Przegląd protokołów komunikacyjnych automatyki przemysłowej w aspekcie bezpieczeństwa sieci OT

Suchy Las, maj 2017

5 mitów dotyczących bezpieczeństwa infrastruktury krytycznej

wg firmy Kaspersky Lab

- **Mit 1:** Nasze systemy automatyki przemysłowej nie są połączone z internetem, zatem są bezpieczne
- **Mit 2:** Mamy zaporę sieciową, dlatego jesteśmy zabezpieczeni przed zagrożeniami z zewnątrz
- **Mit 3:** Hakerzy nie rozumieją systemów przemysłowych SCADA/DCS/PLC
- **Mit 4:** Nasz obiekt nie stanowi celu
- **Mit 5:** Nasz system bezpieczeństwa zabezpieczy nas przed atakami

Zagrożenia

Źródła zagrożeń:

- Zagrożenia zewnętrzne
- Zagrożenia wewnętrzne

Rodzaje zagrożeń:

- Poufność - wyciek informacji
- Bezpieczeństwo - zakłócanie pracy (DoS)
- Bezpieczeństwo - przekłamanie informacji
- Bezpieczeństwo - przejęcie kontroli

Przyczyny podatności na zagrożenia

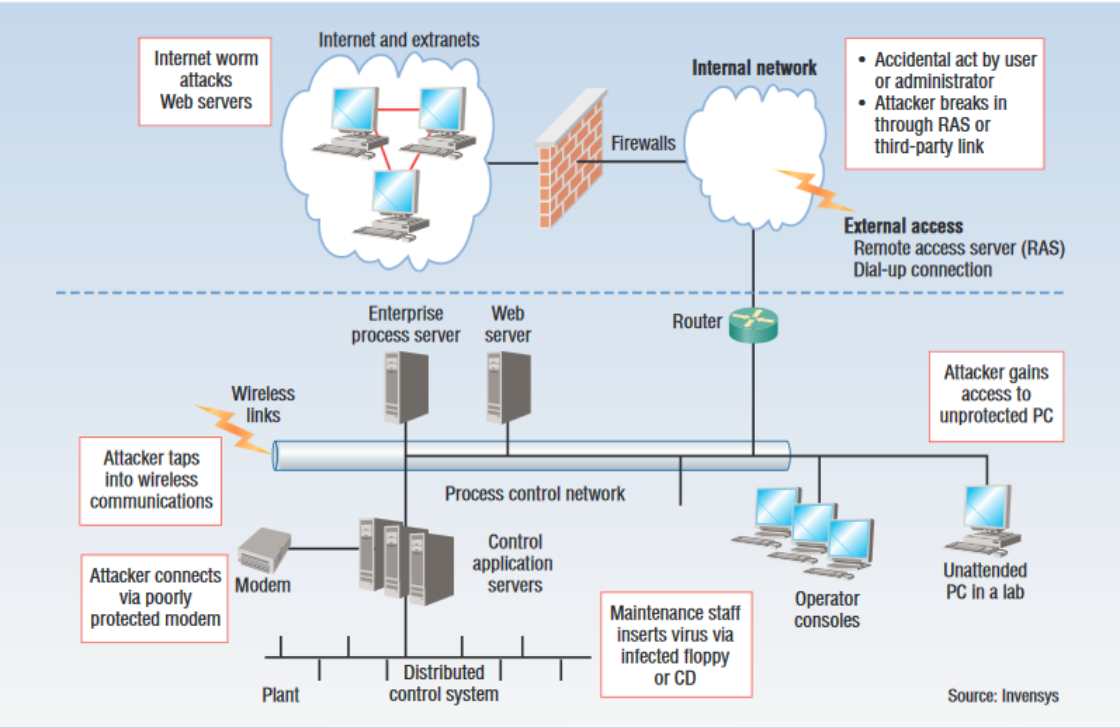
Organizacyjne:

- ❑ Brak polityki bezpieczeństwa, brak procedur
- ❑ Brak odpowiedniej administracji i nadzoru

Techniczne:

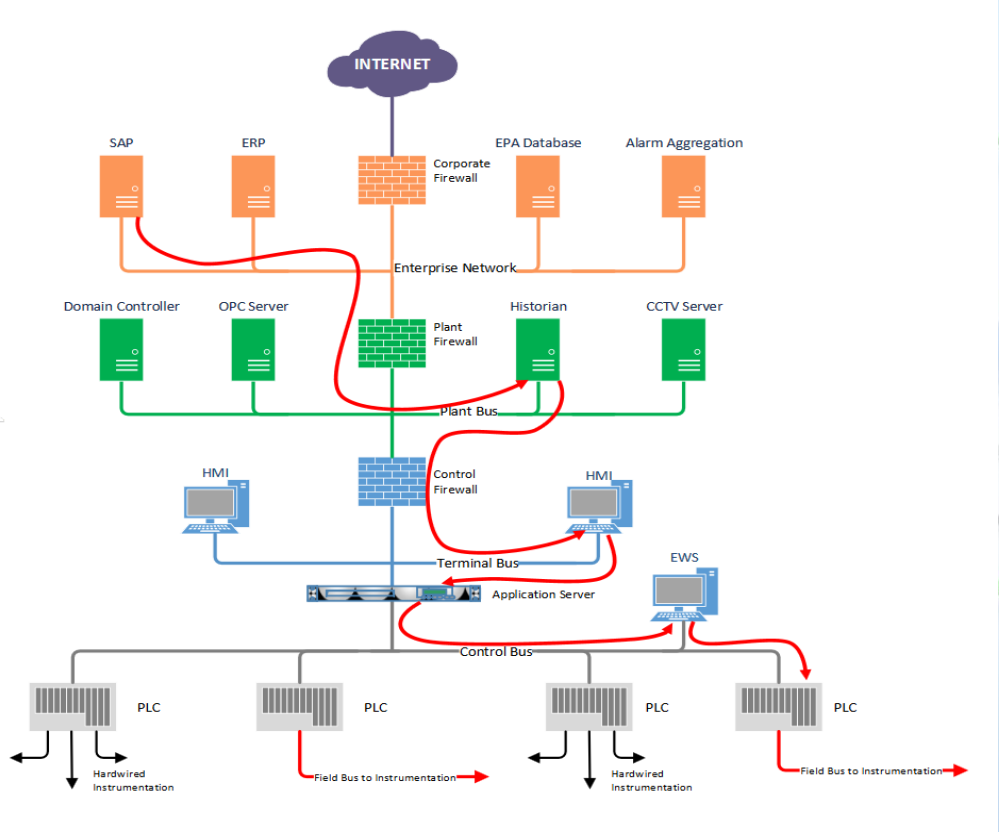
- ❑ Błędna architektura sieci
- ❑ Brak zabezpieczeń zdalnego dostępu
- ❑ Brak zabezpieczeń w sieciach bezprzewodowych
- ❑ Wspólna infrastruktura IT i OT
- ❑ Brak narzędzi do wykrywania zagrożeń
- ❑ Brak zabezpieczeń w sieciach OT

Miejsca potencjalnych ataków



- **Sterowniki PLC**
- **Łącza do sterowników PLC**
- Stacje inżynierskie
- Stacje HMI
- Serwery SCADA
- Inne serwery i stacje robocze
- Zdalny dostęp
- Internet

