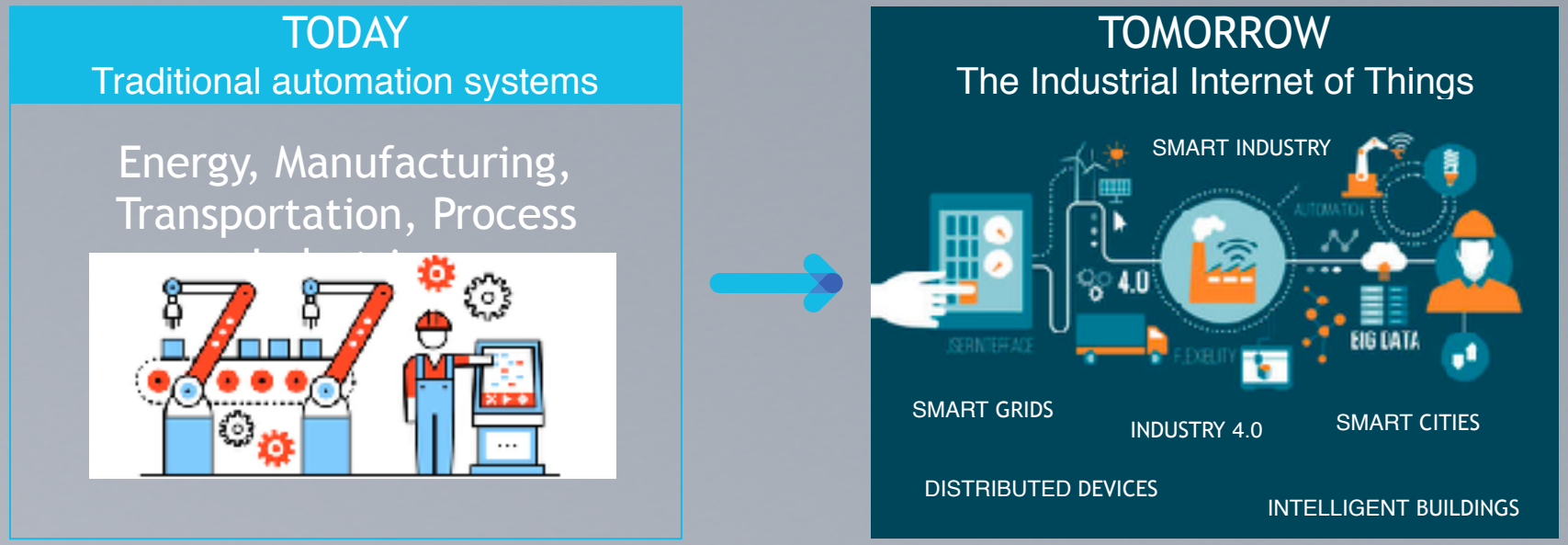

TTC

TTCMARCONI



Segmentace a bezpečnost technologických sítí

Vojtěch Richter

5.10 2021

Historie OT & IT sítí

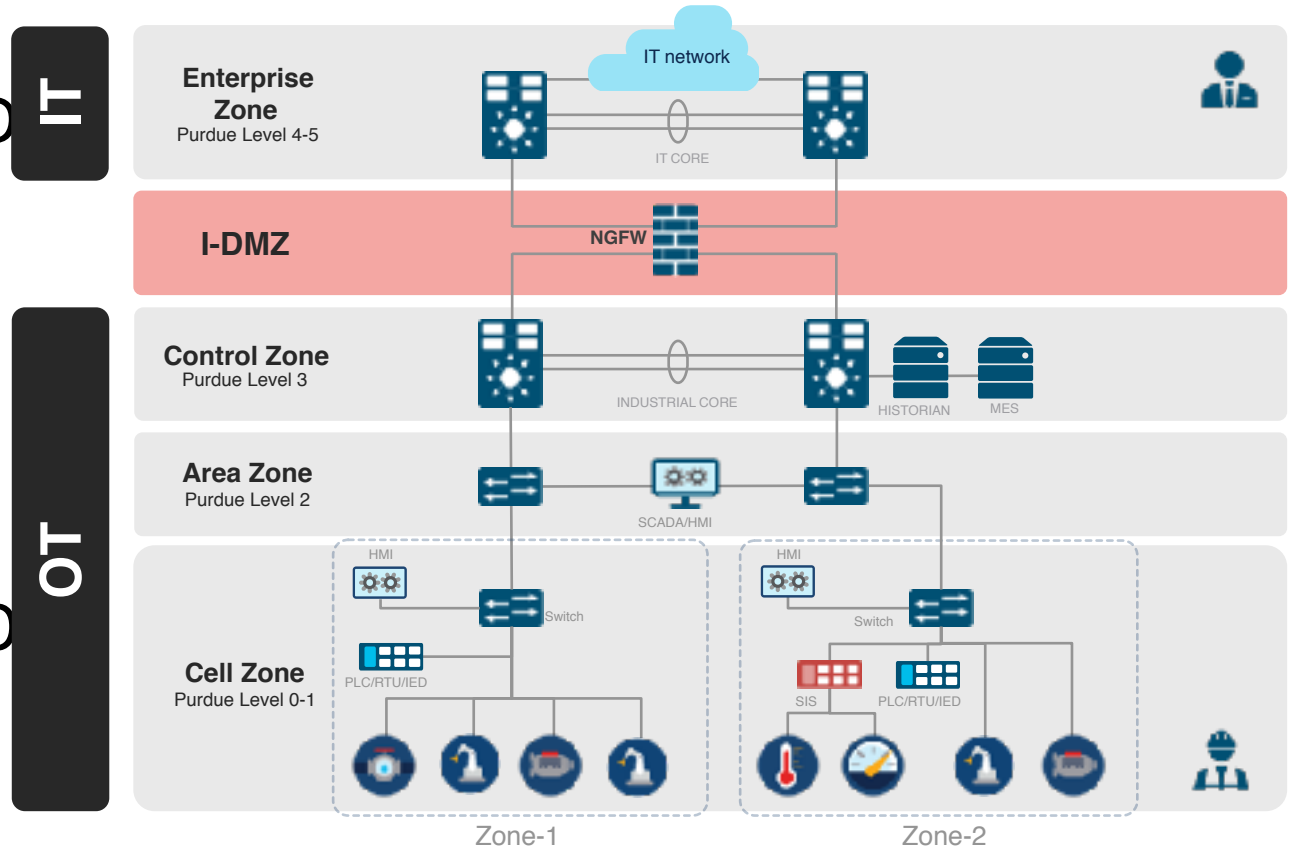
Historicky IT a OT sítě provozovány a ovládány separovaně

- Bezpečnost (preference IT) x Funkčnost (preference OT)
- Ethernet & IP protokoly -> konsolidace IT a OT sítí
  - Snížení provozních/pořizovacích nák
  - Sdílená technologie
  - IT, OT sítě propojeny v centrálních u
  - Logická x fyzická topologie sítí
  - Vrstvená bezpečnost

