IEC 62443

BEGRIFFE, DEFINITION, GRUNDLAGEN

Eine vereinfachte und prägnante Zusammenfassung der Schlüsselkonzepte und bewährten Verfahren für die Implementierung der Norm.

IEC 62443

Security für die Industrie

IEC 62443 ist die Sicherheitsrichtlinie für Personen, die industrielle Anlagen betreiben, zusammenbauen oder herstellen.

Sie konzentriert sich auf Automatisierungssysteme und kann in verschiedenen Automatisierungsbereichen eingesetzt werden, von der Herstellung und Gebäudesteuerung bis hin zu dezentralen Versorgungsnetzen.

Die Norm stellt im Wesentlichen Methoden und Sicherheitsanforderungen für die verschiedenen Rollen in der Automatisierung bereit

Industrial Automation GmbH bietet Ihnen Fachwissen, um die Sicherheitsmaßnahmen Ihres Unternehmens wirksam zu verbessern.

DEFENSE IN DEPTH:

Warum Ihr nächstes Sicherheits-Upgrade auf dem Prinzip der mehrschichtigen Verteidigung basieren sollte

Defense in Depth bedeutet, die Sicherheit in mehrere Schichten aufzuteilen.

Jede Sicherheitsmaßnahme ist wie eine Schicht in einer Burg: Wenn ein Angreifer eine Schicht, wie z.B. eine Firewall, überwindet, trifft er auf die nächste Verteidigungslinie. Eine gut geschützte Burg verfügt nicht nur über eine Außenmauer, sondern auch über einen Graben, Zugbrücken, Türme und Innenmauern, die alle zusammenarbeiten, um Angreifer abzuwehren.

In der Industrie, wo viele verschiedene Systeme und Geräte miteinander kommunizieren, ist es besonders wichtig, diesen mehrschichtigen Sicherheitsansatz zu verfolgen. Von Sensoren und Steuerungssystemen bis hin zu Datenspeichern und Web-Anwendungen – alle haben unterschiedliche Sicherheitsmerkmale. Da nicht alle Systeme moderne Sicherheitsupdates unterstützen, ist es umso wichtiger, eine Vielfalt an Sicherheitsmaßnahmen zu nutzen, um das Gesamtsystem zu schützen.

Die 4 Gruppen der IEC 62443-Norm

Allgemein

Grundlegende **Konzepte**, Begriffe und Vorgehensweisen

IEC 62443-1

Betreiber

Organisatorische **Maßnahmen und Prozesse** für Betreiber und Dienstleister

IEC 62443-2

Integrator

Sicherheitskriterien **an Automatisierungssysteme** und Bericht zu Schutztechniken

IEC 62443-2 & 3

Hersteller

Grundlegende **Konzepte**, Begriffe und Vorgehensweisen - Sicherheitsanforderungen an **Automatisierungskomponenten**

IEC 62443-4

Was davon ist für Sie relevant?

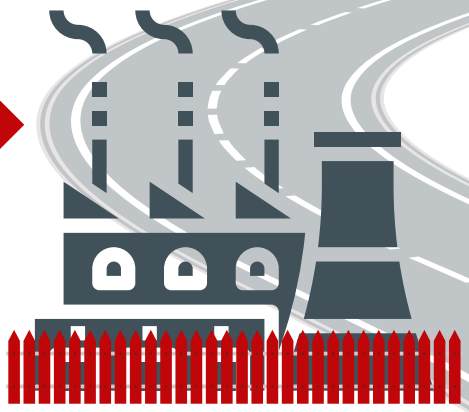
Security Level

als Tool zur Umsetzung des
Defense-in-Depth-Ansatzes

Betreiber	Risko Analyse	2 - 4 3 - 2	**Zielvorgabe Security Level** **SL-T**	**IEC 62443-2**
System Integrator	Automatisierungs Lösung	3 - 2 3 - 3	**Erreichter Security Level** **SL-A**	**IEC 62443-2** **IEC 62443-3**
Hersteller	Komponenten Security Level	4 - 1 4 - 2	**Erreichbarer Security Level** **SL-C**	**IEC 62443-4**

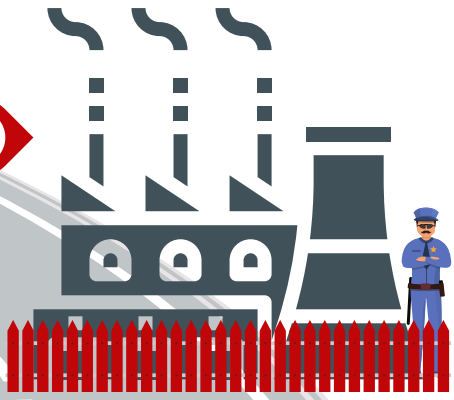
Das Konzept der Securitylevel hilft, den Schutz einer Zone oder eines Conduits qualitativ zu bewerten. Es ist ein Teil des umfassenden Defense-in-Depth-Ansatzes und bietet ein Werkzeug, um die notwendigen Sicherheitsstufen für Anlagenkomponenten festzulegen. Diese Stufen reichen von einfachen Anforderungen auf Level 1 bis zu höchsten Sicherheitsmaßnahmen auf Level 4, etwa für staatliche Einrichtungen.

