Fachbeitrag

HIMA – 50 Jahre Safety-Zertifizierung

(Brühl, November 2020)

1970 hat die HIMA Paul Hildebrandt GmbH die weltweit erste TÜV-zertifizierte Sicherheitssteuerung auf den Markt gebracht. Das Safety-Unternehmen und der TÜV Rheinland arbeiten also bereits seit 50 Jahren hervorragend zusammen – sowohl in Gremien auf dialogischer Basis als auch bei der Zertifizierung von Sicherheitssteuerungen. HIMA ist gemeinsam mit dem TÜV Rheinland auch entscheidend als Normentreiber aktiv, wenn es um die Bereiche Safety und Security geht. Die zentralen Herausforderungen für die Zukunft sind hierbei Cyber Security und die technologische Entwicklung. Blickt man auf die vergangenen 50 Jahre zurück, so stellt sich die Frage: Wie haben sich die Herausforderungen im Laufe der Zeit geändert? Was musste damals bzw. heute beachtet werden? Die Experten des TÜV Rheinland und HIMA berichten eindrucksvoll von ihrer langjährigen Zusammenarbeit.

Die Funktionale Sicherheit hat in Deutschland einen hohen Stand – und das ist kein Zufall. HIMA und TÜV Rheinland haben durch ihre Zusammenarbeit dabei einen wertvollen Beitrag geleistet. Die Systeme der Funktionalen Sicherheit schützen in der Prozessindustrie – und praktisch jeder industriellen Umgebung auch – Menschen, Anlagen und die Umwelt. Sicherheitsteuerungen fahren beispielsweise Anlagen in einen sicheren Zustand, wenn plötzlich gefährliche Situationen auftreten. Dies ist besonders wichtig, wenn Menschen nicht schnell genug reagieren können oder andere Sicherheitsvorkehrungen nicht funktionieren. Die Funktionale Sicherheit soll verhindern, dass es zu Unfällen oder unerwünschten, kostspieligen Anlagenstillständen kommt. Schließlich steht eine Menge auf dem Spiel: die Gesundheit der Mitarbeiter, die Sachwerte des Unternehmens und die Umwelt.

Die Funktionale Sicherheit ist in Deutschland auf einem sehr hohen Niveau angesiedelt und „gilt auch international als vorbildlich“, meint Merlin Hilger vom TÜV Rheinland. Der normgerechte Schutz von Menschen, Umwelt und Anlagen stehe bei deutschen

Unternehmen im Vordergrund. Seit rund 20 Jahren gibt es nun die Basisnorm für sicherheitstechnische Systeme IEC 61508, die branchenübergreifend für alle sicherheitsgerichteten Systeme (elektrische, elektronische und programmierbare elektronische Geräte) gilt – egal, ob in der Prozessindustrie, Feuerungs-, Marine- oder Bahntechnik. „Sie gibt ein sehr hohes Maß an Sicherheit vor“, sagt Hilger. Mit den letzten Änderungen dieser Grundnorm vor 10 Jahren wurde dies nochmal gesteigert. Boris Betz von HIMA pflichtet dem bei: „Wir bewegen uns in Deutschland auf einem sehr hohen Niveau, was die Funktionale Sicherheit betrifft. Allerdings gibt es nach oben kein Limit, und es ist auch eine Herausforderung, normgerechte Produkte lange am Markt zu halten. In der Entwicklung haben wir insgesamt etwa bis zu 150 Normen zu beachten.“

Das führe laut Hilger auch dazu, dass man sich hierzulande auf die Sicherheit an seinem Arbeitsplatz verlassen könne. Es ist daher nach Meinung der TÜV-Experten nicht verwunderlich, dass man sich in Ländern mit einem weniger fortschrittlichen Level der Funktionalen Sicherheit dieser Vorteile bewusst wird und diesbezüglich nun merklich nachziehen wird. „Die Wahrnehmung des Risikos ist von zentraler Bedeutung“, führt der ehemalige TÜV-Experte Heinz Gall zudem an. „In Deutschland ist der Aspekt der Personensicherheit natürlich von höchster Priorität.“

TÜV-Experten wie Heinz Gall, Jana Klaes und Merlin Hilger betonen, es habe während ihrer bisherigen Tätigkeit glücklicherweise keine schwerwiegenden Unfälle oder Katastrophen gegeben, die als zusätzliche Treiber der Normierungen in der Funktionalen Sicherheit gewirkt haben. Dass dies auch ganz anders sein kann, zeigte die Katastrophe der Piper Alpha Ölplattform. 1988 kamen bei dem schweren Unglück 167 Menschen ums Leben. In der Folge wurde damals ein Health, Safety and Environment Management System (HSE, Gesundheits-, Sicherheits- und Umwelt-Management-Systeme) entwickelt, um derartige Katastrophen künftig zu verhindern. Dass die Funktionale Sicherheit in Deutschland einen so hohen Stellenwert hat, habe viel mit dem Verantwortungsbewusstsein der Unternehmen zu tun, die über die Sicherheit und den Schutz der Industrieanlagen hinausgeht, meint auch Jana Klaes vom TÜV Rheinland. „Ebenso will niemand in den Schlagzeilen stehen, wenn Menschen oder die Umwelt zu Schaden kommen“, so die TÜV-Expertin.

Die Zusammenarbeit von HIMA und TÜV Rheinland von damals bis heute

Die Zusammenarbeit zwischen HIMA und TÜV Rheinland ist eine durchgängige Erfolgsschichte. Um Prüfungen durchführen zu können, ist der TÜV Rheinland von der deutschen Akkreditierungsstelle akkreditiert. Die Verfahren und Prozesse, die zur

Durchführung von Zertifizierungsprüfungen notwendig sind, sind dabei streng geregelt. „Das betrifft beispielsweise auch die Dokumentation der verschiedenen Prüfschritte, und hier gibt es definitiv mehr Reglementierungen als früher“, sagt Hilger.

Bei HIMA hat es der TÜV Rheinland vor allem mit Änderungsprüfungen zu tun, die bei Weiterentwicklungen und der Produktpflege von bewährten Sicherheitssteuerungen durchgeführt werden. In der Regel gilt: Prüfungen im Rahmen der Produktpflege benötigen deutlich weniger Zeit als Prüfungen bei kompletten Produktneuentwicklungen. Aber auch bei der Prüfung im Rahmen der Produktpflege käme es hinsichtlich des Zeitaufwandes immer auf die Art der Modifikation an, so Hilger.

