secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

# Workshop Vorgehen zu einer Sicherheitsüberprüfung nach IEC 62443

## Internet Security Days 2017

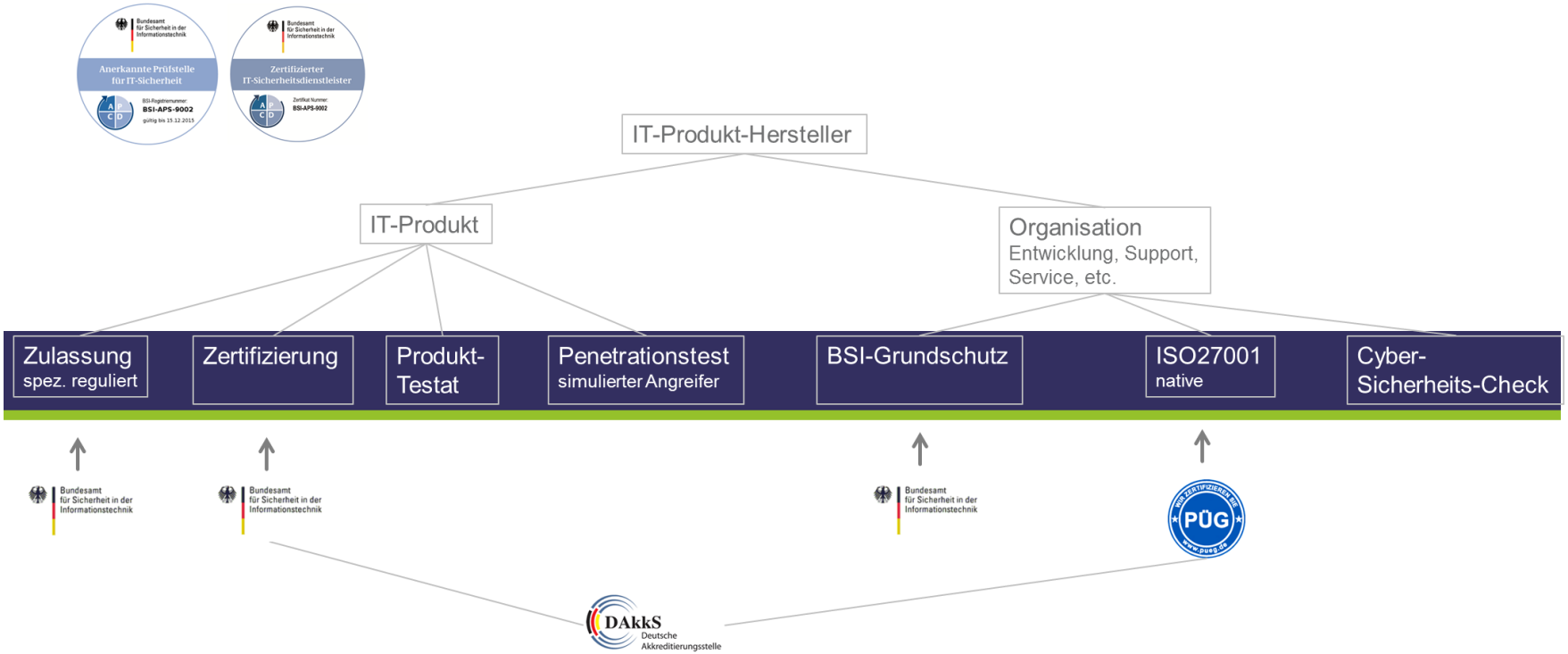
- Kathrin Schäberle
  - Sicherheitsberaterin bei secuvera
  - Penetrationstests
  - Evaluatorin für Common Criteria und ITSEC
  - GICSP (Global Industrial Cyber Security Professional)

- Tobias Glemser
  - Geschäftsführer secuvera GmbH
  - Seit 2000 Pentests, seit 2002 Web-Sicherheit
  - BSI-zertifizierter Penetrationstester
  - Autor
    - c‘t, iX, hakin9, IT-Security, IT-Sicherheit
    - Whitepaper „Projektierung der Sicherheitsüberprüfung von Webanwendungen“
    - OWASP Top10 Übersetzung

