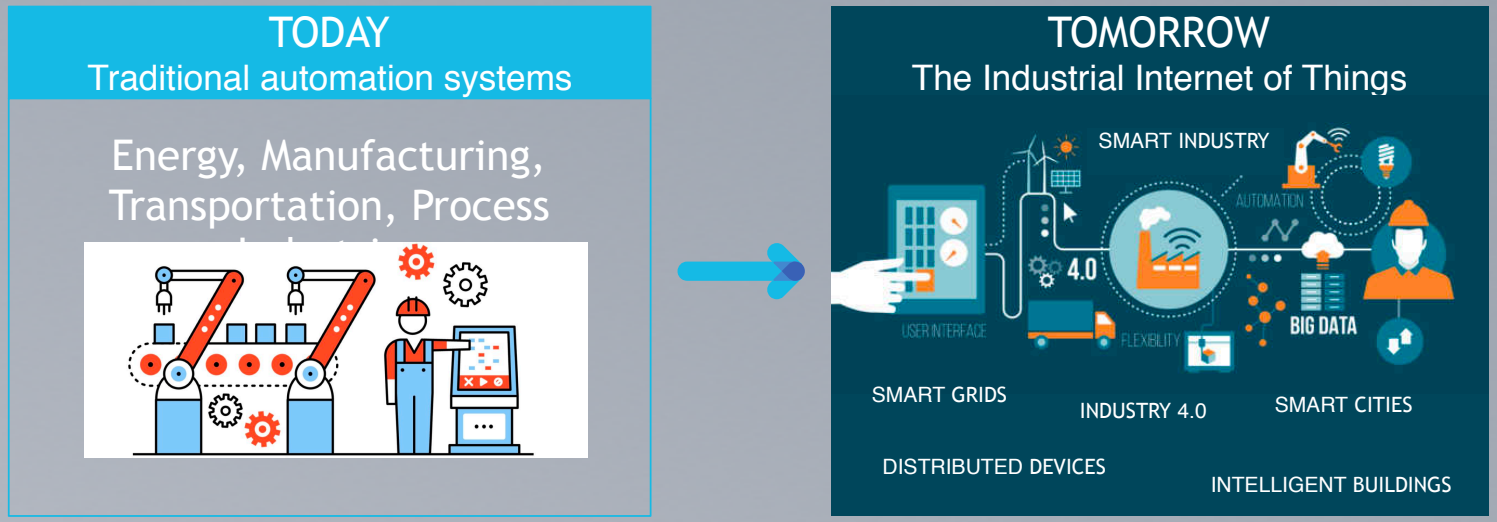

TTC

TTCMARCONI



IoT řešení & bezpečnost pro železnici

Vojtěch Richter

9.11 2023

TTCMARCONI

Architektura IoT sítě pro železnice

Železniční doprava

IoT Architektura železniční sítě

FRMCS a nové požadavky na síť

FRMCS síťová architektura a doporučení

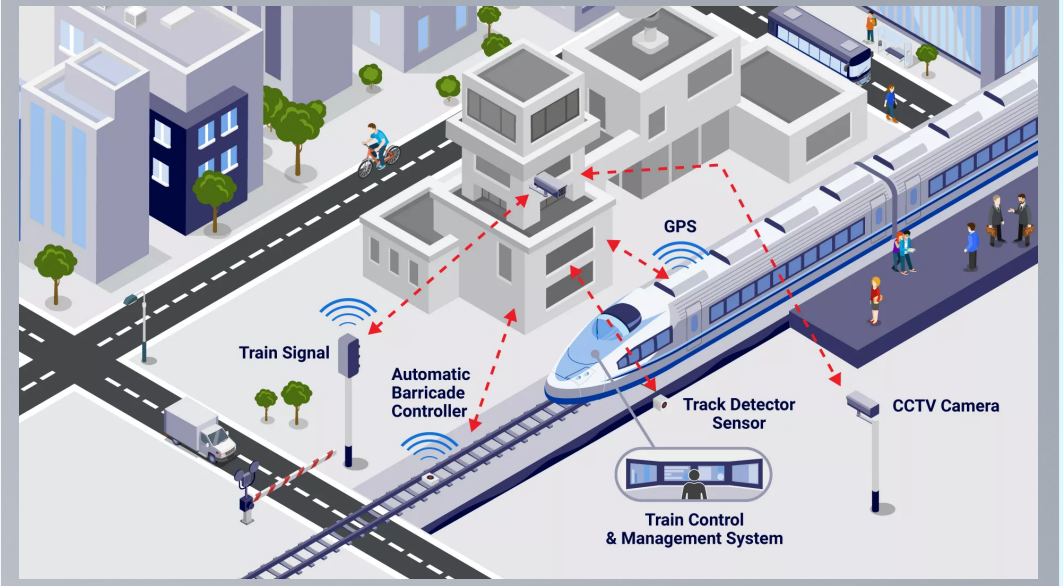
Bezpečnost technologických sítí

Administrativní přístup & Industriální DMZ

Technologická identita & kontrola přístupu do sítě

TTCMARCONI

Železniční doprava



Nároky na železniční dopravu:

