

SEC4YOU

Advanced IT-Audit Services

IT-Sicherheit in der Industrie

Die Normenreihe IEC 62443

ISACA / (ISC)² Cybersicherheit zeigt Zähne 12.10.2017

Manfred Scholz

IT-Sicherheit in der Industrie?



IT-Sicherheit in der Industrie?



SECURITY 4.0

Bedrohungen



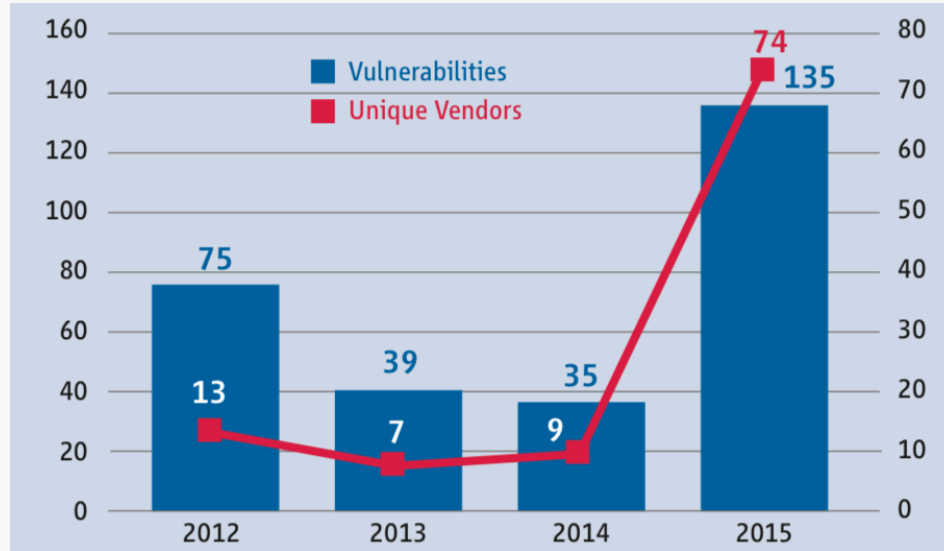
Angriffe auf kritische Infrastrukturen und Produktionsanlagen (z.B. Energieversorgung)

Top 10 Bedrohungen für Industrieanlagen 2016

1. Social Engineering und Phishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet und Intranet
4. Einbruch über Fernwartungszugänge
5. Menschliches Fehlverhalten und Sabotage
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet und Cloud-Komponenten
9. (D)DoS Angriffe
10. Kompromittierung von Smartphones im Produktionsumfeld

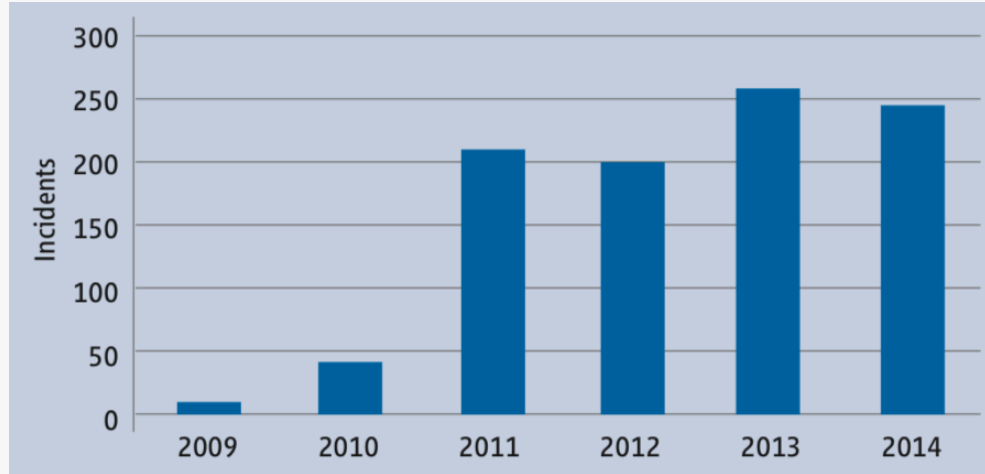
Quelle: BSI - Top 10 Bedrohungen und Gegenmaßnahmen 2016

Schwachstellen in industriellen Steuerungssystemen



Quelle: ZVEI / (Eni16)

Cyber Security Incidents bei industriellen Steuerungssystemen



Industrieanlagen stehen im Visier aktueller Sabotage- und Spionageangriffe

Quelle: ZVEI / (Eni16)