Vrstvená bezpečnost OT sítí

Neexistuje jediný nástroj, který by nám zabezpečil celou technologickou síť

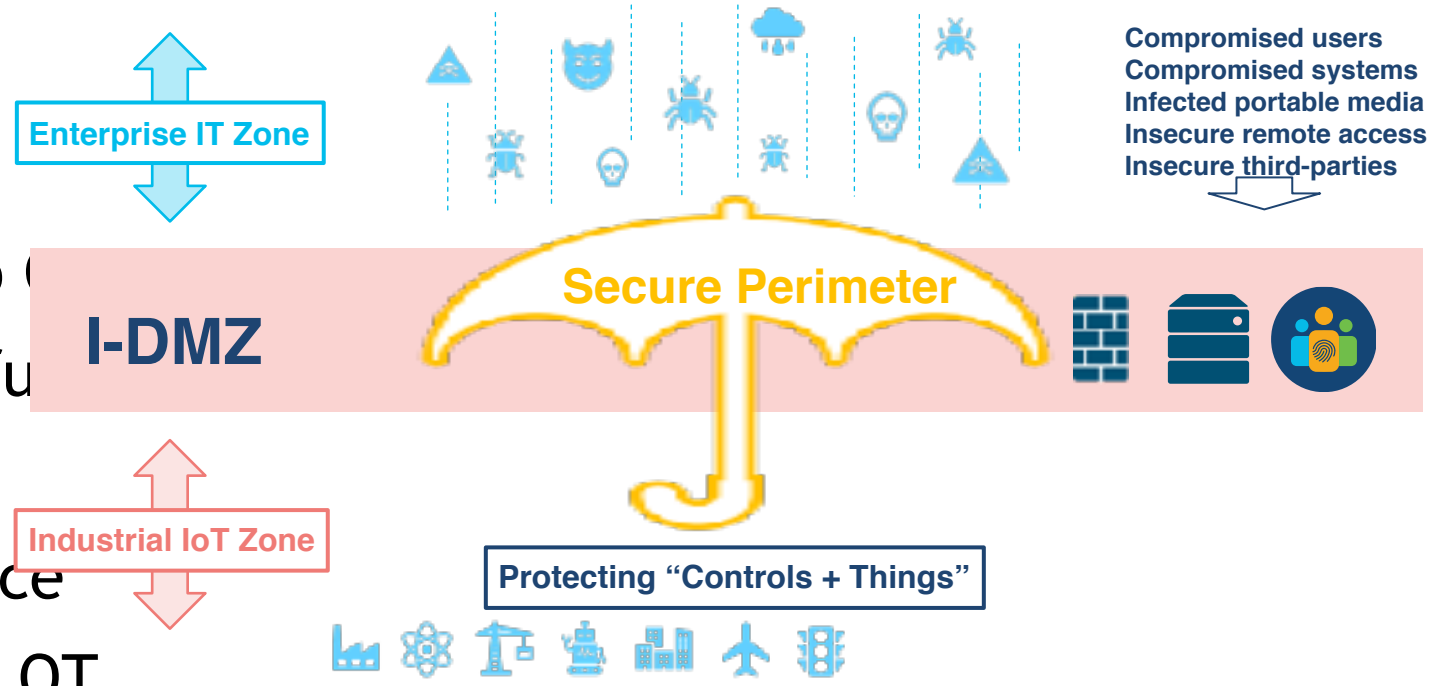
- Rozdělení bezpečnosti do vrstev:
  - Zabezpečení perimetru IT x OT - D
  - Administrativní přístup skrz DMZ
  - Segmentace do OT zón
  - Kontrola přístupu do sítě
  - Bezpečnost na úrovni OT zařízení
  - Monitoring & reakce na hrozby v O



