IEC62443 Überblick, Netzwerksegmentierung & Backup

Markus Ripka, RMG Zukunft GAS 2025

AUSTRIA AG
Renewables and Gas

RAG Austria AG

Ing. Mag. (FH) Markus Ripka
Chief Information Security Officer

Markus.ripka@rag-austria.at
T +43 (0)50 724-5243

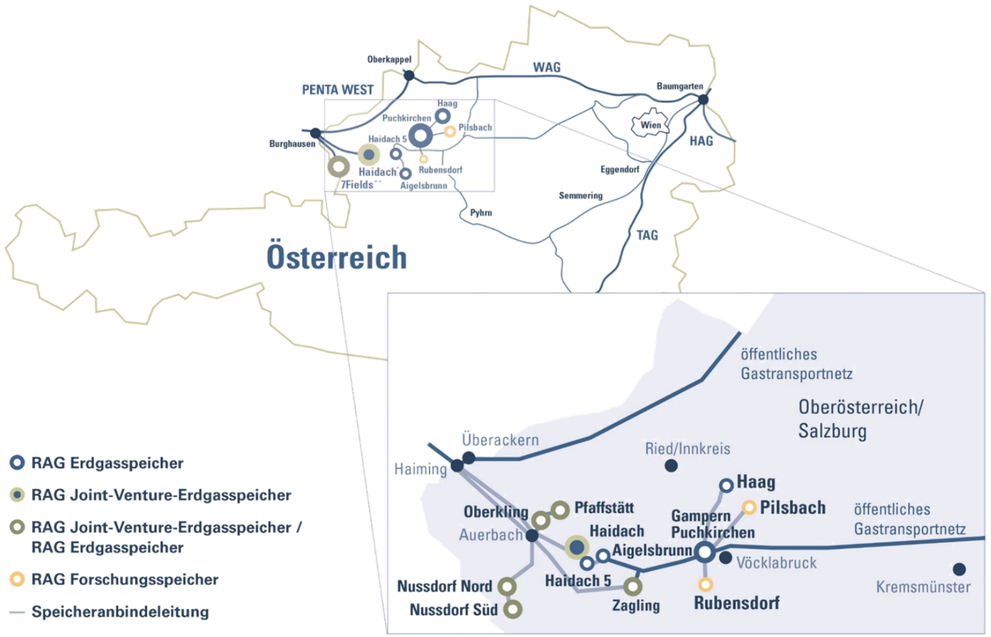
RAG Austria AG
Schwarzenbergplatz 16
A-1015 Wien

www.rag-austria.at

AUSTRIA AG
Renewables and Gas

Überblick RAG und JV Speicher Standorte

- Die RAG entwickelt und betreibt 11 Speicherstationen, sechs davon im Rahmen von Joint-Ventures sowie die Forschungsspeicher Pilsbach und H2-Rubensdorf mit einem Gesamtspeicher-volumen von mehr als 6,2 Mrd. m³



* Haidach: Joint Venture mit Gazprom export und Wingas ** 7Fields: Joint Venture mit Uniper Gas Storage

Erdgasspeicher Puchkirchen/Haag		
Arbeitsgasvolumen	12,2 TWh	1.080 Mio. m³
Max. Ausspeicherkapazität	5,9 GW	520.000 m³/h
Max. Einspeicherkapazität	5,9 GW	520.000 m³/h

Erdgasspeicher Haidach 5		
Arbeitsgasvolumen	181 GWh	16 Mio. m³
Max. Ausspeicherkapazität	227 MW	20.000 m³/h
Max. Einspeicherkapazität	227 MW	20.000 m³/h

Erdgasspeicher Haidach		
Arbeitsgasvolumen	32,9 TWh	2.900 Mio. m³
Max. Ausspeicherkapazität	13,1 GW	1,16 Mio. m³/h
Max. Einspeicherkapazität	11,9 GW	1,05 Mio. m³/h

Erdgasspeicher Aigelsbrunn		
Arbeitsgasvolumen	1,5 TWh	130 Mio. m³
Max. Ausspeicherkapazität	567 MW	50.000 m³/h
Max. Einspeicherkapazität	567 MW	50.000 m³/h

Erdgasspeicher 7Fields (RAG)		
Arbeitsgasvolumen	6,2 TWh	550 Mio. m³
Max. Ausspeicherkapazität	2,6 GW	226.600 m³/h
Max. Einspeicherkapazität	1,7 GW	151.100 m³/h

Erdgasspeicher 7Fields (UNIPER)		
Arbeitsgasvolumen	17,6 TWh	1.550 Mio. m³
Max. Ausspeicherkapazität	9,1 GW	807.300 m³/h
Max. Einspeicherkapazität	6,1 GW	538.200 m³/h

Summe der von RAG betriebenen Speicher		
Arbeitsgasvolumen	70,5 TWh	6.226 Mio. m³
Max. Ausspeicherkapazität	31,5 GW	2.783.900 m³/h
Max. Einspeicherkapazität	26,4 GW	2.329.300 m³/h

Leistungskennzahlen RAG Speicher im Stand Dezember 2020

Überblick RAG und JV Speicher Standorte

- In den letzten Jahren hat sich die „konventionelle“ Sicherheit - i.S. von Einhaltung von technischen Normen und Rechtsvorschriften - verstärkt auch in Richtung digitaler und physischer Sicherheit im Bergbau entwickelt (Cyberattacken, Umweltaktivisten, etc.). Die RAG als Betreiber wesentlicher Dienste (KRITIS) setzt dabei auf international anerkannte Standards und Sicherheitsüberprüfungen.


