PHOENIX CONTACT

100 lat pasji do technologii i innowacyjności

enervigo™

VERSABOX™ AUTONOMOUS MOBILE ROBOTS

POLITECHNIKA GDAŃSKA

INTEX

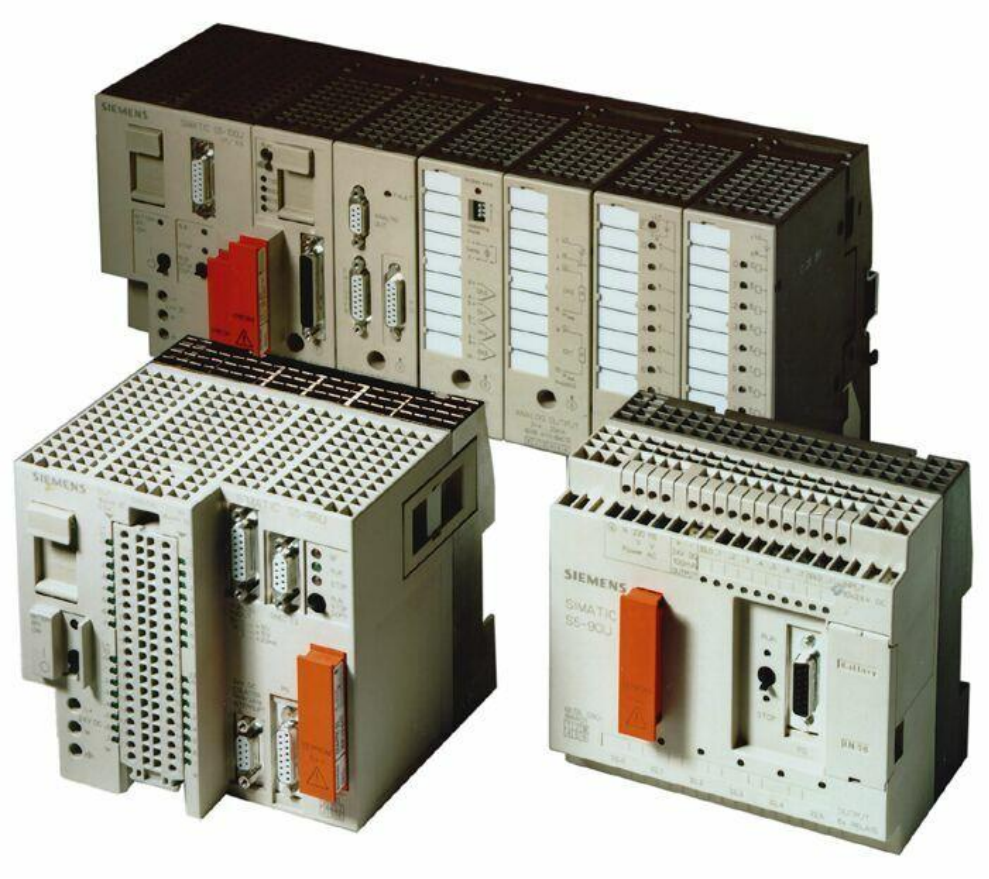
X edycja Technology Days

Cyberbezpieczeństwo systemów automatyki: podatności, konsekwencje oraz sposoby poprawy

Agenda

- Rozwój systemów automatyki
- Przykłady incydentów w zakresie OT oraz ich konsekwencje
- Standardy ISA/IEC 62443
- Cykl życia systemu bezpieczeństwa zgodnie z ISA/IEC 62443

Systemy automatyki w przeszłości

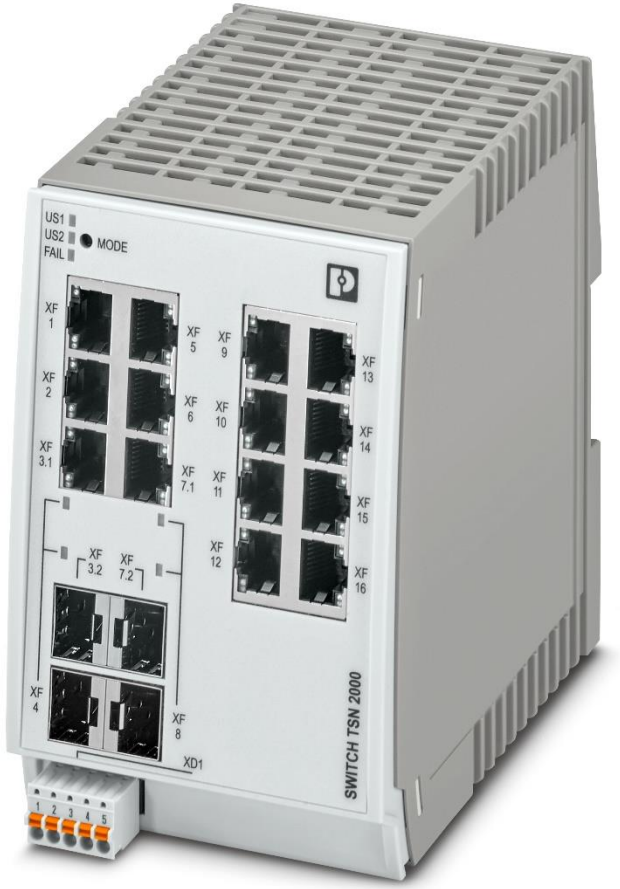


- Dedykowany sprzęt
- Dedykowany system operacyjny
- Bardzo ograniczone możliwości komunikacyjne
- Separacja od otoczenia

Systemy automatyki dziś

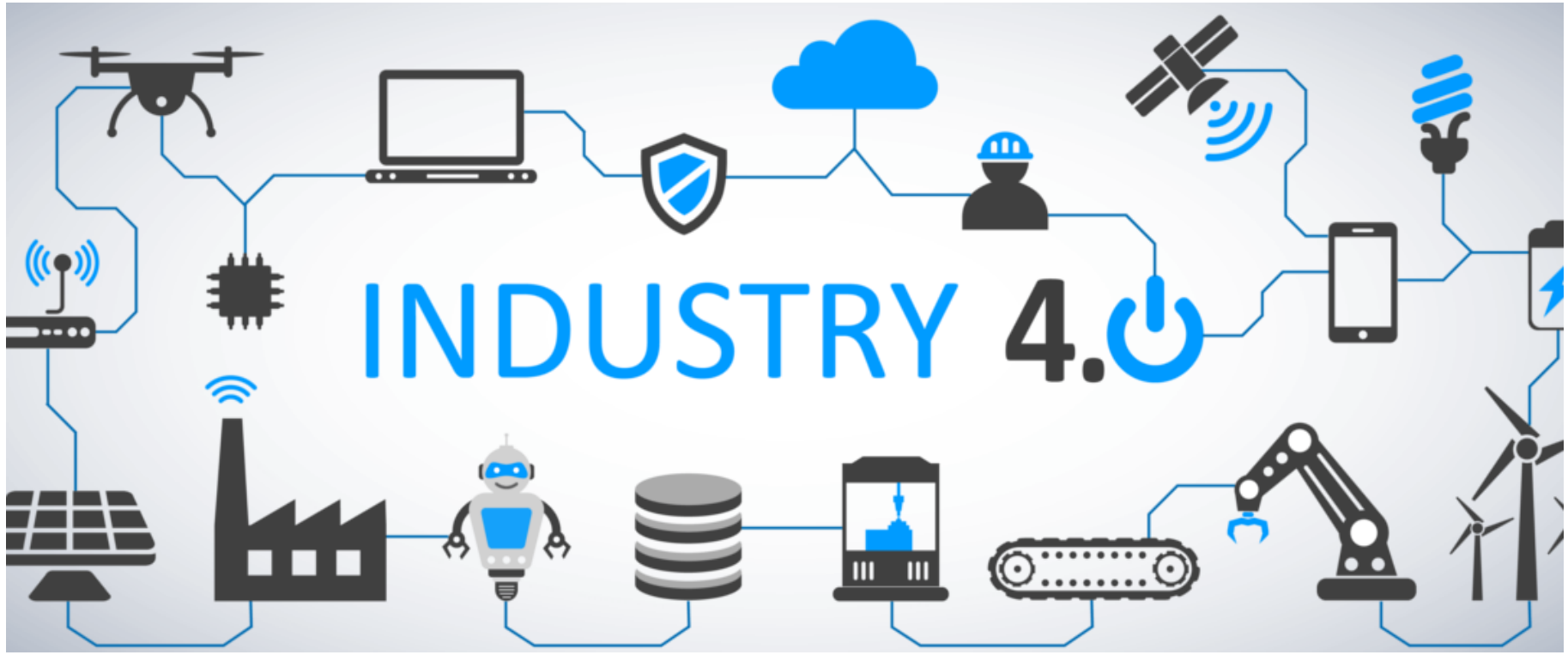
- Duży stopień wykorzystania ogólnodostępnych komponentów sprzętowych i programowych
- Powszechne stosowane systemy operacyjne
- Bardzo duże możliwości komunikacyjne
- Duży stopień integracji z otoczeniem