Zabezpečení perimetru mezi OT a IT sítí

OT & IT sdílí některé centralizované systémy, které oba světy využívají

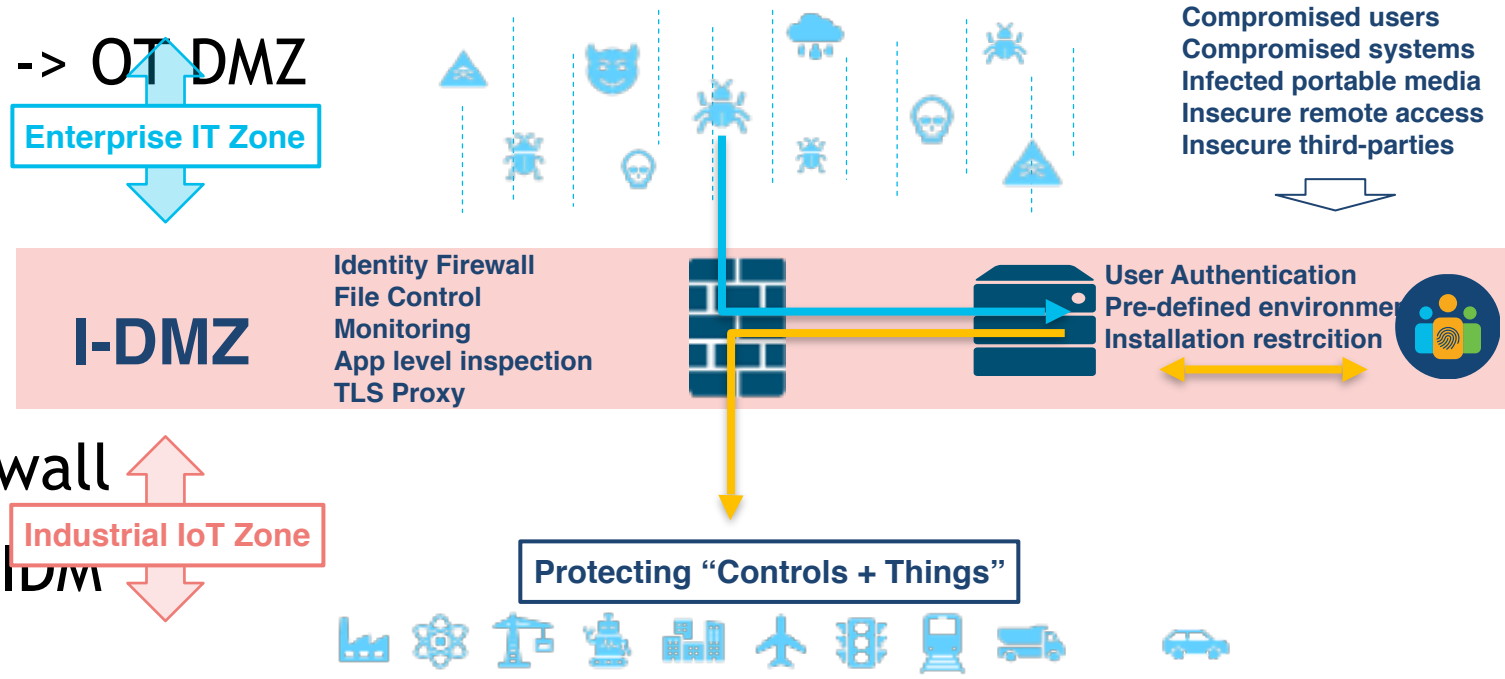
- Hrozby -> nežádoucí komunikace, šíření hrozeb z IT do OT, nepřehlednost protnutí sítí
- Vytvoření OT DMZ:
  - OT NGFW Firewall
  - Samostatné instance APP pro (
  - Proxy funkce centrálních IT fu
  - INET Proxy, filtrace obsahu
  - Filtrace nežádoucí komunikace
  - Bezpečný perimetr mezi IT a OT



Administrativní přístup skrz DMZ

Přístup do OT systému z koncových stanic musí uživatelů zakázán -> pouze zabezpečeně

