TÜV AUSTRIA GRUPPE

TÜV TRUST IT
TÜV AUSTRIA Group

Herausforderungen und Best Practices IEC 62443

Brunn, Oktober 2024

Vortragender

- Senior OT-Security Consultant
- 9 Jahre tätig im Bereich kritischer Infrastruktur (Energie)
- Schwerpunkte NIS, ISMS, IEC 62443, OT-Security, IT-Security
- Berufener Auditor für NIS (technischer Prüfer) und IEC 62443

Florian-Sebastian Prack

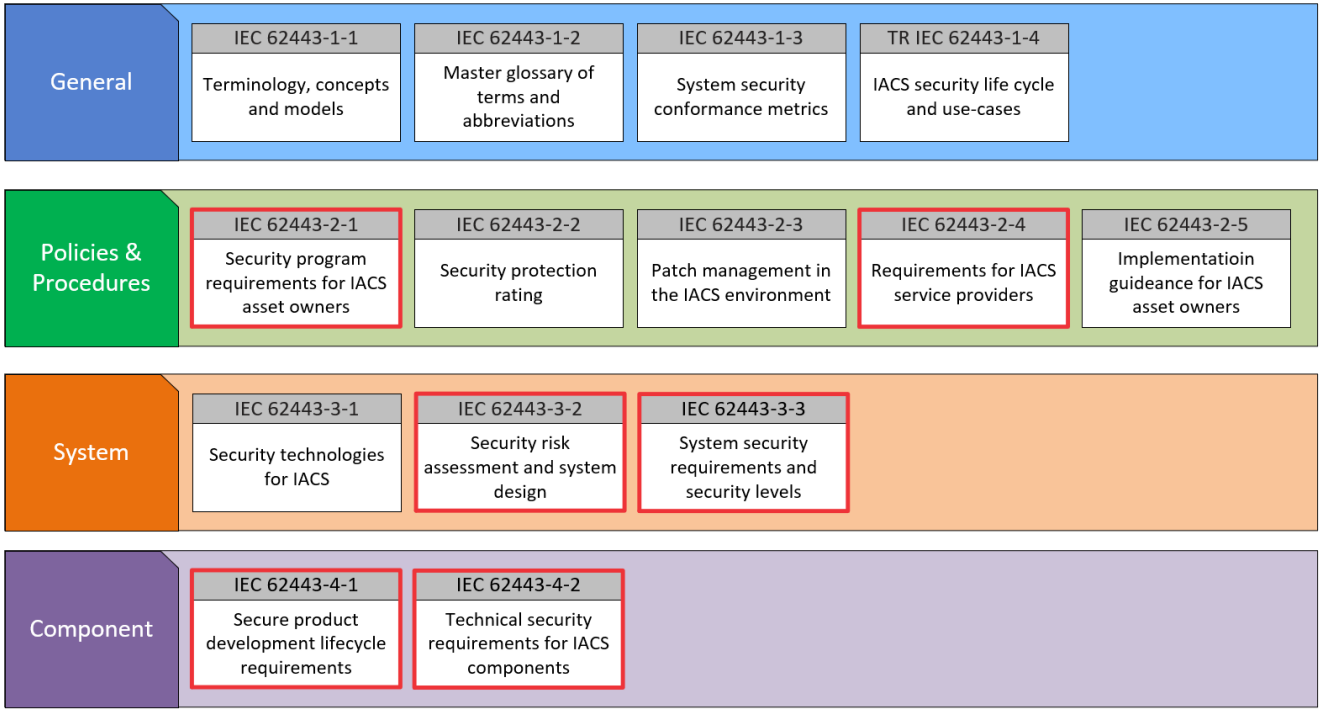
IEC 62443

- ✓ Die IEC 62443-Serie wurde Anfang 2000er Jahre erarbeitet
- ✓ Die erste offizielle Veröffentlichung eines Teils der IEC 62443 erfolgte 2007 durch die ISA als ANSI/ISA-99-Serie.

- ✓ Wer hat schone eine Zertifizierung genossen?

IEC 62443 - Übersicht über die Normenreihe

Was ist davon jetzt zertifizierbar?



TÜV AUSTRIA ist akkreditierte Inspektions- und Zertifizierstelle für diese Teilnormen

Akkreditierung Austria

Agenda

- Die Normenreihe in der Praxis
- Was gibt es bei der Zertifizierung zu beachten (ML & SL)
- Wo haben die Kunden die häufigsten Probleme?
- Wie ist der Ablauf (Zeit) und was sind die Ergebnisse?

