DCS
Rozproszone Systemy Automatyki
Wykład 8

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

Pojęcia

Authentication – uwierzytelnianie Weryfikacja czy użytkownik (proces) jest tym, za kogo się podaje.
Kto to jest?
Jak sprawdzić, że to ten użytkownik?

Authorization – autoryzacja Określenie praw dostępu wybranego użytkownika (procesu) do wybranych zasobów.
Czy użytkownik może to czytać?
Czy użytkownik może to zmienić?

Firewall

Rodzaje

1. Packet Filtering Firewalls
2. Statefull Inspection Firewalls
3. Application–Proxy Gateway Firewalls

Firewall

Funkcjonalność

- Generalne blokowanie komunikacji za wyjątkiem...
- Wymuszanie uwierzytelniania dla wszystkich chcących dostać się do procesu
  - proste hasła
  - skomplikowane hasła
  - tokeny
  - czytniki kart
  - biometryka
- Autoryzacja względem adresów docelowych (tylko to co potrzebne)
- Monitorowanie i logowanie zdarzeń w sieci
- Wymuszanie polityki haseł, uniemożliwianie automatycznego zapamiętywania haseł

Segmentacja sieci

Metodologie

- Podział logiczny
  - Virtual Local Area Networks (VLANs)
  - Encrypted Virtual Private Networks (VPNs)
  - Jednokierunkowe bramy (Unidirectional gateways, data diodes)
- Podział fizyczny
- Filtrowanie ruchu sieciowego
  - Ze względu na adresy IP (routing)
  - W oparciu o urządzenia/systemy (Kto może się komunikować z kim i w jakim celu)
  - Filtrowanie portów i protokołów
  - Filtrowanie ze względu na zawartość pakietów (Application filtering)

Segmentacja sieci

Kontrola pomiędzy segmentami sieci

- Stosowanie „whitelist" zamiast „blacklist"
- Stosowanie serwerów proxy jako pośrednika pomiędzy segmentami
- Zapobieganie nieautoryzowanej exfiltracji informacji
- Zezwalanie tylko na połączenia pomiędzy uwierzytelnionym i autoryzowanym nadawcą i odbiorcą

Segmentacja sieci

Kontrola pomiędzy segmentami sieci c.d.

- Fizyczna kontrola dostępu zdalnego
- Ukrywanie adresów sieciowych urządzeń obiektowych przed wykryciem
- Dezaktywacja zbędnych usług i protokołów (service and troublesooting) szczególnie wykorzystujących broadcast
- Określenie i zdefiniowanie stanu urządzeń sieciowych podczas awarii

Segmentacja sieci

Kontrola pomiędzy segmentami sieci c.d.

- Konfigurowanie urządzeń bezpieczeństwa w osobnych podsieciach (rozłączne podsieci)
- Dezaktywacja informacji zwrotnych (non-verbose mode) aby uniemożliwić uzyskanie informacji
- Tam gdzie możliwe implementacja jednokierunkowego przepływu danych
- Uruchomienie pasywnych monitorów aktywności w sieci w celu wykrycia anomalii i wszczęcia alarmu

Zdalny dostęp

Dwa rodzaje zdalnego dostępu

1. Zdalny dostęp do procesu (serwery web)
2. Zdalny dostęp do urządzeń automatyki (routery)

Zdalny dostęp

Metody zdalnego dostępu do procesu

1. HMI server-browser
2. SCADA server-browser
3. SCADA server-mobile phone app
4. SCADA server-thin client
5. Cloud-based SCADA server-multiple

