Sicher unterwegs in einer manipulierten Umwelt

Eine Frage der Safety oder der Security – oder von beidem?

Stefan Kriso, Jürgen Klarmann, Claudia Loderhose, Franziska Wiemer,
Carsten Gebauer, Simon Burton; Robert Bosch GmbH
Markus Ihle, ETAS GmbH

Für ein sicheres automatisiertes Bewegen im Straßenverkehr ist eine Umwelterfassung durch die Fahrzeugsensorik notwendig. Eine bestimmte Klasse von Gefährdungen ist heute nicht ausreichend adressiert, die „Environmental Hacks“ im Sinne von Umweltmanipulationen. Zum Beispiel soll ein Stoppschild sicher erkannt werden. Eine relativ geringe vom menschlichen Auge nicht unbedingt als solche erkennbare Manipulation eines Verkehrszeichens kann eine Fehlklassifikation zur Folge haben, welche wiederum eine Gefährdung von Personen nach sich ziehen kann. Daher muss das System robust gegen solche Manipulationen sein. Ähnliche Effekte können aber auch durch Verschmutzung des Verkehrszeichens auftreten. Daher muss man dies auch bei der Safety-Betrachtung der Nominalfunktion berücksichtigen. Die Frage ist, wie man das Thema „Environmental Hacks“ behandelt, da es sowohl Security (Manipulation) als auch Safety (Auswirkung) betrifft. Der Beitrag zeigt an Hand von Beispielen, wie diese Frage beantwortet werden kann.

Motivation und Beispiele

Sicherheit im Sinne von Safety hat verschiedene „Feindbilder“, die durch unterschiedliche Methoden und Maßnahmen adressiert werden.

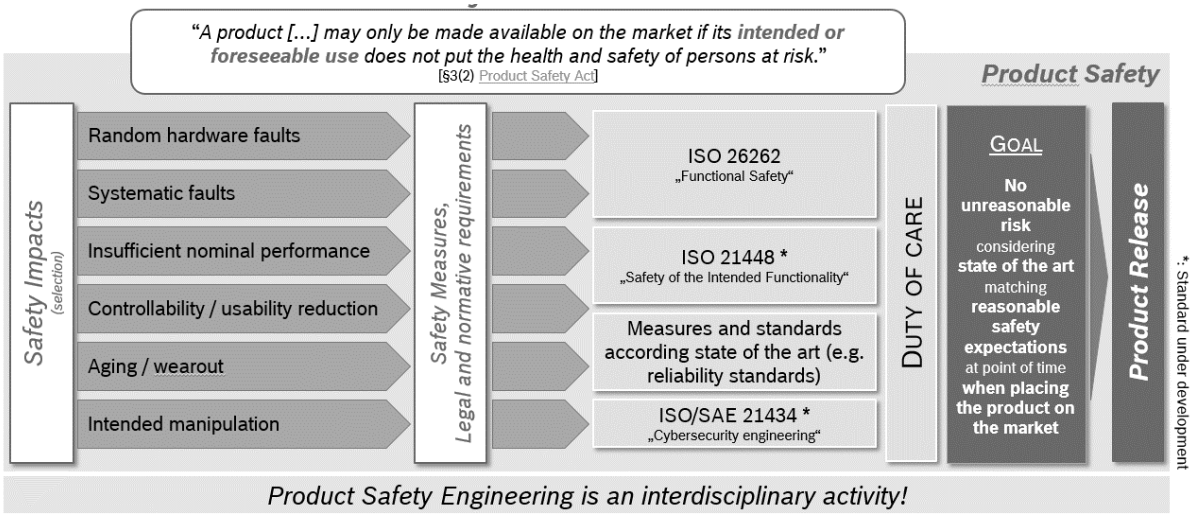

Bild 1: „Feindbilder“ der Automotive Safety (Auswahl)

Systematische Fehler und zufällige Hardware-Fehler, die zu einem fehlerhaften Verhalten des Systems führen können, werden durch die „Funktionale Sicherheit“ adressiert, die entsprechenden Methoden und Maßnahmen sind in der ISO 26262 beschrieben. Für die Sicherheit der Sollfunktion (SOTIF – „Safety of the Intended Functionality“) ist derzeit ein Standard in Arbeit, die ISO 21448. Hier wird die Frage adressiert, wie beispielsweise ein sicheres System gestaltet werden kann unter Berücksichtigung physikalischer

Unzulänglichkeiten der Sensorik. Auch bewusste Manipulationen des Systems können Einfluss auf die Safety haben. Dies ist durch Maßnahmen der Cybersecurity zu adressieren; hierfür ist ebenfalls ein Standard in Vorbereitung (ISO/SAE 21434).

