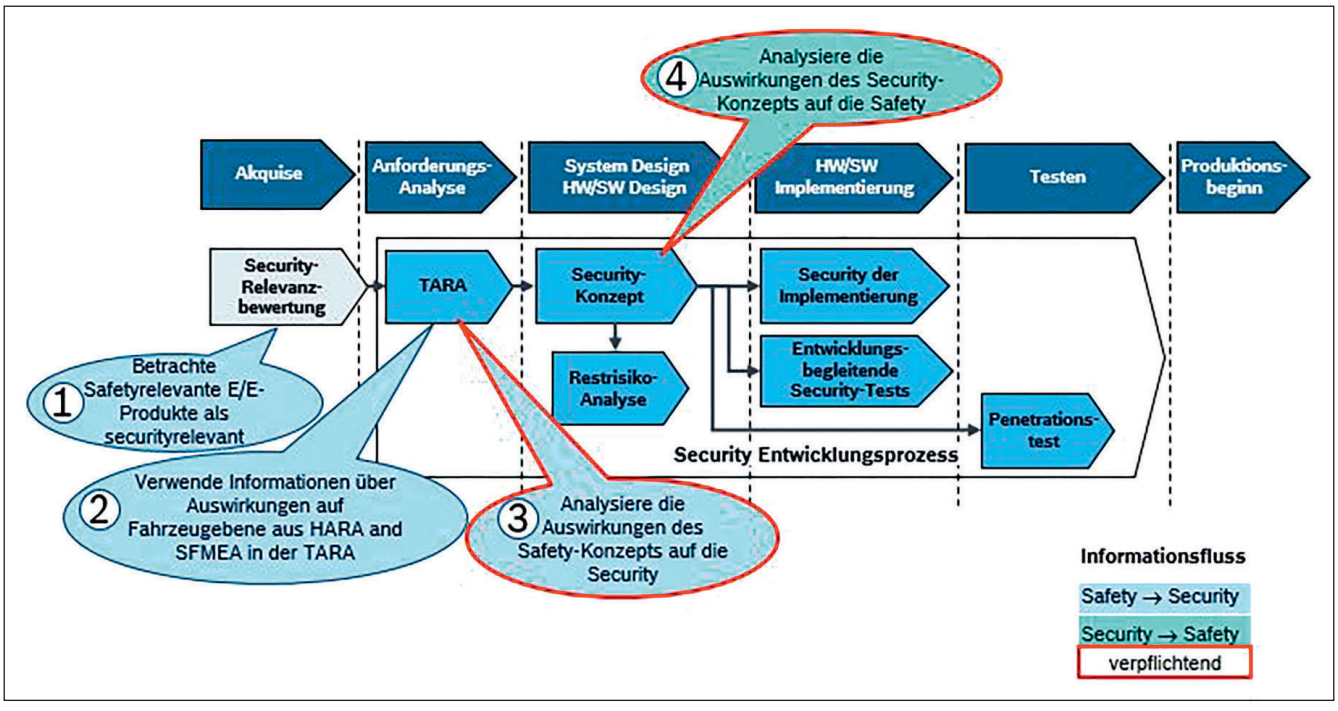

Bild 1: Security-Entwicklungsprozess mit Schnittstellen zum Safety-Entwicklungsprozess. © Bosch

SICHERHEITSSCHNITTSTELLE BEI DER PRODUKTENTWICKLUNG

Gemeinsam safe und secure

Die zunehmende Konnektivität und Automatisierung von Fahrzeugen stellt hohe Anforderungen an Safety und Security. Um diesen Anforderungen gleichermaßen gerecht zu werden, ist bereits in der Produktentwicklung eine enge und systematische Kooperation zwischen beiden Disziplinen erforderlich. Heute ist der Austausch jedoch meist noch informell und unsystematisch.

Sowohl Safety als auch Security befassen sich mit der Sicherheit von Systemen. Jedoch mit unterschiedlichen Zielsetzungen und mit Hilfe verschiedener Maßnahmen. Ziel der funktionalen Sicherheit ist es, dass Fehlfunktionen des Systems oder seiner Bestandteile nicht zu einer Gefährdung von Leib und Leben führen. Gängige Maßnahmen sind beispielsweise Redundanzen, Limiter und Plausibilitäts-Checks. Im Gegensatz dazu hat die Security das Ziel folgenschwere Angriffe auf das System oder seiner Bestandteile möglichst schwierig zu machen. Maßnahmen wie Zugriffsbeschränkungen, Secure Boot und das kryptographisch sichere Signieren von Nachrichten kommen hierfür zum Einsatz.