Efektivní řízení vytížení tratí (Efektivita)

Udržování minimální vzdálenosti mezi soupravami (využití tratě)

Řízení spotřeby energie (prostoje ve stanicích / na trati)

Vysoká dostupnost & Supervize (Spolehlivost)

Redundance na úrovni ovládání a sítě (automatizované zálohy)

Kontrola & regulace rychlosti vlaku (bezpečná vzdálenost zastavení, Záchranné brždění, dodržování lokálních omezení & řídících signálů)

Analýza dat jedoucí soupravy (pozice, rychlost, brždění/akcelerace)

Zvýšení kvality služeb cestujícím (User Experience)

Palubní informační systémy - poloha, jízdní řády a informační tabule

Prediktivní údržba, minimalizace výjezdů specializovaných techniků

On-boarding cestujících - přístup na internet, interaktivní systémy

Bezpečnost & standardy (Safety & Compliance)

Železnice jsou součástí kritické infrastruktury

Tlak na plnění bezpečnostních pravidel, standardů a předpisů

Zajištění bezpečnosti pro pracovníky, cestující i veřejnost

Zvýšení bezpečnosti cestujících ve vlaku/stanicích - kamerový systém

IoT Architektura železniční sítě

Architektura železniční sítě:

Sběr dat a jejich vizualizace, komunikace, zabezpečení

Stanice/Depa - CCTV, Voice, INISS, Měření & el. ochrana

Trať - zabezpečovací zařízení (ZZ), diagnostika, ETCS

Centrální dispečink - GTN - ISOŘ/DEVIS/CDS/GVD, Voice

LAN / Track -> připojení tech zařízení (Ethernet/GSM-R)

DC / Regionální-DMZ -> služby/aplikace pro OT zařízení

Přenosová síť -> MPLS přenos mezi tech-sítěmi, DC & IT

Segmentace & Bezpečnost -> oddělení, filtrace & kontrola

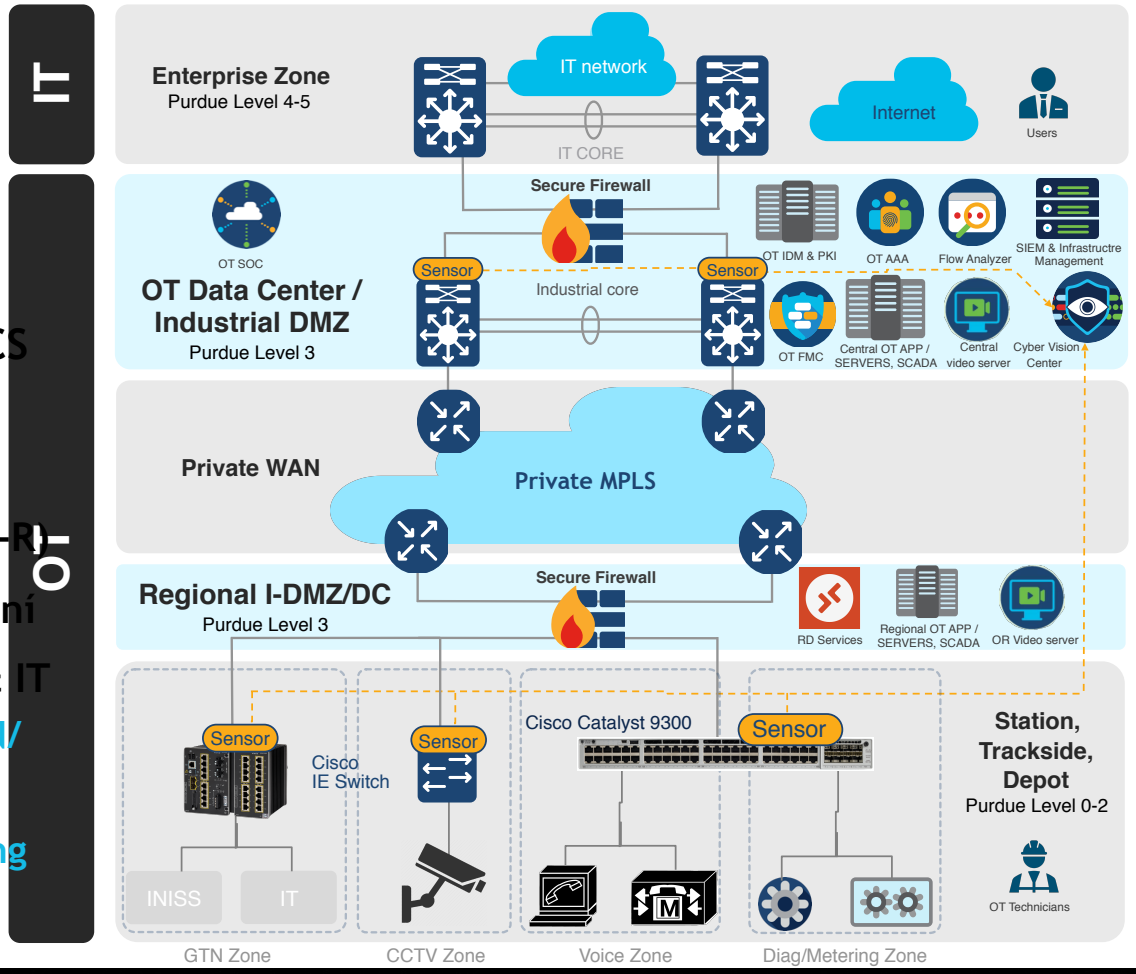
Nové požadavky na technologickou síť:

Nové technologie - FMRCS (Mission critical services, 5G RAN/EPC)

Služby pro nové technologie - QoS, Multi-pathing, Monitoring

Vysoká dostupnost -> Redundance/FRR/Fast-Convergence, více BW

Bezpečnost -> důkaz naplnění NERC/CIP standardů v OT síti



Nové požadavky na transportní síť - FRMCS

ERTMS (European Railway Traffic Management System)

GSM-R (comm/voice), ETCS (protection/signalling – ATO)

PDH GSM-R síť dosluhuje (konec podpory 2030-2035)

Sítě konvergují k IP -> FRMCS soubor standardů/ doporučení

přenos (primárně 5G & Packet core), komunikace (MCX) …

FRMCS je interoperabilní se stávajícími systémy - ETCS

FRMCS podporuje přenos přes GSM-R (koexistence)

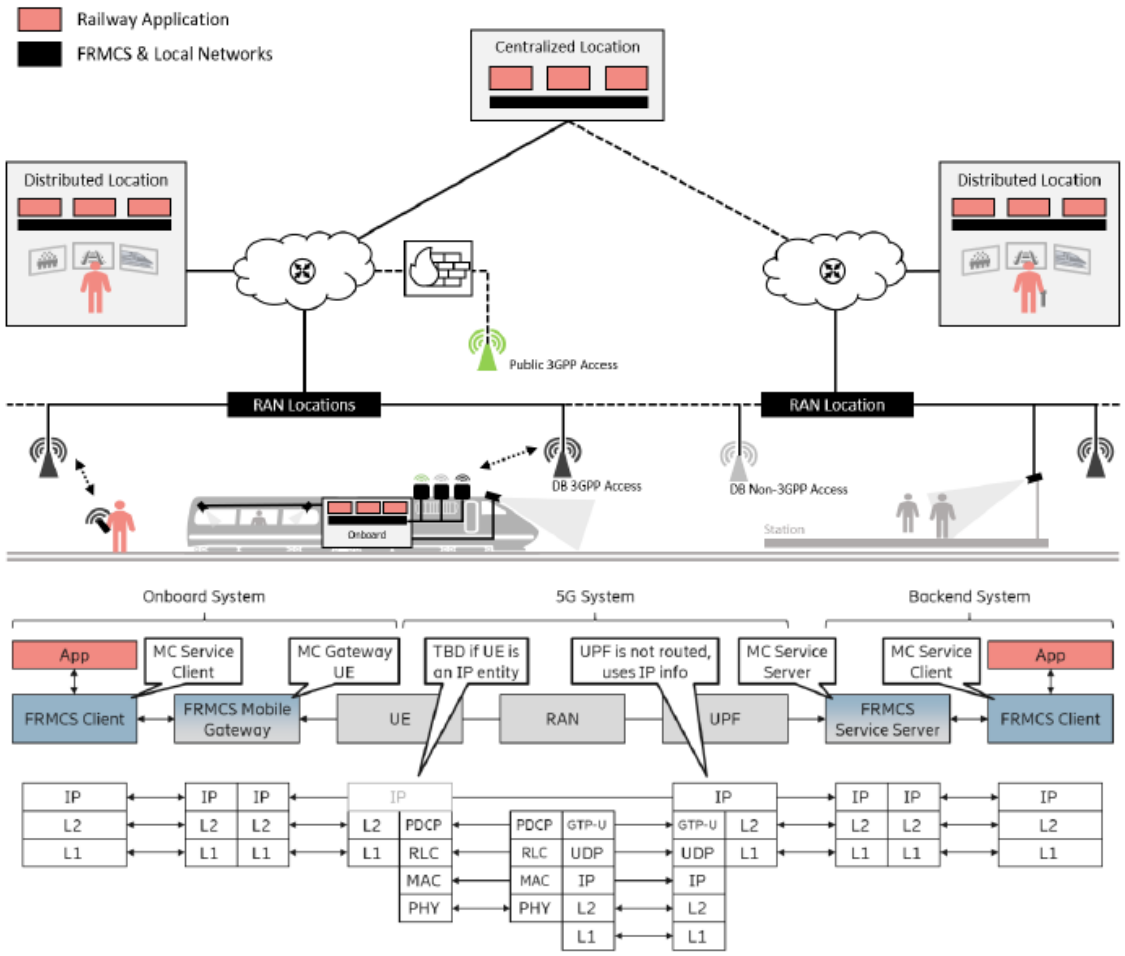
Důležité části FRMCS sítě:

OBN (On Board Network) – ethernetová síť uvnitř vlakové soupravy

Bezdrátový přenos (OBN -> Trackside RAN -> Backbone) - any IP transport - primárně 5G, další IP technologie – Wifi, Eth over Radio

DN Backbone – páteřní síť komunikace do Distribuovaných DC / DC

Bezpečnost - zajistit zabezpečení na úrovni celé komunikační cesty (MCX protokoly nativně podporují



FRMCS – síťové parametry OBN & RAN

FRMCS síťové řešení OBN & RAN:

OBN (On-Board Network)

Má za úkol připojit koncové systémy, aplikace a senzory

Separace LAN sítě pro MCX a komunikaci pasažérů

Dual-LAN pro připojení MC systémů (Master-slave)

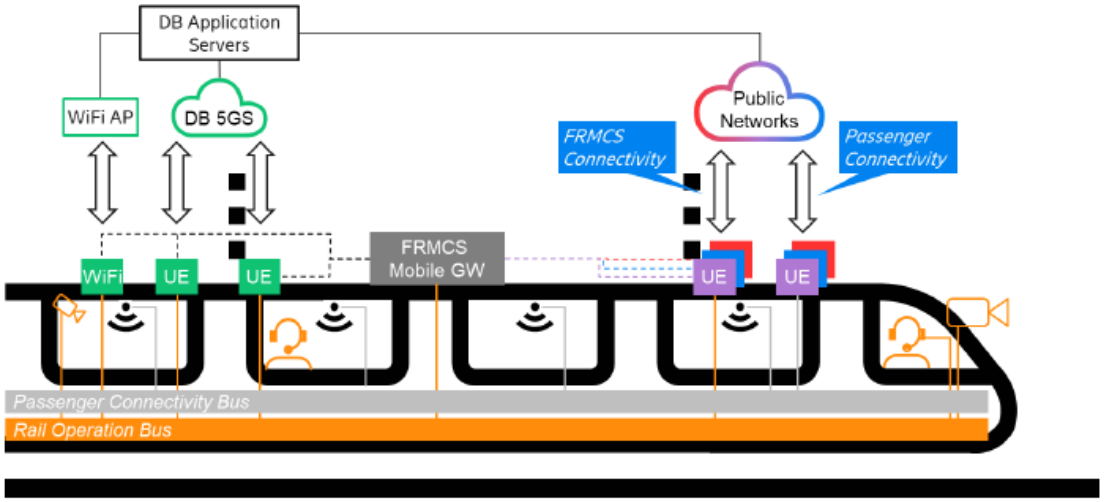
Redundance – LAN (HSR Ring), FRMCS-GW (FHRP + track)

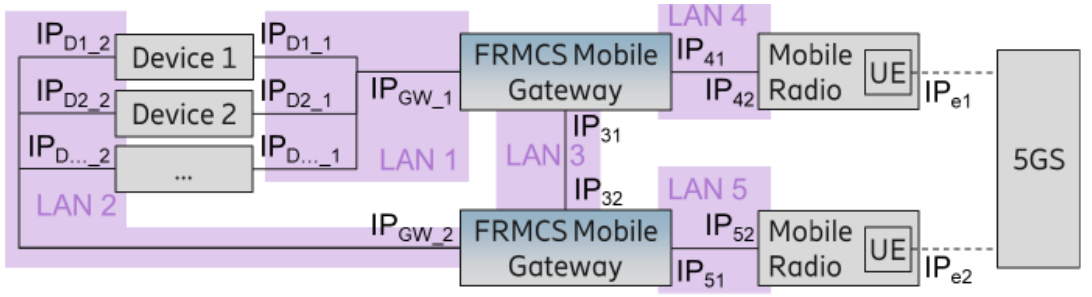
Bezdrátový přenos (Radio Access Network)