Puchkirchen


Haag


Pilsbach / Lehen


Haidach


Oberkling


Zagling


Aigelsbrunn


Haidach 5


Rubensdorf


Nussdorf


Pfaffstätt

Auszugsweiser Überblick Normenreihe IEC62443

- IEC 62443-1: Allgemeine Grundlagen
- IEC 62443-2: Sicherheitsanforderungen für Betreiber und Dienstleister
  - 2-1 Aufbau eines Informationssicherheits-Managementsystems (ISMS)
  - 2-2 Rahmenwerk Evaluation des Schutzes einer Industriesteueranlage (IACS)
  - 2-3 Patch-Managementprogramm
  - 2-4 Anforderungen an IT-Sicherheitsprogramm von Dienstleistern
- IEC 62443-3: Sicherheitsanforderungen an Automatisierungssysteme
  - 3-1 Bewertung verschiedener Cybersicherheits-Tools, Gegenmaßnahmen und Technologien
  - 3-2 Risikoanalyse auf die Definition des betrachteten Systems und Aufteilung Zonen & Übergänge
- IEC 62443-4: Sicherheitsanforderungen an Automatisierungskomponenten
  - 4-1 Anforderungen an einen sicheren Entwicklungsprozess für Produkte & 4-2 Capabilities
- IEC 62443-6: Evaluationsmethodik

IEC62443-1 Foundational Requirements (FR)

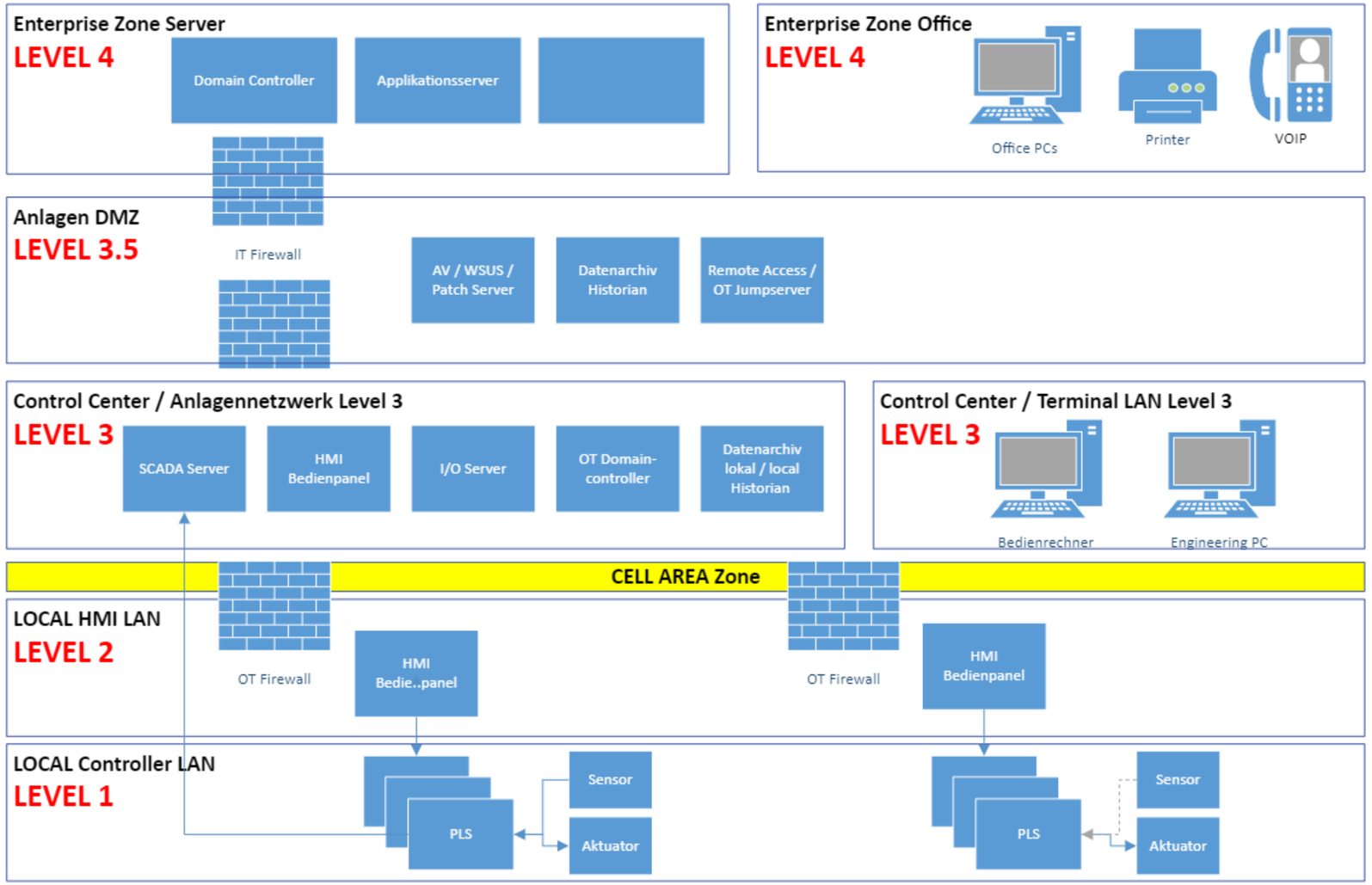
Nach IEC 62443-1-1 gibt es sieben grundlegende Sicherheitsanforderungen (FR) die dann ja nach Security Level Target (SLT) ausgestaltet werden können:

