Digitalisierung der funktionalen Sicherheit nach Industrie-4.0-Grundsätzen

Standardisierung mit der Verwaltungsschale: HIMA treibt nächste Stufe der Digitalisierung der funktionalen Sicherheit voran.

Die Digitalisierung revolutioniert die funktionale Sicherheit, doch mit den neuen Chancen kommen auch weitere Herausforderungen hinzu. HIMA prägt diese Digitalisierung unter dem Schlagwort #safetygoesdigital – und zündet nun die nächste Stufe: Durch Standardisierung via Verwaltungsschale und innovative OT-Security-Konzepte gelingt auch der Spagat zwischen Effizienz und Cybersicherheit.

Der Wandel

Die funktionale Sicherheit schützt Mensch, Umwelt und Anlagen vor Gefahren und steht vor einem Wendepunkt. Traditionelle Arbeitsweisen, die sich über Jahrzehnte bewährt haben, stoßen vor dem Hintergrund einer steigenden Komplexität, des Fachkräftemangels und neuer regulatorischer Vorgaben wie der Cybersecurity-Richtlinie NIS2 oder des Cyber Resilience Acts (CRA) zunehmend an ihre Grenzen. Gleichzeitig eröffnet die Digitalisierung enorme Chancen, durch Automatisierung und Standardisierung den Engineering-Aufwand zu senken und den Betrieb sicherheitsgerichteter Systeme zu vereinfachen. Um die Vorteile der Digitalisierung in der funktionalen Sicherheit vollständig zu nutzen, braucht es einen grundlegenden Wandel. Viele Prozesse, die heute noch manuell und zeitintensiv ablaufen, könnten digitalisiert und automatisiert werden. Wie das geht, zeigt HIMA mit der #safetygoesdigital-Initiative inzwischen seit zwei Jahren mit großem Erfolg. Doch da geht noch mehr!

Beispiel: Parametrierung

Ein gutes Beispiel ist die Parametrierung von Geräten. Früher richteten Ingenieure jedes neue Gerät individuell ein – ein fehleranfälliger und ressourcenintensiver Prozess. In einer digitalisierten Umgebung erkennt das Sicherheitssystem das neue Gerät automatisch, lädt die benötigten Parameter aus einer zentralen Datenbank und übernimmt die Einrichtung eigenständig. Fehler durch falsche Eingaben oder fehlende Informationen werden so vermieden.

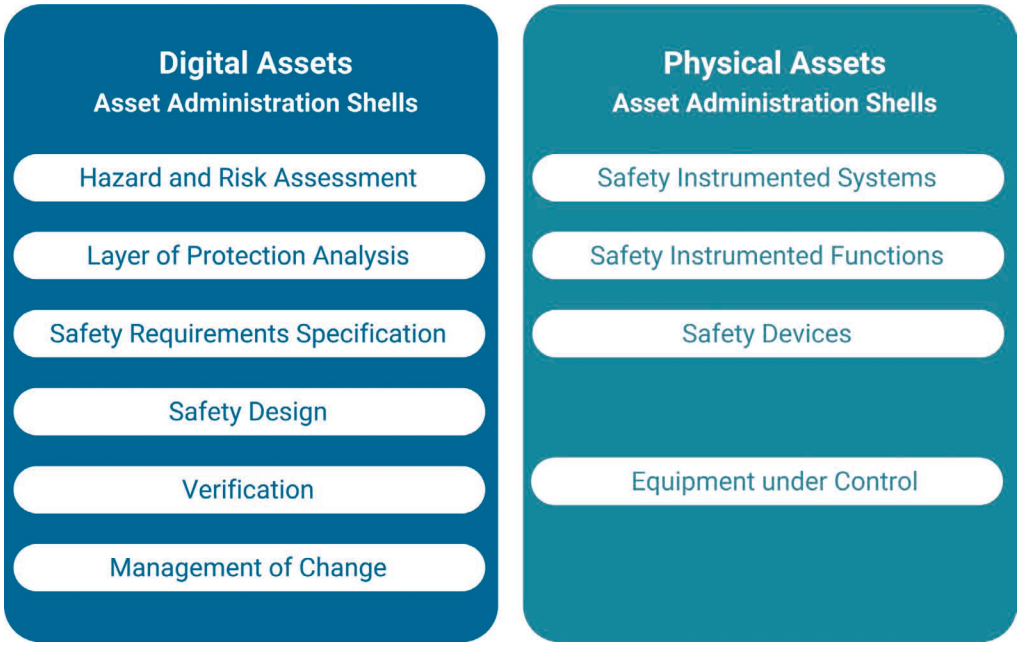
Standardisierung über die Verwaltungsschale der IDTA

