Berührungspunkte und übergreifende Risiken des Security- und Safety Engineering durch die Vernetzung elektronischer Automobilsysteme mit Internet-Konnektivität

Dr.-Ing. C. Robinson-Mallett, Berner&Mattner Systemtechnik, Berlin
Dipl.-Inf. J. Großmann, Fraunhofer FOKUS, Berlin
Dr.-Ing. B. Kaiser, Berner&Mattner Systemtechnik, Berlin

Kurzfassung

Der Einzug innovativer Informations- und Kommunikationstechnologien mit Internet-Konnektivität in Kraftfahrzeuge führt zu neuen Herausforderungen an die Entwicklung und Absicherung der gesamten Fahrzeugelektronik. Im Zuge dieser Entwicklung rücken auch zunehmend der Kundenwunsch nach Schutz von Privatsphäre und Eigentum sowie Gesetzgebung und Standards bezüglich Datenschutz (Security) in den Fokus der Fahrzeughersteller. Zudem führen der zunehmend hohe Vernetzungsgrad der elektronischen Systeme und die Verknüpfung von Info-/Entertainmentsystemen mit sicherheitskritischen Systemen in Telematikeinheiten zu beträchtlichen zusätzlichen Risiken für die Fahrgastsicherheit (Safety). Aus diesen Gründen ist eine systematische Analyse und Absicherung von Security Anforderungen und die Konzeption von Security Gegenmaßnahmen in den Entwicklungsprozeß von elektronischen Fahrzeugsystemen dringend erforderlich. Die enge Verknüpfung mit oder die Adaption von bereits etablierten Methoden des Safety-Engineering stellt eine effiziente und pragmatische Herangehensweise an diese Problematik dar.

Die Wirksamkeit, schnelle Verbreitung und Replizierbarkeit von schadhaften Programmcodes, z.B. Viren und Würmer, sind in der Informationstechnologie (IT) seit langem anerkannte Risiken. Bisher war die Elektronik in Fahrzeugen vor Angriffen dieser Art weitgehend geschützt, da diese in sich geschlossene Systeme darstellten und Architektur- und Schnittstellendokumentationen nur einem eingeschränkten Nutzerkreis zur Verfügung standen. Ein gezielter Angriff auf die elektronischen Systeme eines Fahrzeugs, ähnlich wie im Fall Stuxnet auf Industrieanlagen geschehen, ist neuerdings aber denkbar, wenn ein mit ausreichenden wirtschaftlichen und technischen Mitteln ausgestatteter Angreifer eine Schwachstelle identifiziert und diese auf potentiell jedes Fahrzeug einer Serie mit Mobilfunkschnittstelle und Internetanbindung zum Einschleusen von Schadcode nutzen kann. Im Extremfall kann dieses Szenario sogar zum Zugriff auf sicherheitskritische Systeme führen, was amerikanische Forscher eindrucksvoll am Beispiel eines aktuellen Serienfahrzeugs demonstrieren, bei dem der Zugriff auf die Bremselektronik über eine branchenübliche Telematikeinheit gelungen ist. Angesichts des Einzugs von kabelloser Internet-Konnektivität in diese Systeme sind noch weitaus kritischere Szenarien denkbar, die keinen physikalischen Zugriff auf das Fahrzeug mehr benötigen.

In diesem Beitrag werden die speziellen Bedrohungsszenarien und möglichen Folgen der Einführung von Internet-Konnektivität in Kraftfahrzeuge erläutert und demonstriert. Die Gefährdungspotentiale infolge der Einführung von Internet-Konnektivität und die daraus abzuleitenden Risiken werden systematisch analysiert, dargestellt und anschaulich im Verhältnis zu bekannten Vorfällen in der IT-Domäne und anderen Industrien erläutert. Weiterhin wird ein Vorschlag zur Reduzierung der genannten Risiken durch Entwicklung und Anpassung von Richtlinien und Vorgehensweisen zur Analyse und Absicherung von Security Anforderungen im industriellen Systementwicklungsprozess entwickelt und vorgestellt.

1. Einleitung

Innovative, vernetzte Info-/Entertainment- und Telematikfunktionen werden zunehmend als wettbewerbsentscheidend wahrgenommen und erfüllen unter Anderem Kundenwünsche nach der Verfügbarkeit von persönlichen Daten und Informationzugang über Internetanbindung, z.B. mittels Browsing, per Cloud oder eMail. Mit dem Einzug dieser Technologien in das Automobil werden neue Risiken hinsichtlich Manipulations- und Datenschutz nun auch für die Entwicklung elektronischer Automobilsysteme relevant [1][2].

Ein mit modernsten Info-/Entertainment- und Telematiksystemen ausgestattetes Automobil hat inzwischen eine Vielzahl software-gesteuerter Schnittstellen, wie beispielsweise Mobilfunk, Bluetooth oder WLAN. Zudem werden diese Systeme vermehrt mit Standardtechnologie ausgerüstet und sind häufig über Telematikfunktionen mit der Fahrzeuginfrastruktur vernetzt, so dass theoretisch ein Zugriff über Schnittstellen der Info-/Entertainmenteinheit auf sicherheitskritische Funktionen möglich ist. Dies prädestiniert diese Systeme als Angriffspunkt für einen unautorisierten Zugriff über die Internetschnittstelle auf die Fahrzeuginfrastruktur.

Dieser technologische Wandel von einem geschlossenen Fahrzeugsystem mit vorwiegend proprietärer Softwaretechnologie hin zu einem offenen, vernetzten Fahrzeug-IT-System führt zu neuen Risiken hinsichtlich Datenschutz, Manipulationsschutz und funktionaler Sicherheit, die im Entwicklungsprozess sorgfältig analysiert, behandelt und abgesichert werden müssen. Mit der Verbreitung von AUTOSAR wird darüber hinaus eine komplexe Standard-Basis-SW für Steuergeräte-Applikationen in die Entwicklung safety-relevanter Systeme eingeführt. Es ist denkbar, dass durch deren Verbreitung auf Steuergeräten auch hier mit erhöhten Security-Risiken zu rechnen ist, da nun auch für das Angriffsziel einer sicherheitskritischen Funktion gilt, was bisher nur für den Injektionspfad des Angriffs galt, dass theoretisch eine Replizierbarkeit auf alle (safety-relevanten) Steuergeräte mit gleichem AUTOSAR Versionsstand ermöglicht wird. Eine weitere Eskalation dieser Situation kann erfolgen, wenn die fahrzeuginterne Vernetzung einen Technologiesprung von CAN bzw. FlexRay zu Ethernet machen wird.