- FR1 Identifizierung und Authentifikation (IAC)
- FR2 Nutzungskontrolle (UC)
- FR3 Systemintegrität (SI)
- FR4 Vertraulichkeit der Daten (DC)
- FR5 eingeschränkter Datenfluss (RDF)
- FR6 rechtzeitige Reaktion auf Ereignisse (TRE)
- FR7 Verfügbarkeit der Ressourcen (RA)

IEC62443 Security Levels

Security Level	Beschreibung	Anforderungen	Foundational Requirements (FR)
SL0	kein Schutz erforderlich	- Keine Sicherheitsanforderungen	
SL1	Schutz vor zufälligen Verstößen	- Grundlegende Sicherheitsmaßnahmen - Authentifizierung und Autorisierung - Basis-Sicherheitsrichtlinien	Identifizierung und Authentifikation (IAC) Nutzungskontrolle (UC)
SL2	Schutz vor absichtlichen Verstößen mit geringen Fähigkeiten	- Erweiterte Sicherheitsmaßnahmen - Netzwerksegmentierung - Sicherheitsüberwachung und -protokollierung - Schwachstellenmanagement	eingeschränkter Datenfluss (RDF) Nutzungskontrolle (UC) Systemintegrität (SI)
SL3	Schutz vor absichtlichen Verstößen mit mittleren Fähigkeiten	- Strenge Sicherheitsmaßnahmen - Intrusion Detection Systeme (IDS) - Sicherheitsvorfall-Management - Regelmäßige Sicherheitsüberprüfungen und -tests	rechtzeitige Reaktion auf Ereignisse (TRE)
SL4	Schutz vor absichtlichen Verstößen mit hohen Fähigkeiten	- Höchste Sicherheitsmaßnahmen - Multi-Faktor-Authentifizierung - Verschlüsselung von Daten in Ruhe & Bewegung - Kontinuierliche Sicherheitsüberwachung und Sicherheitsverbesserung	rechtzeitige Reaktion auf Ereignisse (TRE) Verfügbarkeit der Ressourcen (RA)

FR5 Netzwerksegmentierung (Purdue Modell)



-> 9 FR 5 – Restricted data flow (RDF)
-> 9.3 SR 5.1 – Network segmentation
-> 9.4 SR 5.2 – Zone boundary protection

FR7 Verfügbarkeit der Ressourcen – OT Backup

- 11.5 SR 7.3 – Control system backup
  - Regelmäßige Erstellung von Backups
  - Sicherstellung, dass Backups sicher gespeichert werden
  - Implementierung von Mechanismen zur Datenwiederherstellung aus den Backups
- 11.6 SR 7.4 – Control system recovery and reconstitution
  - Implementierung von Wiederherstellungsplänen und -verfahren
  - Regelmäßige Tests und Übungen der Wiederherstellungsprozesse
  - Analyse Wiederherstellungsprozessen zur kontinuierlichen Verbesserung
- 11.7 SR 7.5 – Emergency power
  - Bereitstellung unterbrechungsfreien Stromversorgungen (USV) für kritische Systeme
  - Regelmäßige Tests und Wartung der Notstromversorgungssysteme
  - Dokumentation der Notstromversorgungssysteme und Wartungsprotokolle

OT Backup in der Praxis

- Sichere Backups und Auslagern der aktuellen Steuerprogramme inkl. Versionierung auf externe Datenträger. (3-2-1 Regel)
- Festplattenimage/Backups von Engineering PCs, Leitstand Rechnern sowie SCADA Servern
- Optimal Verwendung eines CVS (Concurrent Versions System) für Versionierung
- Laufende Sicherung flüchtiger Daten wie aktuelle Regelparameter und Grenzwertlisten
- Wiederanlaufplan pro Anlage inklusive MSR von Null. Kaltstart inkl. Einspielen der Steuerprogramme und Anlauf der Anlage
- Passwortmanagement. Sicherstellen Verfügbarkeit der Passwörter im Notfall
- Übungen der Wiederanlaufpläne und Datenrestore
- Ausreichend Redundanzen und Ersatzteile kritischer IT/OT Systeme