Infrastruktura sieciowa – Ethernet



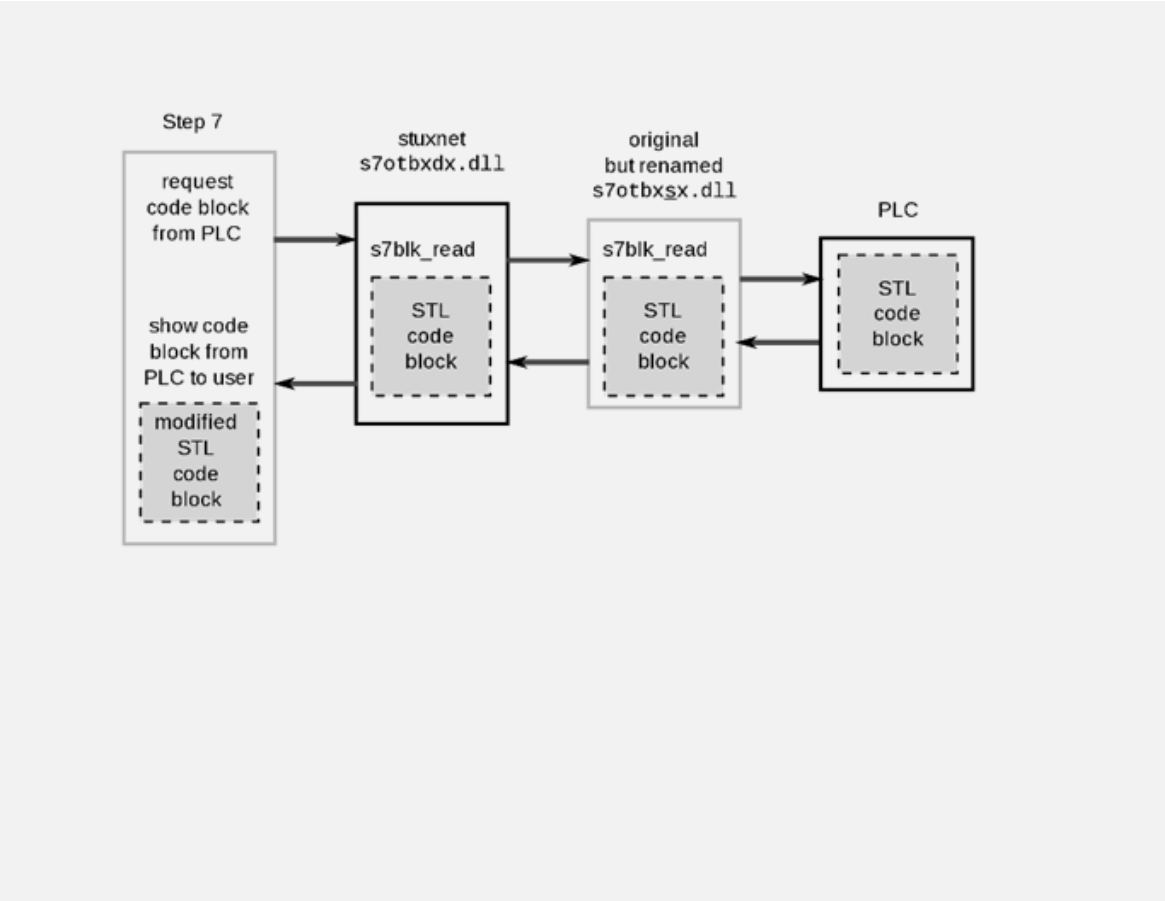
- Powszechnie znany i wykorzystywany standard
- System prosty w rozbudowie
- Zasada działania niezależna od aplikacji (IT <> OT)
- Często ignorowane różnice w specyficznych wymaganiach dla systemów OT

Motywacja i trendy rozwoju systemów automatyki



Rysunek: https://squarespheretechnology.com/wp-content/uploads/2018/10/industry-4.0-1080x450.png

Przykłady incydentów jakie dotknęły systemy OT – Stuxnet 2010



- Pierwsze wystąpienie: wzbogacanie uranu, Iran
- Docelowy system: SIEMENS SIMATIC S7, WinCC
- Działanie: modyfikacja kodu dla PLC
- Efekt: uszkodzenia mechaniczne urządzeń

rysunek: https://en.wikipedia.org/wiki/Stuxnet

Przykłady incydentów jakie dotknęły systemy OT – Industroyer 2016

rysunek: https://www.tuv.com/world/en/power-grid-modelling-and-simulation.html

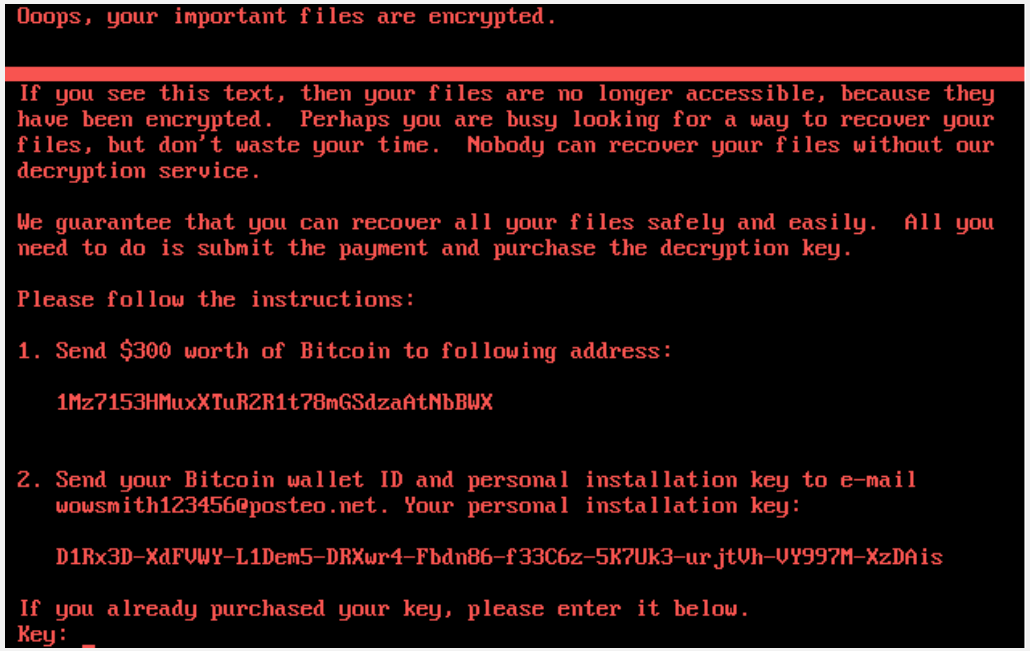
- Pierwsze wystąpienie: dystrybucja energii, Ukraina
- Docelowy system: zabezpieczenia sieci dystrybucyjnej
- Działanie: zdalny dostęp do systemu i jego manipulacja
- Efekt: brak zasilania na dużym obszarze przez 1 godzinę

Przykłady incydentów jakie dotknęły systemy OT – Triton/Trisis 2017

- Pierwsze wystąpienie: zakłady petrochemiczne, Arabia Saudyjska
- Docelowy system: Triconex, Schneider Electric
- Działanie: penetracja systemu sterowania/systemu bezpieczeństwa
- Efekt: awaryjne zatrzymanie instalacji

rysunek: https://marketbulletin.com.pk/index.php/2017/09/09/fears-over-texas-chemical-plant-as-houston-flood-eases/

Przykłady incydentów jakie dotknęły systemy OT – NotPetya 2017



- Docelowy system: systemy komputerowe
- Działanie: szyfrowanie komputerów
- Efekt: straty materialne, wizerunkowe, znaczące zakłócenie dyspozycyjności

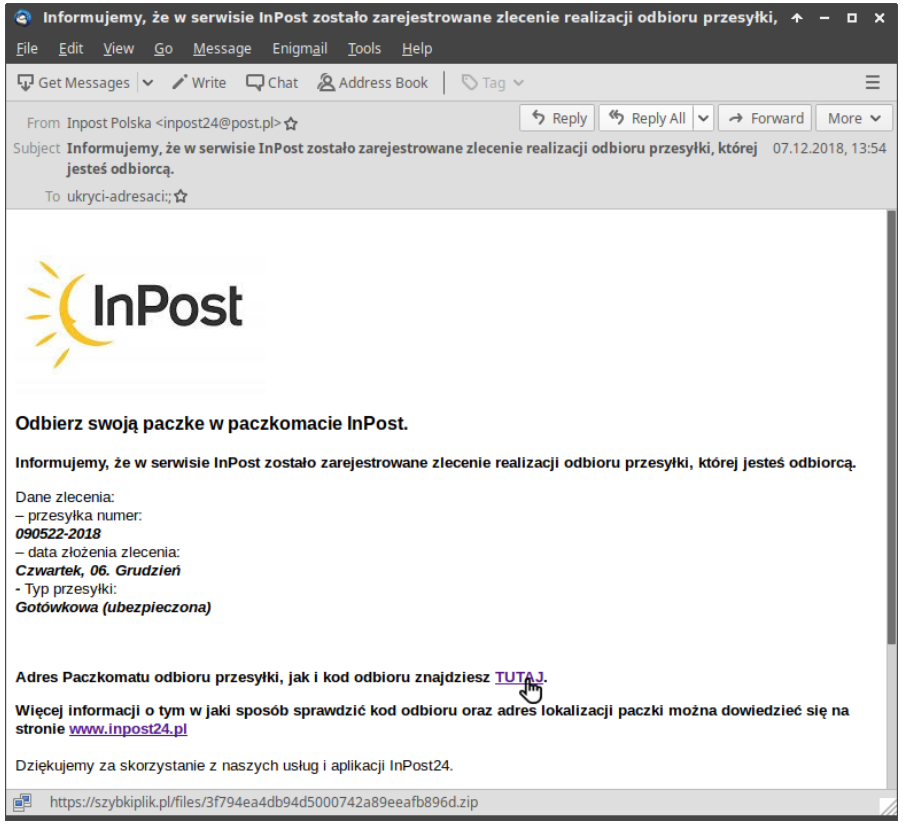
rysunek: https://www.microsoft.com/security/blog/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/?source=mmpc