Darüber hinaus gibt es ein weiteres „Feindbild“, die „Environmental Hacks“, die wir anhand von drei Beispielen einführen wollen:

Die Manipulation von Verkehrszeichen mag für den menschlichen Betrachter noch als solche erkennbar sein und das manipulierte Zeichen in seiner ursprünglichen Intention für den Fahrzeugführer noch als solche erkennbar sein, so muss dies beim automatisierten Fahren nicht zwangsläufig auch gegeben sein. Bereits eine kleine aber gezielte Manipulation kann bei Bilderkennungsalgorithmen zu Fehlklassifikationen führen ([3]), was dazu führt, dass das Verkehrszeichen vom System „übersehen“ werden.

In [4] konnte sogar eine Manipulation demonstriert werden, in der ein System ein manipuliertes Stopp-Schild als ein Tempolimit-Schild fehlinterpretiert hat.

Bild 2: Beispiel für ein manipuliertes Verkehrszeichen [1]

Als ein weiteres Beispiel von „Environmental Hacks“ können die Laser-Attacken angesehen werden, die gelegentlich auch in der Presse Erwähnung finden ([5]). Während dort meist über Attacken auf menschliche Fahrer berichtet wird, haben derartige Attacken auch Auswirkungen auf die Sensorik und können letztendlich zum Ausfall oder zu einem Fehlverhalten führen.

Dieser Angriff führt somit zu einem „Denial of Service“ und lässt sich daher in die Kategorie der DoS-Attacke einordnen, auch wenn die Störungsquelle außerhalb des Systems liegt.

Jammen und Spoofen von GNSS-Signalen (Global Navigation Satellite System) stellen weitere Manipulationen der Umwelt dar. Beim Jammen wird das Empfangen von GNSS-Signalen durch einen Störsender verhindert. GNSS-Spoofing dagegen bezeichnet das Senden

gefälschter GNSS-Dignale. Diese sind von der Sensorik alleine nicht als Fälschungen erkennbar, da sie in sich valide sind.

GNSS-Jamming und -Spoofing können bewusst eingesetzt werden, um das Fahrzeugverhalten zu beeinflussen. Es gibt aber auch Szenarien, in denen GNSS-Jamming oder -Spoofing gegen andere Ziele gerichtet sind und das Fahrzeug nur versehentlich in den Einflussbereich von gestörten oder gefälschten Signalen gerät.

In [13] wird von einem Fall berichtet, in dem ein LKW-Fahrer einen GPS-Jammer verwendet, um den im Fahrzeug eingebauten GPS-Tracker zu stören und damit seinen Aufenthaltsort vor seinem Vorgesetzten zu verbergen. Auf einem nahegelegenen Flughafen kommt es dadurch versehentlich zu Störungen eines GPS-basierten Flugzeugleitsystems. Diese Auswirkungen lassen sich auf Fahrzeuge mit GPS-basierten Funktionen übertragen.

[14] beschreibt eine GPS-Spoofing-Attacke, die Fahrzeuge mit GPS-basierten Funktionen unbeabsichtigt in Mitleidenschaft ziehen kann. Mit Hilfe eines Software Defined Radio werden gefälschte GPS-Signale erzeugt, die der App „Pokemon Go“ einen falschen Aufenthaltsort des Spielers vorgaukeln. Dadurch kann der Spieler von zuhause aus spielen, ohne spazieren gehen zu müssen.

Die Anwendungsfälle von GNSS-Spoofing sind vielfältig. Mit derselben Vorgehensweise lassen sich z.B. ortsgebundene Services unerlaubt aktivieren oder GPS-basierte Mautsysteme überlisten. [12] verzeichnet eine Zunahme von GNSS-Jamming und Spoofing. Daher ist es wichtig, sie im Kontext von GNSS-basierten Fahrzeugfunktionalitäten zu betrachten und zu analysieren.

Relevanz von „Environmental Hacks“ für die Safety

Wie aus den Beispielen deutlich wird, können „Environmental Hacks“ Einfluss auf die Safety, die Verfügbarkeit und die Performance des Produkts haben. Für die Safety wäre ein „Environmental Hack“ ein weiteres zu berücksichtigendes „Fehlerbild“ (Bild 1).
Die Bereiche Verfügbarkeit und Performance bei „Environmental Hacks“ zielen nicht mehr auf die Safety des Produkts, sondern mehr in Richtung Benutzerakzeptanz: Die in unserem Beispiel relevante Fragen wären hierbei, ob es ein Benutzer akzeptieren würde, wenn ein selbst-fahrendes Fahrzeug öfter unvermittelt anhält oder falsch abbiegt bzw. ob er es noch für vertretbar hielte, wenn sich ein automatisiertes Fahrzeug von einem Laser-Pointer zum Preis von 10 Euro außer Kraft setzen ließe.