1



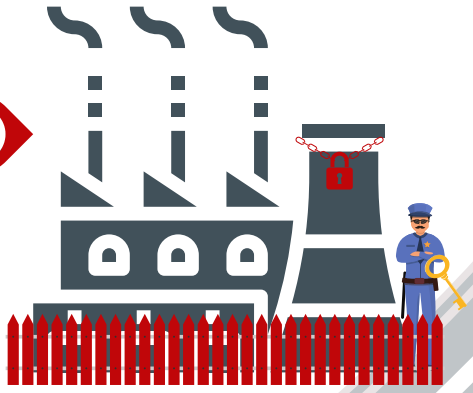
Schutz gegen ungewollten, zufälligen Missbrauch

2



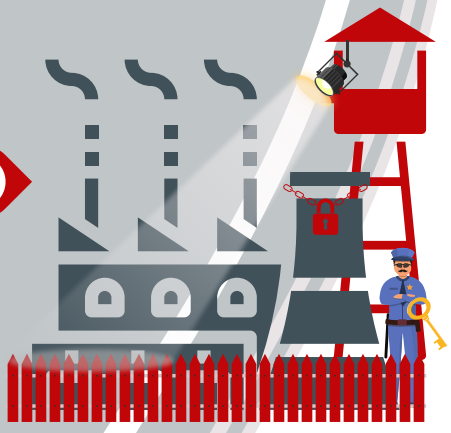
Schutz vor Missbrauch mit einfachen Methoden, wenig Aufwand, Grundkenntnissen und geringer Motivation.

3



Schutz vor Missbrauch mit speziellen Techniken, mittlerem Einsatz, Fachkenntnissen in Automatisierung und mittlerer Motivation.

4



Schutz gegen Missbrauch durch den Einsatz komplexer Techniken, viel Arbeit, Fachwissen in Automatisierung und starker Motivation.

Für umfassende Industrie-Sicherheit müssen die drei Hauptakteure einer Automationslösung - **Betreiber, Integrator, Hersteller** - einbezogen werden. Daraus leiten wir die wichtigsten Schritte zur Normnutzung ab, die wir nun vorstellen.

Integratoren:
die entweder eine bestehende Anlage verbessern oder eine neue planen, beginnen alles mit einer Risikoanalyse. Basierend darauf werden Maßnahmen für die gesamte Anlage festgelegt, die sowohl technisch als auch organisatorisch oder personell sein können. Dies bildet das Sicherheitskonzept. Dann werden die Maßnahmen auf einzelne Komponenten heruntergebrochen, wobei manchmal technische Lösungen durch organisatorische Prozesse ersetzt werden müssen, falls sie nicht umsetzbar sind.
Dieser Top-Down-Ansatz hilft, Sicherheitsmaßnahmen von der Gesamtanlage bis zu einzelnen Komponenten anzuwenden. Ein Problem dabei ist, dass die Norm nicht immer klare Anweisungen gibt, wie bestimmte Schritte umzusetzen sind, was die Anwendung schwierig macht. Es fehlen etwa konkrete Tipps zur Durchführung der Zonierung nach einer Risikoanalyse oder zur Zuordnung von Sicherheitsstufen, was die Nutzung der Norm für Integratoren herausfordernd macht.

Hersteller:
von Automatisierungskomponenten gehen anders vor als Integratoren. Sie entwickeln Komponenten nicht für spezifische Sicherheitsanforderungen einer bestimmten Umgebung, sondern für breitere Anwendungsfälle, um größere Stückzahlen zu erreichen. Dabei müssen sie entscheiden, welche Sicherheitsmaßnahmen und -standards (Security Level, SL) ihre Produkte erfüllen sollen. Oft zielen sie auf die unteren Sicherheitsstufen (SL-1 bis SL-3) ab, da diese am häufigsten benötigt werden und somit praktisch relevanter sind.
Zusätzlich sind Hersteller verpflichtet, einen sicheren Entwicklungsprozess (Security Development Lifecycle, SDL) zu etablieren. Dieser Prozess soll sicherstellen, dass Sicherheitsanforderungen von Anfang an berücksichtigt werden, einschließlich der Möglichkeit, Sicherheitsupdates für die Komponenten durchzuführen. Die Auswahl der passenden SL-Stufe erfordert eine gute Marktkenntnis und eine sorgfältige Analyse durch das Produktmanagement, um eine fundierte Entscheidung zu treffen.