Bei der Entwicklung von Systemen, die sowohl safe als auch secure sein sollen, kann es passieren, dass die Maßnahmen einer Disziplin das Ziel der jeweils anderen Disziplin gefährden: Einerseits vergrößern Safety-Maßnahmen möglicherweise die Angriffsfläche und erleichtern Angriffe, z.B. durch das Hinzufügen eines weiteren redundanten Kommunikationskanals. Andererseits sind Security-Maßnahmen Funktionen, deren Fehlverhalten Auswirkungen auf die Sicherheit der Fahrzeuginsassen oder anderer Verkehrsteilnehmer haben kann. Eine Abstimmung der Maßnahmen während der Produktentwicklung ist daher unerlässlich. Darüber hinaus besteht die Möglichkeit, Synergien zwischen beiden Disziplinen zu nutzen.

Die Entwicklungsprozesse beider Disziplinen sind sehr ähnlich: Beide verfolgen einen risikobasierten Ansatz. Zu Beginn werden Analysen durchgeführt, um die Safety- bzw. Security-Risiken zu bewerten. Sind diese Risiken inakzeptabel werden im nächsten Schritt Safety- bzw. Security-Anforderungen abgeleitet, die im Safety-bzw. Security-Konzept dokumentiert und in der weiteren Entwicklung umgesetzt und getestet werden. Seit 2011 standardisiert die 2018 aktualisierte ISO26262 [1] den Safety-Entwicklungsprozess im Automobilbereich. Für Ende 2020 wird die Veröffentlichung der ISO21434 [2] erwartet, dem Security-Gegenstück zur ISO26262, welche den Security-Entwicklungsprozess im Automobilbereich standardisieren soll. Die Ähnlichkeit der beiden Entwicklungsprozesse spiegelt sich in der Ähnlichkeit der beiden Normen wieder.

Obwohl in der Automobilbranche inzwischen breiter Konsens darüber besteht, dass eine Zusammenarbeit zwi-

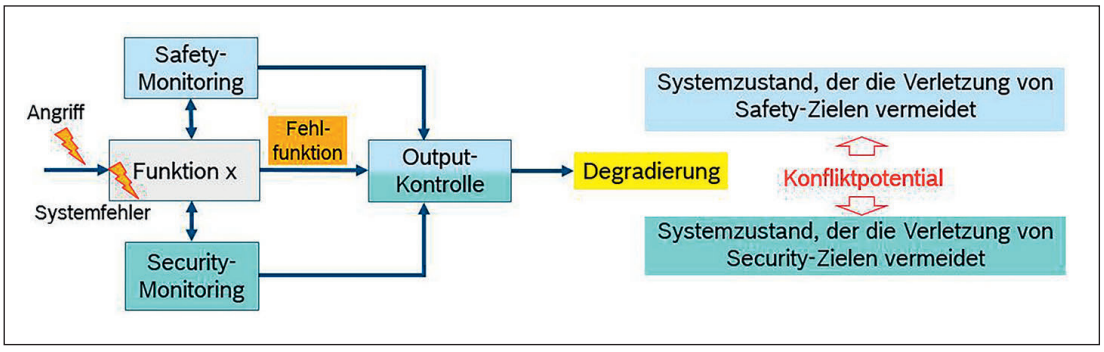

Bild 2: Konfliktpotenzial zwischen Safety- und Security-Reaktionen © Bosch

schen Safety und Security während der Produktentwicklung notwendig ist, ist der Austausch zwischen beiden Disziplinen häufig noch informell und unsystematisch.

Frühere Ansätze verfolgten die Idee eines gemeinsamen Entwicklungsprozesses für Safety und Security basierend auf einer Risikoanalyse, die gleichzeitig Safety- und Security-Risiken beschreibt [3]. Aufgrund der unterschiedlichen Zielsetzungen kann eine solche Analyse jedoch kaum beiden Disziplinen gerecht werden. Zudem würde der Ansatz eine große Umstrukturierung der Produktentwicklung ohne absehbaren Nutzen bedeuten. Im Gegensatz dazu erscheint es vielversprechender, die bestehenden Entwicklungsprozesse und Methoden beizubehalten und durch sinnvolle Prozessschnittstellen zu ergänzen.

