
## Wie die Digitalisierung der funktionalen Sicherheit Mehrwert schafft

# Fachbeitrag

Juli 2023
Peter Sieber,
Vice President Strategic Marketing bei HIMA

# Wie die Digitalisierung der funktionalen Sicherheit Mehrwert schafft

*Mehr Vorschriften, weniger Fachkräfte – die Auslegung und der regelwerkskonforme Betrieb von Sicherheitssystemen stellt Anlagenplaner und -betreiber vor immer größere Herausforderungen. Eine ganzheitliche Digitalisierung der funktionalen Sicherheit eröffnet die Möglichkeit, diese Herausforderungen zu meistern – und deutlichen Mehrwert zu erzeugen.*

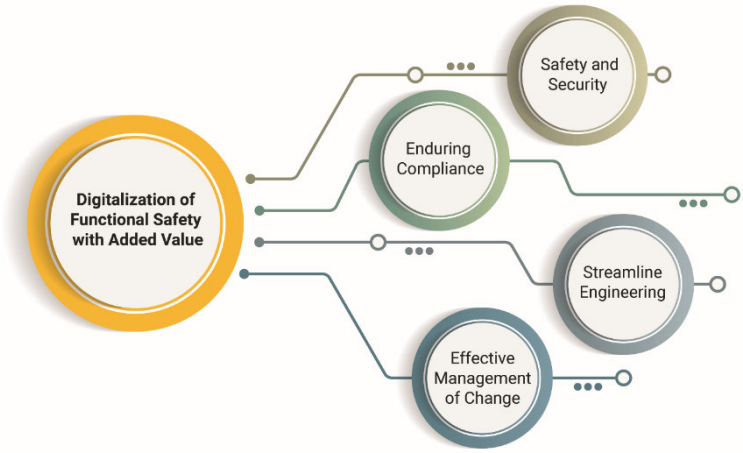
Ohne Sicherheitskonzept und -einrichtungen dürfen Anlagen der Prozessindustrie nicht betrieben werden. Deshalb spielt die funktionale Sicherheit eine Schlüsselrolle. Doch der Aufwand dafür ist hoch und wird immer höher: Die Risikobewertung und Planung der Sicherheitssysteme bis zu deren Betrieb und Wartung fordert den Beteiligten viel spezifisches Know-how ab – auch über den jeweils aktuellen Stand des Regelwerks. Und weil Sicherheitseinrichtungen immer stärker auch in das Fadenkreuz von Hackern geraten, wird auch die Cybersecurity immer wichtiger. Wird die funktionale Sicherheit allmählich zum Fass ohne Boden?

Nicht zuletzt auf dem Anwendertreffen der Namur im November 2022 wurden diese Aspekte kritisch diskutiert – und es wurde klar: Wir brauchen für die Zukunft der funktionalen Sicherheit einen neuen Ansatz, einen Gamechanger. Aus Sicht von HIMA ist dies die Digitalisierung der funktionalen Sicherheit unter dem Motto #safetygoesdigital.

Es geht dabei um mehr als das Automatisieren bestehender Abläufe wie zum Beispiel das Protokollieren von Prüfergebnissen: Die Digitalisierung der funktionalen Sicherheit hat das Potenzial, über die Sicherheitsfunktion hinaus Mehrwert für das Unternehmen zu schaffen, indem sie nicht nur dabei hilft, Kosten zu sparen, sondern auch die Verfügbarkeit von Anlagen zu steigern – und weil sie Daten und Informationen über die Anlage zur Verfügung stellt, die wiederum für Optimierungsprojekte genutzt werden können.

HIMA verfolgt dabei einen ganzheitlichen Ansatz, der vier Kernthemen adressiert:

1. Safety und Security
2. Durchgängige Regelkonformität
3. Optimiertes Safety Engineering
4. Effizientes Änderungsmanagement




**Safety und Security**

Dass die Digitalisierung der funktionalen Sicherheit ohne Security-Maßnahmen nicht gelingen kann, verwundert wohl kaum: Werden die bisher nicht vernetzten Feldgeräte der Sicherheitseinrichtungen „kommunikativ“ und tauschen Daten nicht nur mit Prozessleitsystemen, sondern beispielsweise auch mit Asset Management-Systemen aus, müssen sie selbst gegen Hackerangriffe geschützt werden. Security ist dabei nicht nur eine Aufgabe bei der Entwicklung der Sicherheitssysteme, sondern vor allem auch in der Betriebsphase. Die Vorstellung, dass es in Sachen Security ausreicht, Produkte nach den einschlägigen Normen zu entwickeln und anschließend zu zertifizieren, bleibt allerdings eine Illusion: Eine Security-Zertifizierung der Produkte allein schafft weder Safety noch Security. Sowohl Hardware als auch Applikationen erweitert HIMA deshalb um Funktionen, die Sicherheitssysteme in die Lage versetzen, als sichere Datendrehscheiben zu fungieren.