Betreiber:
industrieller Anlagen konzentrieren ihre Vorgehensweise auf die Aufrechterhaltung und regelmäßige Überprüfung der Sicherheit während des Betriebs.Die IEC 62443 plant, das Konzept eines "Security Program" (SP) einzuführen. Dieses Programm kombiniert technische und organisatorische Anforderungen, die durch SP-Elemente und darunterliegende Security Control Classes (SCC) definiert werden, wobei jede Klasse spezifische Sicherheitsanforderungen stellt. Diese Anforderungen beziehen sich auf bestehende Standards wie die ISO 27001, um Doppelungen zu vermeiden.
Zusätzlich zum SP führt der neueste Entwurf der Norm die "Protection Level" (PL) ein. Diese ermöglichen eine Bewertung, wie gut eine Automatisierungsumgebung in Bezug auf Sicherheit aufgestellt ist, indem sowohl technische als auch organisatorische Kriterien berücksichtigt werden. Die Bewertung erfolgt detailliert für verschiedene Aspekte, um einen Gesamtwert oder einen Wert für spezifische Bereiche zu ermitteln. Dieser Ansatz hilft, den aktuellen Sicherheitsstatus einer Anlage zu "messen". Er kann bei der Erstbewertung, für regelmäßige Überprüfungen oder externe Audits verwendet werden. Die Normteile 2-1 und 2-2 verwenden dabei dieselbe Terminologie.

Wie werde ich mit IEC 62443 sicher?

IEC 62443-2-4
FUNCTIONAL AREAS

Dieser Teil der Norm spezifiziert Security-Fähigkeiten die Integratoren und Serviceanbieter den Betreibern von Industrieanlagen anbieten können. Die Fähigkeiten sind in Functional Areas (SP) strukturiert.

IEC 62443-3-3 & IEC 62443-4-2 FOUNDATIONAL REQUIREMENTS

Dieser Teil der Norm spezifiziert Security-Anforderungen für Lösungen und Produkte. Die Anforderungen sind anhand von sieben Foundational Requirements (FR) strukturiert.

IEC 62443-4-1
PRACTICES

Dieser Teil der Norm spezifiziert Prozessanforderungen an die Entwicklung von angriffssicheren Produkten. Er definiert einen Secure Development Lifecycle (SDL) mit folgenden Praktiken.

1. **Security Management**
   Planung, Dokumentation und Ausführung von sicherheitsrelevanten Aufgaben während des Produktlebenszyklus
2. **Specification of Security Requirements**
   Dokumentation der notwendigen Sicherheitsfunktionen, die für das Produkt laut Verwendungszweck benötigt werden
3. **Secure by Design**
   Umsetzung des Secure-by-Design-Prinzips und Berücksichtigung von Defense-in-Depth-Maßnahmen
4. **Secure Implementation**
   Sichere Implementierung der Produktfunktionen
5. **Security Verification and Validation Testing**
   Überprüfung, ob alle Sicherheitsanforderungen umgesetzt wurden und ob das Produkt sicher in Betrieb genommen wird
6. **Management of security-related issues**
   Umgang mit sicherheitsrelevanten Ereignissen bei einem Produkt, das Defense-in-Depth-Maßnahmen umsetzt
7. **Security Update Management**
   Test der Produktsicherheitsupdates auf Behebung des Problems und rasche Bereitstellung für Produktbesitzer
8. **Security Guidelines**
   Dokumentation der Maßnahmen zur Integration, Konfiguration und Aufrechterhaltung des Defense-in-Depth-Prinzips

Last but not least!

Die Vorgehensweisen in der Norm sind nicht direkt erklärt und werden klarer, wenn man mehrere Teile betrachtet. Das macht es schwer, sie zu verstehen, was viele Nutzer abschreckt. Man kann zwar durch Diskussionen viel lernen, aber das ist nicht für jeden machbar. Auch wenn viele Teile der Norm fertig sind, fehlen noch einige, besonders beim Security Program für Betreiber. Die Norm ist also noch nicht ganz stabil.

★ ★ ★ ★ ★

Um gute mehrstufige Sicherheitsmaßnahmen umzusetzen, braucht man eine gut durchdachte IT-Sicherheitsstrategie. Diese Strategie sollte mit einer gründlichen **Überprüfung der aktuellen Situation** und einer **Risikobewertung** starten. Wichtig ist, die wichtigsten Teile des Unternehmens, wie Produktionsabläufe und geschützte Verfahren, zu erkennen und passende Schutzmaßnahmen einzuführen.

★ ★ ★ ★ ★

Zu den Sicherheitsmaßnahmen gehören:

- Einbeziehung besonderer Anforderungen von Industrie-Systemen in das IT-Sicherheitsmanagement.
- Einstufung von Systemen und Netzen nach Schutzbedarf, z.B. Einfluss auf Produktionsprozesse.
- Erstellen einer Rahmenstruktur und Sicherheitsdokumente für Netzinfrastruktur (Hardware, Software, Firewalls).
- Systeme durch Patch-Management-Richtlinien absichern.
- Verfahren für Systeme ohne Patch- und Virenschutz, z.B. weitere Netzsegmentierung.
- Einsatz industrietauglicher Firewalls und IDS für Industrie-Protokolle wie PROFINET.
- Sicherheit von Anwendungen durch Change-Management und genehmigte Programme.
- Anomalie-Erkennung mit Intrusion-Detection-Systemen, zentralem Logging und SIEM.
- Einführung eines PDCA-Zyklus zur regelmäßigen Überprüfung.
- und andere

GET IN TOUCH

+43 512 272 271 0

office@automation.team

www.scada.online

Technikerstraße 1 - 3,
6020 Innsbruck

März 2024