ZVEI:
Die Elektroindustrie

Orientierungsleitfaden für Hersteller zur IEC 62443

Fachverband Automation

Impressum

Orientierungsleitfaden für Hersteller zur IEC 62443

Herausgeber:
ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Fachverband Automation
Lyoner Straße 9
60528 Frankfurt am Main

Verantwortlich:
Gunther Koschnick
Telefon: +49 69 6302-318
Fax: +49 69 6302-279
E-Mail: koschnick@zvei.org
www.zvei.org

Erstellt von:
Koramis GmbH
Europaallee 5
66113 Saarbrücken

Redaktion:
Lenkungskreis Automation Security

April 2017

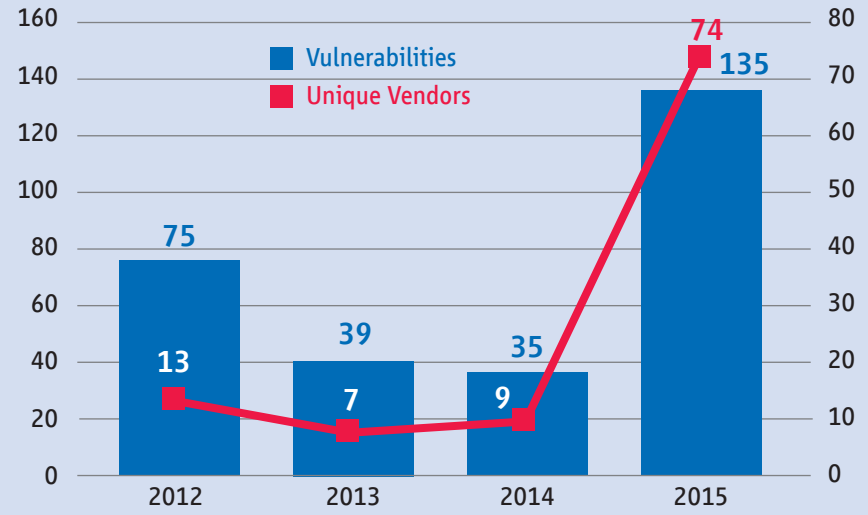
Inhalt

1. Einleitung und Motivation

Der ZVEI vertritt als einer der wichtigsten Industrieverbände Deutschlands die Interessen der Hightechbranche Elektroindustrie. Auf letztere kommen durch die allgemeinen technologischen Entwicklungen sowie durch neue regulatorische Anforderungen und Schlüsselthemen wie Industrie 4.0 und Internet der Dinge besondere Herausforderungen, aber auch Chancen mit Blick auf das Thema Industrial Security von Produkten und Prozessen zu.

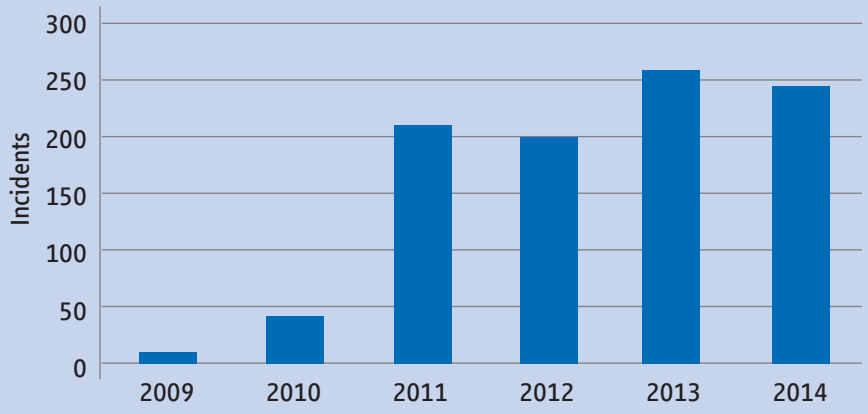
Industrielle Automatisierungskomponenten und -systeme werden in vielfältigen Anwendungen der Fertigungs- und Prozessautomation eingesetzt. Dazu gehören auch kritische Anwendungen im Bereich der Energieerzeugung und -verteilung, Wasserversorgung und -entsorgung bis hin zur Logistik und der Verkehrsleittechnik. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befasst sich seit einigen Jahren mit dem Thema Industrial Security und insbesondere mit kritischen Infrastrukturen (Kritis). In diesem Zusammenhang beobachtet und bewertet das BSI kontinuierlich die Bedrohungslage der Fertigungs- und Prozessindustrie. In regelmäßigen Abständen werden die „Top 10-Bedrohungen für Industriesteuerungsanlagen" veröffentlicht [BSI_ICS]. Im Ergebnis dieser und anderer Übersichten, beispielsweise von den Firmen Symantec [Sym16] oder Kaspersky [Kas16], kann der Industrie ein zunehmendes Risikopotenzial bescheinigt werden.

Abb. 1: Vulnerabilities in industriellen Steuerungssystemen



Quelle: ZVEI / [Sym16]

Abb. 2: ICS/SCADA Cyber Security Incidents



Quelle: ZVEI / [Eni16]

Industrieanlagen stehen im Visier aktueller Sabotage- und Spionageangriffe.

Betreiber, nicht nur von Kritis-Anwendungen, fragen infolgedessen zunehmend nach Industrial Security bei den Lieferanten nach. Auch lassen sich zunehmend Industrial-Security-Anforderungen in den Lastenheften finden. Das hat zur Folge, dass der Druck auf die herstellende Industrie nach und nach größer wird. Verstärkt wird das Ganze durch politische Bestrebungen, Industrial Security bei Gerätezulassungen bzw. Zertifizierungen zu etablieren. Auf europäischer Ebene nimmt hierzu Frankreich eine Vorreiterrolle ein [Eni16]. Auf internationaler Ebene haben die Underwriters Laboratories mit der UL2900-2-2 [UL29] eine Spezifikation erarbeitet, die nachprüfbare Kriterien für die Industrial Security von netzwerkfähigen Produkten und Systemen definiert. Anhand der Kriterien können Softwareschwachstellen beurteilt, deren Ausnutzung minimiert, bekannte Schadsoftware bekämpft und Sicherheitsmechanismen überprüft werden. In Deutschland wurde 2016 die erste Zertifizierung nach der internationalen Norm IEC 62443 vorgenommen [TÜVSüd]. Diese Norm legt den Grundstein für eine ganzheitliche Betrachtung von Industrial Security im gesamten Lebenszyklus von Automatisierungslösungen.

2016 wurden erste Zertifikate für industrielle Komponenten und den dazugehörigen Entwicklungslebenszyklus von einer unabhängigen Institution ausgestellt. Die IEC 62443 spielt dabei eine zentrale Rolle.

Mit diesem Leitfaden werden ZVEI-Mitglieder in die Lage versetzt, sich mit aktuell geltenden normativen Anforderungen sowie internationalen Gesetzgebungen zum Thema Industrial Security auseinanderzusetzen. Aufgrund der Vielzahl an Normungsinstitutionen (z. B. IEC, IEEE, ISA) und ihrer zunehmend branchenspezifischen Orientierung wird sich in diesem Leitfaden auf die IEC 62443 beschränkt. Weitere Anforderungs- oder Richtliniendokumente wie die ISO 27001/27019, Common Criteria (ISO IEC 15408), VDI/VDE Richtlinie 2182 und Namur NE 153 flossen jedoch mit ein.

