Automotive Safety und Security aus Sicht eines Zulieferers

Matthias Klauda, Stefan Kriso, Reinhold Hamann, Michael Schaffert

Zentralabteilung Automotive Systems Integration (C/AI)
Center of Competence „Functional Safety“
Center of Competence „E/E-Architecture“
Robert Bosch GmbH
Robert-Bosch-Allee 1
74232 Abstatt
{matthias.klauda, stefan.kriso, reinhold.hamann2, michael.schaffert}@de.bosch.com

Abstract: Sichere (im Sinne von „safe“) Systeme im Automobil zu entwickeln und zu produzieren, ist seit Jahrzehnten etablierter Stand der Technik. In jüngster Vergangenheit wurde zur Umsetzung eines konsolidierten Ansatzes zur funktionalen Sicherheit in Straßenfahrzeugen eine neue Norm – die ISO 26262 – erarbeitet. Diese Norm trägt insbesondere den wachsenden Herausforderungen immer komplexerer Systeme und neuer Technologien Rechnung. Allerdings sind Teile der ISO26262 bewusst offen oder visionär formuliert, so dass für eine sinnvolle Umsetzung in vielen Fällen eine einheitliche Interpretation innerhalb der Automobilindustrie unabdingbar ist.

Mit steigender Vernetzung der Fahrzeuge sowohl fahrzeugintern als auch mit der Umgebung (Car-2-X-Kommunikation) bietet das Automobil immer mehr Angriffspunkte für externe Attacken, so dass das Thema Automotive Security wachsende Bedeutung gewinnt.

Einerseits gibt es sowohl bei den Entwicklungsprozessen als auch in der technischen Implementierung Synergien, andererseits aber auch konkurrierende Aspekte zwischen Safety und Security. Dies macht eine enge Zusammenarbeit zwischen diesen beiden Domänen notwendig, um mögliche Synergien zu heben sowie die konkurrierenden Aspekte beherrschen zu können. Zum anderen erscheint es sinnvoll, ein gemeinsames Branchenverständnis im Bereich der Security zu schaffen und hierdurch im Sinne der Sicherheit des Kunden erprobte Methoden und Konzepte branchenweit einheitlich zu etablieren. .

1 Motivation

Safety und Security – im Deutschen beides mit Sicherheit übersetzt – stellen aktuell wichtige Treiber in der Entwicklung elektrischer/elektronischer Systeme im Automobil dar. „Safety“ adressiert hierbei den Schutz des Benutzers (Fahrer, Mitfahrer, Passanten,

etc.) vor dem Fehlverhalten des Systems, d.h. von der Benutzung des Systems darf keine größere Gefährdung ausgehen als es nach dem Stand von Wissenschaft und Technik vermeidbar ist [BGH09]. Während „Safety“ also die Sicht auf das System von innen nach außen darstellt, betrachtet die „Security“ den umgekehrten Fall, die Sicht auf das System von außen nach innen: Hier geht es darum, das System vor unbefugter Benutzung und Manipulation (Hacker, Produzent von Billigersatzteilen, etc.) zu schützen. Ein einfaches Beispiel für ein automobiles System, das sowohl Safety als auch Security adressiert ist ein einfaches mechanisches Türschloss: Im Normalbetrieb soll es das Fahrzeug, seine Werte und seine Insassen durch unberechtigten Zugriff von außen schützen (Security), im Falle eines Unfalls soll es jedoch ein leichtes Öffnen der Tür sicherstellen, um Rettungsmaßnahmen zu ermöglichen (Safety). Die Implementierung dieser beiden Aspekte kann sowohl mechanisch als auch elektronisch erfolgen. In diesem Beitrag wollen wir uns jedoch beschränken auf die elektrischen/elektronischen Systeme, d.h. im Bereich der Safety auf die „Funktionale Sicherheit“ (d.h. auf die von Fehlfunktionen elektrisch/elektronischer Systeme ausgehenden Gefährdungen), im Bereich der Security auf die „Datensicherheit“ (d.h. z.B. nicht auf die Panzerung von Fahrzeugen).