Bedrohungen durch Schadsoftware

Stuxnet

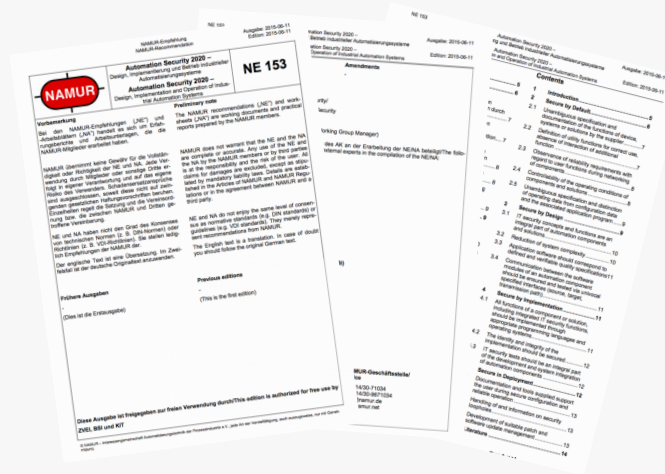
2010 programmiert zur gezielten Sabotage iranischer Atomanlagen

IT-Sicherheit in der Industrie?



Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.

Empfehlung NE 153 Automation Security 2020



Design, Implementierung und Betrieb industrieller Automatisierungssysteme
(11.6.2015)

Wesentliche Forderungen der NE 153

1. Secure by Default
2. Secure by Design
3. Secure by Implementation
4. Secure in Deployment

NAMUR empfiehlt den Einsatz von Normen und Standards

IEC 62443
VDI/VDE 2182

NAMUR empfiehlt den Einsatz von Normen und Standards

IEC 62443

Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme

VDI/VDE 2182

Informationssicherheit in der industriellen Automatisierung
(Allgemeines Vorgehensmodell)

Einsatz von Normen und Standards



Gemeinsame Regeln führen zu vergleichbaren Ergebnissen

Normen und Standards



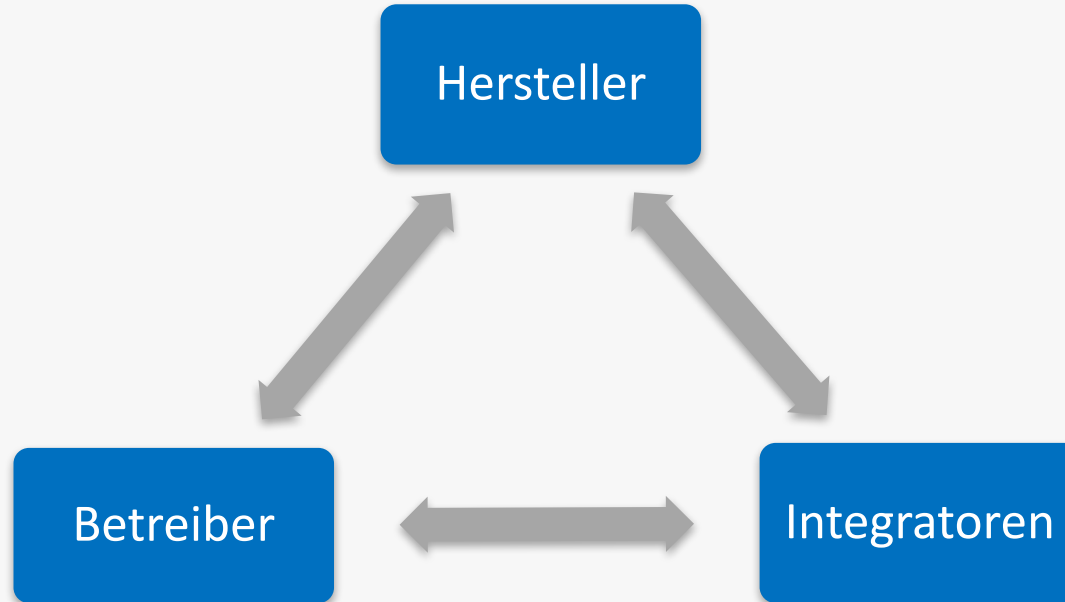
... gelten als Stand der Technik!