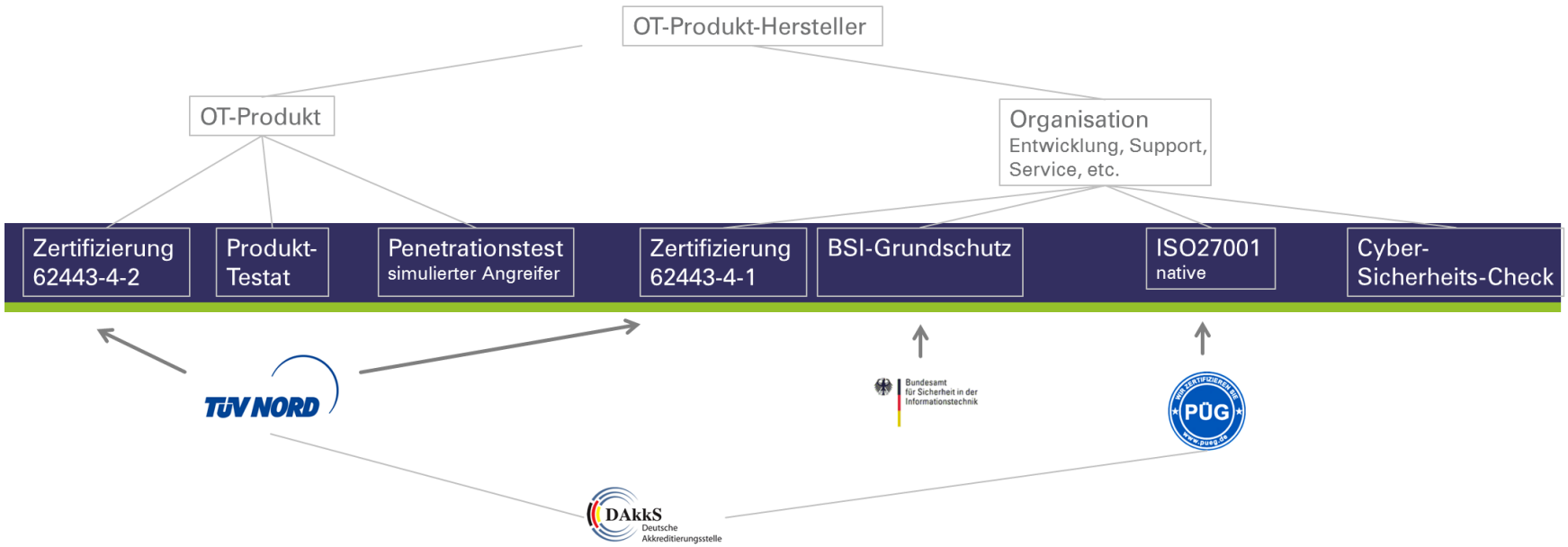
# Ziel: Konformität zu etablierten Sicherheitsstandards

- In der IT-Welt für Produkte
  - 1990: ITSEC
  - 1998: Common Criteria
- In der IT-Welt für Prozesse
  - IT-Grundschutz
  - ISO 27001
- Cyber, Cyber
  - Cyber-Sicherheits-Check (CSC)
  - Penetrationstests

- Drei Beratungsfelder
  - BSI-Prüfstelle für Common Criteria (Produktzertifizierungen)
  - Penetrationstests/Webanwendungsprüfungen
  - BSI-Grundschutz/ISO 27001
- BSI-zertifizierter IT-Sicherheitsdienstleister
  - Kompetenzfeststellung durch das Bundesamt für Firma und Berater



Anerkannte Prüfstelle für IT-Sicherheit
BSI-Registrernummer: BSI-APS-9002 gültig bis 15.12.2015
Zertifizierter IT-Sicherheitsdienstleister
Zertifikat Nummer: BSI-APS-9002
IT-Produkt-Hersteller
IT-Produkt
Organisation
Entwicklung, Support, Service, etc.
Zulassung
spez. reguliert
Zertifizierung
Produkt-Testat
Penetrationstest
simulierter Angreifer
BSI-Grundschutz
ISO27001
native
Cyber-Sicherheits-Check
Bundesamt für Sicherheit in der Informationstechnik
PÜG
DAkkS
Deutsche Akkreditierungsstelle