Schnittstellen und Zusammenarbeit

Die Prozessschnittstellen lassen sich gut anhand eines Standard-Security-Entwicklungsprozesses erläutern (Bild 1). Security-relevante Produkte müssen nach einem Security-Entwicklungsprozess entwickelt werden. Daher wird die Security-Relevanz am Ende der Akquisephase oder spätestens zu Beginn der Anforderungsanalyse überprüft. Wenn ein Hazard Analysis and Risk Assessment (HARA) bereits verfügbar ist, kann sie für diese Aktivität mitverwendet werden: Falls das Produkt ein Sicherheitsziel von ASIL A oder höher aufweist, wird es automatisch als Security-relevant eingestuft. Umgekehrt sind nicht alle Security-relevanten Produkte automatisch Safety-relevant, da die Security auch Aspekte wie Datenschutz oder IP-Schutz abdeckt. (#1 in Bild. 1). Ist das Produkt Security-relevant, erfolgt eine Risiko-und Bedrohungsanalyse (TARA). Diese bestimmt mögliche Security-Risiken des Produkts. Die Risiken werden als eine Kombination aus der Schwere möglicher Angriffsfolgen und der Schwierigkeit der Durchführung entsprechender Angriffe angegeben. Die Folgen eines Angriffs werden dabei meist auf Fahrzeugebene spürbar wenn das Fahrzeug ein unerwünschtes Verhalten zeigt. Im Zweifel geht man vom schlimmsten Fall aus, also von den schwerwiegendsten Auswirkungen und dem am leichtesten durchführbaren Angriff. Daher hängt die Genauigkeit der Risikoeinschätzung und damit auch die Auswahl passender Gegenmaßnahmen stark von der Qualität und dem Detailgrad der Annahmen ab. HARA und FMEA (Failure Mode and Effects Analysis) sind hervorragende Quellen für detaillierte Informationen über angriffsinduzierte Fehlfunktionen und deren Auswirkung auf das Fahrzeugverhalten. Mithilfe dieser Analysen lassen sich nun Safety-bezogene Auswirkungen von Angriffen auf Fahrzeugebene und deren Schwere fundiert abschätzen (#2 in Bild 1). Besonders wichtig ist die Analyse der Auswirkung der geplanten Safety-Maßnahmen auf die Security (#3 in Bild 1). Einerseits kann es Safety-Maßnahmen geben, die die Security verbessern (z. B. Plausibilitätsprüfungen von Sensorsignalen). Andererseits könnte es »