Má za úkol doručení dat mezi soupravou a traťovou sítí

FRMCS MCX Private 5G / síť cestující lze využít public síť

Redundance využívat 2x UE (FRMCS-GW monitoruje UE a přenosové parametry / můžeme





FRMCS – síťové parametry MPLS backbone

FRMCS síťové řešení MPLS backbone

Vysoká dostupnost (zajištění redundance v backbone)

Vybudování nezávislých LSP do central DC (SR-TE PCE Disjoint-path), případně záložních cest (SR TI-LFA)

Na úrovni L3VPN, redundantní připojení UPF (BGP ECMP Active-Active / BGP PIC Edge Active-Backup to 5G EPC)

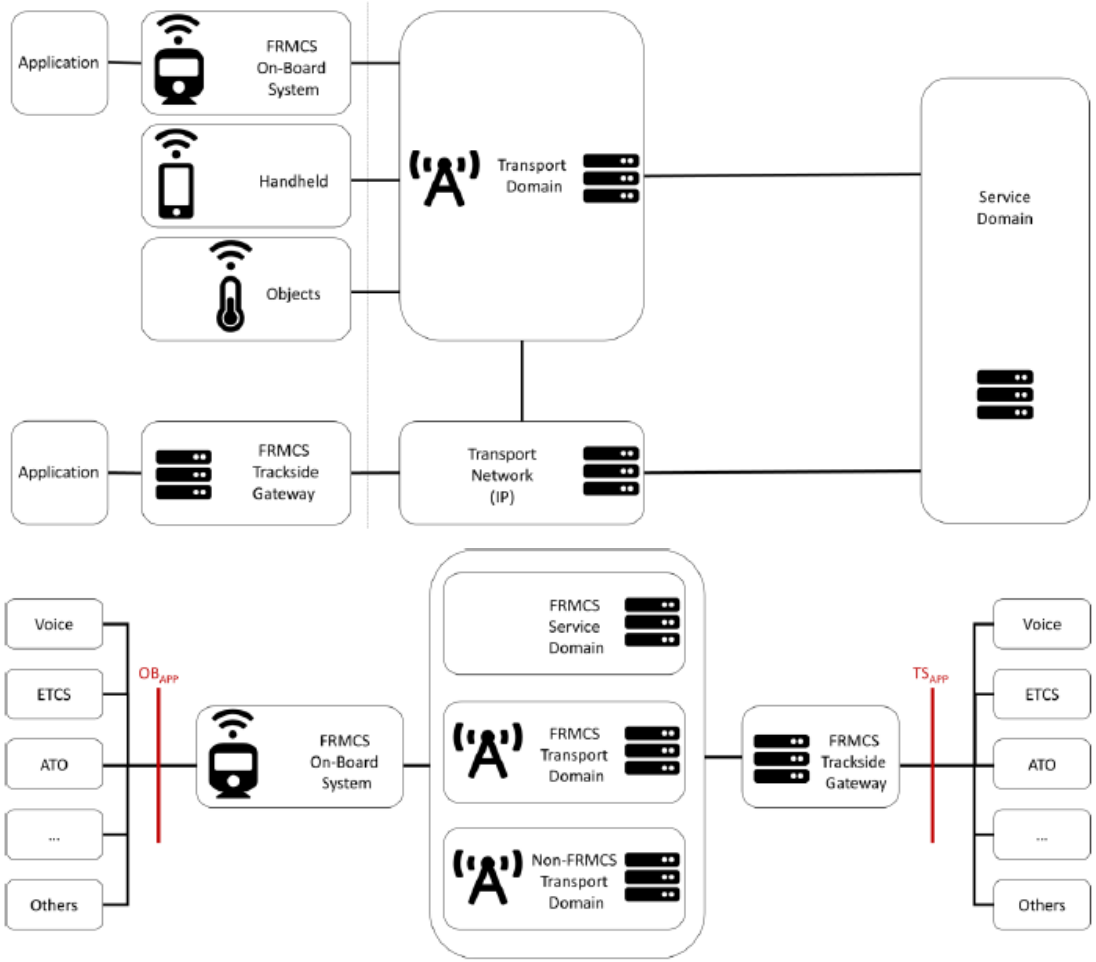
Kvalita služeb & Bezztrátový přenos dat

MCX - stálá latence (prioritizace), garance doručení (BW res)

Různé služby jiný přenos – delay, BW, … (SR-TE & Flex-Algo)

Monitoring & SLA

Aktivní SLA Monitoring mezi distribuovanými UPF a Regionálními / Central DC (latence, ztrátovost, jitter)