# Und in der „OT“/Automatisierung?


OT-Produkt-Hersteller
OT-Produkt
Organisation
Entwicklung, Support, Service, etc.
Zertifizierung 62443-4-2
Produkt-Testat
Penetrationstest
simulierter Angreifer
Zertifizierung 62443-4-1
BSI-Grundschutz
ISO27001
native
Cyber-Sicherheits-Check
TÜV NORD
Bundesamt für Sicherheit in der Informationstechnik
PÜG
DAkkS
Deutsche Akkreditierungsstelle

- Freestyle „Zertifizierungen“
  - „Auf Basis von“
  - „according to“

- BSI-Prüfstelle

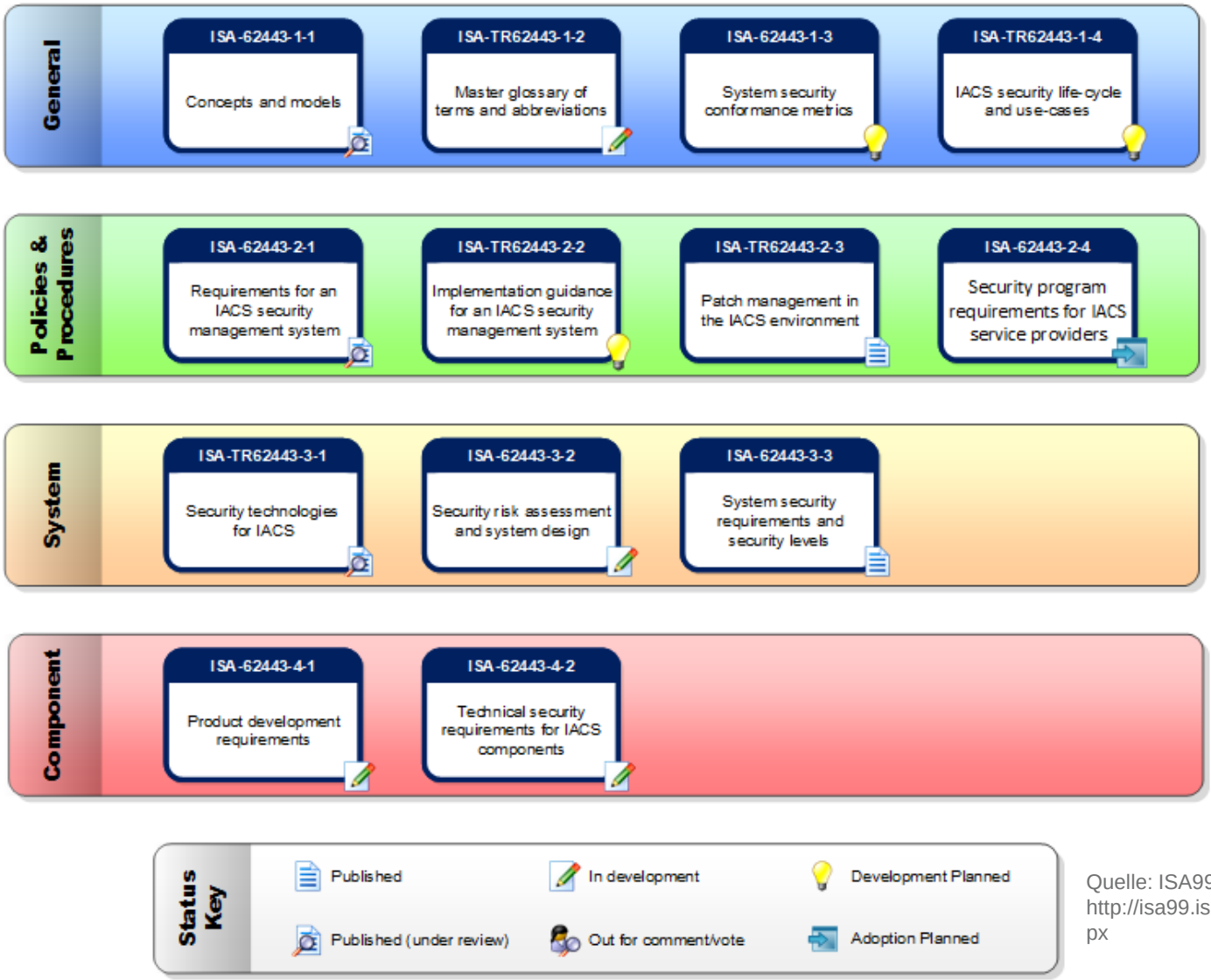
  auch anerkannt bei TÜV NORD CERT
  für Prüfungen nach IEC 62443