Doch dieser Fortschritt erfordert eine solide Grundlage: standardisierte Datenstrukturen, die es verschiedenen Systemen und Geräten ermöglichen, nahtlos miteinander zu kommunizieren. Der Schlüssel dazu ist die Verwaltungsschale der Industrial Digital Twin Association, IDTA. Hinter dem sperrigen Begriff, der zunächst nach Amtsdeutsch klingt, verbirgt sich ein mächtiges Werkzeug, um den Informationsaustausch und die Integration in Industrie-4.0-Umgebungen zu ermöglichen. Die auch „Asset Administration Shell“ (AAS) genannte Verwaltungsschale ist ein Kernkonzept von Industrie 4.0. Die AAS fungiert als digitale Repräsentanz eines physischen Geräts (Physical Asset) aber auch als Darstellungsrahmen für Informationen (Digital Assets) und bietet eine standardisierte Plattform, auf der auch sicherheitsrelevante Daten wie Parameter, Konfigurationen und Prüfvorgaben gespeichert werden. Mit ihrer Hilfe können Geräte unterschiedlicher Hersteller problemlos in bestehende Systeme integriert werden, und das unabhängig davon, ob diese in Sicherheitsfunktionen oder für die Prozessregelung eingesetzt werden – ein entscheidender Schritt, um die Digitalisierung weiter voranzutreiben.

Standardisierte AAS für funktionale Sicherheit

Die Einführung einer standardisierten AAS für funktionale Sicherheit wird aktuell intensiv in der IDTA diskutiert – denn diese bietet nicht nur praktische Vorteile, sondern verändert die Art und Weise, wie funktionale Sicherheit umgesetzt wird, grundlegend. Prozesse, die bisher individuell und aufwändig gestaltet waren, lassen sich nun skalieren und vereinfachen. Ein Betreiber, der mehrere Standorte verwaltet, kann durch die AAS sicherstellen, dass alle seine Sicherheitssysteme auf derselben Datenbasis arbeiten.

Autor:
Peter Sieber
Vice President
of Strategic Marketing
HIMA Group
www.hima.de



Die Verwaltungsschale fungiert als digitale Repräsentanz eines physischen Geräts (Physical Asset) und als Darstellungsrahmen für Informationen (Digital Assets) und bietet eine standardisierte Plattform.
Alle Bilder © HIMA Group

Das spart Zeit und Geld und erhöht die Konsistenz und Zuverlässigkeit der Systeme.

Standardisierung macht unabhängig

Aber diese Standardisierung hat noch einen weiteren Vorteil: Sie macht die funktionale Sicherheit weniger abhängig von hochqualifizierten Fachkräften, die in vielen Unternehmen immer knapper werden. Indem Systeme so gestaltet werden, dass sie weitgehend automatisiert arbeiten und einfach zu bedienen sind, wird es möglich, den Einfluss des Fachkräftemangels zu mindern. Der demografische Wandel, der viele Branchen vor große Herausforderungen stellt, verliert so etwas von seinem Schrecken.

Neue Gefahren durch digitale Angriffsflächen

Doch wie bei jeder technologischen Neuerung gibt es auch hier Schattenseiten. Die zunehmende Digitalisierung schafft auch neue Risiken. Insbesondere Cyberangriffe stellen eine wachsende Bedrohung dar. Mit jeder Schnittstelle, die zwischen Systemen geschaffen wird, entsteht auch eine potenzielle Angriffsfläche. Und wenn im Zuge der Digitalisierung manuelle Kontrollmechanismen entfallen, steigt die Gefahr, dass Manipulationen unbemerkt bleiben. Der einseitige Blick auf die Cybersicherheit von Sicherheitssteuerungen greift dabei zu kurz, denn häufig verfolgen Hacker laterale Angriffsstrategien, bei denen sie nicht sofort das gut gesicherte Kernsystem angreifen, sondern einen weniger abgesicherten Prozess. Danach bewegen sich die Angreifer innerhalb eines Netzwerks horizontal von einem Gerät oder System zum nächsten.

