LIMES SECURITY

IEC 62443

Zusammenfassung

Begriffe, Definitionen und Grundlagen

LIMES SECURITY

SECURITY FÜR DIE INDUSTRIE

IEC 62443

IEC 62443 ist die Security-Norm für Betreiber, Integratoren und Hersteller von Industrieanlagen. Nutzen Sie die Expertise von Limes Security, um Ihr Unternehmen effizient in puncto Security aufzurüsten.

WAS DAVON IST FÜR MICH RELEVANT?

Die IEC 62443-Norm besteht aus vier Gruppen, die sich jeweils aus mehreren Teilen zusammensetzen.

Allgemein

Allgemeine **Konzepte**, Terminologien und Methoden

IEC 62443-1

Betreiber

Organisatorische **Maßnahmen und Prozesse**, die als Bestandteil eines Defense-in-Depth-Konzepts relevant sind

IEC 62443-2

Integrator

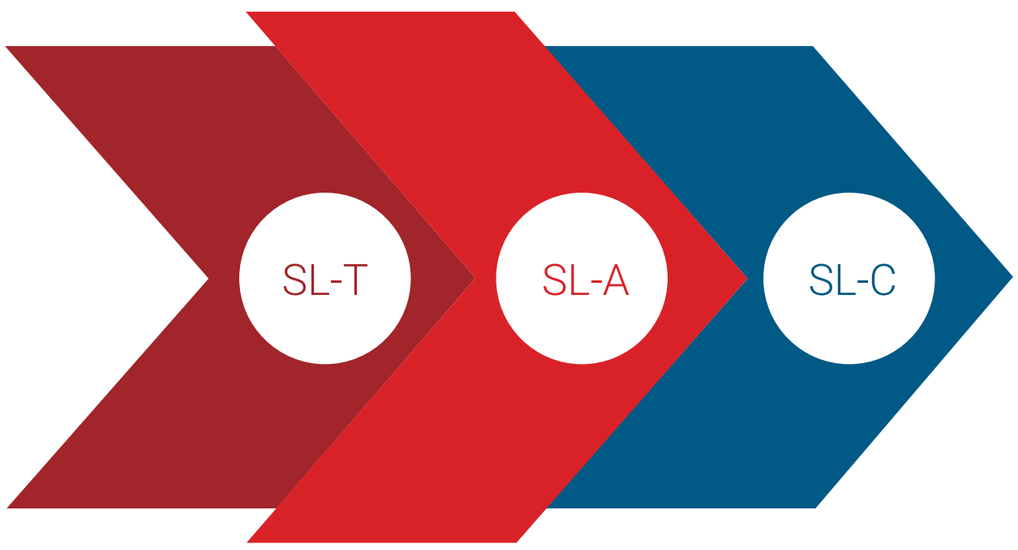
Sicherheitsrelevante Anforderungen an die funktionalen **Fähigkeiten der Automatisierungssysteme** und ein technischer Bericht über aktuelle Schutztechniken

IEC 62443-2 & IEC 62443-3

Hersteller

IT-Sicherheit als integraler Bestandteil des Entwicklungs-prozesses und Anforderungen an funktionale **Fähigkeiten von Produkten**

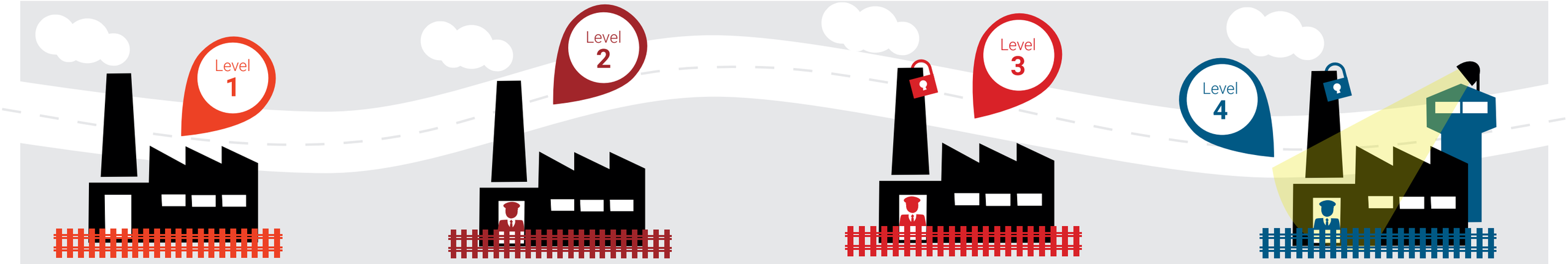
IEC 62443-4



Target Security Level (SL-T)
Erwünschtes Securitv-Level für eine bestimmte Lösung. Der Anlagenbetreiber nutzt die Ergebnisse einer Risikoanalyse um den SL-T zu bestimmen.

Achieved Security Level (SL-A)
Tatsächlich festgestelltes Security-Level für eine bestimmte Lösung. Aktuelles SL-A wird durch ein Assessment ermittelt.

Capability Security Level (SL-C)
Höchstes Security-Level, das das Produkt oder die Lösung bietet, wenn sie richtig konfiguriert ist. Wird vom Hersteller oder Integrator geliefert.



Schutz gegen ungewollten, zufälligen Missbrauch

Schutz gegen Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation

Schutz gegen Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und moderater Motivation

Schutz gegen Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation

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.

1. **Solution staffing**
   Zuordnung von Personal, Hintergrundchecks, Trainings
2. **Assurance**
   Härtungsrichtlinien, Security Tools & Software, Lösungskomponenten
3. **Architecture**
   Risikoanalyse, Datenschutz, Netzwerkdesign, Netzwerk- und Systemgeräte
4. **Wireless**
   Einsatz von drahtloser Kommunikation
5. **SIS**
   Risikoanalyse, User Interface, Netzwerkdesign, Netzwerk- und Systemgeräte
6. **Configuration Management**
   Aktuelle Dokumentation von Komponenten, Netzwerk und Konfigurationen
7. **Remote Access**
   Datenschutz, Security Tools & Software
8. **Event Management**
   Alarme, Events, Logging, Incidents & Kompromittierungen
9. **Account Management**
   Benutzer- und Serviceaccounts, Passwörter
10. **Malware Protection**
    Prozesse, Software & Tools, Systeme, externe Wechseldatenträger
11. **Patch Management**
    Prozesse, Patchliste, Sicherheitsupdates
12. **Backup/Restore**
    Prozesse, Backup, Wiederherstellung, Wechseldatenträger

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.

1. **Identification and Authentication Control (IAC)**
   Zuverlässig alle Benutzer identifizieren und authentifizieren
2. **Use Control (UC)**
   Erzwingen der zugewiesenen Privilegien eines authentifizierten Benutzers, um die angeforderte Aktion auf dem System auszuführen
3. **System Integrity (SI)**
   Sicherstellung der Integrität des IACS zur Verhinderung unbefugter Manipulationen
4. **Data Confidentiality (DC)**
   Gewährleistung der Vertraulichkeit von Informationen über Kommunikationskanäle und in Datenspeichern
5. **Restricted Data Flow (RDF)**
   Segmentierung des IACS mittels Zonen und Conduits
6. **Timely Response to Events (TRE)**
   Reagieren auf Sicherheitsverletzungen, melden erforderlicher Beweise und ergreifen von Korrekturmaßnahmen
7. **Resource Availability (RA)**
   Sicherstellung der Verfügbarkeit des Steuerungssystems gegen Denial-of-Service-Angriffe auf wesentliche Dienste

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