  Zertifizierung von

  - Komponenten (62443-4-1 und 62443-4-2)
  - Systemen (62443-3-3)
  - Anlagen (62443-2-1 und 62443-2-4)

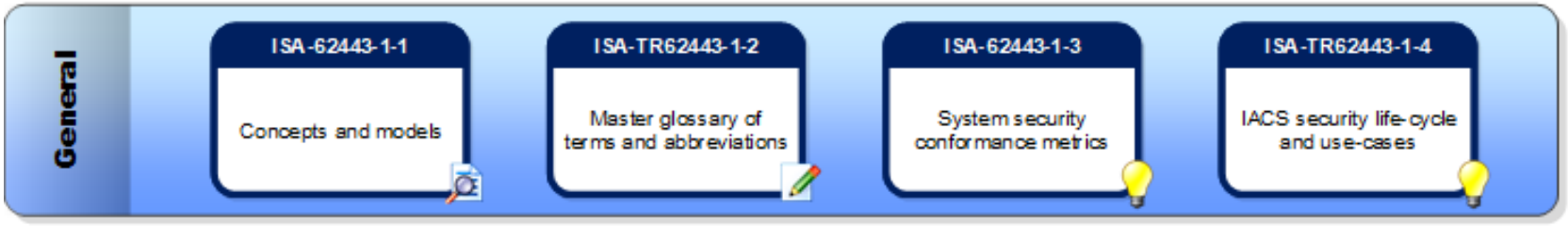
  – DAkkS akkreditierte Prüfungen

# Überblick über die IEC 62443



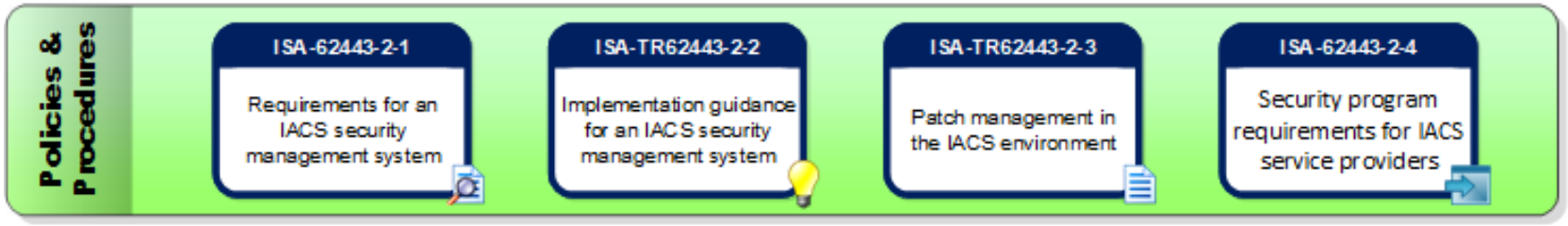

Quelle: ISA99 Committee
http://isa99.isa.org/ISA99%20Wiki/Home.aspx

- General



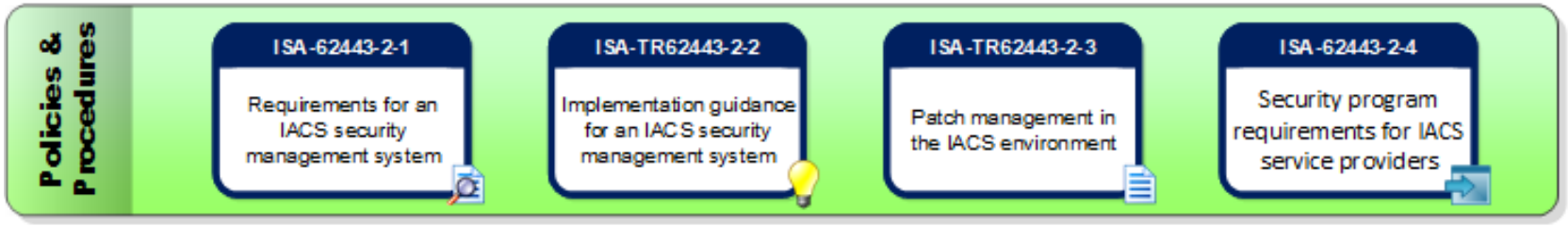

- Beinhaltet Terminologien und Methoden
  - 62443-1-1: Definition von Begriffen, Konzepten, Basis für andere Teile der 62443,
  - 62443-1-2: „Wörterbuch“ (Bezeichnungen und Abkürzungen),
  - 62443-1-3: Compliance Metrik für ein System,
  - 62443-1-4: Modell eines Life-Cycles

