DCS
Rozproszone Systemy Automatyki
Wykład 9

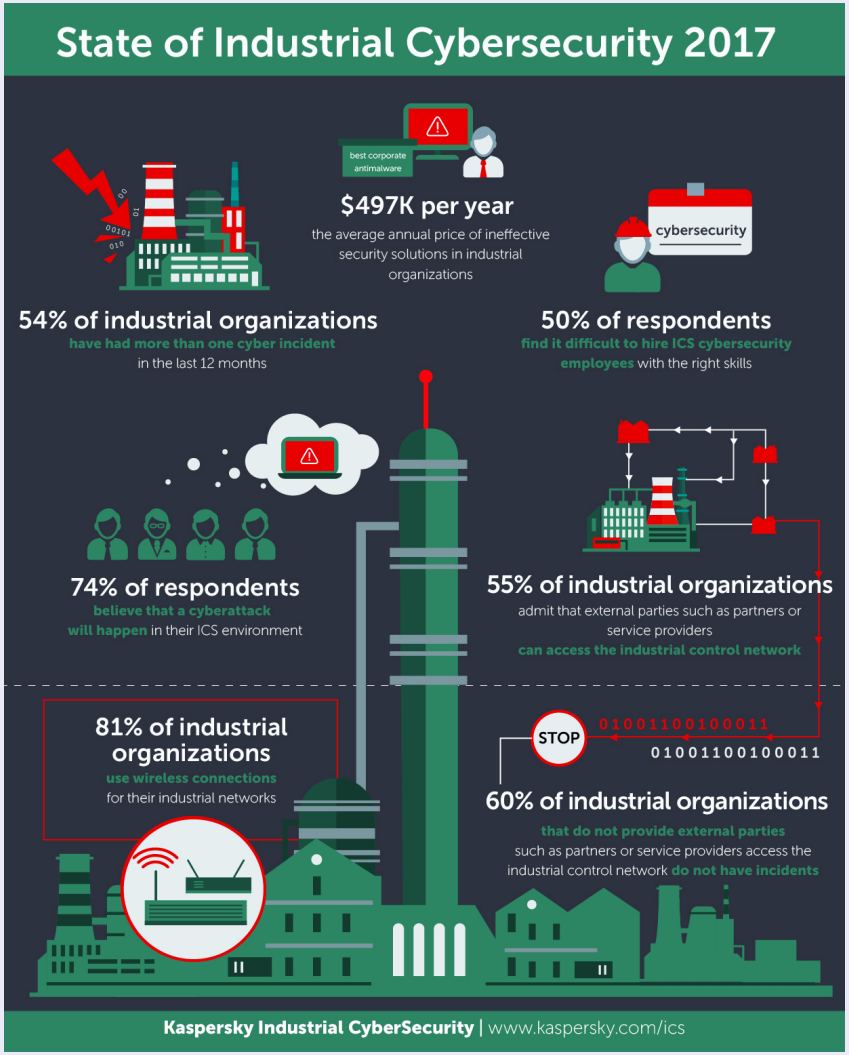
Adam Ratajczak

Pracownia Automatyki, Modelowania i Mechatroniki
Katedra Automatyki, Mechatroniki i Systemów Sterowania
Wydział Elektroniki
Politechnika Wrocławska

[1] Niniejszy dokument zawiera materiały do wykładu z przedmiotu Rozproszone Systemy Automatyki. Jest on udostępniony pod warunkiem wykorzystania wyłącznie do własnych, prywatnych potrzeb i może być kopiowany wyłącznie w całości, razem ze stroną tytułową.

Wstęp

Trochę statystyki



Wstęp

Pojęcia

IT Information Technology
Sieć IT – sieć do przesyłu danych informatycznych

OT Operational Technology
Sieć OT – sieć do przesyłu danych sterowania przemysłowego

Wstęp

Trendy technologiczne

- Technologie COTS (Commercial–Off–The–Shelf)
  - Systemy operacyjne (Windows, WinCE,embedded RTOS, itp.)
  - Bazy danych, serwery web, przeglądarki web
  - Protokoły IP (HTTP, SMTP, FTP, DCOM, XML, SNMP, itp.)
  - Urządzenia sieciowe (switches, routers, firewalls)
- Połączenie sieci IT z siecią OT
  - Poprawa efektywności zarządzania przedsiębiorstwem
  - Zdalny dostęp do procesu (zarówno do centrów sterowania jak i urządzeń obiektowych)
- Sieci typu Ethernet
  - Powszechne w wyższych warstwach sieci w przedsiębiorstwie, coraz bardziej popularne w niższych warstwach
  - Wiele starszych protokołów obudowanych przez TCP lub UDP
  - Każde nowe urządzenie ma port Ethernet
  - Każda nowa instalacja automatyki jest oparta na sieci Ethernet

Cyber–Bezpieczeństwo

CIA czy AIC?

Confidentiality, integrity, and availability
Poufność, spójność i dostępność

- Sieci IT wymagają CIA
  Poufność danych (ochrona własności przemysłowej) jest najważniejsza
- Sieci OT wymagają AIC
  Dostępność i spójność jest najważniejsza
  Dane sterujące zwykle nie muszą być poufne

Bezpieczeństwo cybernetyczne nie może wpływać negatywnie na dostępność.