Przykłady incydentów jakie dotknęły systemy OT – Oldsmar 2021

- Docelowy system: stacja uzdatniania wody/TeamViewer
- Działanie: zwiększenie dozowania NaOH z 100ppm do 11 100ppm
- Efekt: atak został przerwany przez operatora

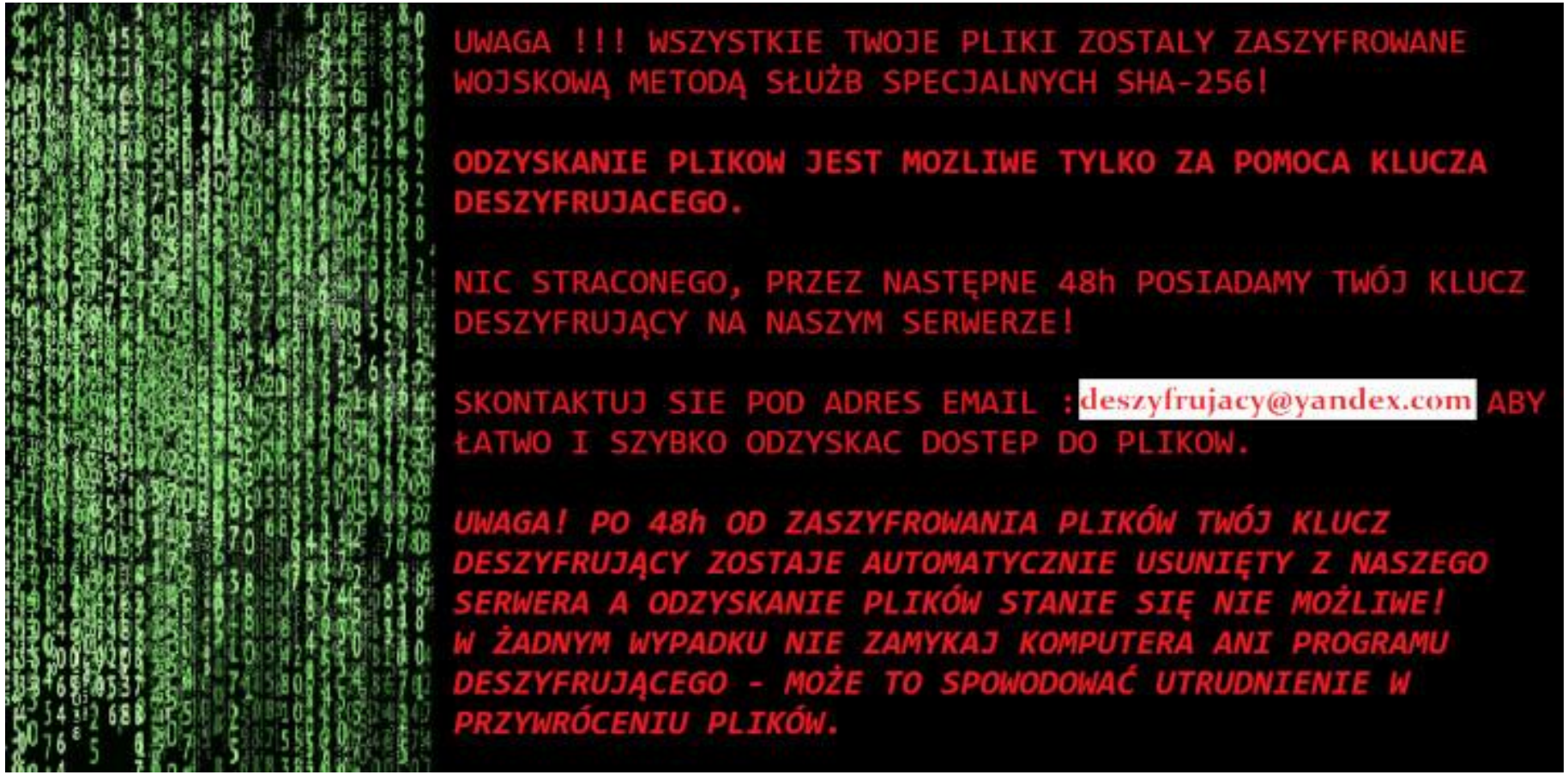
rysunek: https://wusfnews.wusf.usf.edu/politics-issues/2021-03-10/security-at-hacked-oldsmar-water-plant-was-extremely-lax-top-florida-law-official-says

Ostrożności nigdy za wiele …



źródło: https://www.cert.pl/news/single/trojan-oraz-ransomware-w-kampanii-podszywajacej-sie-pod-inpost//

… ponieważ jej brak może sporo kosztować!



źródło: https://www.cert.pl/news/single/trojan-oraz-ransomware-w-kampanii-podszywajacej-sie-pod-inpost//

… a wiadomości ze świata to potwierdzają!

CyberDefence 24 ARMIA I SŁUŻBY POLITYKA I PRAWO CYBERBEZPIECZEŃSTWO STREFA SAMSUNG BIZNES I FINANSE SOCIAL MEDIA ZALOGUJ SIĘ

Atak hakerski na polskiego producenta pociągów

SZYMON PALCZEWSKI
06.04.2023 11:48

DRUKUJ PDF

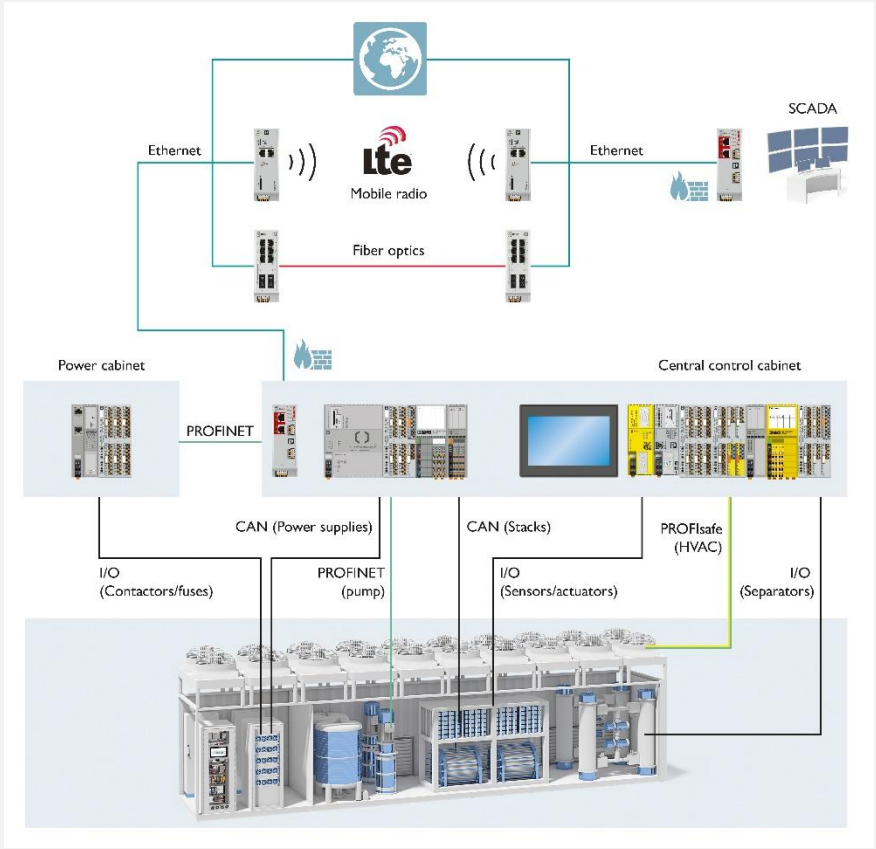
Fot. Adam Kilian/Wikimedia Commons/CC2.0

Do incydentu doszło w spółce PESA Bydgoszcz, która zajmuje się produkcją pojazdów szynowych. Władze potwierdziły wystąpienie problemów. Co z bezpieczeństwem pociągów?

2 kwietnia 2023 r. w spółce PESA Bydgoszcz doszło do naruszenia bezpieczeństwa systemów informatycznych. Mówimy o liderze polskiego rynku produkcji pojazdów szynowych, którego rozwiązania i pojazdy są wykorzystywane w 11 krajach Europy i Azji.