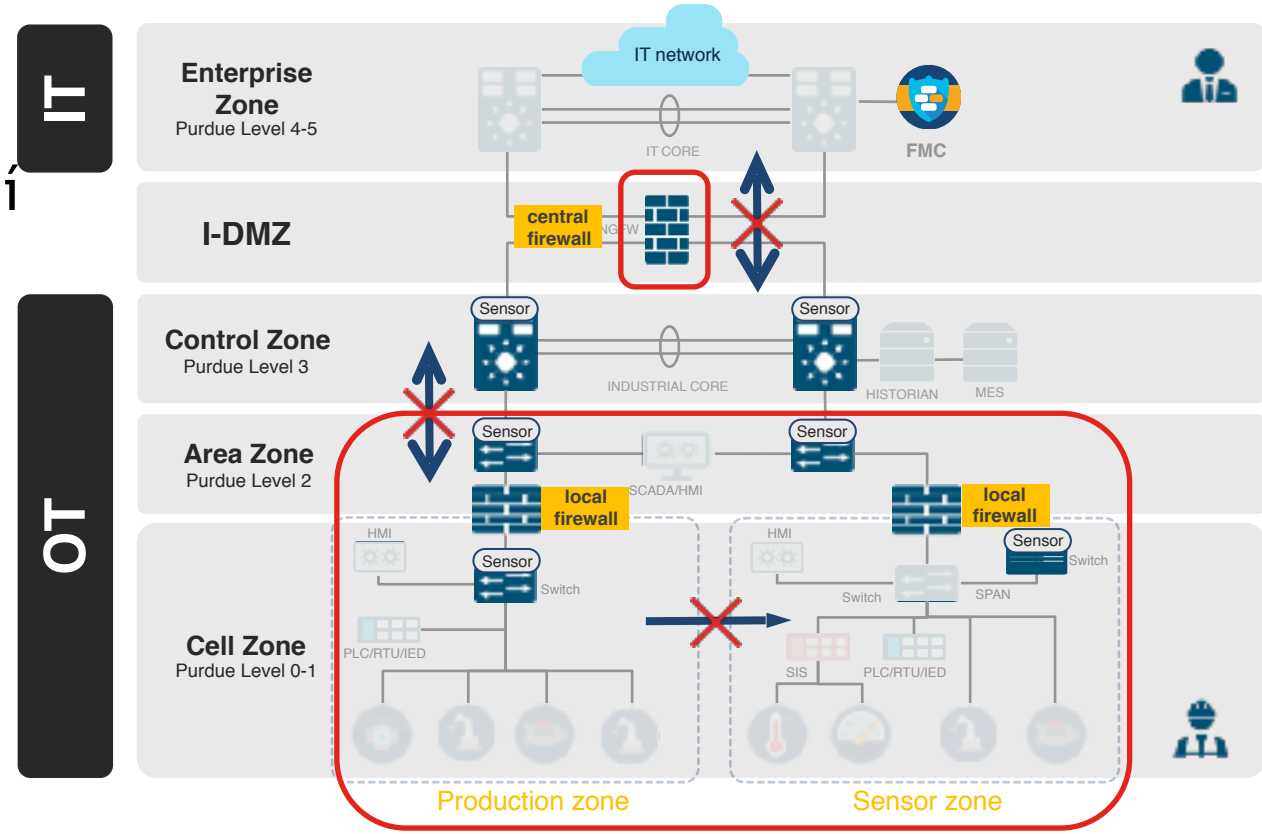
- Hrozby -> šíření škodlivého kódu, neoprávněný a neomezený přístup
- Správci OT sítě musí provádět upgrade, monitoring, diagnostiku a další:
  - Uživatelské VPN do IT DMZ -> OT DMZ
  - Hop servery v DMZ
  - Omezení instalace aplikací
  - Autentizace uživatelů
  - Komunikace - Identity Firewall
  - Technologické dedikované IDM



Segmentace technologické sítě

Technologické systémy komunikují stylem M2M, M2S -> není třeba všichni se všemi

- Hrozby -> nežádoucí komunikace mezi OT zařízeními, rozšíření hrozby mezi zařízeními
- Technologické systémy segmentujeme:
  - Na základě komunikace, skupin zařízení
  - Znalost komunikace tech. zařízení
  - VRF, VLAN, Fyzická segmentace
  - Inter-zone komunikace NGFW
  - App inspekce a kontrola komunikace
  - Snížení rizika rozšíření mezi zónami
  - Centralizovaný vs lokální firewall