TTC MARCONI

Bezpečnost sítí v prostředí IoT

Vrstvená bezpečnost

- Administrativní přístup skrz I-DMZ
- Segmentace OT sítě do menších zón
- Kontrola a zabezpečení komunikace
- Kontrola na úrovni přístupu do OT sítě
- Zabezpečení na úrovni technologického zařízení
- Monitoring a vyhodnocování rizik v OT síti
- Investigace rizik a vytvoření response plánu

Administrativní přístup & Industriální DMZ

Technologická identita & kontrola přístupu do sítě

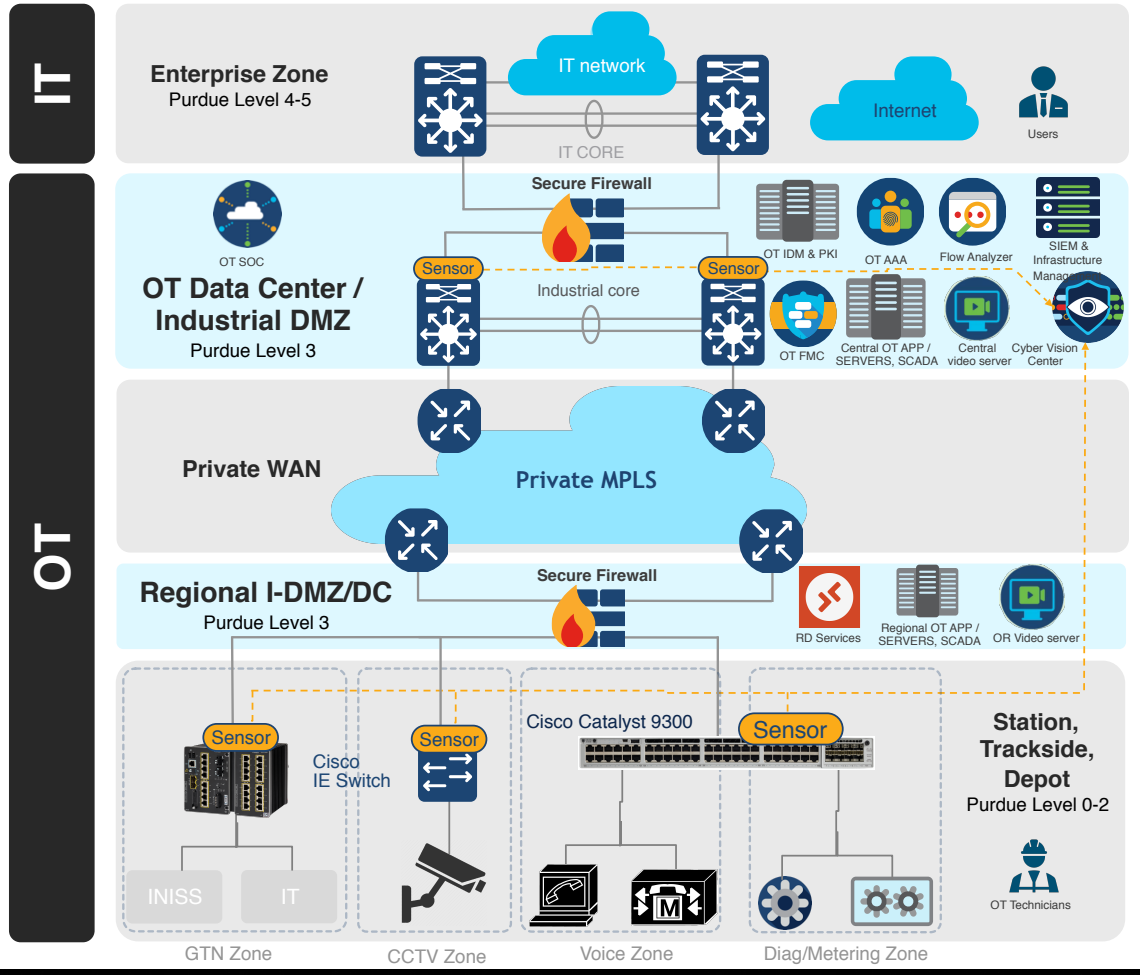
Zabezpečení průmyslové sítě - vrstvená bezpečnost

Neexistuje jeden jediný nástroj, který by nám zabezpečil celou technologickou síť.

Síť zabezpečujeme na několika úrovních pomocí množství bezpečnostních nástrojů/ principů.

Rozdělení bezpečnosti do vrstev/úrovní:

- **Zabezpečení perimetru mezi IT x OT sítí**
- **Administrativní přístup skrz I-DMZ**
- **Segmentace OT sítě do menších zón**
- **Kontrola a zabezpečení komunikace**
- **Kontrola na úrovni přístupu & segmenty OT sítě**
- **Zabezpečení na úrovni technologického zařízení**
- **Monitoring a vyhodnocování rizik v OT síti**



Administrativní přístup skrz I-DMZ

Přístup do OT systému z koncových stanic musí být uživatelů zakázán -> pouze z bezpečného prostředí

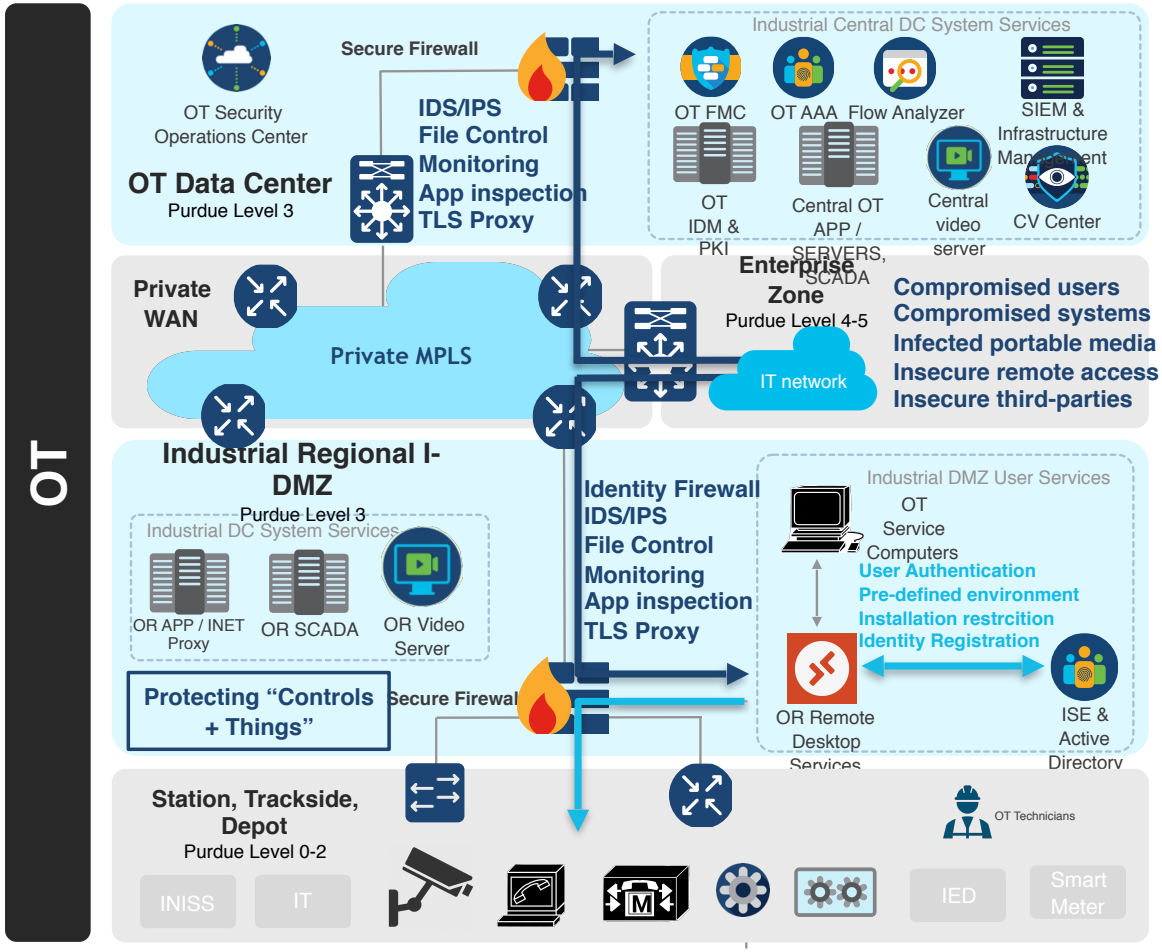
Hrozby -> šíření škodlivých kódů, neoprávněný a neomezený přístup, využívání nebezpečných protokolů

Správci OT sítě / dodavatelé musí provádět upgrade, monitoring, diagnostiku a další činnosti:

Uživatelské VPN do IT-DMZ -> FW -> OT I-DMZ

Hop servery (RDS) v I-DMZ pro přístup do OT sítě

RDS -> Autentizace uživatelů, omezení instalace aplikací (předdefinované prostředí), RDS-HA



Kontrola na úrovni přístupu & Segmenty OT sítě

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

Hrozby -> Neautorizovaný přístup do sítě -> „man-in-the-midle“ útoky, DoS útoky, šíření škodlivého kódu

Identita jako základ u uživatele = username/id, u stroje složitější - x.509 certificate / unikátní chování - profile