Das Thema Safety ist für die Automobilindustrie nichts Neues; sichere Systeme (im Sinne von „safe“) zu entwickeln und zu produzieren ist seit vielen Jahrzehnten Stand der Dinge. In weltweiten Unfallstatistiken spielen technische Mängel von elektrischen/elektronischen System als Unfallursache eine untergeordnete Rolle (< 1%, siehe z.B. [Li10]).

Dagegen ist der Bereich Security eine recht junge Disziplin. In der Vergangenheit war das Thema zwar schon in einzelnen Domänen adressiert (Tuningschutz für Steuergeräte), jedoch erst durch die zunehmende Realisierung von Fahrzeugfunktionen über Software und die immer mehr aufkommende Vernetzung von Fahrzeugen mit ihrer Umwelt (Internet of Things) gewinnt der Zugriffsschutz eine wachsende Bedeutung.

Eine besondere Herausforderung entsteht darüber hinaus durch die Verbindung der beiden Themen Safety und Security, d.h. einerseits Synergien zwischen beiden zu nutzen, andererseits aber auch sich gegenseitig konterkarierende Maßnahmen zu verhindern.

2 Automotive Safety

Bei der Entwicklung von elektrischen/elektronischen Systemen steht die funktionale Sicherheit schon seit langem im Fokus der Entwicklung. Die Automobilindustrie hat in der Vergangenheit gelernt, wie funktional sichere elektrische/elektronische Systeme zu entwickeln und zu produzieren sind. Wachsende Bedeutung erlangt das Thema in jüngster Vergangenheit durch verschiedene Treiber:

- Die Hochintegration elektronischer Bauelemente (kleinere Strukturgrößen) führt zu einer wachsenden Anfälligkeit gegenüber äußeren Einflüssen.

- Durch steigende Komplexität der Systeme an sich besteht die Gefahr ungewollter bzw. unvorhersehbarer Wechselwirkungen zwischen den Teilkomponenten, z.B. bei neuartigen Funktionen, die rein in Software dargestellt und möglicherweise auf mehrere Steuergeräte verteilt sind.

- Neue Technologien wie zum Beispiel die Elektrifizierung des Antriebstrangs führen zu neuartigen Safety-Fragestellungen, mit denen die Automobilbranche bisher nicht in diesem Maße konfrontiert war.

- Die Tatsache, dass es keine absolut sicheren Systeme gibt, setzt jeden Hersteller der Gefahr aus, dass seine spezifische Lösung im Ernstfall als nicht ausreichend eingestuft wird. Dies hat immer mehr Hersteller einsehen lassen, dass diese Produkthaftungsrisiken nur durch einen gemeinsam definierten Sicherheitsstand zu minimieren sind.

Um diesem Rechnung zu tragen, wurde eine neue Norm zur funktionalen Sicherheit speziell von elektronischen Systemen in Straßenfahrzeugen erarbeitet und im November 2011 veröffentlicht - die ISO 26262 [ISO11]. Diese wurde von den Automobilherstellern und -zulieferern gemeinsam erarbeitet und beschreibt als branchenspezifische Ableitung der IEC 61508 auf einer relativ hohen Abstraktionsebene, wie sicherheitsrelevante Systeme im Automobil entwickelt werden (sollen).

Da aus formaljuristischer Sicht die ISO 26262 zum Stand der Technik beiträgt, ist es zur Reduktion unberechenbarer Produkthaftungsrisiken dringend angeraten, die ISO 26262 umzusetzen, auch wenn es hierzu keine direkte gesetzliche Verpflichtung gibt. Die auf Grund ihres Abstraktionsgrades notwendige Interpretation führt hier aber dazu, dass unterschiedliche Norminterpretationen aufeinandertreffen, die der Produktsicherheit teilweise sogar eher ab- als zuträglich sein können.