Cyber–Bezpieczeństwo

Zagrożenia bezpieczeństwa cybernetycznego

- Wirusy i robaki
- DoS (Denial of Service), DDoS (Distributed Denial of Service)
- Nieautoryzowany lub nieznany dostęp
- Nieaktualizowany system
- Nie używanie, lub marne korzystanie z antywirusów
- Nieskonfigurowane firewalls
- Niewłaściwe używanie stacji operatorskich ICS
- Nieautoryzowane aplikacje
- Zbędne aplikacje
- Zbędne otwarte porty (FTP, Telnet, SNMP)
- Wrażliwe urządzenia sterujące
- Skanowanie sieci przez administratorów sieci

Cyber–Bezpieczeństwo

Zagrożenia bezpieczeństwa cybernetycznego c.d.

- Brak możliwości ograniczania dostępu
- Brak możliwości przerwania dostępu
- Nieprzeglądane logi systemowe
- Przypadkowe błędne konfiguracje urządzeń
- Niewłaściwie zabezpieczone urządzenia
- Niewłaściwie zabezpieczone sieci bezprzewodowe
- Połączenia z odległymi urządzeniami nieszyfrowanym połączeniem
- Przesyłanie nazw użytkowników i haseł czystym tekstem
- Używanie domyślnych haseł
- Błędna i problematyczna polityka haseł
- Domyślne konfiguracje zabezpieczeń w systemach operacyjnych

Cyber–Bezpieczeństwo

Anatomia cyber–ataku

1. Faza – Uzyskanie dostępu do sieci OT
   1. Rozpoznanie
   2. Uzbrajanie
   3. Dostarczenie
   4. Wyzysk
   5. Instalacja
   6. Przejęcie kontroli (uzyskanie dostępu)
2. Faza – Wykorzystanie uzyskanego dostępu do przeprowadzenia właściwego ataku
   1. Przygotowanie
   2. Przetestowanie
   3. Użycie (sabotaż procesu produkcyjnego, kradzież własności intelektualnej i/lub przemysłowej, szpiegostwo przemysłowe, gospodarcze)

Cyber–Bezpieczeństwo

Skutki ataku

- Straty w produkcji
- Nałożenie kar
- Pozwy sądowe
- Utrata zaufania publicznego
- Utrata wartości rynkowej
- Fizyczne uszkodzenia
- Szkody w środowisku naturalnym
- Uszczerbki na zdrowiu
- Ofiary w ludziach

Cyber–Bezpieczeństwo

Ryzyko w cyber–bezpieczeństwie

Ryzyko to **prawdopodobieństwo**, że **źródło zagrożenia** zostanie wykorzystane do spowodowania **zdarzenia zagrożenia** za pomocą **wektora zagrożenia**, korzystając z potencjalnej **luki** w zabezpieczeniu **celu** i jakie będą w wyniku tego **konsekwencje** i **skutki**.

Cyber–Bezpieczeństwo

Definicje

Źródłem zagorżenia jest inicjator wyzysku zwany również aktorem zagrożenia.

Zdarzeniem zagrożenia jest fakt wykorzystania (wyzysku) luki w zabezpieczeniach lub bezpośredni atak na system.

Wektor zagrożenia to droga do przeprowadzenia ataku lub metoda dostarczania złośliwego oprogramowania, takie jak używanie zainfekowanego pen–drive lub wysyłanie wiadomości e-mail typu phishing.

Luką w zabezpieczeniu jest słabość systemu, taka jak błędnie skonfigurowane usługi sieciowe, łatwe do odgadnięcia hasła lub błędy w aplikacjach takie jak na przykład przepełniający się buffor.

Cyber–Bezpieczeństwo

Definicje c.d.

Prawdopodobieństwo to szansa z jaką znaleziona luka w zabezpieczeniu może stać się zdarzeniem zagrożenia.

Celem jest rozpatrywany system automatyki

Konsekwencją są bezpośrednie wyniki przeprowadzonego zdarzenia zagrożenia, takie jak awarie urządzeń, zaprzestanie świadczenia usług, instalacja podejrzanego oprogramowania.

Skutkiem jest wpływ zdarzenia zagorżenia na pracę, wizerunek, dobrobyt przedsiębiorstwa.

Cyber–Bezpieczeństwo

Określanie ryzyka

$$R = \frac{D + 2K + 2P + 2S}{4}$$

gdzie

- R ryzyko
- D dotkliwość
- K krytyczność
- P prawdopodobieństwo
- S skutek

Cyber–Bezpieczeństwo

Definicje

Dotkliwość $\in [0, 10]$, przypisane do luki w zabezpieczeniu, określone przez nadrzędną instytucję np. National Vulnerability Database.

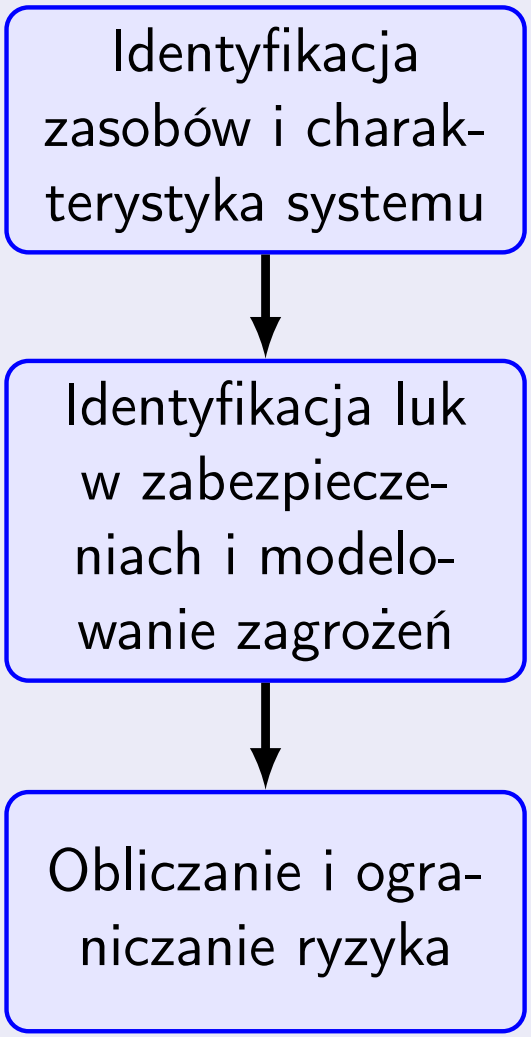
Krytyczność $\in [1, 5]$, określenie wpływu rozpatrywanego systemu na całość procesu.

