Whitepaper

Funktionale Sicherheit und IT-Security in der Automatisierung: eine Positionsbestimmung

Autoren:

Dr. Lutz Jänicke
CTO
Innominate Security Technologies
ljaenicke@innominate.com

Torsten Gast
Leiter Competence Center Safety
Phoenix Contact Electronics
tgast@phoenixcontact.com

Inhaltsverzeichnis

Einleitung

Sicherheit ist ein zentrales Element der Automatisierung. Dabei sind zwei wesentliche Aspekte zu betrachten: Funktionale Sicherheit (Functional Safety), die sich mit dem Schutz des Menschen vor einem technischen System befasst, und IT-Security, die sich mit dem Schutz eines technischen Systems befasst.

Dieses Dokument richtet sich an Entscheidungsträger im Unternehmen – mit dem Ziel, eingängig und anschaulich die heutigen und zukünftigen Herausforderungen und Lösungsansätze zu skizzieren.

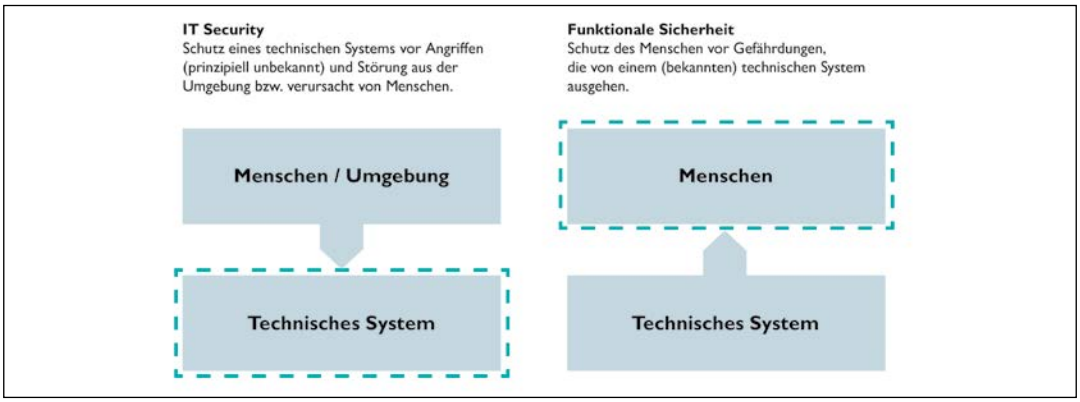

Abbildung: *IT-Security vs. Funktionale Sicherheit*

Waren Funktionale Sicherheit und IT-Security in der Vergangenheit Themen, die getrennt betrachtet werden konnten, führt die Digitalisierung und Vernetzung der Automatisierungssysteme, auch im Hinblick auf Industrie 4.0, zu wechselseitigen Abhängigkeiten.

Beiden Themen gemeinsam ist das Ziel, Sicherheit, also die Abwesenheit nicht akzeptabler Risiken, zu erreichen. Die Bewertung von Risiken ist daher ein zentraler Punkt aller Prozesse, die sich mit Sicherheitsthemen beschäftigen.

Gemeinsamkeiten und Unterschiede

IT-Security und Funktionale Sicherheit haben also viele Gemeinsamkeiten, unterscheiden sich jedoch in den meisten Details. In heutigen Anwendungen ist die Funktionale Sicherheit zumeist lokal zu betrachten, während IT-Security die Berücksichtigung externer Einflüsse erfordert. Mit der Tendenz, Funktionale Sicherheitsfunktionen und -komponenten auch mittels Netzwerkkommunikation erreichbar zu machen, öffnen sich auch neue Angriffsmöglichkeiten auf diese Funktionen.

Dabei lassen sich folgende Szenarien unterscheiden:

- **Direkte Angriffe auf sicherheitsgerichtete Kommunikation:**
  Dies erfordert aufgrund der typischen lokalen Ausprägung von Safety-Systemen zumeist einen Eingriff vor Ort.
- **Angriffe auf Sicherheitssteuerungen:**
  Diese sind zur Programmierung oder Überwachung über Netzwerke erreichbar.
- **Angriffe auf die Programmierumgebungen, mit denen die Sicherheitssysteme konfiguriert und parametriert werden:**
  Zumeist laufen diese Umgebungen heute auf gängigen Office-Systemen, die keine spezielle Security-Härtung erfahren.