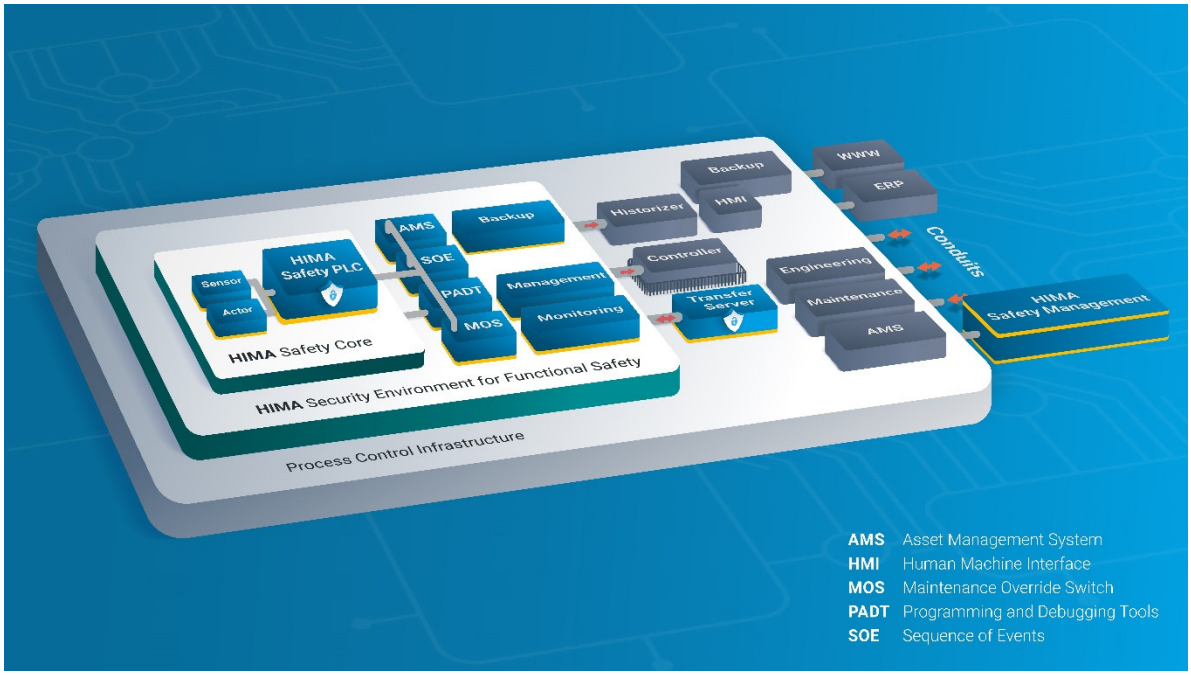
Dazu hat HIMA ein „Security Environment for Functional Safety“ entwickelt, das es ermöglicht, die Sicherheit über den gesamten Lebenszyklus der Sicherheitslösungen aufrecht zu erhalten und gleichzeitig den damit verbundenen Aufwand zu minimieren. Diesen ganzheitlichen Ansatz verfolgt HIMA auch durch die Partnerschaft mit genua, einem Spezialisten für IT-Sicherheit, der über ein umfassendes Security-Portfolio verfügt. Dies wird anwendungsbezogen mit dem HIMA Sicherheitsportfolio kombiniert. So profitieren Kunden von der Trennung von Safety- und Security-Maßnahmen, wodurch die Komplexität sinkt. Weil auf diese Weise standardisierte Set-ups genutzt werden können, lassen sich die Investitions- und Betriebskosten senken. Bei der Planung und Inbetriebnahme sorgt die Standardisierung für geringere Zeitaufwände, Kosten und Risiken. Gleichzeitig wird mit dem Ansatz die Übereinstimmung mit IEC 62443-3-3 (IT-Sicherheit für Netze und Systeme) erreicht.