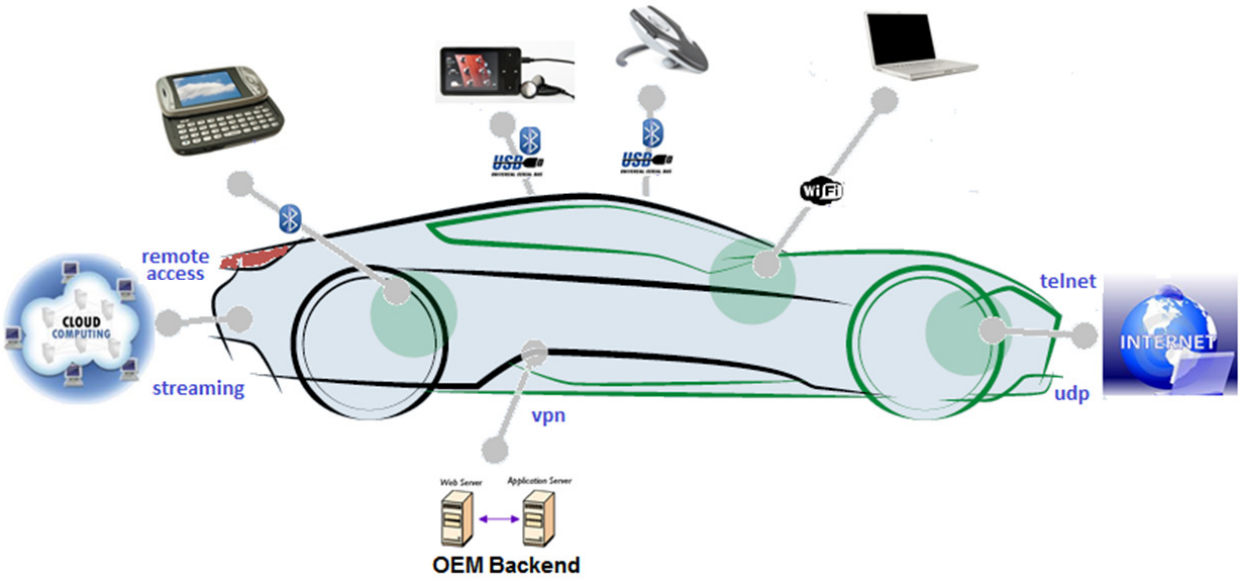

Abbildung 1 Kabellose Schnittstellen moderner Kraftfahrzeuge

In Abbildung 1 wird eine Auswahl software-basierter Schnittstellen, z.B. USB, WLAN oder Bluetooth, in einem modernen Automobil illustriert, über die theoretisch Angriffe auf die Vertraulichkeit, Verfügbarkeit oder Integrität der Automobilsysteme eingeleitet werden können. Im Extremfall kann ein Einbruch über eine dieser Schnittstellen zu einem Angriff auf die sicherheitskritischen Fahrzeugsysteme genutzt werden, was bereits eindrucksvoll demonstriertet werden konnte [4], als der Zugriff auf die Bremselektronik eines handelsüblichen Automobils über das optische Laufwerk einer Info-/Entertainmenteinheit eingeleitet werden konnte. Angesichts des Einzugs von kabelloser Internetkonnektivität in das Automobil sind Szenarien denkbar, in denen, ohne die Notwendigkeit eines physikalischen Zugriffs, potentiell eine gesamte Fahrzeugserie anfällig für eine internetbasierte Angriffstechnik wird.

In diesem Beitrag werden die Risiken und Angriffspotentiale infolge der Vernetzung von IT-Technologien und sicherheitskritischen Fahrzeugsystemen über Info-/Entertainment- und Telematikeinheiten erläutert und diskutiert. Im Folgenden wird ein Vergleich mit StuxNet vorgestellt, um die Risiken für Automobilsysteme anhand eines realen, vergleichbaren Vorfalls anschaulich darzustellen. Es werden vergleichend die Safety- und Securitynormen ISO 15408 und ISO 26262 erläutert und diskutiert, sowie Schnittmengen und Schnittstellen identifiziert. Für erkannte Schwachstellen im Umgang mit der beschriebenen Problematik werden Lösungskonzepte vorgeschlagen. Es werden eine Zusammenfassung und ein Ausblick präsentiert.

2. Ein Vergleich mit StuxNet

Das Beispiel von StuxNet [3][4], dem Angriff auf iranische Atomanlagen mittels Schadsoftware, demonstriert die Risiken der Kombination von Standardsoftware mit sicherheitskritischen, technischen Systemen. Die Vorgehensweise kann als beispielhaft für einen Angriff auf technische Systeme unter Einbeziehung von Internettechnologie angesehen werden. Diese Vorgehensweise ist in angepasster Form auch auf Automobilsysteme denkbar, ein Vergleich ist in Tabelle 1 dargestellt.

Im Gegensatz zu Industrieanlagen, handelt es sich bei Automobilen um Serienprodukte, weshalb erkannte, angreifbare Schwachstellen insbesondere dadurch an Potential entfalten, dass sie in allen Produkten einer Serie ausgenutzt werden können. Um diese Risiken bereits zur Entwicklungszeit zu minimieren, wird es künftig nötig sein, bekannte Techniken und Verfahren zur Entwicklung eingebetteter Software und elektronischer Systeme im Automobil miteinander zu verzahnen, und durch konstruktive, standardisierte Gegenmaßnahmen zu behandeln.

3. Normen zur Beherrschung von Security-und Safety-Risiken

Mit der ISO 26262 [5] ist eine für die Bedürfnisse der Automobilindustrie angepasste Ableitung der etablierten branchenübergreifenden Safety-Norm IEC 61508 eingeführt worden, die innerhalb weniger Jahre einen erheblichen Wandel in der Wahrnehmung und Behandlung von Safety-Risiken in der Entwicklung von Automobilsystemen bewirkt hat.

