solche Szenarien sicher zu implementieren. Notwendig ist es daher, einen angemessenen Reifegrad des Security Engineering in der eigenen Organisation, der Lieferkette und bei den Partnern im Ökosystem zu erreichen, damit diese Mechanismen und Konzepte korrekt und sinnvoll angewandt werden.

Was verändert sich durch die Elektrifizierung für die Fahrzeuge, beispielsweise durch weitere Kommunikationsoptionen zur Ladesäule?
Jede zusätzliche Schnittstelle und jede zusätzliche Zeile Softwarecode erzeugt mehr Komplexität und somit auch weitere Security-Risiken. Das gilt natürlich auch für neue Schnittstellen, wie jetzt zum Beispiel zur Kommunikation mit Ladesäulen bei der E-Mobilität. Diese Fragestellungen wurden daher auch bereits im Pkw-Bereich adressiert und es sind Standards entwickelt worden, die hierfür zum Beispiel die nötigen kryptographischen Mechanismen beschreiben und auch für kommerzielle Fahrzeuge eingesetzt werden können.

Wäre die starke Zusammenarbeit in bestimmten Bereichen auch ein mögliches Vorbild für den Automarkt?
In der Tat würde ich mir im Pkw-Bereich eine noch stärkere Zusammenarbeit wünschen. Auch würde der vermehrte Einsatz von nicht differenzierenden, standardisierten Softwareplattformen viele Vorteile für Hersteller mit sich bringen. Die dadurch ermöglichte Wiederverwendbarkeit von Software ist ökonomisch sinnvoll. Darüber hinaus könnten dadurch auch Ressourcen für die Entwicklung der Kernfunktionalitäten freigesetzt werden, welche das Fahrzeug eines Herstellers auszeichnen. Auch für die Entwicklung von zukünftigen Fahrzeugfunktionen, gerade im Bereich des automatisierten Fahrens, ist dieser Trend entscheidend. Wir wissen, dass die verfügbaren Software-Entwicklungskapazitäten heute eine absolute Begrenzung der Innovationsfähigkeit sind. Durch bessere Zusammenarbeitsmodelle und den Einsatz von nicht differenzierenden, standardisierten Softwareplattformen werden wir auch schneller in der Lage sein, Software-definierte Fahrzeuge zu entwickeln. Mit solchen Fahrzeugen kann der Hersteller über den gesamten Fahrzeuglebenszyklus hinweg mit innovativen Softwarelösungen auf Basis der gleichen, nicht differenzierenden Softwareplattform beim Kunden überzeugen.

Herr Holle, vielen Dank für das interessante Gespräch.

INTERVIEW: Robert Unseld