Das Magazin der Automatisierungstechnik
Ausgabe 02/03 2017

atp plus

Erfolgsfaktor Daten

Wie Smart Services die Produktivität steigern

DIV
Deutscher Industrieverlag

Cyber Security für funktionale Sicherheit – „NA 163"-Verfahren bietet praxistaugliche Risiko-Beurteilungsmethode

Erwin Kruschitz

PLT-Sicherheitseinrichtungen (Safety Integrated Systems, SIS) schützen Anlagen, Umwelt und Personal der chemischen Industrie vor nicht tolerierbaren Schäden. Die Integrität der PLT-Sicherheitseinrichtungen ist neuerdings Gefährdungen aus dem Cyberraum ausgesetzt. Risikoanalysen bilden den ersten Schritt in Richtung Gegenmaßnahmen. Standards wie IEC 61508 / 61511 tragen dieser Erkenntnis Rechnung und fordern IT-Risikobeurteilungen mit entsprechenden Maßnahmen. Detaillierungsgrad, Methode, Zeitpunkt, Zuständigkeit und Umfang werden jedoch nicht näher beschrieben. Der Interpretationsspielraum ist dementsprechend hoch. Die NAMUR hat mit dem NAMUR Arbeitsblatt 163 ein Handlungswerkzeug geschaffen, das eine effektive und ressourcenschonende IT-Risikobeurteilung ermöglicht. Darüber hinaus werden konkrete Handlungsmaßnahmen anhand einer Checkliste formuliert.

1. Rechtliche Rahmenbedingungen

Im Zusammenhang mit Funktionaler Sicherheit fordern gesetzliche Rahmenbedingungen die Einhaltung des „Stand der Technik". IEC 61511 ist ein wesentlicher Indikator für den Stand der Technik und schreibt neuerdings die Durchführung einer IT-Risikobeurteilung für PLT-Sicherheitseinrichtungen vor. Wie man bei einer Risikobeurteilung vorgeht, beschreiben weiterhin VDI/VDE 2182, IEC 62443 3-2 (Entwurf) und ISO/IEC 27005. Die dort beschriebenen Methoden sind jedoch nicht auf PLT-Sicherheitssysteme und Safety-Ingenieure zugeschnitten und eignen sich nur bedingt dazu, die Forderungen der IEC 61511 zu erfüllen.

2. Wie "secure" ist die Safety?

PLT-Sicherheitseinrichtungen (Safety Instrumented Systems) unterscheiden sich technisch kaum von konventionellen Automatisierungssystemen. Die technischen Vorkehrungen zur Wahrung der Integrität (SIL-Level) der Systeme wirken primär gegen zufällige Fehler und weniger gegen bewusste Manipulation. Vielfach wird argumentiert, dass das PLT-Sicherheitssystem nicht mit Netzwerken verbunden ist und entsprechend weniger exponiert sei als andere Systeme. In der Praxis findet man jedoch häufig Verbindungen zu betrieblichen Automatisierungssystemen (z. B. Prozessleitsystemen) und in manchen Fällen auch Visualisierungs-, Erstwertmelde-, oder Alarmierungssystemen. Insbesondere die Verbindungen zu Programmiergeräten - auch Handheld-Geräte zur Sensor-Aktor-Konfiguration - bilden Schnittstellen nach „außen". Applikationsprogramme und Konfigurationsdaten durchlaufen verschiedene IT-Umgebungen bei Systemherstellern, -integratoren und Wartungsabteilungen bevor diese in ein PLT-Sicherheitssystem eingespielt werden.

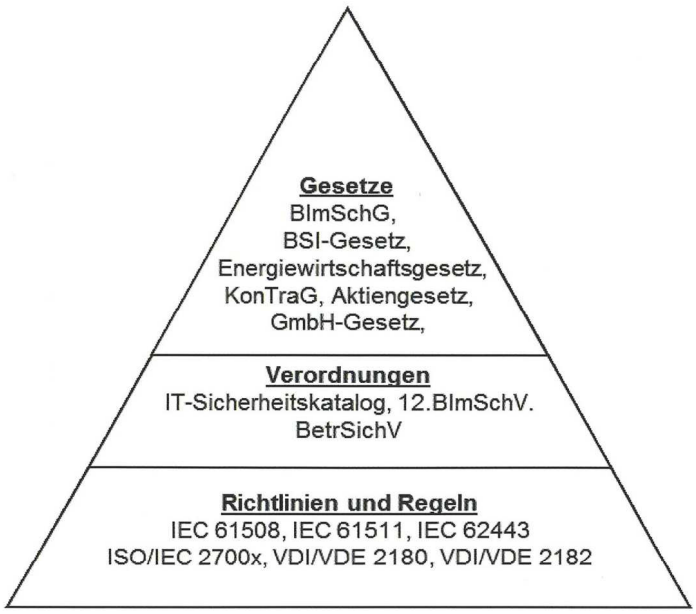

Bild 1: Gesetze, Verordnungen, Richtlinien und Regeln.

Zusammengefasst kann gesagt werden, dass einem PLT-Sicherheitssystem kein viel besseres aber auch kein schlechteres Security-Niveau beigemessen werden kann als einem konventionellen Automatisierungssystem.

3. PLT-Sicherheitseinrichtungen brauchen besonderes Augenmerk

Trotz vergleichbarer Exposition und gleichem Bedrohungspotenzial wird der PLT-Schutzeinrichtung besonderes Augenmerk gewidmet. Der Grund dafür liegt in der potenziellen Auswirkung einer kompromittierten Schutzeinrichtung auf Gesundheit, Umwelt und letztlich die Reputation des Betreibers.

Agieren die Systeme unabhängig, getrennt und rückwirkungsfrei voneinander, muss bei der Risikoanalyse für das konventionelle Automatisierungssystem nicht von einem potenziellen Schaden für die Sicherheit von Gesundheit oder Umwelt ausgegangen werden. Dieser Umstand kann es auch aus Kostenaspekten heraus sinnvoll erscheinen lassen, mehr in die Security des PLT-Sicherheitssystems zu investieren, um beim üblicherweise umfangreicheren konventionellen Automatisierungssystem keine so hohen Maßnahmen mehr ergreifen zu müssen. Bedingung dafür ist die Rückwirkungsfreiheit der beiden Systeme - auch dann, wenn eines der beiden Systeme kompromittiert wurde.

4. Der Begriff „Risiko“

Die Fragen, die bei Risikobeurteilungen beantwortet werden sollten sind im Wesentlichen:

- Wie sicher (secure) ist meine PLT-Schutzeinrichtung?
- Wie sicher muss sie - mindestens - sein?

„Risiko“ wird klassisch als Produkt aus der Schwere der negativen Auswirkung und der Eintrittswahrscheinlichkeit gebildet. Der im Informationssicherheitsmanagement verwendete Risikobegriff geht davon aus, dass ein Risiko erst dann eintritt, wenn eine Bedrohung auf eine passende Schwachstelle trifft. Für die Kombination aus Schwachstelle und Bedrohung wird eine Eintrittswahrscheinlichkeit festgelegt. Die Abschätzung der Eintrittswahrscheinlichkeit erweist sich als problematisch. Erstens liegt einem Cybersecurity-Risiko im Normalfall ein systematischer Fehler bzw. Mutwilligkeit zugrunde und belastbares Zahlenmaterial über Zwischenfälle ist nicht verfügbar. Zum zweiten werden PLT-Sicherheitseinrichtungen der chemischen Industrie fast ausschließlich mit der Anforderungsrate „niedrig“ betrieben. Der Anforderungsfall ist relativ selten. Für die Ermittlung von Risiken sind neben ausgewiesenem Expertenwissen auch die erforderlichen Kapazitäten notwendig. Beide Ressourcen – Kompetenz und Kapazität – sind in der Regel knapp bemessen.

Das „NA 163“-Verfahren der NAMUR wurde entwickelt, um diese knappen Ressourcen optimal einzusetzen. Die ersten dreieinhalb Schritte des Risikobeurteilungsverfahrens nach IEC 62443-3-2 wurden durch den NAMUR AK 4.18 anhand einer in der Prozessindustrie üblichen Systemkonfiguration durchgeführt (s. Bild 2). Das Team, das die individuelle Risikobeurteilung für die einzelne PLT-Sicherheitseinrichtung durchführt, kann sich demnach auf die letzten zwei Schritte beschränken.

5. Ziele des „NA 163“-Verfahrens

Ziel des Arbeitsblattes ist die Bereitstellung einer praxistauglichen Risiko-Beurteilungsmethode für PLT-Ingenieure. Die Besonderheit: Die Durchführung des „NA 163“-Verfahrens ist pro System innerhalb eines Tages und ohne tiefere Cyber-Security-Kenntnisse durchführbar. Vorhandene Schwachstellen werden aufgedeckt und konkrete Verbesserungsmaßnahmen anhand einer Checkliste vorgeschlagen. Mit dem NAMUR-Arbeitsblatt soll die Eintrittsschwelle in IT-Risikobeurteilungen gesenkt werden. Die Beurteilungen

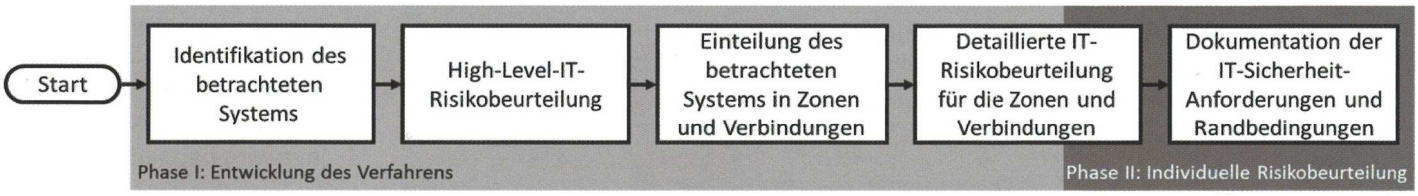

Bild 2: Die Schritte des Risikobeurteilungsverfahrens.

sollen selbstverständlicher Teil des Lebenszyklus einer PLT-Sicherheitseinrichtung werden.

6. Umfang der PLT-Sicherheitseinrichtung aus Security-Sicht

Beginnt man mit einer IT-Risikobeurteilung für PLT-Sicherheitseinrichtungen, stellt sich zu allererst die Frage, welche Komponenten zur PLT-Sicherheitseinrichtung gehören und welche nicht. Sensoren, Aktoren und die programmierbare Steuerung bilden den Kern der PLT-Sicherheitseinrichtung (Zone A, s. Bild 3). Aber auch das Programmiergerät und die Konfigurationseinrichtungen für Sensoren und Aktoren beeinflussen die Sicherheitsfunktion. Datenverbindungen zu Systemen im Umfeld der PLT-Sicherheitseinrichtung müssen betrachtet werden (Zone B). Dienste wie der Verzeichnisdienst zur Regelung des Benutzerzugriffs, Update-Dienste für Virenpattern und Betriebssystem-Updates, Zeitsynchronisation und Sicherung/Wiederherstellung sind für die Security der PLT-Sicherheitseinrichtung relevant und damit im Betrachtungsumfang (befinden sich üblicherweise in der Umgebung). Auch die Integrität von Daten (z. B. Applikationsprogramm, Risiko-Analysen, Anlagendokumentation) spielt zusammen mit der Organisation und Personen eine Rolle und wird entsprechend auf Risiken beurteilt. Gegenstand der Risikoanalyse sind also Komponenten (zumindest Zone A und B), Datenverbindungen, Dienste sowie Prozesse und Personen rund um die PLT-Sicherheitseinrichtung.

7. Schutzziele

Security verfolgt im Kern die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Die funktionale Sicherheit zielt primär auf die Integrität der PLT-Sicherheitseinrichtung ab. D. h. Integrität von Sensor, Aktor und Sicherheits-SPS ist oberstes Schutzziel. Aus betrieblicher Sicht ist natürlich die Verfügbarkeit dieser Komponenten gleichfalls relevant, da das (unnötige) Auslösen der PLT-Sicherheitseinrichtung in den meisten Fällen einen Betriebsstillstand verursacht.

Auf den ersten Blick erscheint die Vertraulichkeit der Daten rund um ein PLT-Sicherheitssystem nicht relevant. Aus der Perspektive eines Angreifers sind für eine wirkungsvolle Manipulation der PLT-Schutzeinrichtung die Kenntnis von Anlagendokumentation, Risikoanalyse und die Dokumentation der PLT-Schutzeinrichtung sehr hilfreich. Insofern sind auch Vertraulichkeitsaspekte zu berücksichtigen.

8. Die wichtigsten Prinzipien bei der Umsetzung im Überblick:

8.1 Prinzip Simplizität

Um Komponenten schützen zu können, ist die Kenntnis der Komponenten und deren Funktionszweck zwingende Voraussetzung. Im Rahmen der IT-Risikobeurteilung werden sowohl Hard- als auch Softwarekomponenten erfasst und deren Einsatzzweck dokumentiert. Hierfür sind entsprechende Rollen, Rechte und effektive Authentifizierungsverfahren erforderlich. Je weniger Komponenten die PLT-Sicherheitseinrichtung enthält, desto weniger Sicherheitsmaßnahmen werden notwendig sein, um diese zu schützen. Diesem Prinzip folgend ist die Verringerung von Verbindungen, Hard- und Softwarekomponenten und Personen mit Zugriff auf das absolut notwendige Minimum die erste und effizienteste Maßnahme.

8.2 Prinzip Kompetenz

IT-Sicherheitsaspekte müssen in der Planung, der Beschaffung, der Validierung, im Betrieb und in der Außerbetriebnahme berücksichtigt werden.

So sollte während der Spezifikationsphase einer PLT-Sicherheitseinrichtung eine initiale IT-Risikobeurteilung vorgenommen werden. Die Wirksamkeit der durchgeführten Maßnahmen sollte bei der Validierung überprüft werden. Im laufenden Betrieb werden Änderungen auf Security-Risiken hin überprüft. Das Lagebild zur allgemeinen IT-Sicherheitslage wird beobachtet.

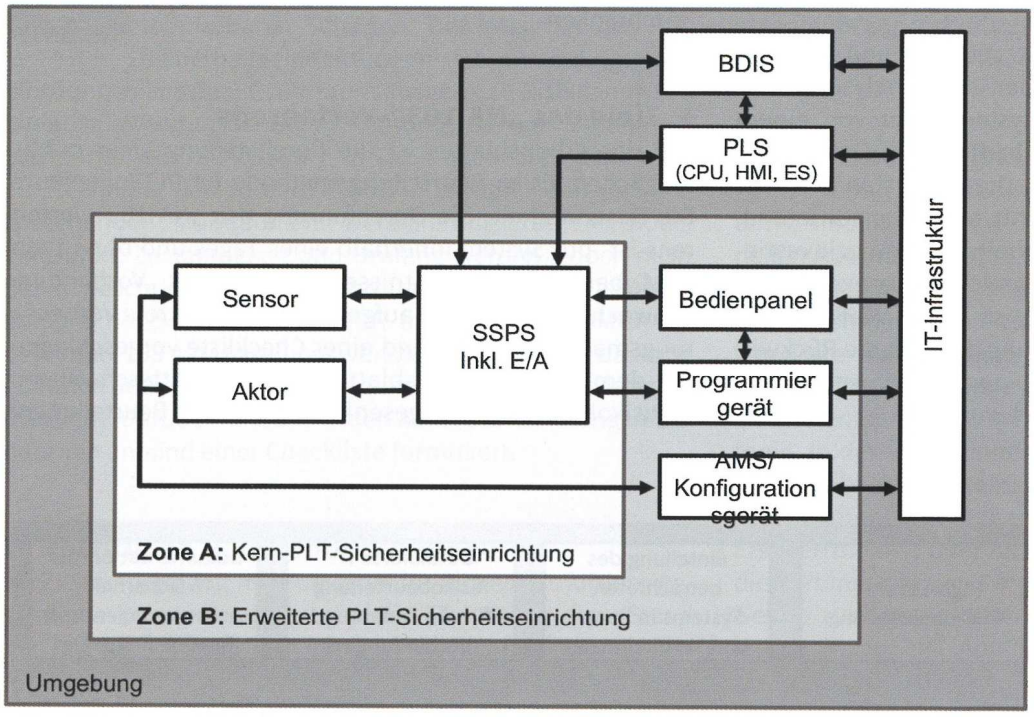

Bild 3: Das Zonenmodell nach NAMUR NA163.

Eine IT-Risikobeurteilung sollte regelmäßig, mindestens aber alle 5 Jahre wiederholt werden sowie obligatorisch sein:

- nach jeder umfangreichen Änderung sowie
- nach IT-Sicherheitsereignissen.

Die Kompetenz der Organisationen und Personen, die eine PLT-Sicherheitseinrichtung planen, implementieren, betreiben oder warten, muss der Komplexität der Einrichtung gewachsen sein.

Grundbaustein für Kompetenz ist die Kenntnis und Dokumentation der Systemkomponenten (Hard- und Software inkl. Versionsstände, Daten und Personen mit Zugang und/oder Zugriff, Verbindungen) sowie deren Konfiguration (Applikationsprogramme, Firewall-Regeln, Sensor-Aktor-Konfiguration, Bus-Konfiguration etc.).

Daten entstehen während des gesamten Lebenszyklus und werden an vielen Orten erzeugt und gespeichert. Manche Daten bestimmen direkt die Integrität der PLT-Sicherheitseinrichtung, andere Daten stehen in einem indirekten Zusammenhang mit der Integrität der PLT-Sicherheitseinrichtung. Daten sollen entsprechend ihrer Relevanz klassifiziert werden. Je nach erfolgter Klassifizierung werden Maßnahmen zum Schutz vor Manipulation veranlasst.

8.3 Prinzip Trennung und Unabhängigkeit

Nach IEC 61508 / 61511 sollen PLT-Sicherheitseinrichtungen getrennt und damit unabhängig und rückwirkungsfrei von ihrer Umgebung (z. B. Prozessleitsystem, IT-Infrastruktur etc.) betrieben werden. In der Praxis ist dies insbesondere für Programmiergeräte und Konfigurationsdaten kaum einzuhalten.

Insbesondere Sicherheitsmaßnahmen wie Verzeichnisdienst, Zeitsynchronisation, Betriebssystemupdates, Firewall-Management, Event-Monitoring werden nicht exklusiv für das PLT-Sicherheitssystem betrieben („gemeinsam genutzte Komponenten"). Unter „gemeinsam genutzt" wird hier die Kombination von „Sicherheits-„ und „betrieblichen" Funktionen innerhalb einer Komponente verstanden. Der Umgang mit diesen Komponenten muss einen entsprechend hohen Grad an Zuverlässigkeit aufweisen, um möglichst geringe Rückwirkungen anderer Systeme auf das PLT-Sicherheitssystem zu gewährleisten.

Für den Umgang mit gemeinsam genutzten Komponenten kommen drei Lösungswege in Frage: Entweder ist die Komponente im Management-System der Funktionalen Sicherheit eingebettet oder es wird der Nachweis erbracht, dass eine nach IEC 61508 oder IEC 61511 und unter Gesichtspunkten der IT-Sicherheit hinreichende Trennung und Unabhängigkeit zwischen dem „sicheren" Teil der Komponente und dem „betrieblichen" liegt. Ferner besteht die Möglichkeit, in einer IT-Risikobeurteilung schriftlich zu dokumentieren, dass die gemeinsame Nutzung von Komponenten zu keinen nicht tolerierbaren IT-Sicherheitsrisiken für die PLT-Sicherheitseinrichtung führt.

9. Durchführung der IT-Risikobeurteilung

Grundsätzlich ist der Betreiber einer PLT-Sicherheitseinrichtung für die IT-Sicherheit – und damit auch für die Durchführung einer IT-Risikobeurteilung – verantwortlich.

Für die Durchführung des Verfahrens zur Risikobeurteilung sollte die durchführende Person mindestens über Grundkenntnisse der IT-Sicherheit verfügen. Ob die Durchführung durch unternehmensinterne Mitarbeiter oder externe Dienstleister erfolgt, hängt im Wesentlichen von der Verfügbarkeit von Ressourcen ab. Entscheidet sich der Betreiber für das Hinzuziehen eines externen Dienstleisters, müssen Leistungsumfang (Art und Umfang der Dokumentation) und Verantwortlichkeiten festgelegt werden.

Das System muss technisch und organisatorisch den Regeln für PLT-Sicherheitseinrichtungen (z. B. IEC 61511) entsprechen. Sofern bereits in der Vergangenheit eine IT-Risikobeurteilung durchgeführt wurde, muss überprüft werden, ob alle wichtigen festgelegten Maßnahmen der letzten Überprüfung umgesetzt worden sind.

Über den Verlauf und das Ergebnis der IT-Risikobeurteilung wird ein Bericht erstellt. Dieser enthält die eindeutige Identifikation des begutachtenden Systems, den Namen der beurteilenden Personen, das Datum sowie eine ausführliche Dokumentation des Ergebnisses.

10. Ausblick

Die Einführung des Verfahrens nach NA 163 ist ein erster Schritt. Jede durchgeführte Sicherheitsanalyse und jedes Security-Ereignis bringen Erkenntnisse zutage, die das Verfahren verbessern werden. Das Bewusstsein bei Herstellern,

Identifikation des Betrachtungsgegenstandes	Systemarchitektur	Maßnahmen für Engineering Station, Field Entry Panel, AMS	Daten	Protokolle & Verbindungen	Organisation, Personen und Prozesse
•Erfassung Hardware-Komponenten •Erfassung Software-Komponenten •Erfassung Daten •Erfassung Verbindungen •Erfassung Organisationsstrukturen	•Zonenkonzept •Trennung und Unabhängigkeit •Zugangs- und Zugriffsschutz •Härtung	•Erfassung Komponenten •Software-Komponenten •Logiksystem	•Konfigurationsdaten •Externe Daten •Sicherung von Daten •Anwendungsprogramm	•Sicherung der Verbindungen •Sicherheitsbeurteilung des Kommunikationspartners •Physische Sicherung	•Sensibilisierung, Schulung •IT-Security-Management •Planung und Spezifikation •Recovery & Business Continuity

Bild 4: Übersicht der Bausteine Checkliste zur IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen.

Betreibern und Gesetzgebern über die Relevanz der Thematik steigt. IT-Risikobeurteilungen werden sich zum „täglichen Brot" des Automatisierungsingenieurs entwickeln. Sie helfen dabei, Maßnahmen zielgerichtet, d. h. dort, wo die größten Risiken auftreten, umzusetzen. Für die Zukunft reift die Erkenntnis, dass die Sicherheit bereits bei der Entwicklung und Integration einer PLT-Sicherheitseinrichtung viel stärker berücksichtigt werden muss. Aus Sicht der chemischen Industrie sollen zukünftige Generationen von PLT-Sicherheitseinrichtungen bereits „Security by Design" (d. h. Security ab Werk) mitbringen. Die Anzahl der zur Sicherung notwendigen Zusatzmaßnahmen kann damit minimiert und Risikobeurteilung stark vereinfacht werden.

Referenzen

[1] ICS-Security-Kompendium (2013), Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html

[2] ICS-Security-Kompendium für Hersteller und Integratoren (2014), Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html

[3] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Version 1.1, 2015), BDEW Bundesverband der Energie- und Wasserwirtschaft e.V, https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm=300010055020

[4] Ausführungshinweise zur Anwendung des Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Version 1.1, 2014), BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. und Oesterreichs E-Wirtschaft, https://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge?open&ccm=300010055020

[5] ISO/IEC TR 27019:2013: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, Internationale Organisation für Normung (ISO), http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759

[6] IEC 61508-1:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, International Electrotechnical Commission (IEC), https://webstore.iec.ch/publication/22273

[7] IEC 61511-1:2016: Functional safety - Safety instrumented systems for the process industry sector, International Electrotechnical Commission (IEC), https://webstore.iec.ch/publication/5527

[8] IEC 62443-2-1:2010: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC), https://webstore.iec.ch/publication/7030

[9] IEC 62443-2-4:2015: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers , International Electrotechnical Commission (IEC), https://webstore.iec.ch/publication/22810

[10] IEC 62443-4-1:ENTWURF: Security for industrial automation and control systems - Technical security requirements for IACS components - Part 4-1: Secure product development life-cycle requirements , International Electrotechnical Commission (IEC)

[11] IEC 62443-4-2:ENTWURF: Technical security requirements for IACS components - Part 4-2: Technical security requirements for IACS components, International Electrotechnical Commission (IEC)

[12] Richtlinie VDI/VDE 2180 Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)

[13] Richtlinie VDI/VDE 2182 Blatt 1 „Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell"

[14] Richtlinie VDI/VDE 2182 Blatt 2.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber - Presswerk"

[15] Richtlinie VDI/VDE 2182 Blatt 3.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber - LDPE-Anlage"

[16] NIST Special Publication 800-82, Revision 2: Guide to Industrial Control Systems (ICS) Security (2015), National Institute of Standards and Technology (NIST) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdfie

Erwin Kruschitz
Namur AK 4.18 Automation Security und Vorstand
anapur AG
67227 Frankenthal
Tel. +49 6233 8803930
info@anapur.de

Erwin Kruschitz
Mitglied im Namur AK 4.18 Automation Security und Vorstand der anapur AG

> Für ein schnelles Ankommen ist eine zuverlässige Bremse genauso wichtig wie ein starker Motor.

Die Digitalisierung ist zum grundlegenden Innovationstreiber geworden. Um auf rasche Veränderungen des Marktes reagieren zu können, ist eine anpassungsfähige, flexible, modulare, vernetzende IT- und Automatisierungs-Infrastruktur dringend notwendig. Anpassungsfähigkeit, Flexibilität, Vernetzung und Modernität bringt aber unweigerlich Volatilität und Komplexität mit sich. D. h. Unternehmen, die sich für die Zukunft erfolgreich aufstellen wollen, müssen ihre Exposition gegenüber unbekannten Risiken erhöhen.

Kurz gefasst: „Wer nicht wagt, der nicht gewinnt".

Damit das Wagnis nicht zur Existenzbedrohung wird, muss die Wirksamkeit der Sicherheitsmaßnahmen gewährleistet sein. Security und Safety sind „Enabler" für die Digitalisierung.