Zu Evaluation und Absicherung der Securityziele von SW-Systemen steht mit der ISO 15408 [6] ebenfalls eine umfassende international anerkannte Norm zur Verfügung, die allerdings noch an die speziellen Bedürnisse in der Entwicklung von Automobilelektronik angepasst werden sollte.

In diesem Abschnitt werden beide Standards kurz vorgestellt und ihre Schnittstellen- und Schnittmengen diskutiert.

Tabelle 1 Vergleich StuxNet und Automotive Embedded Security

	StuxNet	Angriff auf Fahrzeuge
Infektionsweg	Physikalischer Zugang über USB oder optische Medien Diagnoseschnittstellen Funkschnittstellen, Internet-Konnektivität	
Vorgehen	1. Ausnutzung von Lücken in OS und Standard-SW 2. Installation eines Rootkits zur Analyse des Angriffsziels 3. Identifikation eines Angriffsziels 4. Installation eines Rootkits zur Durchführung des Angriffs	
Zielsystem	Elektronische Steuerung einer atomaren Anlage mit Einzelstück-Charakter	Elektronische Fahrzeugfunktion in Serienprodukt
Security-relevante Schwachpunkte	Verwendung und Vernetzung von Standard-SW und sicherheitskritischer Funktionalität	
Angriffsziele	Störung oder Kontrolle der Steuerungssoftware	Störung oder Kontrolle der Steuerungssoftware Zugriff auf persönliche Daten
Worst Case Folgen	Nuklearer Zwischenfall	Serie schwerer Verkehrsunfälle
Replizierbarkeit	Gering *Angriffsziel ist Unikat*	Hoch *auf vergleichbare Serienprodukte*
Entwicklungskosten des Angriffs	>1.000.000 €	<50.000 €
Komplexität der Aufgabe	Extrem erfordert multidisziplinäres Expertenteam	Mittel erfordert einzelnen Technikenthusiasten
Dokumentation des Infektionswegs	Öffentlich verfügbar da IT-Standardsoftware	Öffentlich verfügbar, wenn IT-Standard
Dokumentation des Angriffsziels	Geheim Gesetzlich regulierter Zugriff	Vertraulich Geschütztes Firmenwissen Teilweise veröffentlichungspflichtig
Beschaffbarkeit von Anschauungsobjekten	Sehr kostenintensiv, eingeschränkter Zugang	Kostengünstig, im Einzelhandel verfügbar
Absicherung erkannter Risiken	Vollständig machbar	Vollständig machbar vor Auslieferung Eingeschränkt machbar nach Auslieferung

3.1. Anwendungskonzept der ISO 15408

Die Entwicklung, Bewertung und Absicherung von Informationssystemen gegen spezifische Sicherheitsziele wird durch die ISO 15408 *(engl. Common Criteria for Information Technology Security Evaluation, CC)* mittels eines mehrstufigen Konzepts unterstützt und reglementiert. Als eines der Schlüsselkonzepte dieser Norm werden in einem *Protection Profile* (PP) die notwendigen Security-Anforderungen (engl. *Security Functional Requirements*, SFR) für eine Klasse von Softwaresystemen spezifiziert, deren Erfüllung notwendig ist, um spezifische Sicherheitsziele zu erfüllen. Zur Entwicklung eines Security-Systems einer bestimmten Klasse, z.B. einer kryptografischen Einheit in einem Diagnosesteuergerät oder ein VPN-Client in einer oben beschriebenen Info-

/Entertainmenteinheit im Automobil, kann das entsprechende PP herangezogen und implementiert werden. Um die Vertrauenswürdigkeit eines Systems (engl. *Target of Evaluation*, TOE) bezüglich einer korrekten und vollständigen Umsetzung des PP zu bewerten und nachzuweisen, können die Absicherungsanforderungen (engl. *Security Assurance Requirements*, SAR) der ISO 15408 herangezogen werden, die mit einer Prüftiefe nach dem in der Norm festgelegten *Evaluation Assurance Level* (EAL) durchgeführt werden. Die EAL beziehen neben den abschließenden Analysen und Tests auch die Systematik und Formalität der Entwicklungsaktivitäten mit ein. Die Vertrauenswürdigkeit des Systems kann somit nach der Art der im System implementierten SFRs und der zur Validation aufgewendeten Prüftiefe nach entsprechendem EAL beurteilt werden.

Die ISO 15408 hat im Kern zwei Aufgaben. Sie erleichtert die Spezifikation von Sicherheitszielen und Sicherheitsanforderungen für spezifische Anwendungen durch Bereitstellung eines Katalogs generischer Sicherheitsanforderungen, und sie bietet einen Satz von Prüftechniken, mit denen sich prüfen lässt, dass die funktionalen Sicherheitsanforderungen umgesetzt und ihre Umsetzung den definierten Anforderungen an die Vertrauenswürdigkeit einer erforderlichen Qualitätsstufe genügt.

Die ISO 15408 stellt prinzipiell auch eine geeignete Vorgehensweise für die Absicherung und Evaluation der Security-Ziele eines elektronischen Automobilsystems bereit. Insbesondere die Sicherheitsziele einer Info-/Entertainment- und Telematikeinheit bzw. einzelner Bestandteile wie Betriebssystem oder *Gateways*, lassen sich mit der ISO 15408 erfassen und absichern. Allgemein anerkannte Sicherheitsziele und daraus abgeleitete Anforderungen für die Automobilindustrie existieren derzeit nicht, allerdings können diese im Einzelfall identifiziert und spezifiziert werden. Ähnlich der ISO 26262 ist hier eine Begutachtung durch eine unabhängige Stelle ratsam, um die Einhaltung des Standes der Technik nachzuweisen. Eine Definition von *Protection Profiles* für Telematiksysteme oder für spezielle *security*-relevante Komponenten im Fahrzeug, z.B. HW- oder SW-*Gateway* an der Schnittstelle zwischen Info-/Entertainment-Einheit und Fahrzeuginfrastruktur, als Minimalstandard für Neuentwicklungen erscheint sinnvoll und empfehlenswert.