Im Bereich der industriellen Automatisierung hat sich die branchenunabhängige Norm IEC 62443 etabliert. Sie kann als Grundnorm angesehen werden, ähnlich der IEC 61508 für den Bereich der funktionalen Sicherheit. Mit dem Erscheinen der Edition 2 der IEC 61508-1 besteht sogar ein direkter Zusammenhang beider Normen.

7.5.2 Requirements
7.5.2.2 If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements. NOTE Guidance is given in IEC 62443 series.

Quelle: IEC 61508-1:2010

Durch diesen Zusammenhang wird klar, dass bei der Einhaltung der funktionalen Sicherheit immer auch Aspekte der IT-Sicherheit betrachtet werden müssen. Funktionale Sicherheit setzt demnach immer ein gewisses Maß an Industrial Security voraus.

Des Weiteren wird seitens der EU an Richtlinien zur Gewährleistung der IT-Sicherheit gearbeitet. Die EU-Richtlinie „Network and Information Security" [Nis16] ist kürzlich erschienen. Zur Umsetzung der Richtlinie wird in naher Zukunft eine Liste harmonisierter Normen erwartet. Die Anwendung einer dieser Normen kann dann zur Konformitätsvermutung herangezogen werden.

Ob die IEC 62443 mit ihrem Charakter einer Grundnorm in die Liste harmonisierter Normen aufgenommen werden wird, ist derzeit unklar. Im Vergleich zur Maschinenrichtlinie ist die Grundnorm zur funktionalen Sicherheit, die IEC 61508, nicht Bestandteil der Liste harmonisierter Normen. Vielmehr sind auf Basis dieser Grundnorm branchenspezifische Produkt- oder Produktgruppennormen gelistet (z. B. IEC 62061, IEC 61511, IEC 61513, ISO 26262).

Der Inhalt des Leitfadens gliedert sich wie folgt:

- Abschnitt 2 geht auf regulatorische und normative Anforderungen hinsichtlich der Informationssicherheit ein.
- Abschnitt 3 geht direkt auf die IEC-62443-Familie ein und bildet damit den Schwerpunkt dieser Arbeit. Im Fokus stehen Anforderungen aus Sicht des Herstellers von Automatisierungslösungen.
- Abschnitt 4 geht exemplarisch auf Anforderungen der IEC 62443 ein und zeigt ebenso exemplarisch Umsetzungsbeispiele, wie Hersteller der Norm gerecht werden können.

2. Übersicht relevanter Anforderungen für Herstellerunternehmen

2.1 Regulatorische Anforderungen

2.1.1 EU-Direktive

Die EU-Richtlinie NIS definiert derzeit den aktuellen Stand regulatorischer Anforderungen. NIS beschreibt Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union. Sie richtet folgende Anforderungen an die Mitgliedstaaten:

- Formulierung einer nationalen Strategie für Cybersicherheit
- Anforderungen an Betreiber aus den Bereichen (siehe Annex II NIS):
  - Energie (Strom, Gas, Öl)
  - Transport (Luft, Bahn, Wasser, Straße)
  - Banken und Finanzwirtschaft
  - Gesundheitswesen
  - Trinkwasserversorgung
  - Digitale Infrastruktur
- Etablierung eines „single point of contact“
- Etablierung einer „national competent authority“
- Einrichtung eines „Computer security incident response teams (CSIRTs)“, das mit dem CSIRT auf EU-Ebene zusammenarbeiten muss

Die EU-Richtlinie wurde am 6. Juli 2016 veröffentlicht und mit dem IT-Sicherheitsgesetz in nationales Recht umgesetzt.

Mit der NIS-Richtlinie wird das Thema „Netzwerk und Informationssicherheit“ europaweit reguliert. Es ist eine Frage der Zeit, dass eine Liste harmonisierter Normen erstellt wird. Die ISO 27001, ISO 27019 sowie die IEC 62443 könnten dabei eine zentrale Rolle spielen.

2.1.2 IT-Sicherheitsgesetz

Im Kern geht es beim nationalen IT-Sicherheitsgesetz um die Absicherung Kritischer Infrastrukturen, kurz Kritis. Kritische Infrastrukturen[1] im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die:

- den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
- von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Um eine zielgerichtete Umsetzung in den einzelnen Branchen zu ermöglichen, heißt es im § 8a (Sicherheit in der Informationstechnik Kritischer Infrastrukturen): „(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen.“ Die Energiebranche hat dies mit der Veröffentlichung der ISO 27019 bereits getan. Weitere werden folgen.

Weiter heißt es im § 8a: „(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.“ Spätestens bei der Meldung von Sicherheitsmängeln in Automatisierungskomponenten an die zentrale Meldestelle des BSI (eigens für diesen Zweck eingerichtet) kommt der Hersteller ins Spiel. Im § 8a heißt es: „(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Infrastrukturen führen können oder geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden.“

Sofern bei einem Kritis-Betreiber meldepflichtige Störungen der IT auftreten, darf das BSI erforderlichenfalls auch die Hersteller der entsprechenden IT-Produkte und -systeme gemäß § 8b BSIG zur Mitwirkung verpflichten. Dem BSI wird nach § 7a die Befugnis eingeräumt, zur Wahrnehmung seiner Aufgaben nach § 3 Absatz 1 S. 2 Nr. 1, 14 und 17 BSIG IT-Produkte auf ihre Sicherheit hin zu untersuchen.

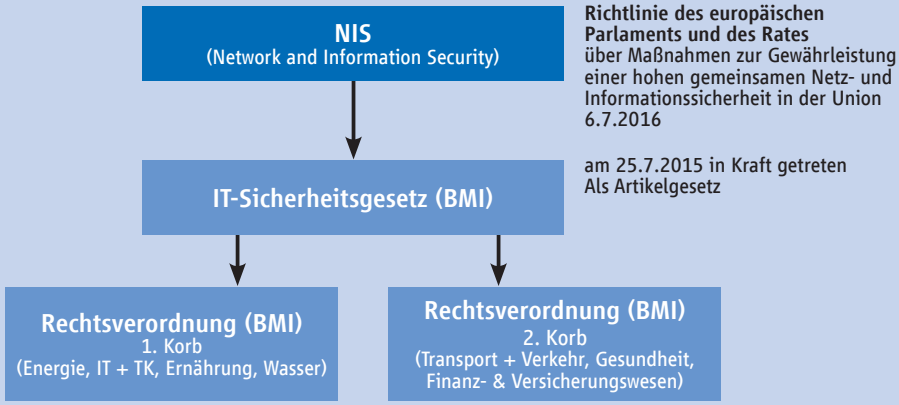
[1] Kritische Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

Anhand dieser Vorgehensweise sollte jeder Hersteller von Kritis-Komponenten das Ziel verfolgen, Industrial-Security-Anforderungen bereits beim Produktdesign, der Implementierung und Fertigung zu berücksichtigen.

Durch das TMG und TKG werden implizit Hersteller angesprochen, die neben Produkten der industriellen Automatisierung auch Kommunikationslösungen herstellen bzw. vertreiben.

Abb. 3: EU-Direktive NIS und Abhängigkeiten

Die NIS Directive wird durch das IT-Sicherheitsgesetz in nationales Recht umgesetzt. Die Umsetzung muss bis 2018 erfolgen.