Kolejna kampania phishingowa. Poczta Polska ostrzega

Typowe wymagania wobec systemów automatyki

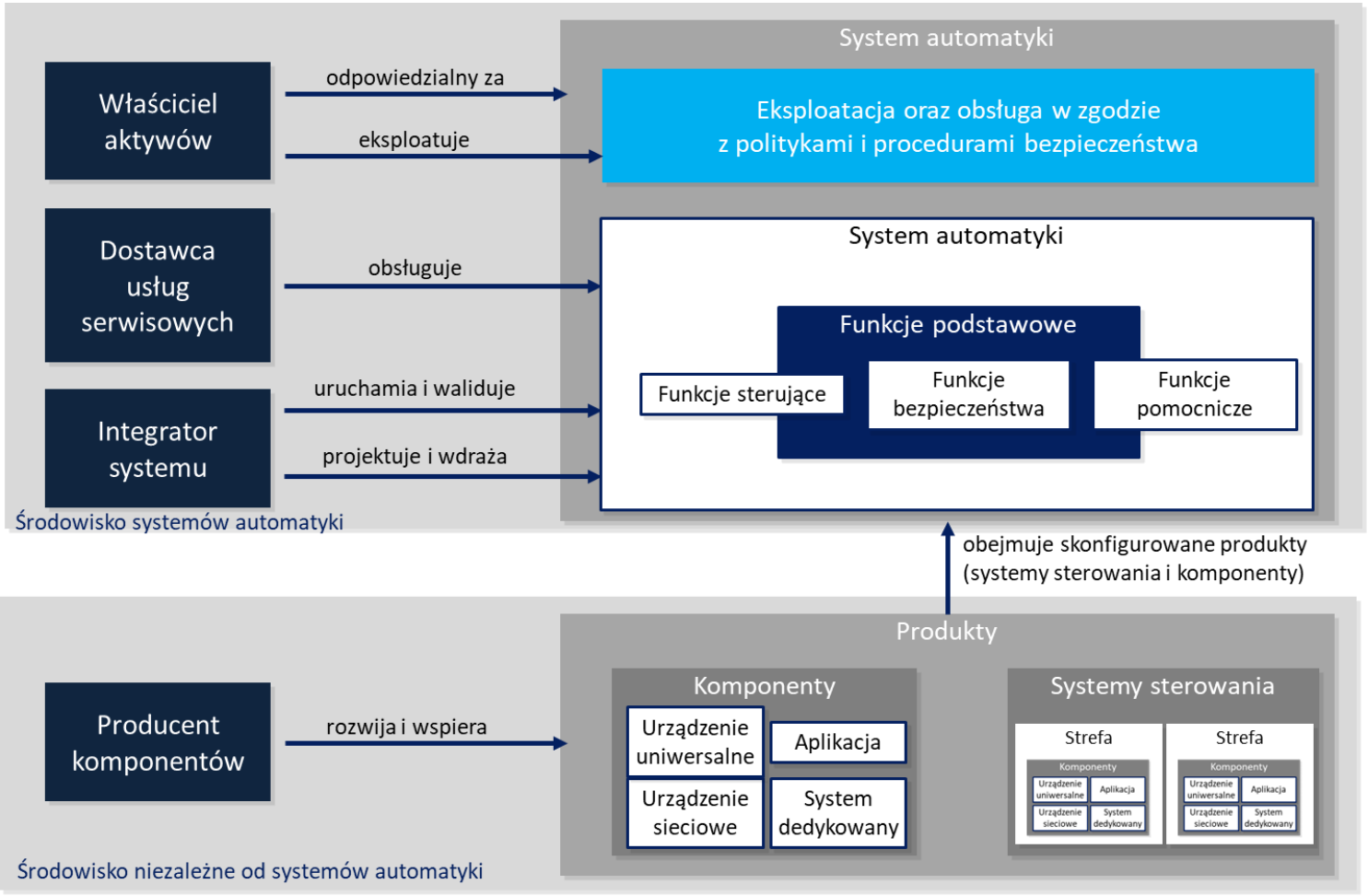


- Bezpieczeństwo oraz ciągłość działania nadzorowanego systemu
- Dyspozycyjność systemu
- Integralność systemu
- Zachowanie oczekiwanej wydajności

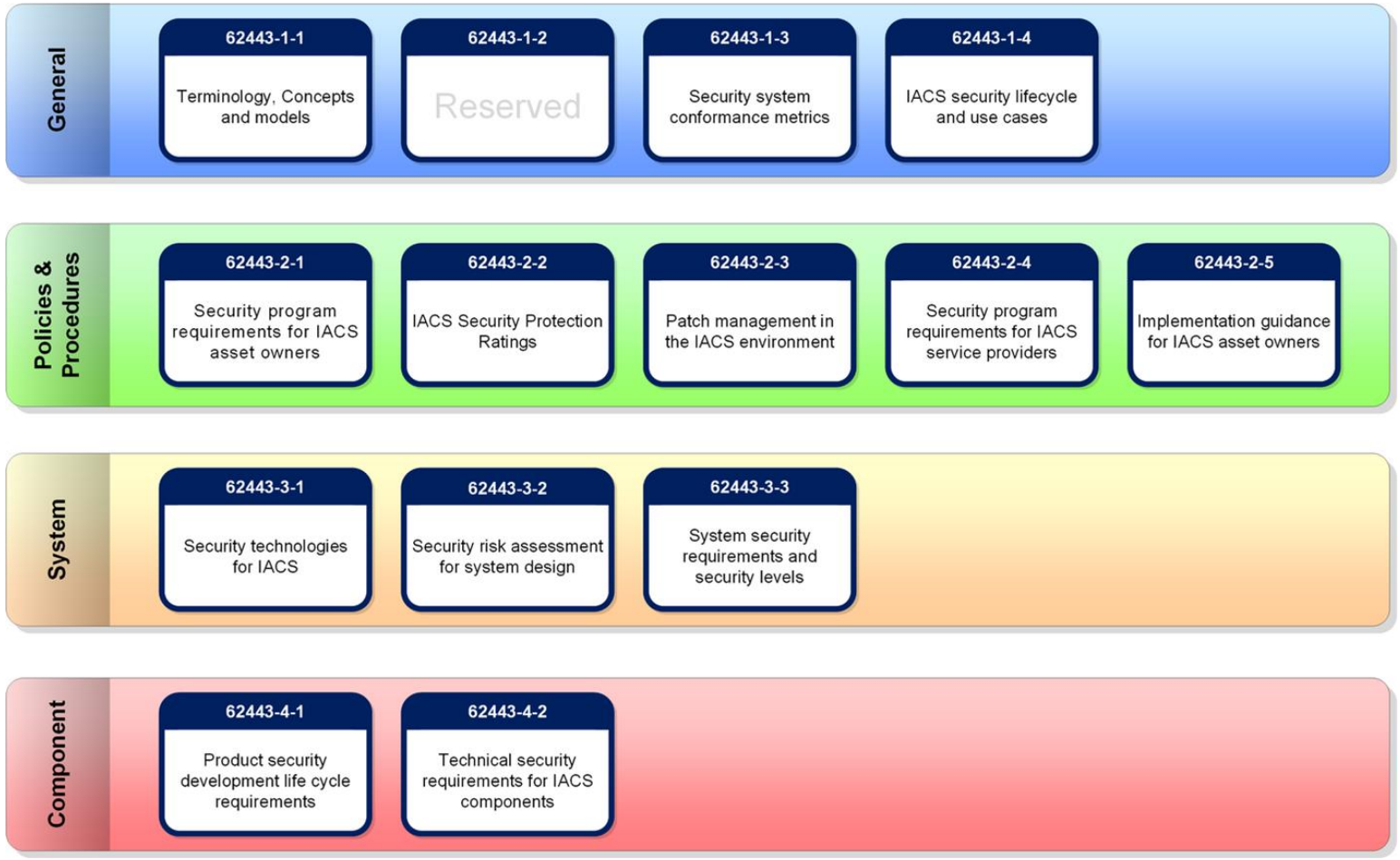
Standardy ISA/IEC 62443

ISA/IEC 62443 - Security for Industrial Automation and Control Systems

Role definiowane przez ISA/IEC 62443



Standardy ISA/IEC 62443 – dokumenty składowe



Certyfikacja producentów i produktów zgodnie z wymogami IEC 62443-4

CERTIFICATE
No. IITS1 029429 0016 Rev. 01

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Site(s): PHOENIX CONTACT Electronics GmbH Industry Management and Automation Business Unit Automation Systems
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

PHOENIX CONTACT Electronics GmbH Industry Management and Automation Business Unit Automation Infrastructure
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

Certification Mark:

Type: Secure Product Development Lifecycle

Scope of Certificate: Product creation process of the Phoenix Contact Group Master Development Guideline

Applied Standard(s): IEC 62443-4-1:2018
PPP 15002B:2021 (IEC 62443-4-1 Full ML2 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

Report No.: 18CR01S007

Valid until: 2024-09-30

Date, 2021-11-18 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

CERTIFICATE
No. IITS2 029429 0027 Rev. 00

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: IACS components

Model(s): PLCnext Control
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S047
Valid until: 2024-10-20

Date, 2021-11-19 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

CERTIFICATE
No. IITS2 029429 0027 Rev. 01

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product Type: IACS components

Model(s): PLCnext Control
(Configuration: Security Profile active)
AXC F 1152, AXC F 2152, AXC F 3152,
SPLC 1000, RFC 4072S, NFC 482S