Stuxnet

Ein Beispiel, das zeigt, wie kritisch diese Gefahr sein kann, ist der Stuxnet-Vorfall. Hier nutzten Angreifer Schwachstellen in einem Engineering-System, um die Parameter von Sicherheitssteuerungen zu manipulieren. Die Folge: fehlerhafte Betriebsparameter führten zu massiven Schäden in Hochgeschwindigkeitszentrifugen. Solche Szenarien verdeutlichen, dass die Digitalisierung der funktionalen Sicherheit nur dann erfolgreich sein kann, wenn Sicherheitsaspekte von Anfang an mitgedacht werden.

Mehrschichtiger Schutz der funktionalen Sicherheit

Die Antwort auf diese Bedrohungen liegt in einem ganzheitlichen Ansatz, der sowohl die Vorteile der Digitalisierung nutzt als auch die neuen Risiken kontrolliert. HIMA zeigt, wie das gelingen kann. Ein zentraler Baustein ist das Konzept der isolierten Sicherheitsumgebung. Hierbei werden Sicherheitssteuerungen von den Prozessautomationssystemen physisch und logisch getrennt, sodass ein Angriff auf die Automatisierungstechnik nicht die Sicherheitsfunktionen gefährden kann. Die Datenflüsse zwischen diesen getrennten Umgebungen erfolgen streng kontrolliert. Einwegverbindungen über Datendioden lesen Daten aus Sicherheitssystemen aus, ohne Angriffsvektoren zu schaffen. So verhindern sie, dass Angreifer über eine kompromittierte Automationsumgebung und Prozessdatenverbindungen auf sicherheitskritische Systeme zugreifen.

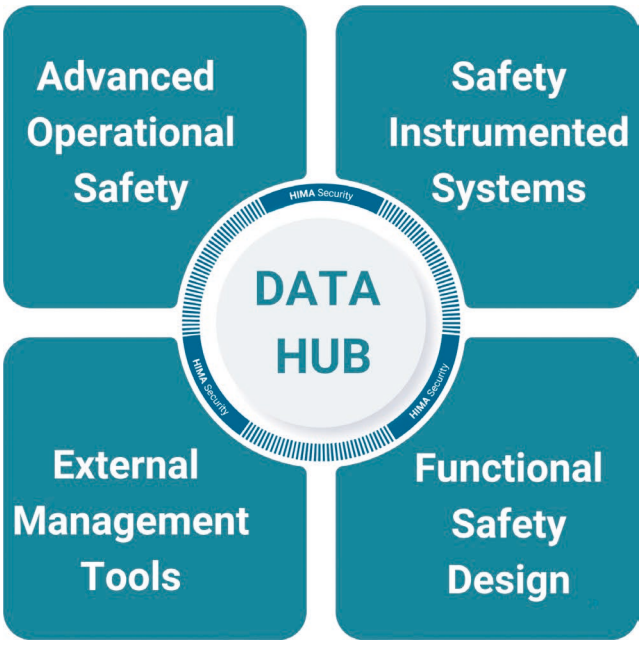
Defense in Depth

Die Digitalisierung der funktionalen Sicherheit erfordert das Erfassen und Verarbeiten von Daten aus verschiedenen Quellen wie Risikoanalysen, Sicherheitsspezifikationen und Anlagenüberprüfungen.