„Environmental Hacks“: Safety oder Security?

Die Feindbilder der Funktionalen Sicherheit sind systematische Fehler und zufällige Hardware-Fehler. Zur Vermeidung systematischer Fehler werden Anforderungen an den Entwicklungsprozess („Safety Life Cycle“), zur Beherrschung zufälliger Hardware-Fehler und verbleibender systematischer Fehler (deren Vermeidung grundsätzlich nicht vollständig sichergestellt werden kann) Anforderungen an die technische Umsetzung im Produkt (z.B. Redundanzen, Monitoring, Diagnosen) gestellt.
Verlassen wir nun die Fehlerdbilder der Funktionalen Sicherheit, nämlich die systematischen Fehler und zufälligen Hardware-Fehler, und schauen uns ein weiteres Feindbild an: den bewussten Angriff auf das Fahrzeug bzw. seine E/E-Systeme. Zunächst gilt festzustellen, dass wir uns mit diesem Feindbild außerhalb der Funktionalen Sicherheit und damit außerhalb des Anwendungsbereichs der ISO 26262 befinden. Trotzdem kann auch dieses Feindbild zu

einem Safety-kritischen Verhalten führen und daher prinzipiell safety-relevant sein [8]. Dieses Feindbild wird adressiert durch die Maßnahmen der Cybersecurity, die momentan in der ISO/SAE 21434 „Cybersecurity Engineering“ standardisiert werden.

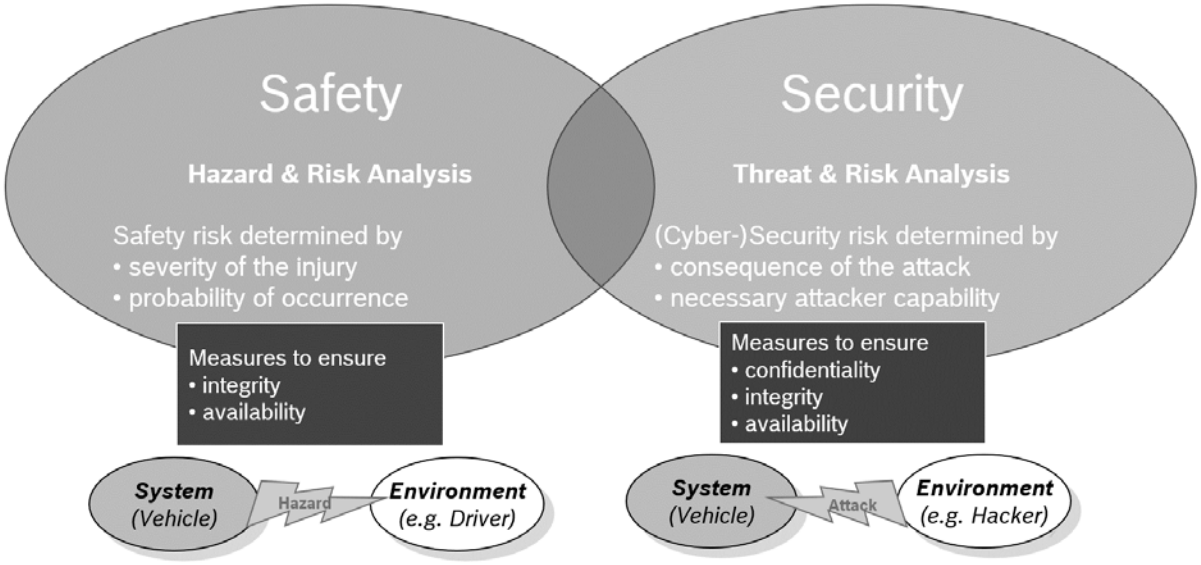

Bild 3: Prinzipielle Vorgehensweisen bei Safety und Security

Cybersecurity setzt als typische Gegenmaßnahme oft Kryptographie ein, dies scheint hier im Falle der „Environmental Hacks“ allerdings untauglich zu sein: Mit kryptographischen Maßnahmen wird der Weg vom Input zum Output einer digitalen Funktion verschlüsselt bzw. authentifiziert. Die Manipulation bei den „Environmental Hacks“ finden aber schon im Vorfeld (vor dem Input) statt, daher ist diese Absicherungsmaßnahme untauglich. In einem einzelnen Eingangskanal kann nicht beurteilt werden, ob der Input valide ist oder nicht.

Somit lässt sich schlussfolgern, dass die „Environmental Hacks“ weder von der Safety-Analyse erfasst werden, weil sie nicht dem typischen Fehlerbild entsprechen, noch von der Security-Analyse erfasst werden, da dort der Blickwinkel meist nur das digitale System selbst und nicht auch dessen Umgebung ist.