3.2. Anwendungskonzepte der ISO 26262

Die ISO 26262 ist eine Norm im Automobilbereich mit dem Ziel, die funktionale Sicherheit oder *Safety* von elektronischen und elektrischen Systemen zu gewährleisten. Sie definiert den aktuellen Stand der Technik in der Entwicklung und Absicherung elektronischer und elektrischer sicherheitsrelevanter Automobilsysteme und zielt auf die Vermeidung bzw. Beherrschung systematischer und zufälliger Fehler, die zu einer Gefährdung von Menschen führen würden. Zu diesem Zweck definiert die Norm ein Prozessmodell und schlägt in Abhängigkeit des zuvor ermittelten Automotive Safety Integrity Levels (ASIL) des Systems Methoden zu dessen Umsetzung vor, die abschließend zu verifizieren und zu validieren sind.

Eine zentrale Maßnahme der ISO 26262 stellt die Durchführung einer Gefährdungsanalyse und Risikoabschätzung dar, durch welche die potentiellen Gefährdungen mittels Betrachtung der potentiellen Fehlfunktionen des Systems identifiziert und in ihren Auswirkungen auf Fahrzeug und Straßenverkehr analysiert werden können. Jeder Gefährdung wird entweder ein ASIL aufsteigend von A bis D zugeordnet, oder sie wird als unkritisch mit QM bewertet. Zu diesem Zweck wird für jede Gefährdung die Schwere der Auswirkung, die Aufenthaltswahrscheinlichkeit in der entsprechenden Situation und die Beherrschbarkeit im Falle des Eintretens des Fehlers abgeschätzt. Aus einer vorgegebenen Tabelle wird die ASIL auf Basis dieser Einflussfaktoren ermittelt. Von der jeweiligen ASIL-Bewertung hängt maßgeblich die Strenge und der Aufwand der nachfolgenden Entwicklungsaktivitäten ab, so etwa der Formalitätsgrad von Anforderungen und Entwurfsmodellen, oder die Testtiefe auf den verschiedenen Ebenen des Software-, Hardware- und Systemtests. Ein weiteres zentrales Element des Safety-Prozesses gem. ISO 26262 ist das Sicherheitskonzept, das in

zwei Stufen (funktionales und technisches Sicherheitskonzept) erstellt wird und zu allen im Rahmen von Sicherheitsanalysen identifizierten Fehlermöglichkeiten entsprechende technische Gegenmaßnahmen vorschreibt. Diese Maßnahmen erstrecken sich auf Prozess-Maßnahmen und technische Maßnahmen im Produkt, beispielsweise Laufzeitdiagnosen von Sensorik. Bei der Definition solcher Maßnahmen sind die normativen und informativen Teile der Norm behilflich, es ist jedoch zusätzlich ein hohes Maß an technischer Domänen-Expertise von Nöten, da die anwendbaren Maßnahmen für ein Lenkungs- oder ein Fahrerassistenzsteuergerät völlig unterschiedlich ausfallen können Ein signifikanter Unterschied zum Security-Engineering liegt in der systematischen Einbeziehung von Hardware-Ausfällen, wofür quantitative Zielgrößen abzuleiten sind, da sich Hardware-Ausfälle nie auf Null reduzieren lassen.

Die Zuständigkeit der ISO 26262 erstreckt sich ausschließlich auf systematische Fehler im Entwurf und zufällige Fehler, z.B. Hardwareausfälle, die zur Laufzeit auftreten. Im Rahmen der geforderten Analysen der ISO 26262, z.B. Fehlerbaumanalyse, werden möglicherweise auch Fehlerursachen erkannt, die auf böswillige Manipulation zurückzuführen sind. Diese werden jedoch im Rahmen der ISO 26262 derzeit nicht behandelt, da es sich nach der Abgrenzung des Gültigkeitsbereichs der Norm nicht um Fehler im System handelt.

Solche böswilligen Eingriffe mit Sicherheitsrelevanz können sein:

- SW-Manipulation der Programmcodes oder der Parametrierung,
  z.B. sogenanntes Chip-Tuning, zur Veränderung von Leistungsparametern; dieses kann zu gefährlichem Systemverhalten führen, das durch die vorhandenen Sicherheitsmaßnahmen nicht abgefangen wird (etwa Erhöhung der Motorleistung oder Verfälschung des Fahrzeug-Geschwindigkeits-Signals)
- Kontrolle oder Manipulation von Aktuatoren über Fahrzeuginfrastruktur
  z.B. direkte Ansteuerung der Bremse oder Lenkung durch fingierte CAN-Nachricht
- Kontrolle oder Manipulation der Datenbasis kooperativer Assistenzsysteme
  z.B. Manipulation von Kameradaten oder Verkehrsmeldungen zur Auslösung von unerwünschten Fahrmanövern durch Stauassistenten

Über die Entwicklungs- und Absicherungsphase hinaus, stellt die ISO 26262 auch Anforderungen an die Produktion, Installation, Betrieb, Wartung, Reparatur und Stillegung des Produkts.

4. Schnittmengen und Schnittstellen von ISO 15408 und ISO 26262

An der technologischen Schnittstelle zwischen Info-/Entertainmentsystemen und Fahrzeuginfrastruktur treffen auch die Domänen des Safety- und des Security-Engineering aufeinander. In Abbildung 2 ist der Verbund von IT-Technologien und sicherheitskritischen Fahrzeugsystemen über Telematikeinheiten schematisch und beispielhaft dargestellt. In der Praxis sind häufig Systeme anzutreffen, bei denen die Schnittstelle zwischen Safety- und Security-Engineering nicht so eindeutig identifiziert werden kann. Beispielsweise, wenn auf Steuergeräten mit sicherheitskritischer Funktion Security-Gegenmaßnahmen implementiert werden, oder wenn bisher als nicht safety-relevant bewertete Geräte durch Telematikfunktionen Schnittstellen zu fahrverhaltensbestimmenden Steuergeräten erhalten. Im ersten Fall ist zu klären, ob die betroffenen Security-Funktionen nach einer Safety-Norm entwickelt werden müssen, da beispielsweise nicht von der Wechselwirkungsfreiheit mit den Safety-Funktionen auf dem gleichen Steuergerät ausgegangen werden kann. Im zweiten Fall ist abzustimmen, ob der Safety-Standard auch auf die betroffenen Funktionen in der Info-/Entertainmenteinheit anzuwenden ist. Beim Zusammenwirken von kommerziellen Security-Software-Komponenten mit safety-relevanten Komponenten auf demselben Prozessor sind zusätzliche Aspekte der Wechselwirkungsfreiheit zu klären, da die Standard-Komponenten in der Regel nicht nach ASIL entwickelt sind, im Fall von Fehlern aber auch die safety-kritischen Prozesse in Mitleidenschaft ziehen könnten.

