

Příspěvek do konference ČVTSS

Koncepce datových sítí SŽ

Ing. Vladimír HORA
GŘ SŽ 014 OTSA

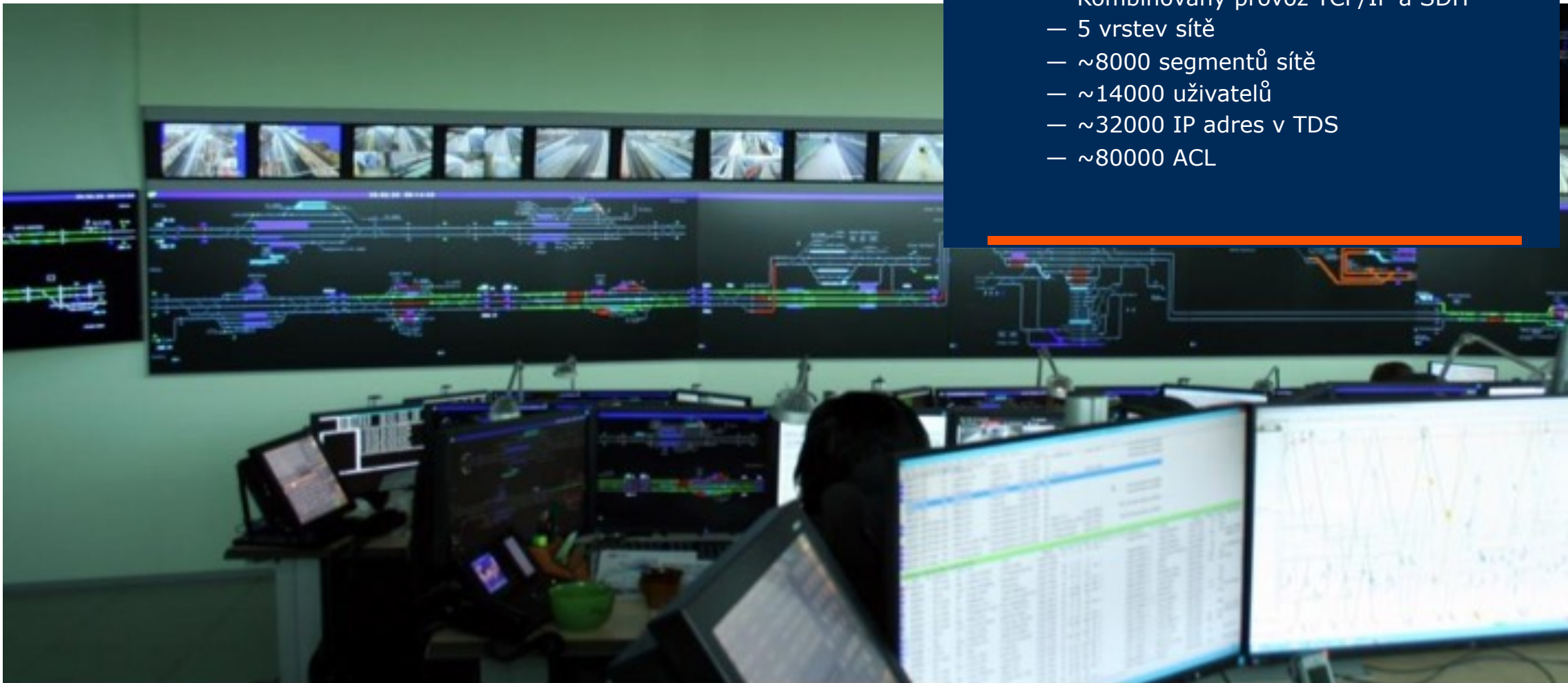
Praha, 1.3.2022

Historie



- Od r. 1925 děrošítkové systémy
- 1962 URAL 2 Laboratoř dopravy
- 1965 LEO 360 ÚVTD Praha
- 1972 systém INTERVOZ ČSD
- 1972 JSEP
- ...