Die Normenreihe in der Praxis

Policies & Procedures	CSMS mit Fokus auf Steuerungstechnik Anforderungen an Lieferanten Zentrales Thema: Risikomanagement, Access Control, Netzwerksegmentierung, Physische Sicherheit, Monitoring und KVP, Systemwartung
System	Systemdesign basierend auf der Risikobeurteilung (Zones & Conduits) Zentrales Thema: Zonendefinition, Festlegung von Security Level Target, Spezifische Anforderungen pro Zone / pro Security Level
Component	Secure Software Development und „Sichere Produkt“ Zentrales Thema: SDL CI/CD Pipeline, Dokumentationen für Kunden, Schwachstellenmanagement, Definition „Sicheres Produkt“ (Härtung)

ML in den Prozessen

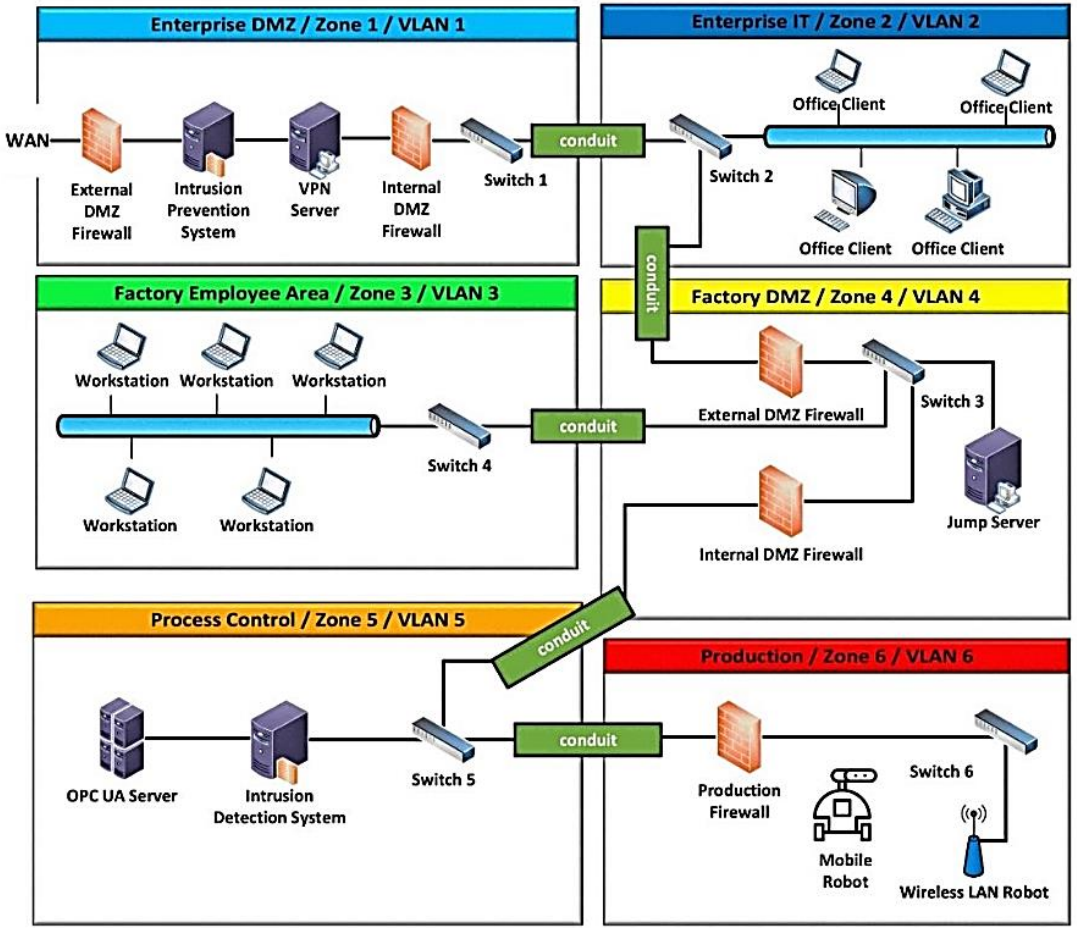
	Maturity Level	Kategorie	Beschreibung
	1	Initial	ohne einen dokumentierten Prozess, der schlecht kontrolliert wird
	2	Managed	mit einem formal dokumentierten Prozess mit Nachweis von Fachwissen und geschultem Personal
	3	Defined	auf Reifegrad 2 und demonstriert die Verwendung definierter, etablierter und dokumentierter Prozesse sowie definierter Schulungsschemata für das Personal
	4 & 5	Improving	auf Reifegrad 3 sowie Nachweis kontinuierlicher Verbesserung

Was sind jetzt Zonen?

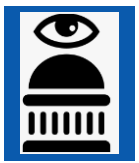
Klare Definition der Assets pro Zone

- WIFI Zone
- Safety Zone
- Temporäre Geräte
- Enterprise IT
- Externe Verbindungen

Definierte Zonenübergange (conduits) vorzugsweise mit FW



Was gibt es zu beachten?