Typische Safety-Maßnahmen wie zum Beispiel Redundanz, Diversität und Plausibilisierungen könnten zwar durchaus erfolgsversprechen sein, allerdings kommen sie dort nicht zum Einsatz, wenn sie in der Safety-Analyse nicht als solche abgeleitet werden.

Ansatz für den Entwicklungsprozess

Bei näherer Betrachtung der Anforderungen an den Entwicklungsprozess stellt man viele Ähnlichkeiten der Safety- und Security-Aktivitäten fest [8]:

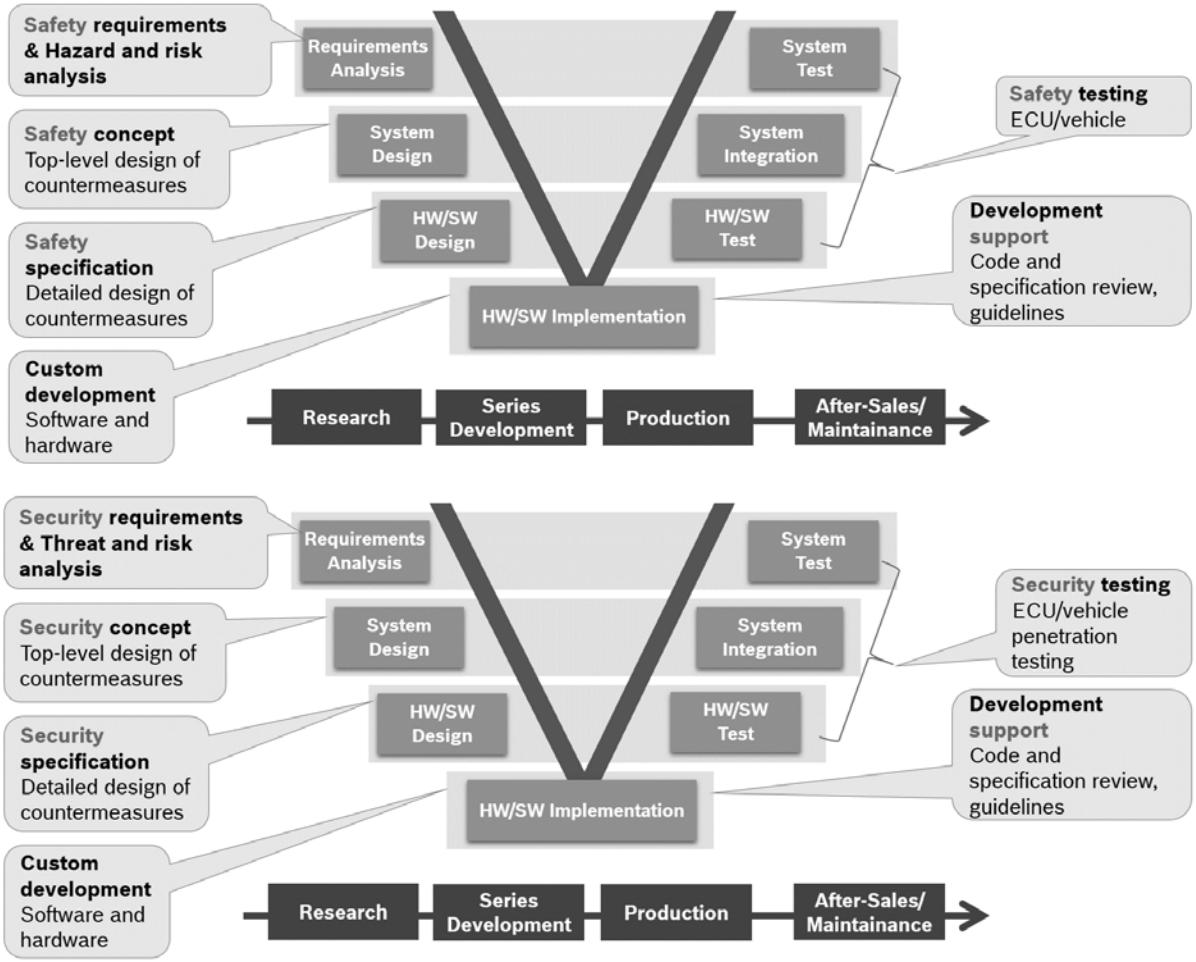

Bild 4: Ähnlichkeiten der Safety- und Security-Prozesse

Bezüglich der „Environmental Hacks“ fällt man jedoch sowohl bei bloßer Anwendung des Safety- als auch des Security-Prozesses durch das Raster, da keiner von beiden dieses Feindbild ausreichend adressiert. Somit führt uns dies zu einem erweiterten prozessualen Lösungsansatz:

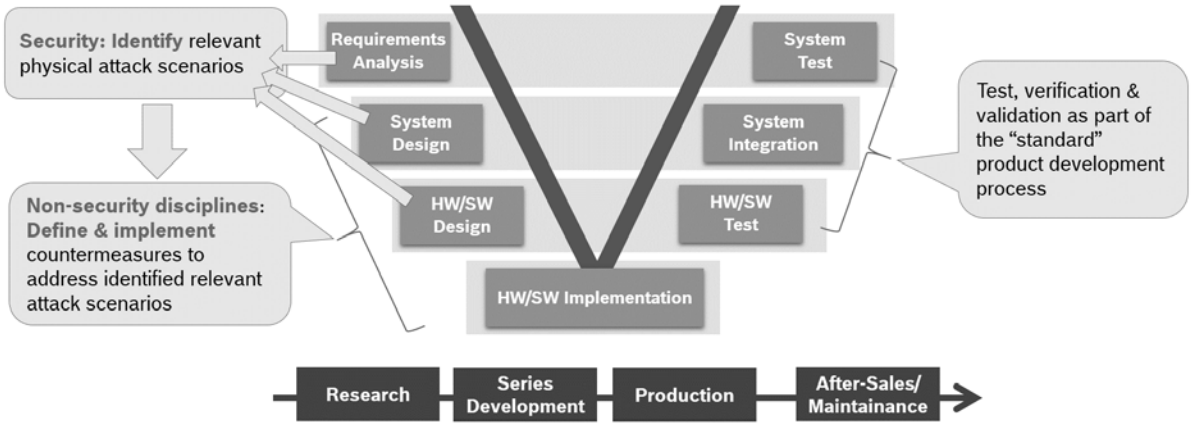

Bild 5: Prozessualer Ansatz zur Behandlung von „Environmental Hacks“

1. Erweiterung des Scopes (TOE = Target of Evaluation [9]) der Risiko- und Bedrohungsanalyse um die potenziellen Einflüsse von „Environmental Hacks“. Dies fällt üblicherweise in den Aufgabenbereich der Security-Domäne.

2. Die Durchführung der anschließenden Analyse führt zu weiteren Top-level Anforderungen (Security Goals).

3. Übergabe der Anforderungen an die jeweils passende Safety-Zieldomäne. Manipulationen an der Umwelt werden oftmals erst dann für das Fahrzeugverhalten relevant, wenn sie über die Sensorik Eingang in die Algorithmik des Fahrzeugs finden. Somit ist zu erwarten, dass üblicherweise eine Übergabe an die SOTIF-Domäne (Safety of the Intended Functionality) erfolgt, es können aber auch andere Domänen wie z.B. Functional Safety betroffen sein.

4. Danach erfolgt dort die Umsetzung mit jeweils vorhandenen Maßnahmen.

5. Test, Verifikation und Validierung erfolgen auf Gesamtsystemebene grundsätzlich gemäß der Vorgaben der Security-Domäne.

Bei der Übergabe von Anforderungen an die Domäne der Funktionalen Sicherheit gilt zu beachten, dass zur Bewertung des Safety-Risikos nicht der ASIL gemäß ISO 26262 herangezogen werden kann, da dieser implizit eine statistische Unabhängigkeit zwischen Fehlerauftreten und Fahrsituation voraussetzt [11], was bei einem „Environmental Hack“ nicht unbedingt gegeben ist. Zur Bewertung des Safety-Risikos einer Manipulation von außen ist daher ein anderes Kriterium notwendig, was momentan Gegenstand der Diskussion in den Safety- und Security-Communities ist [10].

Beispielhafte Umsetzung

a) Verkehrsschilder

Die ursprüngliche Form der Fragestellung zur Erkennung von Verkehrsschilder, auch wenn diese Modifizierungen aufweisen, ist in der Produktentwicklung bereits adressiert. Auch ohne bewusste Manipulation kann heute nicht davon ausgegangen werden, dass z.B. ein Stoppschild nur in Reinform auftritt und sich ohne jegliche Abweichung zu einem Referenzschild in der realen Umgebung befindet. Es muss stattdessen davon ausgegangen werden, dass zum Beispiel das Schild im Winter von Schneeflocken bedeckt oder durch Verschmutzung nur eingeschränkt erkennbar sein könnte. Weiter kann erwartet werden, dass ein System im assistierten oder automatisierten Fahren bei geringfügigen Modifizierungen immer noch in der Lage ist, das Schild als solches zu erkennen und korrekt zu klassifizieren. Lösungsansätze für dieses Problemfeld werden in der SOTIF-Domäne erarbeitet. Die Erweiterung des Fokus von Schneeflocken und Schmutzpartikeln hin zu Klebestreifen oder Abdeckungen erwirkt die Erweiterung dieses Themas um bewusste Umweltmanipulationen und identifiziert somit die SOTIF als die Zieldomäne für die Environmental Hacks.