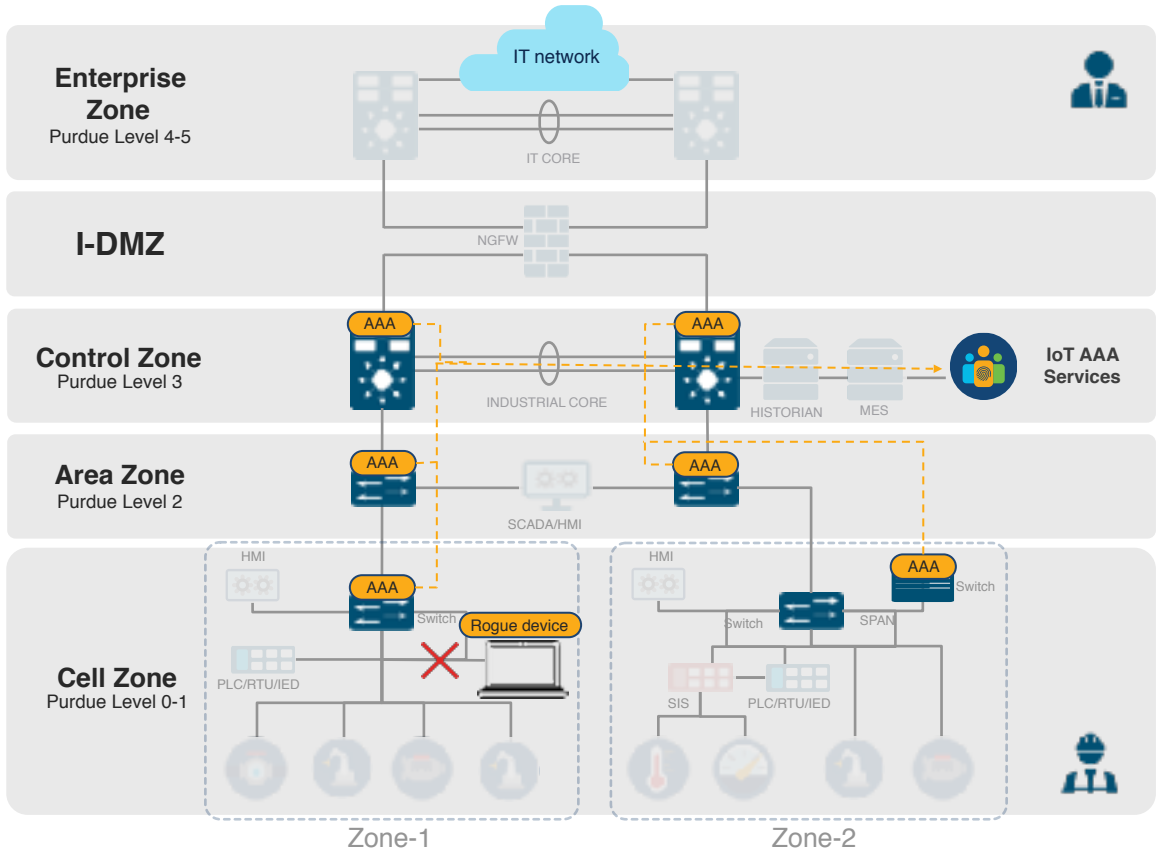
Kontrola na přístupových bodech OT sítě

V OT si nesmíme dovolit možnost aby se mohlo libovolné zařízení připojit

- Hrozby -> Neautorizovaný přístup do sítě, „man-in-the-midle“ útoky
- Na přístupových zařízeních aplikovat:
  - Fyzickou bezpečnost
  - Přístupové zařízení ověřují zařízení
  - MAB/802.1 (EAP-TLS) autentizace
  - Profilování zařízení a probing
  - RADIUS a EAP protokol pro AAA funkce
  - Jednotné politiky pro OT zařízení
  - Dedikovaná PKI infrastruktura pro OT