Prawdopodobieństwo $\in [1, 5]$, odzwierciedla szansę pomyślnego wykorzystania luki w ataku.

Skutek $\in [1, 5]$, odzwierciedla wpływ na finanse i wizerunek przedsiębiorstwa, związane z tym ryzyko narażenia zdrowia pracowników i osób postronnych w wyniku uszkodzenia systemu.

Cyber–Bezpieczeństwo

Określanie ryzyka



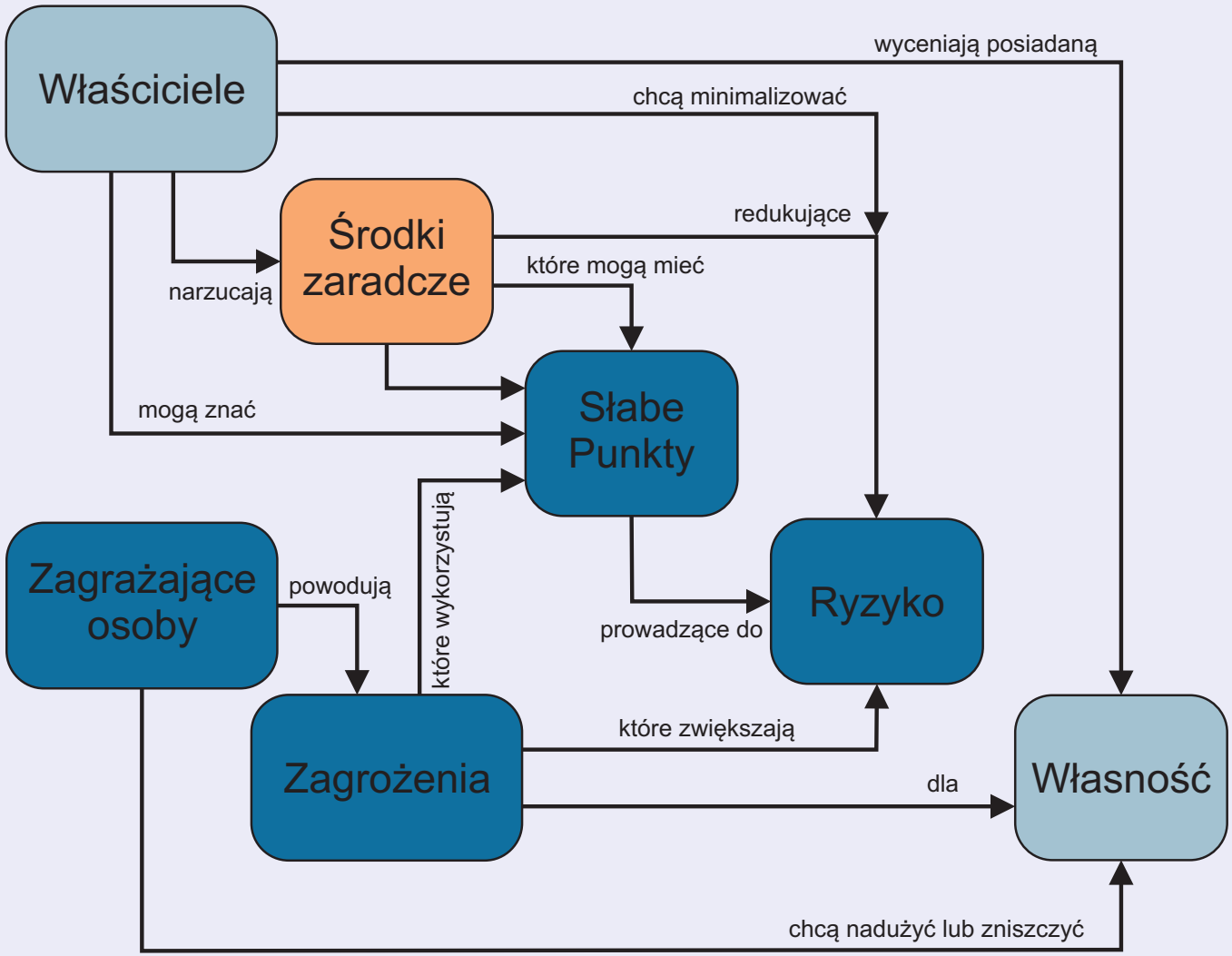
Identyfikacja potencjalnych celów

Identyfikacja potencjalnych luk w zabezpieczeniach, wektorów zagrożeń, źródeł zagrożeń, zdarzeń zagrożeń oraz oszacowanie prawdopodobieństwa i konsekwencji