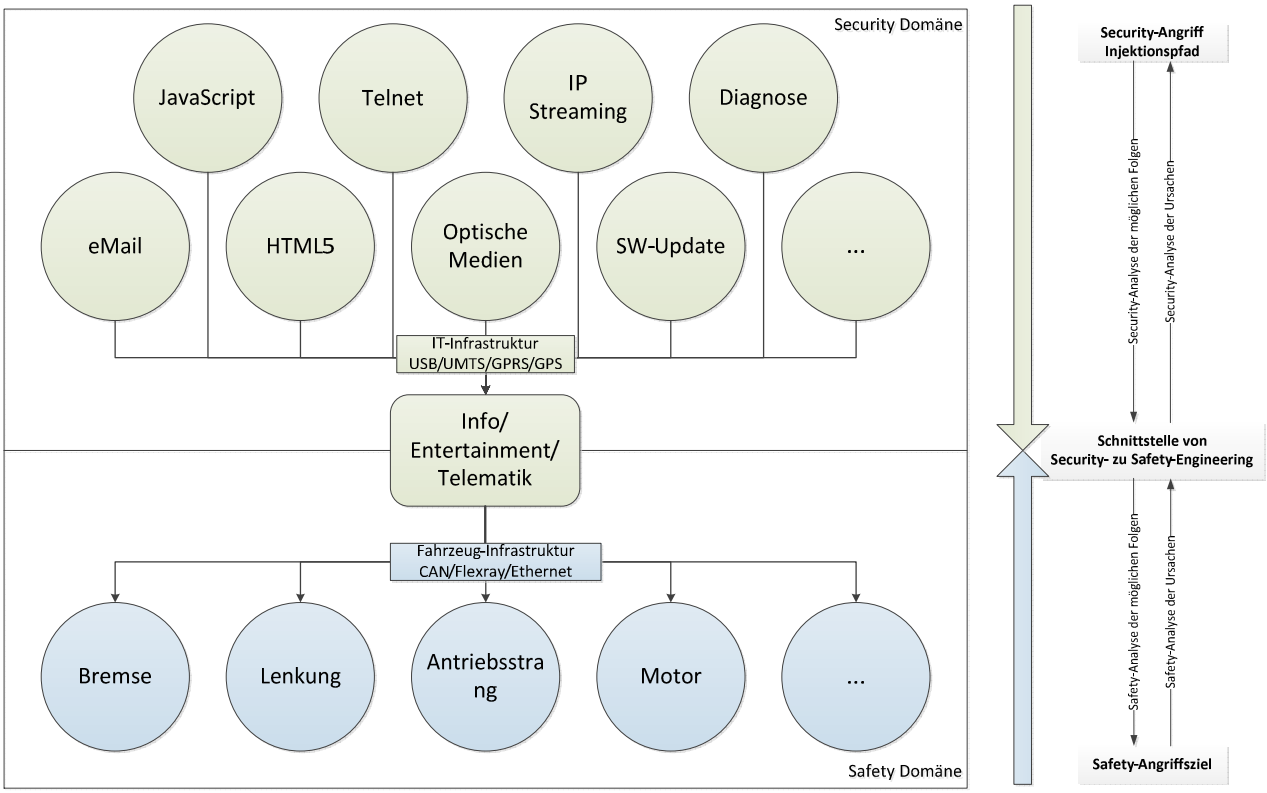

Abbildung 2 IT-Technologie und Fahrzeuginfrastruktur im Verbund

Die Prozessmodelle und Verfahrenweisen von ISO 15408 und ISO 26262 sind den Erfordernissen der jeweiligen Domäne angepasst und unterscheiden sich daher stark. Eine vollständige Analyse der Risiken und Gefährdungen infolge einer böswilligen Manipulation in der Fahrzeuginfrastruktur über einen Einbruch mittels der Internet-Konnektivität würde die Methoden und Werkzeuge des Security-Engineering überfordern, insbesondere da spezielle Expertise über das Ausfallverhalten von Hardwarebausteinen, Sensorik und Aktuatorik erforderlich sind. Es ist ebenso fraglich, ob mittels Safety-Engineering nach Identifikation einer Bedrohung durch böswillige Manipulation der Angriffspfad vollständig zurückverfolgt und geeignete Gegenmaßnahmen getroffen werden könnten - die systematische Vernachlässigung von böswilliger Manipulation und der Prämisse der Schadensmaximierung im Angriffsfall sind hier zwei signifikante Beispiele. Im Safety-Engineering wird das zeitgleiche Eintreten von Fehlern als sehr unwahrscheinlich angenommen, weswegen solche Fehlerkombination nicht notwendigerweise in allen möglichen Folgen untersucht werden. Eine böswillige Manipulation kann dagegen aber auch genau solche Situationen herbeiführen.

Im Folgenden soll daher ein kooperatives Arbeitsmodell und die dazu notwendigen Schnittstellen zwischen Security- und Safety-Engineering vorgeschlagen werden

Ein Vergleich der Prozessmodelle des Security- und Safety-Engineering und eine Definition der Schnittstellen zwischen beiden Domänen erscheint hierzu empfehlenswert. In Abbildung 3 sind Vorschläge für Schnittstellen zwischen den schematisch skizzierten Security- und Safety-Prozessen dargestellt.

