Standardisierung mit der Verwaltungsschale

Die nächste Stufe der Digitalisierung der funktionalen Sicherheit nach Industrie 4.0-Grundsätzen

Die Digitalisierung revolutioniert die funktionale Sicherheit, doch mit den neuen Chancen kommen auch weitere Herausforderungen hinzu. Durch Standardisierung via Verwaltungsschale und innovative OT-Security-Konzepte gelingt auch der Spagat zwischen Effizienz und Cybersicherheit.

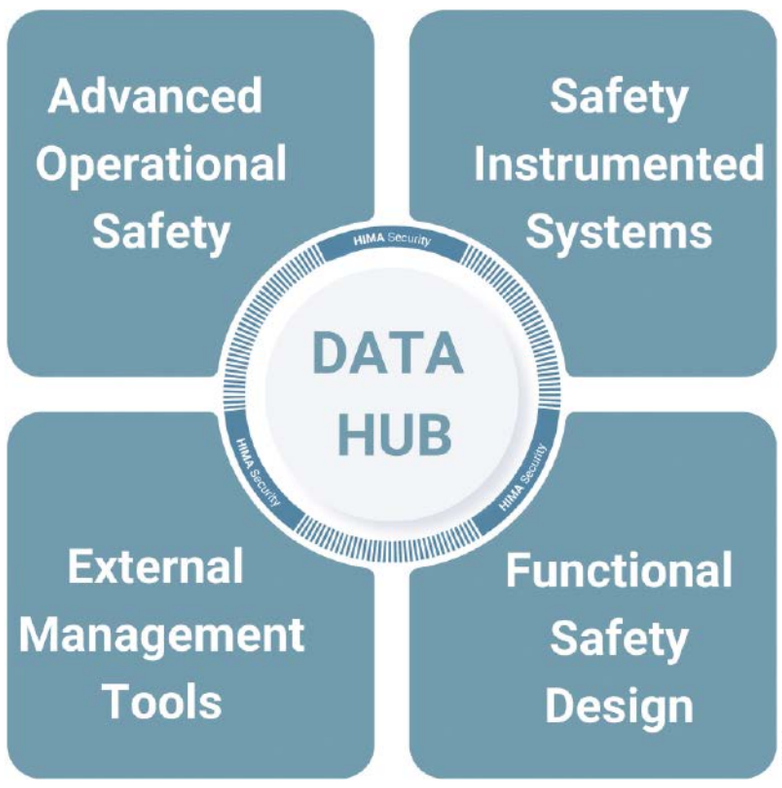
Die funktionale Sicherheit steht vor einem Wendepunkt. Traditionelle Arbeitsweisen, die sich über Jahrzehnte bewährt haben, stoßen vor dem Hintergrund einer steigenden Komplexität, des Fachkräftemangels und neuer regulatorischer Vorgaben wie der Cybersecurity-Richtlinie NIS2 oder des Cyber Resilience 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. Ein gutes Beispiel hierfür 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.

Die Anwendung der Verwaltungsschalen erschließt durch eine standardisierte Datenhaltung weiterführende Potenziale.

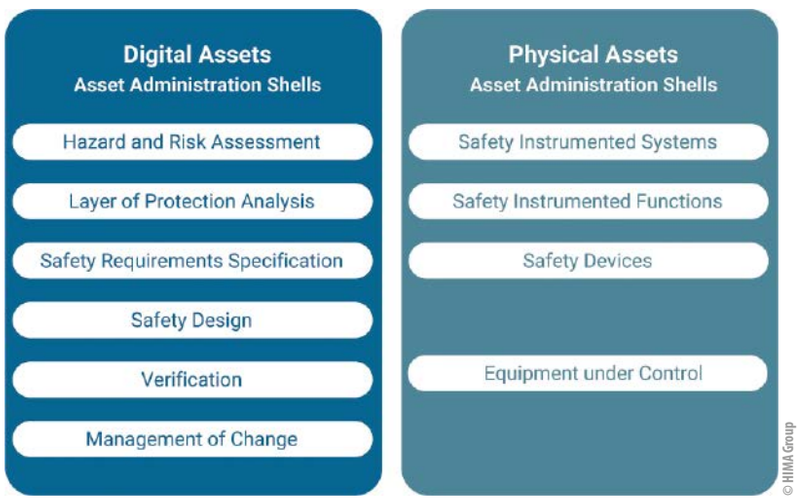
Peter Sieber, Hima

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. Sie 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.



Hima setzt auf effiziente Digitalisierung durch einen cybersicheren Data Hub. Neben der physischen und logischen Trennung der Systeme ist ein mehrschichtiger Schutzansatz entscheidend, um Cyberangriffe abzuwehren.



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

Die Einführung einer standardisierten AAS für funktionale Sicherheit wird aktuell intensiv in der IDTA diskutiert – denn sie bietet nicht nur praktische Vorteile, sondern verändert grundlegend die Art und Weise, wie funktionale Sicherheit umgesetzt wird. 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. Das spart Zeit und Geld und erhöht die Konsistenz und Zuverlässigkeit der Systeme.

Für den Bereich des Engineerings hat Hima bei verschiedenen Großprojekten Digitalisierungskonzepte umgesetzt, die keiner speziellen Tools bedurften und dennoch zu Einsparungen von 40 bis 50% der Projektaufwendungen zwischen Spezifikation und Inbetriebsetzung führten. Bisher machten diese Engineering-Prozesse eine individuelle Festlegung der anzuwendenden Datenmodelle erforderlich. Die Anwendung standardisierter Verwaltungsschalen erschließt dabei durch eine standardisierte Datenhaltung weiterführende Potenziale – sowohl im Hinblick auf die notwendigen Aufwendungen als auch im Hinblick auf die Qualität notwendiger Tests, deren Dokumentation und Archivierung.

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.

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.

Die Digitalisierung der funktionalen Sicherheit ist kein Spaziergang, hat aber enormes Potenzial.

Mehrschichtiger Sicherheitsschutz

Die Antwort auf diese Bedrohungen liegt in einem ganzheitlichen Ansatz, der sowohl die Vorteile der Digitalisierung nutzt als auch die neuen Risiken kontrolliert. Hima verfolgt 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 können.

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 (Defense in Depth) wichtig, 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.

Eine Schlüsselrolle spielt die Datenvalidierung. Während frühere Prozesse oft auf manuelle Eingriffe vertrauten, prüfen moderne Systeme automatisch die Konsistenz und Integrität aller Daten. Dies schließt Sicherheitslücken und macht die gewonnenen Informationen robuster und zuverlässiger.

Blick in die Zukunft

Das von Hima im Rahmen von #safetygoesdigital eingeführte digitale Management der funktionalen Sicherheit erzeugt für Anlagenbetreiber großen Nutzen. Mit der herstellerübergreifenden Standardisierung via AAS 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.

Fortsetzung auf **Seite 18** ▶