Obliczenie potencjalnego skutku ataku

Cyber–Bezpieczeństwo

Ocena wrażliwości systemu bezpieczeństwa



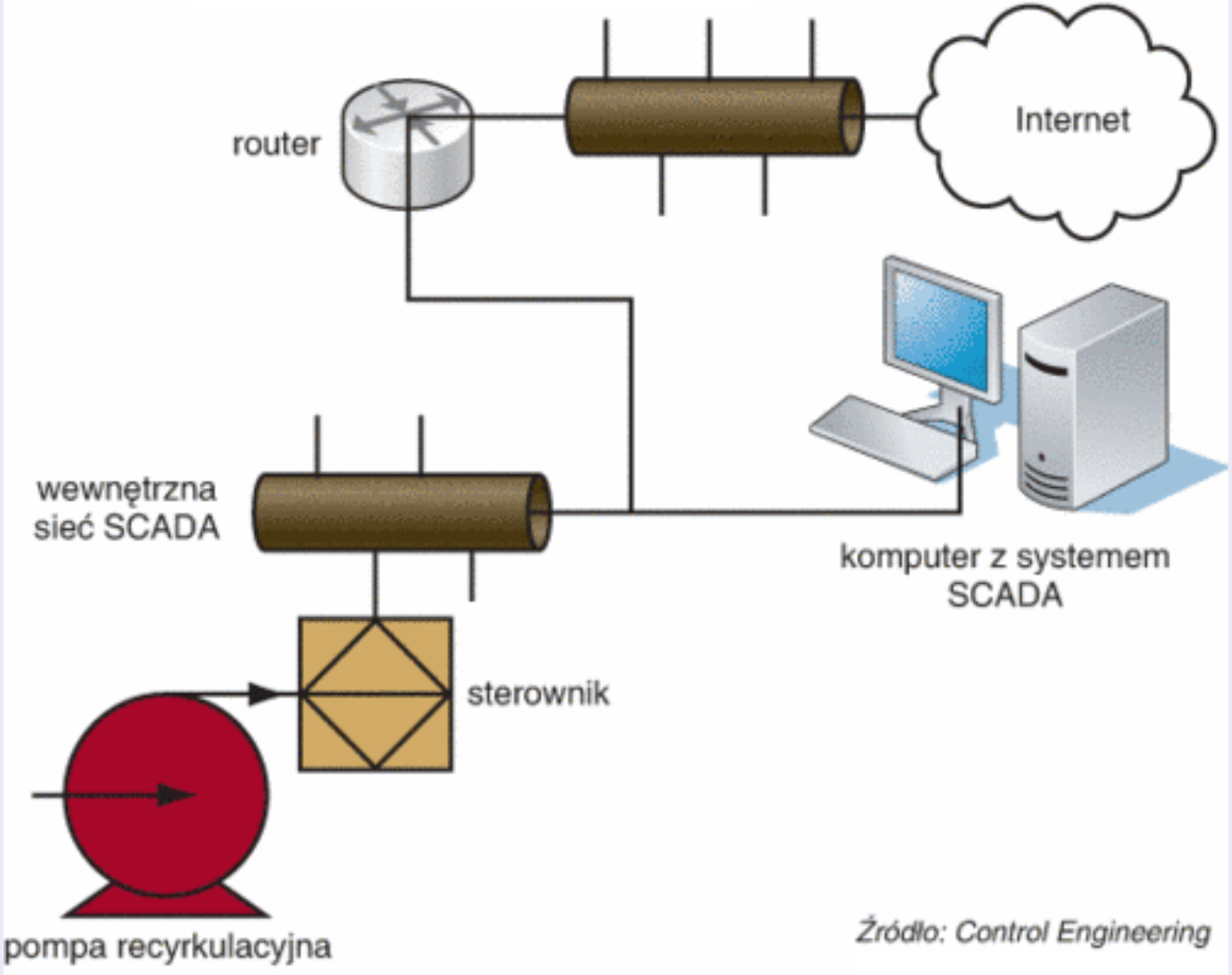
Cyber–Bezpieczeństwo

Tablica oceny zagrożenia bezpieczeństwa cybernetycznego

Poziom zagrożenia	Konsekwencje		
	Małe (1)	Średnie (2)	Duże (3)
Wysoki (A)	A1	A2	A3
Przeciętny (B)	B1	B2	B3
Niski (C)	C1	C2	C3