Současnost



- Pokrytí celé železniční sítě SŽ
- Kombinovaný provoz TCP/IP a SDH
- 5 vrstev sítě
- ~8000 segmentů sítě
- ~14000 uživatelů
- ~32000 IP adres v TDS
- ~80000 ACL

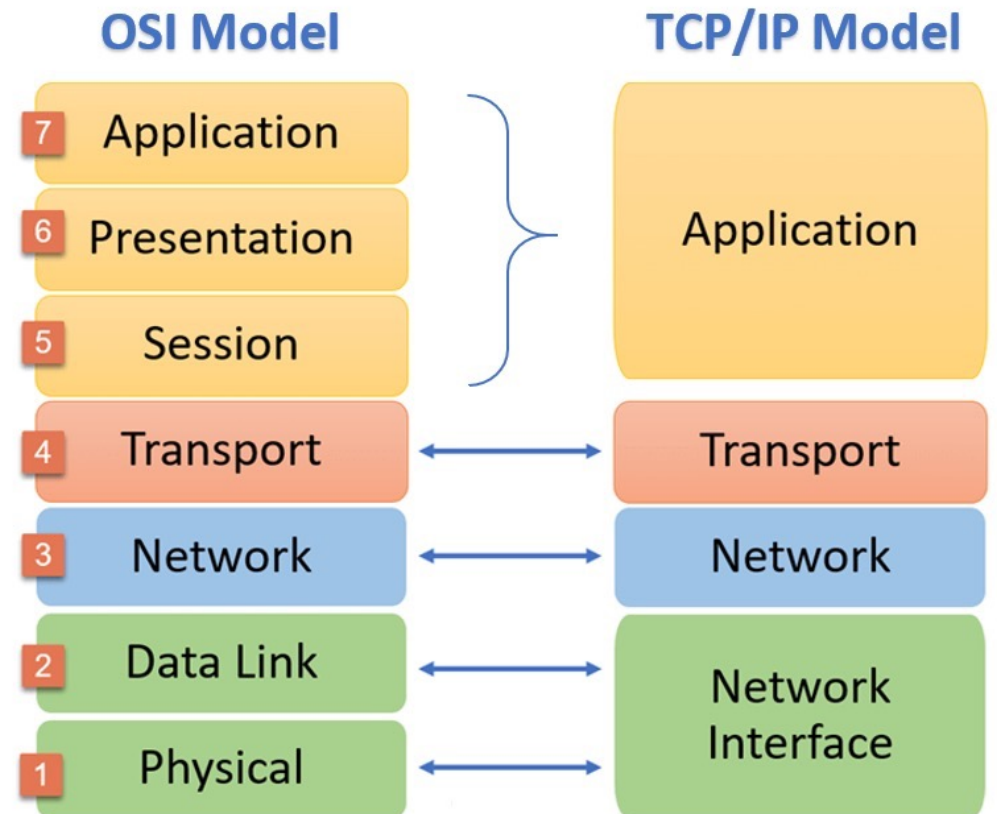
Datové sítě na SŽ

Slabé stránky - hrozby

- Dvourychlostní vývoj *IT/OT technologií*
- Používání nevhodných prvků
- End-of-life technologie v provozu
- Složitost sítě
- Pořizování sdělovačky ve stavbách
- Žádná okna pro údržbu a DR testy