- Policies & Procedures (1)



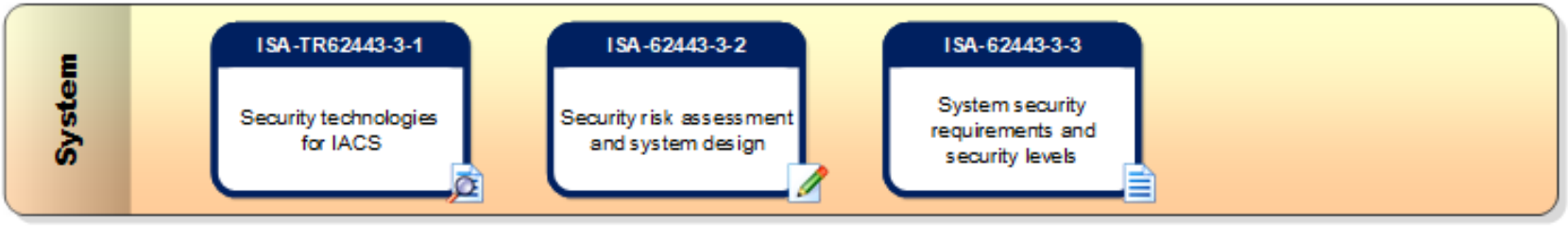

- Organisatorische Maßnahmen und Prozesse
  - 62443-2-1: Organisatorische Maßnahmen und Prozesse des Betreibers,
  - 62443-2-2: Betrieb und Erstellung eines Cyber Security Programms

- Policies & Procedures (2)



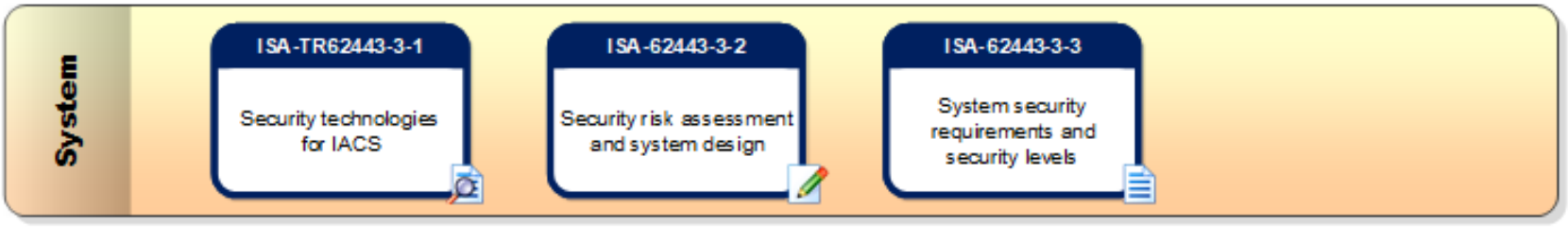

- Organisatorische Maßnahmen und Prozesse
  - 62443-2-3: Technischer Teil, der Anforderungen an die Erstellung/Pflege eines Patch-Managements enthält,
  - 62443-2-4: Anforderungen an die Integrations- und Wartungsprozesse eines Dienstleisters

- System (1)



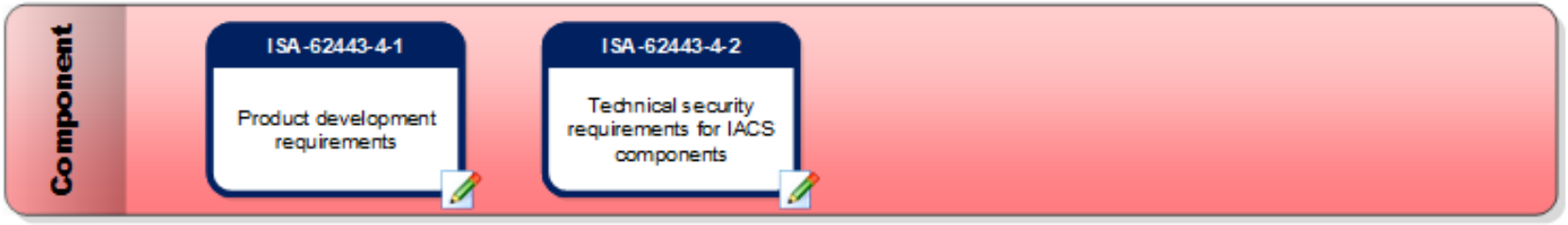

- Beinhaltet Anforderungen an das System an Hersteller / Integrator
  - 62443-3-1: Auflistung von IT- Sicherheitsmaßnahmen nach aktuellem Stand der Technik