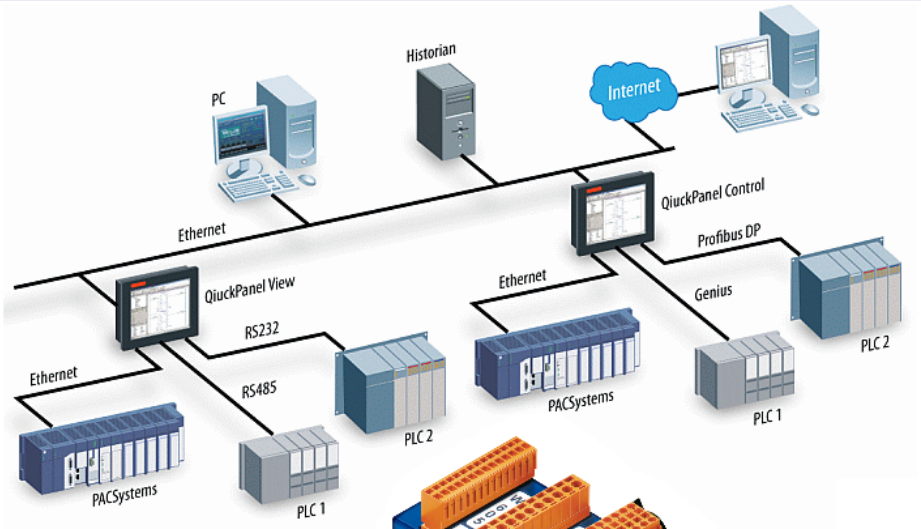
Zdalny dostęp

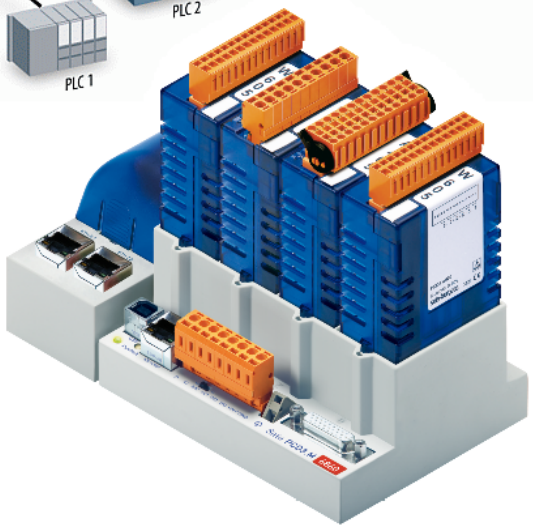
Zalety zdalnego dostępu do procesu

- Zmniejszony czas reakcji operatorów na alarmy i zdarzenia
- Wykorzystanie wiedzy personelu w kilku lokalizacjach
- Zwiększanie jakości poprzez ciągły rozwój procesu
- Redukcja kosztów podróży personelu
- Porównywanie podejmowanych akcji w różnych lokalizacjach