Als Beispiel sei an dieser Stelle die Unabhängigkeit bei einem Functional Safety Assessment genannt: Einerseits wird für ein System mit höchstem Automotive Safety Integrity Level (ASIL D) gefordert, dass ein solches Assessment von einer Person durchgeführt wird, die organisatorisch unabhängig ist vom verantwortlichen Projekt. Andererseits soll das Assessment aber die erreichte funktionale Sicherheit des Produkts bewerten, d.h. es soll die Wirksamkeit und die Angemessenheit der implementierten Sicherheitsmaßnahmen beurteilen. Hierzu ist detailliertes Produktwissen notwendig. Dies steht üblicherweise im Widerspruch zur geforderten Unabhängigkeit, da die Fachexperten mit detailliertem Produktwissen eben nicht aus einer anderen, sondern oftmals aus derselben Organisationseinheit kommen. Wird nun die Unabhängigkeitsanforderung der ISO 26262 in dem Sinne überinterpretiert, als dass sie ausschließlich durch externe Assessoren dargestellt werden kann, besteht die Gefahr, dass das Assessment auf Grund mangelnden Produktwissens wertlos ist.

Ein unterschiedliches Branchenverständnis führt hier nicht nur zu Inkompatibilitäten an Zuliefererschnittstellen, sondern unter Umständen auch zu Produkthaftungsproblemen bei Abweichungen vom Branchenverständnis „nach unten“ oder zu unnötigem Overdesign ohne Sicherheitsgewinn bei Abweichungen „nach oben“ [KHK11, KH11].

Insbesondere Automobilzulieferer stehen vor der Herausforderung, unterschiedliche Anforderungen verschiedener OEM umsetzen zu müssen. Beispielsweise stellt sich bei einer Komponenten-Plattformentwicklung die Frage, nach welchem Sicherheitsintegritätslevel (ASIL) diese sinnvoll entwickelt werden kann, um einerseits möglichst viele Kundenforderungen bedienen zu können, um sich aber andererseits auf ein sinnvolles Maß an Aufwand zu beschränken und kein Overdesign ohne Sicherheitsgewinn zu betreiben. Ein gemeinsames Branchenverständnis – durch Erarbeitung eines gemeinsamen Standards, aber auch durch Bilden einer gemeinsamen Interpretation – stellt sicher, dass ein flächendeckend gleiches Niveau an Sicherheit (Safety) gewährleistet wird.

Um dieses Branchenverständnisses weiter zu harmonisieren, hat die Automobilbranche bereits begonnen, an der 2nd Edition der ISO 26262 zu arbeiten, deren Veröffentlichung gegen 2016/2017 zu erwarten ist. Es ist damit zu rechnen, dass hier das Thema „Automotive Security“ zumindest erwähnt werden wird, da Security eine der wichtigen Voraussetzungen für Safety darstellt.

3 Automotive Security

Die stark anwachsende Komplexität elektrischer/elektronischer Systeme – sowohl innerhalb eines Fahrzeugs an sich als auch außerhalb durch dessen Vernetzung mit seiner Umwelt – schafft immer mehr mögliche Angriffspunkte für Angriffe von außen. Insbesondere bietet die drahtlose Vernetzung (GSM, WLAN, Bluetooth) neue Möglichkeiten des (unautorisierten) Zugriffs auf das Fahrzeug, so dass es nicht mehr in dem Maße wie in der Vergangenheit als ein in sich geschlossenes System betrachtet werden darf. Angriffe auf das Fahrzeug können aus verschiedenen Motivationen heraus erfolgen:

- Angreifer, die versuchen, unautorisierten Zugriff auf das Fahrzeug oder seine Komponenten zu erlangen und Korruption / Deaktivierung einzelner Fahrzeugfunktionen androhen (Angriff auf „Availability of Service“)

- „Tuning“ des Fahrzeugs durch Verändern von Eigenschaften/Funktionen (z.B. Chip-Tuning, Fälschen des Tachometerstandes oder Deaktivieren von störenden Warnmeldungen)(Angriff auf „Functional Integrity“),