Miejsca potencjalnych ataków



Cimation
Innovation Beyond Automation

Out of Control:
Demonstrating SCADA Exploitation

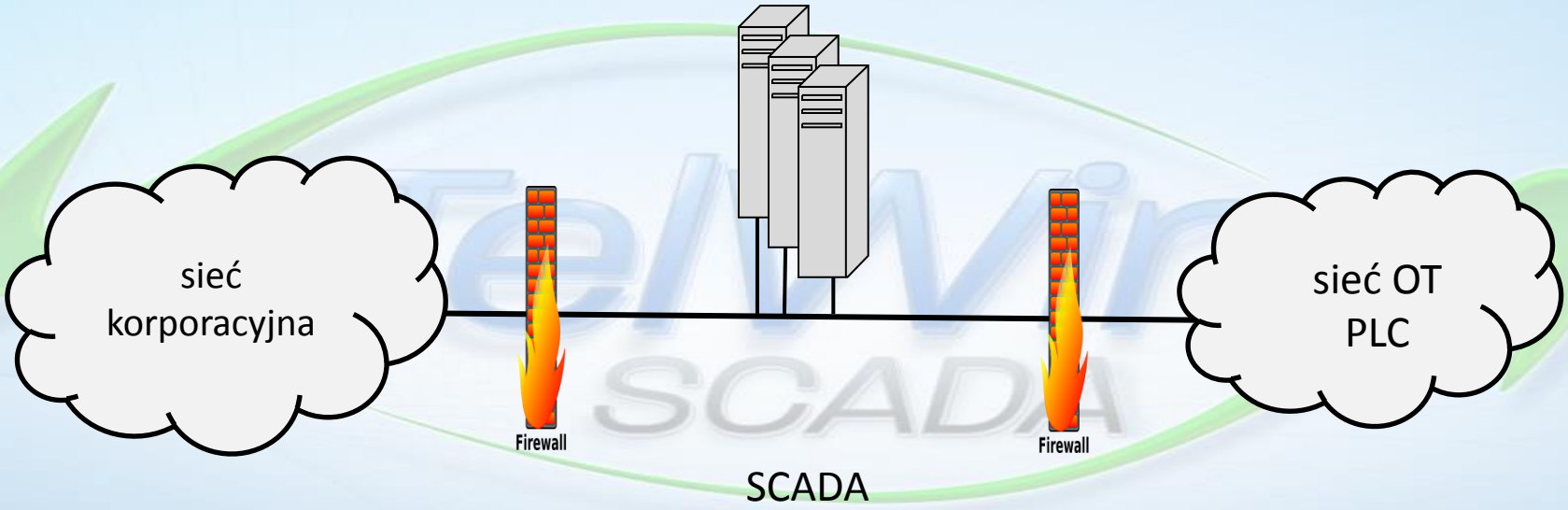
Brian Meixell
Eric Forner

Black Hat 2013

Metody ochrony

- ✓ Izolacja/Separacja/Partycjonowanie
- ✓ Autentykacja
- ✓ Autoryzacja
- ✓ Szyfrowanie
- ✓ Ograniczenie dostępu
- ✓ Przydzielanie minimalnych uprawnień
- ✓ Nadzór
- ✓ Aktualizacje
- ✓ Redundancja, weryfikacja
- ✓ Zabezpieczenia fizyczne
- ✓ Honeynet

DMZ, firewall



Normy

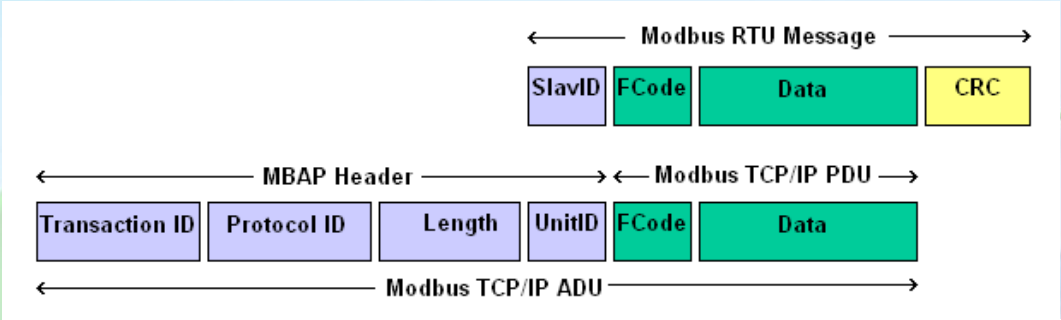
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
  (National Institute of Standards and Technology)
- NIST CSF Framework for Improving Critical Infrastructure Cybersecurity
- NERC CIP - North American Electric Reliability Corporation – Critical Infrastructure Protection
  (North American Electric Reliability Corporation)
- IEC 62351 Security Standards for the Power System Information Infrastructure
  (International Electrotechnical Commission)

Popularne protokoły

- Brak szyfrowania (by design)
- Ograniczenia sprzętowe
- Transmisja sieciowa – najczęściej enkapsulacja protokołów szeregowych

  - Modbus RTU /Modbus TCP
  - GazModem/GazModem2/GazModem3
  - S-Bus
  - Ethernet/IP
  - Profibus / ProfiNet
  - ControlNet/DeviceNet

Enkapsulacja – ModBus TCP



www.simplymodbus.ca

Fields	Length	Description -	Client	Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request / Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (request)	Initialized by the server (Response)
Unit Identifier	1 Byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received request

www.modbus.org

ICCP 2009
(International Conference on Critical Infrastructure Protection)