- System (2)



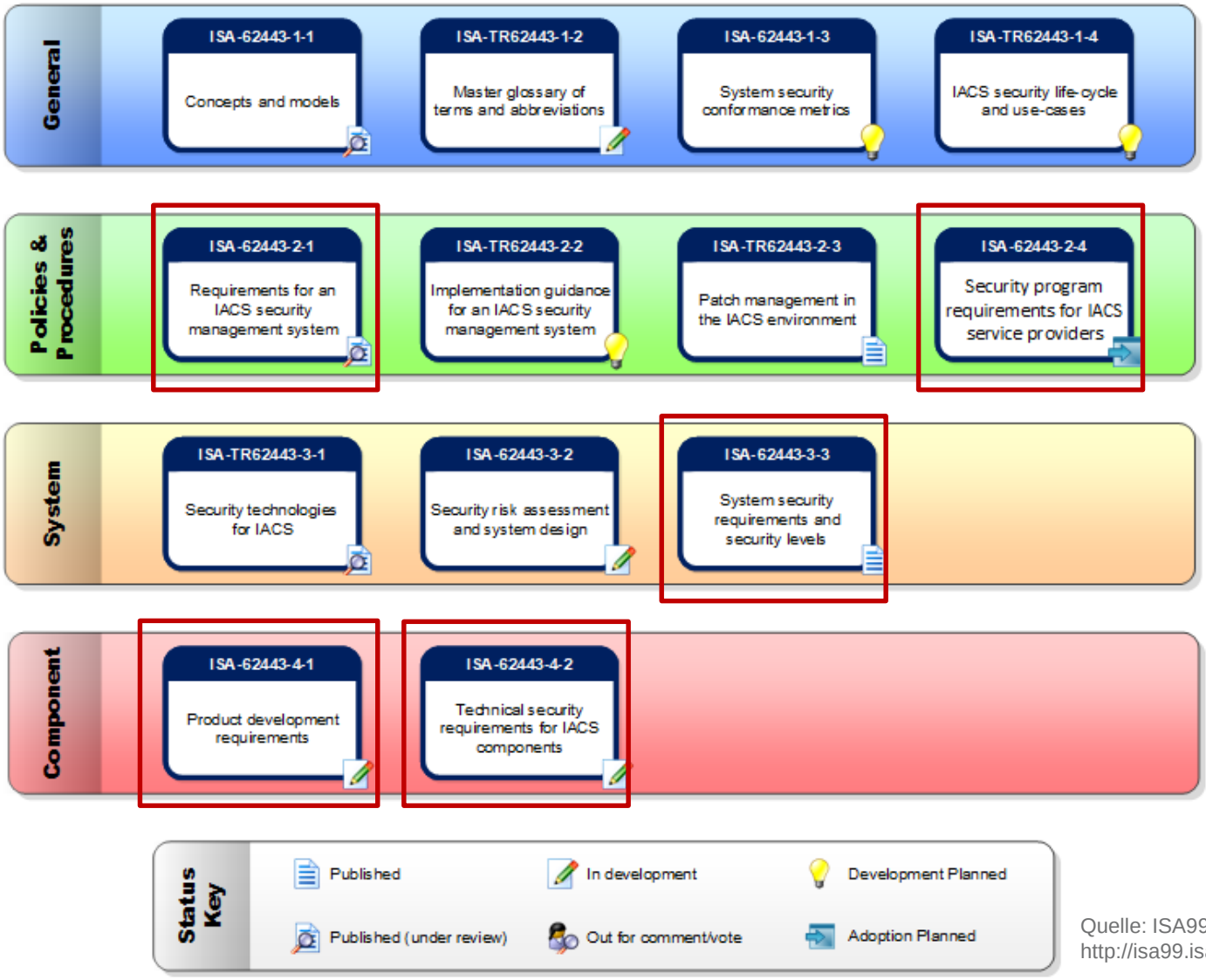

- Beinhaltet Anforderungen an das System an Hersteller / Integrator
  - 62443-3-2: Aufteilung in Zonen und Risk Assessment,
  - 62443-3-3: Funktionale Anforderungen an das System und Definition von Security Levels

