Sicherheit ist funktional, mechanisch, elektrisch und chemisch

Der Product Safety Risk Graph ermöglicht Produktsicherheit

Gerade in der Autoindustrie hat das Thema Produktsicherheit an Bedeutung gewonnen. Die Rufe aus dem Markt werden immer lauter und die Forderungen etwa aus dem VDA-Rotband zur Produktintegrität immer konkreter. Für den Automotive-Zulieferer Hella war es an der Zeit, ein eigenes Konzept für Product Safety zu entwickeln.

Aktuelle Fahrzeugsysteme zeichnen sich durch ein komplexes Zusammenspiel verschiedener Technologien aus, das völlig neue Funktionalitäten ermöglicht. So wird beispielsweise in einem Gaspedal eine mechanische Bewegung genutzt, um ein elektrisches Signal zu erzeugen, das wiederum durch Software ausgewertet wird. Diese Kombinationen verschiedener Technologien zeichnet heutige Fahrzeugkomponenten aus. Gleichzeitig geht dieses Zusammenspiel der Technologien mit neuen Herausforderungen in Sachen Produktsicherheit einher. Mit den unterschiedlichen Technologien sind verschiedene Sicherheitsrisiken verbunden, von der funktionalen Sicherheit über die chemische, elektrische bis zur mechanischen Sicherheit. Während sich die funktionale Sicherheit mit Fehlern einer Fahrzeugfunktion beschäftigt, etwa dem Versagen der Bremse, betrachten die mechanische, die elektrische und die chemische Sicherheit Aspekte, die sich aus dem physikalischen Einfluss eines Geräts auf den Menschen ergeben. Beispielsweise sind Aspekte wie Brennbarkeit, elektrischer Schlag und auch Gefahren durch giftige Substanzen zu betrachten.

Die Forderung nach einem sicheren Produkt setzt voraus, dass alle möglichen Gefahren für Leib und Leben berücksichtigt werden, und damit all diese Aspekte und auch deren Wechselspiel. So können sich die einzelnen Safety-Aspekte gegenseitig ergänzen aber auch gegenseitig einschrän-

ken. In einem Batteriesystem beispielsweise sind Themen wie die Batteriesäure, elektrische Ströme und Spannungen sowie mögliche Eigenerwärmungen zu betrachten. Hier ergänzen sich Maßnahmen, die auf Grund der hohen Ströme ergriffen werden und ein für mechanische Sicherheit gefordertes Kühlsystem gegenseitig. Gleichzeitig schränken sich die Sicherheitsaspekte auch gegenseitig ein. Dies ist beispielsweise der Fall, wenn das aus mechanischer Sicht gewählte Kühlmittel unter Berücksichtigung der Aspekte der chemischen Sicherheit durch ein anderes ersetzt werden muss.

Bei der Erstellung eines Safety-Konzepts ist es daher unabdingbar, alle Safety-Anforderungen zu berücksichtigen und so ein in sich schlüssiges, vollständiges Konzept zu erarbeiten. Doch woher kommen diese Anforderungen und wie entsteht das Safety-Konzept?