Disclaimer

Die RAG Austria AG ist bei der Recherche der in dieser Unterlage dargestellten Informationen, wie auch bei der Auswahl der von ihr verwendeten Informationsquellen um größtmögliche Sorgfalt bemüht. Dennoch kann RAG keinerlei Haftung für die Richtigkeit, Vollständigkeit und/oder Aktualität der in dieser Unterlage zur Verfügung gestellten Informationen bzw. Informationsquellen übernehmen. Die in dieser Unterlage dargestellten Informationen basieren auf dem Wissenstand und der Einschätzung zum entsprechenden, in der jeweiligen Unterlage angegebenen Zeitpunkt. Die RAG Austria AG behält sich das Recht vor, Änderungen (Ergänzungen, Einschränkungen udgl) der bereitgestellten Informationen vorzunehmen.

RAG haftet in keinem Fall für Verluste oder Schäden gleich welcher Art (einschließlich Folge- oder indirekter Schäden oder entgangenem Gewinn), die durch oder im Zusammenhang mit der Verwendung der in dieser Unterlage dargestellten Informationen entstehen könnten.

AUSTRIA AG
Renewables and Gas

RMG

RMG
ONE STEP AHEAD

RMG - Cyber Security - IEC62443 - 2025

AGENDA

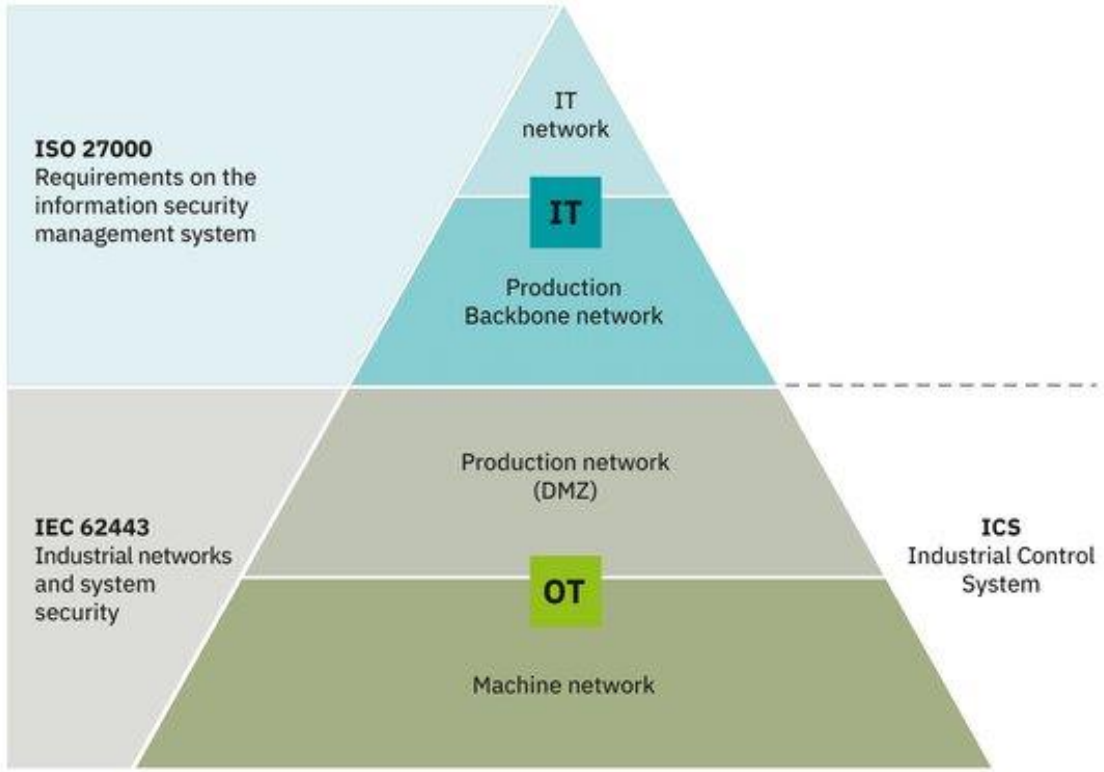
01	Warum IEC62443 – Cyber Security – IT/OT
02	Überblick IEC62443
03	Zusammenfassung- Anwendung

IEC 62443 Übersicht

- Die Normenreihe IEC 62443 *Industrial Communication Networks – Network and System Security* besteht aus mehreren Teilen, die in vier Bereiche eingeteilt werden:
  - **General:** Hier werden die grundsätzlichen Begriffe, Konzepte und Modelle beschrieben.
  - **Policies and Procedures:** Hier wird vor allem ein System zum Management industrieller IT- Sicherheit beschrieben.
  - **System:** Hier werden verschiedene Vorgaben für Sicherheitsfunktionen von Steuerungs- und Automatisierungssystemen beschrieben.
  - **Components and Requirements:** Hier werden die Anforderungen an Prozesse der Produktentwicklung von Komponenten einer Automatisierungslösung beschrieben.