- Angriff auf die Fahrzeug-Infrastruktur, um darüber an personenbezogene Daten zu gelangen, die z.B. auf einem mit dem Fahrzeug vernetzen Smartphone gespeichert sind (Angriff auf „Personal Integrity“),

Bisher stand die Security einzelner Steuergeräte und ihrer Daten im Vordergrund. Hierfür wurden z.B. in Form des Bosch Hardware Security Moduls (HSM) Lösungen gezeigt und implementiert. Dieses bietet Unterstützung bei der Absicherung folgender Funktionalitäten:

- Secure Flashing: Absicherung, dass nur korrekte Software auf ein Steuergerät heruntergeladen werden kann.

- Secure Boot: Absicherung, dass nur korrekte Software zur Ausführung gebracht werden kann.

- Run-Time Tuning Detection: Absicherung, dass die Ausführung nicht korrekter Software erkannt wird.

- Secure Debug: Absicherung, dass kein Angriff über das Debug-Interface des Mikrocontrollers erfolgen kann.

Im Gegensatz zu üblicherweise separaten „Trusted Platform Modules“ (TPM) ist dieses On-Chip Hardware Security Module (HSM) integriert auf dem Mikrocontroller.

Die zunehmende Vernetzung der Steuergeräte untereinander sowie die Vernetzung mit der Fahrzeugumgebung macht jedoch ebenfalls die Absicherung der Kommunikation *zwischen* den Steuergeräten notwendig: Beispielsweise können Steuergeräte heute in der Regel nicht feststellen, ob die im richtigen Format erhaltene BUS-Nachricht auch vom richtigen Steuergerät kommt oder ein Angreifer das sendende Steuergerät simuliert.

Angriffe mit dem Ziel, auf breiter Front bewusst sicherheits-(safety-)kritisches Verhalten zu provozieren, erscheinen aus heutiger Sicht zwar unwahrscheinlich [We12], können für die Zukunft aber nicht ausgeschlossen werden. Daneben können natürlich auch alle anderen Security-Angriffe auf das Fahrzeug safety-kritisches Verhalten auslösen, auch wenn dies vom Angreifer primär nicht gewollt ist. Vor diesem Hintergrund stellt Security eine wesentliche Voraussetzung für Safety dar; ohne geeignete Security-Maßnahmen lassen sich viele Safety-Funktionen nur schwer umfassend absichern. Kann eine zu einfache Manipulation des Fahrzeugs gar als „zu erwartender Missbrauch“ betrachtet werden, ist es fast schon als Stand der Technik anzusehen, Safety durch Security-Maßnahmen sicherzustellen.

Neben der reinen Absicherung der „Safety Integrity“ ist ein weiterer Treiber die Zuverlässigkeit bzw. Verfügbarkeit des Systems an sich. So lassen sich durch Security-Maßnahmen auch nicht safety-kritische Manipulationen am Fahrzeug erkennen und verhindern – wie zum Beispiel die Verwendung nicht zugelassener Ersatzteile mit deutlich verminderter Performance oder Lebensdauer (Produktpiraterie).

Deutlich wird, dass es - wie auch für Safety - auch für Security kein absolutes Maß für Sicherheit gibt. Jede individuelle Lösung kann dem Vorwurf ausgesetzt sein, nicht vollständig sicher zu sein. Ohne eine branchenweite Abstimmung und damit einem gemeinsamen Ringen um einen allgemeingültigen Stand der Wissenschaft und Technik setzt sich jeder Marktteilnehmer einem hohen Risiko aus, dass seine Lösung nach Jahren im Feld als unzureichend bewertet wird.

4 Gemeinsame Betrachtung von Safety und Security

Um Synergien zwischen Safety und Security nutzen zu können, muss man die Frage stellen, wo Gemeinsamkeiten liegen. Diese findet man zum einen im Entwicklungsprozess, zum anderen aber auch in den technischen Lösungsansätzen.