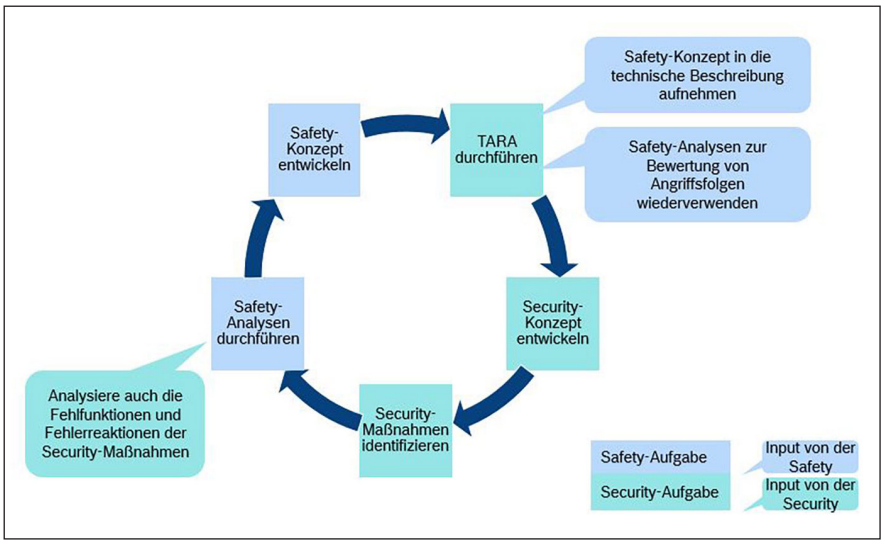

Bild 3: Iterative Abstimmung von Safety-und Security-Konzept © Bosch

Safety-Maßnahmen mit negativen Auswirkungen geben, die die Angriffsfläche vergrößern (z. B. ein zusätzlicher CAN-BUS, der zwei Domänen verbindet, die aus Gründen der Security getrennt sein sollen). Ohne das Wissen um die geplanten Safety-Maßnahmen kann das Security-Risiko unter Umständen als zu gering eingestuft werden könnte. Dies hätte möglicherweise zu schwache Security-Maßnahmen und damit ein unsicheres Produkt zur Folge. Daher sollte diese Prozessschnittstelle verpflichtend sein. Ebenso wichtig ist es, die Safety-Domäne über geplante Security-Maßnahmen zu informieren. Denn im Allgemeinen bedeutet die Implementierung des Security-Konzepts zusätzliche Funktionen des Produkts, Änderungen der HW- oder SW-Architektur usw. Diese neuen oder veränderten Designelemente müssen von der Safety hinsichtlich ihrer Fehlfunktionen systematisch analysiert werden. Ggf. resultieren daraus Safety-Anforderungen an die Security-Maßnahmen, um ein ausreichendes Maß an Sicherheit zu erreichen. Daher sollte auch dieser Prozessschritt verpflichtend sein (#4 in Bild 1). Beispielsweise kann ein Mechanismus zur Überprüfung der kryptographischen Signatur einer Nachricht als Monitor angesehen werden. Seine Fehlermodi „false positive" und „false negative" müssen systematisch analysiert werden. „False positive" beschreibt den Anwendungsfall einer unerwünschten Erkennung oder Erkennung eines nicht vorhandenen Fehlers bzw. Angriffs. „False negative" beschreibt den Anwendungsfall eines erfolgreichen unbemerkten Angriffs. Dies bedeutet, dass der Mechanismus fehlgeschlagen ist. Im Ziel führt ein „false positive"-Ergebnis über eine Safety-Reaktion zu einem zwar unerwünschten aber sicheren Zustand. Der Fehlermodus „false negative" ist unter Safety-Gesichtspunkten sogar noch kritischer. Denn wenn ein Angriff nicht erkannt wird, kann dies möglicherweise zu einer Gefährdung des Fahrzeugs führen (Bild 2).

Das beschriebene Vorgehen erfordert in der Regel einige Iterationen, da die Maßnahmen der einen Domäne die Analysegrundlage der anderen Domäne verändern (Bild 3). Außerdem kann es zu widersprüchlichen Anforderungen der unterschiedlichen Domänen kommen, die ein Überdenken bereits bestehende Konzepte erfordern. Der Prozess zur Abstimmung des Safety- und Security-Konzepts endet, wenn zum einen die Security-Restrisiken akzeptabel sind und zum anderen das Safety-Konzept vollständig ist.

Fazit

Safety und Security sind gleichermaßen Voraussetzung für die Sicherheit eines Systems. Dennoch ist der Austausch zwischen beide Disziplinen häufig noch unsystematisch, informell und unvollständig. Die vorgestellten Prozessschnittstellen zwischen dem Safety- und dem Security-Entwicklungsprozess ermöglichen eine kontinuierliche Synchronisierung und Abstimmung beider Disziplinen während der gesamten Produktentwicklung. Der prozessual verankerte Austausch gewährleistet eine systematische Abdeckung von Security-Aspekten im Safety-Entwicklungsprozess und umgekehrt. Ferner können Widersprüche zwischen dem Safety- und dem Security-Konzept frühzeitig identifiziert werden. Darüber hinaus führt der Ansatz zu realistischeren TARA-Ergebnissen und ermöglicht die Formulierung angemessener Security-Anforderungen und damit eine Optimierung des Entwicklungsaufwands. Da die Schnittstellen auf etablierten und implementierten (Analyse-)Methoden der jeweiligen Disziplin basieren ist der Ansatz mit überschaubarem Aufwand umsetzbar.

Ausblick

Die Definition von Prozessschnittstellen ist nur ein erster notwendiger Schritt. Je nach Produkt führt er zu Safety-Anforderungen an Security-Maßnahmen und Security-Anforderungen an Safety-Maßnahmen mit denen wir in Zukunft umgehen müssen. Beispielsweise werden wir die Reaktionen auf detektierte Angriffe mit den Reaktionen auf detektierte Fehlfunktionen abstimmen müssen. Insbesondere hinsichtlich Degradierung im Fall des autonomen Fahrens ab Level 3 steht die Entwicklung abgestimmter Safety- und Security-Konzepte noch aus. ■ (jr)

www.bosch.com

Quellenverzeichnis

[1] ISO 26262:2018 Road Vehicles – Functional Safety, International Org. for Standardization

[2] ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering, International Organization for Standardization

[3] S. Burton, J. Likkei, P. Vembar and M. Wolf, »Automotive Functional Safety = Safety + Security,« in Proceedings of the First International Conference on Security of Internet of Things, 2012

Jürgen Klarmann ist Safety- und Security-Experte bei der Robert Bosch GmbH in Abstatt.

Claudia Loderhose ist Security-Expertin bei der Robert Bosch GmbH in Schwieberdingen

Franziska Wiemer ist Security-Expertin bei der Robert Bosch GmbH in Abstatt.

Joachim Graf ist Safety-Manager bei der Robert Bosch GmbH in Abstatt.