IIEC 62443

- ist eine internationale Normenreihe über „Industrielle Kommunikationsnetze IT-Sicherheit für Netze und Systeme“.
- Die Normenreihe ist in verschiedene Bereiche unterteilt und beschreibt sowohl technische als auch prozessorale Aspekte der Industriellen Cyber Security.
- Sie unterteilt die Industrie in verschiedene Rollen: den Betreiber, die Integratoren (Dienstleister für Integration und Wartung) sowie die Hersteller. Die verschiedenen Rollen verfolgen jeweils einen risikobasierten Ansatz zur Vermeidung und Behandlung von Sicherheitsrisiken bei ihren Tätigkeiten.



SYSTEMS

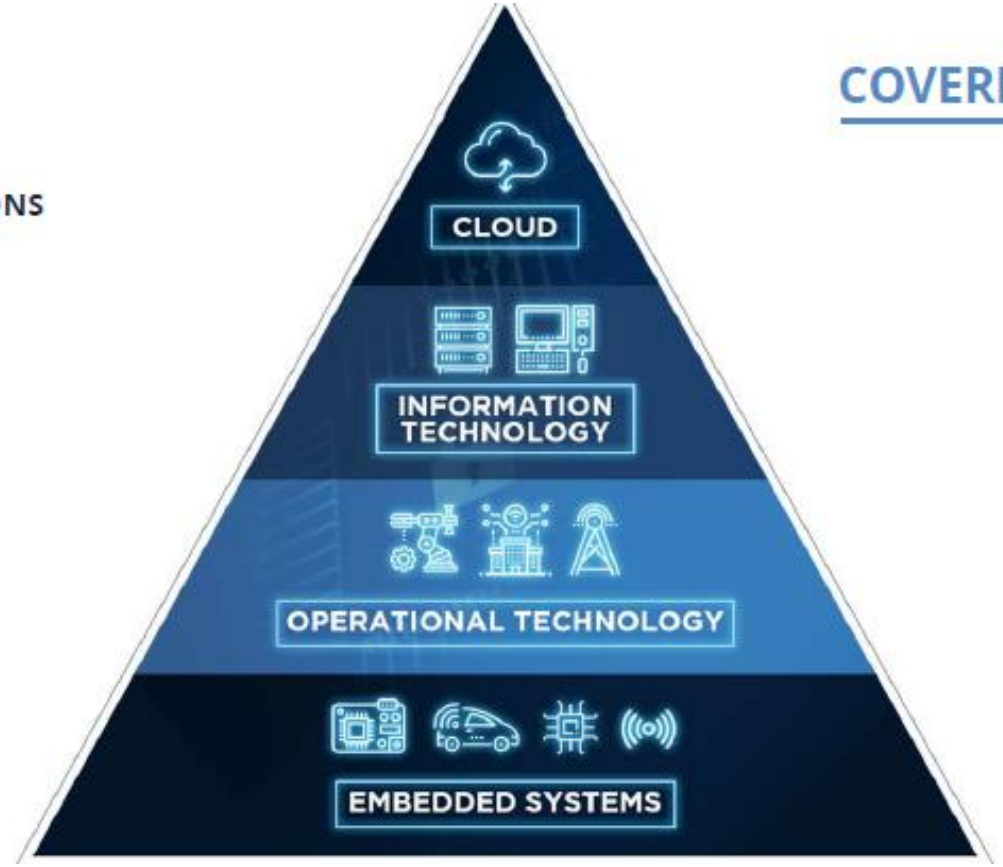
IOT PLATFORMS & APPLICATIONS

ON-PREMISE BACKEND

INDUSTRIAL NETWORKS

AUTOMOTIVE SENSORS & CONTROL UNITS

INDUSTRIAL SENSORS & CONTROL UNITS



COVERED STANDARDS

ISO/IEC 27034

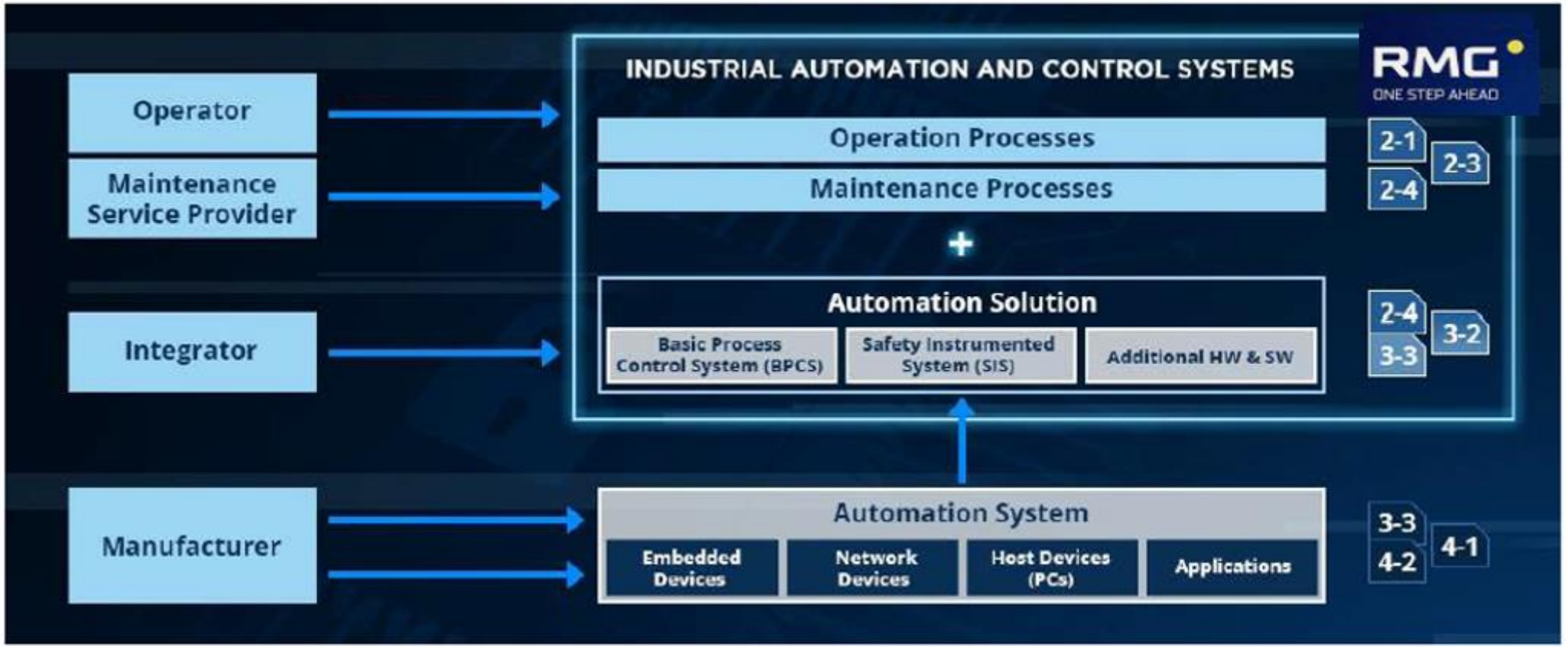
ISO 27001
TISAX®

IEC 62443

ISO/SAE 21434

IEC 62443

We help to achieve targeted protection levels by organizational & technical controls according to IEC 62443.



Security Level

Technische Anforderungen an Systeme (IEC 62443-3-3) und Produkte (IEC 62443-4-2) werden in der Norm durch vier sogenannte Security Level (SL) bewertet. Die verschiedenen Level geben dabei die Widerstandsfähigkeit gegenüber verschiedener Angreiferklassen an. Der Standard betont, dass dabei die Level pro technischer Anforderung gewertet werden sollen (vgl. IEC 62443-1-1) und nicht für die allgemeine Klassifizierung von Produkten geeignet sind.

Die Level sind:

- **Security Level 0**: Keine besondere Anforderung oder Schutz erforderlich.
- **Security Level 1**: Schutz vor unbeabsichtigtem oder zufälligem Missbrauch.
- **Security Level 2**: Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **Security Level 3**: Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen("Industrial Automation and Control Systems“). und moderater Motivation.
- **Security Level 4**: Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