Die Frage, wie IT-Security und Funktionale Sicherheit in diesem Zusammenhang gemeinsam zu bewerten sind, wird aktuell weltweit in Gremien diskutiert.

Funktionale Sicherheit

Der Schutz des Menschen vor den Gefahren von Maschinen ist ein wichtiges Ziel der staatlichen Behörden, Organisationen und Verbände. Entsprechend gibt es in vielen Ländern gesetzliche Vorschriften, die für Maschinenhersteller und Maschinenbetreiber bindend sind. Je nach Land unterscheiden sie sich aber bezüglich der Höhe der Sicherheitsanforderungen sowie hinsichtlich der Zielgruppen, also nach Herstellern, Systemintegratoren, Automatisierern oder Betreibern von Maschinen sind. So muss jeder, der eine Maschine in einem Land in den Verkehr bringt, sich vorab über die lokalen Gesetzmäßigkeiten informieren.

Im Europäischen Wirtschaftsraum (EWR) gibt es einheitliche Richtlinien, die in den jeweiligen Ländern (zum Beispiel Italien, Österreich, Deutschland) eins zu eins übernommen werden müssen. So findet sich in der 9. Produktverordnung die Maschinenrichtlinie wieder. Über das Produktsicherheitsgesetz ist die Umsetzung der Anforderungen aus der Richtlinie bindend.

Die Maschinenrichtlinie (1) gibt Sicherheits- und Schutzanforderungen für die Herstellung von Maschinen vor. Eine Konkretisierung der Anforderungen finden sich in den über 700 harmonisierten Normen (siehe EU-Amtsblatt auf www.europa.eu). Eine wichtige Anforderung aus der Maschinenrichtlinie ist, dass für jede Maschine zum Zeitpunkt der Konstruktion eine Risikobeurteilung durchgeführt werden muss. Dazu müssen neben den Grenzen der Maschine auch alle möglichen auftretenden Gefährdungen in den jeweiligen Lebensphasen erfasst und beurteilt werden. Sollte für eine Gefährdung der Risikofaktor (bestehend aus Schwere, Wahrscheinlichkeit und Möglichkeit der Vermeidung) höher sein als erlaubt, so muss der Maschinenhersteller risikomindernde Maßnahmen durchführen. Hier gilt die restriktive Vorgabe, erst konstruktive, dann technische und (falls noch ein zu hohes Restrisiko besteht) hinweisende Maßnahmen durchzuführen.

Sollten technische Maßnahmen umgesetzt werden müssen, so spricht man von Maßnahmen der Funktionalen Sicherheit. Die Anforderungen der Funktionalen Sicherheit finden sich in den harmonisierten technischen Normen, zum Beispiel der EN ISO 13849-1 (2), EN 62061 (3) oder EN 61511 (4) wieder. Diese Normen beschreiben für den Maschinenbau sowie für verfahrenstechnische Anlagen die Anforderung zum Erreichen der Funktionalen Sicherheit. Diese wird dann ausgedrückt über den Sicherheitslevel oder auch Sicherheits-Integritätslevel. Je nach Norm spricht man dann von einem Performance Level (EN ISO 13849-1) oder SIL (EN 62061). Für verfahrenstechnische Anlagen kann die EN 61511 angewendet werden, die durch die VDI/VDE2180 (5) ergänzt wird.

Der Maschinenhersteller bestätigt abschließend mit der Konformitätserklärung und dem Anbringen des CE-Zeichens die Konformität zur Maschinenrichtlinie und kann anschließend die Maschine auf dem europäischen Markt in den Verkehr bringen. Er bescheinigt damit, alle Vorgaben der Maschinenrichtlinie eingehalten bzw. umgesetzt zu haben. Weiterhin muss er dann auch weitere Richtlinien beachten (EMV-Richtlinie, ATEX-Richtlinie etc.).

Für den Betreiber gelten beim Einsatz einer richtlinienkonformen Maschine weitere für das jeweilige Land gültige Anforderungen an die Arbeitssicherheit. In Deutschland ist dies das Arbeitsschutzgesetz mit der Anforderungsumsetzung in der Betriebssicherheitsverordnung.