Boris Betz von HIMA fügt hinzu: „Da HIMAs Sicherheitssteuerungen extrem lange Produktlaufzeiten haben, kommt es im Rahmen der Produktpflege immer wieder zu Modernisierungen und den notwendigen Rezertifizierungen. Dazu müssen dann natürlich alle Unterlagen eingereicht werden.“ Damals habe man das noch in Papierform in überschaubaren Mengen über den Postweg machen können. Heute erfolgt die Datenübermittlung bei HIMA komplett auf digitalem Wege – aber es gibt auch hier deutliche Unterschiede bei der Datenmenge. Bei Rezertifizierungen bestehender HIMA Lösungen kommt man in der Regel mit wenigen Megabyte an Daten zurecht, die an Prüfstellen wie den TÜV Rheinland übermittelt werden müssen. Bei Neuentwicklungen und insbesondere im Softwarebereich sind hingegen die Datenmengen heute extrem hoch. Hier kommen sehr schnell 20 bis 30 Gigabytes an Dokumentationen und Daten zusammen.

Man müsste eigentlich meinen, dass sich Abläufe insgesamt beschleunigen lassen, eben weil es beispielsweise immer bessere Tools oder Prozessoren gäbe. Hilger meint: „Obgleich die Vorstellung, dass bessere Tools weniger Aufwand bedeuten, naheliegt, ist das in der Realität nicht so.“ Grund dafür ist die steigende Komplexität. Sie sorge auch dafür, dass bei neuen Produkten sowohl der Personal-, Koordinations- als auch der Zeitaufwand steigen könne. Früher waren die Teams oft kleiner als heute. „Damals waren an Prüfungen oft nur wenige Personen beteiligt, heute sind es in (Online-)Meetings meist deutlich mehr Spezialisten des Kunden, die hinzugezogen werden müssen“, so Hilger. Der Anteil der Servicefunktionen nehme zu, die nicht vom Hersteller selbst entwickelt, sondern von externen Partnern dazugekauft werden. Auch das erhöhe gegebenenfalls den Prüf- und Personalaufwand.

Prüfungen und Zertifizierungen führt der TÜV Rheinland sowohl bei Produktneuentwicklungen, als auch bei Rezertifizierungen einer schon existierenden Sicherheitssteuerung durch. Durch die mittlerweile seit fünf Jahrzehnten andauernde gute

Geschäftsbeziehung zwischen TÜV Rheinland und HIMA gibt es ein wichtiges Grundvertrauen, was die professionelle Arbeit der Fachleute auf beiden Seiten sehr positiv gestaltet. „Wir wissen durch unsere langjährige Zusammenarbeit, wie bei HIMA gearbeitet wird“, sagt Jana Klaes. Das zeige sich beispielsweise bei der Dokumentenprüfung, die der TÜV Rheinland bei HIMA durchführt. Aufgrund der gewissenhaften und ordentlichen Arbeit bei HIMA werden nahezu keine Abweichungen zur Norm gefunden. Auch Gall erinnert sich an eine hervorragende Zusammenarbeit zwischen HIMA und dem TÜV Rheinland bei den Zertifizierungen in der Vergangenheit.

Bei neuen Produkten arbeitet der TÜV Rheinland bereits in der Konzeptphase mit. Da es bei der Funktionalen Sicherheit darum geht, Fehler zu vermeiden, ist es naheliegend, bereits auf mögliche Fehler einzugehen, die schon gleich zum Anfang in der Produktentwicklung entstehen. Beim TÜV Rheinland wird dies in der Konzeptprüfung abgedeckt, in der dieser dem Hersteller seine Einschätzung hinsichtlich der angewandten Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung mitteilt: Passen die geplanten Sicherheitsmaßnahmen zu dieser Art von Projekt? Im Weiteren hängt es von der Komplexität des Produkts ab, wann der TÜV Rheinland wieder vom Hersteller hinzugezogen wird. Eine Sicherheitssteuerung hat zum Beispiel eine deutlich längere Entwicklungsdauer als ein Sicherheitssensor. Die Zeitdauer einer Gesamtprüfung kann zwischen drei Monaten und mehreren Jahren liegen, wobei die Spezialisten vom TÜV Rheinland ihre Kunden meist vom Start bis zum Ende begleiten. Gegen Ende nimmt dann die „papierbasierte“ Arbeit stark zu: Hier werden zunächst Testberichte, Designspezifikationen und weitere Dokumente analysiert und geprüft, ob Planung und Umsetzung den gültigen Normen entsprechen.

Gemeinsam mit dem Kunden werden danach vom TÜV Rheinland sogenannte Fehlereinpflanzungstest hinsichtlich der Funktionalen Sicherheit durchgeführt, die einige Tage dauern können. Hier geht es darum, die in der Konzeptphase geplanten Maßnahmen zur Fehlerbeherrschung durch absichtlich herbeigeführte Fehler zu testen. Daher sollte beispielsweise eine Sicherheitssteuerung bei den Fehlereinpflanzungstests sicher und normenkonform reagieren.

Boris Betz begleitet auf der Seite von HIMA die Zertifizierungen mit dem TÜV Rheinland seit 2014 und betont die gute entwicklungsbegleitende Zusammenarbeit mit der Prüfstelle: „Man hat auf beiden Seiten ein gutes Gefühl dafür, wann bei einer anstehenden Zertifizierung oder Rezertifizierung der richtige Zeitpunkt ist, die Zusammenarbeit zu starten“. Ein immenser Vorteil dabei ist, dass HIMA beim TÜV Rheinland eine Kerngruppe von fixen Ansprechpartnern hat, was vieles einfacher mache: „Die TÜV-Experten sind

immer hervorragend im Thema, und wenn es etwas zu klären gibt, so wird das in der Regel direkt, schnell und zielführend gelöst."

Merlin Hilger erlebt in seiner aktuellen Tätigkeit eine „sehr gute, konstruktive und professionelle Zusammenarbeit mit HIMA in den verschiedensten Bereichen." Hierzu zählen Planung und Durchführung von gemeinsamen Trainings, Änderungsprüfungen bei bestehenden HIMA Lösungen oder die Prüfung von neuen, smarten Safety-Lösungen, die das vorhandene HIMA Portfolio ergänzen. Der TÜV Rheinland zertifiziert überdies auch das Functional Safety Managementsystem bei HIMA.

Produktneuentwicklungen wie die HIQuad X oder die HIMax können bei HIMA durchaus fünf bis acht Jahre dauern, erklärt Betz. Den TÜV Rheinland als notifizierte Stelle (engl. „notified body") bei Produktneuentwicklungen von Anfang an mit einzubeziehen, ist laut Betz auch eine wirtschaftliche Risikominimierung für HIMA als Hersteller: „Es hat keinen Sinn, trotz aller Erfahrungen einfach aufs Geratewohl etwas Neues zu bauen, wo es dann wesentliche Bedenken etwa bezüglich der Maschinenrichtlinie gibt. Daher ist der regelmäßige Austausch mit dem TÜV während der Entwicklung für uns von fundamentaler Bedeutung." Selbstverständlich gäbe es aber auch unmittelbar vor einer Zertifizierung hin und wieder Rückfragen der Prüfer in letzter Minute – aber alles in einem positiven und konstruktiven Verhältnis, meint Betz. Das hohe Kompetenzlevel bei allen beteiligten HIMA Experten trägt nicht nur zur hohen Qualität und zum hohem Niveau der Zusammenarbeit bei – es sorgt auch, wie Hilger erklärt, für den nötigen Spaß bei der Arbeit. „Zertifizierungen sind immer das Ergebnis von viel Arbeit, die ein ganzes Team an Mitarbeitern bei HIMA über längere Zeiträume geleistet hat", resümiert Betz.

Am Anfang war die Einzelfehlerbetrachtung

Dem heutigen hohen Stand der Funktionalen Sicherheit gingen Jahrzehnte der Entwicklung der heute gültigen Normen voraus. Von den 1970er bis in die 1980er Jahre hinein wurde vor allem mit niedrigkomplexer und zugleich hartverdrahteter Technologie gearbeitet, die vom TÜV Rheinland zertifiziert wurde. Damals gab es noch andere Betrachtungsweisen, die sich nach einem deterministischen Ansatz ausrichteten. Es gab damals noch keine Klassifizierungen hinsichtlich von Sicherheitsklassen oder Safety Integrity Levels (SIL). Dementsprechend wurden auch keine Risikobetrachtungen durchgeführt. Lediglich Fehlerraten- und Ausfallberechnungen wurden schon gemacht, aber eben „nicht in Bezug auf die Versagenswahrscheinlichkeit", so Gall. Ab den 1980er Jahren rückten zunächst die programmierbare Technologie und dann verstärkt die Mikrocomputer in den Vordergrund.

„Beim früher üblichen deterministischen Ansatz stand die Einzelfehlerbetrachtung im Fokus, was heute nicht mehr möglich ist“, sagt Gall. „Man konnte sich einzelne Bauteile und Komponenten anschauen und überlegen, was denn passiert, wenn dort ein Fehler auftritt.“ Diese FMEA (Failure Mode and Effects Analysis; Fehlermöglichkeits- und Fehlereinflussanalyse) fand immer auf der Bauteilebene statt. Dabei stellte man sich die Frage: Was ist die Reaktion auf diesen Einzelfehler im Ausgangssignal? Die zu beachtenden Standards waren anwendungsbezogen: Ist die Komponente immer noch sicher in Bezug auf die Anwendung? Gall erinnert sich: „Wenn die Anwendung trotz Fehler immer noch sicher war, nahm man einen weiteren Fehler hinzu – bis zu drei Fehler in Kombination wurden betrachtet.“

Die Anwendung konnte alles Mögliche sein: Von Pressen bis hin zu Aufzügen, kurzum: jegliche Art von Maschinen. Um für die Technologie eine sichere Funktion zu realisieren, ging es immer um die Fehlerbetrachtung und Fehlerbeherrschung durch die in den Standards beschriebenen Maßnahmen. Zeitlich darauf folgten dynamische Systeme, die ebenfalls in den 1980er Jahren im Einsatz waren: „Sofern ein dynamisches Signal aus einer Betrachtungseinheit kommt, scheint alles in Ordnung zu sein“, so Gall. „Die Schaltkreise waren so designed, dass Fehler in einzelnen Bauelementen dazu geführt haben, dass eben jede Dynamik verloren ging. Damit konnte man dann feststellen, ob die sichere Funktion der Anwendung noch gegeben war – oder eben nicht.“

Die Mikrocomputer änderten dann vieles. 1984 wurde ein Forschungsprojekt vom TÜV Rheinland und dem TÜV Bayern publiziert, was Mikrocomputer in der Sicherheitstechnik zum Thema hatte. Hier wurden erstmalig fünf Sicherheitsklassen auf den damals verfügbaren Standards definiert und Fehlerzählungen als Herangehensweise angewendet. Die Sicherheitsklassen waren allerdings nicht mit den heutigen SIL-Leveln zu vergleichen. „Man hat sich Fehlermodelle in integrierten Schaltkreisen angeschaut und auch über mögliche Redundanzen und Diagnosemaßnahmen, beispielsweise für CPU, RAM und ROM nachgedacht“, erklärt Gall rückblickend. „In dem Handbuch wurden aber noch keine Versagenswahrscheinlichkeit und Risikobetrachtungen thematisiert. Aber es wurde die programmierbare Technik im Hinblick auf sicherheitsrelevante Anwendungen erstmalig in den Fokus genommen.“

Nach Erscheinen des Handbuchs setzte Mitte der 1980er Jahre in Deutschland eine verstärkte Normungstätigkeit ein. „Die DIN-Standards definierten Gefährdungen und Risikoklassen – wobei immer noch die Wahrscheinlichkeiten fehlten,“ erinnert sich Gall. Einzelne Normen im Bereich der Feuerungstechnik beispielsweise haben den Einsatz der programmierbaren Technik beschrieben. „Ende der 1980er Jahre kamen dann mit der DIN

V 19250 oder der DIN V VDE 0801 zur Sicherheit mit Rechnertechnik auch die deutschen Standards heraus.“

Betrachtet man die deutsche Vornorm DIN V 19250, gab es damals noch die Anforderungsklassen (AK), die heute mit den SIL-Leveln der Normen IEC 61508 oder IEC 61511 abgebildet werden. Die IEC Normen erschienen Anfang der 1990er Jahre und übernahmen vieles der deutschen Standards. „Hier kamen jetzt auch die Versagenswahrscheinlichkeit und Verfahren zur Risikoreduzierung hinzu“, erklärt Gall. „Aufgrund des ermittelten Schadensausmaßes und Häufigkeit des Auftretens war eine entsprechende Risikoreduzierung notwendig, die über die SIL-Level definiert wurde.“

Wollte man Risiken reduzieren, so bedurfte es bestimmter Maßnahmen, die die zufällig auftretenden Fehler beherrschen und systematisch auftretenden Fehler vermeiden konnten – und zwar schon während der Entwicklung eines Produktes oder einer Lösung. „Ziel war es hier dann schon, fehlerarme Systeme zu designen“, meint Gall. Mit den geeigneten Diagnoseverfahren war dann auch die Ermittlung einer Ausfallwahrscheinlichkeit möglich. In der IEC 61508 wurden diese Konzepte grundsätzlich definiert. Sie diente nun neben der IEC 61511 als Grundnorm zur Betrachtung der Funktionalen Sicherheit für die unterschiedlichsten Anwendungsstandards.