Design and Implementation of a Secure Modbus Protocol

Igor Nai Fovino, Andrea Carcano, MarceloMasera and Alberto Trombetta

- Integrity
- Authentication
- Non-Repuditation
- Replay protection

- RSA
- SHA2

Protokoły w branży energetycznej

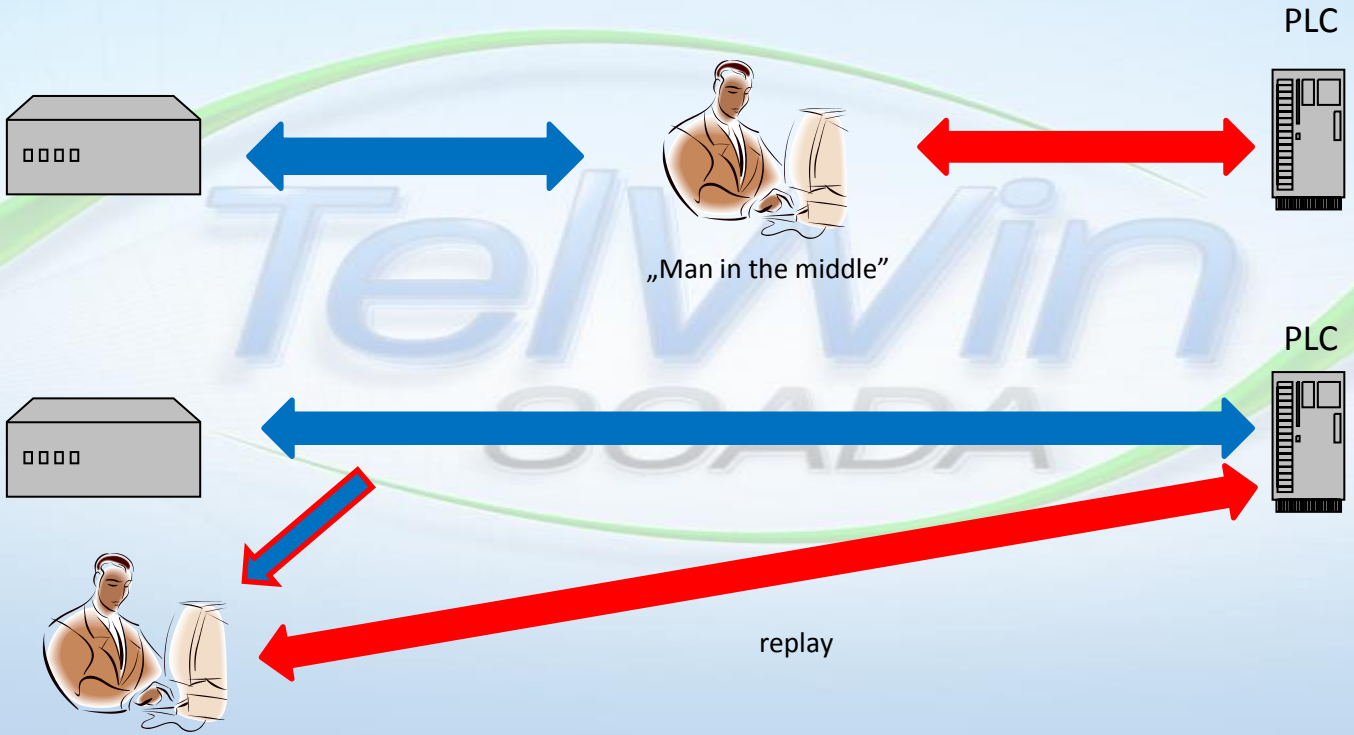
- **IEC 80870-5**
- **IEC 80870-6 – TASE.2/ICCP**
- **IEC 61850**
- **IEC 61968 (CIM)**
- **IEC 61334 (DLMS)**
- **IEC 62056**

IEC 62351:

TCP: TLS (Transport Layer Security)