- Component




- Anforderungen an den Hersteller von Komponenten
  - 62443-4-1: Entwicklungsprozess, beinhaltet 8 Practices von Spezifikation bis zur Testphase,
  - 62443-4-2: Funktionale Anforderungen an die Komponente

# Zertifizierungen nach IEC 62443




Quelle: ISA99 Committee
http://isa99.isa.org/ISA99%20Wiki/Home.aspx

# IEC 62443-4-1

- Überblick IEC 62443-4-1
  - Fokus liegt nicht auf dem einzelnen Produkt
  - Fokus: Bewertung des Entwicklungsprozesses
  - „Security By Design“
  - 8 Practices
  - Bewertung anhand eines Reifegrad-Modells

- Practices innerhalb der IEC 62443-4-1
  - Practice 1 - Security Management
  - Practice 2 - Specification of security requirements
  - Practice 3 - Secure by design
  - Practice 4 - Secure implementation
  - Practice 5 - Security verification and validation testing
  - Practice 6 - Security defect management
  - Practice 7 - Security update management
  - Practice 8 - Security guidelines

- Reifegradmodell (Maturity Model)

| Level | CMMI-SVC | 62443-4-1 | Beschreibung |
|---|---|---|---|
| **1** | Initial | Initial | Die Prozesse sind ad-hoc, schwach kontrolliert und nicht voraussagbar. |
| **2** | Managed | Managed | Prozesse werden reaktiv gelebt. |
| **3** | Defined | Defined (Practiced) | Die Prozesse sind dokumentiert und werden proaktiv umgesetzt. |
| **4** | Quantitavely Managed | Improving | Die Prozesse werden bewertet, kontrolliert und kontinuierlich verbessert. |
| **5** | Optimizing | | |

- Beispiel
  - Practice 7 – Security Update Management
    - PM-2 Security update documentation
  - Anforderungen:
    - Implementierung eines Prozesses für die Entwicklung von Dokumentation für den Produkt-Anwender bezüglich Security Updates
      - Versionsnummer
      - Anleitung zum Einspielen des Updates
      - Anleitung zur Überprüfung des Updates

# Zertifizierungen nach IEC 62443-4-2

- Auswahl eines Security Levels (SL)

| SL-Stufe | Widerstandsfähigkeit gegen Angriffe |
|---|---|
| SL 1 | • nicht gezielter Angriff |
| SL 2 | • aktiver, zielgerichteter Angriff<br>• einfache Mittel<br>• allgemeines IT-Wissen<br>• geringe Motivation |
| SL 3 | • aktiver, zielgerichteter Angriff<br>• erweiterte Werkzeuge und Ressourcen (Zeit, Geld)<br>• industrie-spezifisches Wissen<br>• mittlere Motivation |
| SL 4 | • aktiver, zielgerichteter Angriff<br>• umfangreiche Werkzeuge und Ressourcen (Zeit, Geld)<br>• industrie-spezifisches Wissen<br>• hohe Motivation |

→ SL-Stufe definiert die Tiefe der Prüfungen

- Einordnung in Komponenten-Klassen
  - Embedded Devices
    - z. B.: Sensoren, PLCs
  - Host Devices
    - z. B.: Workstations, Notebooks
  - Network Devices
    - z. B.: Industrial Router, Firewalls
  - Applications
    - z. B.: Software für Archivierung

→ Komponenten-Klasse definiert die zu erfüllenden Anforderungen

# Anforderungen der 62443-4-2

- Anforderungen der Prüfung (1)
  - FR 1 – Identification and authentication control
    - Identifizierung und Authentifizierung
    - 14 Anforderungen (Component Requirements)
  - FR 2 – Use control
    - Nutzungskontrolle
    - 12 Component Requirements
  - FR 3 – System integrity
    - Systemintegrität
    - 10 Component Requirements
  - FR 4 – Data confidentiality
    - Vertraulichkeit der Daten
    - 3 Component Requirements