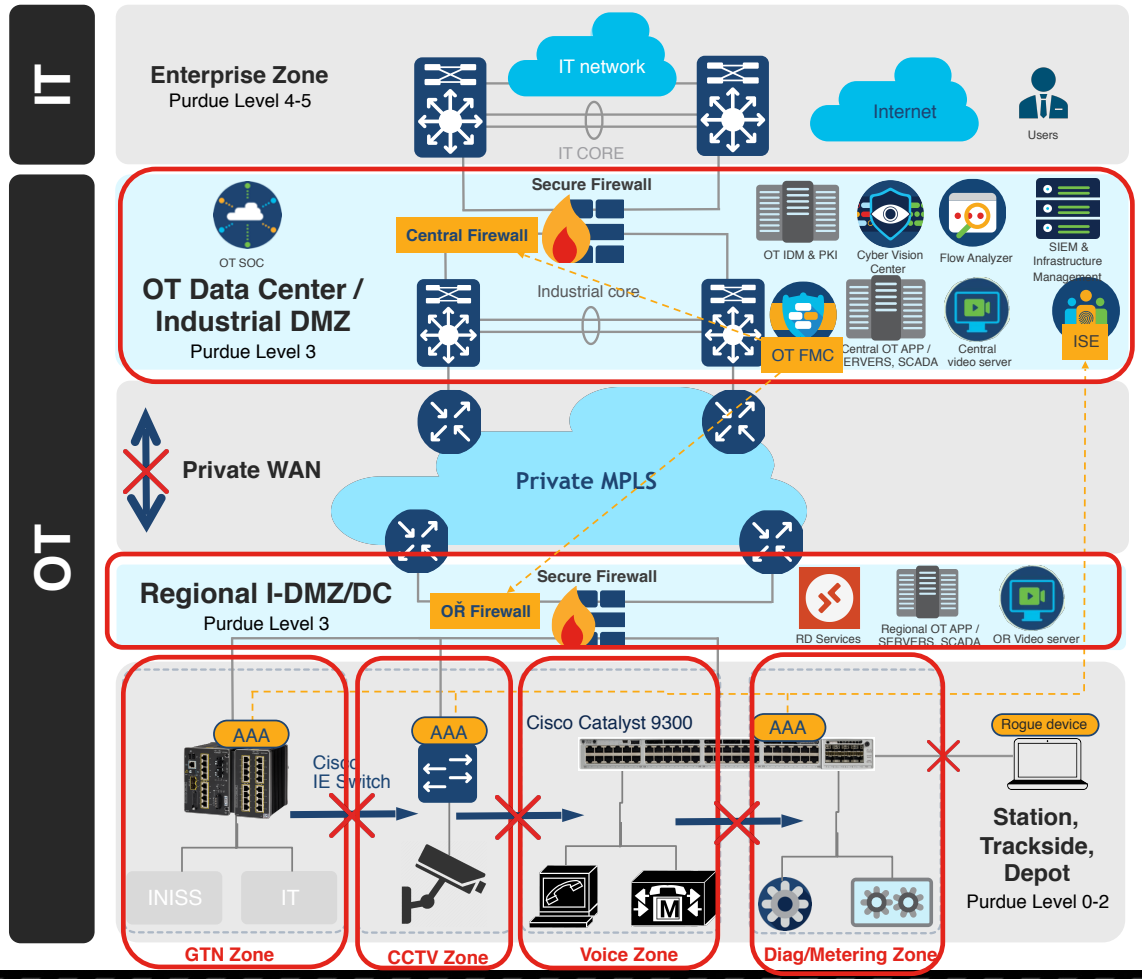
Na přístupových zařízeních/lokalitách aplikovat:

Fyzická bezpečnost, PKI infrastruktura pro OT

Přístupové zařízení (SW) ověřují připojené zařízení

802.1x (EAP-TLS) X.509 machine autentizace

Pro ostatní MAB + profilování (dVLAN, dACL,



TTCMARCONI

Co si odnést

OT sítě jsou postupně digitalizovány a automatizovány

Díky tomu můžeme zefektivnit náš provoz (snížit nálady na provoz, snížit zásahy techniků/odstávky systémů) a zvýšit kvalitu poskytovaných služeb

Na naši síť vznikají nové nároky hlavně z hlediska vysoké dostupnosti a kvality služeb - je potřeba využívat vhodné zařízení a funkce pro tyto služby

V OT síti klademe důraz na funkčnost, počítám s tím při návrhu bezpečnostních funkcí a mechanismů

OT síť je bezpečná tak jak zabezpečíme její

International union of railways (FRMCS Documents)
https://uic.org/rail-system/telecoms-signalling/frmcs

Visit cisco.com/go/iotsecurity

Děkujeme za pozornost

Vojtěch Richter

TTCMARCONI

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