IT

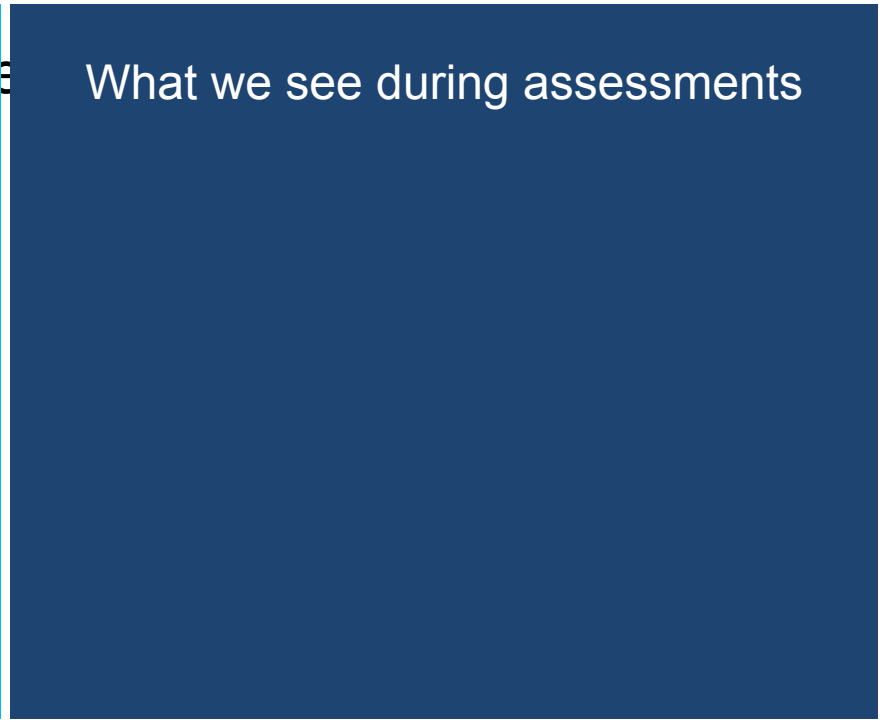
OT



Zabezpečení na úrovni technologického zařízení

Do OT dodáváme pouze bezpečné zařízení -> častá chyba -> starší zařízení čistá funkce

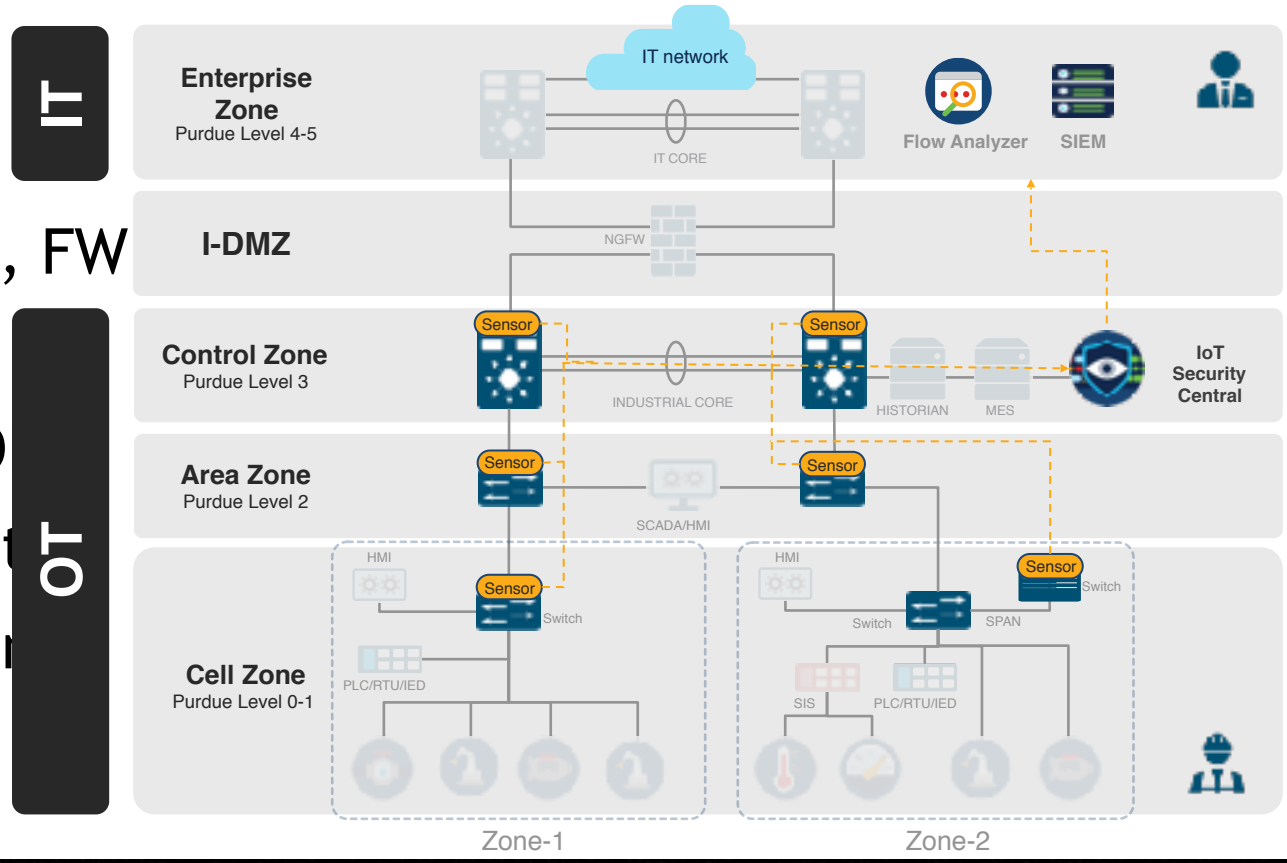
- Hrozby -> Napadení koncového systému, využití zařízení k šíření škodlivého kódu/ DoS
- na OT zařízení aplikovat
  - Patchování software
  - OS Firewall a RBAC
  - Šifrování komunikace
  - Vypnutí nepotřebných služeb a funkcí
  - Monitorování aktivit