IEC 62443 Normenreihe

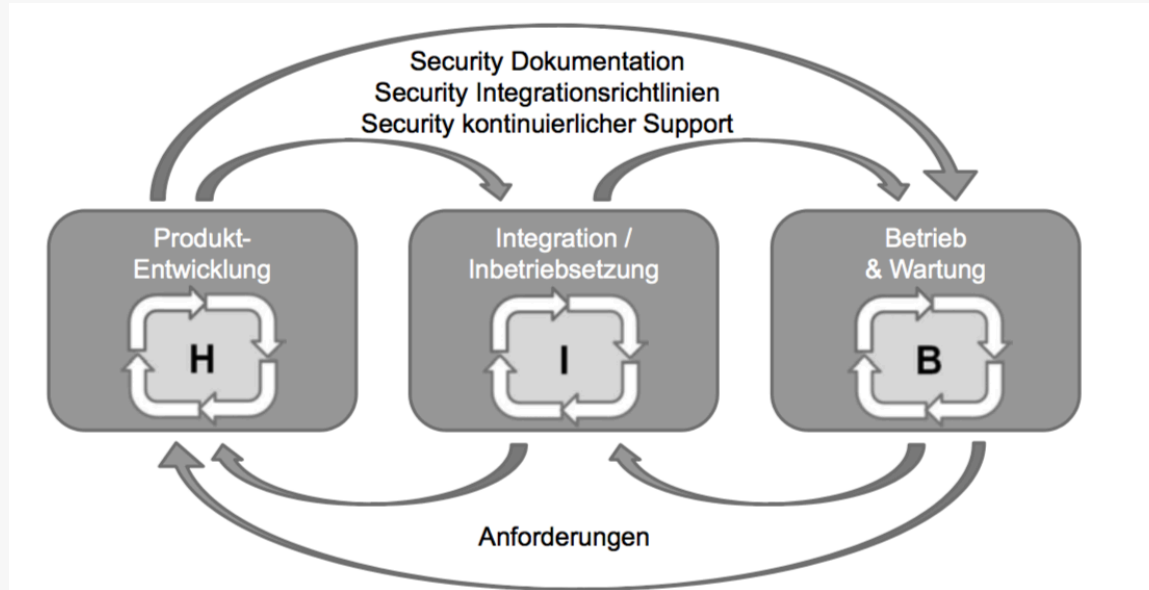
General		Policies & Procedures		System		Component/Product	
1-1	Terminology, concepts and models	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	Implementation 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

Verantwortungen für IT-Sicherheit gemäß IEC 62443



Verantwortungen für IT-Sicherheit gemäß IEC 62443



Quelle: VDI/VDE 2182-1

Securitylevel

1. Schutz gegen ungewollten oder zufälligen Missbrauch;
2. Schutz gegen gewollten Missbrauch unter Verwendung einfacher Mittel;
3. Schutz gegen gewollten Missbrauch unter Verwendung hoch entwickelter Mittel;
4. Schutz gegen gewollten Missbrauch unter Verwendung hoch entwickelter Mittel und erweiterter Ressourcen.

Unterscheidung der Security-Levels

Typ	Security-Level	Eigenschaften
SL-T	Target	Der notwendige Security-Level ist meist das Ergebnis der Bedrohungs-/Risikoanalyse.
SL-C	Capability	Der Security-Level, den ein Produkt erreichen kann, wenn es korrekt eingesetzt und konfiguriert wird.
SL-A	Achieved	Der nach der Implementierung erreichte und messbare Security-Level

Grundanforderungen - Foundational requirements (FR)