Eigene Software entwickelt HIMA nach defensiven Gestaltungsgrundsätzen. So werden beispielsweise beim Windows-basierten Engineering-Werkzeug SILworX keine Windows-Funktionen für Datentransfers oder die Absicherung von Daten- und Authentifizierungs-Funktionen verwendet. Außerdem verzichten die Entwickler auf zugelieferte Software-Module und gestalten die Produkte so, dass die darin verwendeten Softwaremodule keine ungenutzten Funktionen enthalten – denn auch von diesen können Security-Risiken ausgehen. Und schließlich unterzieht HIMA die Software einer aufwändigen 100-%-Kontrolle, erst dann wird sie freigegeben.

HIMA stellt die Sicherheitsfunktionen in einer geschützten Umgebung bereit, welche von externen Einflüssen so weit wie möglich abgeschottet sind (HIMA Safety Core). Beim Konzept des „Security Environment“ wird um die eigentlichen Sicherheitssysteme ein Kokon gebildet, der neben den Sicherheitssystemen auch alle zu deren Betrieb notwendigen Einrichtungen einbezieht. Die Grenzen dieses Security Environment werden durch Firewalls gesichert, soweit es sich um Datenübertragungen mit vorhersehbaren Inhalten handelt.

Innerhalb des Security Environment werden für unterschiedliche Aufgaben physikalisch getrennte Schnittstellen verwendet. Mit diesem Ansatz minimiert HIMA den Aufwand im Betrieb, da eine logische Trennung mittels VPN oder Netzwerksegmentierung kontinuierlichen Aufwand zum Nachweis der Security Effizienz erfordert.

HIMA betreibt ein eigenes Security Lab, in dem reale Set-ups nahe an der Kundenumgebung erprobt und Anwendungsfälle aus dem Industrieumfeld entwickelt und getestet werden können.



Das *HIMA Security Environment for Functional Safety* trennt Safety und Security. (Bild: HIMA)

**Durchgängige Regelkonformität**

Ein weiterer „Pain Point“ aus Sicht von Planern und Betreibern von Sicherheitseinrichtungen ist es, sicherzustellen, dass die einschlägigen Vorschriften jederzeit eingehalten werden, denn die Konformität mit dem Regelwerk bildet die Voraussetzung für die Betriebsgenehmigung einer Anlage. Doch das Regelwerk ist inzwischen enorm umfangreich und die geforderten Prozesse für Prüfung, Nachweis und Dokumentation sind komplex. Die wachsende Flut an Safety-Vorschriften muss in den Betrieben von immer weniger Fachkräften beherrscht werden. Hier kann die Digitalisierung helfen – sie schafft allerdings auch neue Herausforderungen im Bereich der Security. Der Aufwand für Planung, Betrieb und Lebenszyklusmanagement ist bis heute hoch.

Mit der ganzheitlich digitalisierten Sicherheitsumgebung von HIMA wird die Übereinstimmung mit internationalen Standards und Praktiken sichergestellt: Darin werden sicherheitsrelevante Daten, die in allen Phasen des Lebenszyklus der funktionalen Sicherheit erzeugt werden und die bislang häufig in isolierten Datensilos vorliegen, einfacher nutzbar. Die erforderlichen Auswertungen werden einmal definiert und dann automatisch durchlaufen. So lässt sich deutlich einfacher eine vollständige Konformität mit den für die funktionale Sicherheit wichtigen Normen IEC61511 und IEC61508 erreichen. Durch Anwendung dieses End-to-End-Konzepts für funktionales Sicherheitsmanagement lassen sich zudem die Kosten der funktionalen Sicherheit minimieren.

Umgesetzt wird dies unter anderem in der digitalen Gesamtlösung von HIMA, die auf dem Produkt „Safety Lifecycle Manager, SLM®“ des strategischen HIMA Partners Mangan Software Inc. basiert. Diese deckt alle bisher manuell zu erledigenden Aufgaben rund um Sicherheitseinrichtungen bei der Planung und dem Betrieb sowie bei Änderungen an der Anlage ab. Zusätzlich werden Betriebsdaten aus den Sicherheitssystemen sowie Instandhaltungsdaten aus den Wartungssteuerungssystemen durch eine automatische Datenerfassung übernommen. Die automatische Korrelation dieser Daten liefert die für einen normgerechten Betrieb erforderlichen Informationen. Dadurch wird ein normkonformer Betrieb erleichtert und die Effizienz steigt.