Monitoring a vyhodnocování hrozeb v OT síti

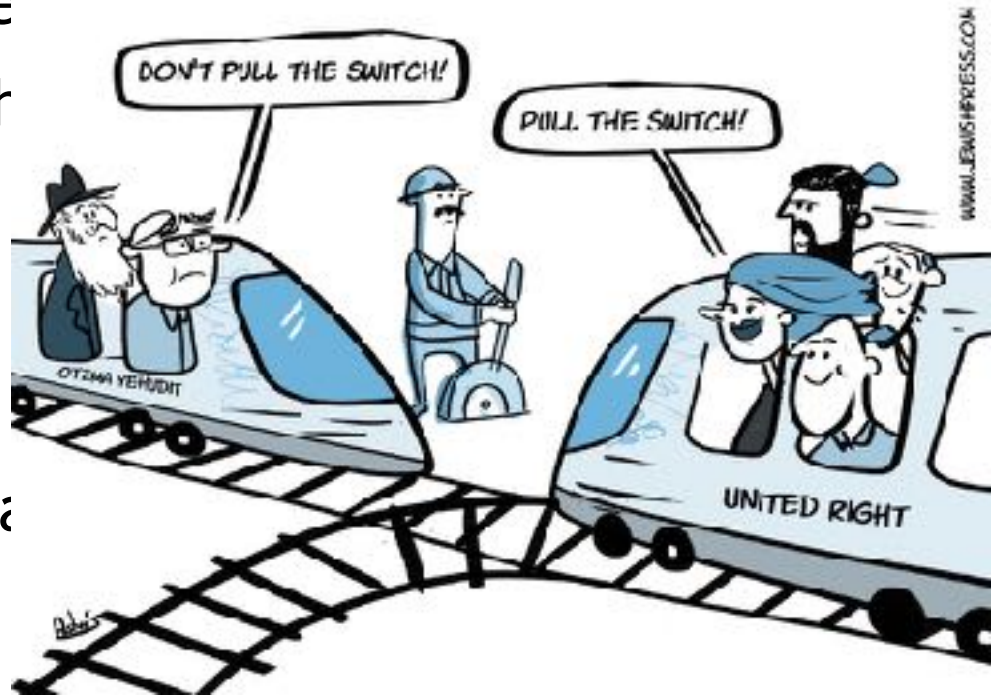
Základem každé sítě je monitorování událostí/komunikací a vyhodnocování rizik

- Hrozby -> Neošetřená/neznámá komunikace, díry v návrhu OT bezpečnosti
- Nasazení monitorovacích funkcí:
  - Sledování/odchytávání komunikací úrovni sítě -> Sondy, Netflow, SPAN, FW
  - Dohlížení koncových zařízení a síťových prvků(SNMP, NET/REST-CO
  - K analýze a vyhodnocování využívat specializované OT nástroje zaměře na OT sítě a protokoly



Co si odnést

- IT i OT sítě se vyvíjí a jsou provozovány konsolidovaně, nemusí to být nutně chyba
- IT i OT sdílí bezpečnostní rizika, ale v OT klademe důraz na provoz a funkci
- Neexistuje jeden jediný nástroj pro zabe[illegible]
- Sítě zabezpečujeme na několika vrstvách pomocí desítek nástrojů a protokolů
- OT síť je bezpečná tak jak zabezpečíme nejslabší článek
- Zabezpečení OT sítě neustále monitorova[illegible] reagovat na nové bezpečnostní hrozby



Děkujeme za pozornost

Vojtěch Richter

TTC MARCONI

E-mail: richter@ttc.cz
www.ttc.cz