Witterungsbedingte Abweichungen werden in der Bilderkennung berücksichtigt und sind schon jetzt Bestandteil der Anlernphase eines „Deep Neural Networks“. Ein Ansatz zur Erweiterung der Problemlösung um „Environmental Hacks“ ist, auch solche manipulierten

Objekte gezielt in das Deep Learning einzubringen, um so die Algorithmen diesbezüglich zu sensibilisieren und die Robustheit zu verbessern.

Es sind aber auch Gegenmaßnahmen, die bereits im SOTIF-Umfeld zur Anwendung kommen, für diese Angriffsklasse adaptierbar: So sind zusätzliche Validierungsmaßnahmen über den Kontext eine vielversprechende Gegenmaßnahme. Es wäre beispielsweise nicht plausibel, wenn ein Stoppschild an einem kreuzungslosen Feldweg im Wald aufgestellt wäre, oder ein Tempo-60 Schild direkt an einer Verkehrskreuzung erscheinen würde.

Eine weitere wirkungsvolle Gegenmaßnahme, die ebenfalls im SOTIF-Kontext ihre Anwendung findet, wäre beispielsweise die Etablierung einer zusätzlichen Infrastruktur (Verkehrsschilder senden diversitäre Sensorsignale aus) oder ein Abgleich der erfassten Verkehrsschilder mit Karteninformationen.

b) Laser-Pointer

Die Safety-Relevanz einer Blendung durch Laser-Pointer ist zum Beispiel aus der Luftfahrt hinlänglich bekannt und wird auch entsprechend geahndet ([5]). Hierbei stand bisher insbesondere die Blendung von Personen im Fokus. Vorstellbar ist jedoch auch eine Blendung von Sensoren, so dass diese bei der Erfassung der Fahrzeugumgebung eingeschränkt sind.

Prinzipiell sollte dieses Fehlerbild in einer ähnlichen Art und Weise bereits im SOTIF-Umfeld betrachtet werden, da auch natürliche Quellen für Blendungen vorstellbar sind, zum Beispiel eine tiefstehende Sonnenscheibe. Auch dies darf nicht zu einem ungewünschten, safety-kritischen Verhalten des Fahrzeugs führen. Daher bietet sich an, die Fragestellung einer Blendung durch Laser-Pointer an die SOTIF-Domäne zu geben, da dort Maßnahmen zur generellen Vermeidung bzw. Beherrschung dieses Fehlerbildes erwartet werden können, wenn man die dort getroffenen Betrachtungen auf die Frequenzbereiche der Laser-Pointer erweitert.

Als Lösungsmöglichkeiten sind beispielsweise redundante Sensorik, das Aufrechterhalten einer Mindestfunktionalität oder die Übergabe der Fahraufgabe an den Fahrer vorstellbar.

c) GPS Spoofing

Auf technischer Ebene sind Maßnahmen gegen die Auswirkungen von GNSS-Jamming und -Spoofing verfügbar. Auf Fahrzeugebene hat GNSS-Jamming eine ähnliche Wirkung wie der Ausfall des GNSS-Sensors. Szenario dieser Art sind Teil der Safety-Betrachtung und können durch Safety-Maßnahmen abgemildert werden, wie z.B. das Ausweichen auf einen redundanten Kanal zur Positionsbestimmung oder die Degradierung des Fahrzeugs in einen Zustand, der keine GNSS-Daten benötigt.

Die Auswirkungen von GNSS-Spoofing sind schwerer abzuwenden, da der GNSS-Sensor gefälschte GNSS-Daten nicht von echten unterscheiden kann. Es gibt jedoch Maßnahmen, mit denen das System „merken“ kann, dass eine Unregelmäßigkeit vorliegt. Ein plötzlicher Versatz in den empfangenen Positionsdaten um eine größere Distanz kann mittels kontinuierlicher Plausibilitätsprüfung der empfangenen Positionsdaten bemerkt werden. Ein schleichender Versatz fällt beim Abgleich mit redundanten Positionsdaten, z.B. Kartendaten, auf.