Serial: autentykacja, VPN

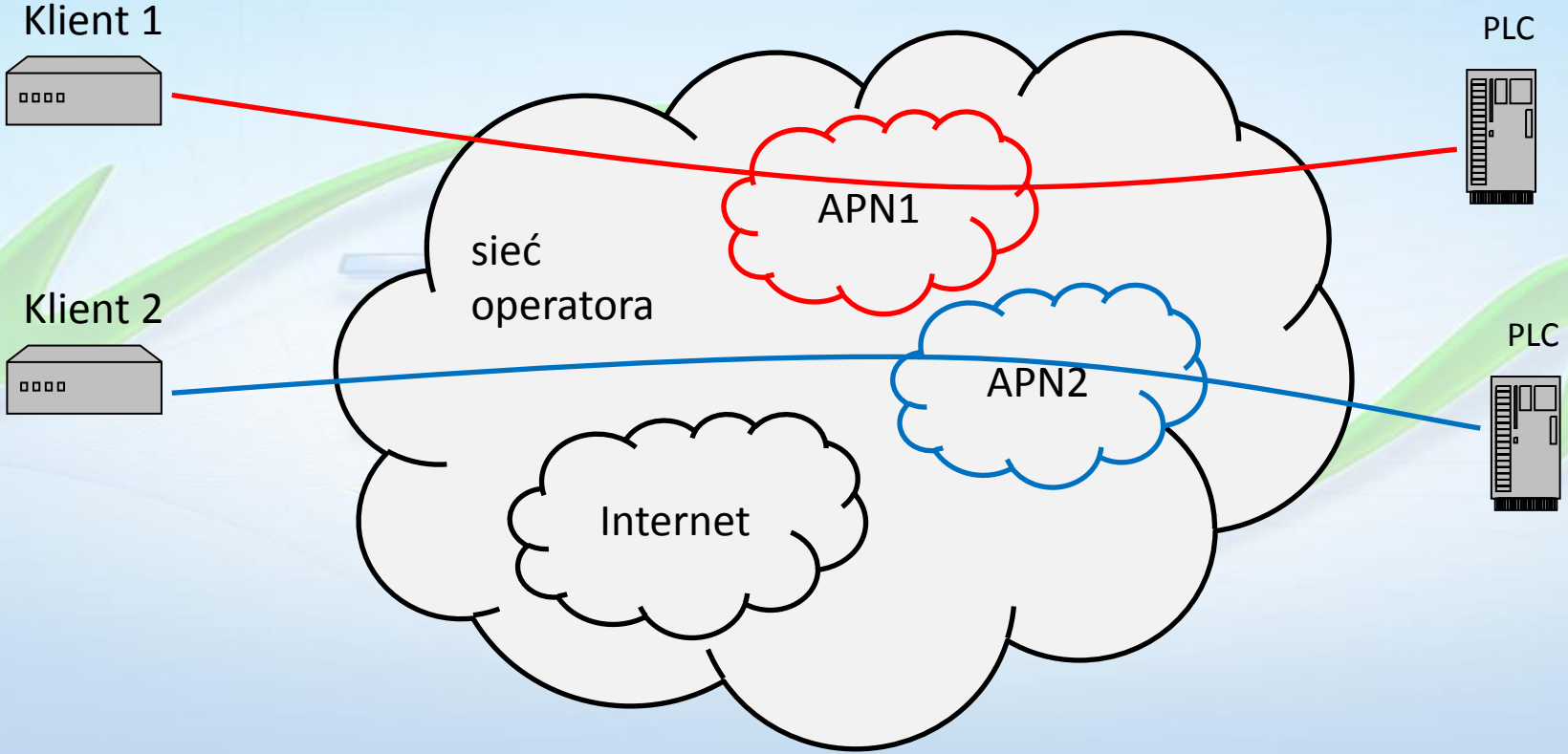
Metody ataków



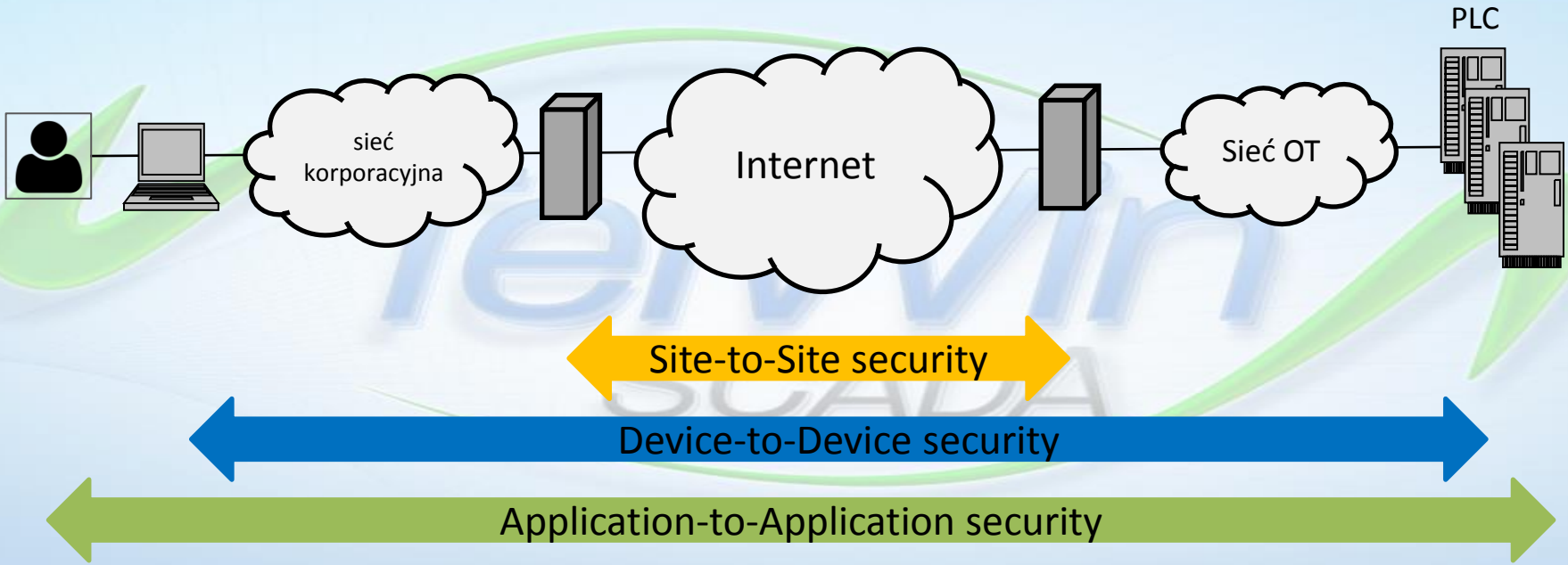
Metody ochrony w istniejącej infrastrukturze

- Ochrona sterowników
  - fizyczna
  - zdalny dostęp
- Ochrona łączy PLC
  - fizyczna
  - kontrola dostępu (IP)