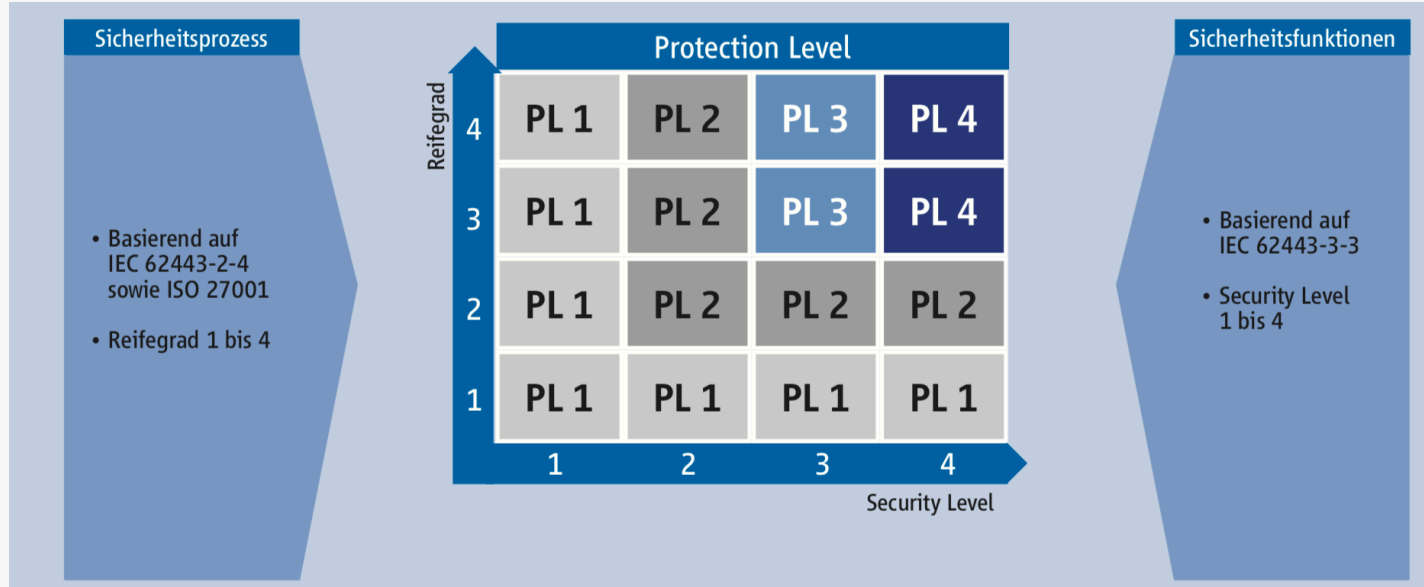
1. Identifizierung und Authentifizierung (IAC)
2. Nutzungskontrolle (UC)
3. System Integrity (SI)
4. Vertraulichkeit der Daten (DC)
5. Eingeschränkter Datenfluss (RDF)
6. Rechtzeitige Reaktion auf Ereignisse (TRE)
7. Verfügbarkeit der Ressourcen (RA)

Detailliert beschrieben in der IEC 62443-3-3 (System) und IEC 62443-4-2 (Produkt)

Ableitung der Security Requirements

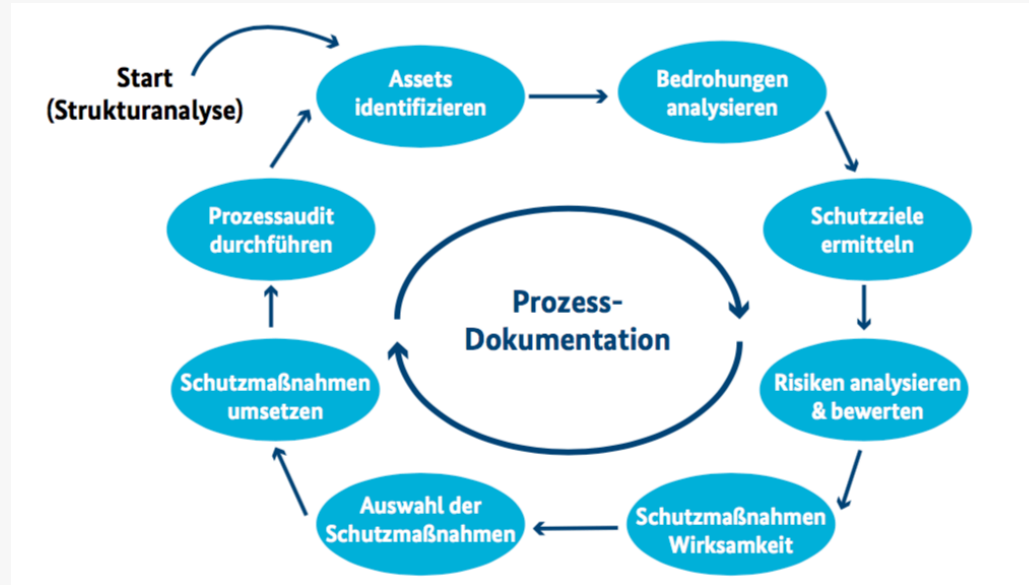
SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓

Erweiterung um Sicherheitsprozesse



Quelle: VDI/VDE Richtlinie 2182-1

Vorgehensmodell



Quelle: VDI/VDE Richtlinie 2182-1

Zertifizierungen nach IEC 62443

- IEC 62443-4-1 → Produktzertifizierung
- IEC 62443-3-3 → Anforderungen an die IT-Sicherheitsfunktionen
- IEC 62443-2-4 → Anforderungen an Systemintegratoren

Finale



Manfred.Scholz@sec4you.com
<https://sec4you.com>
XING, LinkedIn
Tel.: +43 1 2531 797-10