



Dzień dobry

„Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych”

Kamil Wachowicz

Agenda

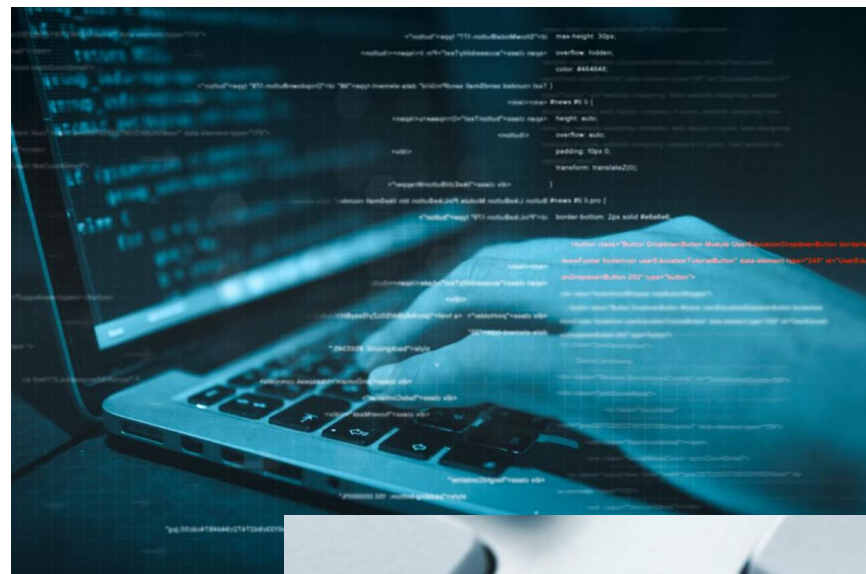
- Regulacje prawne w skrócie
- Koncepcje bezpieczeństwa i środki zaradcze
- Wybrane rozwiązania zapewniające bezpieczeństwo sieci
- IEC 62443 w Phoenix Contact



Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych

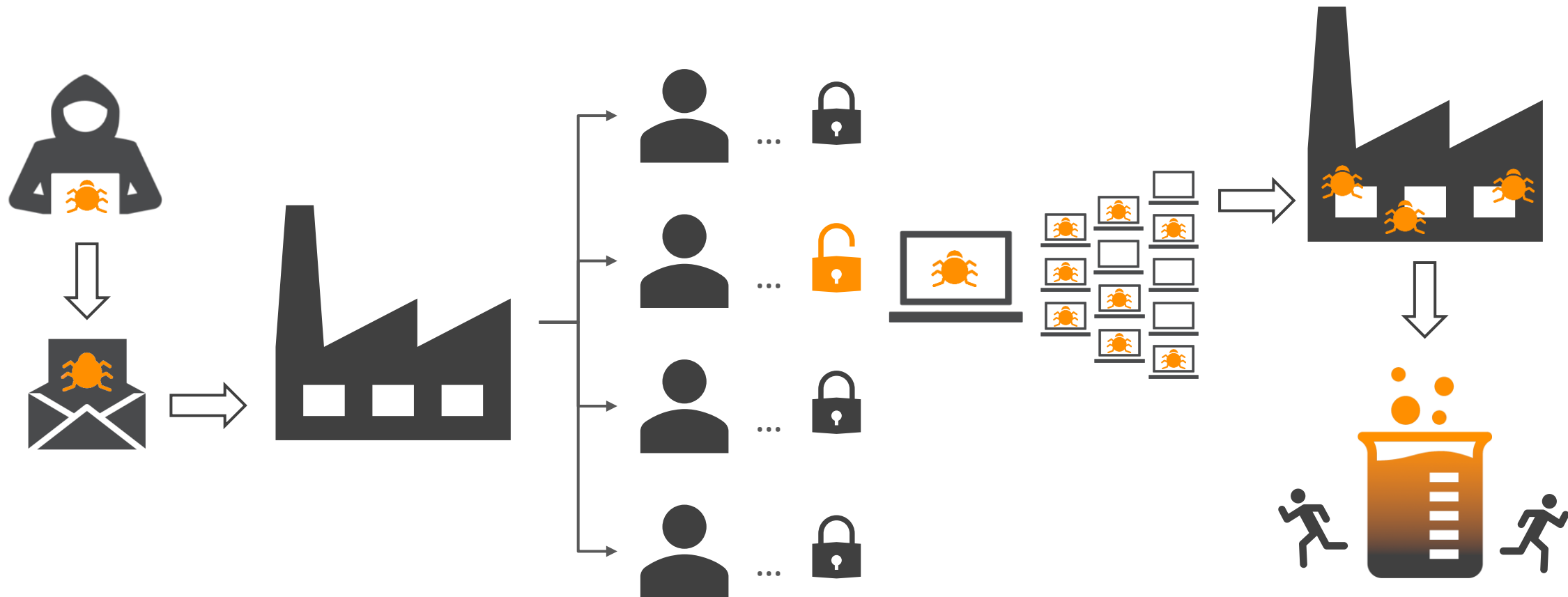
Cyberataki w Polsce

Ile było cyberataków w 2024 r ?



Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych

Jak przeprowadzane są cyberataki?



Regulacje prawne

Regulacje prawne, normy i standardy

IEC 62443 to zestaw globalnie akceptowanych (UE, USA,...) standardów bezpieczeństwa dedykowanych specjalnie do ochrony systemów automatyki przemysłowej i sterowania (IACS).

NIS 2 (Network and Information Systems Directive 2)

- Dyrektywa EU która zaostrza wymagania w zakresie cyberbezpieczeństwa dla sektorów takich jak **energetyka, transport, bankowość i zdrowie**,
- Nowe obowiązki **podmiotów kluczowych i ważnych**,
- Procedura zgłaszania **incydentów bezpieczeństwa komputerowego**,
- Środki **zarządzania ryzykiem** w cyberbezpieczeństwie,
- Nowe przepisy powinny być stosowane we wszystkich krajach Unii Europejskiej od **18 października 2024 r**
- **W razie ataku** musimy poinformować **CSIRT** (Computer Security Incident Response Team) – zespół reagowania na incydenty bezpieczeństwa

Cyber Resilience Act (CRA)

- Wymogi dla **producentów, importerów i dystrybutorów produktów wyposażonych elementy cyfrowe**, które mogą komunikować się z innymi produktami,
- **Ocena ryzyka i gwarancja** odpowiedniego poziomu cyberbezpieczeństwa przez producentów w całym cyklu życia produktu,
- **Zarządzanie lukami** w zabezpieczeniach i wydawanie aktualizacji
- **Obowiązek zgłaszania** wykrytych luk do **CSIRT**
- Rozporządzenie CRA stosuje się od dnia **11 grudnia 2027 r.**