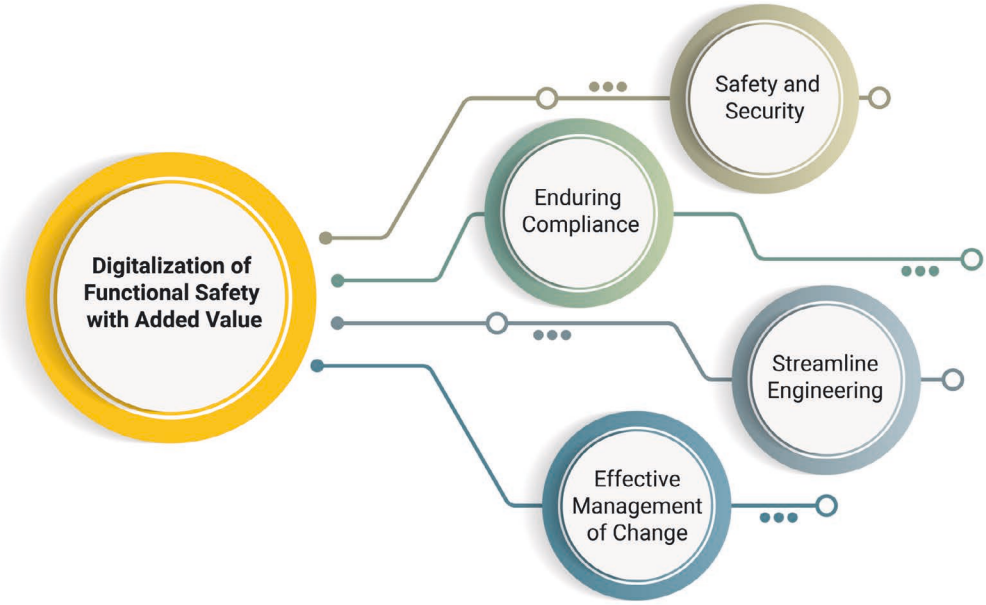
Neben der physischen und logischen Trennung der Systeme ist ein mehrschichtiger Schutzansatz, bekannt als „Defense in Depth", entscheidend, um Cyberangriffe abzuwehren. Sicherheitsmechanismen auf verschiedenen Ebenen wirken zusammen, um Angriffe zu verhindern. Netzwerksegmentierung, Endpoint-Schutz und Anomalieerkennung sind einige der Maßnahmen in modernen Sicherheitssystemen.

Datenvalidierung

Eine Schlüsselrolle spielt die Datenvalidierung. Moderne Systeme



Neben der physischen und logischen Trennung der Systeme ist ein mehrschichtiger Schutzansatz entscheidend, um Cyberangriffe abzuwehren.



Die HIMA-Strategie zur Digitalisierung der funktionalen Sicherheit mit Mehrwert basiert auf vier Kernthemen.

prüfen automatisch die Konsistenz und Integrität aller Daten, während frühere Prozesse oft auf manuelle Eingriffe vertrauten. Dies schließt Sicherheitslücken und macht die gewonnenen Informationen robuster und zuverlässiger.

Blick in die Zukunft

Die Digitalisierung der funktionalen Sicherheit hat längst begonnen: Bereits das von HIMA im Rahmen von #safetygoesdigital eingeführte digitale Management der funktionalen Sicherheit erzeugt für Anlagenbetreiber großen Nutzen. Mit der herstellerübergreifenden Standardisierung via Asset Administration Shell lassen sich die vorhandenen Potenziale leichter erschließen und der erreichbare Kundennutzen steigt. Auf diese Basis-Funktionen werden in Zukunft zusätzlich Technologien wie künstliche Intelligenz und Blockchain aufgesetzt werden, um die Sicherheit weiter zu erhöhen. KI-Systeme könnten beispielsweise genutzt werden, um Anomalien wie Cyberangriffe in Echtzeit zu erkennen und automatisch Gegenmaßnahmen einzuleiten. Blockchain hingegen kann dabei helfen, die Integrität und Nachverfolgbarkeit von Daten entlang kompletter Lieferketten – auch im Engineering – noch besser zu gewährleisten.

HIMA Group hat im Februar 2024 das Unternehmen Origo Solutions aus Norwegen übernommen. Die Fachleute dort entwickeln seit geraumer Zeit eine digitale Plattform für die Zusammenfassung unterschiedlicher industrieller Datenquellen und die Verarbeitung dieser Daten. Die daraus gewonnenen Ansätze ergänzen das in diesem Beitrag beschriebene Konzept. So entsteht eine Datendrehscheibe, die unternehmensweite Daten sammelt und aufbereitet, um die für die Digitalisierung der funktionalen Sicherheit nötigen Informationen zu generieren.