Produktsicherheit muss sich messen lassen

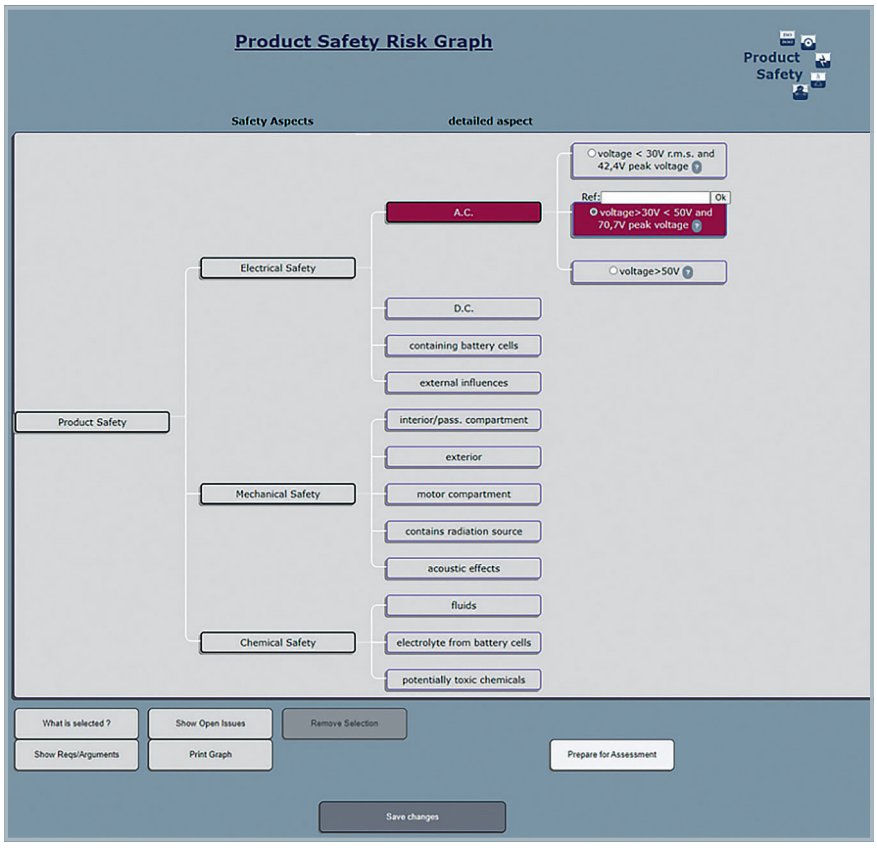
Aus der funktionalen Sicherheit gemäß ISO 26262 ist das Hazard Analysis and Risk Assessment H&R bekannt, bei dem Fahrfunktionen auf Fahrzeugebene bezüglich möglicher Risiken bewertet und Safety Goals abgeleitet werden. Bei der chemischen, elektrischen und mechanischen Sicherheit greift dieses Konzept nicht. Bei diesen Aspekten werden keine Fahrfunktionen betrachtet, sondern vielmehr der physikalische Einfluss, den zum Beispiel ein Sensor auf den Menschen haben kann. So etwa ein elektrischer Schlag bei Berührung des Sensors, Verätzungen durch freigesetzte Chemikalien oder Verbrennungen durch hohe Temperaturen. Für diese Aspekte gibt es keine Vorgaben von den Fahrzeugherstellern, und dennoch sind die Zulieferer verpflichtet ein sicheres Produkt zu liefern und State-of-The-Art sicherzustellen.

Um der Forderung nach Produktsicherheit gerecht zu werden und den aktuellen Trends der Automobilindustrie nachzukommen, muss das Entwicklungsmodell um die Themen chemische, elektrische und mechanische Sicherheit erweitert werden. Um effektiv und vor allem effizient an die Anforderungen zur Produktsicherheit zu gelangen, hat Hella den *Product Safety Risk Graph* entwickelt, der eine umfängliche Analyse der Safety-Aspekte in der Entwicklung gewährleistet.

Entwicklung des Product Safety Risk Graph

Dabei ergaben sich verschiedene Herausforderungen. So müssen die Anforderungen bereits in einem frühen Stadium der Entwicklung bekannt und ein ganzheitliches Bild der Sicherheitsanforderungen erreicht sein, um rechtzeitig Einfluss auf Desig- »»

»»

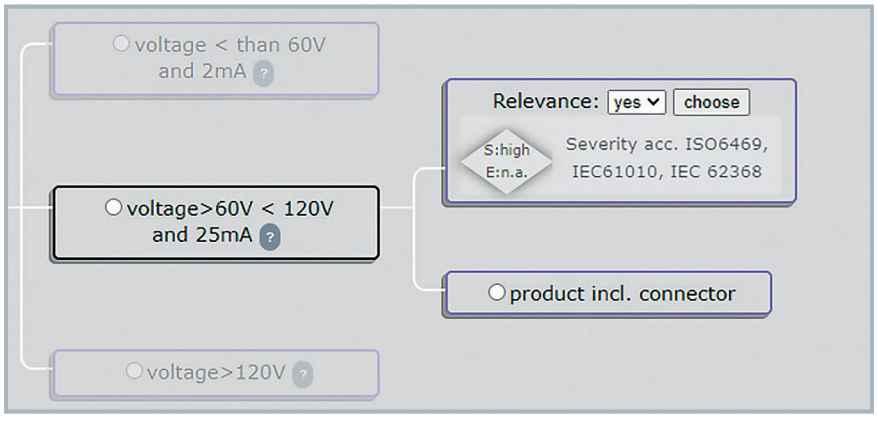


Der Product Safety Risk Graph umfasst alle Merkmale die potenzielle Risiken darstellen.

Quelle: Hella ©Hanser

nentscheidungen nehmen zu können. Auch das Produktportfolio von Hella spielt hier eine entscheidende Rolle. So muss die Methodik auf einfache, rein mechanische Produkte genauso anwendbar sein, wie auf Produkte mit einem komplexen Wechselspiel der Technologien.

Die Basis dieser Analyse bilden Normen und Standards zur chemischen, elektrischen und mechanischen Sicherheit. Normen und Standards bieten hier zwar allgemeine Richtlinien, allerdings obliegt es den Herstellern selbst diese Aspekte für ihr Produkt zu analysieren und umsetzbare Anforderungen daraus abzuleiten. Als Kriterien sind hier die *Schadensschwere* sowie die *Eintrittswahrscheinlichkeit* gewählt worden, um den verschiedenen Produkten und Einbausituationen Rechnung zu tragen. Beispielsweise ergeben sich je nach Spannung und Einsatzort verschiedene Maßnahmen zum Schutz vor elektrischem Schlag. Bei geringen Spannungen ergeben sich keine besonderen Maßnahmen. Bei höheren Spannungen reichen die Maßnahmen von einem Gehäuse bis hin zu einer separaten Isolationsmessung. Um das richtige Maß zu finden sind Kriterien wie Schadensschwere und Eintrittswahrscheinlichkeit unabdingbar.



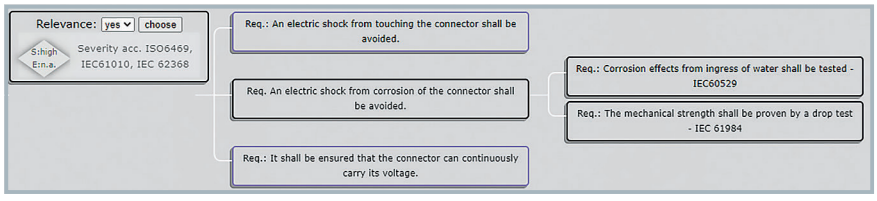
Schadensschwere und Auftretenswahrscheinlichkeit werden bewertet. Quelle: Hella © Hanser

Auf die *Kontrollierbarkeit* als zusätzliches Kriterium wurde bewusst verzichtet, da Fehler im Bereich der chemischen, mechanischen und elektrischen Sicherheit meist erst erkannt werden, wenn der Schaden bereits eingetreten ist und somit nicht kontrollierbar sind. Beispielsweise wird ein elektrischer Schlag nur erkannt, wenn dieser bereits eingetreten ist.

Für die Analyse wurde eine Baumstruktur gewählt, um trotz der großen Zahl an Normen und Standards die Übersicht nicht zu verlieren. Auf diese Weise ist der Graph für alle Produkte nutzbar und ermöglicht es, einfach und schnell detaillierte Anforderungen für das Produkt abzuleiten. Für jedes Produkt wird der Graph von links nach rechts durchlaufen und jeweils der zutreffende Zweig weiterverfolgt. So wird für ein einfaches Produkt nur ein kleiner Teil des Graphen durchlaufen, während in einem komplexen Produkt deutlich mehr Zweige weiterfolgt werden. Relevante Aspekte werden markiert und mit Referenzen hinterlegt um die *Traceability* sicherzustellen und gleichzeitig die Vollständigkeit der Analyse zu belegen.