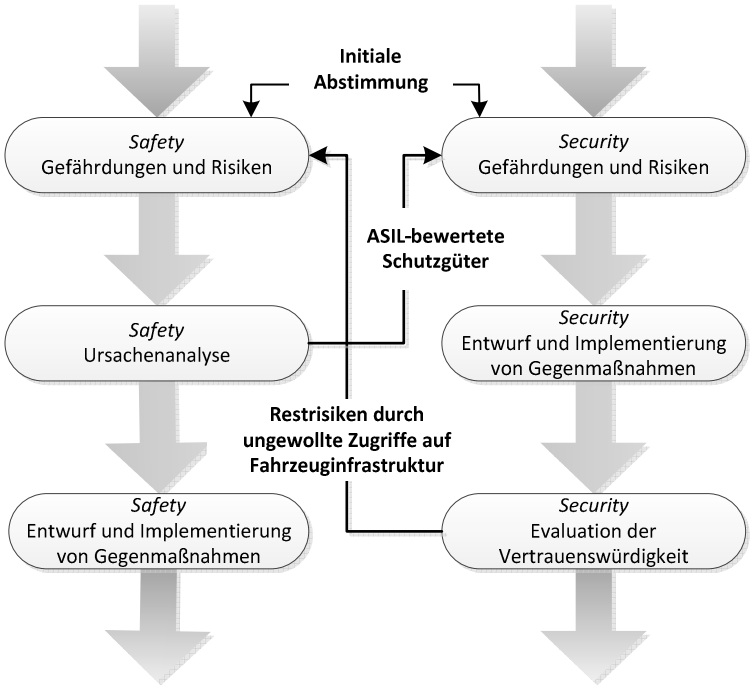

Abbildung 3 Synchronisationspunkte zwischen Security und Safety

Allgemein sollte vor Beginn einer Entwicklungsmaßnahme eine Abstimmung zwischen Security- und Safety-Engineering stattfinden. Da in der Regel nicht von einem zeitgleichen Beginn der Aktivitäten ausgegangen werden kann, sollten sowohl auf Seiten des Security-Engineering, als auch auf Seiten des Safety-Engineering entsprechende Abstimmungsmechanismen etabliert werden. Dabei muss insbesondere davon ausgegangen werden, dass Security-Lücken als mögliche Fehlerursachen mit Safety-Risiken als Folge nicht schon in der Gefährdungsanalyse der Safety entdeckt werden, sondern erst später, in detaillierteren Analysen, wie etwa der Fehlerbaumanalyse. Infolgedessen muss die Gefährdungsanalyse der Security bezogen auf Ergebnisse der Safety-Analysen, gegebenenfalls in mehreren Iterationen oder sogar regelmäßig, aktualisiert werden

Auf Seiten des Safety-Engineering kann während der Rückverfolgung von Systemfehlern als Ursache eine böswillige Manipulation erkannt werden. Diese Information steht allerdings erst zu einem Zeitpunkt zu Verfügung, wenn das Security-Engineering möglicherweise bereits die Gefährdungs- und Risikoanalysen abgeschlossen hat. Die Ergebnisse der Safety-Ursachenanalyse müssten als zusätzliche Schutzgüter in den Security-Prozess aufgenommen werden. Ob solche Manipulationen möglich oder auszuschließen sind, müsste Gegenstand der Analysen und der Entwicklung von Gegenmaßnahmen im Security Engineering werden. Der Umfang und die Strenge der Entwicklung und Umsetzung von Gegenmaßnahmen sollte dabei grundsätzlich vergleichbar zum jeweiligen ASIL der resultierenden Gefährdung erfolgen. Zu diesem Zweck wird an späterer Stelle in diesem Abschnitt eine Abstimmung von ASIL und EAL vorgeschlagen.

Im Security-Engineering werden in einer Gefährdungs- und Risikoanalyse Schutzgüter definiert und entsprechende Gegenmaßnahmen spezifiziert, umgesetzt, validiert und deren Vertrauenswürdigkeit evaluiert. Erst nach einer abschließenden Evaluation der Vertrauenswürdigkeit der Gegenmaßnahmen kann das Restrisiko einer böswilligen Manipulation in der Fahrzeuginfrastruktur abgeschätzt werden. Diese bewerteten Fälle böswilliger Manipulation könnten zur weiteren Analyse im Safety-Engineering genutzt werden. Zu einer Umsetzung solcher Abstimmungsprozesse in der Praxis, fehlen allerdings noch geeignete praxistaugliche Methoden zur Bewertung oder sogar Quantifizierung der

Restrisiken, deren Erforschung und Entwicklung sehr zu empfehlen ist. Neben der Bewertung der Eintrittswahrscheinlichkeit des ursprünglichen Systemfehlers könnte ebenso eine weitergehende Analyse und Identifikation der weiteren potentiellen Systemfehler erfolgen.

4.1. Synchronisation des Umfangs und der Strenge der Entwicklung von Gegenmaßnahmen im Security und Safety-Engineering

Die ISO 26262 sieht eine Diversifikation der Entwicklungs- und Absicherungsprozesse nach der Schwere der möglichen Schäden und dem Potential der Risiken und Gefährdungen vor. Sie definiert ASILs, nach denen die Safety-Anforderungen umgesetzt und abgesichert werden müssen. Die ISO 15408 definiert eine siebenstufige numerische Bewertungsskala, die Evaluation Assurance Level (EAL). Diese Stufen bilden eine aufsteigende Skala, die im Wesentlichen durch zunehmende Anforderungen an den Entwicklungsprozess, Entwurf, Verifikation und Test, des Prüfgegenstands und der Transparenz des Prozesses in der Evaluation charakterisiert sind. Ein grundsätzliches Paradigma der ISO 15408 ist die getrennte Betrachtung von Funktionalität und Vertrauenswürdigkeit. Eine höhere EAL ist nicht gleichbedeutend mit höherem Schutz gegen Security-Gefährdungen. Es ist eher so zu verstehen, dass die beanspruchte Sicherheitsgarantie, durch SFRs spezifiziert und mit entsprechendem Umfang und Formalitätsgrad überprüft wurde.

Die Forderungen an den Entwicklungsprozess gemäß ASIL und EAL haben viele Überschneidungen, weswegen prinzipiell eine Abstimmung von Methoden und des Umfangs und Formalitätsgrads von deren Anwendung über einen Abgleich von ASIL und EAL erfolgen kann.