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

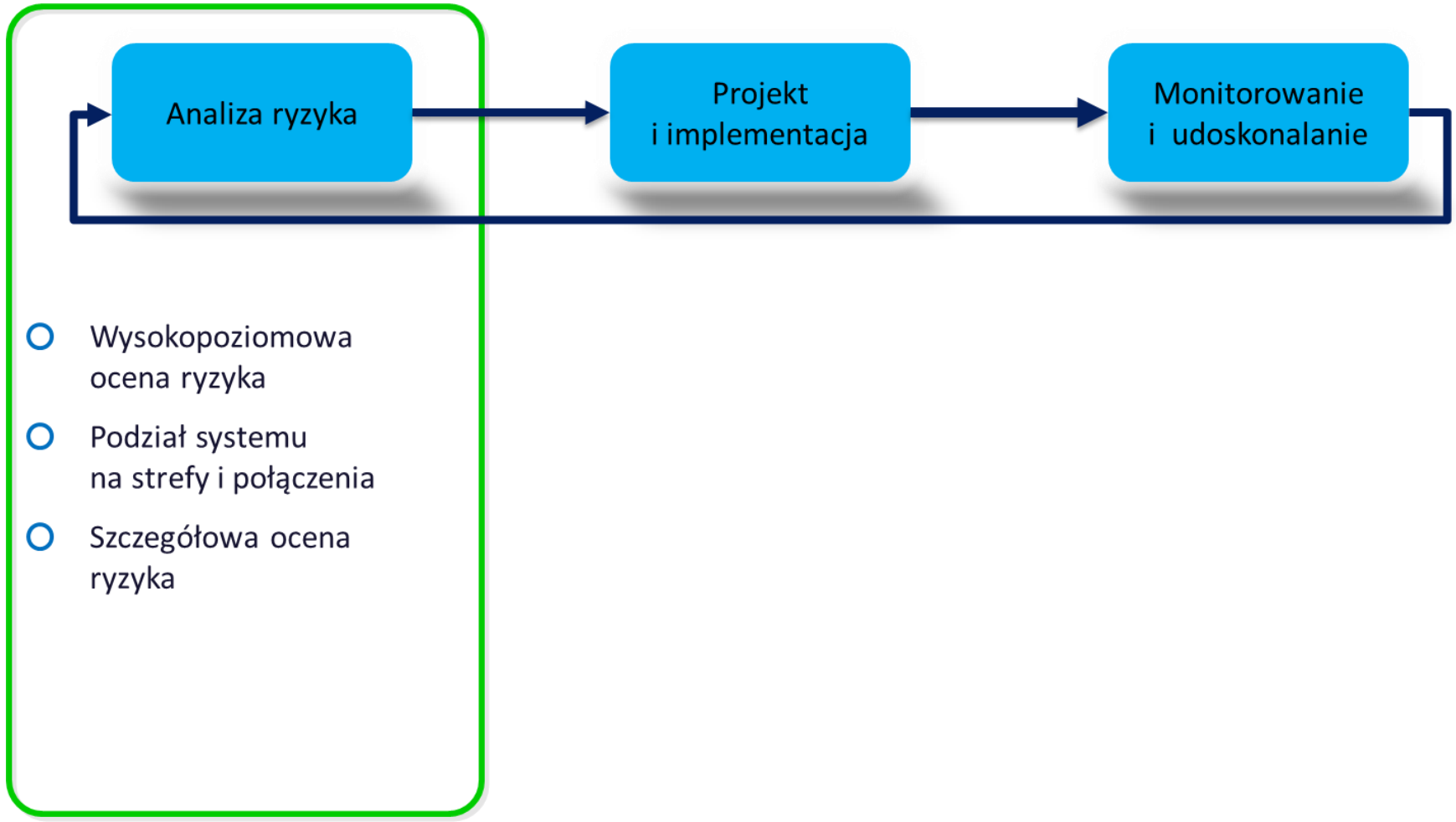
The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S047
Valid until: 2025-11-01

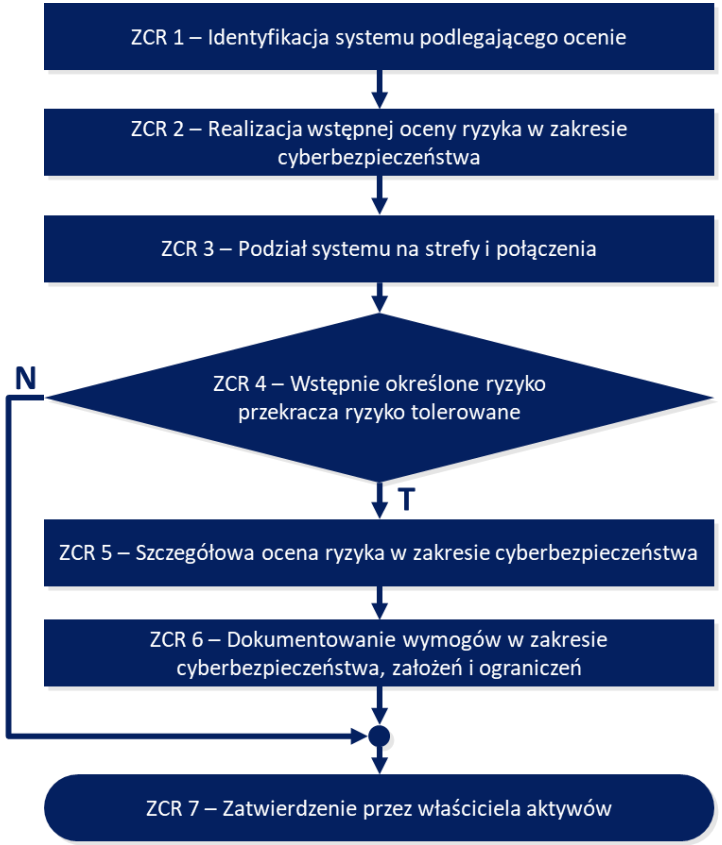
Date, 2022-11-02 (Nadia Patricia Stefan)

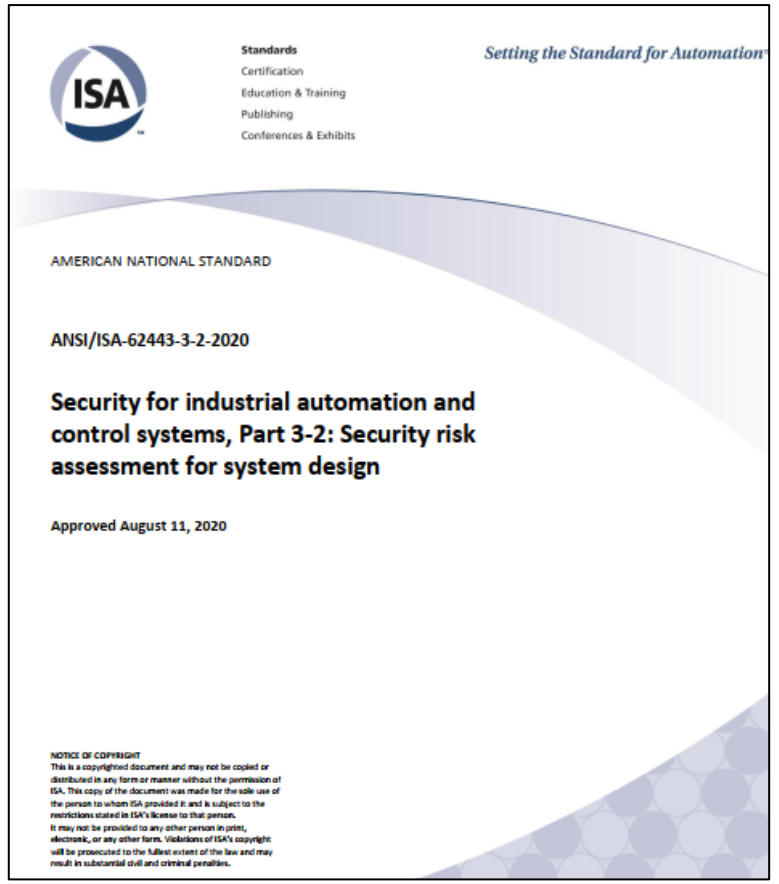
Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443