Für Korb 1 in Kraft seit 3.5.2016

Quelle: ZVEI

Da das IT-Sicherheitsgesetz ein Artikelgesetz ist, werden auch bestehende Regelungen in anderen Gesetzen geändert, um die oben genannten Ziele zu erreichen. Telemedien-Diensteanbieter sind durch Änderungen in § 13 TMG (Telemediengesetz) dazu verpflichtet, präventive technische und organisatorische Maßnahmen nach Stand der Technik zum Schutz der Systeme und der darauf aufbewahrten Daten zu treffen. Es gilt dabei vor allem, diese nachzuweisen. Ferner gab es Änderungen im Telekommunikationsgesetz (TKG), um einen besseren Schutz der Bürgerinnen und Bürger zu erreichen. Telekommunikationsanbieter werden dazu verpflichtet:

- IT-Sicherheitsmaßnahmen nach dem „Stand der Technik" nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur einzusetzen und zu erhalten (§ 109 Absätze 1 und 2 TKG),
- ihre Nutzer über Schadprogramme und ihre Erkennung und Beseitigung zu informieren (§ 109a Absatz 4 TKG) und
- erhebliche IT-Störungen zu melden (§ 109 Absatz 5 TKG).

2.1.3 Weitere regulatorische Anforderungen

EU-Ebene: Richtlinie zum Schutz von vertraulichem Know-how und Geschäftsgeheimnissen (Trade-Secret-Directive): Diese Richtlinie wurde zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung verabschiedet. Die Richtlinie wurde am 15. Juni 2016 im Amtsblatt der Europäischen Union veröffentlicht und trat ab 5. Juli 2016 – mit einer zweijährigen Umsetzungsfrist für die EU-Mitgliedstaaten – in Kraft.

Know-how-Schutz ist ein wichtiger Aspekt in der Industrieautomation. Insbesondere Hersteller sollten ihr Wissen in Bezug auf Design, Implementierung, Qualitätssicherung und Fertigung ihrer Lösungen schützen.

Nationale Ebene: Neben den internationalen Vorschriften gibt es für den Bereich der Informationssicherheit weitere nationale Spezialvorschriften, die insbesondere für

Hersteller relevant sind:

- Produkthaftungsgesetz (ProdHaftG, Produkt muss bekannten Standards entsprechen)
- Bürgerliches Gesetzbuch (BGB, § 823 hinsichtlich Softwarekauf)
- Urheberrechtsgesetz (UrhG, § 2 Geschützte Werke – dazu gehören auch Computerprogramme – sowie § 69a-g Besondere Bestimmungen für Computerprogramme)
- Strafgesetzbuch (StGB, IT-bezogene Straftaten)

Das StGB ist branchenunabhängig. Das bisherige Verständnis, dass sich das StGB allein auf die Office-Welt bezieht, ist durch den bereits bestehenden hohen Grad der Digitalisierung und Vernetzung innerhalb der industriellen Automation nicht mehr gegeben. Insbesondere bei cloudbasierten Anwendungen stellt sich heute bereits die Frage, in welchem Rechtsraum sich die Daten befinden. Dabei spielt eine Rolle, um welche Daten es sich handelt und welches Schutzbedürfnis sie besitzen.

Tabelle 1: Unterschiede in den Anforderungen zwischen Office- und Industrial-IT

	Office-IT	Industrial-IT
Lebensdauer	3–5 Jahre	5–20 Jahre Hinweis: Die IEC 62443 verwendet im Teil 1-1 den Begriff Lebensdauer in Bezug zum Schlüsselmanagement, gibt jedoch keine Zeitspanne an
Patchmanagement	Oft, täglich	Selten, benötigt Freigabe vom Anlagenhersteller Hinweis: Die IEC 62443 regelt das Thema explizit im Teil 2-3
Zeitabhängigkeit	Verzögerungen akzeptiert	Kritisch Hinweis: Die IEC 62443 definiert Sicherheitsziele im Teil 1-1, wobei die Echtzeitfähigkeit als Millisekundenbereich angegeben wird
Verfügbarkeit	Kurze Ausfälle toleriert	24 x 7 Hinweis: Die IEC 62443 definiert Sicherheitsziele im Teil 1-1, wobei die Verfügbarkeit als höchstes Schutzziel definiert wurde

Aufgrund der zunehmenden Digitalisierung und Vernetzung, der Nutzung von Cloud-Diensten und der Bildung dynamischer Wertschöpfungsketten im Sinne der Industrie 4.0 werden spezielle Anforderungen an die Daten gestellt. Daher besitzen folgende Paragrafen des StGB auch für die Industrie eine hohe Relevanz:

- § 202a: Ausspähen von Daten
- § 202b: Abfangen von Daten
- § 263a: Computerbetrug
- § 303a: Datenveränderung
- § 303b: Computersabotage

2.2 Industrial Security

Die industrielle Automatisierung wird im Zuge der Digitalisierung und Industrie 4.0 mehr und mehr vernetzt. Grundlage der Vernetzung sind ethernetbasierte Kommunikationstechnologien wie OPC-UA. Trotz des hohen Standardisierungsgrads im Automatisierungsumfeld und der zunehmenden Nutzung von Standard- bzw. IKT-Technologien gibt es Unterschiede zwischen Office- und Produktionsnetzwerk. Damit lassen sich nicht immer bewährte technische wie auch organisatorische Schutzmaßnahmen aus der Office-Welt im Industriebereich unverändert einsetzen. Tabelle 1 zeigt daher ein paar der wesentlichen Unterschiede.

2.3 Industrial Security in Industrie 4.0

Die AG3 „Sicherheit vernetzter Systeme" der Plattform I4.0 bearbeitet das Thema Industrial Security explizit. Bis heute stehen zahlreiche Leitfäden und Hilfestellungen auf der Webseite der Plattform zur Verfügung. Im Kern geht es bei der AG3 um dynamische Wertschöpfungsnetzwerke mit automatisiertem Austausch von sensiblen Produktions- und Prozessdaten. Voraussetzung solcher Netzwerke ist das Vertrauen zwischen den Akteuren, dass sämtliche Daten und Informationen sicher, korrekt und ausschließlich zwischen den berechtigten Partnern ausgetauscht werden können. Für eine sichere Zusammenarbeit in unternehmensübergreifenden Wertschöpfungsnetzwerken ist der Aufbau von Vertrauensbeziehungen durch technische und organisatorische Maßnahmen notwendig. Vertrauen entsteht, wenn der Schutz gegen Bedrohungen von außen im vereinbarten Umfang von den Akteuren gewährleistet werden kann, dies überprüfbar ist und den jeweiligen Partnern glaubhaft nachgewiesen werden kann [Pla40].

3. Einstieg in die IEC 62443

Tabelle 2: Teile der internationalen Norm IEC 62443

IEC 62443: Industrial communication networks – Network and system security

General		Policies & Procedures		System		Component/Product	
1-1	Terminology, concepts and models	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	Implementation guidance for an IACS security management system	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	2-4	Security program requirements for IACS service providers				

veröffentlicht

3.1 Übersicht

Die IEC 62443 wird in Deutschland durch das Spiegelgremium DKE UK 931.1 „IT-Sicherheit in der Automatisierungstechnik" betreut.