Synergien

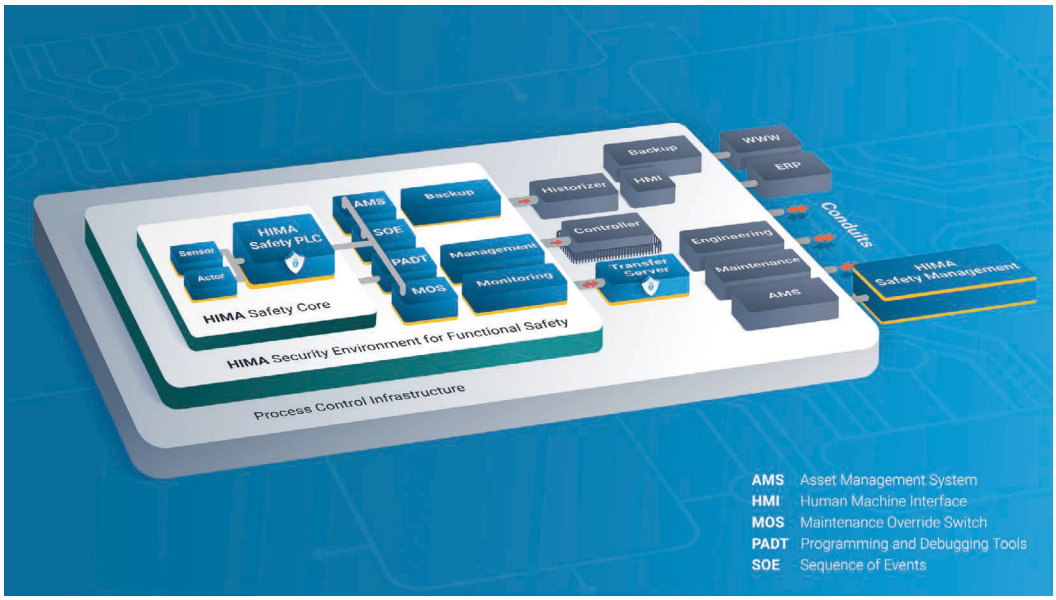
Auch die Synergien zwischen funktionaler Sicherheit und präventiver Instandhaltung werden in Zukunft stärker genutzt werden. Mechanismen, um Daten zu sammeln, die heute für Sicherheitszwecke gesammelt werden, könnten in Zukunft dazu verwendet werden, Daten über den Zustand von Anlagen zu sammeln und diese zu überwachen, so dass frühzeitig Hinweise auf mögliche Probleme geliefert werden können. Dies würde nicht nur die Sicherheit erhöhen, sondern auch die Produktivität steigern.

Fazit

Die Digitalisierung der funktionalen Sicherheit ist kein Spaziergang, hat aber enormes Potenzial. Sie ermöglicht es, die Effizienz zu steigern, die Qualität zu verbessern und den Herausforderungen von Fachkräftemangel und steigenden regulatorischen Anforderungen zu begegnen. HIMA zeigt, wie ein solcher ganzheitlicher Ansatz aussehen kann und treibt die Standardisierung aktiv voran. Durch die Kombination von Standardisierung, innovativen Sicherheitskonzepten und moderner Technologie wird es möglich, die Digitalisierung nicht nur effizient, sondern auch sicher zu gestalten. Der Weg in die Zukunft der funktionalen Sicherheit mag anspruchsvoll sein – aber er ist es wert, denn die Digitalisierung der funktionalen Sicherheit schafft Mehrwert für die Betreiber. Am Ende steht ein Gewinn, der weit über den rein wirtschaftlichen Nutzen hinausgeht: der Schutz von Menschen, Umwelt und Industrieanlagen.

Wer schreibt:

Die HIMA Group ist ein globaler unabhängiger Anbieter sicherheitsgerichteter Automatisierungslösungen für die Prozess- und Bahnindustrie zum Schutz von Menschen, Anlagen und Umwelt. Die offene und unabhängige ‚HIMA Safety Platform' vereint Hard- und Software auf einer einzigen Technologieplattform und weist ein einheitliches Security-Konzept vor. Mit mehr als 50.000 installierten Sicherheitssystemen (SIL 3 / SIL 4, PL e, CENELEC SIL 4) gilt das 1908 gegründete Familienunternehmen als Technologieführer. ◄



Das "HIMA Security Environment for Functional Safety" trennt Safety und Security.