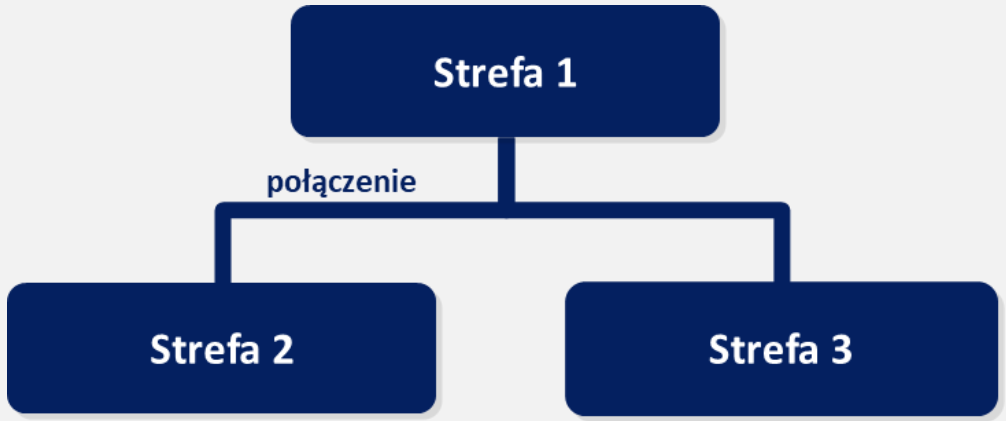


Analiza ryzyka wg. ISA/IEC 62443



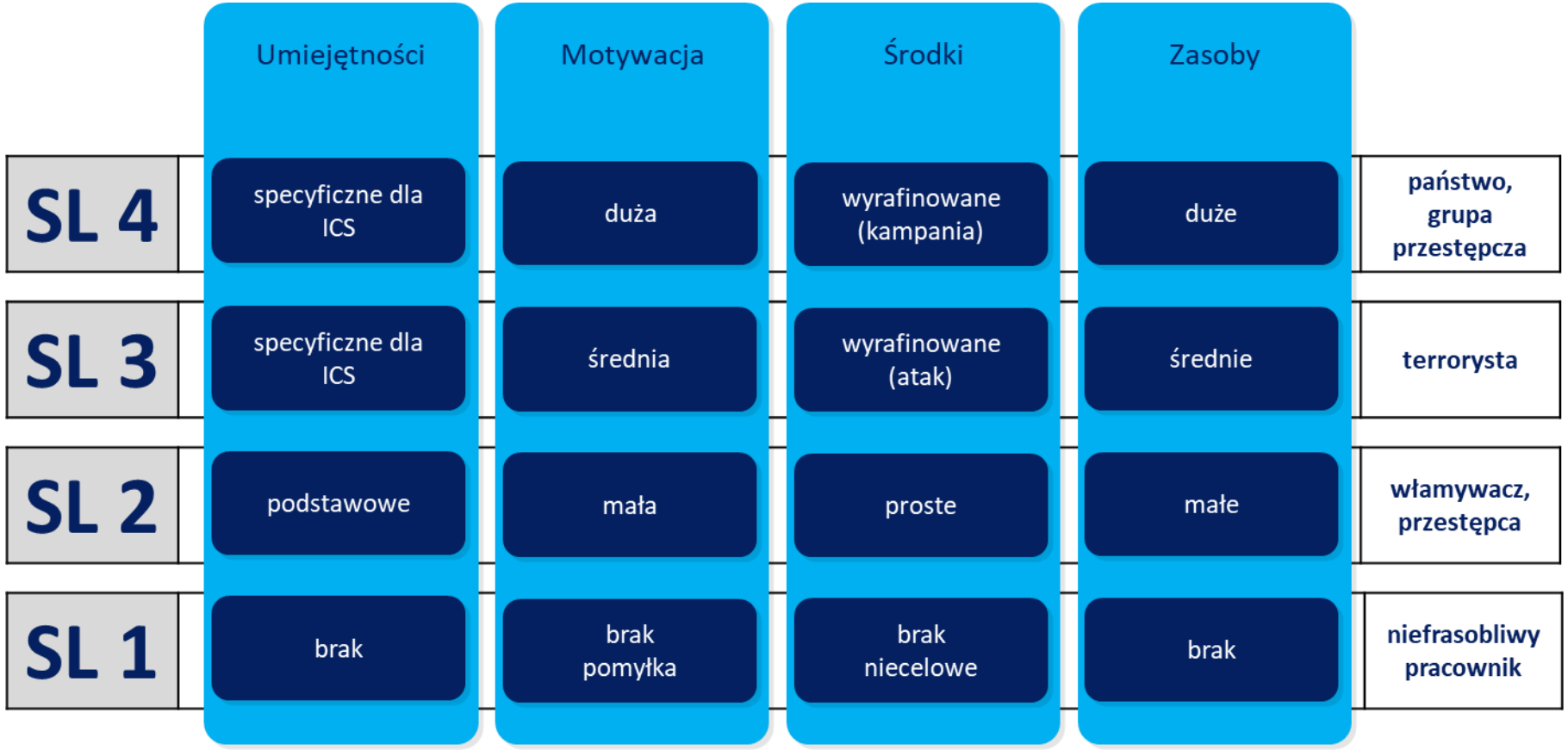


Strefy i kanały komunikacyjne



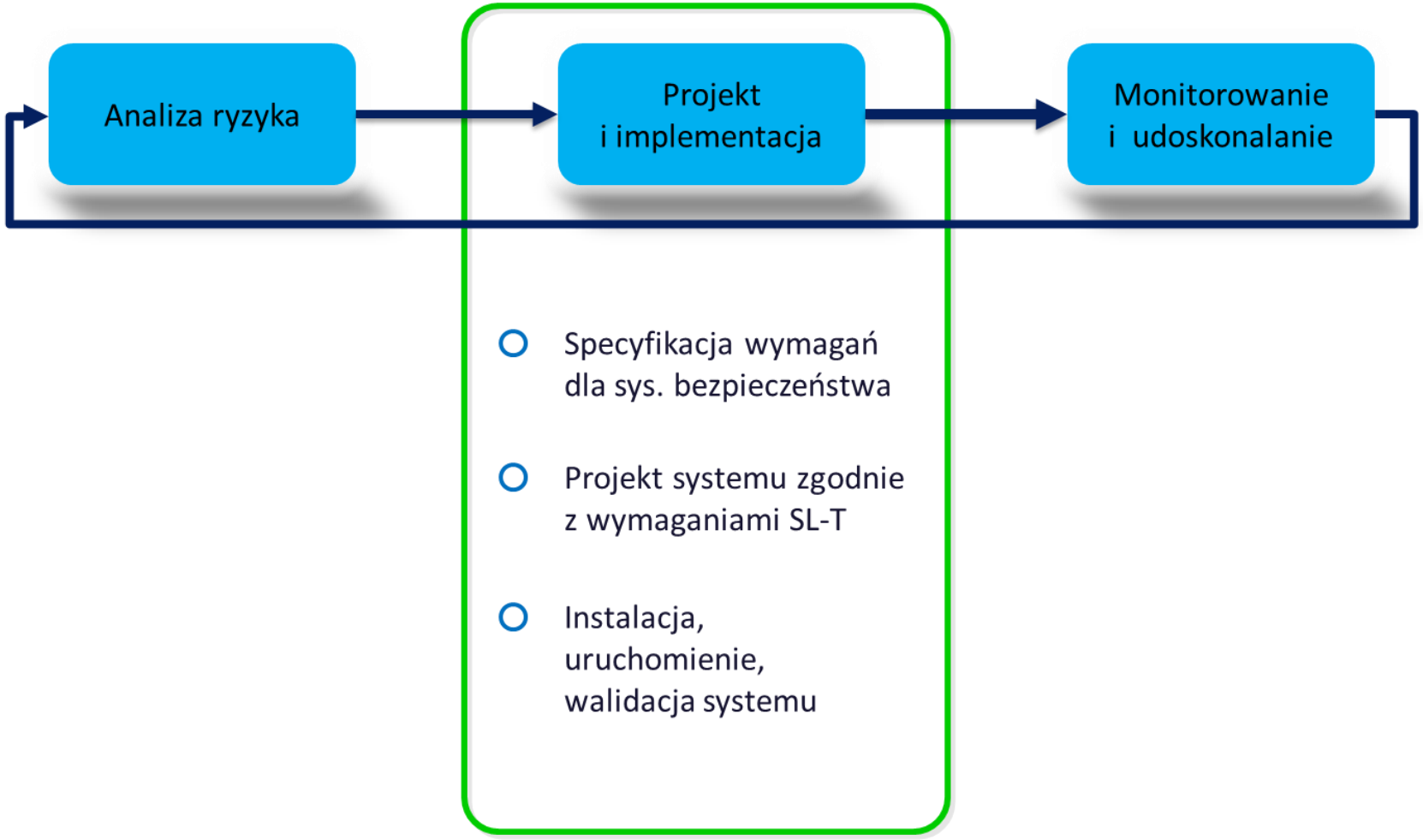
- Nie wszystkie elementy systemu automatyki wymagają takiego samego stopnia ochrony
- Segmentacja systemu znacznie ułatwia zarządzanie i monitorowanie systemu
- Wydzielenie kanałów komunikacyjnych ułatwia ich monitorowanie oraz zabezpieczenia

Poziom bezpieczeństwa (Security Level)