Die Norm hat mit dem heutigen Datum (04/2017) insgesamt sieben der 13 geplanten Teile veröffentlicht. Tabelle 2 zeigt die Normenteile und den Stand der Veröffentlichung.

3.2 Modelle, Definitionen, Methoden

In diesem Abschnitt werden jene Definitionen und Grundprinzipien vermittelt, die für das Verständnis der IEC 62443 nötig sind.

Tabelle 3: Lebenszyklus und Rollen gemäß IEC 62443

Asset Owner (Betreiber)	Für ein oder mehrere industrielle Automatisierungssysteme verantwortliche Person oder Gesellschaft
Service Provider (Dienstleister)	Organisation (interne oder externe Organisation, Hersteller usw.), die zugesagt hat, entsprechend einer getroffenen Vereinbarung die Verantwortung zur Erbringung eines bestimmten Unterstützungsdiensts und, wenn es so festgelegt wurde, von Lieferungen zu übernehmen
Integration Service Provider	Spezieller Dienstleister, der für Integrationsaufgaben wie Design, Installation, Konfiguration, Tests und Inbetriebnahme sowie die Übergabe verantwortlich ist
Maintenance Service Provider	Spezieller Dienstleister, der für die Unterstützung einer Automatisierungslösung nach der Übergabe verantwortlich ist
Product Supplier (Produktlieferant)	Hersteller eines Hardware- und/oder Softwareprodukts

Ein wesentlicher Schritt zur Abstufung der Sicherheitszeile ist die Definition der Security-Levels. Die folgende Tabelle zeigt die Definition der Levels 1 bis 4.

Dabei besitzt der Security-Level eine Abhängigkeit zum Lebenszyklus bzw. der entsprechenden Rolle.

Tabelle 4: Security Level gemäß IEC 62443

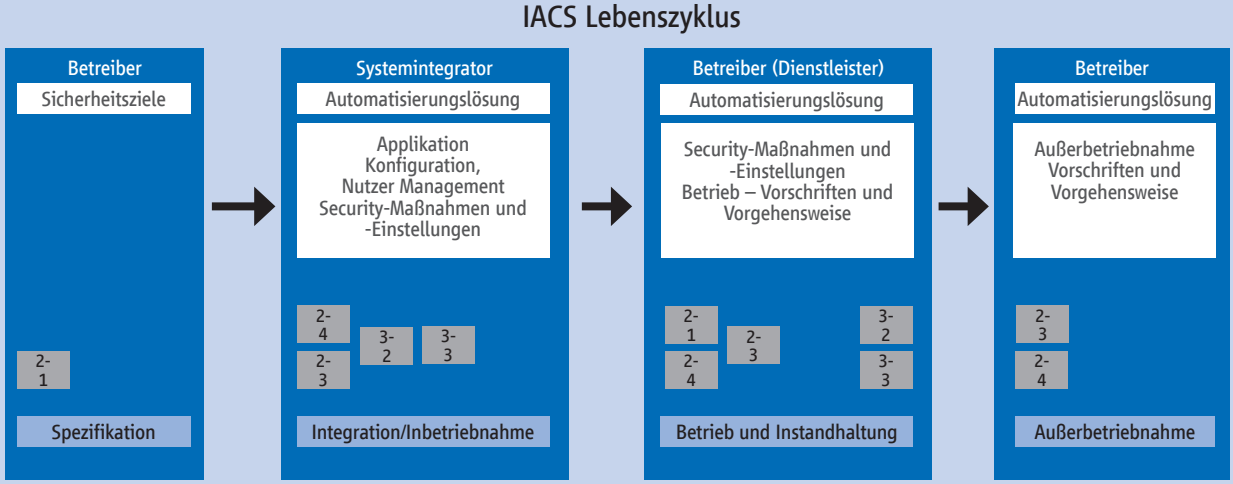
Level	Schutz gegen...
1	Zufällige Fehlanwendung
2	Absichtliche Versuche mit einfachen Mitteln
3	SL2, jedoch mit erweiterten Kenntnissen und erweiterten Mitteln
4	SL3, jedoch mit spezifischen Kenntnissen und erheblichen Mitteln

Tabelle 5: Security Level im Lebenszyklus IEC 62443

Kurzform	Langform	Bedeutung
SL-C	Security-Level – Capability	Security-Level, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert wird
SL-T	Security-Level – Target	Dieser zu erzielende Security-Level ist ein Ergebnis der Bedrohungs-/Risikoanalyse
SL-A	Security-Level – Achieved	Der im Gesamtsystem erreichte und messbare Security Level

Ein Hersteller gibt seinem Gerät Fähigkeiten (Capabilities, SL-C) mit. Dafür berücksichtigt er einerseits funktionale bzw. nicht funktionale IT-Security-Anforderungen während der Lösungsentwicklung, und andererseits basiert seine Lösungsentwicklung auf einem IT-sicheren Entwicklungsprozess.
Der Integrator bzw. Maschinenbauer erreicht in Anbetracht seiner konkreten Dienstleistung (beispielsweise im Rahmen eines Projekts mit den Phasen Design, Integration, Konfiguration, Test, Inbetriebnahme, Übergabe) und der einzelnen Fähigkeiten der verwendeten Geräte und Komponenten einen definierten Level (Achieved, SL-A). Hierbei bleibt hervorzuheben, dass es sich

Abbildung 4: Lebenszyklus und seine Zusammenhänge gemäß IEC 62443



Quelle: ZVEI

Tabelle 6: Basisanforderungen gemäß IEC 62443

Fundational Requirements	Grundanforderung
Identification and Access Control (IAC)	Identifizierung und Authentifizierung
Use Control (UC)	Nutzungskontrolle
System Integrity (SI)	Systemintegrität
Data Confidentiality (DC)	Vertraulichkeit der Daten
Restricted Data Flow (RDF)	Eingeschränkter Datenfluss
Timely Response to Events (TRE)	Rechtzeitige Reaktion auf Ereignisse
Resource Availability (RA)	Verfügbarkeit der Ressourcen

beim SL-A um eine bewertbare Größe handelt. Nur so kann nachgewiesen werden, dass die Zielgröße, der sogenannte Security Level Target (SL-T), mindestens erreicht wird.

Der Betreiber definiert im Rahmen einer Risikoanalyse das Schutzbedürfnis seiner zu betreibenden Automatisierungsanlage. Er drückt das z. B. im Rahmen des Lastenhefts durch die Angabe des Security Level Target (SL-T) aus.

Die Zusammenhänge dieser Rollen im Bezug zum gesamten Lebenszyklus einer industriellen Automatisierungsanlage und den Security-Levels zeigt Abbildung 4.