  - APN
  - hasła, hash, certyfikaty, podpisy cyfrowe
  - szyfrowanie
    (zarządzanie kluczami)

APN



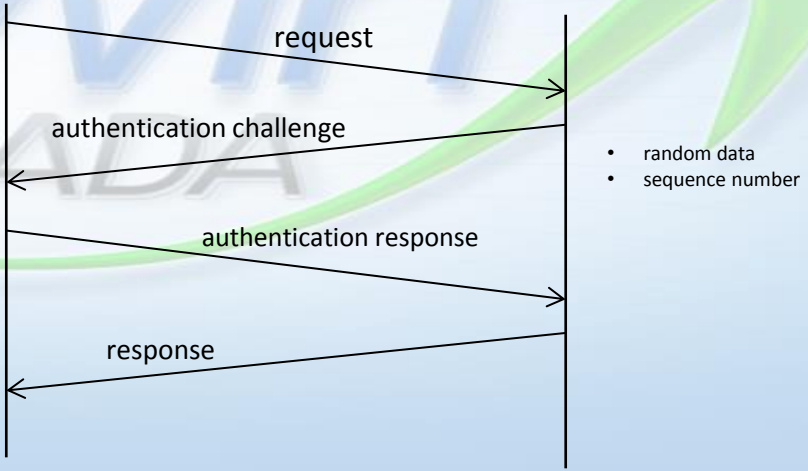
Ochrona kanałów komunikacyjnych



- Bump-in-the-wire (external devices)
- Bump-in-the-stack (integral to the protocol)