4.1 Entwicklungsprozess

Während es in der ISO 26262 für Safety einen beschriebenen Entwicklungsprozess gibt, findet man diesen für Security in dieser Form bislang nicht. Genauere Betrachtung zeigt jedoch auf einer entsprechenden Abstraktionsebene viele Gemeinsamkeiten. Es erscheint durchaus sinnvoll, die beiden Entwicklungsprozesse miteinander zu verweben [Eh10, Bu12]. Abbildung 1 schlägt einen Entwicklungsprozess vor, der die Aspekte Safety und Security gemeinschaftlich adressiert:

Nach einer Festlegung des Betrachtungs- / Entwicklungsgegenstandes („Item Definition“) werden in einer Gefährdungsanalyse und Risikobewertung („Hazard Analysis and Risk Assessment“) die Gefährdungen aus Safety-Sicht ermittelt, die Sicherheitsrelevanz (ASIL = Automotive Safety Integrity Level) festgelegt, die umzusetzenden Sicherheitsziele („Safety Goals“) abgeleitet und Maßnahmen („Safety Measures“) zur Umsetzung der Sicherheitsziele definiert. Analog hierzu erfolgt auf der Security-Seite in einer Bedrohungsanalyse („Security Rrisks Analysis“) die Ermittlung möglicher Bedrohungsszenarien, woraus ebenfalls Sicherheitsziele („Security Objectives“) und dementsprechende Maßnahmen („Security Measures“) abgeleitet werden.

Nach Design und Implementierung des Systems sowie dessen Verifikation und Validierung erfolgt einerseits ein „Functional Safety Assessment“, das die erreichte funktionale Sicherheit bewertet, andererseits auf der Security-Seite ggf. eine Begutachtung der erreichten Bedrohungssicherheit.

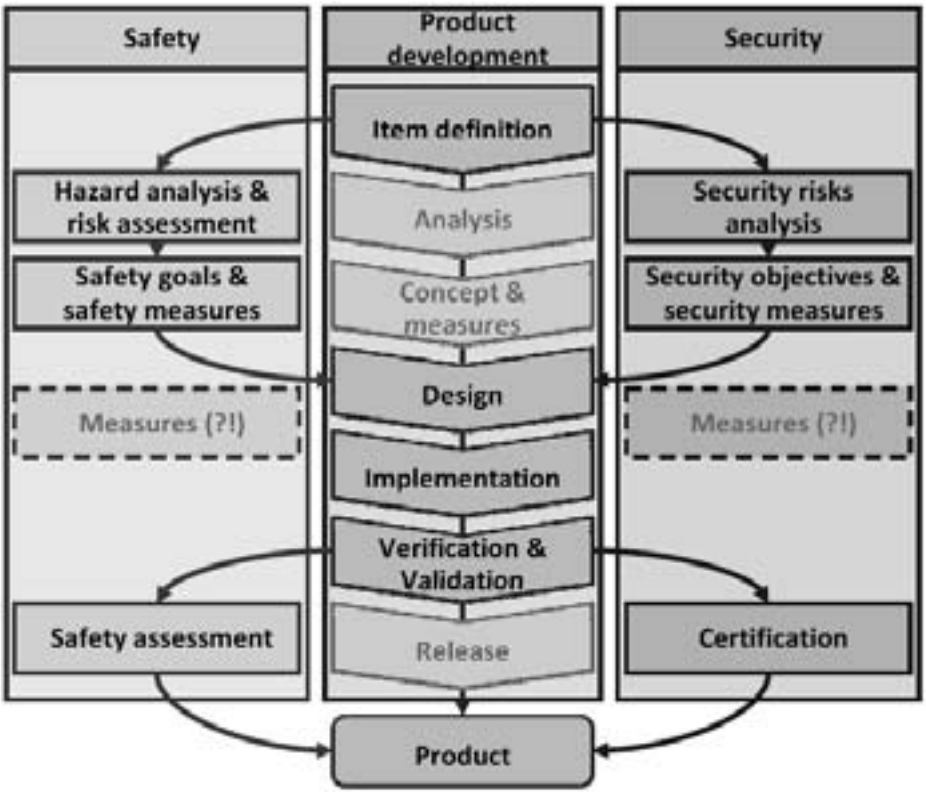

Abbildung 1: Vorschlag für die Berücksichtigung von Safety und Security in einem gemeinsamen Entwicklungsprozess [Eh10]