Auf Prozessebene ist es dagegen schwierig, GNSS-Jamming und -Spoofing einzuordnen. Es ist weder Gegenstand der Functional Safety, da keine systematischen Fehler oder zufälligen Hardwarefehler ursächlich sind. Noch sind derartige Angriffe ein Thema für SOTIF, weil sie nicht auf Unzulänglichkeiten der Sensorik an sich basieren. Aktuell wird die Behandlung von GNSS-Jamming und -Spoofing nicht vollständig von der Security abgedeckt, da im Rahmen der Risiko- und Bedrohungsanalyse nur (absichtliche) Angriffe auf das Fahrzeug oder einzelne Komponenten betrachtet werden. Der Kollateralschaden, der durch GNSS-Jamming oder –Spoofing mit anderer Zielsetzung entstehen kann, bleibt außen vor. Es muss daher eine Zieldomäne identifiziert werden, die ggf. ihren Betrachtungsumfang und möglicherweise ihre Methoden erweitern muss, um derartige Angriffe zu analysieren und geeignete Gegenmaßnahmen abzuleiten.

Zusammenfassung

„Environmental Hacks“ können signifikanten Einfluss auf das Fahrzeugverhalten und seine Sicherheit (sowohl i.S.v. Safety als auch Security) haben. Dies ist durch die bisherigen Disziplinen (Bild 1) nicht vollständig adressiert, da es sich um eine domänenübergreifende Fragestellung handelt. Die Identifikation der betroffenen Fehlerbilder kann im Rahmen einer Security-Betrachtung erfolgen, danach erfolgt die Übergabe an die jeweils betroffenen Safety-Zieldomänen. Hierzu sollte die bestehende Risiko- und Bedrohungsanalyse der Security entsprechend um die „Environmental Hacks“ erweitert werden. Als Zieldomäne für die Safety-Betrachtung wird sich oftmals die SOTIF (Safety of the Intended Functionality) anbieten, da hier die größten Synergien zu erwarten sind, es sind aber auch andere Safety-Zieldomänen denkbar.

Referenzen

[1] https://upload.wikimedia.org/wikipedia/commons/4/41/Stop_eating_animals_sign.jpg

[2] Autonome Autos: Unsaubere Verkehrszeichen komplett falsch erkannt, www.winfuture.de/news,99034.html (abgerufen am 24.07.2018)

[3] Robust Physical-World Attacks on Deep Learning Models, https://arxiv.org/abs/1707.08945 (abgerufen am 30.07.2018)

[4] https://www.youtube.com/watch?time_continue=2&v=1mJMPqi2bSQ (abgerufen am 30.07.2018)

[5] Haftstrafe für Laser-Blendung, https://www.aerokurier.de/general-aviation/haftstrafe-fuer-laser-blendung-in-berlin/738030 (abgerufen am 27.09.2018)

[6] Anschlag mit Laserpointer: Busfahrer am Auge verletzt http://www.ln-online.de/Lokales/Luebeck/Anschlag-mit-Laserpointer-Busfahrer-am-Auge-verletzt (abgerufen am 24.07.2018)

[7] Black Hat Europe: It’s easy and costs only $60 to hack self-driving car sensors, https://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html (abgerufen am 24.07.2018)

[8] Security im Kontext der Funktionssicherheit: Wie Safety und Security zusammenhängen, Embedded Software Engineering Kongress 2015, Sindelfingen

[9] ISO/IEC 15408: “The Common Criteria for Information Technology Security Evaluation“

[10] Benjamin Glas, Carsten Gebauer, Jochen Hänger, Andreas Heyl, Jürgen Klarmann, Stefan Kriso, Priyamvadha Vembar, Philipp Wörz: „Automotive Safety and Security Integration Challenges“, Automotive Safety and Security 2015, Stuttgart-Feuerbach

[11] Stefan Kriso, Markus Ihle: “Automotive Security im Kontext der Funktionalen Sicherheit“, Forum Safety & Security, München, 06.–07. Juli 2016

[12] GPS unter Beschuss: Jamming und Spoofing nehmen zu https://www.heise.de/newsticker/meldung/GPS-unter-Beschuss-Jamming-und-Spoofing-nehmen-zu-4038137.html (abgerufen am 27.09.2018)

[13] Truck driver has GPS jammer, accidentally jams Newark airport, https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/ (abgerufen am 27.09.2018)

[14] We Declare The Grandmaster Of Pokemon Go GPS Cheats https://hackaday.com/tag/gps-spoofing/ (abgerufen am 27.09.2018)

Autoren

Dipl.-Phys. Stefan Kriso trat nach dem Studium der Physik 1995 in die Robert Bosch GmbH ein. In verschiedenen Positionen beschäftigte er sich mit Fragestellungen der Hard- und Softwareentwicklung. Von 2005 bis 2011 leitete er in der zentralen Forschung und Vorausentwicklung ein Projekt, das einerseits die Bosch-Interessenvertretung in den nationalen und internationalen Normungsgremien zur ISO 26262, andererseits die Koordination der konzernweiten Einführung der ISO 26262 zur Aufgabe hatte. Seit 2011 leitet er bei Bosch das „Center of Competence Functional Safety“. Seit 2005 ist er nebenberuflich Dozent für Physik an der Dualen Hochschule Baden Württemberg, Stuttgart.