	Security Level	IACS Angreifer gegen den ich mich verteidigen möchte…
	1	zufällige oder unbeabsichtigte Systemverletzung
	2	vorsätzliche Cyberbedrohungen durch böswillige Benutzer mit grundlegenden, allgemeinen Fähigkeiten und geringem Zugriff auf Ressourcen
	3	vorsätzliche Cyberbedrohungen durch erfahrene und versierte böswillige Benutzer mit Zugriff auf moderate Ressourcen
	4	vorsätzliche Cyberbedrohungen durch motivierte, geschickte und versierte böswillige Benutzer mit Zugriff auf erhebliche Ressourcen

Häufigsten Probleme

- ✔ Security in der OT wofür? Ist doch eh alles abgeschottet
- ✔ 4-1 Zertifizierung nach ML 2 =! 4-2 Zertifizierung nach SL 2
- ✔ Gewachsene Strukturen
- ✔ Wenig zertifizierte Komponenten am Markt für eine 3-3 SL 3+
- ✔ Scope Eingrenzung
- ✔ Netzwerksegmentierung
- ✔ Ressourcen

Maturity Level					
	ML 4	PL 1 +	PL 2 +	PL 3 +	PL 4+
	ML 3	PL 1	PL 2	PL 3	PL 4
	ML 2	PL 0	PL 0	PL 0	PL 0
	ML 1	PL 0	PL 0	PL 0	PL 0
		SL 1	SL 2	SL 3	SL 4
PL = Protection Level	Security Level				

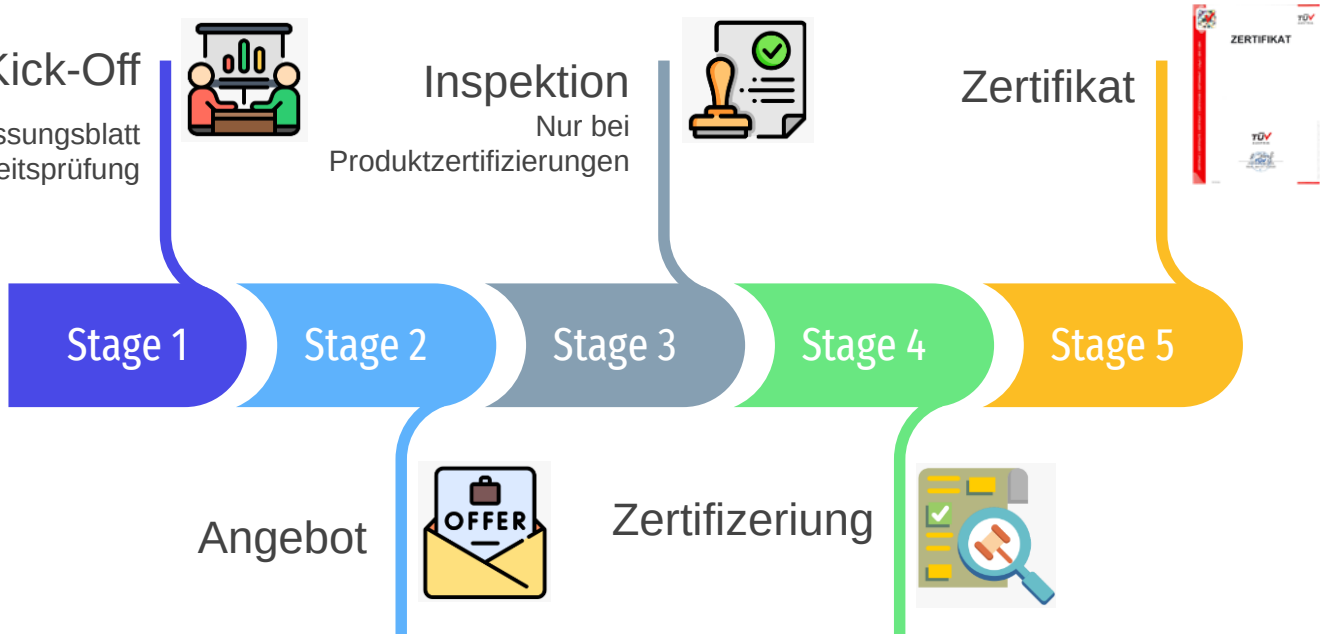
PERA – PURDUE Model

4	Enterprise Systems	Engineering, Business, Planning, Logistics
3	Manufacturing operations	Central SCADA, MES/MOMS, Historian
2	Control Systems	Local SCADA, DCS, HMI
1	Smart Devices	PLC, DCS, Safety Systems
0	Process	Smart field devices Sensors, Actuators

PERA – Added ICS Security Boundaries

5	Enterprise Networks	Datacenter
4	Business Planning & Logistics	Site Systems & Networks
3	Operations & Controls	Simulation, Engineering, Test
2	Area Supervisory Control	HMIs, Historians
1	Basic Control	PLCs, RTUs, IEDs
0	Process	Smart field devices Sensors, Actuators
S	Safety	Safety Instrumented System

Ablauf



Zeitraum 4-6 Monate

Fragen?

TÜV TRUST IT
TÜV AUSTRIA Group

Brunn, Oktober 2024

TÜV AUSTRIA GRUPPE

TÜV TRUST IT
TÜV AUSTRIA Group

Vielen Dank für Ihre Aufmerksamkeit!

Florian-Sebastian Prack, Msc
Senior OT-Security Consultant

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
Mobil: +43 664 60454 6735

florian-sebastian.prack@tuv.at
www.tuv.at

Brunn, Oktober 2024