Auf Grund der Ähnlichkeit beider Vorgehensweisen, der sich daraus ergebenden Synergien sowie des fortgeschrittenen Status des Safety Lifecycles in der bereits veröffentlichten ISO 26262 wurde in [Bu12] vorgeschlagen, die Methodik ISO 26262 um den Aspekt der Security zu erweitern. Inwieweit diese Idee jedoch dem Thema Security gerecht wird, oder ob andere Ansätze eher zielführend sind, muss detailliert evaluiert werden. Eine Community-weite Standardisierung des Themas Security, wie es bei der Safety mit der ISO 26262 gelungen ist, erscheint jedenfalls notwendig und sinnvoll.

4.2 Technische Abhängigkeiten

Nicht nur auf der Ebene der Entwicklungsprozesse und der Methodiken gibt es Abhängigkeiten, sondern auch auf technischer Ebene. Als Beispiele, in denen Security-Lösungen die Safety des Produkts erhöhen können, seien genannt [We12]:

- Sicheres Software-Update und Hochfahren des Systems, um Manipulationen am Steuergerät (Chip-Tuning) zu verhindern. Außerdem lässt sich dadurch das

Einschleusen von „Malware“ (z.B. Viren) verhindern, von welcher weitere Angriffe auf das System ausgehen könnten.

- Komponentenidentifikation durch Authentifizierung sichert ab, dass nur Original-Hardwarekomponenten verbaut werden und keine (möglicherweise gefälschten) Billigkomponenten mit verminderter Performance zum Einsatz kommen.

- Logische Trennung von Infotainment und Safety-relevanten Bereichen im Fahrzeug sichert ab, dass stattfindende Angriffe auf den nicht (oder gering) sicherheitsrelevanten Teil des Systems beschränkt bleiben.

- Absicherung der Kommunikationsbusse erlaubt die Erkennung manipulierter oder ausgeblendeter Botschaften auf Grund eines ungewollten Angriffs auf die Datenkommunikation an sich oder auf Grund einer Manipulation in einem Steuergerät.

Es ist daher notwendig, bei der Implementierung von Safety-Mechanismen auch die Security-Aspekte zu berücksichtigen und umgekehrt. Neben dem organisatorischen Aspekt, dass hierzu eine enge Vernetzung der Experten beider Domänen notwendig ist muss dies auch in der technischen Lösung Niederschlag finden. So mag zum Beispiel das Konzept der Virtualsierung (Hypervisor) geeignet sein, sowohl Safety-Funktionen von nicht-sicherheitsrelevanten Funktionen zu kapseln, gleichzeitig aber auch die Security des Safety-relevanten Teils sicherzustellen.

4.3 Konkurrierende Aspekte

Eine gemeinsame Betrachtung von Safety und Security ermöglicht auf der einen Seite die Nutzung von Synergien, ist aber auf der anderen Seite auch zwingend notwendig, um zu verhindern, dass durch konkurrierende Aspekte die Safety oder die Security des Systems kompromittiert werden.

Ein „Zuviel“ an Security kann beispielsweise Auswirkungen auf die Safety des Produkts haben. So könnte eine Fehlfunktion in der Security-Funktion das Deaktivieren einer Safety-Funktion oder –Komponente zur Folge haben. Wie zum Beispiel in [St12] ausgeführt ist es hier wichtig darauf zu achten, dass als Handlungsleitlinie die Security-Maßnahmen wichtige Safety-Funktionen nicht beeinträchtigen dürfen und die Verfügbarkeit der Safety-Funktion hier gegenüber der Security-Funktion Vorrang haben muss.

5 Zusammenfassung

Bei der Betrachtung von Automotive Safety und Automotive Security darf man sich nicht darauf beschränken, beide Themen unabhängig voneinander zu betrachten.

Zum einen ist es notwendig, Safety und Security gemeinschaftlich zu bearbeiten, um vorhandene Synergien nutzen zu können. Im Bereich der Entwicklungsprozesse heißt das, Vorgehensweisen und Methoden zu finden und in der Organisation zu verankern, die ein gemeinsames Bearbeiten der beiden Themenfelder erlaubt und fördert; dies stellt in erster Linie eine organisatorische Herausforderung dar, da es heute noch nicht sichergestellt ist, dass Safety- und Security-Experten um ihre gegenseitigen Arbeitsfelder wissen und eine Zusammenarbeit systematisch erfolgt. Diese ist aber notwendig, um auch die Synergie auf technischer Ebene in der Implementierung des Systems heben zu können. Gleichzeitig ist dies aber auch nicht nur notwendig, um Synergien zu heben, sondern auch um Security-Maßnahmen, die zur Umsetzung von Safety-Anforderungen dienen, effizient implementieren und potenzielle Konflikte zwischen beiden Domänen verhindern zu können.

Analog zum Safety-Umfeld ist auch bei der Security eine Standardisierung und die Schaffung eines gemeinsamen Branchenverständnisses notwendig, da es ansonsten durch Reibungsverluste zwischen den beteiligten Stakeholdern eines weltweit verteilten OEM- / Zulieferernetzwerks dazu führen kann, dass Security-Lücken entstehen, in die potenzielle Angreifer eindringen und beispielsweise Safety-Probleme provozieren können. Wie beim Thema Safety besteht diese Notwendigkeit insbesondere dann, wenn die Systemsicherheit (Security) von mehreren Beteiligten - d.h. z.B. von Subsystemen verschiedener Zulieferer - abhängt und eine gemeinsame Abstimmung auf Basis eines einheitlichen Verständnisses notwendig wird.

Literaturverzeichnis

[BGH09] BGH Urteil v. 16.6.2009 VI ZR 107/08

[Bu12] Burton, S. et al.: Automotive Functional Safety = Safety + Security. In: 1st International Conference on Security of Internet of Things (SecurIT 2012), Kerala, Indien, 17.-19.08.2012

[Eh10] Eherer, S. et al.: Synergetic Safety and Security Engineering – Improving Efficiency and Dependability. In: 8th escar Embedded Security in Cars conference, Bremen, 16.-17.11.2010

[ISO11] International Organization for Standardization: ISO 26262:2011(E). Genf, 2011.

[KHK11] Klauda M.; Hamann R.; Kriso S.: ISO 26262 – Was kommt da auf uns zu? In: VDI-Berichte 2132, 2011, S. 285-297.

[KH11] Kriso S.; Hamann R.: Die ISO 26262 ist veröffentlicht - Konsequenzen für OEMs und Zulieferer. In: VDI-Berichte 2132, 2011, S. 299-308.

[Li10] Lich, T.: Unfallforschung, Möglichkeiten und Grenzen – Bezug zur ISO 26262. In: 2. Euroforum Jahrestagung zur ISO 26262, Stuttgart, 27.-28.10.2010.

[PW11] Pelzl, J.; Wolf, M.: Mehr Funktionssicherheit durch IT-Sicherheit! In: 3. Euroforum Jahrestagung zur ISO 26262, Stuttgart, 26.-27.09.2011.

[St12] Störtkuhl, T.: Securiy for Safety in der Industrieautomation – Bedrohungen, Schwachstellen, Risiken und Lösungsansätze. In: safe.tech 2012, München, 14.03.2012.

[We12] Weimerskirch A.: Functional Safety by Sound Data Security. In: CTI conference on ISO 26262, Detroit, 12.06.2012.