Uwierzytelnianie

- użytkownik/hasło
- Hash, challenge-response
- podpisy cyfrowe



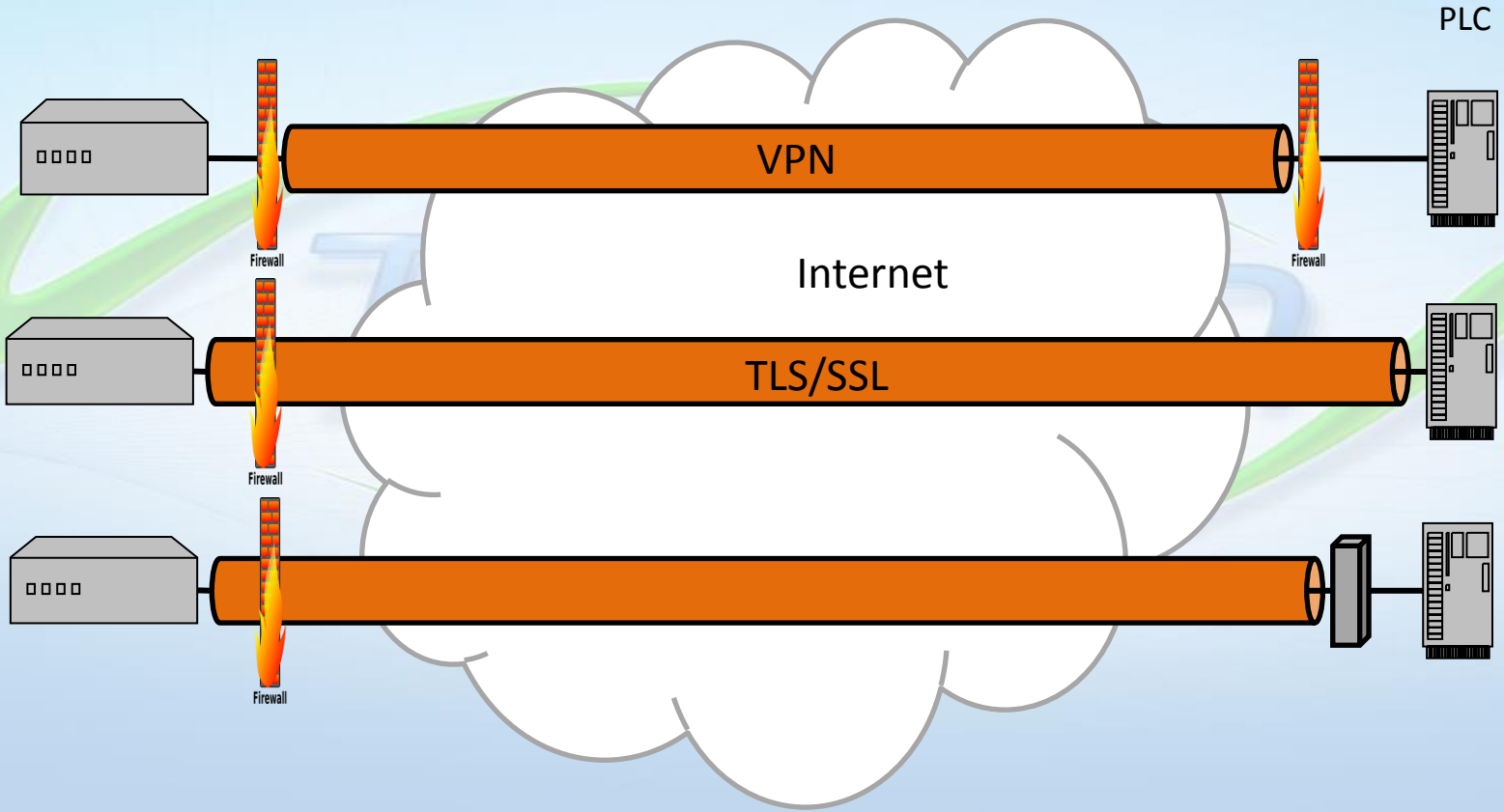
VPN, TLS/SSL

Wikipedia:

TLS (ang. Transport Layer Security) – przyjęte jako standard w Internecie rozwinięcie protokołu SSL (ang. Secure Socket Layer), zaprojektowanego pierwotnie przez Netscape Communications. TLS zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509.

VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

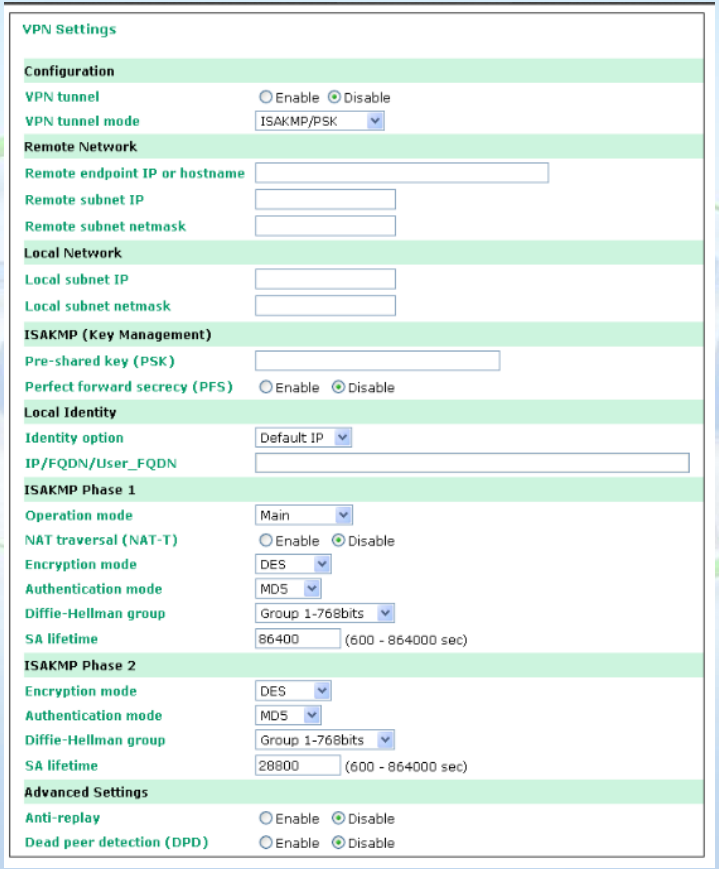
Tunelowanie/szyfrowanie



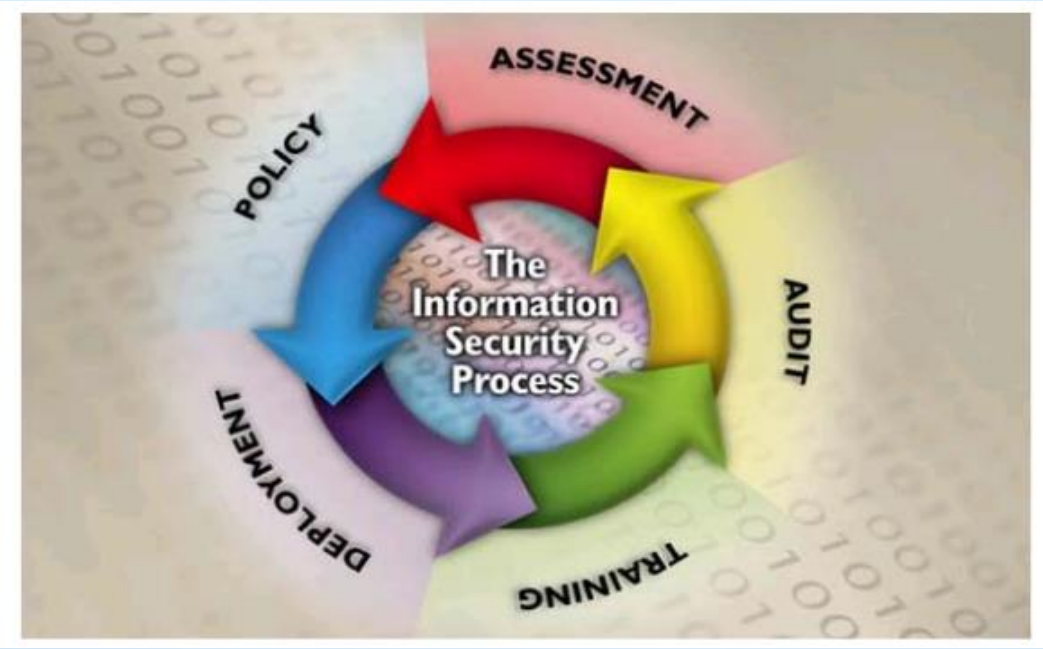
Przykłady urządzeń

- Moxa OnCell G3110/G3150 – IPSec
- Advantech EKI-1321 – OpenVPN
- Siemens SCALANCE M (IPSec, OpenVPN, firewall)
- Allen-Bradley 1756-EN2T - IPSec
- …

Moxa OnCell – konfiguracja VPN



Podsumowanie



IEC 62351 Security Standards for the Power System Information Infrastructure
Frances Cleveland