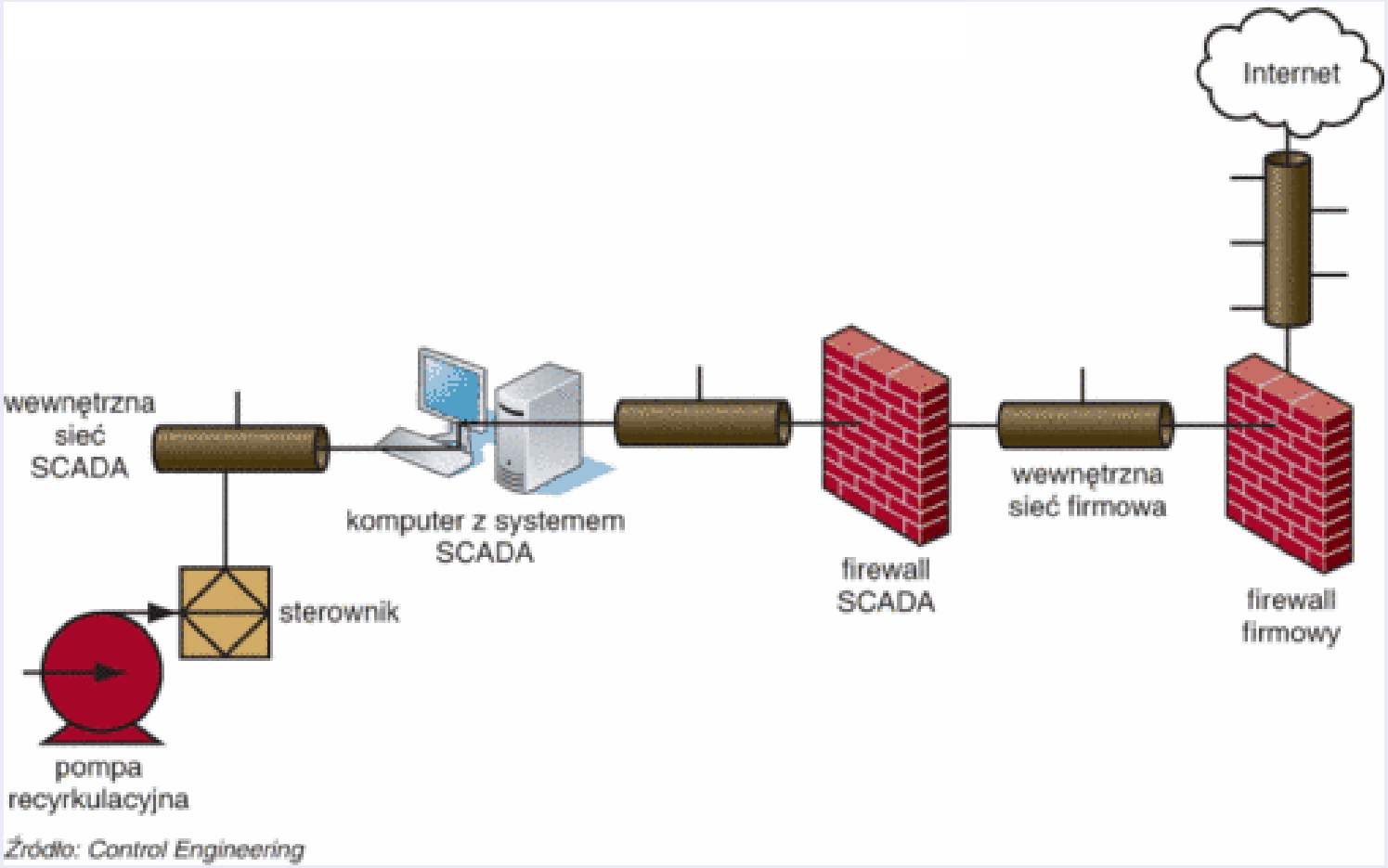
Cyber–Bezpieczeństwo

Niezabezpieczony system sterowania



Cyber–Bezpieczeństwo

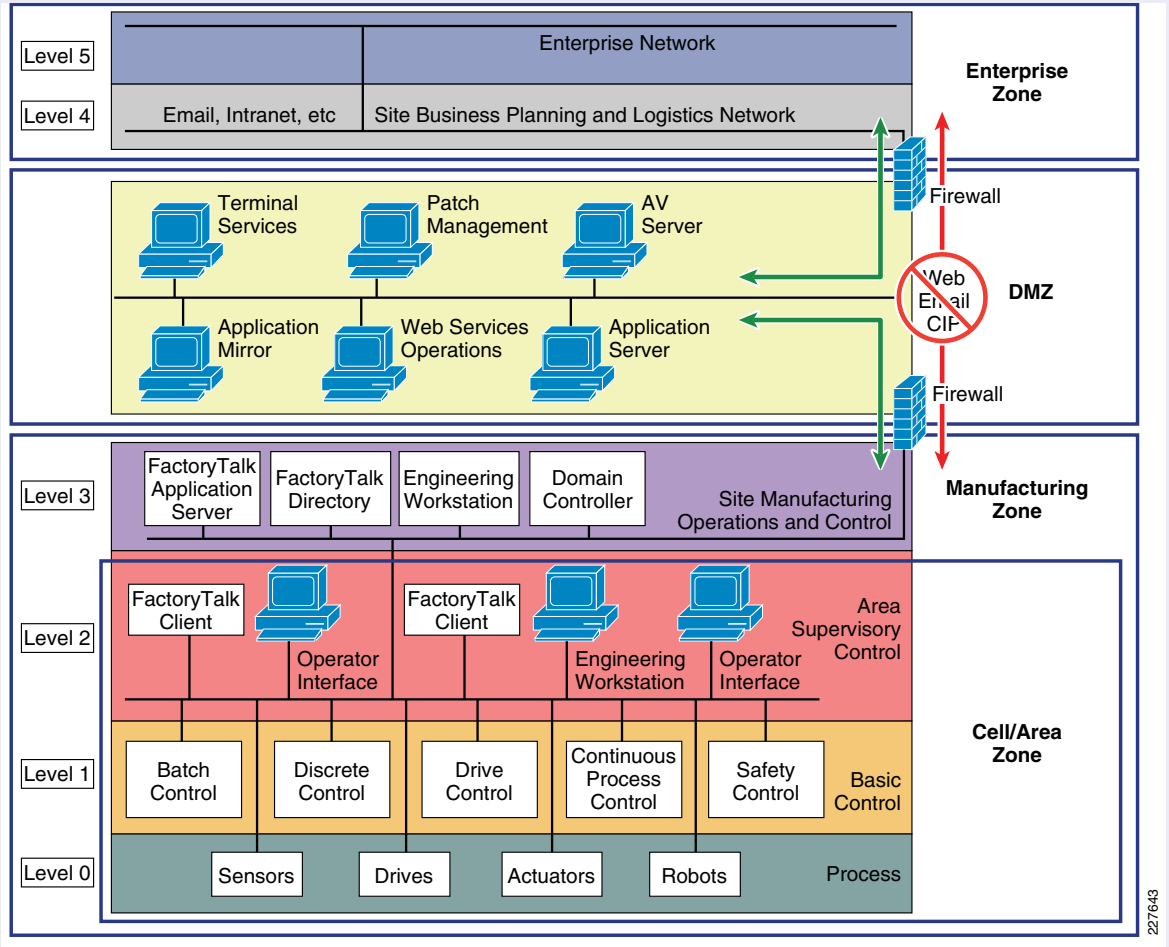
Zabezpieczony system sterowania



To dziś już nie wystarcza!!!