Zdalny dostęp

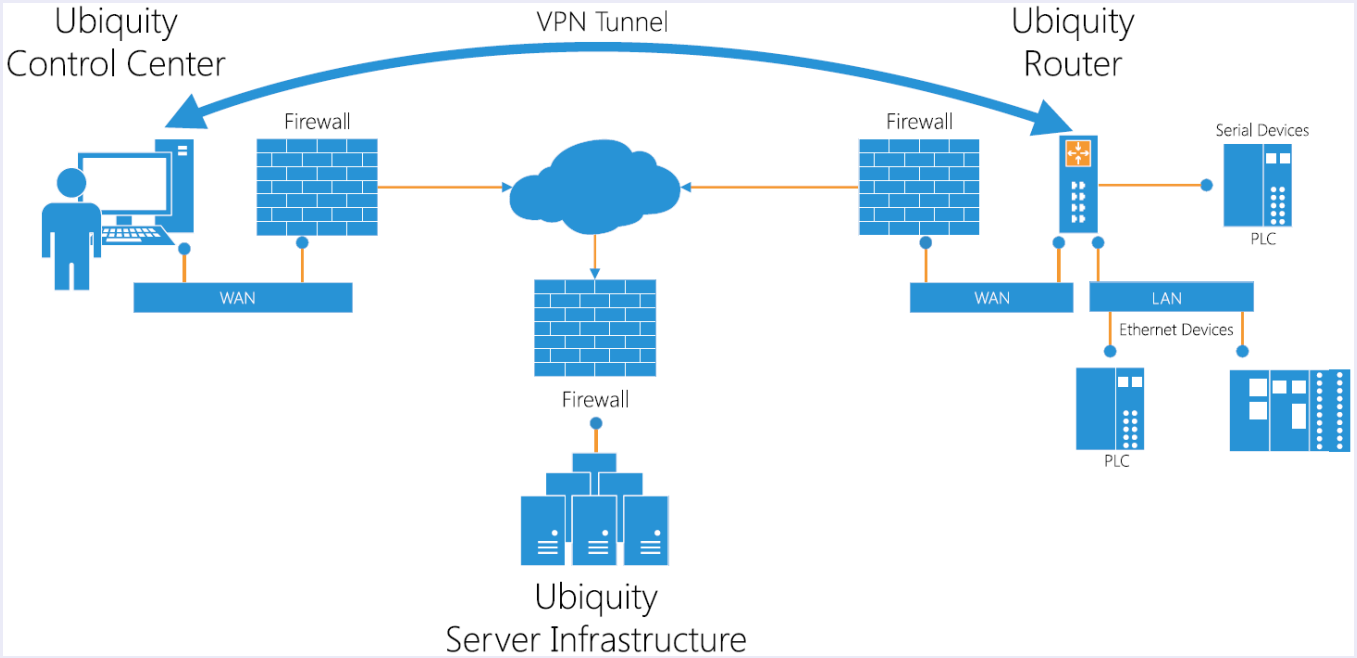
Serwery web





Zdalny dostęp

Zdalny dostęp do urządzeń automatyki



Zdalny dostęp

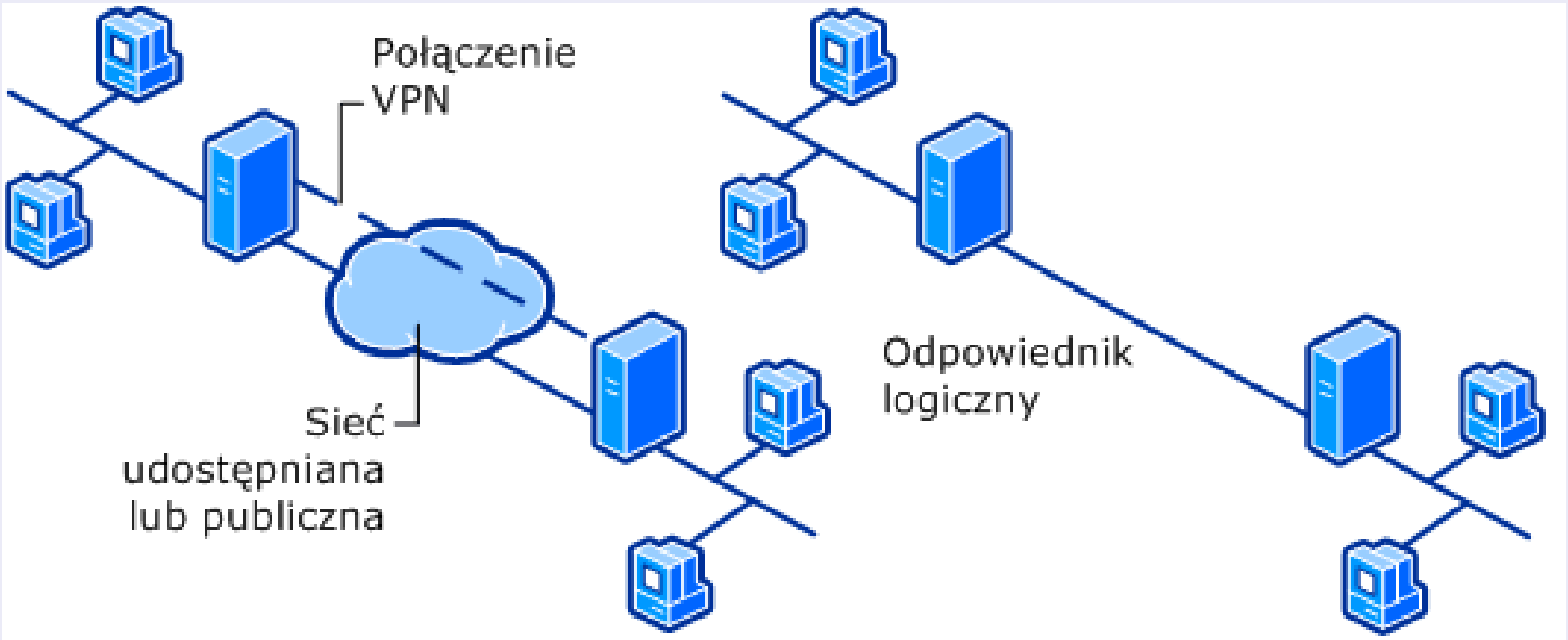
Własności

- Nielimitowane połączenie
- Nieograniczona liczba urządzeń
- Redundantna i rozproszona infrastruktura serwerów
- Zmodyfikowane połączenie VPN do zastosowań przemysłowych
- Najwyższe standardy bezpieczeństwa: szyfrowania i integralności danych
- Grupy użytkowników i zróżnicowany poziom dostępu do urządzeń
- (Logowanie danych historycznych)
- (Alarmowanie poprzez e-mail i SMS)

Ubiquity Router

Zdalny dostęp

VPN – Virtual Private Network



Zdalny dostęp

Właściwości VPN

- Hermetyzacja
  Prywatne dane są hermetyzowane przy użyciu nagłówka, który zawiera informacje o rutingu umożliwiające przesyłanie danych przez sieć publiczną.
- Uwierzytelnianie
  Serwer VPN uwierzytelnia klienta, a także klient uwierzytelnia serwer. Dane mogą zostać opatrzone kryptograficzną sumą kontrolną opartą na kluczu szyfrowania, co umożliwia sprawdzenie czy dane pochodzą od właściwego nadawcy oraz czy nie zostały zmodyfikowane podczas przesyłania
- Szyfrowanie danych
  Obie strony łącza VPN dysponują kluczem szyfrowania, który jest niezbędny do poprawnego odszyfrowania przesyłanych danych

Słowniczek

VPN	Virtual Private Network
VLAN	Virtual Local Area Network-
IP	Internet Protocol
IoT	Internet of Things
ICS	Industrial Control System

Literatura


HMI Mobility
F. Terezinho, InduSoft


Baza Wiedzy TechNet
https://technet.microsoft.com


Automatyka
Biuletyn Informacyjny Firmy SABUR


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