Auf diese Weise lassen sich beispielsweise Kennzahlen (Safety KPI) definieren, anhand derer die Normkonformität nachgewiesen wird und gleichzeitig Verbesserungs- und Optimierungsmaßnahmen beurteilt werden können. Und noch ein weiterer Aspekt ist aus Betreibersicht bedeutend: Diese können günstigere Versicherungsprämien aushandeln, wenn sie ihren Sachversicherern nachweisen, dass die Sicherheitsvorschriften jederzeit eingehalten werden.

**Optimiertes Safety Engineering**

Konformität mit dem Regelwerk ist allerdings nicht nur im Betrieb, sondern auch bei der Planung wichtig. Auch hier ist eine tiefe Kenntnis der regulatorischen Anforderungen und der spezifischen Risiken der Anlage notwendig. Erschwerend kommt allerdings hinzu, dass relevante Dokumente und Daten im Engineering häufig an unterschiedlichen Stellen mit isolierten Tools entstehen. Die Informationen sind stark fragmentiert und es erfordert große manuelle Anstrengungen, um Datenkonsistenz in den Abläufen zu erreichen. Das Konzept #safetygoesdigital ermöglicht die nahtlose Integration von Daten aus der Risikoanalyse über den gesamten Entwicklungsprozess bis hin zur Wartung und Nachweisprüfung. Die Produkte und Tools von HIMA unterstützen den Datenfluss von und zu externen Systemen. So lässt sich nicht nur die Datenintegrität während des gesamten Lebenszyklus der Sicherheitsfunktion sicherstellen, sondern es sinkt auch der Personalaufwand für Entwurf, Installation und Betrieb der Sicherheitssysteme.

Um dem Engineering-Prozess eine Vielzahl von Tools zugänglich machen zu können, nutzt HIMA in seinem Programmiersystem SILworX Plug-Ins. Dadurch ist es möglich, schnell und flexibel auf Kundenanforderungen zu reagieren, ohne die SILworX-Zertifizierung nach IEC 61508 zu beeinträchtigen. Der Ansatz unterscheidet Kern- und Industrie-4.0-Funktionen. Während Erstere alle Sicherheitszertifikate erhalten, ist dies für die Plug-Ins nicht notwendig. Geplant sind zum Beispiel die Plug-Ins External Communication Configurator, Digital Inventory Manager und Digitalized Engineering. Letzteres hilft dabei, den gesamten Engineering Prozess zu digitalisieren, von der Spezifikation über die Programmierung bis hin zu den notwendigen Prüfungen.

Die Digitalisierung des Safety Engineerings rechnet sich für Betreiber, weil weniger Personalaufwand und niedrigere Kosten entstehen, wenn vor-getestete Typicals verwendet werden und der Test von Sicherheitsapplikationen automatisiert werden kann. Zudem kann das Betriebspersonal bereits vor der Inbetriebnahme an der digitalen Anlage geschult werden. Auch Anlagenbau und Systemintegratoren profitieren sowohl vom niedrigeren Inbetriebnahmeaufwand als auch vom geringeren Implementierungsrisiko.

**Effizientes Änderungsmanagement**

In der Betriebsphase einer Anlage beginnt deren Optimierung meist unmittelbar nach der Inbetriebnahme. Im Laufe der Zeit werden neue Komponenten hinzugefügt, die Anlage wird modifiziert, um Produkt- und Verfahrensparameter zu verändern oder neue Anforderungen zu erfüllen. All diese Veränderungen müssen auch im Sicherheitssystem berücksichtigt werden. Für einen regelwerkskonformen Betrieb der Sicherheitssysteme (SIS) ist es notwendig, diese kontinuierlich auf Änderungen hin zu überwachen. Zudem müssen Änderungen am SIS in geeigneter Weise umgesetzt werden.