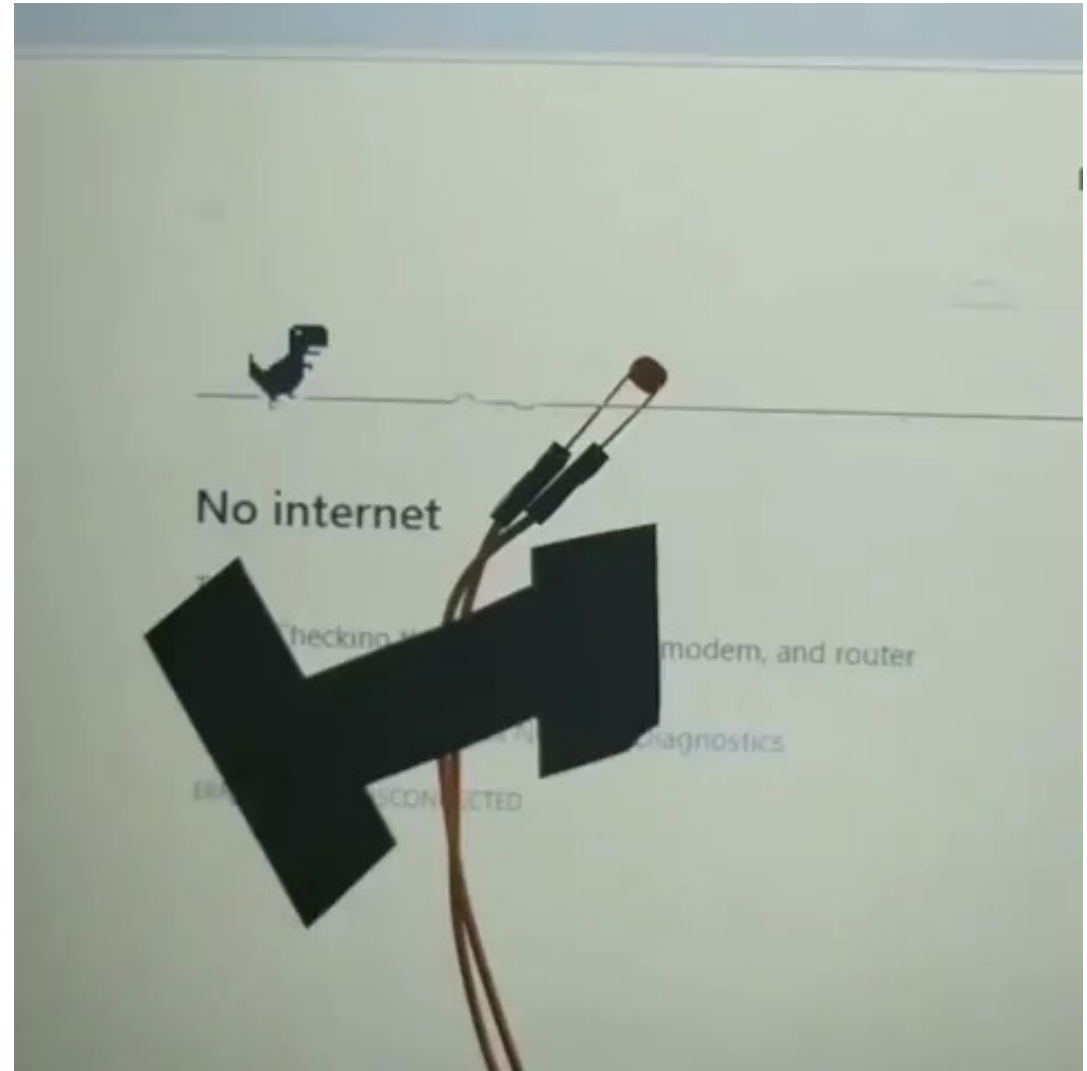
Silné stránky - příležitosti

- Přenos dat pro veškerou činnost dráhy
- Implementace moderních technologií
- Rozdělení na IT a OT – *konvergence*
- Nové standardy FRMCS, 3gpp apod.



Definice IT a OT

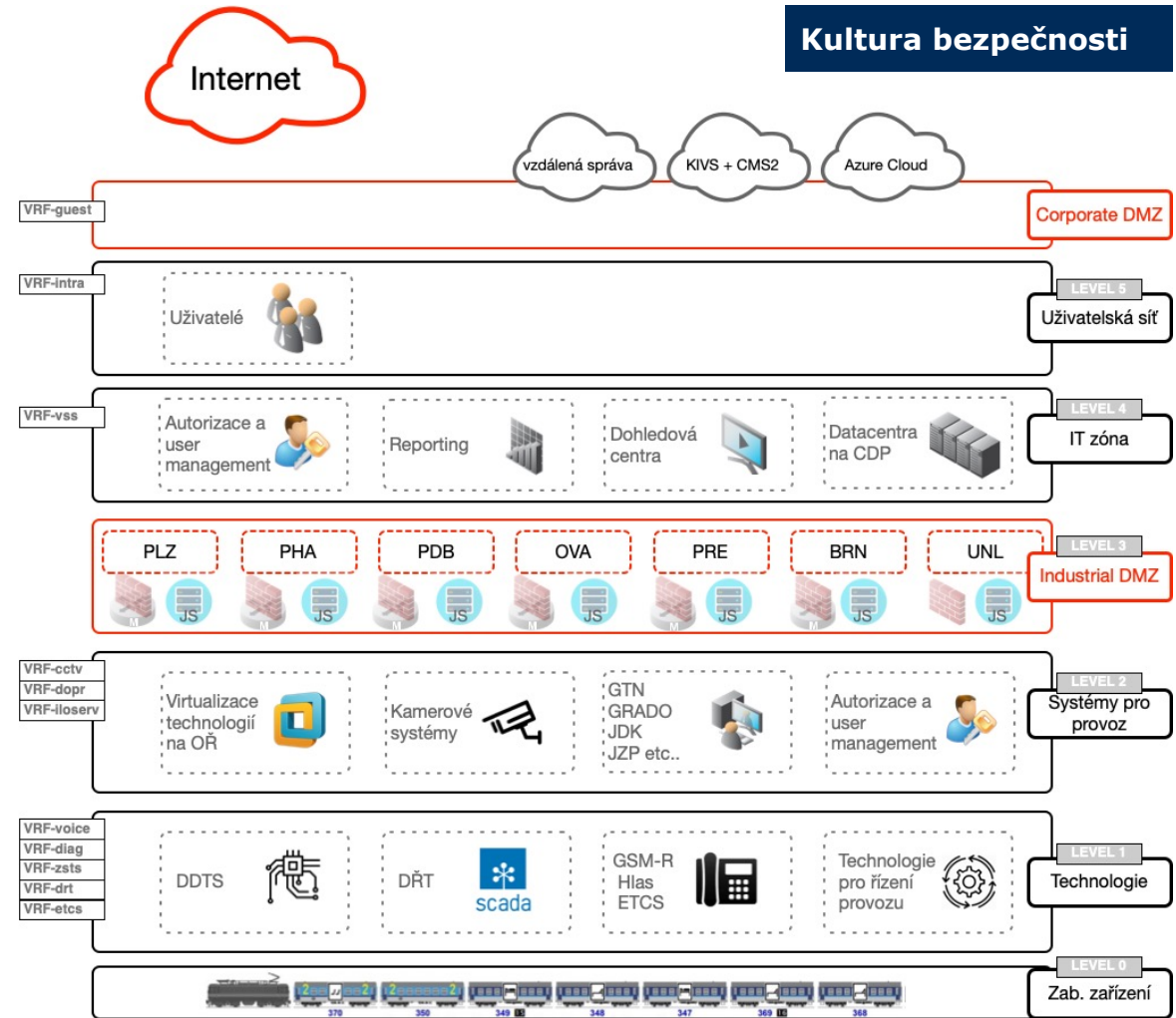
- IT
 - **Kancelářské aplikace, SAP**
 - **Manažerské systémy, dopravní aplikace**
 - **Intranet/UAS**
- OT
 - **GDS/LDS, DOZ**
 - **GTN, GRADO, dopravní deníky**
 - **DDTS, DŘT, GSM-R a komunikace ETCS**
 - **IP telefonie, zapojovače, hlas**
 - **Techlan/TDS**
- IT/OT paradigma – definuje základní charakteristiky síťového prostředí v SŽ
- Konvergence IT/OT
- Oddělení segmentů pomocí DMZ



Konvergence IT/OT

- Segmentace
- Stanovení bodu konvergence
- Implementace ISA/IEC 63443
- Stanovení bezpečnostních zón
- Nastavení pravidel pro komunikaci

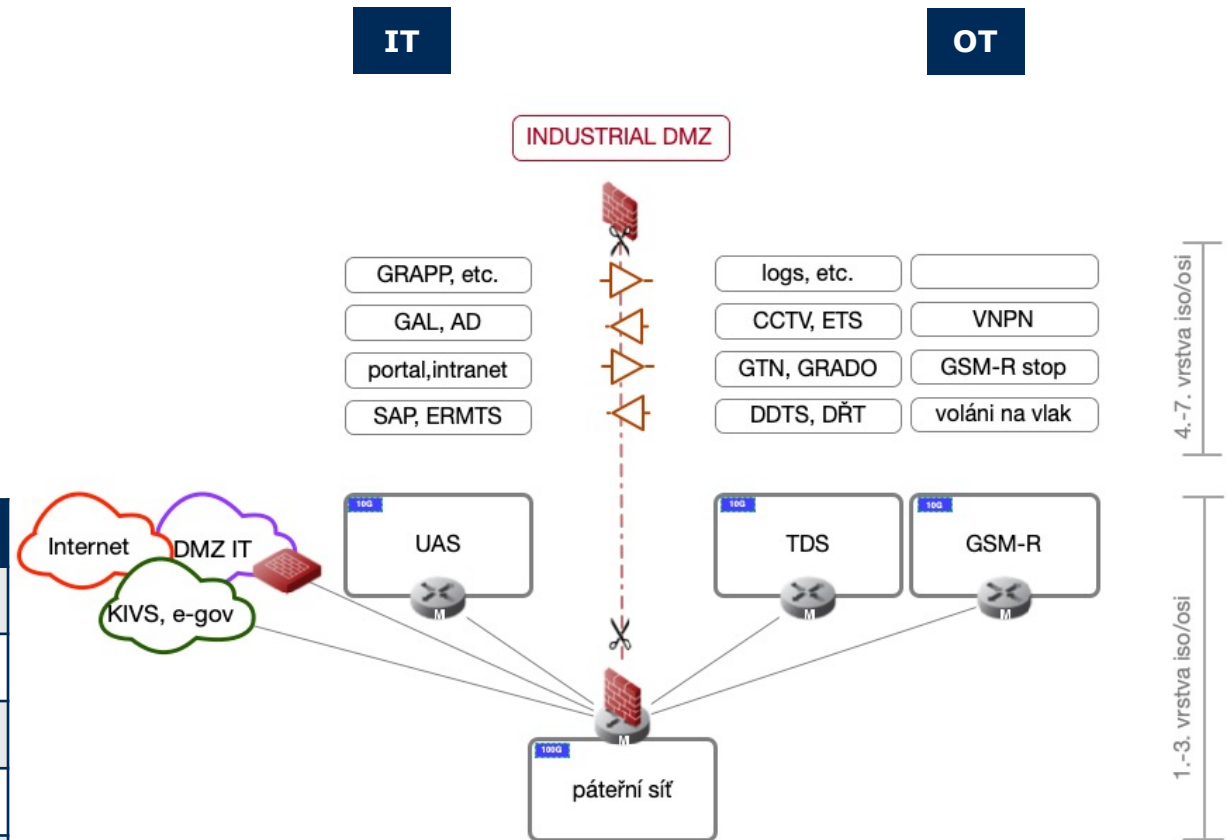
bod konvergence ->



Datová infrastruktura SŽ

- Robustní infrastruktura pro IT i OT
- 1-3.5 vrstva sítě SŽ
 - **jádro (core) sítě sjednotit na MPLS**
 - **dedikované GSM-R služby**
- od 3. vrstvy

IT	OT
updating	hardening
blacklisting	whitelisting
tisíce uživatelů	stovky uživatelů
Manažerské výstupy	Sběr dat
Plochá síť	Segmentovaná síť
UAS	TDS
Progresivní přístup	Konzervativní přístup



ISO/OSI model sítě SŽ

Datová infrastruktura SŽ - rozvoj

- Upgrade core sítě a segmentace TDS
- Robustní 10Gbit konektivita do RDP
- Implementace ISA/IEC 63443
- Hardening, industrial DMZ, Certifikační autorita
- OŘ TDS datová centra, Předávací body služeb
- Virtualizační farmy v TDS DC
- KIVS a CMS2, eGovernment
- IoT, secure LTE -> 5G
- Unifikace SW prostředí - API
- Migrace SDH/TDH -> MPLS
- Ústup od E1 a legacy služeb -> TCP/IP (TSN)
- Promyšlený sběr dat

Resumé

- Robustní 10Gbit konektivita do RDP
- Předávací body služeb
- Datová centra v TDS
- Centra po segmentaci TDS na OŘ
- Umístění conduitů
- Sídlo routingu a firewallingu v OŘ
- Ideální pro umístění služeb v TDS
- Aplikace pro řízení provozu
- Zálohování a sběr dat
- Terminování datově náročných služeb



Děkuji za pozornost

Koncepce datových sítí SŽ

Ing. Vladimír Hora

GŘ SŽ 014

horav@spravazeleznic.cz