IEC 62443
Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 IACS Security Protection Ratings	3-2 Security risk assessment for 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		
	2-5 Implementation guidance for IACS asset owners		

Process requirements (maturity level)
Technical requirements (security level)

Reifegrade

Die IEC 62443 beschreibt verschiedene Reifegrade für Prozesse und technische Anforderungen. Die Reifegrade für Prozesse orientieren sich dabei an den Reifegraden aus dem CMMI-Framework.

Maturity Level

Angelehnt an CMMI(Capability Maturity Model Integration) beschreibt die IEC 62443 verschiedene Reifegrade für Prozesse durch sogenannte „Maturity Level“. Für die Erfüllung einer bestimmten Stufe eines Reifegrades müssen immer alle prozessualen Anforderungen bei der Produktentwicklung bzw. Integration praktiziert werden, d. h. die Auswahl von nur einzelnen Kriterien („Cherry Picking“) ist nicht standardkonform.

Die Reifegrade sind dabei wie folgt beschrieben:

- Maturity Level 1 **- Initial**: Produktlieferanten führen die Produktentwicklung in der Regel ad hoc und oft undokumentiert (oder nicht vollständig dokumentiert) durch.
- Maturity Level 2 - **Managed**: Der Produktlieferant ist in der Lage, die Entwicklung eines Produkts gemäß schriftlicher Richtlinien zu verwalten. Es muss nachgewiesen werden, dass das Personal, das den Prozess durchführt, über das entsprechende Fachwissen verfügt, geschult ist und/oder schriftliche Verfahren befolgt. Die Prozesse sind wiederholbar.
- Maturity Level 3 - **Defined** (practiced): Der Prozess ist in der gesamten Organisation des Lieferanten wiederholbar. Die Prozesse sind praktiziert worden, und es gibt Belege dafür, dass dies geschehen ist.
- Maturity Level 4 - **Improving**: Anhand geeigneter Prozessmetriken kontrollieren die Produktlieferanten die Wirksamkeit und Leistung des Prozesses und weisen eine kontinuierliche Verbesserung in diesen Bereichen nach.