Kontakt: stefan.kriso@de.bosch.com

Dr. Jürgen Klarmann studierte Informatik an der Universität Stuttgart und schloss sein Studium 1995 mit dem Diplom ab. Von 1995 bis 2002 war er als Wissenschaftlicher Angestellter an der Universität Stuttgart tätig, an der er auch zum Dr. rer. nat. promovierte. Seit 2002 arbeitet er in der Robert Bosch GmbH in unterschiedlichen Funktionen im Unternehmensbereich Mobility Solutions. Seit 2008 ist er verstärkt in die Functional Safety und die ISO 26262 involviert. Von 2013 bis 2015 war in der der ETAS GmbH als Senior Consultant für Safety, Security und Embedded Systems tätig. Seit 2016 arbeitet er im Geschäftsbereich Chassis Systems Controls im dortigen „CC Center of Competence Security“.

Kontakt: juergen.klarmann@de.bosch.com

Dr. Claudia Loderhose ist Diplom-Mathematikerin und promovierte Informatikerin. Seit 2017 arbeitet sie bei der Robert Bosch GmbH im Geschäftsbereich Chassis Systems Controls. Ihre Themenschwerpunkte sind Methoden zur Risiko- und Bedrohungsanalyse, die Einbindung von Securityaspekten in den Produktentwicklungsprozess sowie das Zusammenspiel zwischen Safety und Security.

Kontakt: claudia.loderhose@de.bosch.com

Franziska Wiemer hat an der Ruhr-Universität Bochum IT-Sicherheit und Informationssicherheit (B.Sc und M.Sc) studiert und ist 2017 in die Robert Bosch GmbH eingetreten. Seitdem beschäftigt sie sich mit Themen der IT-Sicherheit (Security) innerhalb von Fahrzeugen. Sie arbeitet unteranderem an der Entwicklung von Prozessen zur Integration von Security in Steuergeräten – dabei spielt aktuell auch das Zusammenspiel zwischen Safety und Security eine große Rolle. Ein weiterer Schwerpunkt ihrer Arbeit ist der Datenschutz innerhalb von Chassis-Steuergeräten, sowohl während der Entwicklung, als auch bei Datenrückfluss im späteren Serienbetrieb.

Kontakt: franziska.wiemer@de.bosch.com

Dipl.-Phys. Carsten Gebauer trat 2000 nach Abschluss seines Studiums der Bosch Gruppe bei. Sein Themenschwerpunkt ist seit 2004 die Safety. Er ist Mitglied der nationalen und internationalen Arbeitsgruppen, die mit der Erstellung der ISO 26262 und der ISO (PAS) 21448 beauftragt sind und arbeitet seit 2014 im „Bosch Center of Competence Functional Safety“.

Kontakt: carsten.gebauer@de.bosch.com

Dr. Simon Burton studierte Informatik an der Universtiy of York, an welcher er auch zum Thema Verifikation und Validierung von sicherheitsrelevanten Systemen promovierte. Dr. Burton ist seit über 20 Jahren in verschiedenen sicherheitsrelevanten Industrien tätig gewesen. Er hat unter anderem Forschungs- und Entwicklungsprojekte bei großen OEMs sowie auch Beratungs-, Dienstleistungs- und Produktorganisationen geleitet. Zurzeit hat er die Rolle des Chief Experts bei Robert Bosch GmbH inne, in welcher er die Forschungs-strategie in den Bereichen funktionale Sicherheit, Security, Zuverlässigkeit und Verfügbarkeit von Software-intensiven Systemen koordiniert.

Kontakt: simon.burton@de.bosch.com

Markus Ihle studierte an der Universität Karlsruhe Elektrotechnik und schloss 1999 mit dem Diplom ab. Seit 2003 ist er in verschiedenen Bereichen und Funktionen des Bosch-Konzerns tätig. Er war unter anderem an der Forschung und Entwicklung von Halbleiterbauelementen sowie Software für eingebettete Produkte, z.B. für fahrzeuginterne Kommunikation (CAN, FlexRay) und Securitymodulen für erhöhten Manipulationsschutz von Microcontrollern („HSM“) beteiligt. Seit 2013 leitet er das konzernweite „Bosch Center of Competence Security“ bei ETAS.

Kontakt: markus.ihle@etas.com