Struktura IEC 62443

General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life cycle and use-cases		
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners	 Właściciel
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels			 System integrator
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components				 Producent

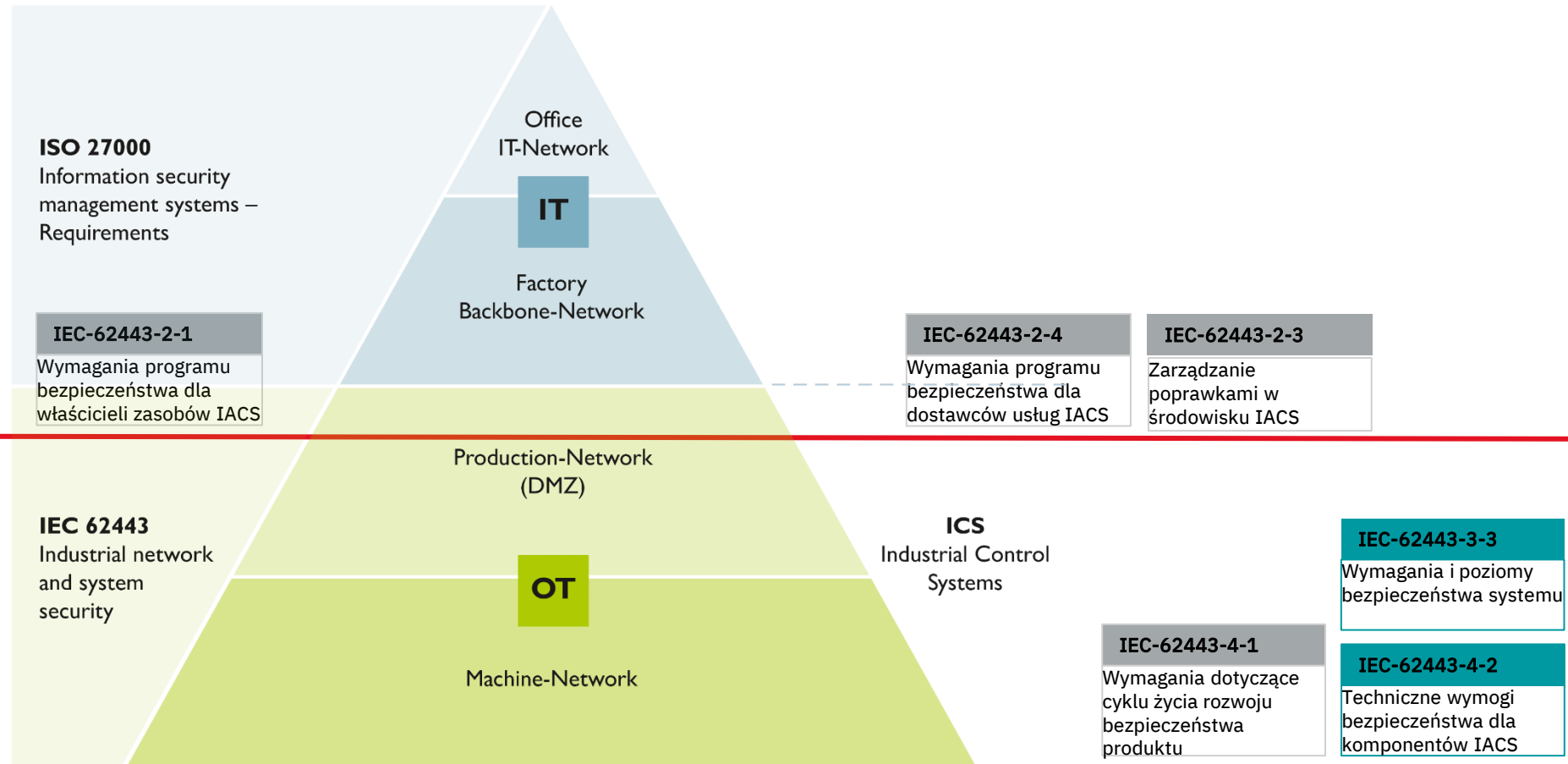
Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych

NIS 2, CRA i Regulacja maszynowa

Dyrektywa NIS 2
Network & Information
Security

Regulacja maszynowa

Cyber Resilience Act
(CRA)



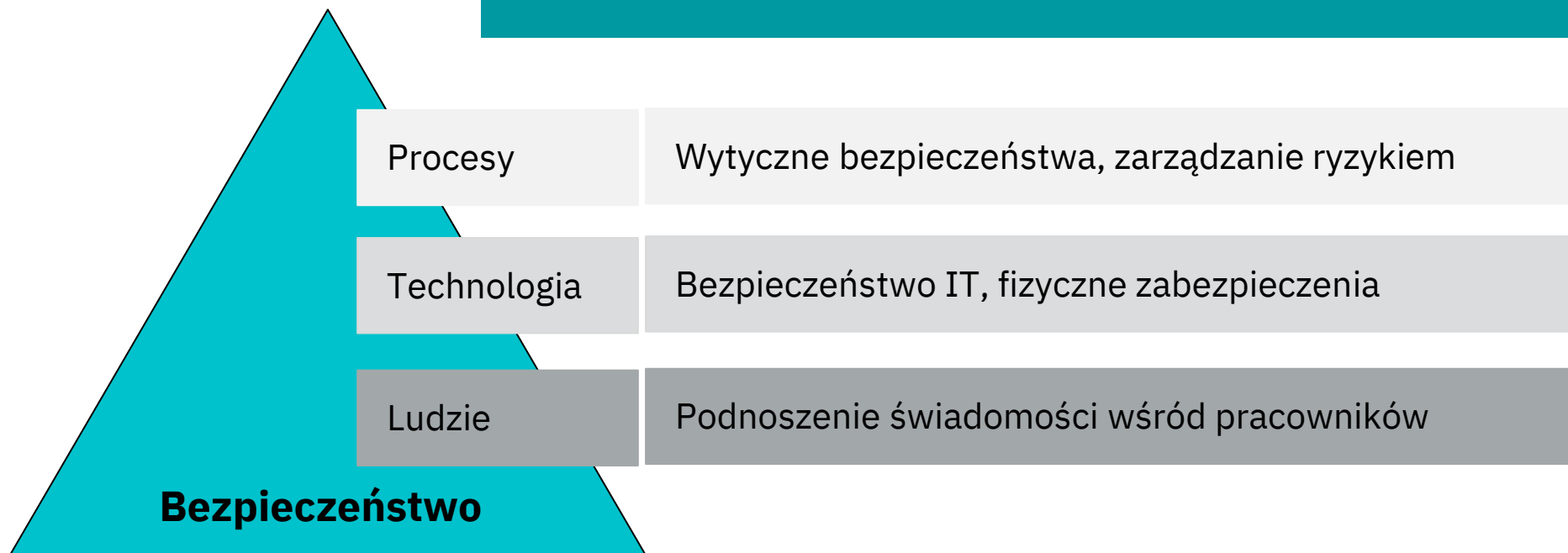
Koncepcje bezpieczeństwa i środki zaradcze