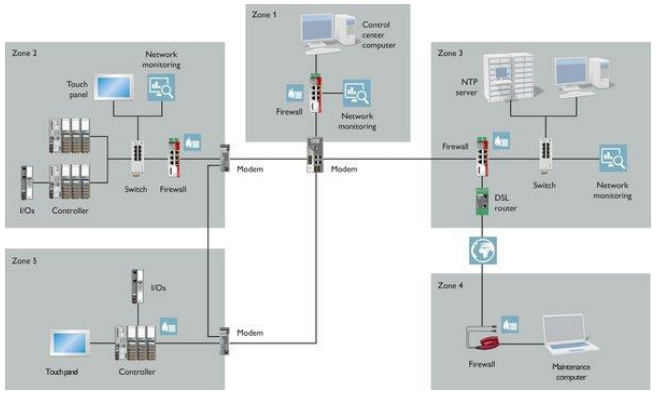
IIEC 62443

Defense in Depth

Defense in Depth („Verteidigung in der Tiefe“) ist ein Konzept, bei dem mehrere Ebenen von Sicherheitsvorkehrungen (Verteidigung) über das gesamte System verteilt sind. Das Ziel ist hierbei, Redundanz für den Fall zu schaffen, dass eine Sicherheitsmaßnahme ausfällt oder eine Schwachstelle ausgenutzt wird.

Zones & Conduits

Zones unterteilen ein System in homogene Zonen durch Gruppierung der (logischen oder physischen) Anlagen mit gemeinsamen Sicherheitsanforderungen. Die Sicherheitsanforderungen werden über Security Level (SL) definiert. Das für eine Zone erforderliche Niveau wird durch die Risikoanalyse ermittelt.
Conduits gruppieren die Elemente, die die Kommunikation zwischen zwei Zonen erlauben. Sie stellen Sicherheitsfunktionen bereit, die eine sichere Kommunikation ermöglichen und die Koexistenz von Zonen unterschiedlicher Sicherheitsstufen erlauben.