Für den hier vorgestellten Ansatz gilt die Einschränkung, dass zwar für einen vorgegebenen ASIL ein minimaler EAL angegeben werden kann, siehe Tabelle 2, aber umgekehrt nicht von einem EAL auf einen ASIL geschlossen werden sollte. Ebenso sollte berücksichtigt werden, dass die Security-Eigenschaften eines Systems wesentlich vom Schutzprofil PP abhängen. Daher gilt dieser Vorschlag ausschließlich für Schutzgüter, die in der Folge einer Safety-Analyse in den Security-Prozess einfließen, wie es in Abbildung 3 dargestellt ist. Für den allgemeinen Fall soll an dieser Stelle keine Aussage erfolgen.

Tabelle 2 Synchronisation EAL und ASIL

Vorliegender ASIL	Minimaler EAL infolge ASIL-Vorgabe	Erläuterung
ASIL A-B	EAL 4 methodisch entwickelt, getestet und durchgesehen	ASIL A-B, als auch EAL 4 empfehlen u.a. mind. systematische Vorgehensweise zur Spezifikation, Verifikation und Validation
ASIL C-D	EAL 5 semiformal entworfen und getestet	ASIL A-B, als auch EAL 5 empfehlen u.a. mind. semi-formale Methoden zur Spezifikation, Verifikation und Validation

Der EAL ist neben der ASIL der verbundenen Systeme auch von der Ausprägung der Schnittstelle zwischen Info-/Entertainmentsystem abhängig. Wenn die Schnittstelle geschlossen ist, liegt offensichtlich keine Abhängigkeit von den ASIL vor, dass System kann unabhängig von Safety-Aspekten nach gängigen IT-Standards entwickelt werden. Bei einer offenen bidirektionalen Verbindung liegt eine weitgehende Abhängigkeit vor, die Safety-Aspekte müssen berücksichtigt werden. Durch Verwendung von Software- und Hardware-Gateways kann die Abhängigkeit reduziert werden. Neben den zusätzlichen Entwicklungskosten sind allerdings Einschränkungen in der Realisierbarkeit von Produkteigenschaften hinzunehmen, die von bidirektionaler Kommunikation Gebrauch

machen. Ebenso kann auch ein SW-Gateway zum Ziel eines Security-Angriffs werden, und durch geeignete, möglicherweise noch unbekannte Maßnahmen deaktiviert werden.

Die Wartung von Systemen, zur Schließung der erst nach der Produktauslieferung erkannten Security-Lücken, stellt im Security-Engineering eine Schlüsselkonzept zur Absicherung von Security-Zielen dar. Im Security-Engineering muss von einer befristeten Haltbarkeit der Security-Gegenmaßnahmen ausgegangen werden, da die Erfahrung gezeigt hat, dass heute vermeintlich sichere Systeme in Zukunft durch neue Technologien oder durch Aufdecken von Fehlern kompromittiert werden können. Erfahrungen zeigen ebenfalls, dass mit Rückrufaktionen selten sämtliche ausgelieferten Fahrzeuge einer Serie erreicht werden können. Ob Fernaktualisierungen von Steuergerätesoftware für Automobile eine sinnvolle Lösung sind, ist fraglich. Der notwendige Aktualisierungsmechanismus im Steuergeräte würde einen weiteren security-relevanten Zugang zum Fahrzeugsystem darstellen, der zusätzlichen Entwicklungs- und Absicherungsaufwand verursachen würde. Weiterhin ist eine Softwareaktualisierung an die Randbedingungen vorhandener Security- und Safety-Nachweise gebunden, oder erfordert auch deren Aktualisierung.

5. Absicherungskonzepte nach ISO 26262 und ISO 15408

Die Absicherung der korrekten und vollständigen Umsetzung der spezifizierten Gegenmaßnahmen ist sowohl im Security- als auch im Safety-Engineering ein wichtiger Schritt zur Erreichung der Sicherheitsziele. Es werden Überdeckungsmetriken, Testtiefe bzw. Analysetiefe, erfahrungsbasiertes Testen und funktionales anforderungsbasiertes Testen vorgeschlagen. Der Aufwand bzw. die Testtiefe kann für ein Testobjekt anhand der EAL skaliert werden. Die Testaktivitäten nach ISO 15408 adressieren die Validierung der technischen Security-Anforderungen und basieren daher vorrangig auf funktionalen Testverfahren unter Einbeziehung von unabhängigen, erfahrungsbasierten Tests. Penetrationstest sind nicht Gegenstand der Testaktivitäten im Entwicklungsprozess, obwohl sie im Rahmen der Schwachstellenanalyse für eine abschließende Evaluation des Produkts durch ein Prüflabor vorgeschrieben werden können. Mit der Forderung nach Überdeckung wird die funktionale Vollständigkeit adressiert, die eine vollständige Verfolgbarkeit der Testergebnisse auf die Anforderungen erfordert.

Mit der Forderung nach einer Schwachstellenanalyse durch den Evaluator eines Prüflabors kann durch die ISO 15408 ein Assessment nach verbliebenen potentiellen Lücken und Schwachstellen im System gefordert werden. Im Rahmen dieser Analyse werden Bedrohungen durch Fehler untersucht, die einen unautorisierten Zugriff auf Daten und Funktionalität erlauben würden, oder die eine Veränderung der Zugriffsrechte des Angreifers bewirken könnten. Dieses geschieht einerseits durch die Analyse der verwendeten Software und andererseits durch die Durchführung von Penetrationstests. Als Eingangsdaten für eine solche Schwachstellenanalyse können Erfahrungswerte, Felddaten oder Normen und Standards herangezogen werden. Ein wichtiges Hilfsmittel zu diesem Zweck sind bestehende Kataloge von bekannten Schwachstellen und Sicherheitslücken. OWASP, MITRE und SANS [7][8] veröffentlichen jährlich Listen der für ihren jeweiligen Bereich bekanntesten und am meisten verwendeten Angriffe, Schwachstellen und Sicherheitslücken, die bereits ein Großteil der zu erwartenden Angriffsszenarien für einen Anwendungsfall liefern können. Speziell für die Anwendungen der Automobilindustrie wären eine Adaption solcher Kataloge und deren Anpassung sinnvoll. In neuen, sicherheitskritischen Teilbereichen wie der Car2X gibt es bereits solche Ansätze [9], die entsprechend auch für andere Anwendungsgebiet ausgebaut werden könnten. Weiterhin können die Ergebnisse der aus der Entwicklung und Entwurf vorliegenden Security- und Safety-Analysen für eine Testauswahl herangezogen werden.