HIMA hat dazu beispielsweise ein sicherheitskonformes Verfahren zum Upgrade von Sicherheitssystemen entwickelt, das sowohl Migrationen als auch Umrüstungen abdeckt. Digitalisierung ermöglicht es dabei, einerseits die Stillstandszeiten zu minimieren, andererseits auch eine Basislinie für weitere Änderungen zu schaffen. In diesem Zuge werden bestehende Projekte bzw. deren Projektdaten in das Engineering-Tool SILworX importiert und dort anhand der Projektanforderungen modifiziert.

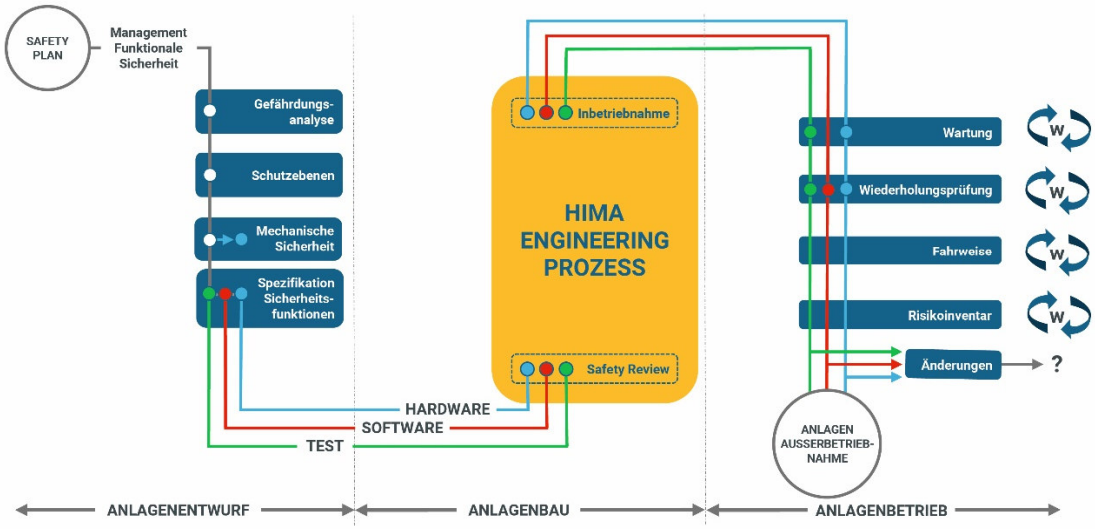
Durch Verwendung des SILworX-Features Smart Safety Test kann auf einfache Art und Weise nachgewiesen werden, ob die geforderte Funktion nach der Änderung dargestellt wird. Der Einsatz von Templates und Typicals beschleunigt die Planung von Migrations- und Revamp-Projekten erheblich, da dann auf vordefinierte Prüfprogramme zurückgegriffen werden kann.

Ein sehr augenfälliges Beispiel für den Mehrwert durch Digitalisierung ist die Automatisierung der wiederkehrenden Prüfung von Sicherheitseinrichtungen. Der Smart Safety Test von HIMA erlaubt es, neben den Diagnosemöglichkeiten der Feldgeräte Prüfroutinen zu definieren, die es erlauben Feldgeräte automatisch auf korrekte Funktion zu prüfen, ohne dass dazu die Anwenderprogramme der Sicherheitssysteme modifiziert werden müssen. So ist es beispielsweise möglich, mit regelmäßigen Teilhubtests die Prüfzyklen für Armaturen mit Sicherheitsfunktion, die einen Anlagenstillstand erfordern, deutlich zu verlängern.

**Fazit:**

Betreiber von Prozessanlagen versprechen sich von der Digitalisierung geldwerte Vorteile durch bessere Geschäftsprozesse und Anlagen, die im optimalen Betriebspunkt betrieben werden. Als Insellösung in der Regel von den Datennetzen der Automatisierungssysteme getrennt, entzieht sich die funktionale Sicherheit bisher den Bemühungen von IT und OT. Dabei kann Digitalisierung gerade hier helfen, die wachsenden Sicherheitsanforderungen rechtssicher zu erfüllen.

Der HIMA Sicherheitsprozess deckt als End-to-End Prozess die Phasen Anlagenentwurf, Anlagenbau und den Anlagenbetrieb ab. (Bild: HIMA)




Der HIMA Engineering-Prozess ermöglicht eine nahtlose Integration von der Risikoanalyse über den gesamten Entwicklungsprozess bis hin zur Wartung und Nachweisprüfung. (Bild: HIMA)