Jeder Aspekt des Graphen ist bezüglich Schadensschwere und Eintrittswahrscheinlichkeit bewertet, wobei sich diese Bewertungen aus Normen und Standards ergeben und entsprechend verlinkt sind. Indem diese Kriterien zentral bewertet wurden, ist sichergestellt, dass gleichartige Produkte auch zu gleichen Anforderungen führen, unabhängig davon wo und von wem die Analyse durchgeführt wird. Dies trägt dem Einsatz in einem internationalen Konzern Rechnung. Gleichzeitig wird dem Projektteam die Analyse erleichtert und verhindert, dass jedes Projektteam für sich erneut die jeweilige Norm interpretieren muss.

Für jeden Aspekt sind die entsprechenden Anforderungen aus den Normen extrahiert und im Graphen hinterlegt. Auf der ersten Ebene finden sich dabei Anforderungen auf Systemebene die zusammengenommen das Product Safety Konzept ergeben. Aus diesen ergeben sich auf den folgenden Ebenen die Anforderungen zur Umsetzung auf Hardware-, Software-Ebene, sowie Anforderungen zu Verifikation und Validierung. Ebenso ergeben sich aus



Die Anforderungen aus den Normen sind extrahiert und im Graphen hinterlegt. Quelle: Hella © Hanser

dem Graphen Anforderungen, die an Produktion und Logistik gerichtet sind.

Vollständiges Bild der Sicherheitsanforderungen

Sobald der Graph vollständig ausgefüllt ist, werden die Anforderungen sowie deren Verlinkung untereinander exportiert und in die Spezifikation übernommen. Auf diese Weise ergibt sich ein vollständiges Bild der Sicherheitsanforderungen und notwendigen Maßnahmen.

Der Product Safety Risk Graph bietet zudem die Möglichkeit einen Aspekt als *nicht relevant* zu kennzeichnen, jedoch nur wenn eine entsprechende Argumentation bereitgestellt wird. Diese Argumentation kann zum Beispiel eine Maßnahme sein, die das übergeordnete System bereitstellt. Eine solche Argumentation muss entsprechend abgestimmt und belegt sein.

Integration in das V-Modell bringt zusätzlich Sicherheit

Um die Aspekte der *chemischen, elektrischen und mechanischen Sicherheit* effektiv umzusetzen und somit der Forderung der Produktsicherheit gerecht zu werden, bedarf es also einer Erweiterung des altbewährten V-Models.

Auf der einen Seite ergeben sich die Anforderungen der *funktionalen Sicherheit* die vom Fahrzeughersteller in der H&R abgeleitet werden und somit Input für das Safety-Konzept sind. Auf der anderen Seite stehen die Anforderungen der chemischen, elektrischen und mechanischen Sicherheit. Diese werden wie beschrieben mit Hilfe des Product Safety Risk Graph abgeleitet und fließen zusammen mit den funktionalen Sicherheitsanforderungen in das Safety-Konzept ein. Die Verantwortung für diesen Schritt liegt in Händen des Zulieferers, der sein Produkt bewertet. Die so abgeleiteten Anforderungen adressieren sowohl die Umsetzung in der Entwicklung als auch die Testebene, wirken sich aber auch direkt auf Produktion und Logistik aus. Damit ergibt sich ein direkter Pfad in die Produktion und Logistik, um den das V-Model erweitert wurde, sodass es nun die Form des griechischen Buchstaben *Psi* annimmt.