Mit suche- und zufallsbasierten Test- und Analyseverfahren, beispielsweise evolutionäres Testen oder Fuzz Testen, stehen Techniken zum automatisierten Aufdecken von potentiellen

Schwachstellen zur Verfügung. Ziel ist es, fehlende oder fehlerhafte Eingabevalidierungsmechanismen aufzudecken, die genutzt werden können, um ein System zu kompromittieren oder Schadcode einzuschleusen.

Grundsätzlich bildet die Zertifizierung von Software oder Softwarekomponenten z.B. Firewalls, Krypto-Algorithmik oder SW-Gateway, einen Baustein zur Absicherung von Systemen. Dies ermöglicht die Etablierung von Standard-Security-Lösungen, die einerseits wiederverwendet werden können und für die es definierte Anforderungskataloge und Prüfvorschriften gibt. Die Anwendung der ISO 15408, könnte für ausgesuchte Problem- bzw. Geräteklassen zur Definition von Schutzprofilen genutzt werden, die als generische Anforderungskataloge zur Sicherstellung eines Mindestmaßes an Schutz gegen Security-Gefährdungen dienen könnten.

Im Safety-Engineering nach ISO 26262 werden Absicherungsmethoden in Abhängigkeit von der ASIL-Bewertung des betrachteten Systems empfohlen. Grundsätzlich wird eine Absicherungsstrategie verlangt, die statische Analyse mit dynamischen Testverfahren kombiniert. Eine Auswahl geeigneter Testableitungsmethoden und Teststrategien sollte pragmatisch nach Software-, Hardware- und Systemtestphasen differenziert erfolgen. Generell wird ein großer Spielraum bei der Auswahl konkreter Testmethoden zugestanden. Die empfohlene Testmethodik deckt Anforderungen an die Funktion, Schnittstellen und Robustheit für Software, Hardware vom Modul über diverse Integrationsstufen bis zum Systemlevel weitgehend ab, klammert jedoch die Frage nach böswilligen Manipulationen auch beim Test absichtlich aus. Dafür liegt in der Safety ein besonderer Fokus auf Robustheits-, Stress- und Fehlerinjektionstests. Ebenso werden Mindestanforderung an den Nachweis der Verfügbarkeit und Zuverlässigkeit erfüllt. Die Verfolgbarkeit und Nachvollziehbarkeit, sowie funktionale Vollständigkeit der Tests werden empfohlen.

Es lässt sich eine grundsätzlich kompatible Philosophie der abgestuften Verifikations-Intensitäten beim Security- wie auch beim Safety-bezogenen Testen erkennen, was zur Vereinheitlichung der Prozesse ausgenutzt werden kann, wenn auch auf fachlicher Ebene für die Security andere Testfälle aufgestellt werden müssen als für die Safety, und daher die Experten beider Fachrichtungen gefragt sind.

6. Zusammenfassung

In diesem Beitrag wurde ausführlich auf die Risiken infolge der Einführung von Internetkonnektivität in Automobile eingegangen. Mögliche Gefährdungen der funktionalen Sicherheit als Konsequenz einer böswilligen Manipulation in sicherheitsrelevanten Automobilsystemen wurden erläutert. Ein Vergleich mit StuxNet hat gezeigt, dass ähnliche Szenarien, wie im Fall des Angriffs auf iranische Atomanlagen, mit weitaus geringeren Investitionskosten auch auf Automobilsysteme übertragbar sind.

Weiterhin wurden die Unterschiede, Schnittmengen und Schnittstellen der Aktivitäten des Security- und Safety-Engineering zur Entwicklung geeigneter Gegenmaßnahmen diskutiert. Es wurden Maßnahmen zur Überwindung einiger Schwachstellen in den aktuellen Vorgehensweisen vorgeschlagen. Insbesondere wird empfohlen einen Abgleich existierender Normen vorzunehmen, beispielsweise der ISO 26262 und der ISO 15408, und die Definition von geeigneten Schnittstellen voranzutreiben, um Umfang und Formalitätsgrad der Entwicklungs- und Absicherungsprozesse den erhöhten Risiken durch böswillige Manipulationen in der Fahrzeuginfrastruktur anzupassen.

Zukünftige Forschungsaktivitäten werden die Entwicklung einheitlicher Werkzeuge und Vorgehensweisen zum Ziel haben. Weiterhin werden die Methoden und Werkzeuge zur Umsetzung der beschriebenen Prozesse auf Praxistauglichkeit untersucht und gegebenenfalls verbesserte Konzepte, Methoden und Werkzeuge entwickelt.

Literatur

[1] J. Meyer, B. Kaiser, C. Robinson-Mallett, Sicherheit ganzheitlich betrachten, Automobil Elektronik 06/12, Hüthig Verlag, 2012

[2] C. Robinson-Mallett, Automotive Security: From Security to Safety Issues through the Introduction of In-Car Internet Connectivity, Invited Talk on 8th Cyber Security and Information Intelligence Research Workshop, 01/2013, Oak Ridge National Research Laboratory, TN, USA

[3] Gefährliches Schadprogramm Computer-Virus Stuxnet trifft deutsche Industrie, Süddeutsche Zeitung am 02.10.2010

[4] Hacker greifen nach dem Steuer, Heise Online am 27.07.2012

[5] International Organization of Standardization (ISO), ISO 26262 Road Vehicles – Functional Safety, www.iso.org

[6] International Organization of Standardization (ISO), ISO 15408 Common Criteria for Information Technology Security Evaluation, www.iso.org

[7] SANS: CWE/SANS TOP 25 Most Dangerous Software Errors

[8] OWASP: OWASP Top Ten

[9] ETSI: ETSI TR 102 893 V1.1.1, Intelligent Transport Systems (ITS) Security Threat, Vulnerability and Risk Analysis (TVRA)