Cyber–Bezpieczeństwo

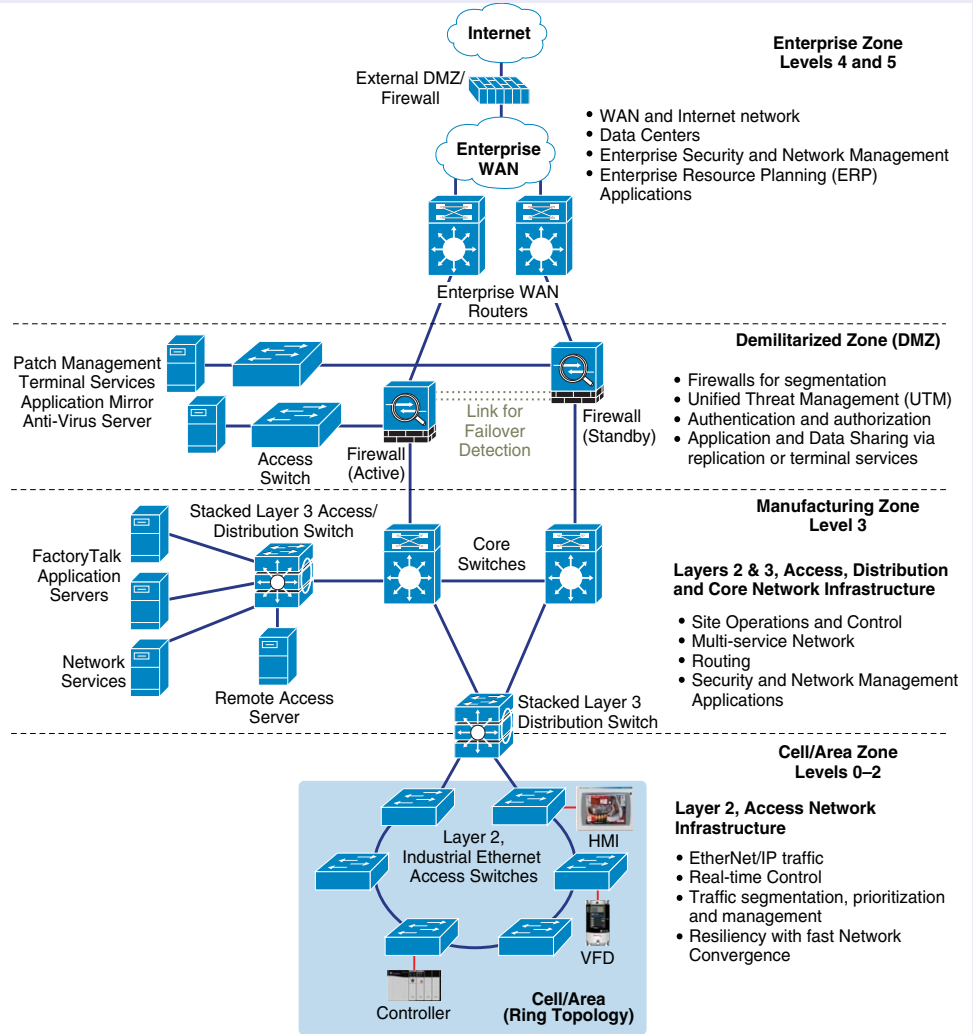
Właściwie zabezpieczony system sterowania



CPwE – Converged Plantwide Ethernet

Cyber–Bezpieczeństwo

Właściwie zabezpieczony system sterowania



Cyber–Bezpieczeństwo

Podsumowanie

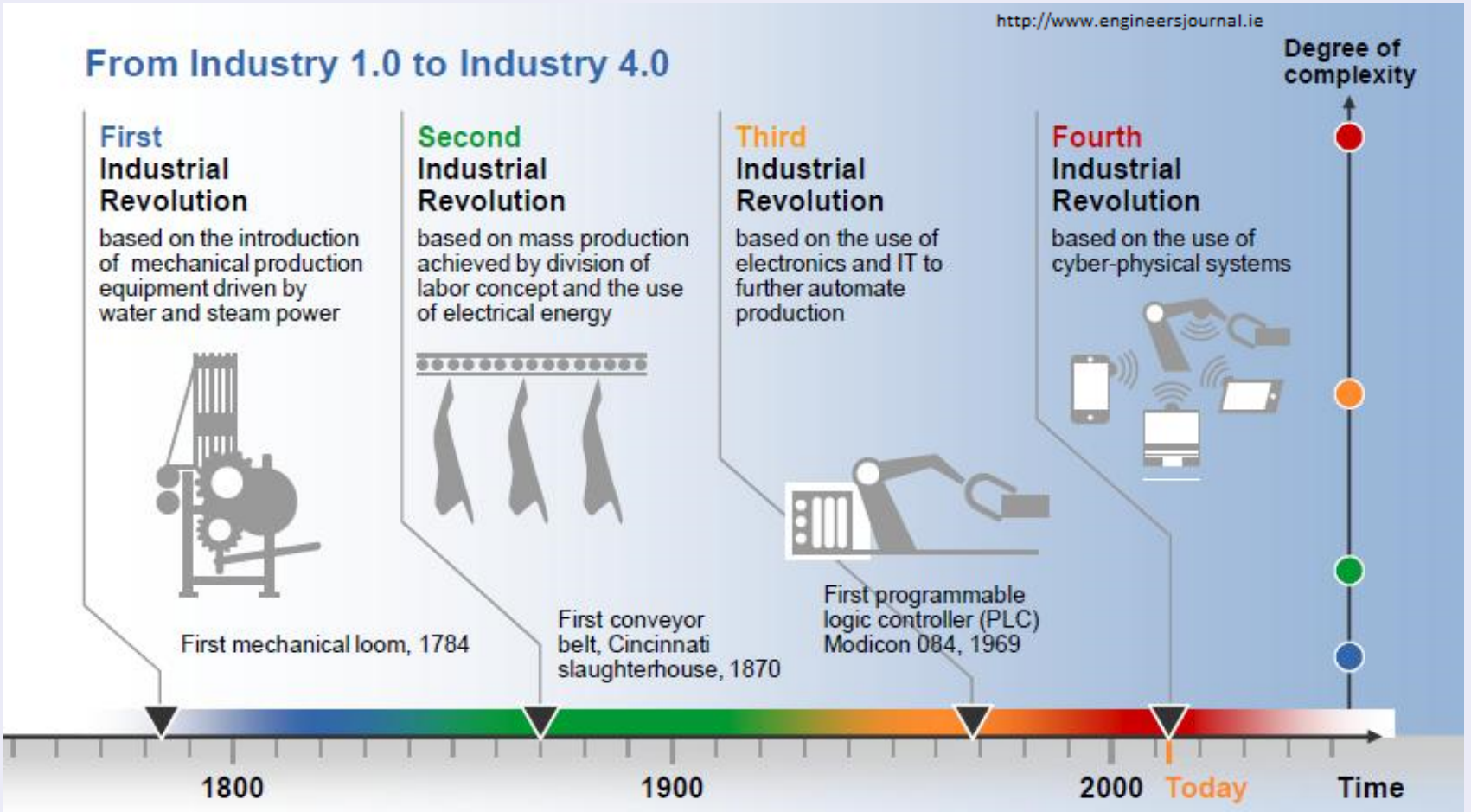
W kwestiach cyber–bezpieczeństwa
nie powinno się pytać **„Czy?”** lecz **„Kiedy?”**.

Procedura postępowania:

1. Określ co posiadasz i jakimi środkami dysponujesz
2. Określ co jest nieprawidłowe wewnątrz tego co posiadasz
3. Napraw to co wiesz, że jest nieprawidłowe
4. Wyczyść i powtórz

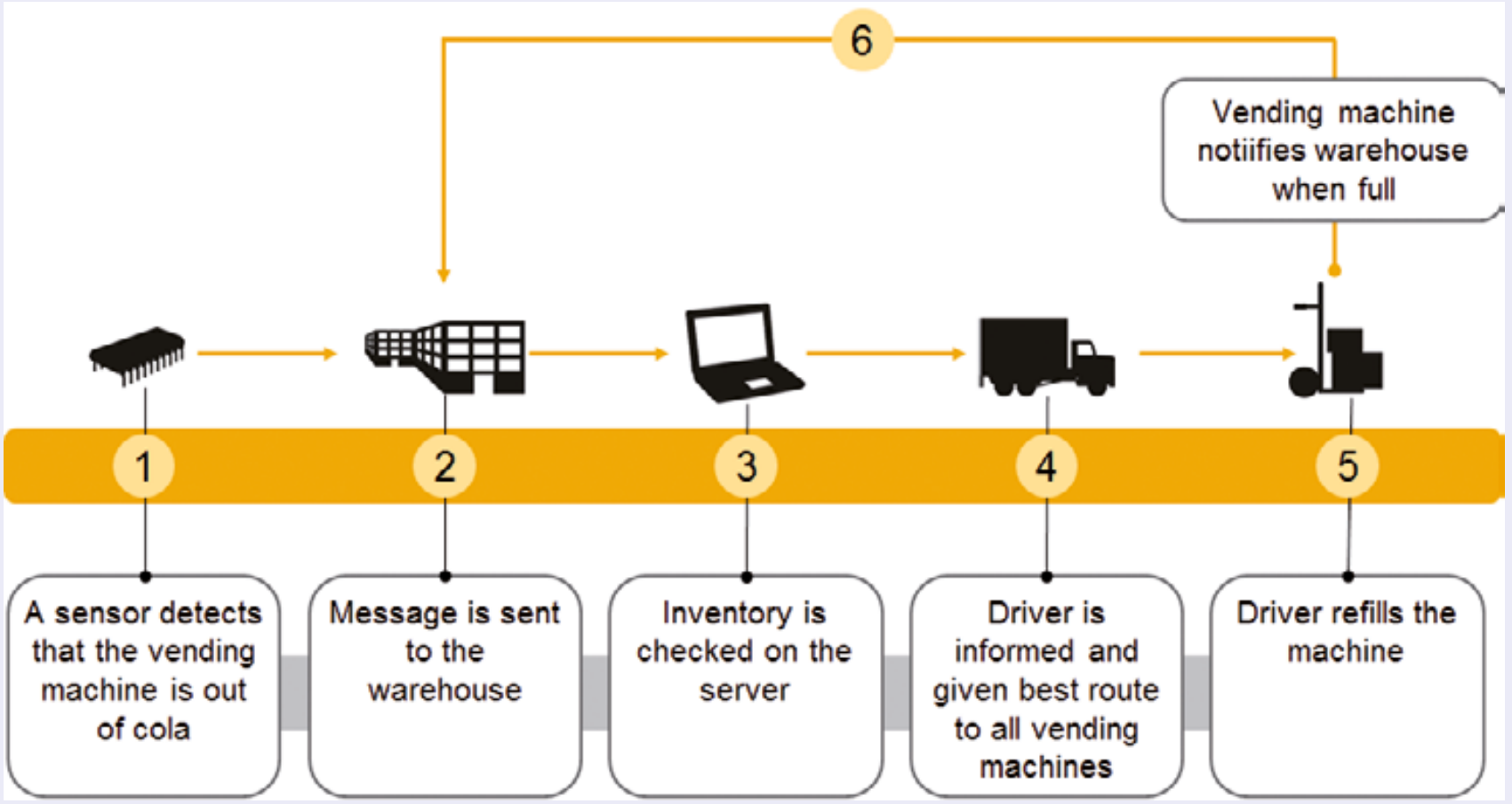
Industrie 4.0

Ewolucja



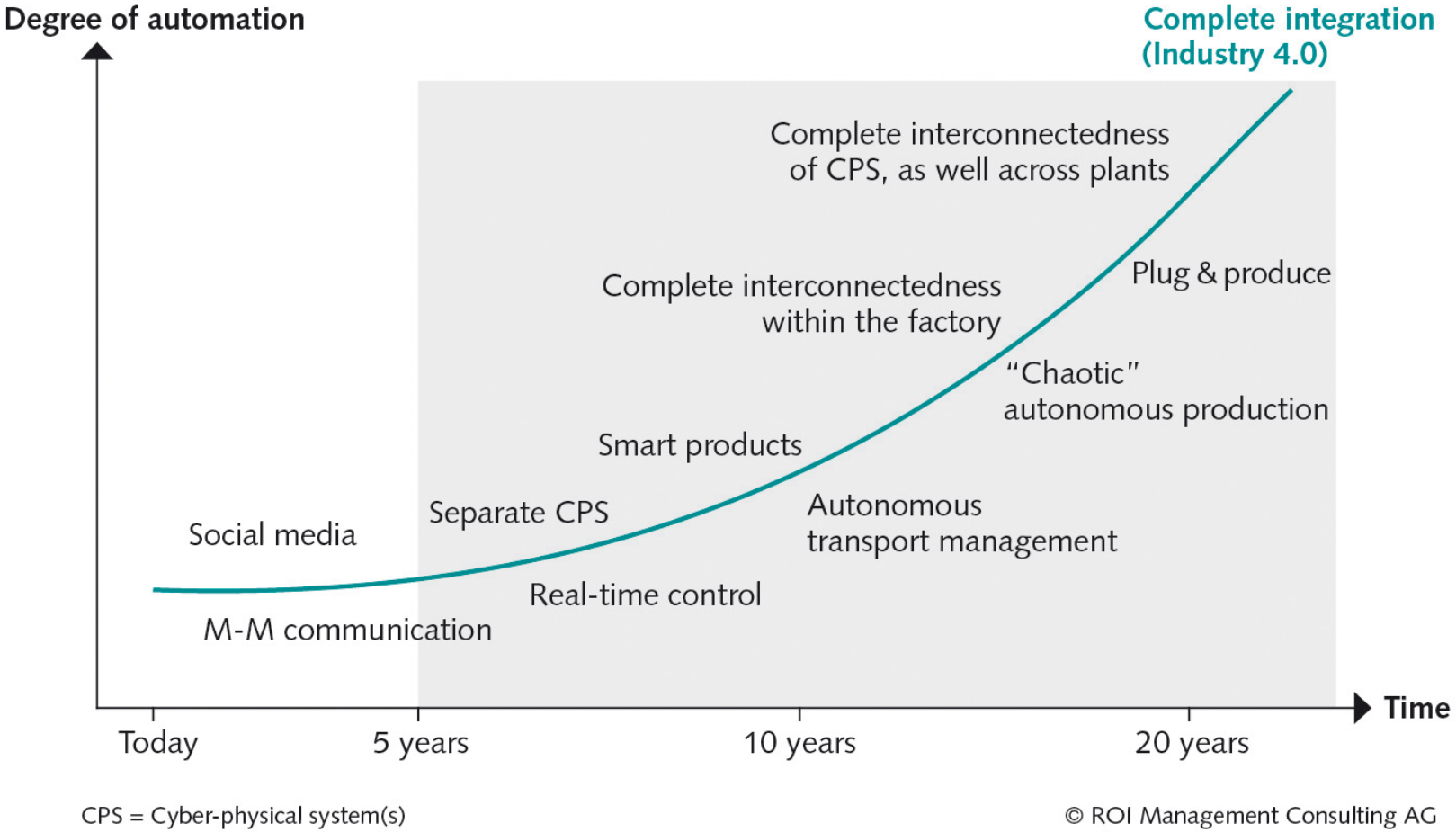
Industrie 4.0

Internet of Things – przykład



Industrie 4.0

Dokąd to zmierza



Słowniczek

LAN	Local Area Network
WAN	Wide Area Network
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
IoT	Internet of Things
IP	Internet Protocol
ICS	Industrial Control System
DMS	Demilitarized Zone
CPwE	Converged Plantwide Ethernet
DoS	Denial of Service
DDoS	Distributed Denial of Service

Literatura


Industrial Cybersecurity
Pascal Ackerman


Guide to Industrial Control Systems (ICS) Security
NIST Special Publication 800-82


Converged Plantwide Ethernet (CPwE) Design and Implementation Guide
Cisco and Rockwell Automation


Recommendations for implementing the strategic initiative INDUSTRIE 4.0