Basisanforderungen und Erweiterungen

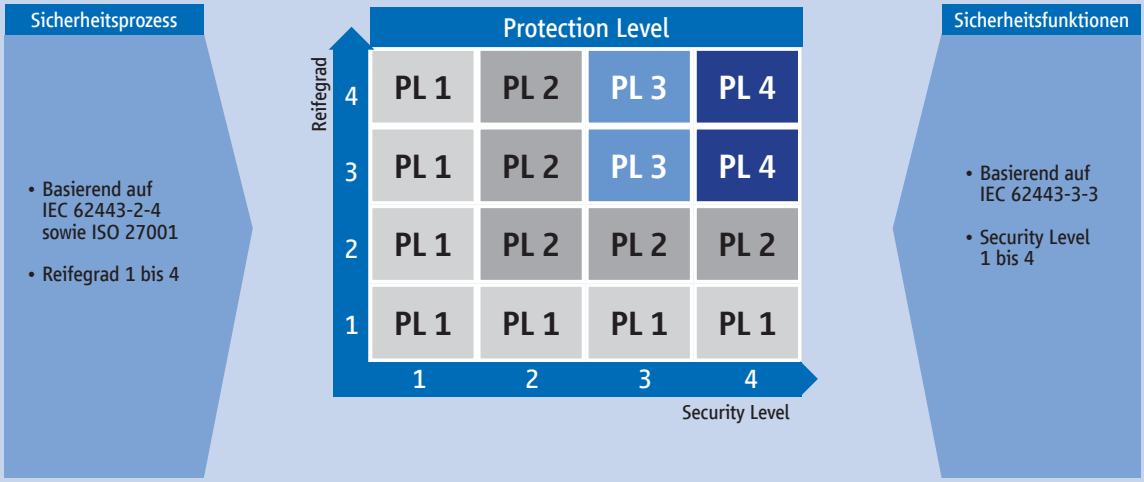
Die IEC 62443-1-1 definiert sieben Grundanforderungen. Auf Basis dieser Grundanforderungen werden in den Teilen 3-3 und 4-2 detaillierte Anforderungen gestellt.

Compliance-Metriken

Mit der Compliance-Metrik wird ein noch nicht veröffentlichtes Konzept vorgeschlagen. Es soll zum Ausdruck bringen, dass ein Produkt mit seinen dedizierten Schutzmaßnahmen und entsprechend seinem SL-C nicht von sich aus sicher betrieben werden kann. Es bedarf dazu eines gewissen Reifegrads in der betreibenden Organisation. Erst dadurch kann sichergestellt werden, dass ein sicher entwickeltes Produkt auch adäquat sicher betrieben werden kann.

Mit steigendem SL soll auch der Reifegrad steigen. Die folgende Abbildung soll das vorgeschlagene Konzept verdeutlichen.

Abbildung 5: Konzept der Protection-Levels gemäß IEC 62443



Quelle: ZVEI / [Kob15]

3.3 Industrial-Security-Aspekte für Hersteller

Der Hersteller entwickelt nicht nur seine Produkte, er integriert auch vorhandene (Teil-)Lösungen. Aus diesem Blickwinkel nimmt der Hersteller neben der Rolle des Herstellers auch die Rolle des Integrators ein.

Ferner fertigt der Hersteller sein Produkt oftmals mit Unterstützung von externen Dienstleistern (z. B. EMS). Damit schlüpft ein Hersteller auch in die Rolle eines Betreibers.

In den folgenden Abschnitten werden Anforderungen an den Hersteller beschrieben, die sich aus diesen verschiedenen Sichtweisen bzw. Rollen ergeben. Letztlich geht es nicht ausschließlich um ein IT-sicheres Produkt, sondern auch um eine IT-sichere Entwicklung, Integration und Fertigung.

Schwerpunkt der nachfolgenden Betrachtung liegt in den Herstelleranforderungen. Dabei wird zwischen funktionalen bzw. nicht funktionalen Anforderungen an das Produkt und Anforderungen an die Organisation (Prozesse) unterschieden.

3.3.1 Herstellersicht

Mit der IEC 62443-4-1 werden organisatorische bzw. prozessuale Anforderungen an die herstellende Organisation gestellt. Mit dem Secure Product Development Lifecycle (SPDLC) werden acht Ansätze definiert, die einen IT-sicheren Entwicklungslebenszyklus mit der Festlegung von IT-Sicherheitsanforderungen, einem gesicherten Entwurf, einer gesicherten Implementierung (einschließlich Programmierrichtlinien), Verifikation und Validierung, einer Mängelbehandlung, der Patchverwaltung und dem Ende des Produktlebenszyklus erlaubt.

Ein Produkt gemäß IEC 62443-2-4 wird dabei als ganzes System, Teilsystem bzw. Komponente definiert.

3.3.2 Integratorsicht

IEC 62443-2-4 legt Security-Anforderungen an die Fähigkeiten von Lieferanten von Integrations- und Instandhaltungsdiensten für industrielle Automatisierungs- und Regeltechniksysteme fest, die diese Dienstleister dem Betreiber gegenüber während der Integrations- und Instandhaltungstätigkeiten einer Maßnahme („Lösung“) erbringen müssen.

Die IEC 62443-2-4 fokussiert dabei auf den Systementwicklungsprozess. Es werden jedoch Prozess- und technische Anforderungen vermischt. Die technischen Anforderungen sind teilweise sehr spezifisch, wie das folgende Beispiel zeigt.

SP .04.03 - RE(2) – Der Dienstleister muss sicherstellen können, dass die Drahtloszugänge der Lösung statische IP-Adressen verwenden und dass die dynamischen Adresszuweisungsmechanismen (z. B. DHCP) ausgeschaltet sind.

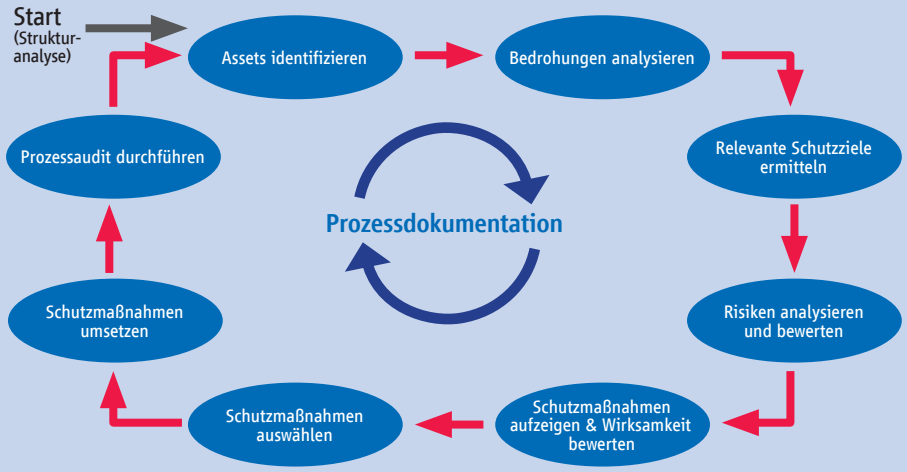
3.3.3 Betreibersicht

Der Betreiber hat die Verantwortung für Security. Er wendet unmittelbar die IEC 62443-2-1 an, indem er ein Informationssicherheitsmanagementsystem, kurz ISMS,

Tabelle 7: Secure Product Development Lifecycle gemäß IEC 62443

	Ansätze
1	Verwaltung der IT-Sicherheit
2	Spezifikation der IT-Sicherheitsanforderungen
3	IT-Sicherheit durch den Entwurf
4	Gesicherte Implementierung
5	Verifikations- und Validierungsprüfung der IT-Sicherheit
6	Behandlung von Mängeln der IT-Sicherheit
7	Verwaltung von IT-Sicherheitsupdates
8	IT-Sicherheitsrichtlinien

Abb. 6: Vorgehensmodell der VDI/VDE-Richtlinie 2182 Blatt 1



Quelle: ZVEI

aufbaut und betreibt. Der ursprüngliche Teil 2.1 wird jedoch derzeit überarbeitet. Ziel der Überarbeitung ist es, sich stärker an der ISO 27001 zu orientieren. Bis zum Erscheinen der Revision kann auch der Teil 2-4 angewendet werden. Mit diesem Teil wird zwar der Dienstleister adressiert, jedoch wird auch hier ein ISMS bzw. IT-Sicherheitsprogramm beschrieben, das durch eine tabellarische Form eine sehr brauchbare und kompakte Darstellung aufweist.

Die IEC 62443 verfolgt, wie alle neueren Managementnormen, einen risikobasierten Ansatz. Eine Risikoanalyse im Sinne der Security kann wie folgt durchgeführt werden:

1. Struktur- und Istanalyse: Es werden alle Komponenten der zu untersuchenden IT-Infrastruktur und ihrer Abhängigkeiten ermittelt. Zudem werden dabei alle bereits umgesetzten Sicherheitsmaßnahmen identifiziert.
2. Identifikation aller relevanten Bedrohungsszenarien: Auf Basis des Bedrohungskatalogs werden alle für den Untersuchungsgegenstand relevanten Bedrohungsszenarien identifiziert.
3. Abschätzung von möglichem Schaden und Eintrittswahrscheinlichkeit: Für alle in Schritt zwei als relevant identifizierten Bedrohungsszenarien werden mögliche Schäden und Eintrittswahrscheinlichkeiten abgeschätzt. Auf Grundlage dieser Abschätzungen kann eine Risikomatrix erstellt werden.
4. Ableitung von Security-Maßnahmen: Auf der Grundlage der Risikoabschätzung können Security-Maßnahmen abgeleitet werden, mithilfe derer die nicht akzeptablen Risiken auf ein akzeptables Maß reduziert werden können.

Anwendung der ISO 27001

Alternativ zur IEC 62443-2-1 bzw. 4-2 kann der Betreiber auch die ISO 27001 umsetzen. Auf dieser Basis lässt sich auch eine Zertifizierung anstreben. Die nachfolgende Abbildung zeigt das prinzipielle Vorgehensmodell der ISO 27001:2013. Bekannt hierbei ist das Vorgehen nach den Phasen „Plan-Do-Check-Act“.

Abb. 7: Plan-Do-Check-Act-Modell der ISO 27001

ISO 27001:2013
Information technology – Security techniques – Information security management systems – Requirements

Plan				Do	Check	Act
4 Context of the organization	**5 Leadership**	**6 Planning**	**7 Support**	**8 Operation**	**9 Performance evaluation**	**10 Improvement**
Organization and context	Leadership & commitment	Actions to address risks & opportunities	Resources	Operational planning & control	Monitoring, measurement, analysis & evaluation	Nonconformity and corrective action
Needs and expectations	Policy	Information security objectives & plans to achieve them	Competence	Information security risk assessment	Internal audit	Continual improvement
Scope of ISMS	Roles, responsibilities and authorities		Awareness	Information security risk treatment	Management review	
ISMS			Communication			
			Documented Information			

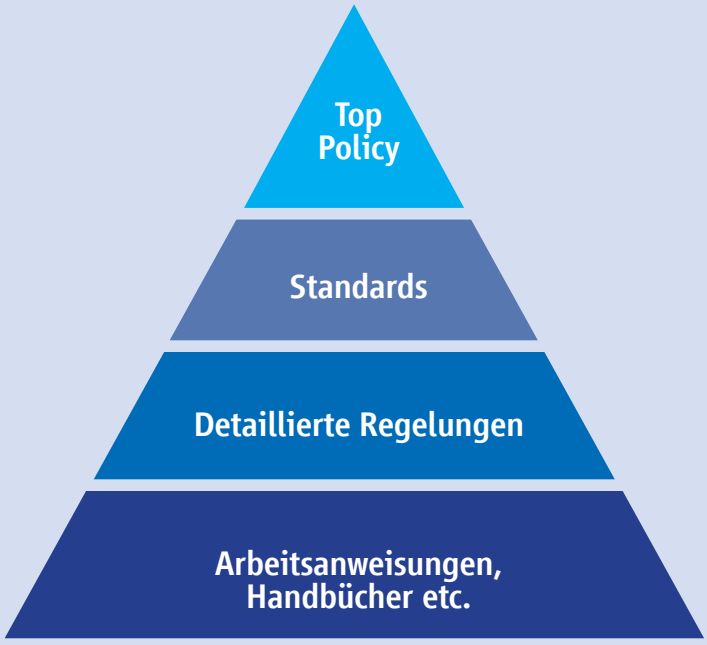
Annex A – Reference control objectives and controls

Quelle: ZVEI

Abb. 8: Security-Dokumentation ISO 27001

Beispielhafte Maßnahme im Rahmen der Dokumentationsanforderungen:

- Die Top Policy ist die sogenannte Security Policy. Diese sollte mindestens enthalten: Management commitment, Definition der Security-Ziele und -Prinzipien, kurze Beschreibung der Security-Organisation.
- Standards definieren die Anforderungen gemäß ISO 27001 und gestalten die Security Policy weiter aus.
- Detaillierte Regelungen: Diese beschreiben die Anforderungen detaillierter, bezogen auf bestimmte Themen.
- Standards und detaillierte Regelungen beschreiben das „Was" für das ISMS.
- Auf der untersten Ebene wird beschrieben, „wie" Security umgesetzt wird.



Quelle: ZVEI

4. Anwendung der IEC 64223 – Anforderungen für den Hersteller

In den nachfolgenden Abschnitten werden exemplarisch Normenanforderungen behandelt. Dabei wird ein einheitliches Schema verwendet, das zu folgenden Inhalten Auskunft gibt: Normenanforderung, Interpretation/Aktivitäten sowie Umsetzung und Nachweis der Erfüllung.

4.1 Voraussetzungen

Zur Festlegung der herstellerseitigen Anforderungen an das Produkt stellt sich eingangs die Frage, ob und nach welchem SL-C das Produkt ausgelegt werden soll. Diese Festlegung ist im Sinne der IEC 62443 nicht sinnvoll!

Vielmehr geht es darum, dem Produkt ausgewählte Industrial-Security-Fähigkeiten (engl. Capabilties) mitzugeben, die es für die geplante Einsatzumgebung benötigt. Damit kann die Einsatzumgebung die Liste der relevanten Anforderungen einschränken. Eine weitere Einschränkung der Produktanforderungen kann sich auch aus der Leistungsfähigkeit eines Produkts ergeben. Nicht alle Industrial-Security-Eigenschaften, meist realisiert durch Softwarefunktionen, können in einem Produkt ressourcentechnisch bzw. wirtschaftlich sinnvoll umgesetzt werden. Zudem gibt es systemspezifische Eigenschaften, die ein einzelnes Produkt nicht vollständig umsetzen kann (z. B. Prüfung einer Signatur).

Fähigkeiten, die ein Produkt nicht inhärent mitbringt, kann das System bzw. die Gesamtlösung auch durch den Einsatz zusätzlicher Maßnahmen erlangen. Die IEC 62443-3-3 führt dazu den Begriff „Ausgleichsmaßnahmen“ (engl. compensating countermeasures) ein. Er sagt aus, dass es auch mit der Anwendung zusätzlicher oder substituierender Maßnahmen möglich ist, die geforderten Industrial-Security-Anforderungen zu erfüllen. In solch einem Fall muss das Produkt oder die Gesamtlösung eine „Schnittstelle“ zu dieser externen Komponente bereitstellen. Einige Beispiele für solche Ausgleichsmaßnahmen sind Nutzeridentifizierung (zentral, verteilt), Gültigkeitsprüfung einer Signatur und Außerbetriebnahme von Geräten (Dauerhaftigkeit von Informationen).

Normenanforderung

IEC 62443-4-1: → Verwaltung der IT-Sicherheit:
→ SM-1 „Entwicklungsprozess“

Interpretation/Aktivitäten

Es muss ein allgemeiner Produktentwicklungs-/Produktinstandhaltungs-/Produktunterstützungsprozess dokumentiert und durchgesetzt werden, der mit anerkannten Produktentwicklungsprozessen (z. B. nach ISO 9001 zertifizierte Prozesse) vereinbar und in diese eingebunden ist, und das schließt unter anderem ein:

a) Konfigurationsverwaltung
b) Produktbeschreibung und Definition der Anforderungen inkl. deren Rückverfolgbarkeit
c) Software- oder Hardwareentwurf und Implementierungsverfahren
d) Wiederholbarer Verifikations- und Validierungsprozess
e) Überprüfung und Zulassung aller Artefakte des Entwicklungsprozesses
f) Unterstützung während des Lebenszyklus

Umsetzung/Nachweise

Diese Normenanforderung referenziert auf die ISO 9001. Alternativ steht mit der DIN EN ISO 9001:2015 eine deutsche Fassung zur Verfügung. In dieser lassen sich folgende Umsetzungsmöglichkeiten finden:

- 8.3 „Entwicklung von Produkten und Dienstleistungen“ durch beispielsweise Erstellung von Verfahrensanweisungen, Verantwortlichkeitsmatrix, FMEA, Risikoabschätzung, Projektplänen, Ablaufdiagrammen, Meilensteinplänen, Mess- und Prüfplänen, Verzierungs- und Validierungsvorgaben, Freigabebestimmungen, Lasten-/Pflichtenheften, Änderungsmanagement
- 8.5.2 „Kennzeichnung und Rückverfolgbarkeit“ durch beispielsweise Erstellung von Arbeitsanweisungen, Fertigungsplänen, EDV-Aufzeichnungen, Produktkennzeichnungen, Prüfnachweisen, Sperrzetteln, Freigaben
- 9.1 „Überwachung, Messung, Analyse und Bewertung“ durch beispielsweise Erstellung von Risikoanalysen (FMEA), Qualitätsaufzeichnungen, Prüfprotokollen, statistischen Auswertungen, Ergebnissen interner und externer Audits, Kundenzufriedenheitsanalysen, Lieferantenbewertungen

4.2 Prozessurale Anforderungen

Die Teilanforderung Konfigurationsverwaltung bzw. -management wird in der ISO 9001 nicht behandelt. Dafür wird auf die ISO 10007 „Quality management systems — Guidelines for configuration management" verwiesen. Sie dient der Unterstützung von Organisationen bei der Anwendung des Konfigurationsmanagements zur technischen und administrative Leitung des gesamten Produktlebenszyklus.

Mit diesem Beispiel wird sichtbar, dass Anforderungen der IEC 62443 durch bereits angewendete z. B. qualitätssichernde Normen wie ISO 9001 erfüllt werden können. Die Güte dieser Erfüllung wird jedoch durch das IEC-62443-Audit bestimmt.

4.3 Anforderungen an das Produkt (SL-C)

Mit diesem Beispiel soll gezeigt werden, dass systemweite Anforderungen nicht immer isoliert durch das zu entwickelnde Produkt umgesetzt werden können. Dabei sind zwei Lösungswege möglich. Erstens: Der Hersteller entwickelt sein Produkt gezielt auf eine Endanwendung hin. In diesem Fall muss er den Betreiber fragen, welche Identifikationsmerkmale existieren sollen und wie eine Prüfung erfolgen soll (intern im Gerät, extern durch eine zu definierende Schnittstelle). Als zweite Möglichkeit sieht der Hersteller keine Schutzmaßnahmen vor. In diesem Fall dokumentiert er das in der externen technischen Dokumentation. Damit fordert der Hersteller z. B. den Integrator auf, kompensierende Schutzmaßnahmen im System vorzusehen. Sieht

Normenanforderung

IEC 62443-4-2: → FR 1 „Identifizierung und Authentifizierung":
→ CR 1.2 „Identifizierung und Authentifizierung von Softwareprozessen und Geräten"

Interpretation/Aktivitäten

Identifizierung: Die Anwendung oder das Gerät muss sich selbst identifizieren können.

Authentifizierung (Komponente): Die Anwendung oder das Gerät muss sich gegenüber einer anderen Komponente (Anwendung, eingebettetes Gerät, Host und Netzwerkgeräte) authentifizieren können (siehe 3-3 SR 1.2).

Authentifizierung (Menschen): Läuft eine Anwendung oder das Gerät im Kontext eines menschlichen Nutzers, dann muss sich der menschliche Nutzer identifizieren und authentifizieren (siehe 3-3 SR1.1).

Umsetzung/Nachweise

Diese Normenanforderung umfasst Aspekte der Identifizierung und der Autorisierung, wobei die eindeutige Identifikation eine Grundvoraussetzung für die meist anschließende Autorisierung ist. Dies stellt aus heutiger Sicht die Hersteller vor folgende Fragen: Welche Identifikationsmerkmale müssen herangezogen werden? Welche technischen Maßnahmen und verbundene organisatorische Prozesse sind zum Erhalt und zur Verwaltung (über den gesamten Gültigkeitszeitraum) notwendig? Welche technischen Lösungen sind bereits standardisiert und was ist dabei Geräte- und/oder Systemfunktionalität?

Ohne technische Festlegungen (bisher fehlt solch ein technischer Standard innerhalb der IEC-62443-Familie) kann eine Systemfunktionalität wie die des Identitätsmanagements und der Autorisierung nicht herstellerneutral gewährleistet werden. Insbesondere für reine Gerätehersteller wird es schwer, eine einheitliche Lösung zu implementieren.

Diese Normenanforderungen sind für Gerätehersteller derzeit nicht adäquat umsetzbar! Gerätehersteller werden diese Anforderungen an den Integrator weiterreichen. Der Integrator muss dann gegebenenfalls kompensierende Maßnahmen implementieren, falls die Gesamtlösung den geforderten Security-Level (SL-T) nicht erreicht. Es wäre auch möglich, dass der Integrator spezifische Anforderungen an den Gerätehersteller z. B. per Lastenheft stellt.

der Integrator oder letztlich der Betreiber keine kompensierenden Schutzmaßnahmen vor, so wird das Produkt nicht bestimmungsgemäß eingesetzt.

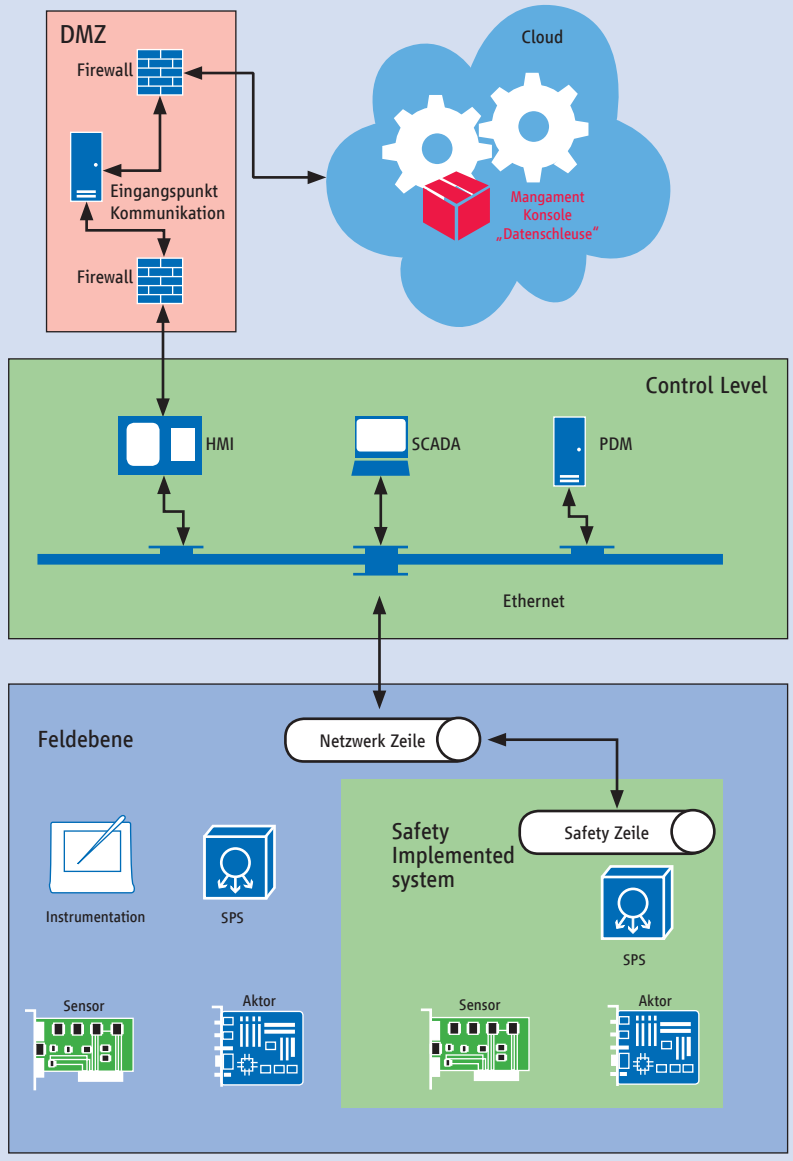
4.4 Anforderungen an das Produkt (Risikoanalyse)

Zur Bestimmung eines angemessenen, letztlich wirtschaftlichen Schutzniveaus und damit zur Identifikation der Produktanforderungen ist aus Sicht des Herstellers eine Risikoanalyse durchzuführen. Diese Vorgehensweise der IEC 62443 hat ihren Ursprung in der VDI/VDE-Richtlinie 2182 Blatt 1 [VDI21821].

Bei einem breit angelegten Produkt (breiter Markt, verschiedene Anwendungen) ist der Einfachheit halber ein „typisches Einsatzszenario" zu skizzieren. Im folgenden Beispiel (Abbildung 9) soll das zu entwickelnde Produkt, eine SPS in der Feldebene, wie folgt bestimmungsgemäß eingesetzt werden.

Mit dieser IT-Infrastruktur-Darstellung, der sogenannten physischen Sicht gemäß [VDI21821], lassen sich nun folgende Parameter für die Risikoanalyse ableiten.

Abb. 9: IT-Infrastruktur des Betrachtungsgegenstands



Quelle: ZVEI / [VDI21821]

Malware

Betrachtungsgegenstand (Asset) und seine Umgebung

SPS in der IT-Infrastruktur (Abbildung 9)

Gefahrenanalyse

Bedrohung: Malware (Trojaner, Würmer, Viren)

Infektionswege: Fernwartung durch Zulieferer, unkontrollierte externe mobile Datenträger (USB-Sticks, SD-Card etc.), Engineering-Station von Zulieferern

Schadensabschätzung

Infektionsweg Fernwartung: Aufgrund des Verbreitungsmechanismus der Malware (Kommunikationsverhalten) wird das Netzwerk überlastet.

Infektionsweg mobile Datenträger / Engineering-Station: Malware kann sich auf alle Systeme inklusive SIS ausbreiten, wenn mobile Datenträger und Engineering-Station in allen Bereichen uneingeschränkt eingesetzt werden.

Schutzmaßnahmen (vorhandene)

Im Betrachtungsgegenstand keine, da:

- bisher keine Anti-Malware-Applikation vorgesehen wurde und
- kein Schutzkonzept vorliegt.

Außerhalb des Betrachtungsgegenstands ungenügend, da:

- Schutzmaßnahmen (DMZ, per Firewall) nur den Kommunikationspfad „Fernwartung“ abdecken
- Der Infektionsweg mobiler Datenträger nicht oder nur ungenügend abgedeckt wird

Abschätzung der Eintrittswahrscheinlichkeit

Auch wenn die einzelnen Systeme so weit wie möglich gehärtet wurden, ist eine Malware-Infektion wahrscheinlich.

Risiko

Hoch

Schutzmaßnahmen (neue/verbesserte/kompensierende Maßnahmen)

- Entwicklung eines ganzheitlichen Schutzkonzepts bzgl. Malware
- Nutzung einer cloudbasierten Lösung z. B. Datenschleuse zur Prüfung mobiler Datenträger

Relevante Anforderungen gemäß IEC 62443-3-3

SR3.2 Malicious code protection
SR 3.4 Software and information integrity

Als Ergebnis der Risikoanalyse, die gegebenenfalls mit Unterstützung des oder der Betreiber(s) realisiert werden kann, liegen dem Hersteller nun Anforderungen (SR3.2, SR3.4) an das Produkt vor. Basis ist in diesem Beispiel der Teil 3-3 der IEC 62443. Darüber hinaus dokumentiert der Hersteller die für das Produkt geltenden Einsatz- und Umgebungsbedingungen. Dies erfolgt für gewöhnlich durch die externe technische Dokumentation, konkret durch die Definition des bestimmungsgemäßen Gebrauchs.

5. Literaturverzeichnis

[BSI_ICS] Industrial Control System Security, Top 10-Bedrohungen und Gegenmaßnahmen 2016, BSI-CS 005, Version 1.20, 01.08.2016

[Sym16] Symantec Corporation: Internet Security Threat Report, Vol. 21, April 2016

[Kas16] Kaspersky Lab, "Industrial Control Systems Vulnerabilities Statistics," 2015

[Eni16] Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, 2015, ISBN: 978-92-9204-135-9

[UL29] UL 2900-2-2: Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, Ed. 1, 2016

[TÜVSüd] Webkatalog der Zertifikate z. B. Z2-16-1062845-001: https://www.tuev-sued.de/produktpruefung/zertifikatsdatenbank

[Nis16] Richtlinie (EU) 2016/1148: Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, 6. Juli 2016

[Pla40] Webseite der Plattform: http://www.plattform-i40.de

[Kob15] Pierre Kobes: Protection Levels, ISA-99 Meetings, Frankfurt, Juni 2015

[VDI21821] VDI/VDE 2182 Blatt 1: Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell, 2011

Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org