Ein weiterer wichtiger Punkt ist die Entwicklung eines strukturierten Safety-Managements. Auch hier gab es anfänglich weder Standards noch eine offizielle Vorgehensweise, an der sich Anwender oder Hersteller zu orientieren hatten. Gall blickt zurück: „Maßnahmen zur Qualitätssicherung gab es natürlich in jeder Firma. Diese waren aber mehr personen- als systemabhängig. Ein strukturiertes Safety-Management wie heute, was durchgängig in Unternehmen verfolgt wird und an dem sich alle Mitarbeiter, die in der Entwicklung tätig sind, orientieren können – das war damals noch nicht existent.“

Über die Jahrzehnte veränderte sich die Denkweise: „Von der deterministischen Einzelfehlerbetrachtung bei Komponenten entwickelte es sich hin zu einer Betrachtung von hochkomplexen Systemen hinsichtlich der Versagenswahrscheinlichkeit und der Reduzierung des Risikos“, fasst Gall die Entwicklung zusammen. „Die heute vorhandene Komplexität macht es unmöglich, wie früher nur umfänglich zu testen. Das wird einfach zu aufwändig.“

HIMA und TÜV Rheinland brachten die Normenwelt entscheidend mit voran

Die Normen wurden durch die Beteiligten in den Normungsgremien gemeinsam diskutiert und entwickelt. Ab 1984/85 war Heinz Gall zusammen mit ein bis zwei HIMA Vertretern in

dem Gremium tätig, was sich explizit mit der Funktionalen Sicherheit beschäftigte. Jede Seite brachte ihre Sichtweisen und Kompetenzen mit ein: Der TÜV Rheinland die Betrachtungsweise der Prüfstelle und HIMA die Expertise als Hersteller von Sicherheitssteuerungen. Gall erklärt: „Die Gremien setzten sich aus Vertretern der verschiedenen TÜVs sowie Experten aus der Industrie, den Verbänden, den Instituten der Berufsgenossenschaften und den Hochschulen zusammen.“ In den Normungsgremien habe es über die Jahrzehnte immer eine gute, enge und dialogische Zusammenarbeit mit den Fachleuten von HIMA gegeben, erinnert sich Gall. Aus der Sicht von HIMAs Prüfspezialist Betz ist es auch notwendig, dass Hersteller die Blickwinkel der Industrie mit in die Normungsgremien dialogisch hineintragen. „Gerade bei der Normenfindung sind das sehr dynamisch verlaufende Prozesse mit vielen Gesprächen und Abstimmungen“, so Betz.

Ein gutes historisches Beispiel für die erfolgreiche dialogische Zusammenarbeit war die Entwicklung der Standards für die Feuerungstechnik wie der VDE 0116, die sich sehr früh mit Rechnertechnik beschäftigt hat und mittlerweile in die DIN EN 50156 übergegangen ist. Die Zusammenarbeit zwischen TÜV Rheinland und HIMA setzte sich auch bei der IEC 61508 und der IEC 61511 fort. „Gerade bei den drei Standards – VDE 0116 für die Feuerungstechnik, IEC 61508 als grundlegender Norm für die Funktionale Sicherheit und IEC 61511 für die Prozessindustrie auf der Anwenderseite – arbeitete ich an den verschiedenen Versionen jahrelang persönlich mit den Vertretern von HIMA zusammen“, fasst Gall zusammen.

In Europa legt die EU die Richtlinien fest, aus denen sich letztlich die Normen ergeben. „Die Sicherheit muss in Europa immer nach dem Stand der Technik gegeben sein“, so Gall. Nach Hilgers Ansicht müssen die Normengremien einen vernünftigen Mittelweg wählen, um gerade bei Grundnormen wie der IEC 61508 ein Gerüst aufzustellen, was nicht nur aktuell gültig ist, sondern auch noch in Jahren Bestand hat. Auch hier sind die sich rasant entwickelnden Technologien der Grund, mit denen die Normen gar nicht Schritt halten könnten. Hilger erklärt: „Deswegen gehen die Normen wie die IEC 61508 auch nicht auf technische Details ein, sie beschreiben vielmehr Verfahren, aus denen man auch den Umgang mit neuen Technologien ableiten kann.“ Ein gutes Beispiel dafür ist die Multicoretechnologie bei Prozessoren, auf die die Verfahren der Norm anwendbar sind und deshalb genutzt werden müssen. Multicoreprozessoren sind extrem leistungsfähig, da ihre Kerne parallel laufen. Dies habe aber neben der gesteigerten Leistung auch neue Fehlerbilder zur Folge, die ein Prozessor mit nur einem Kern nicht hat. „Da es bei der Funktionalen Sicherheit darum geht, Fehler in den Griff zu bekommen, sind die Fehlerbilder

der Multicoreprozessoren eine Herausforderung“, erklärt Hilger. „Hier ist es notwendig, dass die Normen dahingehend an die Realität der neuen Fehlerbilder angepasst werden.“

„Man hat schon das Gefühl, die Anzahl der Normen, welche bei einer Prüfung zu berücksichtigen sind, zunimmt, was aber nicht unbedingt an den gesetzlichen Vorgaben oder den Normen selbst liegt, sondern daran, dass sich Technologie rasant entwickelt. Mit einem Produkt sollen möglichst viele Märkte und Anwendungen abgedeckt werden. Im Fall von HIMA eignen sich deren Steuerungen ja nicht nur für die Prozessindustrie, sondern auch für andere Bereiche – etwa für Bahn-Anwendungen, Maschinensicherheit und in der maritimen Industrie“, erklärt Hilger.

Für Betz haben die Normen sowohl qualitativ als auch quantitativ stark zugenommen: „Ganz zu Anfang der Zertifizierungen von HIMA Sicherheitssteuerungen gab es gerade einmal eine Handvoll Normen – mehr nicht. Heute ist alles viel detaillierter definiert und festgehalten.“ Aus der Sicht von HIMA müssten die Normen angepasst werden, um mit den technologischen Entwicklungen Schritt halten zu können, so Betz. „Die Normen sollten idealerweise den tatsächlichen technologischen Gegebenheiten entsprechen. Das ist ein Anliegen von HIMA als Hersteller, und daher sehen wir uns hier auch als Normen-Treiber.“ Normierungen und die Weiterentwicklung von Normen sind dialogische Prozesse, weshalb die einbringenden Parteien bereits im Vorfeld eine gute Argumentation und Begründung vorlegen sollten, um in der dann folgenden Normendiskussion Aussicht auf Erfolg zu haben.

Bedingt durch die variablen Anwendungsbereiche moderner Produkte müssen diese auch immer mehr Normen berücksichtigen. „Dieser Zuwachs an Normen ist also auch herstellergetrieben“, folgert Hilger. Für diese unterschiedlichen Bereiche kommen verschiedene Normen zum Tragen, die aber alle auf die gleiche Grundnorm zurückzuführen seien. „Hier haben die Normengremien mitgedacht, damit dies überhaupt von uns noch bewältigt werden kann“, meint Hilger.

Technologieentwicklung und Cybersecurity als Herausforderungen

Technologisch hat sich im Laufe der Jahrzehnte sehr vieles geändert. „Früher war die Technik komplett hartverdrahtet, teilweise auf Relais basierend. Software, die heute überall zu finden ist, gab es kaum“, erklärt Betz. „Die einzelnen Prozessoren sind kleiner und auch viel leistungsfähiger als früher. Trotzdem sind die modernen Sicherheitssteuerungen als Ganzes nicht kleiner geworden, was vor allem an der gestiegenen Komplexität liegt. Diese muss sowohl in der Software als auch in der Hardware abgebildet werden.“

Die Sicherheitssteuerungen decken mehr Möglichkeiten und Funktionen ab. Das bedeutet auch, dass die Funktionale Sicherheit hier auch vor wachsenden Herausforderungen steht.

Während sich die Konzepte der Funktionalen Sicherheit – eben die Vermeidung von Fehlern – kaum verändert haben, ist die extrem schnelle Technologieentwicklung die größte Herausforderung heute. „Die Technologie treibt ganz klar die Normen“, meint auch Gall. Als Beispiel führt sein Kollege Hilger erneut die Multicoreprozessoren ins Feld. Die Technologie sei bereits vorhanden und marktreif, daher wollten Unternehmen sie auch einsetzen. Doch zu der Zeit, als die Normen wie IEC 61508 zum letzten Mal aktualisiert wurden, haben Multicoreprozessoren damals noch keine große Rolle in der Sicherheitstechnik gespielt – und sind demnach von der Norm noch nicht behandelt worden.

Die Hersteller, die sich seit vielen Jahren mit dem Thema der Funktionalen Sicherheit beschäftigen, hätten ihre Diagnosen und ihre Lösungen sehr gut unter Kontrolle, meint Klaes: „Man könne quantitativ bestimmen, wie hoch die Wahrscheinlichkeit ist, dass eine Sicherheitsfunktion bei Anforderung nicht im Sinne des Anwenders arbeitet.“ Wenn man also innerhalb der Lösung auch alles „im Griff“ habe, oder Ausfallwahrscheinlichkeiten gut berechnen könne, so wirkt hier die Cybersecurity tatsächlich als Game-Changer. Cybersecurity kam erst durch die Vernetzung ins Spiel. Es ging früher nur um reine Fehlervermeidung (FMEA). Angriffe von außen und die Manipulation eines Systems waren – wenn überhaupt – nur dann möglich, wenn der Angreifer direkt physikalischen Zugang, etwa zu den Schaltschränken oder der Hartverdrahtung hatte. „Dieser direkte Angriff über die Hardware ist heute nicht mehr nötig, da Angreifer nun den Weg über das Netzwerk wählen können“, so Gall.

Für Gall sind die gestiegene Kommunikation und auch die Netzwerkfähigkeit der Systeme der entscheidende Grund, auch hinsichtlich der Cybersecurity sehr aktiv zu werden. „Keinesfalls sollte man die Dinge komplexer machen als nötig. Einfach deshalb, weil man ja selbst immer noch alles überblicken muss. Auch hinsichtlich der Funktionalen Sicherheit gilt das Gleiche“, merkt Gall an. „Saubere Strukturen sind wichtig, um das komplette System zu überblicken und zu bewerten. Sind die Strukturen allerdings nicht wirklich sauber angelegt, so nimmt auch die Komplexität und die Schwierigkeit unnötigerweise zu, alles im Blick zu haben und das geforderte Sicherheitsniveau zu erfüllen. Auch darf man sich nicht zu sehr auf interne Diagnosen und Test verlassen.“

Die grundsätzlichen Anforderungen für eine sichere Funktion seien gleichgeblieben, meint Gall. Gleichzeitig seien die Herausforderungen durch die mit der Zeit gestiegene

Komplexität deutlich größer geworden. Durch den Einsatz von mehr Software komme es auch zu mehr Fehlermöglichkeiten – „Safety verschiebt sich klar in Richtung Software“, resümiert Gall. Hierauf sei schließlich mit der Norm IEC 61508 Edition 2 reagiert worden. Systeme werden immer flexibler und modularer im Aufbau, die HIMA Smart Safety Platform ist ein gutes Beispiel dafür. Der Software kommt verglichen mit der Hardware immer größere Bedeutung zu. Hier geht es auch die Vermeidung von Obsoleszenz: „Safety verschiebt sich Richtung Software, was auch an der höheren Dynamik liegt“, meint auch Betz.

Auch für Gall kommt der Software eine sehr wichtige Rolle bei der der Fehlervermeidung zu. „In der Software sind eben nur systematische Fehler und keine zufälligen Fehler zu betrachten – das bedeutet: Man muss sich hier schon wirklich Mühe hinsichtlich der Fehlervermeidung und der Risikoreduzierung geben und damit auch folgerichtig seinen Fokus auf eine klare Struktur und Architektur richten“, folgert Gall.

Cybersecurity war früher auch für Betz eine rein physikalische Zugangskontrolle. Heute ist die Cybersecurity ein gestuftes Gesamtkonzept mit einer systematischen Bedrohungsanalyse, bei der auch Faktoren wie Social Engineering eine wichtige Rolle spielen. „Was bei der Safety die FMEA ist, ist bei der Cybersecurity die systematisch vorgenommene Bedrohungsanalyse“, meint Betz. Die Risikoabwägung ist hierbei elementar, kann aber anhand von Systematiken durchgeführt werden, an deren Ende ein schlüssiges Gesamtkonzept steht. Ein gutes Beispiel ist die Verwendung des STRIDE-Ansatzes (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure; privacy breach or data leak, **D**enial of service, **E**levation of privilege). „Die Verantwortung liegt hierbei beim Anwender. Er muss sich fragen, was passieren muss, damit ein bestimmtes Angriffsszenario stattfinden kann. Als Hersteller können wir hier die Verwendung von geeigneten Lösungen im Gesamtkonzept vorschlagen“, fasst Betz zusammen. In einigen Fällen eignen sich hinsichtlich der Bedrohung durch Cyberangriffe auch die bewährten hartverdrahteten Lösungen, wie sie auch HIMA mit dem Produkt Planar herstellt. Die Hartverdrahtung ist laut Betz deswegen an neuralgischen Punkten nach wie vor wichtig und behält ihre Bedeutung, etwa bei der Verwendung in kritischen Infrastrukturen. „Die hier verwendeten hartverdrahteten Steuerungen werden nicht hinsichtlich einer Vernetzung ertüchtigt, sie haben ganz klare Aufgaben und sind in diesem Sinne so einfach wie möglich gehalten“, weiß Betz.

Werden Sicherheitsfunktionen von außen angegriffen und möglicherweise kompromittiert, stellen sich für alle – Hersteller wie Betreiber – ganz neue Herausforderungen. Dass jemand bewusst die Safety-Funktionen manipulieren möchte, habe vor Jahren so niemand

erwartet. Ebenso habe die Vernetzung stark zugenommen, um den Anwendern mehr Möglichkeiten zu bieten, etwa einem Zugriff von Zuhause aus. Die Hersteller wären diesen Wüschen für ihre Industriekunden gerne nachgekommen, so Klaes, doch hätte man so auch viele Angriffspunkte für potentielle Cyberangriffe geschaffen. Aus der Sicht von Klaes ist es momentan die größte Herausforderung, die Funktionale Sicherheit auch hinsichtlich der Cybersecurity zu denken: Daher werden auch seit einiger Zeit folgerichtig große Anstrengungen unternommen, ‚safe' Sicherheitslösungen auch gleichzeitig ‚secure' zu machen.

Die Lebenszyklen der Anlagen hinsichtlich der Funktionalen Sicherheit sind völlig anders als bei den Systemen der Cybersecurity, wo ständig Sicherheitsupdates notwendig sind, um bestmöglichen Schutz bieten zu können. Der Lifeycle der Cybersecurity ist im Vergleich zu dem der Funktionalen Sicherheit sehr kurz und von kontinuierlichen Modifikationen charakterisiert.

Es ist daher wichtig, schon vom Anfang der Entwicklung von Systemen der Funktionalen Sicherheit an auch an Cybersecurity zu denken. Dabei sollten auch Trennbarrieren eingebaut werden, damit eine kleine Änderung an der Security nicht auch die Safety beeinträchtigt. Diese Herausforderungen müssen in der Industrie in Einklang gebracht werden.

In Hilgers Zeit beim TÜV Rheinland war kein zertifiziertes Produkt je in einen Unfall verwickelt, der in den Bereich der Safety fällt. Ganz anders sieht das hingegen bei der Cybersecurity aus. Spätestens seit aktiven Cyberangriffen wie Stuxnet werden mögliche Gefahren bei Herstellern von Sicherheitssteuerungen sehr ernst genommen. Folgerichtig ist deshalb die Cybersecurity aufgrund der steigenden Bedrohungslage ein wichtiges Tätigkeitsfeld für den TÜV Rheinland als Zertifizierungsstelle geworden. „Wenn man als Anwender ein Cybersecurity-Risiko sieht, muss man die Norm beachten. Die Initiative liegt hier beim Anwender", sagt Hilger. „Wenn eine Vernetzung vorliegt und die Funktionale Sicherheit durch Cyberangriffe bedroht sein könnte, dann ist diese Situation laut IEC 61508 zu betrachten", fügt Gall hinzu. „Die Norm 61508 verweist dann weiter auf die Cybersecurity-Standards, wie etwa IEC 62443."

Vernetzung werde heute immer wichtiger, auch weil es die Kunden hinsichtlich Kommunikation und Steigerung der Produktivität wünschen. Gute Beispiele sind die Wünsche nach Dezentralisierung, mehr Fernwartung oder guten Remotesteuerungen in der Industrie. Um diesen Kundenbedürfnissen entgegen zu kommen, wird auf der Seite von HIMA derzeit an einer API für das HIMA Engineering Tool gearbeitet, mit der Kunden ihre

Abläufe plattformunabhängig remote automatisieren können. Auch die HIMA Smart Safety Platform kommt den Marktbedürfnissen entgegen. Werkzeuge (Tools) wie etwa die HIMA Engineering Platform werden immer wichtiger – sowohl für die eigene Entwicklungsumgebung als auch für die spätere Bedienung durch den Anwender. Tools müssen dementsprechend qualifiziert werden. Da sie auf Software basieren, ist hier besonderes Augenmerk auf die Cybersecurity zu richten.

Bei HIMA werden nach strategischen Angriffen wie durch Stuxnet alle Bestandsprodukte hinsichtlich ihrer Cyberangreifbarkeit geprüft und einsprechend abgesichert. Die Bedrohungen nimmt das Unternehmen sehr ernst: „Nachweislich wurden bislang keine HIMA Sicherheitssteuerungen durch Angriffe korrumpiert – und wir arbeiten hart daran, dass dies auch so bleibt. Es ist aber unseriös zu behaupten, dass es eine absolut sichere Steuerung überhaupt geben kann“, sagt Betz. „Letztlich hängt es immer vom Aufwand ab, den ein Angreifer betreiben will. Staaten stehen ganz andere Ressourcen zur Verfügung als den ‚Script-Kiddies‘ oder kleinen Gruppen von Cyberkriminellen.“

„In den vergangenen fünf Jahren ist die Cybersecurity klar in den Fokus gerückt – aus gutem Grund“, sagt Klaes. IEC 61508 hat schon vor zehn Jahren auf die IEC 62443 verwiesen. Als Beispiele für diese Verweise nennt Klaes die ‚Threat Analysis‘ und die Vulnerability Analysis‘. Das vorhersehbare Risiko von Cyberattacken wird fraglos durch die starke Vernetzung deutlich erhöht und auch die Norm IEC 62443 findet in der funktional sicheren Sicht viel mehr Anwendung als früher. Seit 2018 steht der Standard IEC 62443-4-1 – hinsichtlich Managementprozesse / Lifecyle zur Verfügung und seit 2019 der Standard IEC 62443-4-2 – hinsichtlich technischer Anforderungen. Für Komponenten wie beispielsweise Steuerungen ist der 2019 veröffentlichte Teil 4 der IEC 62443 wichtig. Dies zeige, für wie wichtig die Cybersecurity von den betreffenden Normengremien eingestuft wurde, meint Klaes.

„Es gibt eine klare Tendenz auf dem Markt, dass sich viele Unternehmen und Anbieter mit dem Thema Cybersecurity beschäftigen, um ihre Lösungen ‚secure‘ zu machen. Hier wächst angesichts der realen Bedrohungen ein völlig neuer Markt heran, auf den die Hersteller von Sicherheitslösungen reagieren“, weiß Klaes. Betz pflichtet dem bei und betont: „Die IEC 62443-4-1 und die IEC 62443-4-2 haben für uns als Hersteller in Bezug auf die Cybersecurity höchste Bedeutung bei der Produktpflege und der Produktneuentwicklung. Gerade der Teil 4-1 ist hier wichtig: Security muss von Anfang an betrachtet werden.“

Weitere Herausforderungen der Zukunft

Die COVID-19-Krise beeinflusst die Arbeit des TÜV Rheinlands kaum. Der Grund hierfür ist, dass alle Dokumente, die für die Prüfung überprüft und mit den Normen abgeglichen werden müssen, auch auf digitalem Wege vom Hersteller zur Verfügung gestellt werden können. Früher kamen die zu prüfenden Dokumente noch per Post. Heute ist alles digital verfügbar und wird zuvor Tool-gestützt generiert. Lediglich Tätigkeiten, bei denen das Aufeinandertreffen von Menschen zwingend notwendig ist, sind von der aktuellen Krise betroffen.

Persönliche Kundenbesuche sind vor allem bei Prüfungen in der Produktpflege einfacher, als bei den aufwändigeren Prüfungen bei komplett neuen Produkten. Viele Tests, vor allem die internen bei Herstellern wie HIMA, werden immer stärker automatisiert. Hier kommen bereits seit Jahren Scripte und automatisierte Testumgebungen in Prüffeldern zum Einsatz. Auch die Testberichte sind daher nicht mehr handschriftlich wie früher, sondern werden vollständig von einem Tool generiert.

Die Prüfverfahren sind festgelegt und bis vor ein paar Jahren habe man alles manuell geprüft, sagt Betz. „Das waren langwierige Abläufe, bei denen viele Personen beteiligt waren." Fast die Hälfte der Zeit wird bei der Entwicklung an Nachweisen, Prüfungen, Tests und Verifikationen aufgewendet. Vor einigen Jahren hat HIMA angefangen, im Sinne einer Optimierung möglichst viele Funktionalitäten bei den Prüfungen zu automatisieren. Was früher ein halbes Jahr und länger gedauert hat, ist heute dank der Automatisierung in wenigen Wochen, manchmal sogar nur Tagen abbildbar und spart bei der Entwicklung einige Mannjahre an Zeit ein. Bei den Prüfungen selbst kann im Vergleich zu früher eine vergleichbare Zeitdauer gehalten werden, was Betz als guten Erfolg sieht: „Hier ist durch die gestiegene Komplexität einfach zusätzlich viel mehr Aufwand da."

Dass HIMA in der Digitalisierung bereits gut vorangeschritten ist, kommt den Testabläufen während der aktuellen COVID-19-Krise sehr entgegen. Die vorhandene Infrastruktur ermöglicht es beispielsweise, dass HIMA Experten die Tests von Zuhause, also remote, anfahren können und nur bei wenigen Prüfungen zwingend vor Ort sein müssen. Für den TÜV Rheinland musste geklärt werden, ob bei einem Fehlereinpflanzungstest die physikalische Anwesenheit eines TÜV-Mitarbeiters zwingen notwendig ist. Generell gibt es Prüfungen, wo die Fachleute des TÜVs persönlich vor Ort sein sollen – bei anderen hingegen nicht.

Beim Nachweis der Sicherheitsfunktionen – also der erfolgreich demonstrierten Abschaltung – gibt es das sogenannte „Witness Testing“, bei dem bisher Zeugen der Prüfstelle vor Ort anwesend sein müssen. „Vor Kurzem haben wir hier etwas völlig Neues umgesetzt: Mit Hilfe einer sehr guten Kamera und einem sicheren Videokonferenz-Tool haben wir das Witness Testing nun auch erfolgreich remote umsetzen können – der Prüfer war also auch hier live dabei, und das hat im Sinne der Rezertifizierung im Rahmen der Produktpflege genügt“, erzählt Betz. „Wir sind optimistisch, dass wir diese Remote-Prüfungen auch bei anderen Zertifizierungen anwenden können. Der Digitalisierungs-Schub durch COVID-19 ist hier klar erkennbar und eröffnet uns neuen Chancen: Witness Tests sind mit Videoübertragungen einfach viel effizienter und auch direkter als früher durchführbar.“

„Es wäre es auf jeden Fall wünschenswert, insgesamt noch mehr Prüfungen digital durchführen zu dürfen“, denkt Hilger. Im Falle der Fehlereinpflanzungstest gibt es noch keine Entscheidung, ob der TÜV diese zukünftig weiterhin remote durchführen wird. Auch die Fortschritte bei der VR-Technologie eröffnen neue Möglichkeiten. Allerdings sei da zuerst der Gesetzgeber für die Definition der Rahmenbedingungen gefragt: Ist eine Prüfung unter der Verwendung von VR-Technologien überhaupt zulässig? Die Krux: Ist eine Prüfung ohne persönliche Anwesenheit überhaupt komplett möglich, selbst wenn es der Gesetzgeber (bzw. der Akkreditierer) erlauben würde? Wie kann sichergestellt werden, dass das Testergebnis richtig ermittelt wird? Neben dem Gesetzgeber kommt es aber immer noch auf das Urteil des Sachverständigen und dessen Sachverstand an.

Fazit

HIMA und TÜV Rheinland haben durch ihre gute Zusammenarbeit in den Normungsgremien einen wertvollen Beitrag geleistet, die Funktionale Sicherheit in Deutschland auf den heutigen Stand zu bringen und die Normenwelt voran zu treiben. Etappen waren die deutsche Vornorm DIN V 19250, der vorläufige Endpunkt Normen wie IEC 61508, IEC 61511 und IEC 62443. Dabei haben die zu beachtenden Normen sowohl qualitativ als auch quantitativ stark zugenommen, was sich auch auf die Prüfungen und Zertifizierungen auswirkt, die der TÜV Rheinland bei Unternehmen wie HIMA durchführt. Auch die Betrachtungsweisen bei den Prüfungen selbst haben sich im Laufe der Jahrzehnte deutlich geändert: Statt einem deterministischen Ansatz der Einzelfehlerbetrachtung von Komponenten steht nun die Betrachtung von hochkomplexen Systemen hinsichtlich der Versagenswahrscheinlichkeit und der Reduzierung des Risikos im Vordergrund. Die zentralen Herausforderungen auf diesem andauernden Weg ergeben sich durch den ständigen technologischen Fortschritt, mit dem die Normen nur schwer

mithalten können, neuen Bedrohung durch Cyberangriffe und die derzeitige COVID-19-Situation. Hierbei kommen auch remote Tests und Automatisierungen zum Einsatz, was die tagtägliche Arbeitsweise aller Beteiligten stark verändert.

(ca. 5.484 Wörter, 40.011 Zeichen)

Über die Autoren

Jana Klaes

Elektroingenieurin bei TÜV Rheinland Industrie Service GmbH (Spezialgebiet Cybersecurity)

Seit zwei Jahren als Assessor beim TÜV Rheinland im Bereich der Funktionalen Sicherheit beschäftigt. In der Zusammenarbeit mit HIMA ist sie sowohl in den Bereichen Cybersecurity als auch Funktionale Sicherheit tätig.

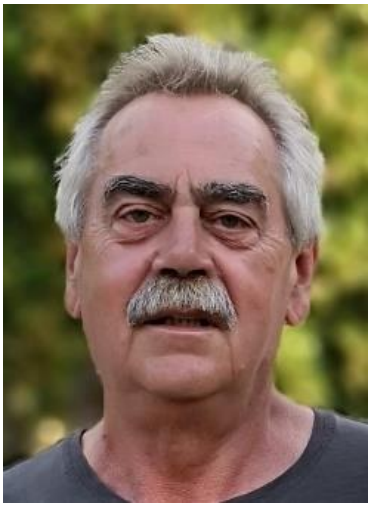
Bild © TÜV Rheinland Industrie Service GmbH

Merlin Hilger

Sachverständiger für Funktionale Sicherheit bei TÜV Rheinland Industrie Service GmbH (Spezialgebiet Funktionale Sicherheit)

Seit vier Jahren beim TÜV Rheinland tätig. Zusammenarbeit mit HIMA im Bereich Trainings, Änderungsprüfungen und der Prüfung von neuen Produkten.

Bild © TÜV Rheinland Industrie Service GmbH



Heinz Gall

Heinz Gall, war seit den 1980er Jahren bei TÜV Rheinland als Experte für Funktionale Sicherheit und Cybersecurity beschäftigt. Er ist seit 2019 im Ruhestand.

Bild © Privat

Boris Betz, HIMA Paul Hildebrandt GmbH

Boris Betz ist seit 2013 bei der HIMA tätig und betreut als Teamleiter in der Produktentwicklung Systemtests und Zertifizierungen

Bild © HIMA Gruppe

Über HIMA

Die HIMA Gruppe ist der weltweit führende unabhängige Anbieter smarter Safety-Lösungen für die Industrie. Mit global mehr als 40.000 Installationen TÜV-zertifizierter Sicherheitssysteme gilt HIMA als Technologieführer der Branche. Die spezialisierten Ingenieure des Unternehmens entwickeln individuelle Lösungen, mit denen Kunden im digitalen Zeitalter die Funktionale Sicherheit erhöhen, Cybersecurity stärken und die Rentabilität ihrer Anlagen und Fabriken steigern. Seit mehr als 50 Jahren gilt HIMA als verlässlicher Partner der weltgrößten Unternehmen der Öl-, Gas-, Chemie- und energieerzeugenden Industrie. Sie alle vertrauen auf Lösungen, Services und Beratungsleistungen von HIMA, stellen so einen unterbrechungsfreien Betrieb ihrer Anlagen sicher und schützen ihre Wirtschaftsgüter, ihre Mitarbeiter und die Umwelt. Zum HIMA-Portfolio gehören smarte Safety-Lösungen, die Daten in geschäftsrelevante Informationen umwandeln und damit zu höherer Sicherheit und Anlagenverfügbarkeit beitragen. Darüber hinaus bietet HIMA umfassende Lösungen für die effiziente Kontrolle und das Monitoring von Turbomaschinen (TMC), Brennern und Kesseln (BMC) und Pipelines (PMC). In der globalen Bahnindustrie sind die CENELEC-zertifizierten SIL 4-Safety-Controller auf COTS-Basis von HIMA führend in puncto Funktionaler und IT-Sicherheit sowie bei der Rentabilität. Das 1908 gegründete Familienunternehmen mit Hauptsitz in Brühl in Deutschland ist heute an mehr als 50 Standorten weltweit vertreten. Rund 800 Mitarbeiter erwirtschaften dabei einen Umsatz von €123 Millionen (2018). Erfahren Sie mehr unter: www.hima.com

Redaktioneller Kontakt / Belegexemplare bitte an:

Mark Herten, Publitek
Postfach 12 55, 21232 Buchholz
Tel.: +49 (0)4181 968 09820
Mobil: +49 (0)1520 748 3901
E-Mail: mark.herten@publitek.com

Carsten Otte, Publitek
Tel.: +49 (0)4181 9680 09880
Mobil: +49 (0)1520 915 8629
E-Mail: carsten.otte@publitek.com

Pressekontakt HIMA Headquarters
HIMA Paul Hildebrandt GmbH
Daniel Plaga
Group Manager Global PR

Albert-Bassermann-Straße 28
68782 Brühl
Tel.: +49 6202 / 709-405
Fax: +49 6202 / 709-123
E-Mail: d.plaga@hima.com

www.hima.com