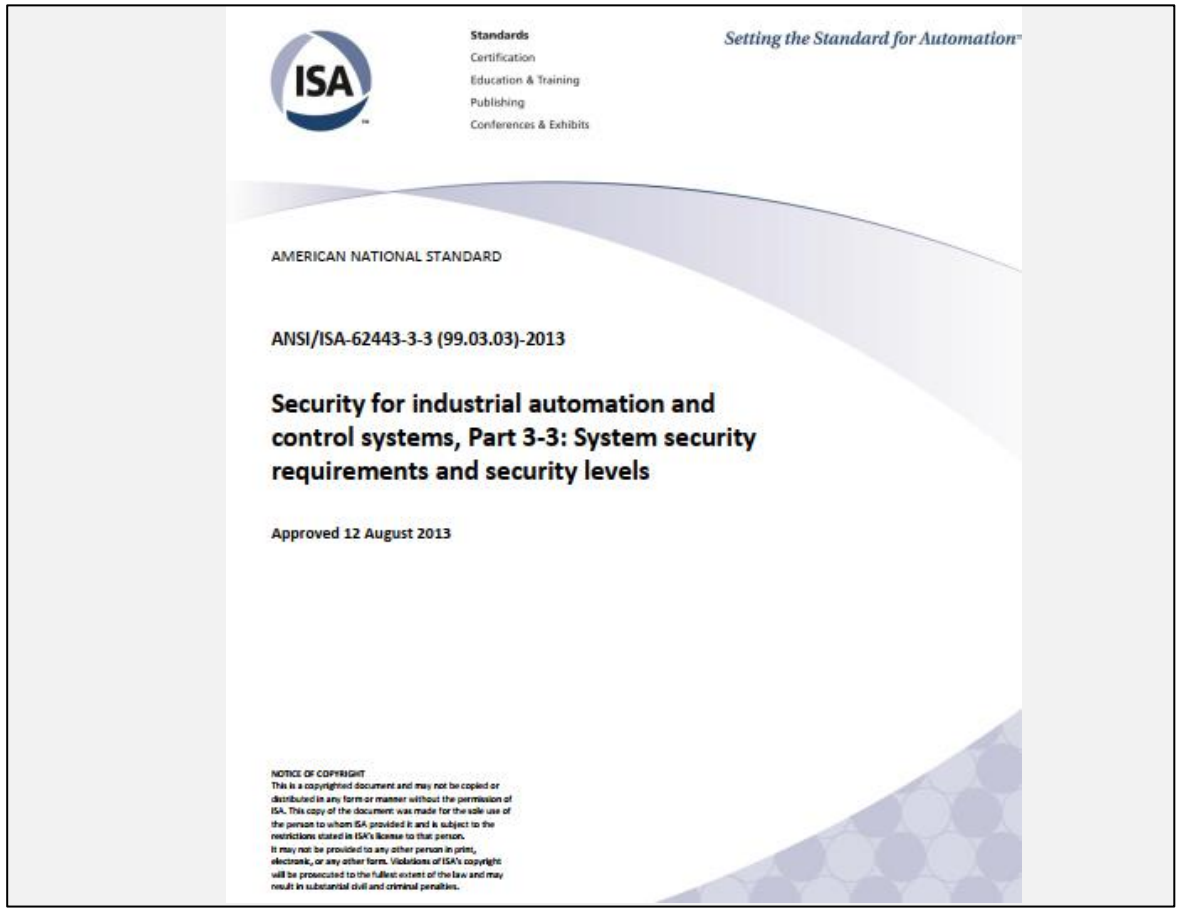


Specyfikacja wymagań w zakresie cyberbezpieczeństwa

Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443

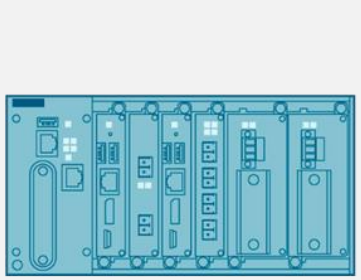


Poziom bezpieczeństwa, a wymagania jakie należy spełnić



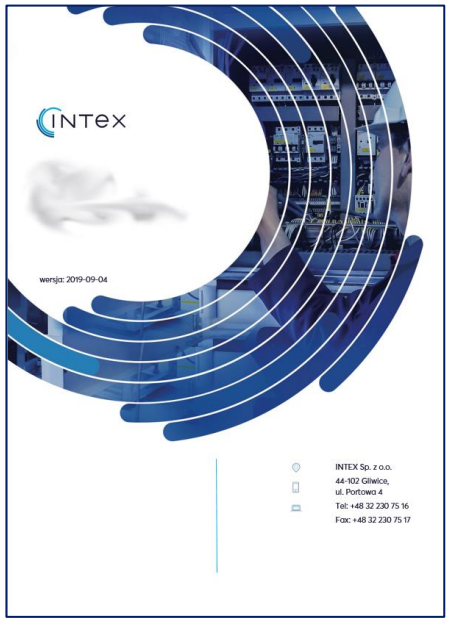
- IEC 62443-3-3 Annex B definiuje zestaw wymagań jakie należy spełnić aby osiągnąć wymagany poziom bezpieczeństwa SL
- Zestaw wymagań obejmuje:
  - 37 wymagań dla SL1
  - 60 wymagań dla SL2
  - 90 wymagań dla SL3
  - 100 wymagań dla SL4

Projekt systemu zgodnie z wymogami specyfikacji cyberbezpieczeństwa

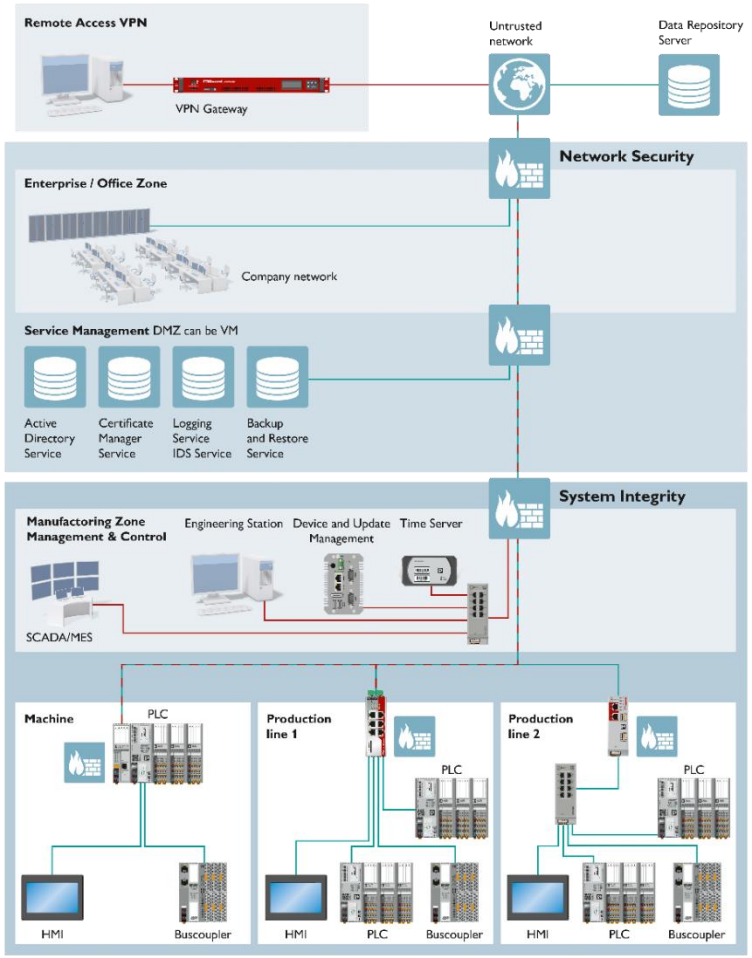


- Implementacja systemu cyberbezpieczeństwa powinna obejmować:
  - rozwiązania techniczne
  - rozwiązania organizacyjne
  - rozwiązania w zakresie ochrony fizycznej

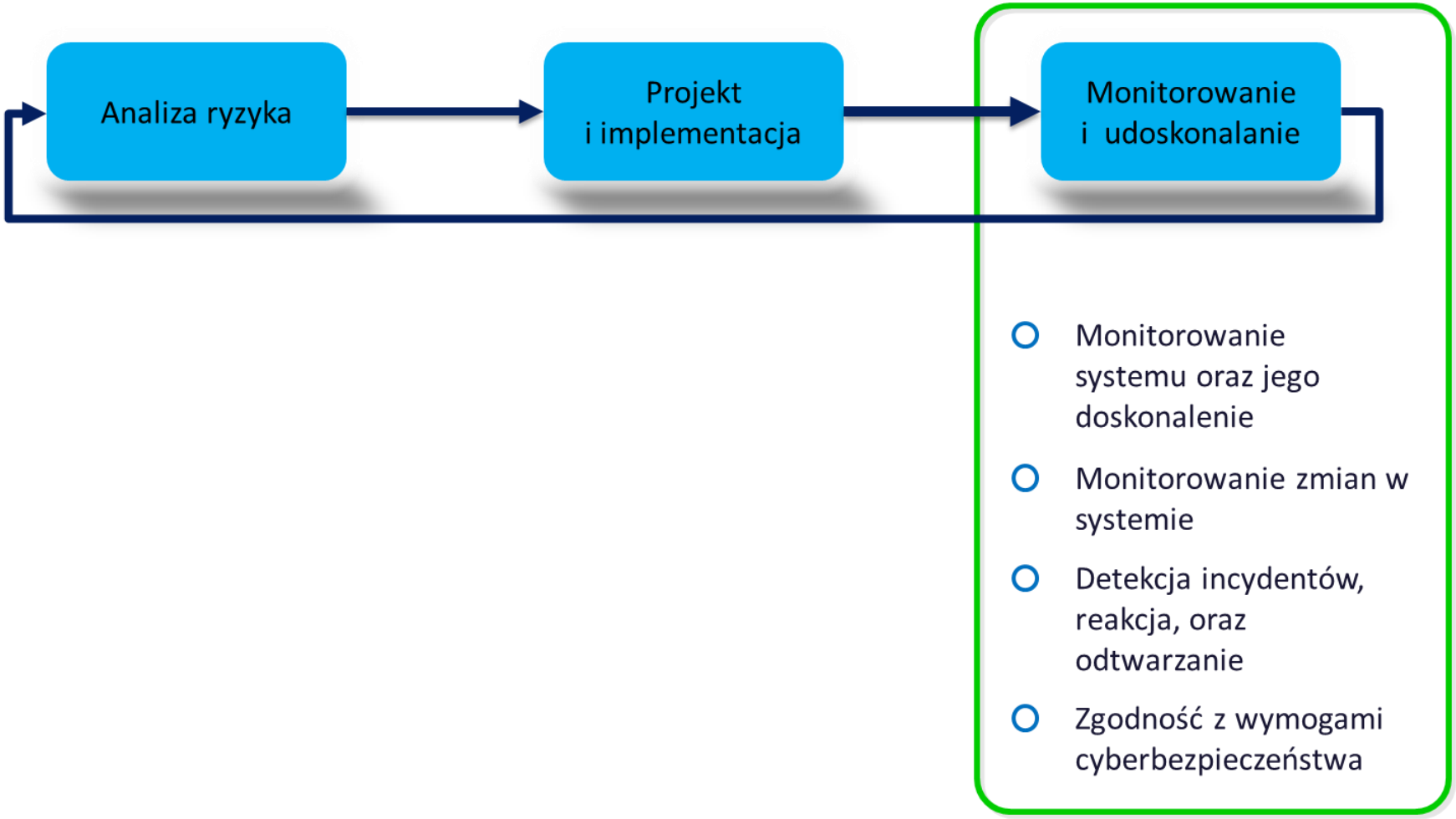
Instalacja, uruchomienie i walidacja systemu



?



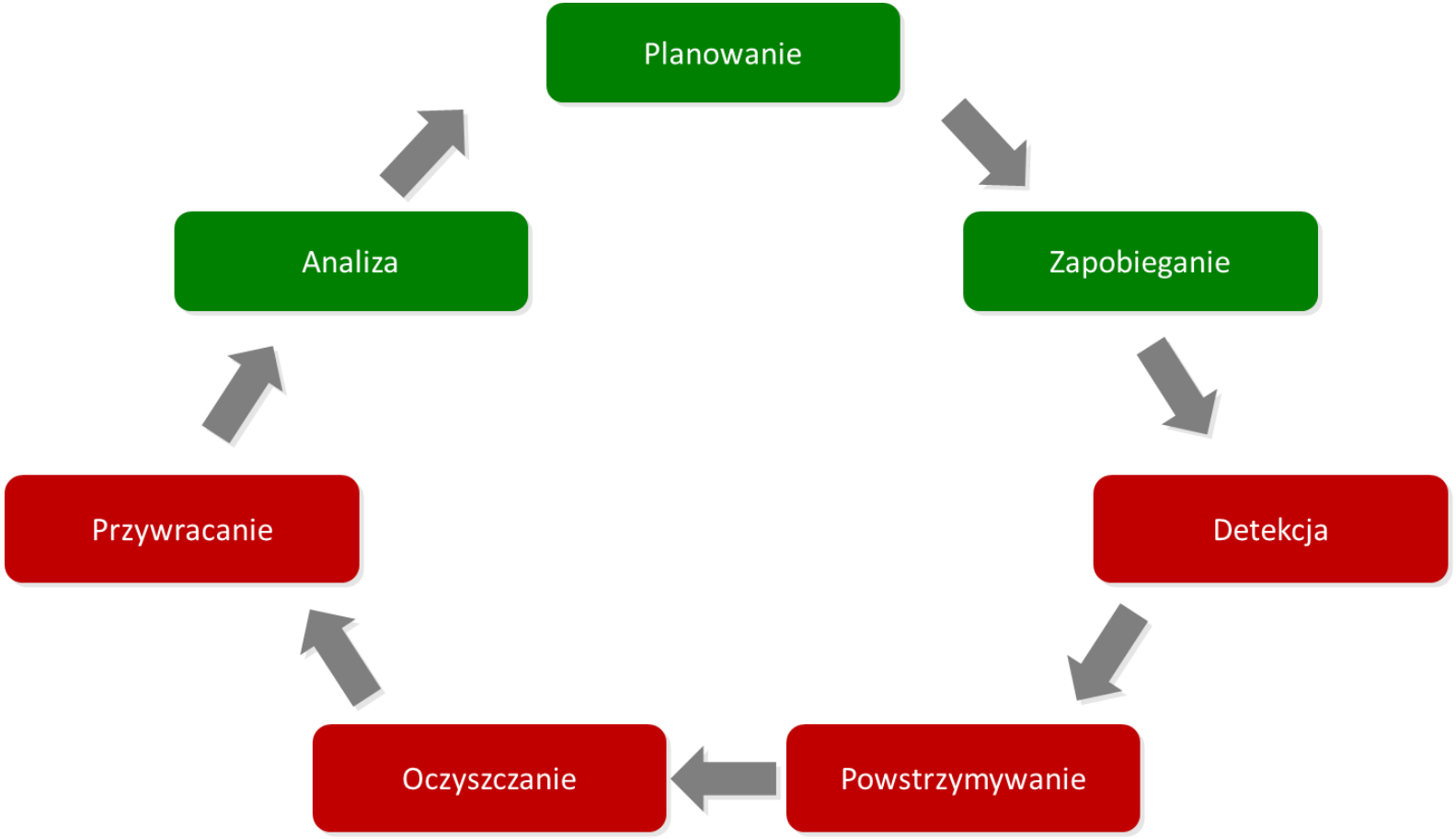
Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443



Zarządzanie systemem

- Monitorowanie bezpieczeństwa systemów
- Aktualizacja urządzeń, systemów
- Zmiany i zarządzanie zmianami
- Przygotowanie i zarządzanie kopiami systemu

Incydenty – przygotowanie, obsługa, wnioskowanie



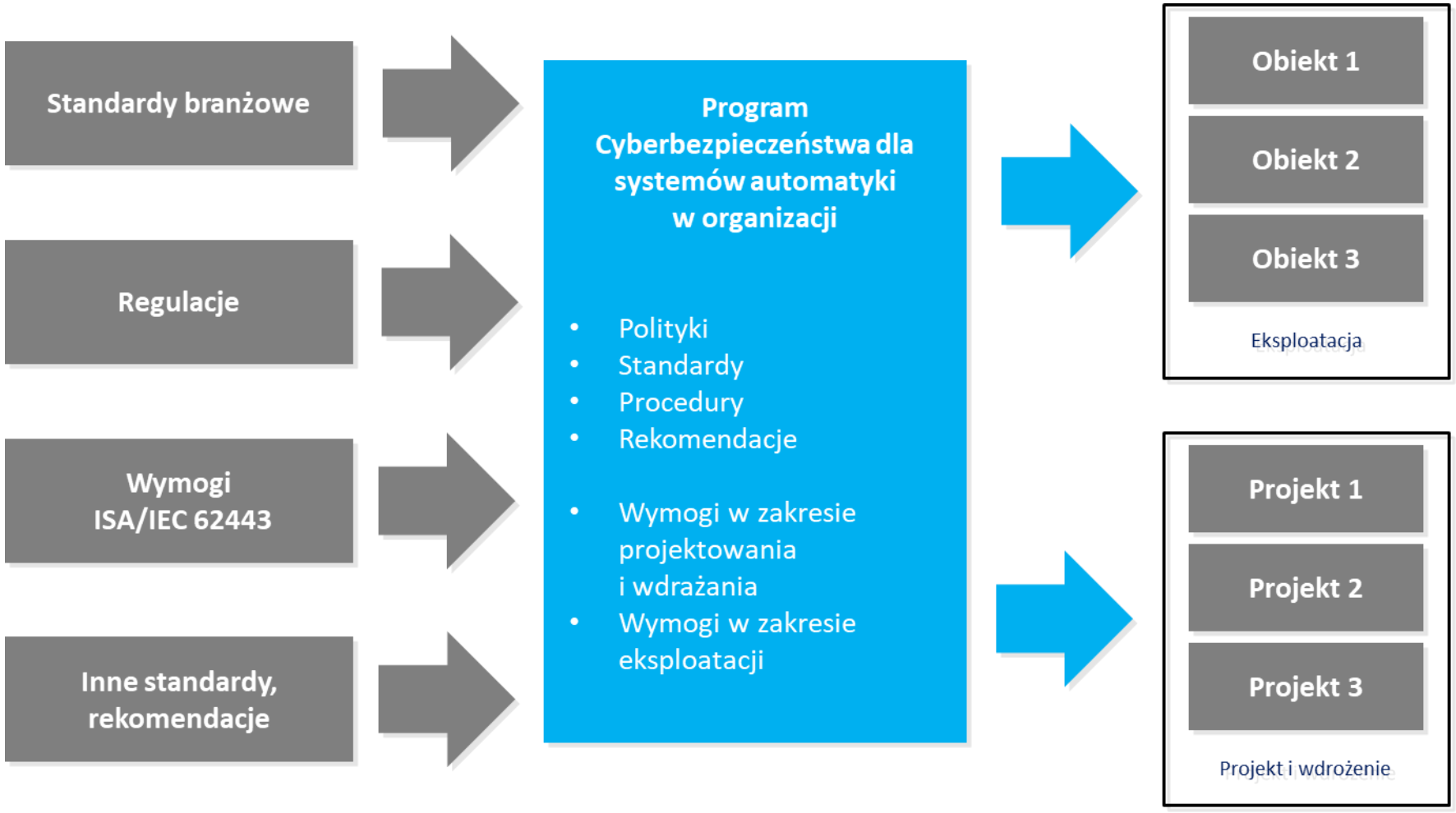
Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443

- **System zarządzania: polityka, procedury, szkolenia, budowa świadomości**
- **Okresowe audyty systemu bezpieczeństwa**

Wsparcie dla systemu cyberbezpieczeństwa: audyty, testy, edukacja

- Wewnętrzna, okresowa weryfikacja systemu bezpieczeństwa
- Audyty wewnętrzne i zewnętrzne
- Testy systemu bezpieczeństwa
- Podnoszenie świadomości użytkowników systemu

Przygotowanie kompletnego programu cyberbezpieczeństwa dla systemu



(Cyber)bezpieczeństwo systemów OT

- Bezpieczeństwo systemów sieciowych to nie wszystko
- Bezpieczeństwo systemu powinno być uwzględnione na etapie projektu technicznego
- Bezpieczeństwo systemu powinno być wspierane przez aplikacje (PLC/HMI/SCADA)
- Bezpieczeństwo fizyczne pełni kluczową rolę

Dyrektor Techniczny

Artur Szymiczek

+48 664 441 930

aszymiczek@intex.com.pl

INTEX Sp. z o.o.
ul. Portowa 4
44-102 Gliwice

tel: +48 32 230 75 16
faks: +48 32 230 75 17

www.intex.com.pl

intex@intex.com.pl