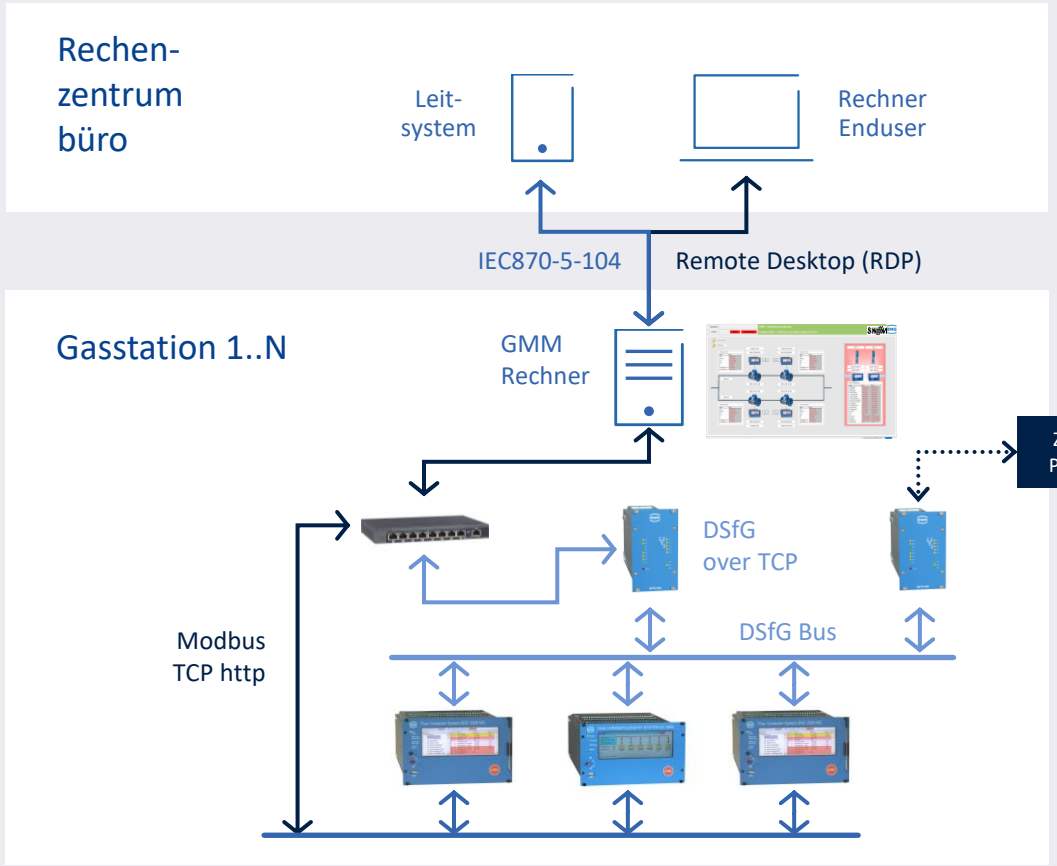


Auf den Punkt gebracht

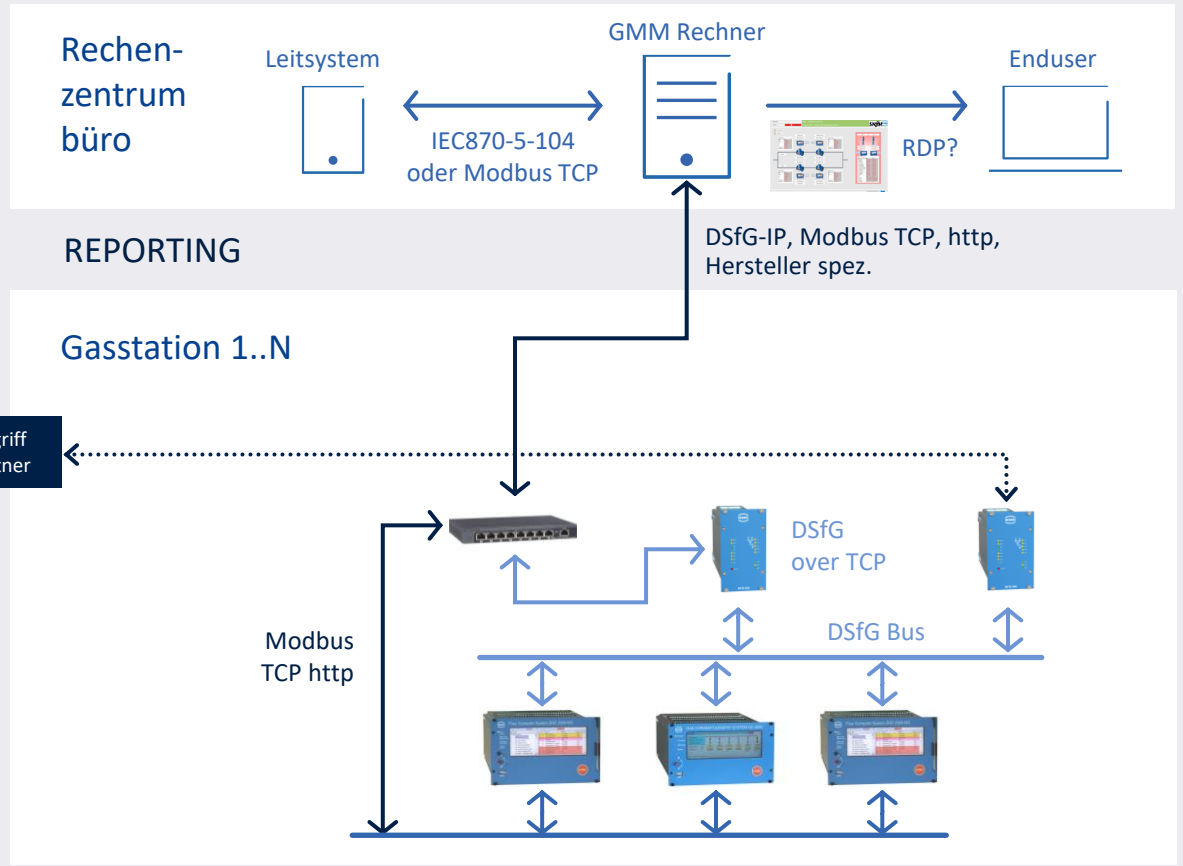
- Security Level, Zonen
- Verschlüsselte Kommunikation, auch auf dem Bus
- IP – Kommunikation, **OPC-UA** ist explizit genannt
- Der Anlagenbetreiber steht in der Aufsichtspflicht
- Hersteller müssen Geräte auf den Einsatzort abstimmen.

GAS METERING MANAGEMENT | Terminal - Installationsvarianten

Variante 1: Ein GMM Rechner in jeder Gasstationen



Variante 2: Ein GMM Rechner für alle Gasstationen (Geplant)




THANK YOU
Teşekkürler
Merci
Obrigado
Gracias
ありがとうございました
Danke
Děkuji
谢谢
Спасибо
நன்றி
धन्यवाद
شكرا
ευχαριστώ
Grazie
Tack ska ni ha
Cảm ơn bạn
감사합니다

JÖRG SCHÖNBACH
DIRECTOR BUSINESS DEVELOPMENT & AUTOMATION

RMG Messtechnik GmbH

Otto-Hahn-Straße 5
35510 Butzbach
Deutschland
Tel. +49 (0) 6033 897-411
Mob: +49 1725372266
Joerg.schoenbach@rmg.com
www.rmg.com

Mail info@rmg.com