Die Hersteller von sicheren Schaltgeräten, sicheren Komponenten wie auch sicheren Steuerungen müssen ebenfalls die Anforderungen der Maschinenrichtlinie (CE-Zeichen auf den jeweiligen Geräten) einhalten. Um zusätzlich internationalen Anforderungen zu genügen, wird die IEC 61508 (6) bei vielen Herstellern angewendet. Diese Norm wendet sich speziell an die Hersteller von elektrischen, elektronischen und programmierbaren elektronischen (E/E/PE) Systemen, die eine Sicherheitsfunktion ausführen. Dabei macht die Norm umfangreiche Anforderungen, beginnend mit dem Functional Safety Management bis hin zur Ausfallwahrscheinlichkeitsberechnung für die einzelnen Komponenten. Anforderungen an eine Hardware-Entwicklung finden sich dort genauso wieder wie die an eine sichere Firmware und Software-Oberfläche.

Die Sicherheitsgerätehersteller weisen auf ihren technischen Unterlagen aber auch den Sicherheitsnachweis nach den Anwendungsnormen EN ISO 13849-1, EN 62061 oder EN 61511 aus, um den Maschinen- oder Systemintegratoren den Einsatz ihrer Komponenten und Systeme in die Gesamtmaschine zu erleichtern. So kann dann direkt das jeweilige Produkt in den Sicherheitsnachweis der jeweiligen Sicherheitskette eingerechnet werden.

IT-Security

Grundsätzlich ist die Umsetzung von IT-Security-Maßnahmen in der Automatisierung nicht gesetzlich geregelt. Während der Schutz des Menschen und der Umwelt aus den gesellschaftlichen Grundzielen ableitbar ist und somit gesetzliche Eingriffe rechtfertigt, dienen Security-Maßnahmen in erster Linie wirtschaftlichen Zielen und unterliegen damit der wirtschaftlichen Freiheit unternehmerischer Entscheidung. Gesellschaftliche Interessen sind dann berührt, wenn zum Beispiel die Versorgungssicherheit gefährdet ist und Regulierung mit dem Ziel der Daseinsvorsorge notwendig wird. Ein erster Schritt in diese Richtung ist das IT-Sicherheitsgesetz (7), das Anforderungen für bestimmte Branchen aufstellt, die aus der Nationalen Strategie zum Schutz Kritischer Infrastrukturen abgeleitet sind. Dabei sind die Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit für die betriebenen Kritischen Infrastrukturen zu erfüllen. Diese Anforderungen wurden jedoch noch nicht in spezifische, prüfbare Normen umgesetzt. Eine entsprechende, im Gesetz referenzierte Rechtsverordnung ist noch nicht veröffentlicht. Es ist davon auszugehen, dass die Rechtsverordnung auf den Aufbau und die Umsetzung eines Information Security Management Systems nach ISO 27000 (8) zielen wird. Die einzelnen Branchenverbände haben dabei die Möglichkeit, branchenspezifische Sicherheitsstandards entsprechend dem Stand der Technik vorzuschlagen. Insofern werden sich konkrete Anforderungen im Bereich der Automatisierung noch entwickeln müssen. Auf europäischer Ebene ist zu diesem Thema in naher Zukunft eine entsprechende Richtlinie zur Netz- und Informationssicherheit (9) zu erwarten.

Vorgehen

Auch im Bereich der IT-Security wird die Betrachtung mit einer Risiko- und Bedrohungsanalyse begonnen. Hierbei ist jedoch zu beachten, dass die Bedrohungen von Menschen oder Organisationen ausgehen, deren Motivation und Fähigkeiten eine quantitative Einschätzung erschweren. Die verschiedenen Normen haben hier Ansätze, in denen Motivation und Fähigkeiten in Klassen eingeteilt werden. Die daraus folgende Festlegung eines Schutzbedarfs anhand dieses Kriterienkatalogs lässt daher Interpretationsspielraum.

Im Bereich der Funktionalen Sicherheit werden die Standardfunktion und die Sicherheitsfunktion häufig komplett getrennt realisiert, um Einflussfaktoren fehlerbehafteter Standardfunktionen auf die Integrität der Sicherheitsfunktion weitestgehend zu minimieren. Im Bereich der IT-Security ist dies nicht möglich, da relevante Angriffe auch an dieser Stelle erfolgen können. Ein entsprechend aufwändiger Entwicklungsprozess etwa nach Common Criteria wird daher in der Praxis nur in den wenigsten Anwendungen betrieben.

Ein weiteres Merkmal der IT-Security ist die Frage, wie ein sicherer Zustand im Fehlerfall festgelegt werden sollte. Für die Schutzziele Vertraulichkeit und Integrität ist eine Abschaltung des Betriebs im Fehlerfall denkbar, führt aber sofort in Konflikt mit dem Schutzziel Verfügbarkeit. Insbesondere in der Automatisierung ist die Verfügbarkeit ein wichtiges Schutzziel.

Eine besondere Herausforderung ist die Behandlung von Schwachstellen. Für alle nicht-trivialen Systeme ist davon auszugehen, dass Fehler in Implementierungen oder Protokollen existieren. Angreifer suchen mit immer neuen Methoden aktiv nach entsprechenden Schwachstellen, die im Bereich der Funktionalen Sicherheit als systematische Fehler betrachtet würden. In der IT-Security ist daher davon auszugehen, dass ein System mit Bekanntwerden einer Schwachstelle, die als systematischer Fehler schon lange vorhanden war, plötzlich als unsicher erscheint und

Gegenmaßnahmen ergriffen werden müssen. IT-Security ist insofern ein „Moving Target“ und erfordert eine ständige Neubewertung der Bedrohungslage.

Grundsätzlich ist davon auszugehen, dass die Wahrscheinlichkeit des Eintritts eines IT-Security-Vorfalls in den verschiedenen Einsatzszenarien deutlich höher sein dürfte als das Versagen einer Einrichtung der Funktionalen Sicherheit. Detektions- und Reaktionsfähigkeiten gehören daher in der IT-Notfallplanung zum Standard.

Office-Anwendungen und Automatisierung

Grundsätzlich sind Security-Maßnahmen in Rechenzentren und Büroumgebungen schon viel länger etabliert. Die meisten dieser Maßnahmen lassen sich jedoch aus vielfältigen Gründen schwer auf die Automatisierung übertragen. Viele dieser Maßnahmen zielen auf menschenbediente Systeme, bei denen ein vorübergehender Ausfall tolerierbar ist. Auch sind entsprechende Systeme unter der Kontrolle der IT-Organisation und werden regelmäßig aktualisiert oder ausgetauscht. In der Automatisierung werden auch kurze Ausfälle nicht akzeptiert. Die Lebensdauer von Installationen richtet sich nach der technischen Lebensdauer des physikalischen Systems, die erheblich länger ist als der typische Innovationszyklus der IT-Industrie. Zudem hat der Betreiber nicht die Kontrolle über die IT-Systeme in den Automatisierungskomponenten, sondern ist auf den Automatisierungsanbieter angewiesen. Hintergrund ist, dass der Anbieter Aktualisierungen vor der Freigabe auf Rückwirkungsfreiheit hinsichtlich der Automatisierungsfunktion testen muss.

Standards

Die ISO 2700x Normreihe (8) beschreibt ein Information Security Management System, das den generellen Konzepten eines Managementsystems wie ISO 9000 für Qualitätsmanagement oder ISO 31000 für Risikomanagement folgt. Es richtet sich daher an Organisationen und Prozesse. Ausprägungen für spezifische Branchen entstehen, etwa für die Energieversorgung nach ISO/IEC TR 27019:2013 (10). Details der technischen Umsetzung werden dann in anderen Normen, wie der IEC 62351 (11), behandelt.

In der industriellen Automatisierungstechnik haben sich verschiedene Ansätze herausgebildet. In Deutschland wurde die VDI/VDE 2182 (12) erarbeitet, die unter anderem das abgestimmte Vorgehen zwischen Anbietern, Integratoren und Betreibern beschreibt. Auf internationaler Ebene wurde, ausgehend von der US-amerikanischen Initiative ISA 99, die Ausarbeitung der IEC 62443 (13) begonnen, die bereits weit fortgeschritten ist. Die IEC 62443 besteht aus verschiedenen Teilen, die sich wiederum an Betreiber, Integratoren und Anbieter richten. Hinsichtlich der Betreiberebene wird ein Information Security Management System eingeführt, das in aktuellen Versionen der Norm nicht zur ISO 2700x-Reihe abgestimmt ist, eine Umstellung auf ISO 2700x ist aber in Arbeit. Für Produkte verwendet die IEC 62443 Security Level (SL-1 bis SL-4), die zusammen mit dem Reifegrad des Betreibers einen bewertbaren Protection Level (PL) ergeben sollen. Die Diskussionen hierzu sind jedoch noch nicht abgeschlossen. Grundsätzlich scheint die IEC 62443 aktuell bei den beteiligten Parteien von Betreiber bis Anbieter eine große Akzeptanz zu finden.

Eine Sonderrolle nimmt die kürzlich veröffentlichte NAMUR-Empfehlung NE 153 (14) ein, deren Ziel es ist, kurze und konkrete Anforderungen für zukünftige Automatisierungslösungen mit Schwerpunkt in der Prozessindustrie zu benennen, ohne die umfassenden Konzepte einer IEC 62443 abzudecken.

Einen guten Überblick zum Thema Security in der Automation bieten auch die Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) (15) (16).

Die Common Criteria nach ISO/IEC 15408 (17) zielen speziell auf Security-Produkte. In der Methodik der Common Criteria werden Schutzziele definiert, deren Einhaltung entsprechend einer Prüftiefe (Evaluation Assurance Level, EAL-1 bis EAL-7) validiert wird. Die Schutzziele bauen dabei aufeinander auf, um eine sinnvolle Abdeckung von Themen zu erreichen. Die notwendige Prüftiefe muss aus den Fähigkeiten der Angreifer abgeleitet werden und reicht je nach Stufe von

einer Prüfung der Benutzerdokumentation über Design-Reviews bis zum Beweis der Korrektheit – sofern dies überhaupt möglich ist. Zu beachten ist hierbei, dass nur die Kombination aus Schutzzielen und Prüftiefe, das Schutzprofil, aussagekräftig ist. Vorhandene Schutzprofile zielen auf Produkte wie Smart Cards, die Gesundheitskarte, das deutsche Smart Meter Gateway. Schutzprofile für Firewalls und VPN-Gateways existieren, werden aber nur von wenigen Produkten angewendet. Generell ist zu beobachten, dass die Common Criteria mit den verbundenen Kosten und Einschränkungen nur im regulierten Umfeld zum Einsatz kommen. Ein weiteres, grundsätzliches Problem ist die Inflexibilität, da bei jeder Änderung am Produkt eine aufwendige und insbesondere zeitintensive Rezertifizierung notwendig ist, die im Widerspruch zur notwendigen schnellen Reaktion auf sich ändernde Security-Herausforderungen steht.

Anforderungen an Industrie 4.0

Mit der Digitalisierung und Vernetzung eröffnen sich neue, zum Teil noch nicht vorhersehbare Möglichkeiten. Gleichzeitig steigt jedoch die Bedrohung aus Sicht der IT-Security. Die Steigerung des Security-Niveaus ist daher ein elementarer Bestandteil der Bemühungen in entsprechenden weltweiten Initiativen, zum Beispiel der Plattform Industrie 4.0. In der Umsetzungsstrategie (18) wird dem Thema Sicherheit ein eigener Abschnitt gewidmet.

Die Erreichung der gewünschten, unternehmensübergreifenden Vernetzung bringt verschiedene Herausforderungen mit sich:

- In Industrie 4.0 werden viele Partner in Echtzeit zusammenarbeiten: Hersteller und Anwender, Lieferanten, Dienstleister und Betreiber. Die Trennung der unterschiedlichen Kommunikationsdomänen der beteiligten Partner wird aufgeweicht, sodass zwischen ihnen Vertrauensbeziehungen aufgebaut werden müssen. Daten und Informationen sollen zwischen diesen Partnern ausgetauscht werden, wozu gemeinsame Security-Niveaus vereinbart werden müssen. Aktuell existieren noch keine Modelle, wie Bewertungsverfahren zu Security-Niveaus aussehen könnten.
- Arbeiten Menschen und Maschinen verschiedener Parteien zusammen, müssen Zugriffsverfahren und -rechte aufeinander abgestimmt werden. Hierzu müssen sich die Kommunikationspartner gegenseitig mittels geeigneter, sicherer Identitäten authentifizieren und autorisieren können. Modelle für unternehmensübergreifende, sichere Identifikation und Rollen werden hierzu notwendig.
- Der Austausch von Daten wird über Firmen- und Landesgrenzen hinweg erfolgen. Hierzu sind rechtliche Rahmenbedingungen notwendig, die zum Beispiel das Eigentumsrecht an Daten betreffen. Auch bestehen große, weltweite Unterschiede in der gesetzlichen Behandlung verschlüsselter Kommunikation, die für sicheren Datenaustausch notwendig ist. Die Einbindung der deutschen Politik ist über die Plattform Industrie 4.0 sichergestellt.
- Durch die intelligente Produktion ergibt sich die Anforderung, Maschinen produktionstechnisch kurzfristig umzustellen, umzubauen oder anzupassen. Diese Vorhaben dürfen nicht im Widerspruch zur Funktionalen Sicherheit stehen. Systeme und Modelle, die dieses unter anderem auch in Bezug auf die Überprüfung der Funktionalen Sicherheit unterstützen, müssen definiert und beschrieben werden.

Der richtige Partner auf dem Weg zu Industrie 4.0

Für den Kunden ist eine ganzheitliche Betrachtung der Automatisierungsaufgabe bedeutend. Die Themen Funktionale Sicherheit und IT-Security zeigen von der Anforderungsseite her Überschneidungspunkte, die es kundenspezifisch zu analysieren und in ein gesamtheitliches Konzept umzusetzen gilt. Anschließend stellt sich die Frage der Umsetzung und der anschließenden Überprüfung (Verifikation und Validierung). Zusätzlich muss das eigene Personal informiert, eingewiesen und geschult werden. Ein durchgängiger Aufbau von Know-how ist notwendig, wobei sich gerade im Bereich der IT-Security ständig neue Anforderungen und Bedrohungen ergeben.

Um diesen Aufgaben gerecht zu werden, muss der richtige Partner für die Umsetzung verschiedene Kompetenzen besitzen.

Branchenspezifisches Know-how

Die Ausprägungen der spezifischen Anforderungen an Funktionale Sicherheit und IT-Security unterscheiden sich in den Branchen. Insofern ist langfristig erworbene Erfahrung in den verschiedenen Branchen notwendig, um die geeigneten Produkte, Lösungen und Dienstleistungen anbieten zu können. Durch die Mitwirkung in Branchenverbänden und Standardisierung kann der Stand der Technik weiterentwickelt und gleichzeitig die Aktualität des Portfolios sichergestellt werden.

Angepasstes Produkt- und Lösungsportfolio

Das Produkt- und Lösungsportfolio von Phoenix Contact umfasst eine Vielzahl spezifischer Produkte zu den Themen Funktionale Sicherheit und IT-Security. Im Bereich der Funktionalen Sicherheit erstreckt sich das Portfolio von Sicherheitsrelais über konfigurierbare Sicherheitslösungen bis zu zentralen Sicherheitssteuerungen. Im Bereich der IT-Security stehen mit der mGuard-Produktfamilie Lösungen für Netzwerksicherheit und sichere Fernwartung auf aktuellem Stand der Technik zur Verfügung.

Dienstleistungsportfolio

Um Kunden optimal bei der Umsetzung ihrer Automatisierungsprojekte unterstützen zu können, ist ein umfassendes Portfolio an themenbezogenen Dienstleistungen notwendig:

Mit Schulungsprogrammen wird ein optimaler Einstieg in die Themen Funktionale Sicherheit und IT-Security geboten. Für die Umsetzung von Kundenprojekten ist dann eine maßgeschneiderte Beratung notwendig.

Mit spezifischer Beratung unterstützt Phoenix Contact seine Kunden in den Projekten. Das Dienstleistungsangebot im Bereich Funktionale Sicherheit ist dabei seit vielen Jahren bewährt. Im Bereich IT-Security wird das verfügbare Angebot weiter ausgebaut.

Aktive Weiterentwicklung

IT-Security, die bisher nicht im Fokus der Automatisierungsanwender stand, muss in der kommenden Welt der Industrie 4.0 im Sinne eines „Security by Design“ von Anfang an berücksichtigt werden. Für die Umsetzung müssen zukünftig IT-Security-Eigenschaften in allen Prozessen und Produkten und Lösungen auf aktuellem Stand der Technik abgebildet werden. Phoenix Contact ist hier führend in Organisationen und Gremien unterwegs.

Mit einem Partner, die neben den passenden Produkten und Lösungen auch ein umfangreiches Dienstleistungsportfolio aufzeigen kann, bewegt sich der Kunde auf der Zielgerade zur Industrie 4.0.

Literaturverzeichnis

1. RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG. Maschinenrichtlinie.
2. Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen. ISO 13849.
3. Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme. IEC 62061.
4. Functional safety – Safety instrumented systems for the process industry sector. IEC 61511.
5. Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT). VDI/VDE 2180.
6. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. IEC 61508.
7. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. IT Sicherheitsgesetz. 2015.
8. Information technology – Security Techniques – Information Security Management System. ISO/IEC 27000:2014.
9. RICHTLINIE ZUR NETZ- UND INFORMATIONSSICHERHEIT (in Beratung). NIS-RL.
10. Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. ISO/IEC TR 27019:2013.
11. Information Security for Power System Control Operations. IEC 62351.
12. Informationssicherheit in der industriellen Automatisierung. VDI/VDE 2182.
13. Industrial Communication Networks – Network and System Security. IEC 62443.
14. Automation Security 2020 – Anforderungen an Design, Implementierung und Betrieb künftiger industrieller Automatiseirungssysteme. NAMUR NE153.
15. ICS Security Kompendium. Bonn: BSI, 2013.
16. Empfehlungen für Hersteller von Komponenten. Bonn: BSI, 2014.
17. Common Criteria for Information Technology Security Evaluation. ISO/IEC 15408.
18. Umsetzungsstrategie Industrie 4.0. Berlin/Frankfurt: Plattform Industrie 4.0, 2015.

PHOENIX CONTACT

Phoenix Contact ist weltweiter Marktführer für Komponenten, Systeme und Lösungen im Bereich der Elektrotechnik, Elektronik und Automation.

Produziert wird mit hoher Fertigungstiefe, wobei nicht nur Schrauben, Kunststoff- und Metallteile, sondern auch hochautomatisierte Montagemaschinen selbst gebaut werden. Das Produktspektrum umfasst Komponenten und Systemlösungen für die Energieversorgung inklusive Wind- und Solar, den Geräte- und Maschinenbau sowie den Schaltschrankbau.

Ein vielfältiges Programm von Reihen- und Sonderklemmen, Printklemmen und Steckverbindern, Kabelanschlusstechnik und Installationszubehör bietet innovative Komponenten. Elektronische Interfaces und Stromversorgungen, Automatisierungssysteme auf Basis von Ethernet und Wireless, Sicherheitslösungen für Mensch, Maschine und Daten, Überspannungsschutz-Systeme sowie Software-Programme und -Tools bieten Errichtern und Betreibern von Anlagen sowie Geräteherstellern umfassende Systeme.

Die Märkte der Automobilindustrie, regenerativer Energien und der Infrastruktur werden durch ganzheitliche Lösungskonzepte inklusive Engineering-, Service- und Trainingsleistungen gemäß ihrer spezifischen Bedürfnisse betreut. In Entwicklungsbereichen an den Standorten in Deutschland, China und den USA entstehen Produktinnovationen und spezifische Lösungen für individuelle Kundenwünsche. Zahlreiche Patente unterstreichen, dass viele Entwicklungen von Phoenix Contact einzigartig sind. In enger Zusammenarbeit mit Hochschule und Wissenschaft werden Zukunftstechnologien wie Elektromobilität und Umwelttechnologien erforscht und in marktgerechte Produkte, Systeme und Lösungen überführt.

PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Deutschland
Tel.: +49 (0) 52 35 3-00
Fax: +49 (0) 52 35 3-4 12 00
phoenixcontact.net