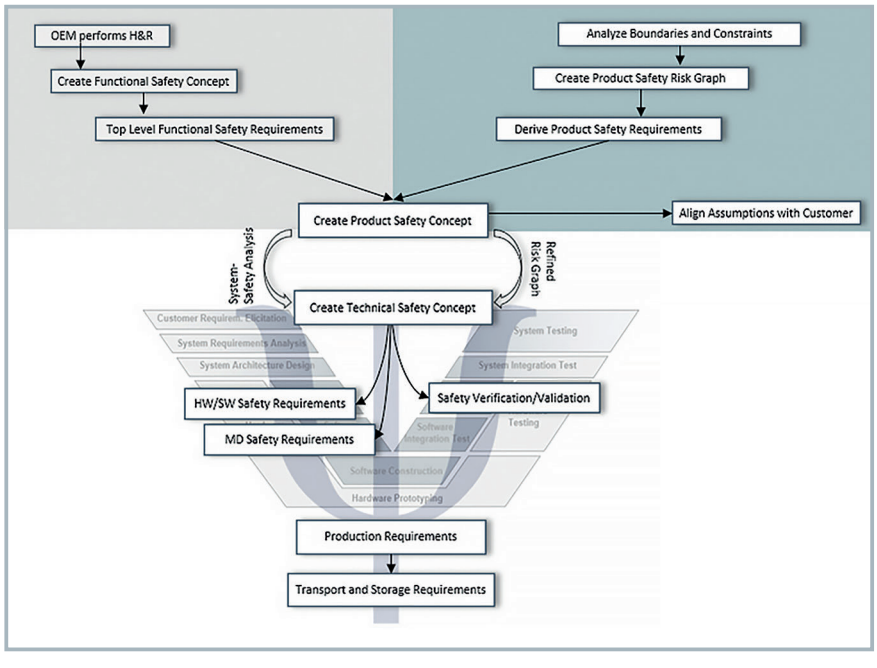
Um sicherzustellen, dass die während der Analyse getroffenen Annahmen hinsichtlich des übergeordneten Systems zutreffen, ist eine Abstimmung des Konzepts mit dem Kunden unabdingbar.

Das somit erweiterte V-Modell in Kombination mit dem Product Safety Risk Graph ermöglicht es, die Forderungen nach einem sicheren Produkt gemäß State-of-the-Art zu garantieren und dabei praktikabel zu bleiben.

Normen und Standards bleiben die Basis

Der Product Safety Risk Graph steht und fällt mit den angewandten Regelwerken. Bei Hella umfasst der Graph mehr als 150 Normen und Standards aus diversen Bereichen. Mit der Zahl der verwendeten Normen steigt auch der Aufwand zur Erstellung des Graphen, aber eben auch die möglichen Anwendungsbereiche. Bei Verwendung des Graphen werden die Normen allerdings einmal zentral interpretiert und nicht in jedem Projekt von neuem, sodass der Graph den Aufwand für das Unternehmen erheblich reduziert.

Während sich das V-Model auf Entwicklung und Produktion bezieht, kann der Risk Graph ebenso zur Bewertung von Rückläufern genutzt werden. Dies stellt sicher, dass Fehler auf gleiche Weise bewertet werden, egal ob diese während der Entwicklung oder im Zuge eines Vorfalls betrachtet werden, und ermöglicht es Erkenntnisse aus dem Feld in den Graphen und damit zur Entwicklung zurückfließen zu lassen. ■



Erweiterung des V-Modells garantiert die Umsetzung aller Sicherheitsaspekte. Quelle: Hella © Hanser

INFORMATION & SERVICE

AUTOREN

Dr. rer. nat. Simone Hamerla ist Leiterin des Bereichs Product Safety Incidents & Product Conformity bei Hella. Sie verantwortet Aufbau und Implementierung von Produktsicherheit in Prozess und Projekt.

Dipl.-Ing. Nastaran Fiegler arbeitet im Bereich Produktsicherheit von Hella. Er ist spezialisiert auf reaktive und proaktive Marktbeobachtung.

KONTAKT

simone.hamerla@forvia.com