Bezpieczeństwo sieci OT vs IT

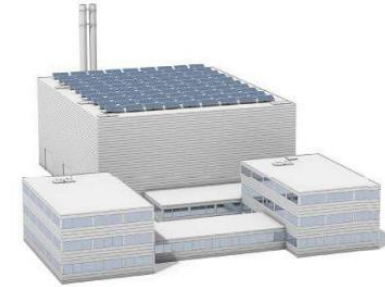
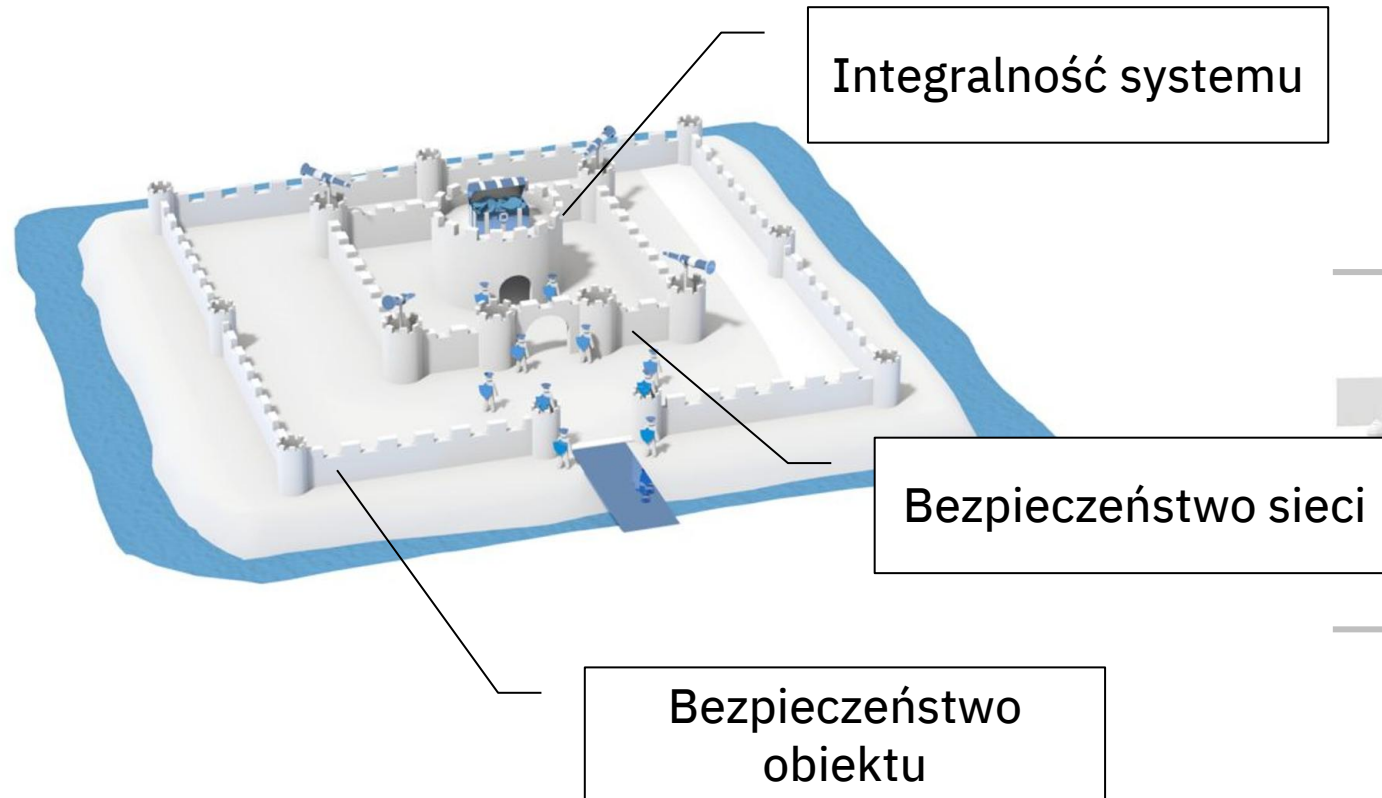


Koncepcja bezpieczeństwa

Odpowiednia koncepcja bezpieczeństwa musi obejmować **wykorzystywaną technologię, zdefiniowane procesy i zaangażowanych ludzi**, tj. musi określać zarówno środki technologiczne, jak i organizacyjne.



Koncepcja Defense-in-Depth



Poziom korporacyjny:

- Bezpieczeństwo fizyczne
- Koncepcja autoryzacji (wstęp, dostęp)
- Szkolenia
- Procesy ISMS



Poziom sieci:

- Segmentacja sieci
- Zapory sieciowe
- Szyfrowanie
- VPN
- Detekcja ataku



Poziom produktu

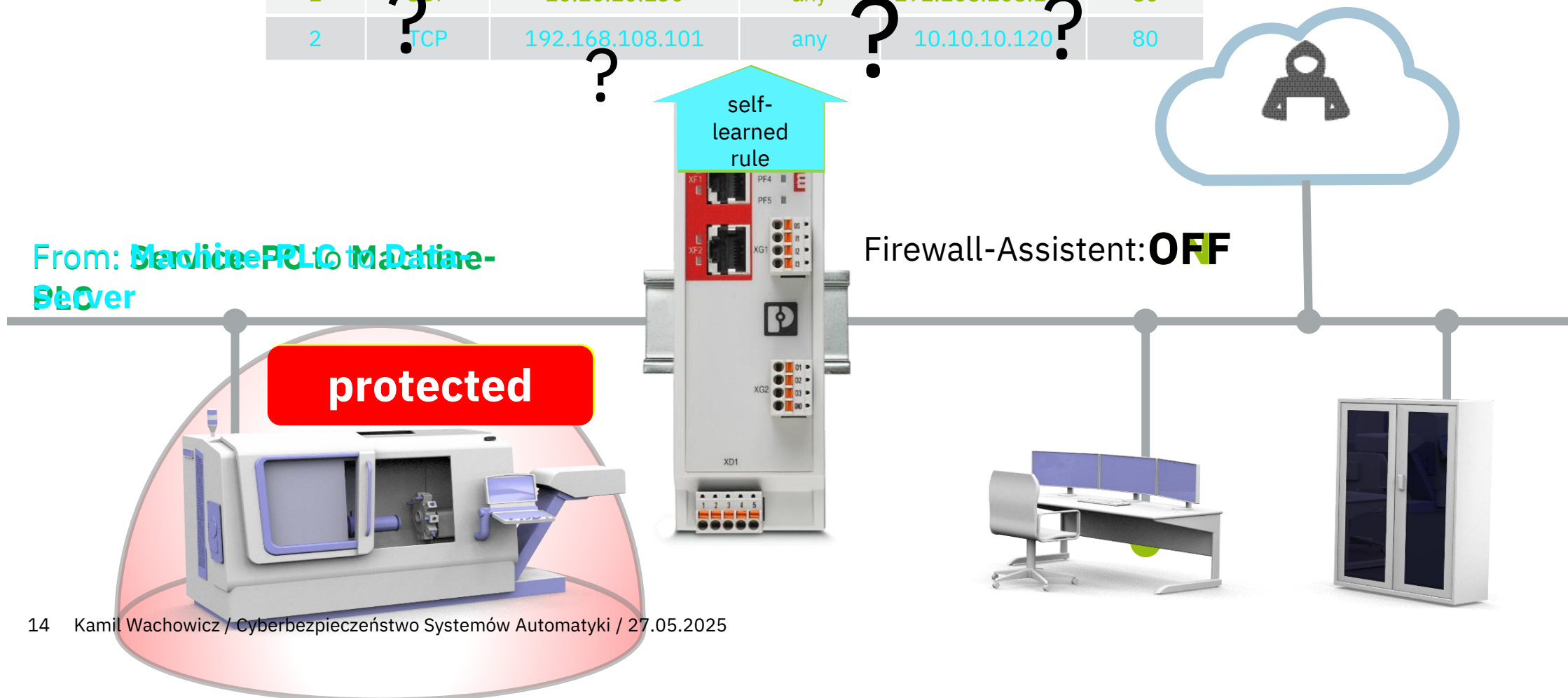
- Zabezpieczenia
- „Security-by-design”
- System hardening

Rozwiązania zapewniające bezpieczeństwo sieci i procesów

Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych

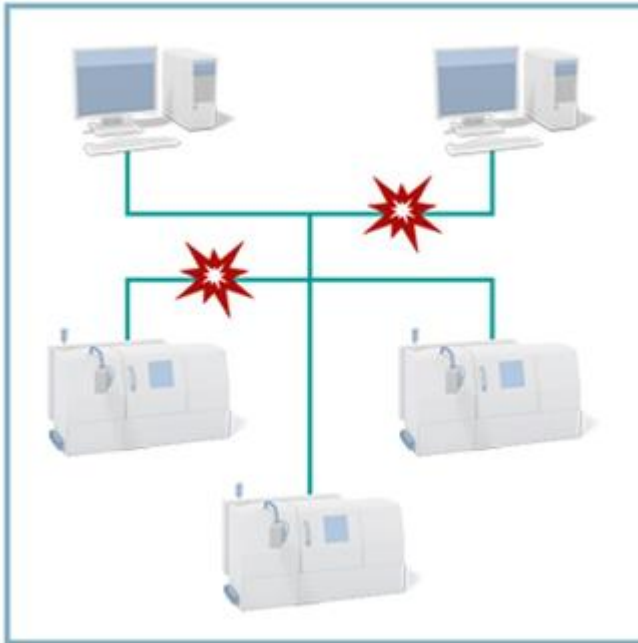
Wykorzystanie zapór sieciowych

Seq.	Protocol	From IP	From port	To IP	To port
1	UDP	10.10.10.130	any	192.168.108.101	80
2	TCP	192.168.108.101	any	10.10.10.120	80

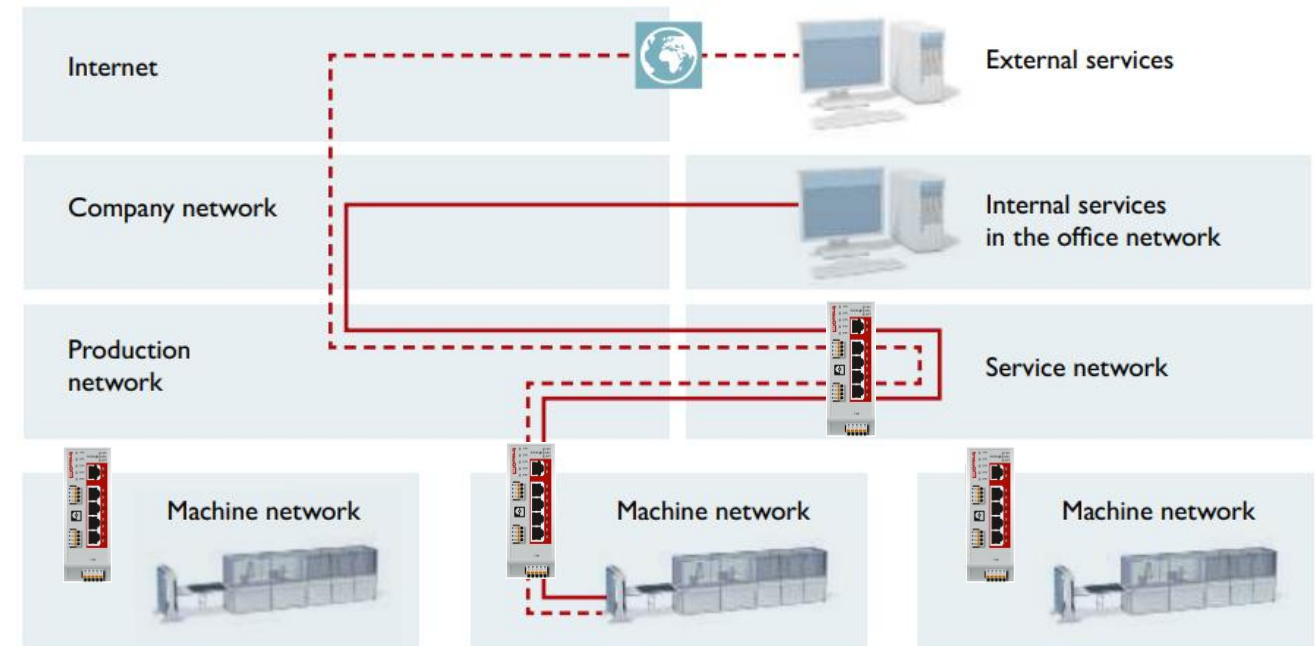


Segmentacja sieci

Zagrożenie: atak od strony sieci biurowej

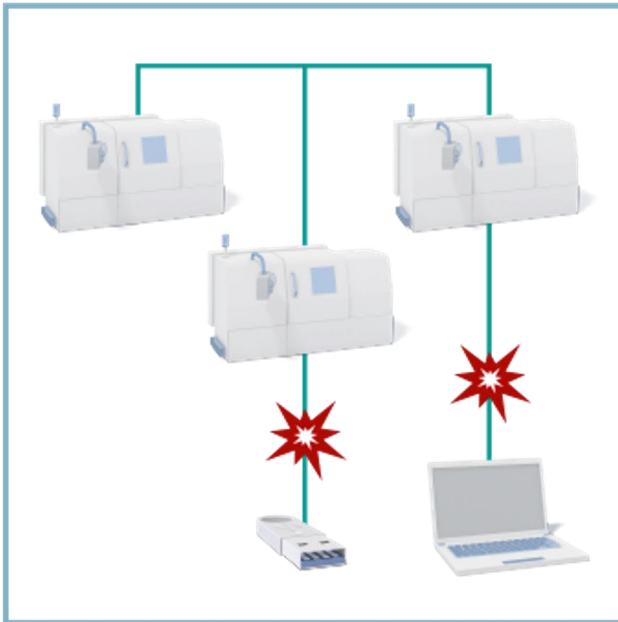


Rozwiązanie: segmentacja sieci

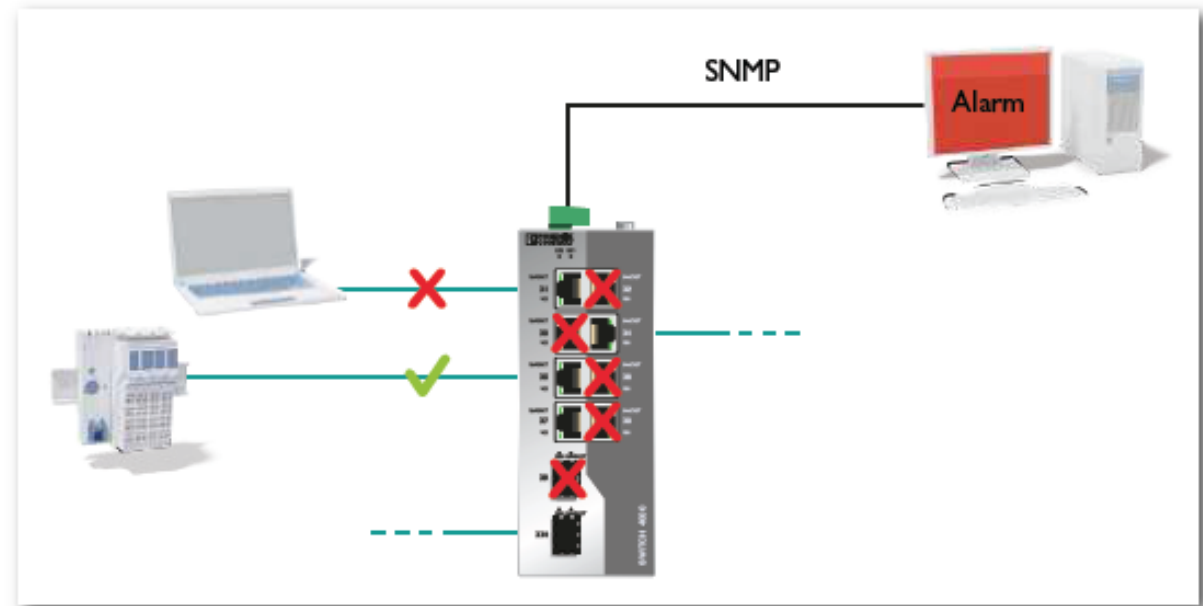


Zabezpieczenie portów oraz alerty o nieautoryzowanym dostępie

Zagrożenie: zainfekowany sprzęt



Rozwiązanie: zabezpieczenie portów

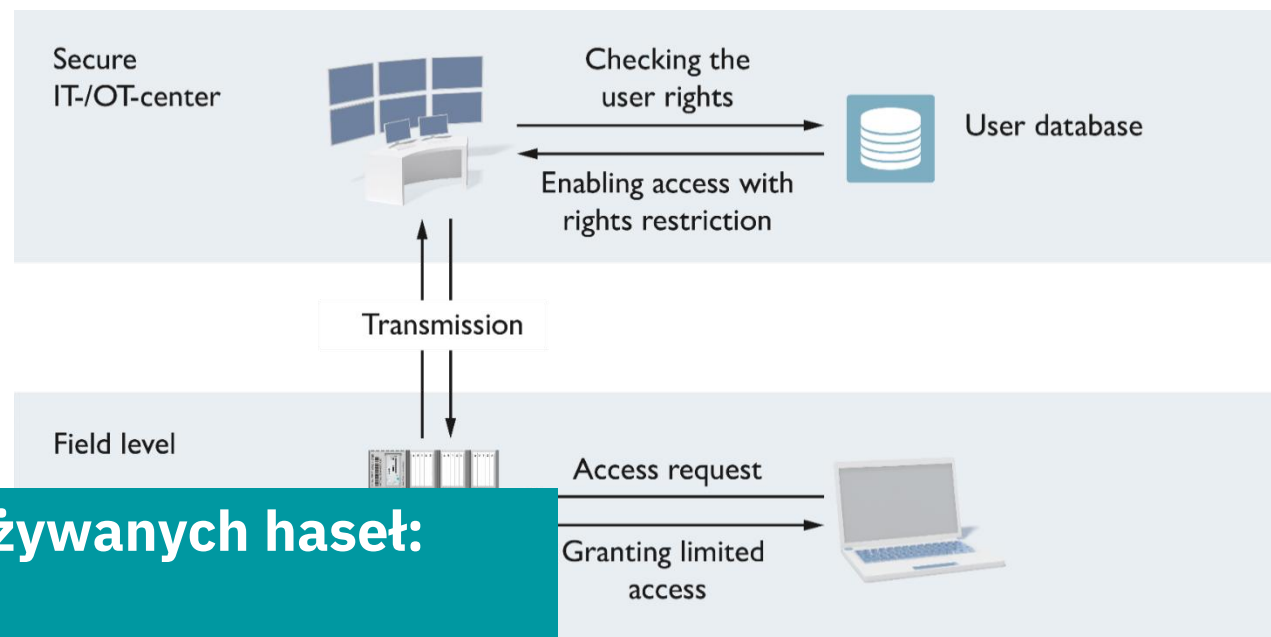


Zasady dotyczące użytkowników i haseł

Zagrożenie: niewłaściwe zarządzanie użytkownikami



Rozwiązanie: centralne zarządzanie użytkownika

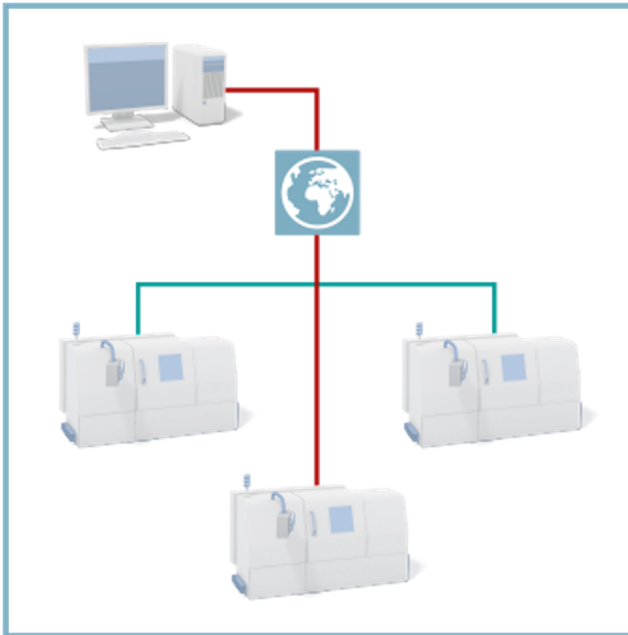


Top 5 najczęściej używanych haseł:

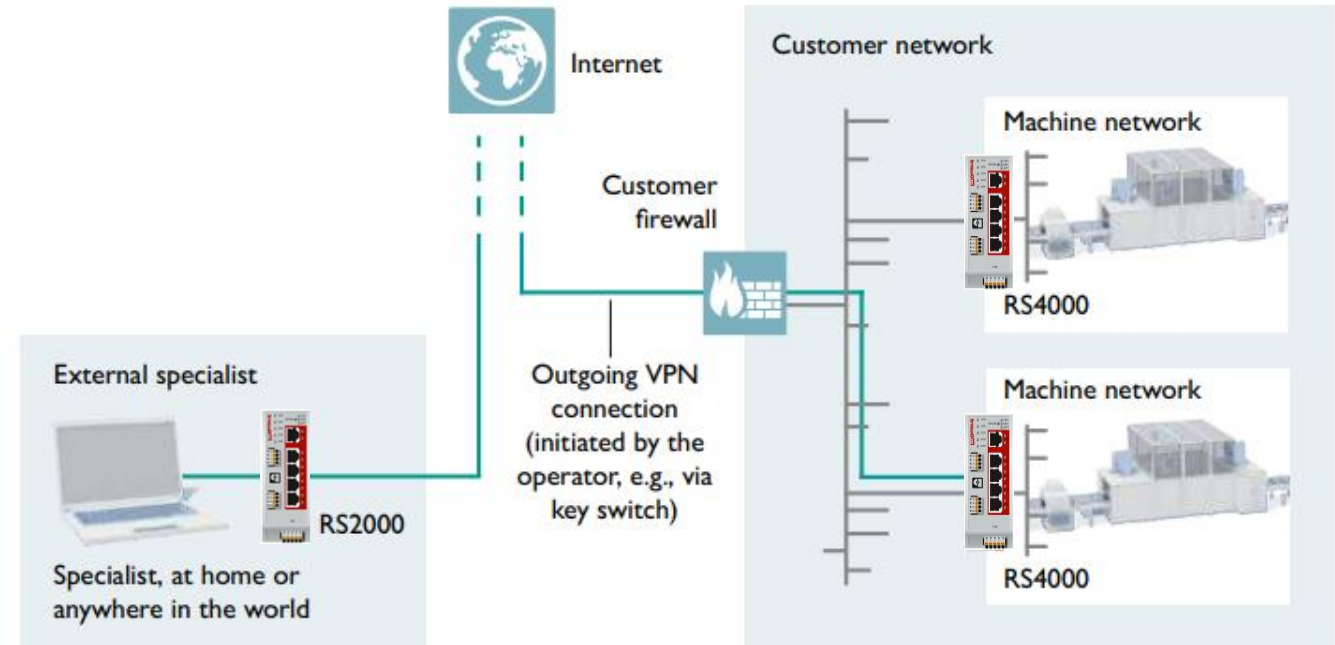
1. 123456
2. 123456789
3. 12345678
4. password
5. qwerty123

Bezpieczny zdalny dostęp

Zagrożenie: atak na niezabezpieczone połączenie

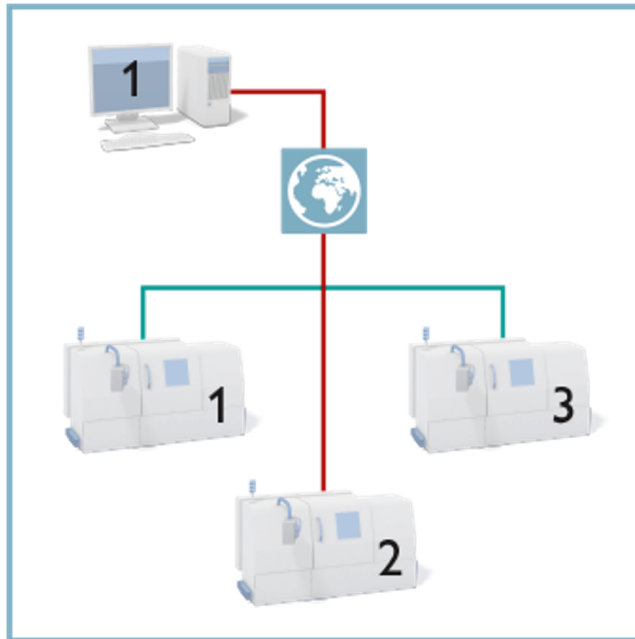


Rozwiązanie: szyfrowana komunikacja

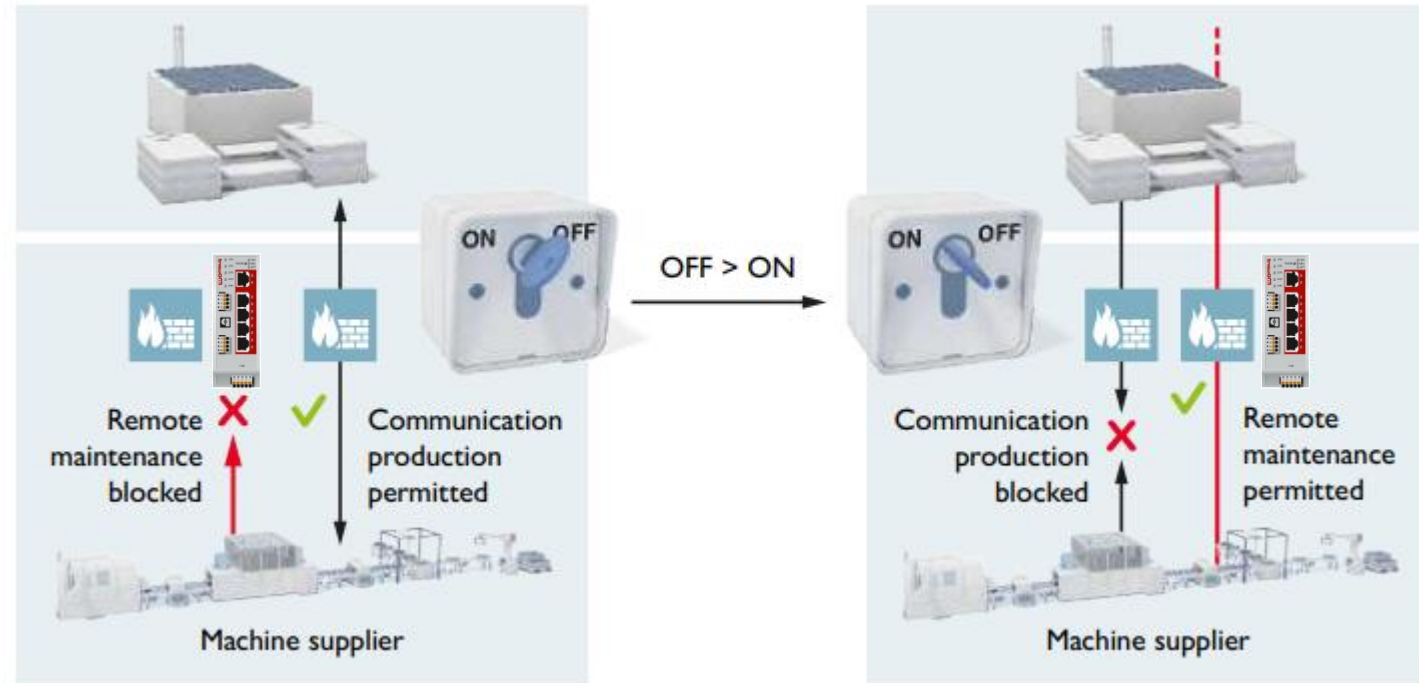


Bezpieczny zdalny dostęp

Zagrożenie: nieautoryzowany dostęp do systemu

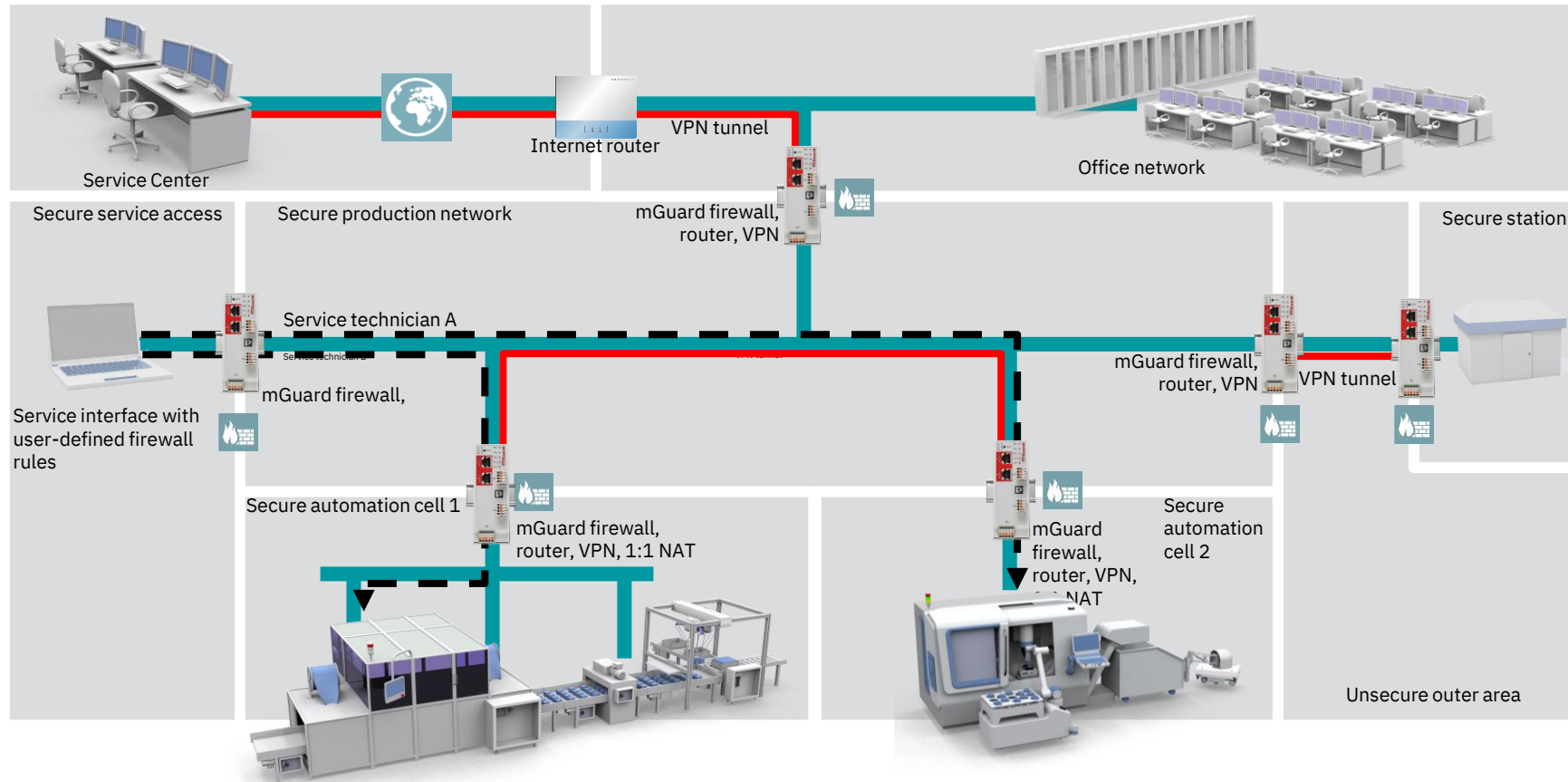


Rozwiązanie: bezpieczny zdalny dostęp



Cyberbezpieczeństwo systemów automatyki w zakładach produkcyjnych

Bezpieczny zdalny dostęp – prawa użytkownika

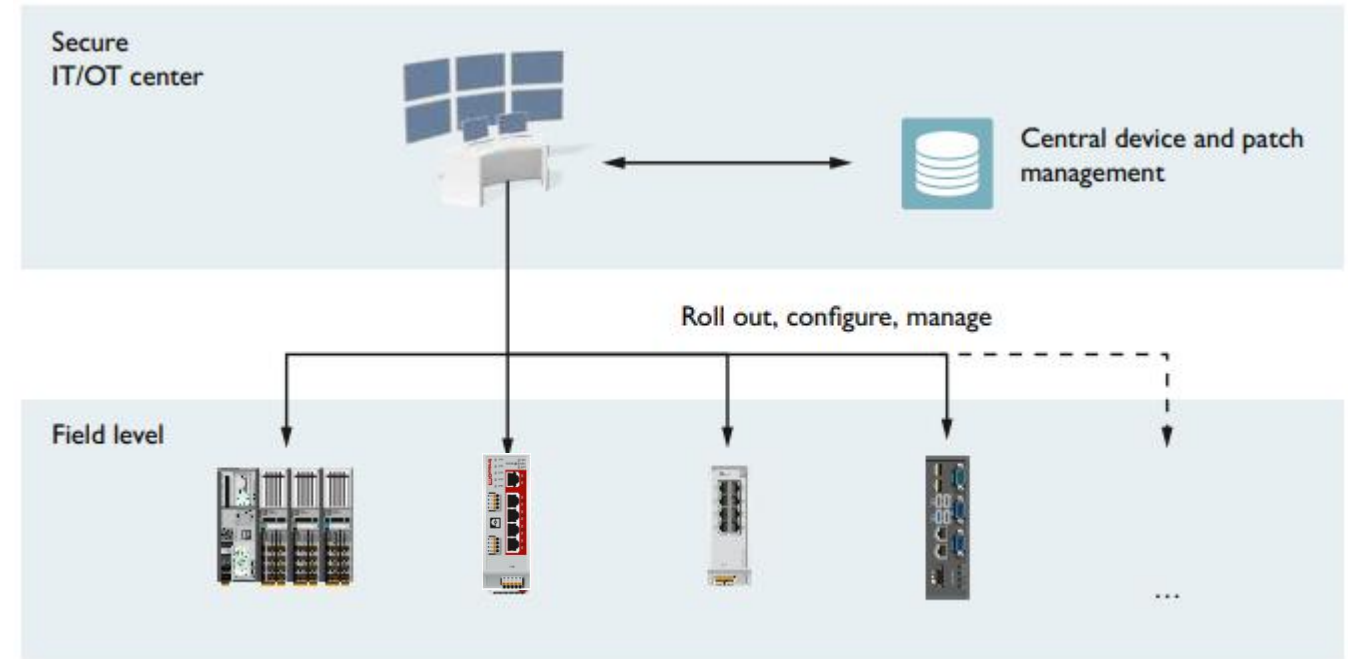


Centralne zarządzanie urządzeniami

Zagrożenie: niezabezpieczona lub nieaktualna konfiguracja urządzenia



Rozwiązanie: zarządzanie urządzeniami i poprawkami



Regularny backup -> reguła 3-2-1

IEC 62443 w Phoenix Contact

Certyfikowana zgodność z IEC 62443

- mGuard są certyfikowane:
 - Zgodność procesu rozwoju produktu z normą **IEC 62443-4-1**
 - Zgodność urządzeń z **IEC 62443-4-2**, spełnienie wymagań **Security Level Capability 2 (SL-C 2)**
- Certyfikat dotyczy modeli:
 - FL MGuard 2102
 - FL MGuard 2105
 - FL MGuard 4302
 - FL MGuard 4305
 - FL MGuard 4102 PCI
 - FL MGuard 4102 PCIE

Certificate



Nr./No.: 968/CSP 1029.00/25

Prüfgegenstand Product tested	Industrial Security Router	Zertifikatsinhaber Certificate holder	Phoenix Contact GmbH & Co. KG Flachsmarktstr. 8 32825 Blomberg Germany
Typbezeichnung Type designation	FL MGuard		
Prüfgrundlagen Codes and standards	IEC 62443-4-1:2018 (Edition 1.0)	IEC 62443-4-2:2019 (Edition 1.0)	
Bestimmungsgemäße Verwendung Intended application	The Industrial Security Router FL MGuard complies with the requirements according to IEC 62443-4-1 and Security Level Capability 2 (SL-C 2) according to IEC 62443-4-2.		
Besondere Bedingungen Specific requirements	The Industrial Security Router FL MGuard is only valid in the dedicated security context as documented in the user manuals. The instructions of the associated user manuals released by manufacturer must be considered. The current versions of the product are specified in the currently valid Revision List. The Revision List is released by the manufacturer in cooperation with the certification body.		
Gültig bis / Valid until 2030-03-06			
Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/CSP 1029.00/25 vom 06.03.2025 dokumentiert sind. Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/CSP 1029.00/25 dated 2025-03-06. This certificate is valid only for products which are identical with the product tested. TÜV Rheinland Industrie Service GmbH Bereich Automation Funktionale Sicherheit Am Grauen Stein, 51105 Köln Köln, 2025-03-06 Certification Body Safety & Security for Automation & Grid Dipl.-Ing. (FH) Sergei Biberdorf			

www.fs-products.com
www.tuv.com



Podsumowanie produktowe IEC 62443

Grupa produktów		Zgodność z IEC 62443-4-2	Certyfikacja z IEC 62443-4-2
	Routery mGUARD	TAK	TAK
	Switche zarządzalne	TAK	W toku
	Switche Raptor	W toku	W toku
	Modemy GSM CELLULINK	TAK	TAK
	Sterowniki PLCnext Control	TAK	TAK



Dziękuję za uwagę

**„Cyberbezpieczeństwo
systemów automatyki w
zakładach produkcyjnych”**