- Anforderungen der Prüfung (2)
  - FR 5 – Restricted data flow
    - Eingeschränkter Datenfluss
    - 4 Component Requirements
  - FR 6 – Timely response to events
    - Rechtzeitige Reaktion auf Ereignisse
    - 2 Component Requirements
  - FR 7 – Resource availability
    - Verfügbarkeit der Ressource
    - 8 Component Requirements

- Vergleich Anforderungen in verschiedenen SL-Stufen

| | SL 1 | SL 2 | SL 3 | SL 4 |
|---|---|---|---|---|
| **FR 1 – Identification and authentication control** | | | | |
| CR 1.1 – Human user identification and authentication | x | x | x | x |
| RE (1) Unique identification and authentication | | x | x | X |
| RE (2) Multifactor authentication for all interfaces | | | | x |
| CR 1.2 – Software process and device identification and authentication | | x | x | x |
| RE (1) Unique identification and authentication | | | x | x |
| […] | | | | |

# Ablauf einer exemplarischen Prüfung am Beispiel „Industrial Firewall“

- Ablauf einer Prüfung (1)
  - Initialer Workshop
    - Einordnung Produkt-Klasse
      - Network Device
    - Festlegung SL-Stufe
      - Exemplarisch SL 2
    - Diskussion der Anforderungen
    - Produktumfang kennenlernen
      - Bsp: Anzahl Interfaces des Produkts
  - Angebotsphase

- Ablauf einer Prüfung (2)
  - Übergabe Systemspezifikation
    - Schnittstellenbeschreibung
  - Kick-Off und Inbetriebnahme mit dem Hersteller
  - Konformitätsprüfungen
    - Beispiele
      - FR 1, CR 1.1: Human user identification and authentication
      - FR 7, CR 7.1: Denial of service protection
      - FR 1, CR/NDR 1.6: Wireless access management

- Beispiel – FR 1, CR 1.1 Human user identification and authentication
  - Relevant für alle Komponenten-Klassen
  - Relevant ab SL 1
  - SL 1:
    - The application or device shall provide the capability to identify and authenticate all human users according to […] on all interfaces capable of human user access […].
    - Authentifizierung und Identifizierung von menschlichen Nutzern an allen Interfaces mit menschlichem Zugang

- Beispiel – FR 1, CR 1.1 Human user identification and authentication
  - SL 2 und SL 3:
    - […] shall provide the capability to **uniquely** identify and authenticate all human users.
    - Unterschied zu SL 1: Ein Benutzer muss eindeutig identifiziert werden
  - SL 4:
    - […] shall provide the capability to **employ multifactor authentication** for all human user access […]
    - Unterschied zu SL 2 und SL 3: Möglichkeit zur Multifaktor Authentifizierung

- „Peak-Beispiel“ – FR 7, CR 7.1 Denial of service protection
  - Relevant für alle Komponenten-Klassen
  - Für SL 1:
    - […] shall provide the capability to maintain essential functions in a degraded mode during a DoS event
  - Ab SL 2:
    - […] shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information and/or message flooding types of DoS events.

- Beispiel – Network Device Requirement
  - FR 1, CR 1.6 – Wireless access management
  - Ausschließlich für Komponenten der Klasse “Network Device” relevant
  - Anforderung:
    - SL 1: […] supporting wireless access management shall provide the capability to **identify and authenticate all users** (humans, software processes, or devices) engaged in wireless communication.
    - Ab SL 2: […] **uniquely** identify and authenticate […]

- Ablauf einer Prüfung (3)
  - Schwachstellenanalyse
    - Beispiel „Human user identification and authentication“
      - Prüfung auf Umgehung der Authentifizierung / Identifizierung
  - Zertifizierungsphase
    - Übergabe / Abnahme Prüfbericht
    - Entscheidung über Zertifizierung und Zertifikatsvergabe

# Fazit / Ausblick

- Fazit / Ausblick
  - **Der** Standard für Industrieprodukte
  - Bereits Adaption in anderen Märkten, z. B. Medizin
  - „offizielle“ Akkreditierung ermöglicht vergleichbare Zertifizierungen
  - Meist Vorarbeiten und ggf. Änderungen im Produkt nötig
  - Frühzeitig Anforderungen in den Entwicklungsprozess integrieren
  - Erste zertifizierte Komponenten 2018
  - „Compliance“

# secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle