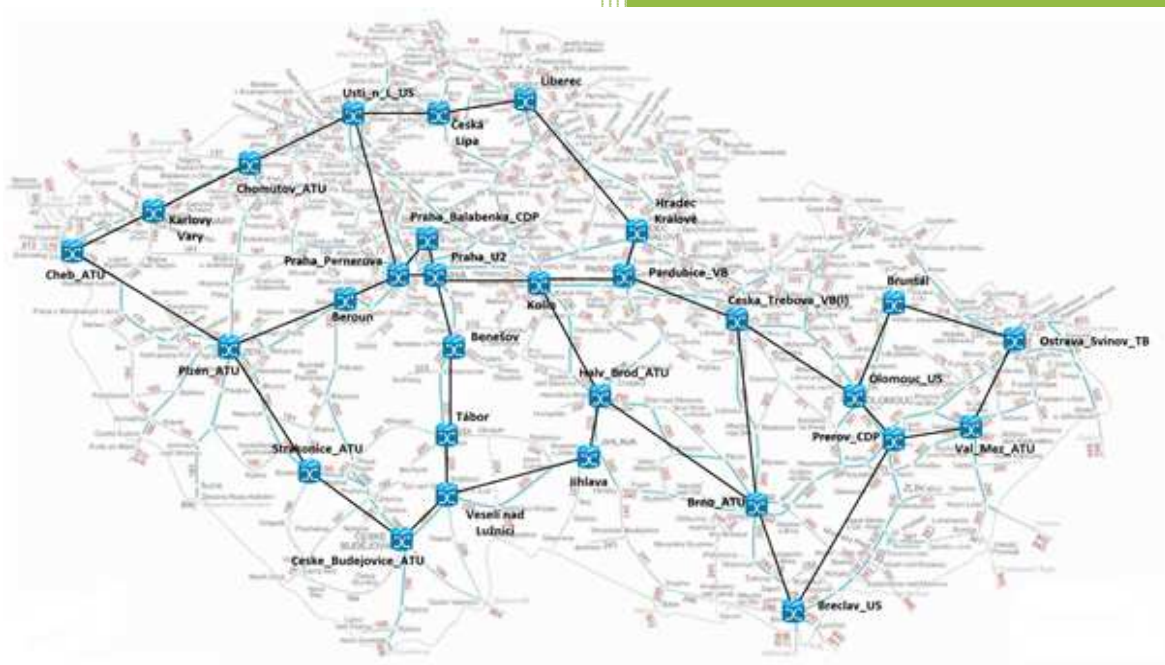


SDĚLOVACÍ SÍŤ PROVOZOVATELE DRÁHY SŽDC s.o.

C. METODIKA NÁVRHU DALŠÍ VÝSTAVBY SDĚLOVACÍ SÍTĚ SŽDC



C. ČÁST

METODIKA NÁVRHU DALŠÍ VÝSTAVBY SDĚLOVACÍ SÍTĚ SŽDC

OBSAH

1	ÚVOD	9
1.1	SDĚLOVACÍ ZAŘÍZENÍ V PROSTŘEDÍ SŽDC	9
1.2	KATEGORIE ŽELEZNIČNÍCH TRATÍ	10
2	KABELIZACE	11
2.1	METALICKÁ DÁLKOVÁ KABELIZACE	11
2.1.1	NAVRHOVANÝ STAV	11
2.2	TRAŤOVÉ METALICKÉ KABELY	12
2.2.1	NAVRHOVANÝ STAV	13
2.3	DÁLKOVÁ OPTICKÁ KABELIZACE	13
2.3.1	NAVRHOVANÝ STAV	14
2.3.1.1	Topologie a rozvoj sítě	15
2.3.1.2	Kapacita DOK	16
2.3.1.3	Rezervy na trase a spojky	19
2.3.1.4	Ukončování	19
2.3.1.5	Vyvádění a obsazení vláken	19
2.4	MÍSTNÍ KABELIZACE METALICKÁ	21
2.4.1	NAVRHOVANÝ STAV	22
2.5	MÍSTNÍ KABELIZACE OPTICKÁ	22
2.5.1	UKLÁDÁNÍ KABELŮ	23
2.5.1.1	Prostor pro vedení kabelových tras	23
2.5.1.2	Technické řešení sdružených kabelových tras v mezistaničních úsecích	24
2.5.1.3	Vedení kabelů po mostech	25
2.5.1.4	Vedení kabelů v železničních stanicích a pod zpevněnými plochami	25
3	PŘENOSOVÝ SYSTÉM A TECHNOLOGICKÁ DATOVÁ SÍŤ	26
3.1	DWDM	26
3.1.1	NOVÉ TRASY PRO ZAOKRUHOVÁNÍ SLUŽEB A PŘIPOJENÍ VÝZNAMNÝCH LOKALIT	27
3.1.1.1	Posílení vrstvy SDH a 1G páteřní sítě	28
3.1.2	POSÍLENÍ STÁVAJÍCÍ 1G PÁTEŘE NA 10G	29
3.1.3	TOPOLOGIE MPLS 1G/10G ETH	29
3.1.4	PROPOJENÍ DC 10G NA 100G	30
3.2	PŘENOSOVÁ SÍŤ MPLS	31
3.2.1	DOVYBAVENÍ STÁVAJÍCÍCH LOKALIT	31
3.2.2	SEGMENTACE PROVOZU DO VRF	32
3.2.2.1	Vyčlenění externích organizací do oddělené sítě	32
3.2.3	VARIANTY PŘIPOJENÍ LOKALIT DO MPLS	33
3.2.3.1	Varianta č.1 – Varianta připojení ŽST a ZAST pomocí PE, CE a L2 přepínači	33
3.2.3.2	Varianta č.2 – Varianta připojení ŽST a ZAST pomocí PE, CE a L3	35
3.2.3.3	Varianta č.3 – Varianta připojení ŽST a ZAST v redundantním řešení	36
3.2.4	VZÁJEMNÉ PROPOJENÍ SDH A MPLS SÍTĚ	37
3.2.5	MOŽNOSTI ZÁLOŽNÍHO PŘENOSU E1 PRO PŘÍPAD ZÁLOŽNÍHO PROPOJENÍ MPLS A SDH SÍTĚ	38
3.2.5.1	Záloha E1, která začíná a končí v SDH	39

3.2.5.2	Záloha E1, která začíná a končí v MPLS	39
3.2.5.3	Zálohované připojení GSM-R BTS s rozhraním E1 do sítě MPLS.....	40
3.3	SYNCHRONIZACE PŘENOSOVÉHO SYSTÉMU A TDS	41
3.3.1	VYUŽITELNOST DATOVÉ SÍTĚ A MOŽNOSTI JEJÍ OPTIMALIZACE	41
3.3.2	SYSTÉMY S ŠÍŘENÍM PO FYZICKÉ VRSTVĚ.....	42
3.3.3	ŠÍŘENÍ PAKETOVÝMI TOKY	44
4	DOHLEDOVÝ MANAGEMENT SÍTĚ	46
4.1	TEORETICKÉ PŘEDPOKLADY	46
4.1.1	ARCHITEKTURY KOMUNIKACE S MONITOROVANÝMI PRVKY	46
4.1.2	MODEL MANAGEMENTU SLUŽEB	47
4.1.2.1	Korelační model	49
4.1.2.2	End-to-end model.....	50
4.1.2.3	Specifika dohledu hlasových služeb.....	51
4.1.2.4	Výběr modelu	51
4.1.3	VLIV BEZPEČNOSTNÍCH DOMÉN.....	52
4.1.4	NÁVAZNOST NA PROCESY	54
4.1.4.1	Standardy ITIL	54
4.1.4.2	Technické prostředky řízení procesů	55
4.1.5	OBEČNÉ POŽADAVKY NA CÍLOVÝ UMBRELLA-SYSTÉM	55
4.2	INVENTURA DOHLEDOVÉHO PROSTŘEDÍ.....	57
4.2.1	AUDIT DOHLEDOVANÝCH TECHNOLOGIÍ	57
4.2.2	AUDIT DOHLEDŮ SÍTÍ.....	58
5	KOMUNIKACE DŘT, DDTS ŽDC V ENERGETICKÝCH OBJEKTECH	59
5.1	NORMY, PŘEDPISY	59
5.1.1	KLASIFIKACE PROVOZNÍCH PARAMETRŮ DLE ČSN IEC 870-4.....	59
5.1.2	KLASIFIKACE KVALITATIVNÍCH POŽADAVKŮ DLE ŘADY ČSN EN 61850-X-X	60
5.1.3	POŽADAVKY NA SYSTÉMY PRO PŘENOS POVELŮ OCHRAN DLE ČSN EN 60834-1	64
5.2	KOMUNIKACE DISPEČERSKÝCH SYSTÉMŮ V PŘENOSOVÉ SÍTĚ SŽDC	67
5.2.1	KOMUNIKACE NA ÚROVNI ENERGETICKÝCH OBJEKTŮ	67
5.2.1.1	Zabezpečený způsob výměny mezi DŘT, DDTS ŽDC a jinými systémy	68
5.2.2	KOMUNIKACE NA ÚROVNI OCHRAN DISTRIBUČNÍCH ROZVODŮ	68
5.2.3	KOMUNIKACE OSTATNÍCH TECHNOLOGICKÝCH CELKŮ	70
6	HLASOVÁ A TELEFONNÍ SÍŤ	71
6.1	DRUHY SLUŽEB A DRUHY ZAŘÍZENÍ	71
6.2	ARCHITEKTURNÍ POŽADAVKY NA SLUŽBY UCC	71
6.3	NAVRHOVANÁ ARCHITEKTURA UCC.....	72
6.4	SPRÁVA UŽIVATELŮ, UŽIVATELSKÝCH SLUŽEB A KOMUNIKAČNÍCH ZAŘÍZENÍ UCC	73
6.5	ÚDRŽBA SYSTÉMU – UPGRADY	73
6.5.1	ÚSTŘEDNY / CLUSTER.....	73
6.5.2	TERMINÁLY.....	74
6.5.3	TELEFONY	74
6.5.4	HLASOVÉ BRÁNY.....	74
6.6	TELEFONNÍ SÍŤ.....	74
6.6.1	SLUŽEBNÍ TELEFONNÍ SÍŤ SŽDC	74
6.6.2	STÁVAJÍCÍ STRUKTURA TELEFONNÍ SÍTĚ.....	75

6.6.3	IP TELEFONIE.....	75
6.6.4	NÁVRH NOVÉ STRUKTURY.....	77
6.6.5	ZPŮSOBY IMPLEMENTACE.....	78
6.7	BEZPEČNOST SLUŽEBNÍ SÍŤE	79
7	DOTYKOVÉ TERMINÁLY A ZAPOJOVAČE	80
7.1	DOPRAVNÍ SÍŤ	80
7.2	KONSOLIDACE TERMINÁLŮ	80
7.3	PROSTUPY MEZI SLUŽEBNÍ A DOPRAVNÍ SÍŤÍ	81
7.4	ČÍSLOVACÍ PLÁN	81
7.5	BEZPEČNOST DISPEČERSKÉ SÍŤE.....	81
7.6	SÍŤOVÁ BEZPEČNOST	82
7.6.1	SEGMENTACE INFRASTRUKTURY.....	82
7.6.2	OCHRANA DŮVĚRNOSTI A INTEGRITY PŘENÁŠENÝCH DAT.....	83
7.6.3	ZABEZPEČENÍ PŘÍSTUPU DO SÍŤE.....	83
7.6.4	PODPORA SUBSYSTÉMŮ KYBERNETICKÉ BEZPEČNOSTI	84
8	RÁDIOVÉ SYSTÉMY	86
8.1	ROZVOJ STÁVAJÍCÍCH RÁDIOVÝCH SYSTÉMŮ	86
8.2	ÚDRŽBA STÁVAJÍCÍCH RÁDIOVÝCH ZAŘÍZENÍ	86
8.2.1	TRAŤOVÝ RÁDIOVÝ SYSTÉM	87
8.2.1.1	Postup migrace a souběhu rádiových systémů TRS a GSM-R.....	87
8.2.2	SRV.....	88
8.3	RÁDIOVÝ SYSTÉM GSM-R	88
8.3.1	ROZVOJ GSM-R	88
8.3.2	VÝSTAVBA GSM-R.....	89
8.3.3	FUNKCIONALITA GSM-R STOP	91
8.3.4	GSM-R JAKO NÁHRADA RÁDIOVÝCH SÍŤÍ TRS SRD A TRS SRV	91
8.4	MÍSTNÍ RÁDIOVÝ SYSTÉM MRS.....	92
8.4.1	VÝSTAVBA MRS.....	92
8.5	BUDOVNOST RÁDIOVÝCH SYSTÉMŮ PRO ŽELEZNICI.....	93
8.6	ŽELEZNIČNÍ BEZDRÁTOVÁ SÍŤ	93
9	KONTROLNĚ ANALYTICKÉ CENTRUM ŘÍZENÍ DOPRAVY	94
9.1	ROZŠIŘOVÁNÍ FUNKCIONALIT A MOŽNOSTÍ APLIKACE KAC	95
9.1.1	ROZŠIŘOVÁNÍ STÁVAJÍCÍCH FUNKCIONALIT KAC	95
9.1.2	NOVÉ FUNKCIONALITY APLIKACE KAC.....	96
10	INFORMAČNÍ MANAGEMENT ŽELEZNIČNÍ INFRASTRUKTURY	99
10.1	DÁLKOVÁ DIAGNOSTIKA TECHNOLOGICKÝCH SYSTÉMŮ ŽELEZNIČNÍ DOPRAVNÍ CESTY	99
10.2	ZÁKLADNÍ TOPOLOGIE SYSTÉMU	101
10.2.1	STRUKTURA SYSTÉMU	102
10.3	HLAVNÍ ZDROJE DAT	102
10.4	MOŽNOSTI VYUŽITÍ DAT Z TECHNOLOGICKÝCH SYSTÉMŮ.....	103
10.5	INFORMAČNÍ MANAGEMENT	104
10.6	ZAČLENĚNÍ DO SYSTÉMU KAC.....	104
10.7	PŘÍNOSY ŘEŠENÍ	105
11	KAMEROVÉ SYSTÉMY.....	107
11.1	KAMEROVÉ SYSTÉMY V ŽELEZNIČNÍCH STANICÍCH A ZASTÁVKÁCH	107

11.1.1	STÁVAJÍCÍ STAV.....	107
11.1.2	NAVRHOVANÝ STAV	107
11.2	TRAŤOVÉ KAMEROVÉ SYSTÉMY (KAMEROVÉ SYSTÉMY NA PŘEJEZDECH)	108
11.2.1	STÁVAJÍCÍ STAV.....	109
11.2.2	NAVRHOVANÝ STAV	109
11.3	KAMEROVÉ SYSTÉMY A KONTROLNĚ ANALYTICKÉ CENTRUM ŘÍZENÍ DOPRAVY	109
11.4	SYSTÉM AUTOMATICKÉ VÝSTRAHY OHROŽENÍ PROVOZU (SAVOP)	111
11.4.1	STÁVAJÍCÍ STAV.....	111
11.4.2	NAVRHOVANÝ STAV	111
11.5	KAMEROVÉ SYSTÉMY A FUNKCIONALITA GSM-R STOP, RESP. GENERÁLNÍ STOP TRS	112
11.6	VIDEODISPEČINKY (CDP).....	112
12	INFORMAČNÍ SYSTÉMY PRO INFORMOVÁNÍ CESTUJÍCÍCH	115
12.1	STANDARDIZACE INFORMAČNÍHO ZAŘÍZENÍ	115
12.2	CENTRÁLNÍ SPRÁVA INFORMAČNÍHO SYSTÉMU	116
12.2.1	NÁVRH ARCHITEKTURY A DEFINOVÁNÍ KONCEPCE CENTRÁLNÍ SPRÁVY	116
12.2.2	CENTRÁLNÍ SPRÁVA ISIC.....	117
12.2.2.1	Dostupné funkce.....	117
12.2.3	LOKÁLNÍ INFORMAČNÍ SYSTÉM STANICE	118
12.2.4	TECHNICKÉ PARAMETRY CENTRÁLNÍ SPRÁVY ISIC.....	119
12.2.4.1	Centrální server	119
12.2.4.2	Lokální systémy ISIC.....	119
13	ROZHLASOVÉ ZAŘÍZENÍ	121
13.1	NAVRHOVANÝ STAV.....	121
13.1.1	ROZHLAS PRO POSUN.....	121
13.1.2	EVAKUAČNÍ ROZHLAS.....	122
14	ZABEZPEČOVACÍ A PROTIPOŽÁRNÍ SYSTÉMY.....	123
14.1	AUTONOMNÍ SAMOČINNÝ HASICÍ SYSTÉM	123
14.2	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	123
14.3	ELEKTRONICKÁ ZABEZPEČOVACÍ SIGNALIZACE	124
15	KYBERNETICKÁ BEZPEČNOST – metodická doporučení pro IT projekty v prostředí SŽDC	125
15.1	LEGISLATIVNÍ RÁMEC	126
15.2	NAVAZUJÍCÍ VYHLÁŠKY	126
15.3	DEFINICE POJMŮ.....	126
15.4	POVINNOSTI OSOB A ORGÁNŮ DLE ZKB.....	127
15.5	DOPORUČENÍ PRO KOMPLEXNÍ PROSTŘEDÍ VÍCE DODAVATELŮ – BEZPEČNOSTNÍ OPATŘENÍ DLE ZKB	127
15.6	CELOEVROPSKÁ SMĚRNICE NIS (NETWORK AND INFORMATION SECURITY)	128
16	SYNCHRONIZACE ČASU SDĚLOVACÍHO ZAŘÍZENÍ V SÍTI SŽDC	131
16.1.1	SYNCHRONIZACE ČASU POMOCÍ GPS	131
16.1.2	SYNCHRONIZACE ČASU POMOCÍ SIGNÁLU DCF 77	132
17	PROSTORY PRO SDĚLOVACÍ ZAŘÍZENÍ V PROSTŘEDÍ SŽDC.....	133
17.1	SDĚLOVACÍ MÍSTNOST VE VELKÉM ŽELEZNIČNÍM UZLU	134
17.2	SDĚLOVACÍ MÍSTNOST VE STŘEDNÍ ŽELEZNIČNÍ STANICI.....	135
17.3	SDĚLOVACÍ MÍSTNOST V MENŠÍ ŽELEZNIČNÍ STANICI.....	136
17.4	SDĚLOVACÍ MÍSTNOST V ŽELEZNIČNÍ ZASTÁVCE	138

17.5 VENKOVNÍ ROZVADĚČE PRO SDĚLOVACÍ ZAŘÍZENÍ.....	139
17.6 KABELOVÝ MANAGEMENT	140
18 DATOVÁ CENTRA	142
18.1 PRÁVNÍ POŽADAVKY NA DATOVÁ CENTRA	142
18.1.1 PRÁVNÍ PROSTŘEDÍ ČR	142
18.1.2 PRÁVNÍ PROSTŘEDÍ EU	142
18.1.3 NADNÁRODNÍ NORMY	142
18.1.4 ZÁKLADNÍ NADNÁRODNÍ NORMY	143
18.2 ZÁKLADNÍ POŽADAVKY NA DATOVÁ CENTRA.....	143
19 ZÁVĚREČNÁ SHRNUTÍ A DOPORUČENÍ.....	145
19.1 KABELIZACE	145
19.2 PŘENOSOVÁ SÍŤ SŽDC	146
19.3 KOMUNIKACE APLIKACÍ DŘT, DDTS ŽDC V ENERGETICKÝCH OBJEKTECH	147
19.4 TELEFONNÍ SÍŤ	148
19.5 DOTYKOVÉ TERMINÁLY A ZAPOJOVAČE.....	149
19.6 KONTROLNĚ ANALYTICKÉ CENTRUM	149
19.7 INFORMAČNÍ MANAGEMENT PRO ŽELEZNIČNÍ INFRASTRUKTURU	150
19.8 KYBERNETICKÁ BEZPEČNOST V PROSTŘEDÍ SŽDC	151
19.9 RÁDIOVÉ SYSTÉMY.....	151
19.10 KAMEROVÉ SYSTÉMY	152
19.11 INFORMAČNÍ ZAŘÍZENÍ PRO INFORMOVÁNÍ CESTUJÍCÍCH	152
19.12 EPS, EZS, ASHS	153
19.13 DATOVÁ CENTRA	153

SEZNAM PŘÍLOH - VÝKRESOVÁ A TABULKOVÁ ČÁST**VÝKRESOVÁ ČÁST**

Stávající stav – tranzitní úroveň	C.2.1
Stávající stav – uzlová úroveň	C.2.2
Stávající stav – koncová úroveň	C.2.3
Navrhovaný stav – tranzitní úroveň	C.2.4
Navrhovaný stav – koncová úroveň	C.2.5

SEZNAM TABULEK

Tab. 1 – Obsazení kabelu 36 vláken Tlumačov – Přerov	16
Tab. 2 – Obsazení kabelu 12 vláken Tlumačov - Přerov	17
Tab. 3 – Cenové srovnání DOK 48 vláken a 72 vláken.....	18
Tab. 4 – Navrhovaná kapacita DOK.....	18
Tab. 5 – Návrh zásad obsazování vláken	21
Tab. 6 – Návrh segmentace provozů do VRF	32
Tab. 7 – Typické obsazení lokalit v síti SŽDC	33
Tab. 8 – Třídy výkonu	63
Tab. 9 – Třídy pro přenosové časy.....	63
Tab. 10 – Třídy synchronizace času pro synchronizaci IED	64
Tab. 11 – Použití synchronizace času pro časové značky nebo vzorkování	64

SEZNAM OBRÁZKŮ

Obr. 1 – Topologie přenosové sítě (cílový stav)	15
Obr. 2 – Schématické vyvádění vláken DOK.....	20
Obr. 3 – Stávající topologie přenosové sítě DWDM.....	27
Obr. 4 – Vytvoření velkých kruhů pokrývajících nepřipojené lokality	27
Obr. 5 – Současná topologie DWDM (6 kruhů)	28
Obr. 6 – Nová topologie DWDM (vytvoření 8 kruhů).....	29
Obr. 7 – Současná topologie agregačních routerů MPLS.....	30
Obr. 8 – Nová topologie agregačních routerů MPLS.....	31
Obr. 9 – Obecná struktura MPLS.....	31
Obr. 10 – Připojení koncových zařízení s L2 přepínači.....	34
Obr. 11 – Připojení kaskády L3 switchů	35
Obr. 12 – Připojení koncových zařízení (L3).....	36
Obr. 13 – Zálohované řešení ŽST.....	37
Obr. 14 – Propojení MPLS a SDH sítě	38
Obr. 15 – Přenos E1 mezi SDH a MPLS sítí	38
Obr. 16 – Přenos E1 v SDH a záložně MPLS sítí.....	39
Obr. 17 – Přenos E1 v MPLS a záložně SDH sítí.....	40
Obr. 18 – Přenos E1 v MPLS a záložně DWDM sítí.....	40
Obr. 19 – Připojení GSM-R BTS v síti MPLS	41

Obr. 20 – Začlenění polokruhu SEC (EEC) mezi vrstvy šíření synchronizace (praporky symbolizují zprávy řídicího protokolu QL/SSM)	43
Obr. 21 – Příklad schématu ACR s překrývajícími se stromy.....	45
Obr. 22 – Modely managementu služeb	48
Obr. 23 – Rozpad ICT služby na komponenty a vazby mezi nimi	49
Obr. 24 – Korelační model.....	49
Obr. 25 – End to End model	50
Obr. 26 – Rozdělení na dvě domény s možnými interakcemi prvků monitorovacího systému	53
Obr. 27 – Vztahy mezi modelováním a mapováním částí souboru IEC 61850.....	61
Obr. 28 – Typické provozní doby pro systémy ochrany ve spojení se zařízením pro přenos povelů ochrany.....	66
Obr. 29 – Topologie komunikace DŘT, DDTS ŽDC, ochrany a ostatních aplikací	67
Obr. 30 – konfigurace zařízení pro přenos povelů ochrany v hovorovém pásmu	69
Obr. 31 – konfigurace zařízení pro přenos povelů ochrany po VF spoji po silových vedeních	69
Obr. 32 – Přímě propojená digitální zařízení pro přenos povelů ochrany.....	69
Obr. 33 – Digitální zařízení pro přenos povelů ochrany přes komunikační systém	69
Obr. 34 – Vyčlenění provozů do samostatných VRF	70
Obr. 35 – Navrhovaná architektura UCC.....	72
Obr. 36 – Schéma clusteru CUCM dopravní sítě	80
Obr. 37 – Princip autentizace 802.1X	82
Obr. 38 – Výstavba rádiového systému GSM-R jako náhrada sítě TRS SRD a TRS SRV	92
Obr. 39 – Stávající funkcionality a struktura aplikace KAC.....	94
Obr. 40 – Obecné schéma nadstavby DDTS ŽDC.....	100
Obr. 41 – Základní architektura systému	101
Obr. 42 – Struktura informačního managementu.....	104
Obr. 43 – Začlenění do systému KAC.....	105
Obr. 44 – Přehledové schéma Centrální správy ISIC	119
Obr. 45 – přehledové blokové schéma k zákonu a jeho prováděcím předpisům	125
Obr. 46 – Návrh na uspořádání zařízení v místnosti – Střední ŽST	136
Obr. 47 – Návrh na uspořádání zařízení v místnosti – malá ŽST	137
Obr. 48 – Návrh na uspořádání zařízení v místnosti – zastávka	138
Obr. 49 – Příklad venkovní klimatizované skříně (antivandal provedení).....	139
Obr. 50 – Příklad umístění bezklíčového vstupu do klicy	140
Obr. 51 – Příklad kabelového managementu rozvaděče	141

1 ÚVOD

Cílem této části studie „*Sdělovací síť provozovatele dráhy SŽDC, s.o.*“ je navrhnout metodiku pro další postup výstavby sdělovací infrastruktury na úrovni fyzické, linkové a síťové vrstvy podle ISO/OSI referenčního modelu tak, aby byly zajištěny veškeré potřeby provozu tzv. „malé sdělovací techniky“ a „velké sdělovací techniky“, zabezpečovací techniky, dispečerské řídicí techniky a dálkového odečtu energetických dat v prostředí SŽDC, a to pro jednotlivé kategorie tratí, které budou pro tento účel stanoveny zpracovatelem studie. Součástí bude analýza předpokládané potřeby přenosu dat v jednotlivých úsecích tratí na síti SŽDC v časovém horizontu stanoveném řešitelem tak, aby byly pokryty i potřeby nových technologií, jejichž nasazení se u SŽDC předpokládá (časově se předpokládá minimálně do roku 2025 – 2030).

Pro zajištění přenosu dat pro tyto technologie s předpokladem jejich budoucího zavedení do provozu musí studie již nyní uvažovat z hlediska další výstavby příslušný potřebný rozsah sdělovacího zařízení.

1.1 Sdělovací zařízení v prostředí SŽDC

Pod pojmem sdělovací zařízení v prostředí SŽDC si můžeme představit soubor technických zařízení, které slouží pro potřeby provozního spojení, systémy sloužící k předávání informací k řízení a organizování drážní dopravy a také systémy, které mají za úkol chránit osoby i majetek. Sdělovací zařízení v prostředí SŽDC lze rozdělit na tzv. „malou sdělovací techniku“ a „velkou sdělovací techniku“. Do první kategorie patří telefonní zapojovače, rozhlasová a informační zařízení pro informování cestujících, kamerové systémy, systémy elektrické požární signalizace (v prostředí SŽDC nazývané také zařízení pro detekci požáru), elektronické zabezpečovací signalizace, autonomní samočinný hasicí systém. Do druhé kategorie patří především přenosová a technologická datová síť, telefonní síť (služební, dopravní).

Pokud se podíváme na stávající železniční sdělovací zařízení všeobecně, bez rozdílu pohledu o jakou železniční trať se jedná (celostátní, regionální), zjistíme, že stav těchto zařízení je velmi různorodý od analogových systémů až po plně digitální (B. Analýza a popis stávajícího stavu sdělovací sítě). V zásadě lze ale říci, že v celé železniční síti bez rozlišení významu trati se používají následující zařízení a systémy:

- Kabelizace (vzdušné vedení, metalická vedení, optická vedení);
- Přenosové systémy;
- Dotykové terminály a zapojovače;
- Telefonní ústředny a hlasové služby;
- Rádiové systémy;
- Informační systémy pro cestující (rozhlasové zařízení, vizuální informační systém);
- Kamerové systémy (KAMS);
- Zařízení pro detekci požáru (ZPDP);
- Elektrická požární signalizace (EPS);
- Elektronická zabezpečovací signalizace (EVS);

- Autonomní samočinný hasicí systém (ASHS)
- Dálková diagnostika technologických systémů železniční dopravní cesty (DDTS ŽDC)
- Dispečerská řídicí technika (DŘT)

Jak předcházející část studie „B. Analýza a popis stávajícího stavu sdělovací sítě“ ukázala je tento rozmanitý stav způsobem zejména vývojem sdělovací techniky a také investicemi do jednotlivých systémů na různých železničních tratích dle jejich významu a kategorie. Samozřejmě, že použití jednotlivých sdělovacích zařízení je odlišné na celostátních a regionálních tratích a to zejména z hlediska rozsahu.

Studie „Sdělovací síť provozovatele dráhy SŽDC, s.o.“ se v níže popsaných kapitolách bude převážně věnovat metodice návrhu výstavby v oblasti kabelizace (metalické, optické), přenosové a datové síti pro drážní aplikace (DŘT, DDTS ŽDC, dálkové ovládání ochrany, dálkový odečet elektroměrů a další), telefonní a rádiové síti, rozšiřování kontrolně analytického centra, dotykovým terminálům, informačním zařízením a kybernetické bezpečnosti.

Ostatní sdělovací technologie (rozhlasové zařízení, EZS, EPS, ASHS) jsou ve studii zmíněny pouze okrajově.

1.2 Kategorie železničních tratí

Železniční dráhy se na základě zákona č. 266/1994 Sb., o dráhách, v platném znění, člení do jednotlivých kategorií z hlediska významu, účelu a technických podmínek, stanovených prováděcím předpisem. Kategoriemi železničních drah jsou:

- a) **Dráha celostátní**, již je dráha, která slouží mezinárodní a celostátní veřejné železniční dopravě a je jako taková označena,
- b) **Dráha regionální**, již je dráha regionálního nebo místního významu, která slouží veřejné železniční dopravě a je zaústěná do celostátní nebo jiné regionální dráhy,
- c) **Vlečka**, již je dráha, která slouží vlastní potřebě provozovatele nebo jiného podnikatele a je zaústěná do celostátní nebo regionální dráhy, nebo jiné vlečky,
- d) **Speciální dráha**, která slouží zejména k zabezpečení dopravní obslužnosti obce.

Pro účely studie bude zpracovatel používat pouze kategorie drah celostátní a regionální.

2 KABELIZACE

2.1 Metalická dálková kabelizace

Podél celostátních tratí a částečně i tratí regionálních jsou položeny metalické kabely dálkového typu. Jejich plášťová ochrana proti indukčním vlivům střídavé trakce a vedení VVN je při souběhu s tratí elektrifikovanou střídavou trakční soustavou 25kV na dobré úrovni. Byly používány kabely s hliníkovým pancířem, které mají vysoký redukční činitel. U tratí neelektrifikovaných byly pokládány kabely s olověným pancířem, které mají redukční činitel nižší, což nevadí, pokud trať nebyla dodatečně elektrifikována.

Přenosové vlastnosti těchto kabelů jsou oproti dnes používané traťové kabelizaci výborné, nicméně význam těchto kabelů v dálkovém spojení je v současné době nízký, využívají se především pro nf okruhy starších analogových technologií. Vf technologie využívající nepupinované čtyřky byly postupně nahrazeny moderními přenosovými systémy (metalické trakty PDH, modemy HDSL, xHDSL apod.). Pupinace je dnes na překážku využívání těchto čtyřek.

Kapacita dálkových kabelů se pohybuje nejčastěji od 20 do 40 čtyřek v provedení DM, XV nebo XPI. Obecně lze říct, že přenosová kapacita okruhů, které lze na kabelu provozovat je malá a zcela nedostačuje požadavkům na moderní provozovaná zařízení.

Navíc stárí těchto kabelů je značné. Převážná většina těchto kabelů byla položena v šedesátých a sedmdesátých letech, některé kabely byly položeny až v letech osmdesátých. Poslední dálkové metalické kabely byly položeny v r. 1991. Jedná se tedy většinou o zařízení na hraně životnosti.

Na technický stav těchto kabelů v řadě případů měla negativní dopad i stavební činnost při modernizaci železničních tratí v posledních dvaceti letech, kdy došlo k mnoha přeložkám těchto kabelů a tím i ke zhoršení parametrů a zvýšení poruchovosti těchto kabelů. V některých úsecích již musely být tyto kabely provozně opuštěny. V jiných úsecích jsou využívány tyto kabely jen v mezistaničním styku jako rezerva nebo doplnění traťových kabelů. V řadě případů však nebyl ve stavbách převeden celý provoz z těchto kabelů do nových traťových kabelů a DOK a tak jsou i nadále udržovány. Na řadě tratí v současnosti jsou i dnes jediným přenosovým médiem.

Výroba těchto kabelů byla víceméně ukončena, pouze omezené množství kabeloven je na objednávku schopné vyrobit náhradní délky kabelů pro opravy a přeložky. Cena kabelových délek těchto kabelů je vysoká. **Výhledově se jednoznačně jedná o dožívající kabelovou síť, jež význam klesá a která se již neobnovuje a dále nebude rozvíjena.**

2.1.1 NAVRHOVANÝ STAV

Studie jednoznačně navrhuje postupné převedení provozu z metalických DK do přenosového zařízení provozovaného po diagnostickém optickém kabelu (dále jen DOK), případně do nověji budovaných traťových kabelů (dále jen TK) a tím i zcela opuštění těchto DK. Dojde tak jednoznačně k úspoře provozních nákladů na údržbu těchto kabelů i úspoře investičních nákladů ve stavbách při jejich nákladných přeložkách.

Tam, kde tyto kabely tvoří dnes jedinou variantu pro provozování telematických služeb, je třeba realizovat pokládku nových TK a DOK a vytvořit tak podmínky pro jejich náhradu dříve než zcela dožijí a nebude možné je dále udržovat v provozu. Vlastní převedení provozu z nahrazovaných kabelů, zejména DK musí být vždy zahrnuto do projektové dokumentace staveb nové kabelizace.

Ke zrychlení nutnosti náhrady těchto kabelů může přispět i navrhovaný přechod ze stejnosměrné trakční soustavy na střídavou, který řešený samostatnou studií „*Koncepce přechodu na jednotnou napájecí soustavu ve vazbě na priority programového období 2014-2020 a naplnění požadavků TSI ENE*“.

2.2 Traťové metalické kabely

Traťové kabely jsou kabely v celoplastovém provedení se čtyřkami typu XN s měděnými žilami. Z hlediska útlumu jsou používány pouze žíly s průřezem 0,8mm. Přenosové vlastnosti těchto kabelů jsou principiálně horší než přenosové vlastnosti kabelů dálkového typu, pro krátká mezistaniční spojení (cca 10km) jsou však dostatečné. V souběhu s železniční tratí, která je elektrifikovaná střídavou trakční soustavou nebo v blízkosti linek VVN jsou používány kabely v provedení s ochranným pancířem z hliníkových drátů, který má výhodný redukční činitel. U ostatních železničních tratí byly pokládány kabely bez tohoto ochranného pancíře.

Traťové kabely této konstrukce začaly být budovány při modernizaci železničních koridorů v první polovině 90-tých let. Stáří traťových kabelů je v průměru 10-15 let. Ojedinele jsou v síti kabely z osmdesátých let, kdy byly z úsporných důvodů místo dálkových kabelů již kladeny celoplastové kabely starších konstrukcí. Nejstarší používané kabely jsou v provedení TCEKEZE nebo TCEKE. Postupně však bylo zavedeno používání kabelů dvouplášťových s protivodní zábranou (gelem) v duši kabelu a s izolací žil pěnovým polyethylenem. Dnes jsou systémově nepoužívanějšími typy kabely v provedení TCEPKPFLEZE respektive TCEPKPFLEY (na železničních tratích se stejnosměrnou trakční soustavou).

Kapacita traťových kabelů se pohybuje nejčastěji v profilech 10XN a 15XN. Zřídka, jsou použity kabely s větší kapacitou – 20XN a 25 XN, většinou jen v železničních uzlech nebo místech rozbočení železničních tratí.

Na regionálních tratích je častá kapacita 5XN nebo i 3XN, která zajišťuje alespoň nejnutnější spojení kolem železniční trati. V mnoha případech se jedná o provizorní kabely kladené pokladačem do šterkového lože, nebo tzv. „pohozáky“, což jsou kabely připevněné k patě kolejnici nebo závěsné kabely na zbytcích starých sloupových tras.

Obecně lze říct, že stav metalické traťové kabelizace u celostátních tratí je pro současné potřeby uspokojivý a vzhledem k vývoji technologií dostačuje i kapacitně, hlavně na tratích, kde je souběžně v provozu optická kabelizace. Problémy s kapacitou se objevují pouze na regionálních tratích, kde je mnohdy použit malý profil kabelu, nebo kde je využíván stávající dožívající dálkový kabel a nová kabelizace nebyla zatím vybudována. V řadě případů není podél regionálních tratí žádné kabelové vedení.

S nástupem IP technologií a jejich používáním nejen v železničních stanicích, ale i na zastávkách, napájecích stanicích a trakčních měnících dochází v poslední době k poklesu požadavků na počet okruhů, které jsou přenášeny po metalických kabelech.

Ukončování kabelů se provádí zářezovou technologií. Ochrana proti přepětí na žilách se řeší využitím bleskojistik.

2.2.1 NAVRHOVANÝ STAV

Za stávající situace je traťová kabelizace budovaná ve stavbách modernizací, elektrizací, optimalizací, revitalizací... technicky i kapacitně dostačující. Vzhledem k plánovanému přechodu na střídavou trakční soustavu již do budoucna navrhujeme budovat pouze traťovou kabelizaci v provedení TCEPKPFLEZE XN0,8. Pouze na železničních tratích, u kterých se elektrizace jednoznačně neplánuje a nevyskytují se v oblasti vlivů střídavé trakční soustavy nebo indukčních vlivů vedení VVN s hodnotou ovlivnění přesahující normou povolené meze, lze budovat kabely v provedení TCEPKPFLEY XN0,8.

U kabelů TCEPKPFLEZE je třeba řešit propojování Al pancíře a jeho zemnění v souladu s platnými normami.

Výhledově je ekonomicky vhodné sledovat možnost snížení dimenze traťových kabelů na 10XN0,8, což pro nastávající období považujeme za minimum (v odůvodněných případech doložených obsazovacím plánem je možno použít i vyšší dimenzi). Část okruhů, jako traťový a nehodový spoj, měřicí čtyřka i okruhy pro zabezpečovací zařízení apod. bude realizována i nadále po metalických kabelech. Metalický kabel je možno rovněž využít jako vytyčovací vodič souběžně pokládaných optických kabelů. Zároveň mohou sloužit jako pohotovostní rezerva, po které je možno zprovoznit rychle bez nutnosti technologických dodávek potřebné operativní okruhy v případě stavebních úprav na železničních tratích nebo v případě havarijních stavů.

2.3 Dálková optická kabelizace

Počátky budování dálkové kabelizace se datují do první poloviny 90-tých let minulého století. V současné době jsou optické kabely položeny takřka podél všech koridorových tratí. Na ostatních železničních tratích je situace znatelně horší. Většinou byly optické kabelizace budovány ve stavbách modernizací, optimalizací, elektrizací a revitalizací tratí, stavbách dálkového ovládání zabezpečovacího zařízení (dále jen DOZ), GSM-R nebo při větších rekonstrukcích. Pouze výjimečně byly budovány v samostatných stavbách. Zdaleka však nejsou pokryty ani všechny objížděné tratě železničních koridorů, natož regionální tratě. V dálkové síti jsou používány kabely s jednojádrovými (dále jen SM) vlákny.

V železniční síti jsou většinou využívány kabely, které jsou zafukovány do HDPE trubek. V některých případech, zejména tam, kde pro pokládku kabelů bylo použito kolejového pokladače a kabely se kladly do vzdálenosti cca 2,2 - 2,8m od osy koleje se používal DOK pro přímé uložení do země. Postupem času se projeví slabiny tohoto řešení. Není možné jednoduchým způsobem vyměnit kabel v případě potřeby navýšení dimenze kabelu bez nových zemních prací a v případě jakýchkoliv úprav železničního svršku, spodku nebo mostů a

železničních přejezdů bývá optický kabel většinou poškozen a musí se před zahájením stavebních prací překládat.

V několika málo případech byl pokládán kombinovaný kabel, obsahující metalické i optické prvky. Ani toto řešení se v praxi neosvědčilo.

Rovněž využití závěsných optických kabelů se nejeví jako vhodné řešení. Přineslo sice zrychlení výstavby optické sítě, ale ukázalo se, že přenosové parametry optického kabelu s věkem klesají, životnost kabelu je kratší a poruchovost spojená např. s pádem stromů na vedení, lovem zvěře apod. je výrazně vyšší. Problematické momenty byly v počátečních fázích budování dokonce spojeny i se samotnou realizací (zvýšený útlum v bodech uchycení kabelu, problémy s nevhodnou konstrukcí pláště některých typů kabelů).

V rámci velkých modernizačních a obdobných staveb byly uloženy do výkopu pro DOK převážně dvě HDPE trubky, jedna byla vždy určena pro obsazení samotným optickým kabelem, druhá trubka byla ukládána jako rezervní. U některých regionálních tratí však byla kladena trubka pouze jedna. V některých případech, včetně I.TŽK jsou již obsazeny obě HDPE trubky. Většinou se jedná o úsek, kde byl v dřívějších dobách položen málo kapacitní kabel a který byl později doplněn kabelem s vyšším počtem vláken.

Samostatnou kapitolou je optická síť společnosti ČD-Telematika a.s. (dále jen ČD-T). V jejich kabelech je smluvně vyhrazeno 6 vláken pro potřeby SŽDC. Jedná se o kapacitně malé množství vláken, která jsou využívána, někde ovšem umožňují jediné optické spojení, nicméně koncepčně se nejedná o zásadní přínos k řešení sítě SŽDC a dále se jimi nebudeme ve studii zabývat.

2.3.1 NAVRHOVANÝ STAV

Tato studie doporučuje nadále realizovat výhradně DOK určený pro zafouknutí do HDPE trubky. Pouze ve zcela výjimečných a odůvodněných případech (zejména v případě provizorního řešení, kde jde o rychlost realizace, nebo překlenutí majetkově neprojednatelného území) lze budovat závěsný optický kabel nebo optický kabel přichycený přímo ke kolejnici.

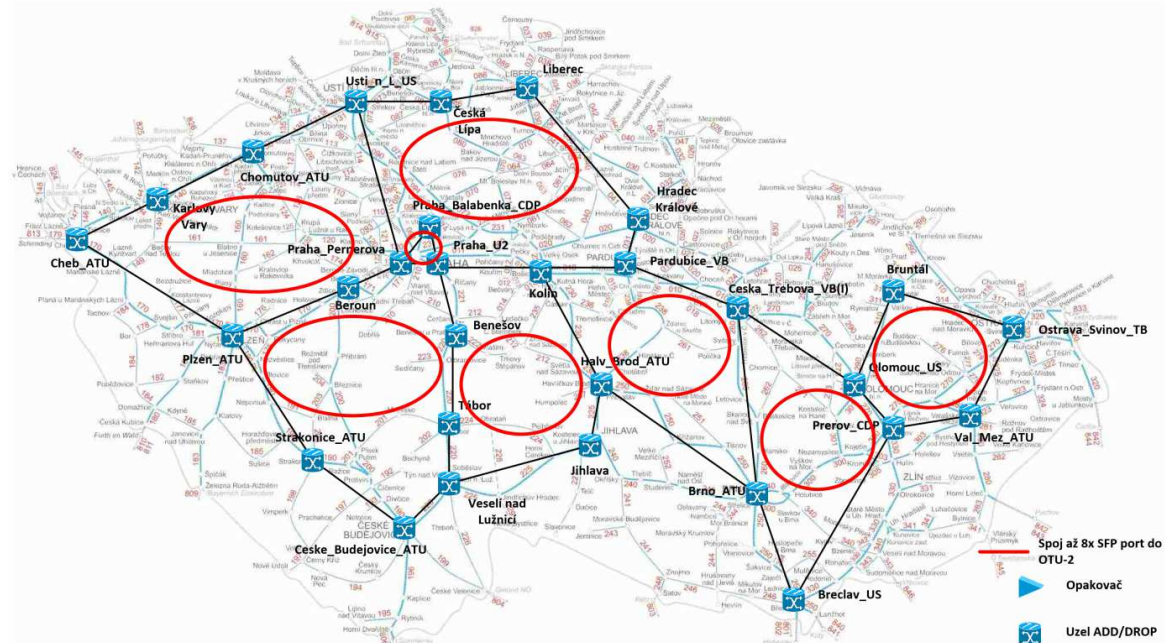
Proto ve všech stavbách v prostředí SŽDC (investiční, opravné práce), ve kterých je realizována kabelová trasa sdělovacích nebo zabezpečovacích kabelů se souvislým výkopem delším 500m a nejsou podél železniční trati položeny HDPE trubky, musí být do výkopu přikládány minimálně dvě HDPE trubky s průměrem 40mm a v barevném značení dle předpisu SŽDC (modrá provozní a černá rezervní). Pokládka HDPE trubek musí být řešena v obvodu staveniště i pro odbočné tratě. V případě souběhu více trubek je možné další rozlišení například barevnými pruhy. Použité trubky musí splňovat podmínky technické specifikace vydané SŽDC, Odborem 14. Rovněž je nutno v těchto stavbách společně s pokládkou HDPE trubek řešit účelně náhrady stávajících metalických kabelů (DK, TK za hranicí životnosti, provizorních u paty koleje, pohořových, ve špatném technickém stavu) v souladu s kapitolami 2.1.1 a 2.2.1 předmětné studie. Ekonomické hodnocení takové stavby by nemělo mít dopad na vyjmutí části sdělovací kabelizace a HDPE trubek při výkopu kabelové trasy. Investice a opravné práce by měly být koordinovány tak, aby nedocházelo k opakovaným výkopovým pracím v témže úseku, tj. kabeláž řešit komplexně.

2.3.1.1 Topologie a rozvoj sítě

V rámci návrhu tranzitní úrovně přenosové sítě SŽDC byly stanoveny lokality uzlů přenosového zařízení SDH STM-16, v rámci stavby KAC také lokality přenosových uzlů DWDM a v nižší úrovni i přenosových uzlů IP/MPLS, stanoveno bylo současně trasování jejich propojení. Základním předpokladem je u všech tří páteřních úrovní přenosové sítě SŽDC zaokružování všech větví z důvodu redundance spojení. Aby bylo možno tyto požadavky splnit, je třeba podél těchto páteřních tras zejména v úrovni DWDM dobudovat optické sítě, po kterých bude zařízení provozováno.

Vedení těchto základních tras je patrné z přiloženého obrázku (Obr. 1). Současně odpovídá potřebě doplnění optických tras vedených podél koridorů a objízdných tras koridorů, aby byly naplněny požadavky interoperability těchto páteřních dopravních tras Českou republikou (viz směrnice TSI).

Současně je nutno pokračovat v budování optických tras i podél regionálních tratí. Zde je vhodné postupovat tak, aby nově vybudované prvky optické sítě byly napojeny na již existující část optické sítě. Zejména je třeba se soustředit na napojení již vybudovaných úseků optických kabelů, které jsou zatím izolovány od ostatní optické kabelové sítě. I v nižší úrovni optické sítě je vhodné a žádoucí budovat obchodní trasy, které umožní zaokružování spojení, alespoň tam, kde je to možné z pohledu topologie železniční sítě. Takový požadavek kruhové redundance bude zřetelně vystávat i z důvodu dalších technologií např. v souvislosti s dalším budováním systému GSM-R podél dalších, nekoridorových tratí.



OBR. 1 – TOPOLOGIE PŘENOSOVÉ SÍTĚ (CÍLOVÝ STAV)

Zvláštní kapitolou jsou optické kabelizace ve velkých železničních uzlech. I zde je při návrhu kabelových tras vhodné zvážit kruhovou topologii páteřní trasy, tak aby do ní bylo možno

v jednotlivých uzlových bodech zaústit všechny kabely z jednotlivých tratí při současném požadavku bezpečnosti zálohování směrů.

2.3.1.2 Kapacita DOK

První DOK, kladené v první polovině devadesátých let minulého století, měly kapacitu 12 vláken, později 24 a 36. Navyšování dimenze používaných kabelů se tak měnilo zhruba každých pět let, s tím, že tato kapacita je dostatečná. Dnes je směnicí SŽDC požadovaná kapacita 48 vláken byla zatím zrealizována jen u několika nejnovějších staveb. V rámci staveb rádiového systému GSM-R byly na koridorových tratích zafouknuty doplňující optické kabely, někdy i s kapacitou 72 vláken. Toto postupné měnění kapacity kabelu společně s postupnou výstavbou DOK vytvořilo úzké hrdlo všude tam, kde je kapacita kabelu nízká a již nepostačuje potřebám provozu. Nejednotný profil kabelu také způsobuje nejednotnost v obsazování a vyvádění optického kabelu.

Jaký je stav obsazenosti stávajících DOK na páteřních trasách lze zdokumentovat například na úseku trati Tlumačov – Přerov. Zde byl v devadesátých letech položen optický kabel o kapacitě 12 vláken, ve stavbě GSM-R v roce cca 2010 byl do rezervní trubky zafouknut optický kabel o kapacitě 36 vláken. Kromě těchto vláken jsou k dispozici i tři páry vyhrazených vláken v kabelu ČD-T. Obdobná je i situace na jiných místech. Následující údaje v Tab. 1 a Tab. 2 byly dodány správcem kabelu.

TAB. 1 – OBSAZENÍ KABELU 36 VLÁKEN TLUMAČOV – PŘEROV

VLÁKNA	ZPŮSOB VYUŽITÍ
1.-8.	ZABEZPEČOVACÍ ZAŘÍZENÍ
9.-10.	STM-4 ZABEZPEČOVACÍ ZAŘÍZENÍ
11.-12.	ETCS 2.KORIDOR
13.-14.	VOLNO (REZERVA)
15.-16.	STM1
17.-18.	VOLNO (REZERVA)
19.-20.	STM4 (DOZ)
21.-24.	DOZ VLÁRSKÁ TRATĚ
25.-26.	INTRANET
27.-28.	STM-16
29.-34.	DWDM - KAC
35.-36.	STM-4 ONS

TAB. 2 – OBSAZENÍ KABELU 12 VLÁKEN TLUMAČOV - PŘEROV

VLÁKNA	ZPŮSOB VYUŽITÍ
1.-2.	VOLNO (REZERVA)
3.-4.	STM-16 PRO DOZZ
5.-6.	VOLNO
7.-8.	KAC
9.-10.	KAC (ZÁLOHA)
11.-12.	PRONÁJEM

Obsazené jsou i 3 páry vláken SŽDC v optickém kabelu ČD-T. Z uvedeného vyplývá, že za volné se dá považovat maximálně 5 párů ze 48 vláken, pomíneme-li pár pro měření a případně rezervní havarijní vlákna. Navíc v současnosti jsou na tomto rameni připravované další stavby, zejména stavba Elektrizace trati Otrokovice – Vizovice, která bude mít další požadavky na vlákna pro zab. zařízení a DOZ z CDP Přerov. Další požadavky na optická vlákna vznášejí odvětví silnoproudé technologie, které jej požaduje pro vazbu napaječů z důvodu velké časové odezvy u okruhů vedených přes přenosové zařízení (tato problematika je řešena v samostatné kapitole 5.2). Po ukončení této stavby tedy budou oba kabely v podstatě plné. Je samozřejmě možné diskutovat o skutečnosti, že při optimalizaci okruhů by bylo možno za cenu dalších investic do zařízení obsazení vláken snížit, ale příliš to nezmění na skutečnosti, že je kabel 48 vláken na páteřní trase již plný bez případných rezerv do budoucnosti. Navíc uvažuje-li se s výhledem do roku 2030 a s případnými novými technologiemi, které zcela jistě přijdou a které dnes nedokážeme zatím konkretizovat, natož stanovit jejich požadavky na optickou cestu. Z uvedeného je zcela zřejmé, že stávající kapacita 48 vláken je na celostátních tratích do budoucna **ZCELA NEDOSTAČUJÍCÍ**.

Současné je jasné, že stávající množství HDPE trubek je vyčerpáno a při výměně kabelu bude nutno řešit, jak zajistit náhradní provoz stávajících okruhů, které jsou např. na kabelu 12 vláken provozovány, aby jej bylo možné vyfouknout a vyměnit za kapacitnější kabel.

Pokud započítáme minimální rezervu v obsazenosti 30%, potřebujeme navýšit kapacitu minimálně o 14 vláken. Máme-li zamezit dalším přechodovým stavům, při případném dalším navýšení kapacity v budoucnu za pět let je vhodné stanovit minimální kapacitu DOK realizovaného ve stavbách na 72 vláken.

Přitom finanční rozdíl mezi dnes budovanými kabely 48 vláken a nově navrhovanými 72 vlákny je minimální, jak dokládá následující Tab. 3.

TAB. 3 – CENOVÉ SROVNÁNÍ DOK 48 VLÁKEN A 72 VLÁKEN

DRUH PRACÍ	MĚRNÁ JEDNOTKA	ROZDÍL CEN [KČ]	ROZDÍL CEN NA ÚSEK V KČ NA 10 KM
ZEMNÍ PRÁCE	M	0	0
HDPE TRUBKY	M	0	0
KABEL MATERIÁL	M	10	100 000
ZAFOUKNUTÍ	M	0	0
SVÁR	KS	1 000	72 000
ROZVADĚČ+PIGTAIL	KS	1 500	36 000
MĚŘENÍ	VLÁKNO	500	12 000
CELKEM			220 000
CELKEM NA METR			22

Z toho plyne, že cenový rozdíl je zanedbatelný. Na základě těchto faktů navrhujeme stanovit minimální kapacitu dle následující Tab. 4.

TAB. 4 – NAVRHOVANÁ KAPACITA DOK

TRATĚ	KAPACITA OPTICKÉHO KABELU	POZNÁMKA
TRATĚ REGIONÁLNÍ KONCOVÉ	48 VLÁKEN	BEZ MOŽNOSTI
TRATĚ CELOSTÁTNÍ A REGIONÁLNÍ	72 VLÁKEN	S MOŽNOSTÍ ZAOKRUHOVÁNÍ
KORIDOROVÉ TRATĚ	72 VLÁKEN	
VRT	72 VLÁKEN	OBOUSTRANNĚ
VNITŘNÍ OKRUH VE VELKÝCH ŽEL. UZLECH	144 VLÁKEN	DLE MÍSTNÍCH PODMÍNEK

Přičemž, považujeme za důležité stanovit minimální kapacitu DOK i pro koridorové tratě. Koridory jsou sice již z větší části dokončené, nicméně patrně dojde k výměně stávajících kabelových tras podél minimálně poloviny koridorových tratí v souvislosti se změnou stejnosměrné trakční soustavy na střídavou.

U tratí VRT je zpracovávána samostatná studie, na budování tratí VRT, nicméně vzhledem k možnosti zaokružování provozu i podél těchto tratí považujeme za důležité stanovit minimální kapacitu DOK v této Studii.

Vnitřní okruh ve velkých železničních uzlech (Praha, Brno, Ostrava ...) propojující nejvýznamnější technologické a administrativní objekty v uzlu doporučujeme z důvodu bezpečnosti budovat všude tam, kde to má z topologického hlediska význam. Kapacita je volena s ohledem na počet zaústění tratí a tedy DOK do uzlu (za minimum je uvažováno s dvěma DOK v jednom objektu).

2.3.1.3 Rezervy na trase a spojky

Systémově je třeba využívat co největší kabelové délky, aby byl minimalizován počet spojek a tím i útlum optické trasy u dlouhých okruhů. Na druhé straně zafukování dlouhých kabelů v terénu může přinášet problémy. Vhodné je využít i umístění dělicích spojek jako spojky rovných na trase, pokud to délkově při alokaci vychází. Navrhujeme systémově využívání kabelových délek 4-6km. Kratší délky lze využívat k doplnění délky a v odůvodněných případech, schválených správcem.

K situování spojek je vhodné využít drážní pozemek a místo pokud možno přístupné k příjezdu vozu s měřicí technikou.

Spojky a rezervy se umísťují do kabelových plastových komor a osazují se markery.

Dle platné TNŽ se rezervy umísťují u mostních objektů, v případě propustků to není vyžadováno. V případě DOK je vhodné tuto praxi zachovat. Na HDPE trubkách není možné z důvodu poloměru ohybu a budoucího zafukování rezervy umísťovat. Rezerva se tedy buduje pouze na kabelu v kabelové komoře a kabel se v případě potřeby potáhne či pofoukne. Je tedy vhodné kabelovou rezervu pro několik mostů v blízkosti sdružit.

Rezervy je vhodné zanechat i v místech, ve kterých se dá očekávat v budoucnu manipulace s kabelem, např. u přejezdů nebo v zastávkách, kde se kabel zatím nevyvádí.

2.3.1.4 Ukončování

V současné době se DOK ukončuje převážně na modulárních optických rozvaděcích s konektory E2000 APC. Tento stav je zcela vyhovující. Složitější je otázka umísťování rezerv DOK a MOK na optické kříže na stěně. U malých železničních stanic tato praxe není až tak problémová, ale u velkých železničních stanic bývají rozsáhlé úseky stěn sdělovacích (telekomunikačních) místností pokryty rezervami a už není možné umísťovat novou technologii. Doporučujeme v takových případech zvážit systémové nasazení stojanu, či upraveného rozvaděče, tak aby v ní bylo možné soustředit větší počet rezerv a současně ukončit HDPE trubky ve spodní části (viz kapitola 17). Obdobné řešení je využíváno například v objektech společnosti CETIN.

2.3.1.5 Vyvádění a obsazení vláken

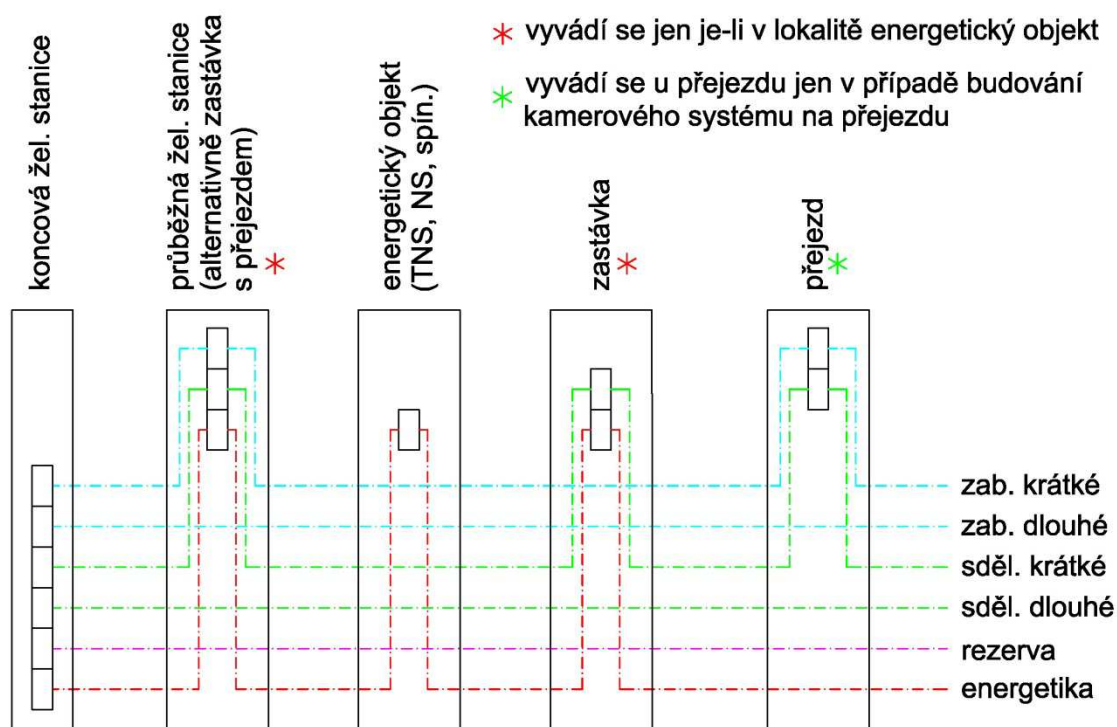
Používaný kabel by měl obsahovat 6 bufferů po 12 vláknech. Některé vlákna respektive buffery jsou již dnes vyhrazeny pro zabezpečovací zařízení, přičemž je předepsáno, že nemají být ukončeny nikde jinde, než v prostorech zabezpečovací techniky. Jedná se o vlákna 1-12 a dále o šest vláken z bufferu, který je dnes určen pro vyvádění v mezistaničních úsecích (tedy u přejezdů a v zastávkách).

V případě vláken pro zabezpečovací účely, právě kvůli předpisům určujícím, kde musí být vyváděny, musí dojít k jejich přesnému určení. Nevýhodou je ztráta variability. Tento stav je zachován i v novém návrhu vyvádění a obsazování vláken. Dělení jednoho bufferu při vyvádění není optimální a přináší problémy, navíc v některých případech je počet vláken pro zabezpečovací zařízení již vyčerpán. V novém návrhu jsou pro tuto techniku proto vyhrazeny dva celé buffery, přičemž v jednom jsou preferovány dlouhé spoje.

Nově se objevuje požadavek na skupinu vláken určených pro potřeby energetiky, konkrétně pro přenos vazby napáječů a ochran. Nejedná se ale o striktní vyčlenění jako v případě zabezpečovací techniky. Předpokládá se, že tato vlákna budou kromě energetických objektů vyváděna i ve sdělovacích místnostech. Nechceme další vyčleněná vlákna, která budou komplikovat obsazování kabelů. Přesto považujeme za užitečné zvážit určení skupiny, z které budou vlákna v případě potřeby poskytována. Přednostně by měla být využívána vlákna ze skupiny sdělovacích traťových vláken.

Variantou je v případě pokládky magistrálního rozvodu 22kV, který umožňuje zafouknutí optického mikrokabelu, zafouknutí samostatného OK s 12 vlákny smyčkovánými shodně s kabelem 22kV.

Následující obrázek Obr. 2 shrnuje principiální místa vyvádění vláken a účel jejich vyvádění:



OBR. 2 – SCHÉMATICKÉ VYVÁDĚNÍ VLÁKEN DOK

V následující tabulce Tab. 5 je zobrazen návrh zásad obsazování vláken ve dvou variantách. Tento návrh si neklade za cíl určit závazný obsazovací plán, spíše se snaží podnítit diskusi na toto téma a vytvořit jakousi startovací pozici. Má-li nastat v této oblasti jednotnost, aby nevznikaly nelogické disharmonie v různých úsecích, je třeba se touto problematikou zabývat. Obecně platný způsob vyvádění a rozvláknění DOK bude určen novelizovaným výnosem SŽDC, O14.

TAB. 5 – NÁVRH ZÁSAD OBSAZOVÁNÍ VLÁKEN

	VARIANTA 1 - MIN. ZMĚN	VARIANTA 2 - SYSTÉMOVÁ
1-12VL.	ZABEZPEČOVACÍ TRAŽOVÉ	ZABEZPEČOVACÍ TRAŽOVÉ
13-24VL.	SDĚLOVACÍ TRAŽOVÉ	ZABEZPEČOVACÍ DLOUHÉ
25-36VL.	SDĚLOVACÍ DLOUHÉ	TRAŽOVÁ VLÁKNA
37-48VL.	REZERVA	SDĚLOVACÍ TRAŽOVÉ
49-60VL.	ZABEZPEČOVACÍ DLOUHÉ	SDĚLOVACÍ DLOUHÉ
61-72 VL.	SDĚLOVACÍ DLOUHÉ	DLOUHÁ VLÁKNA

Varianta 1 se snaží maximálně respektovat stávající směrnici SŽDC pro obsazování kabelů 48 vláken, aby se snížila potřeba zasahovat do obsazení kabelu a vyvádění vláken při přechodu na 72 vláknový kabel. Druhá varianta se snaží poskládat skupiny vláken logicky k sobě, vyžaduje však větší zásahy do stávajících kabelizací (převaření konců kabelů v rozvaděčích a přepojení okruhů na jiná vlákna z důvodu jednotnosti).

V každém případě je potřeba na stávajících kabelech provést jakousi základní optimalizaci, a to z důvodu přeskládání obsazení do jednotné podoby a z důvodu úspory vláken. Tato optimalizace musí být provedena vždy při realizaci jakékoliv stavby, která do provozu DOK zasahuje, a to v rozsahu stavby.

2.4 Místní kabelizace metalická

V místní síti v jednotlivých železničních stanicích se vyskytují kabely různých provedení a konstrukcí, poplatných době pokládky. Problematická situace je zejména ve velkých železničních uzlech. V některých případech jsou ještě v provozu kabely s hliníkovými žilami o průřezu 1,06. Poměrně často se vyskytují kabely s oloveným pancířem nebo hliníkovým pancířem a papírovou izolací měděných žil. Stáří těchto kabelů dosahuje 40 i více let. V pozdější době byly kladeny kabely v celoplastovém provedení TCEKE nebo TCEKEZE. Ve většině případů jsou použity kabely čtyřkované s průřezem žil 0,8. V některých případech (pro hodiny, EZS nebo signalizace) byly kladeny i kabely párované s žilami 1,0. V 90-tých letech se v rámci železničních staveb modernizací a obdobných velkých staveb započalo s pokládkou moderních celoplastových kabelů s protivodní zábranou gelem a s izolací žil pěnovým polyethylem. Zde již byl z ekonomických důvodů snížen průřez žil na 0,6. Což je z útlumových důvodů u kratších kabelů dostatečné.

U tratí, které jsou elektrifikovány střídavou trakcí nebo v blízkosti linek VVN jsou používány kabely v provedení s ochranným pancířem z hliníkových drátů, který má výhodný redukční činitel. U ostatních tratí byly pokládány kabely bez tohoto ochranného pancíře.

Tyto kabely propojují jednotlivé objekty v železničních stanicích, případně připojují do sítě venkovní telefonní objekty, výtahy apod. Slouží převážně pro hlasovou komunikaci, či řízení dopravy.

S nástupem IP technologií a snižováním počtu železničních pracovníků dochází v poslední době k poklesu požadavků na počet okruhů, které jsou přenášeny po metalických kabelech.

Ukončování kabelů se provádí zářezovou technologií. Ochrana proti přepětí na žilách se řeší využitím bleskojistik.

Kapacita stávajících kabelů je většinou dostatečná, místy spíš nadbytečná. V modernizovaných stanicích je také většinou v dobrém technickém stavu. U nemodernizovaných tratí je kabelizace většinou zastaralá. Nejsložitější je situace ve velkých uzlech, kde byly v kolejišti často kabely obnoveny novými typy kabelů, ale v napojení různých areálů zůstávají zastaralé typy kabelů na hranicích životnosti.

2.4.1 NAVRHOVANÝ STAV

Nové kabelizace budou i nadále budovány dle současných zvyklostí, tedy v provedení TCEPKPFLEZE nebo TCEPKPFLEY. Jejich kapacita bude převážně nižší a musí vycházet ze stávajících požadavků na okruhy. V blízké budoucnosti se dá očekávat vydání předpisu, který sníží ve stanicích počty venkovních telefonních objektů, což dále omezí rozsah místních kabelizací.

Nová kabelizace bude budována převážně v rámci rozsáhlých železničních staveb, většinou jako vyvolaná investice, případně budou řešeny požadavky na nová připojení nebo náhrada stávajících dožívajících a přitom potřebných kabelizací.

2.5 Místní kabelizace optická

Po nástupu IP technologií se zvýšily požadavky na počty okruhů provozovaných po místních optických kabelech. Největší poptávka je po distribuci připojení do DDTS a sběr dat pro dálkové ovládání jednotlivých zařízení. Ve stanicích se MOK buduje k jednotlivým technologickým a administrativním budovám, trafostanicím, rozvaděčům osvětlení a elektrického ohřevu výměn, stanicím BTS a kamerám.

V 90-tých letech v počátcích budování místní optické sítě, převládal z ekonomických důvodů trend budování sítě místních optických kabelů s gradientními vlákny. Dnes se ceny jednoznačně srovnaly ve prospěch kabelů s jednovidovými vlákny. Do budoucnosti je žádoucí z důvodu variability a snadného propojování budovat pouze MOK s jednovidovými vlákny. Vzhledem k nízkým cenám těchto kabelů měla by být minimální kapacita kabelu 12 vláken (pro EOv a osvětlení je dostačující kapacita 6 vláken).

Technické parametry kabelů, ukončování, umísťování rezerv apod. jsou shodné a měly by být shodné s DOK.

Do budoucna zpracovatel Studie doporučuje zvážit otázku dimenzování HDPE trubek. Běžně se dnes používají trubky HDPE s průměrem 40mm, stejně jako je tomu v dálkové síti. Tyto trubky pro místní kabely jsou však výrazně kratší a dosahují délky maximálně kolem 1 kilometru, většinou jen pár stovek metrů. Pro zafukování tenkých místních kabelů se tedy jedná o poměrně drahý standard. Ve veřejném sektoru se běžně používají trubky HDPE 32mm i HDPE 24mm. Jednak jsou tyto trubky levnější, ale jejich hlavní výhoda je v menších rozměrech. Ve většině stanic se v hlavních kabelových trasách, v kabelovodech, v chráničkách pod kolejemi bojuje s nedostatkem prostoru. Pokud se takových HDPE trubek klade do výkopu víc, může znamenat úspora velikosti

průřezu úsporu otvoru v kabelovodech, nebo počtu chrániček, žlabů a může znamenat i zmenšení šířky výkopu. Tyto finanční úspory již budou vysoké.

Navíc užší HDPE trubka je lépe ohebná. Snadněji se s ní manipuluje a potenciálně může signalizovat ve výkopu oproti HDPE trubce snadnější rozlišení, mezi DOK a MOK a to i při stejné barvě HDPE trubek. Na druhou stranu používání menších průměrů trubek navyšuje sortiment prvků o další prvky, které je třeba držet skladem pro případy oprav.

Druhou alternativou zejména ve větších železničních uzlech je použití mikrotrubičkových systémů. Pro drážní aplikace se nám zdají vhodné pouze z odolné mikrotrubičky s průměrem přes 1cm. Je zachována jejich pevnost, takže v krátkých úsecích z hlavní trasy k zařízení by mohly být ukládány přímo do země. Takovýchto mikrotrubiček je možné zatáhnout či zafouknout do jedné HDPE i 5 - 6 ks. To znamená, že ve společné trase je možno ušetřit cca 15x15cm místa. Jen je třeba mít na zřeteli, že mikrotrubičky musí být instalovány do HDPE trubky současně, není možno je instalovat po částech, respektive jen omezeně, obdobně jako při zafukování druhého kabelu do jedné trubky.

2.5.1 UKLÁDÁNÍ KABELŮ

2.5.1.1 Prostor pro vedení kabelových tras

Při realizaci staveb různého typu bývají budovány poměrně rozsáhlé kabelové trasy. Protože terén kolem železniční trati není uzpůsoben pro bezproblémové vedení těchto tras, dochází zákonitě k problémům se situováním kabelových tras. V případě drážního úzkého drážního pozemku je třeba volit ze dvou špatných variant:

- zatížení stavby projednáváním vstupů na cizí, často i soukromé pozemky;
- nedodržení platných norem a předpisů.

V případě vedení kabelových tras mimo drážní pozemek, byť v ochranném pásmu dráhy, nastává dlouhé vyjednávání s vlastníky, domlouvání podmínek, smluv a vyrovnávání závazků vyplývajících z dočasného záboru či věcného břemene. Tyto komplikace nastávají ve všech fázích projektové přípravy (územní řízení, stavební řízení), ale i při vlastní výstavbě a následně při kolaudaci a v neposlední řadě i v případě údržby.

V projektové přípravě se jedná o dlouhou dobu projednávání, stavby se opoždějí, v některých případech zůstávají dlouhodobě v hibernovaném stavu, kdy stavbu není možné prosadit a pustit do realizace. Jednou z možností řešení je prosadit změnu zákona O drahách, aby stavby železnic byly uznány za veřejně prospěšné. Ale největším usnadněním by bylo prosazení požadavku, že SŽDC má právo ve svém ochranném pásmu budovat své sítě související s dopravou jen na základě oznámení vlastníkům. Vlastníkovi by samozřejmě muselo zůstat právo na náhradu škod a náhradu za věcné břemeno. Jednalo by se o obdobu práv veřejných provozovatelů telekomunikačních služeb.

Ale ani změna zákona nedokáže usnadnit realizaci a následné zřizování věcných břemen, uzavírání smluv a jejich vkládání do katastru nemovitostí. Ne nadarmo zůstává většina staveb

modernizací, nebo kabelizací dlouhodobě ve zkušebním provozu a vypořádávání stavby probíhá ještě mnoho let po dokončení stavebních činností.

Druhou alternativou je ukládání kabelů do svahů, příkopů, narušení sanačních vrstev atd. Ve všech případech se jedná o atypická řešení, která přinášejí obtíže a vícenáklady pro případ údržby svršku či spodku v budoucnu a v některých případech vytvářejí přímo potenciál k havarijním stavům, či poškození kabelů a ovlivnění provozu při poškození kabelu nebo tělesa dráhy při sesuvech svahů, zavodnění drážního tělesa apod.

Proto by bylo velkým zjednodušením, kdyby při výstavbě nových tratí (VRT, zdvojkolejnění...) nebo při rozsáhlých přestavbách stávajících tratí byl systémově přímo v tělese dráhy definován prostor pro ukládání kabelů, který by měl pevně definovanou šířku a polohu a v tomto koridoru by se nenacházely jiné překážky. Znamená to však vypracovat změnu předpisu S4.

V tomto koridoru by mohlo být vybudováno technické zařízení, aby v případě údržby, výměny kabelu nebo další investici bylo možno tuto instalovat bez nutnosti dalších zemních prací. Toto řešení by snižovalo náklady na realizaci těchto sítí, byť místy za cenu zvýšení vstupní stavební investice. Současně je zřejmé, že začlenění takového koridoru nebude možné do všech staveb. Záleží na terénních podmínkách, majetkových poměrech a dalších okolnostech.

2.5.1.2 Technické řešení sdružených kabelových tras v mezistaničních úsecích

Principiálně existují tři druhy řešení společné trasy:

1. Stávající přístup k trasám. Kabely se uloží volně do výkopu. Toto řešení zahrnuje kromě ceny kabelů a jejich montáže pouze zemní práce spojené s výkopem, v některých případech v podpovrchové trase, nebo v okraji komunikací s uložením do žlabů. Nevýhodou je nedostupnost kabelů pro údržbu a dále nutnost opakovat zemní práce v případě oprav nebo doplnění kabelů. Z toho plyne i delší doba potřebná k opravě případných poruch a vyšší náklady na odstranění poruchy. Výhodou je nižší riziko krádeží a vandalizmu, i když jsou známy krádeže i kabelových tras takto uložených.
2. Druhou variantou je vybudování povrchové trasy z pochozích žlabů, do kterých se ukládají kabely. Tento systém je využíván hojně u zahraničních železničních správ. Výhodou je minimalizace zemních prací jak při výstavbě, tak i při případné opravě, či při doplňování dalších kabelů v případě takové potřeby. Zařízení je viditelné v terénu a snadno přístupné pro údržbu. Nevýhodou je navýšení investičních nákladů stavby o cenu tohoto žlabu a hlavně v podmínkách České republiky i riziko krádeží kabelů. Zkušenosti údržby s krádežemi jsou špatné, na druhé straně je faktem, že po změně zákonů počet krádeží významně poklesl. A v budoucnu se je možná podaří takřka eliminovat.
3. Třetí variantou je výstavba kabelovodu s nižším krytím a plastovými přístupovými komorami po cca 80-120m. Pokud bude definován koridor pro vedení trasy v pravidelné vzdálenosti od koleje, bude trasa takřka rovná a tedy i vzdálenost šachet může být větší. Zemní práce budou rozsáhlejší při výstavbě než v předchozí variantě „žlab“. Přístup pro údržbu a výměnu kabelů však bude vyhovující a kabely budou také opticky lépe ochráněny proti krádežím a poškozením. Nicméně ani v tomto případě nebude ochrana

proti možným krádežím stoprocentní. To bude souviset s obtížností a komplikovaností možného přístupu do kabelových komor a tím i zajištění proti neoprávněné manipulaci. Pokud do kabelové komory záškodník vnikne, je schopen vytáhnout celou kabelovou délku k sousední šachtě. Součástí návrhu kabelovodu musí být i požární řešení a protipožární ucpávky.

Požární bezpečnost prostorů takto provedeného kabelového rozvodu je vhodné zvýšit použitím požárního utěsnění vstupů a výstupů ze šachet a tím vytvořením požární přepážky. Upravit požárně bezpečnostní podmínky obdobně jak je uvedeno v ČSN 730848 pro instalaci vedení kabelových tras železničních tratí se jeví jako vhodné v příslušné vyhlášce MD ČR.

Zpracovatel studie preferuje a doporučuje variantu 2 nebo 3 dle místních podmínek, použití těchto možností je však závislé na změně stávajících předpisů a norem SŽDC, zejména předpisu S4. Řeší se v legislativní části studie.

2.5.1.3 Vedení kabelů po mostech

V kapitole: „Prostor pro vedení kabelových tras“ byly popsány obtíže, ke kterým dochází v případě ukládání kabelů do cizích pozemků. Tyto obtíže se stupňují v případě přechodu kabelových tras přes přírodní překážky (potoky, řeky, silnice, hluboká údolí...). Mnohdy nestačí jednat s vlastníky pozemků, ale často i s dalšími orgány a absolvovat další správní řízení. Tento proces se opakuje při každé změně nebo úpravě v budoucnosti.

Jednoznačně je třeba definovat a prosadit, aby prostory pro převedení kabelových tras přímo souvisejících s provozem dráhy byly budovány jako nedílná součást mostních konstrukcí.

Toto se samozřejmě nevztahuje na stávající mostní konstrukce, u kterých by docházelo k velkým a finančně náročným přestavbám, či ke konstrukcím, které jsou v plánu oprav.

2.5.1.4 Vedení kabelů v železničních stanicích a pod zpevněnými plochami

V železničních stanicích je ukládáno do země obzvláště velké množství kabelů různého určení. V řadě míst jsou přitom stísněné podmínky a ukládání kabelů se musí řešit formou kabelovodů. Toto řešení je dnes již běžné a není věcí této Studie řešit konstrukci kabelovodu. Podstatné je, že kabely v oblasti nástupišť, nákladišť a obecně zpevněných ploch budou ukládány tak, aby je bylo možno vyměnit a doplňovat bez nutnosti zemních prací (které jsou ve zpevněných plochách obzvláště nákladné), tedy do kabelovodů.

Dalším důležitým pravidlem by mělo být, že každý kabelovod bude budován s patřičnou rezervou pro všechny kabely, které jím budou i výhledově vedeny a bude obsahovat rezervu minimálně 20%. Což odpovídá zkušenostem na nárůst požadavků na počty kabelů z provozu. Obdobný požadavek na kabelovody je uplatňován i v jiných resortech.

3 PŘENOSOVÝ SYSTÉM A TECHNOLOGICKÁ DATOVÁ SÍŤ

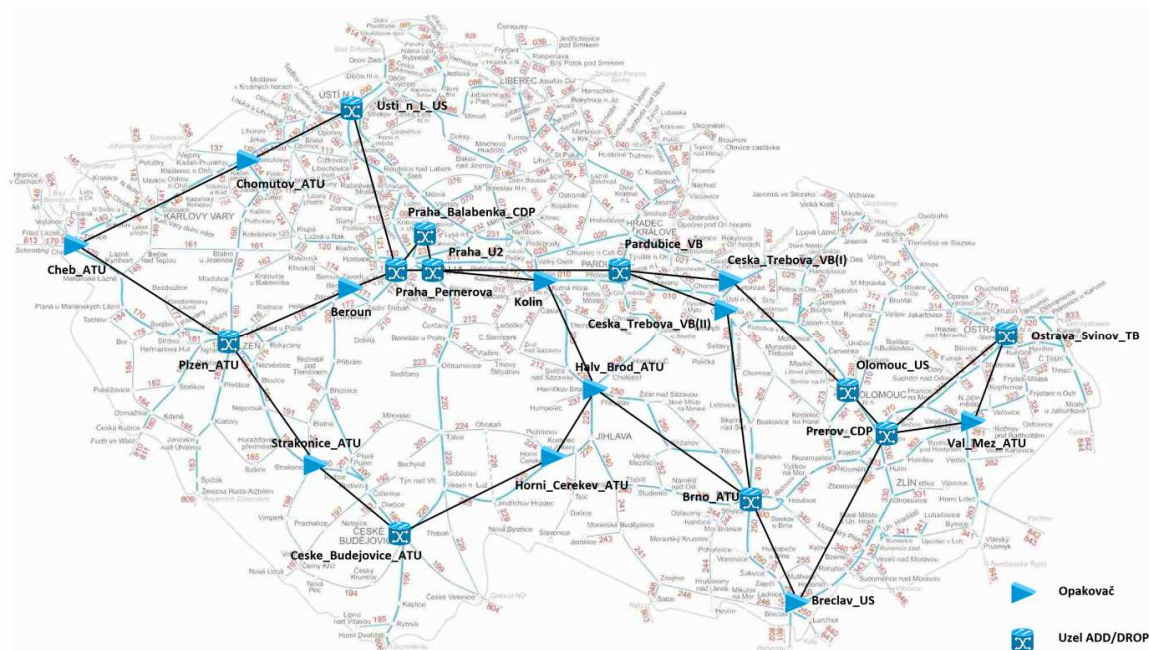
Klíčovým aspektem efektivního zavádění rozsáhlých propojitelných systémů ITS v dopravě vyžaduje dostatečně dimenzovanou a v jakémkoliv okamžiku dostupnou přenosovou síť. Kromě dostatečné kapacity vlastní přenosové sítě, její modernizace je zde ještě otázkou dostupnosti přenosové sítě v menších dopravních uzlech ležící zejména na regionálních tratích.

Dalším aspektem kromě kapacity a dostupnosti odpovídající přenosové sítě je spolehlivost a bezpečnost datových spojení, přičemž s ohledem na požadavky některých dopravních aplikací není možné využít komerčně nabízená řešení. Z těchto důvodů jsou instalovány datové trasy podél jednotlivých železničních tratí.

V současné době jsou přenosové sítě SŽDC tvořeny dvěma hlavními přenosovými systémy. Starší systém budovaný v souvislosti s „*Modernizací a Optimalizací tratí*“ je přenosový systém SDH (synchronní digitální hierarchie). Jednotlivé uzly přenosové sítě SDH jsou provozovány s použitím technologie Cisco ONS 15305 a uzly pro překryvnou síť s rychlostí STM-16 jsou provozovány na technologii Cisco ONS 15454. Přenosové rychlosti v síti SDH jsou STM-1 (menší železniční stanice, BTS rádiového systému GSM-R, energetické objekty), STM-4 (většina železničních stanic) a STM-16 (překryvná úroveň přenosové sítě). Firma Cisco ukončila dodávky uvedené technologie ONS 15305 do ČR, pokračuje se ještě s výstavbou větších přenosových uzlů ONS 15454 v rámci překryvné sítě. I tato technologie však u SŽDC nebude dále nově realizována. V případě dodržení jednotného přenosového traktu se výjimečně nově dobudované SDH používají přenosové zařízení od společnosti Ericsson a to typy SPO 1410 používané jako náhrada ONS 15305 a SPO 1460 jako náhrada ONS 15454. Pro nově připravované stavby se již uvažuje s přenosovou technologií synchronního ethernetu s MPLS protokolem.

3.1 DWDM

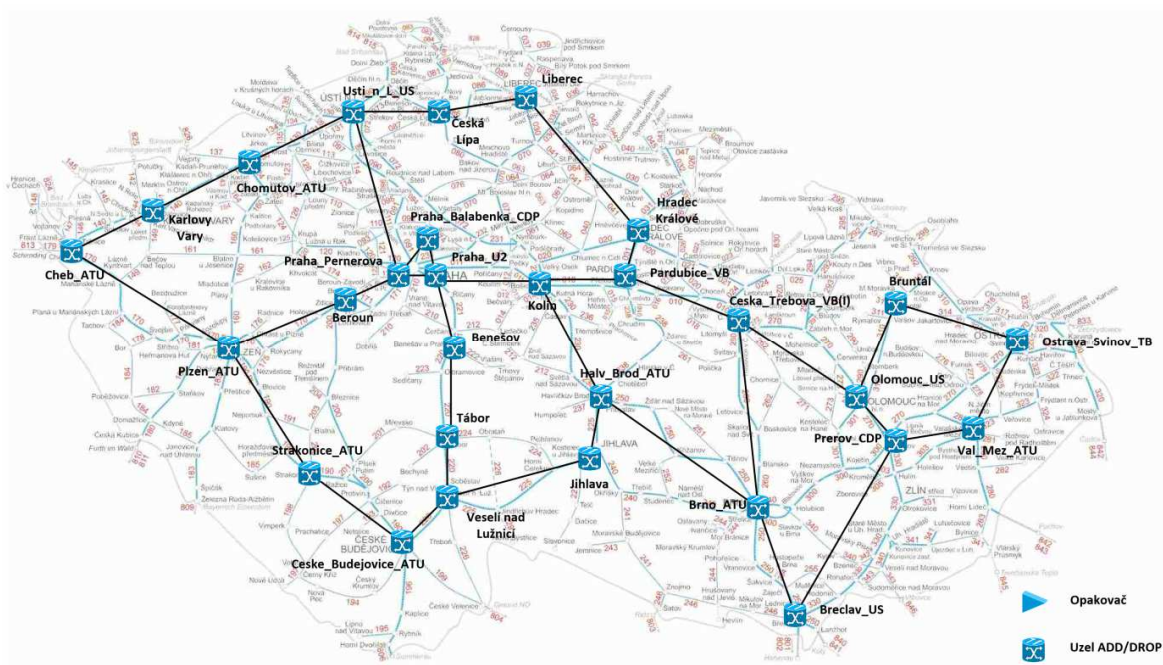
Pro zabezpečení přenosu předpokládaného masivního objemu dat je v rámci sítě SŽDC vybudován na síti stávajících optických kabelů SŽDC a ČD-T přenosový systém DWDM (Dense Wavelength Division Multiplexing) se současnými 11 lokalitami umístění uzlových stanic a dalšími lokalitami, ve kterých jsou instalovány nezbytné opakovače DWDM (celkem 10 lokalit) z důvodu nevyhovujícího útlumu přenosové cesty a z důvodu velké vzdálenosti. V identických lokalitách jsou rovněž vybudovány Core routery MPLS (Multiprotocol Label Switching), které zabezpečují přechod mezi oběma úrovněmi přenosů, tedy mezi úrovní DWDM a nižší agregační úrovní tvořenou technologií MPLS. Samotnou agregační vrstvu pak kromě Core routerů vytvoří síť dalších přenosových bodů MPLS, ve kterých bude prováděn sběr příspěvkových signálů systému KAC a z navazujících železničních tratí. Tyto přenosy budou realizovány zejména jako datové s rozhraním Ethernet.



OBR. 3 – STÁVAJÍCÍ TOPOLOGIE PŘENOSOVÉ SÍTĚ DWDM

3.1.1 NOVÉ TRASY PRO ZAOKRUHOVÁNÍ SLUŽEB A PŘIPOJENÍ VÝZNAMNÝCH LOKALIT

Stávající optická síť SŽDC neumožňuje plnohodnotně připojit další významné lokality a zejména z nedostatku optických propojení mezi těmito lokalitami. Proto je do budoucna nutné provést doplnění optických tras (Kapitola 2) a následně připojení dalších významných lokalit.



OBR. 4 – VYTVOŘENÍ VELKÝCH KRUHŮ POKRÝVAJÍCÍ NEPŘIPOJENÉ LOKALITY

Mezi lokality bez vrstvy DWDM patří:

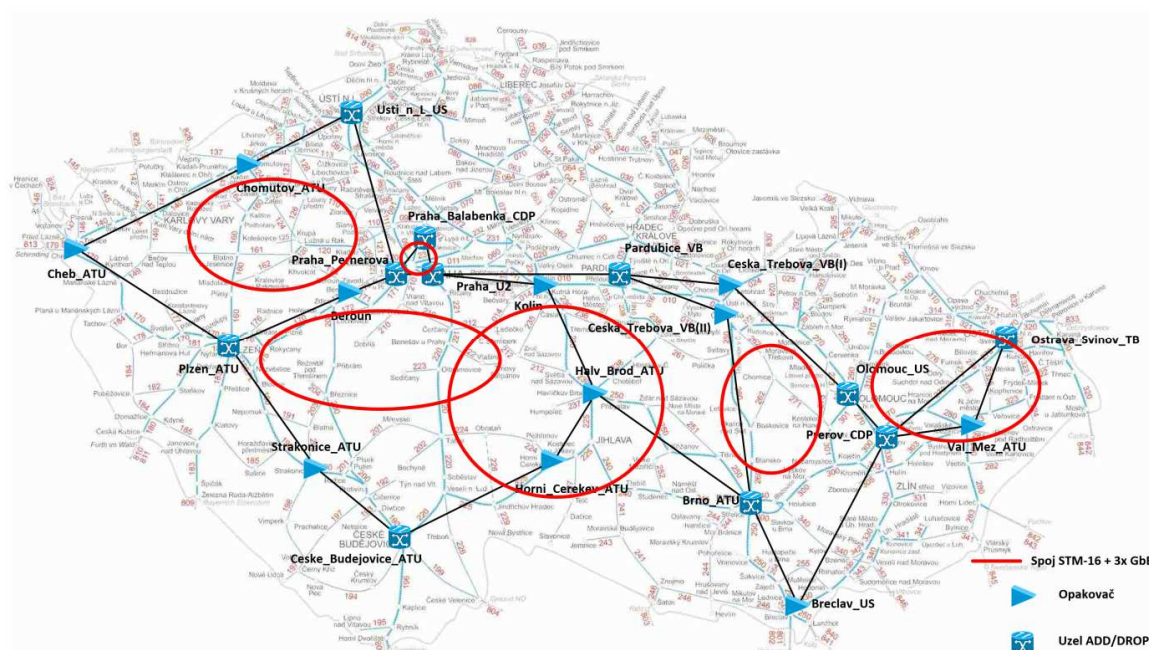
- Benešov, Tábor, Veselí nad Lužnicí, Česká Lípa, Liberec, Hradec Králové, Zábřeh, Karlovy Vary, Bruntál (uvolnění příčky Přerov - Ostrava), Jihlava.

Mezi další lokality s vrstvou DWDM bez vyvedeného provozu patří:

- Cheb, Chomutov, Beroun, Strakonice, Kolín, Česká Třebová, Horní Cerekev (přesunutí uzlu do Jihlavy), Břeclav, Valašské Meziříčí, Havlíčkův Brod.

3.1.1.1 Posílení vrstvy SDH a 1G páteřní sítě

V dnešní topologii (Obr. 3) propojení vrstev SDH (STM-16) a Ethernet (3x GbE) mezi lokalitami je patrné šest velkých kruhů (Obr. 5). Tyto kruhy v sobě zahrnují dvě, tři nebo čtyři lokality.

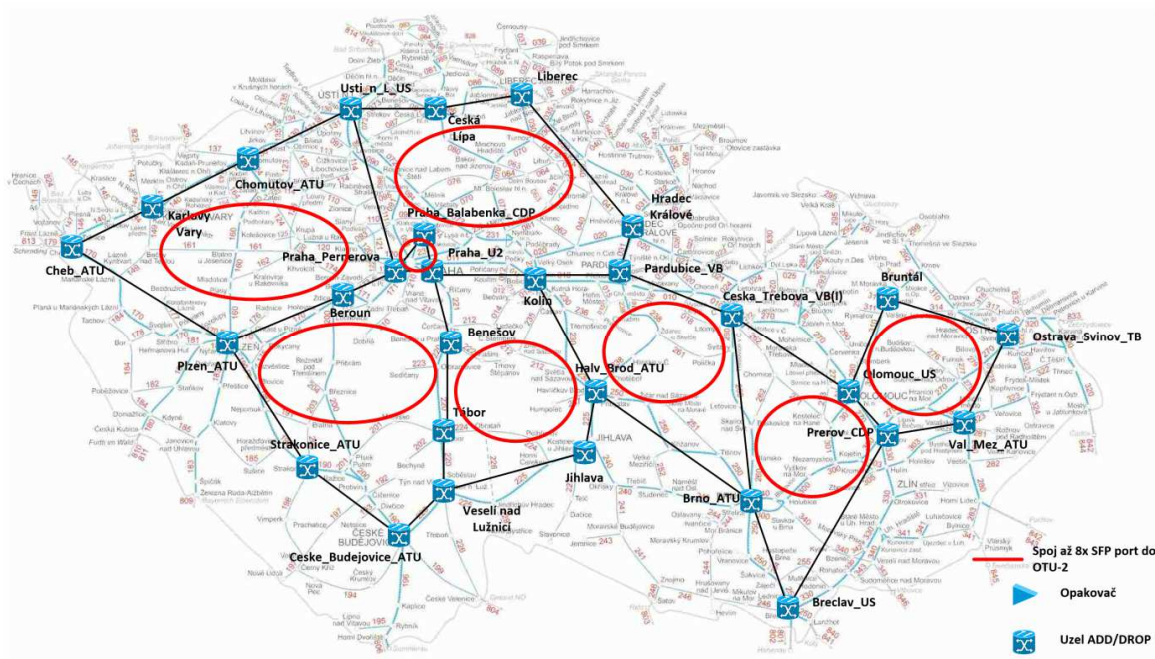


OBR. 5 – SOUČASNÁ TOPOLOGIE DWDM (6 KRUHŮ)

Z Obr. 3 je patrné, že v současné topologii sítě dochází v trase Praha U2 – Kolín k souběhu dvou kruhů, které je vhodné do budoucna rozdělit a stávající topologii doplnit o příčku ve směru Praha – Benešov – Tábor – Veselí n. L. – České Budějovice (viz Obr. 6).

S novou topologií by vznikly další možnosti posílení transportu STM-16 a GbE. Výhodou je, že karty, které se v současnosti používají, jsou universální a využívají možnosti mapovat osm libovolných potů do OTU-2 trunku.

Doplněním příček (Praha – Benešov – Tábor – Veselí n. L. – České Budějovice, Ústí n. L. – Liberec – Hradec králové – Pardubice a Olomouc – Bruntál – Ostrava Svinov) by v budoucnu vzniklo osm kruhů zahrnující všechny významné lokality s možností přenosu protokolů STM-1/4/16, FE/GbE, FC 1/2G (viz Obr. 6) a eliminovali by se souběhy tras.



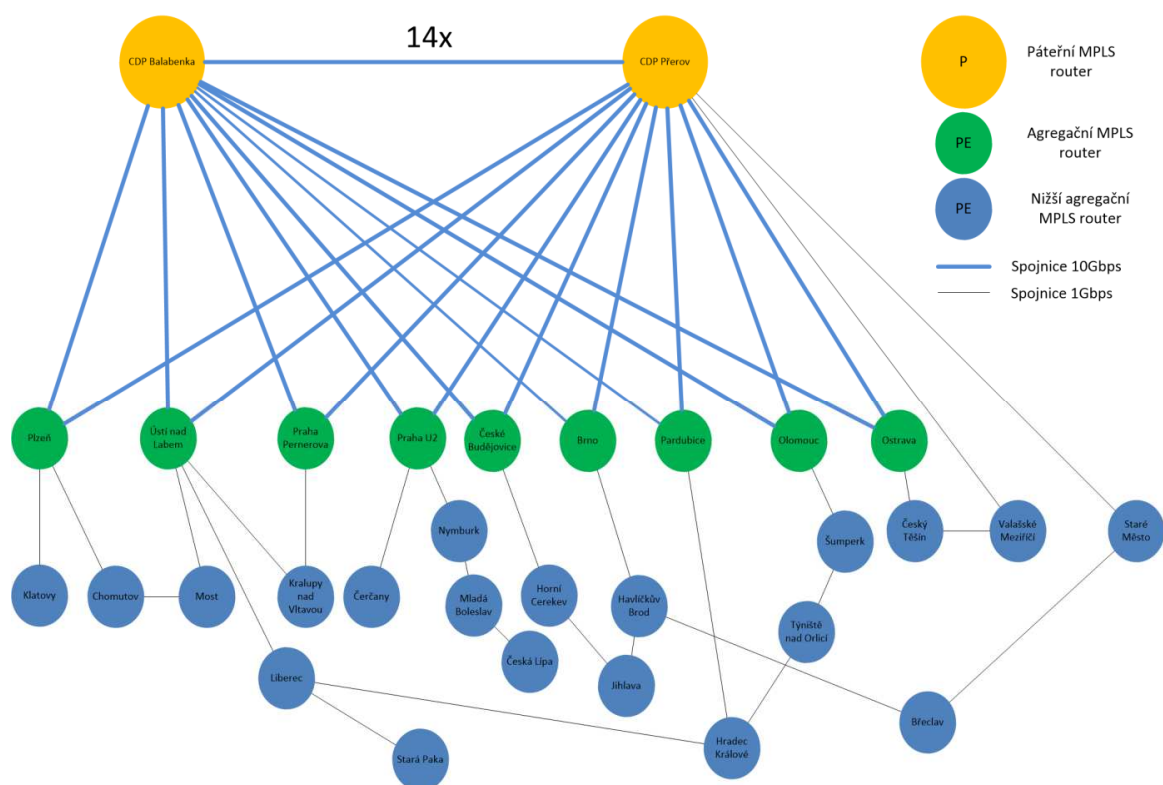
OBR. 6 – NOVÁ TOPOLOGIE DWDM (VYTVOŘENÍ 8 KRUHŮ)

3.1.2 POSÍLENÍ STÁVAJÍCÍ 1G PÁTEŘE NA 10G

Topologie zobrazená na Obr. 6 dovoluje realizovat po doplnění 10G karet propojení i na vrstvě 10Gb Ethernetu. Došlo k navýšení kapacity stávající páteře a zároveň by se tak zrušili DWDM pronájmy pro napojení MPLS PE routerů v lokalitách Chomutov, Beroun, Liberec, Hradec Králové.

3.1.3 TOPOLOGIE MPLS 1G/10G ETH

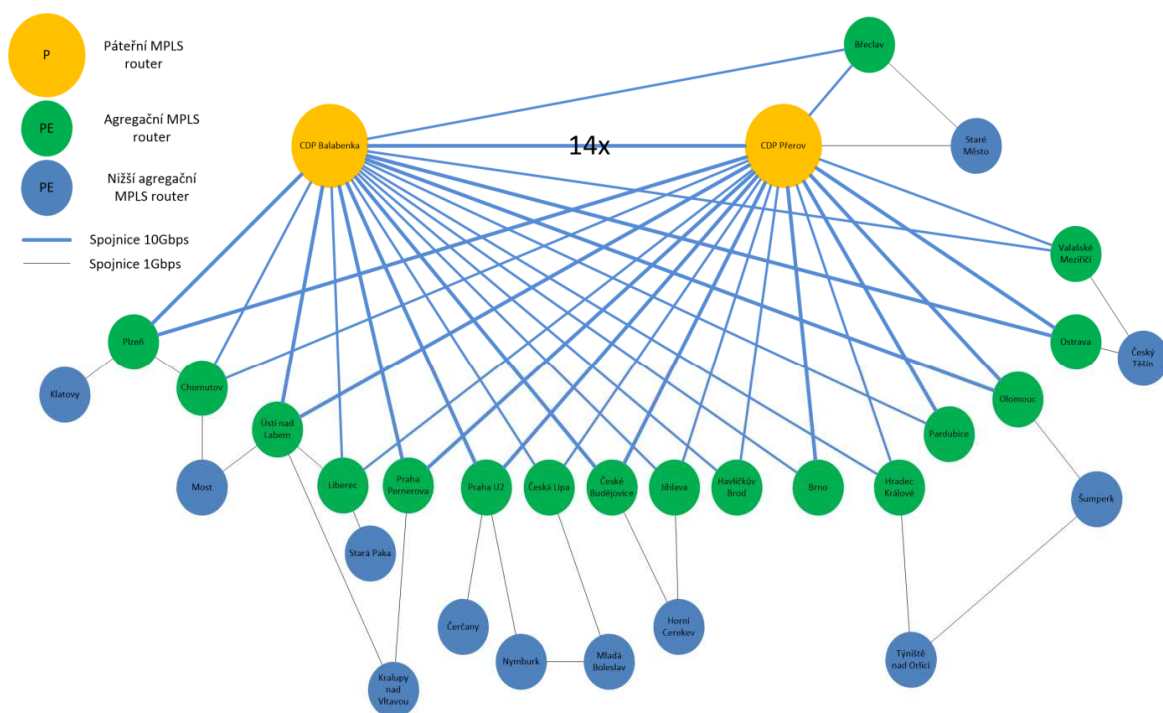
Dnešní topologie zapojení agregačních routerů MPLS je zobrazena na Obr. 7. Doplněním fyzické topologie podle Obr. 4 je možné některé PE routery nižší agregační úrovně povýšit na agregační úroveň a propojit s páteřními routery 10G ethernetem, viz. Obr. 8.



OBR. 7 – SOUČASNÁ TOPOLOGIE AGREGAČNÍCH ROUTERŮ MPLS

3.1.4 PROPOJENÍ DC 10G NA 100G

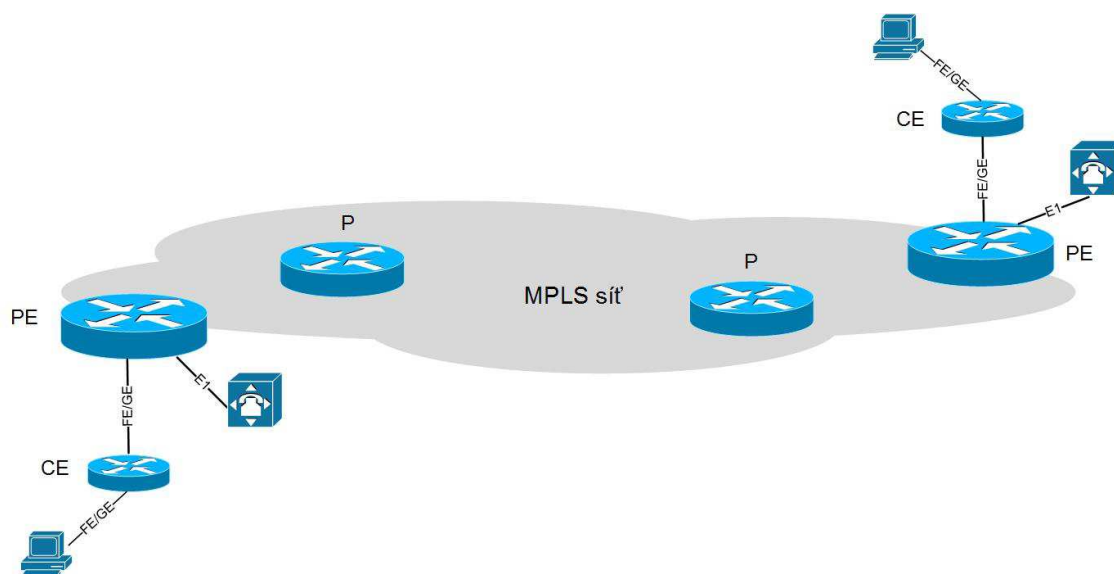
Dnes propojení 7x10G přímou trasou a 7x10G zálohovanou trasou. Posílení jak přímé, tak i záložní trasy na interface n x 100Gbps.



OBR. 8 – NOVÁ TOPOLOGIE AGREGAČNÍCH ROUTERŮ MPLS

3.2 Přenosová síť MPLS

S masivním rozvojem IP technologie, kdy postupně dochází k převodu legacy protokolů na společný IP protokol, je důležité pro taková řešení připravit páteřní síť, která nejen že dovolí jejich přenosy ale i zajistí správné chování sítě k těmto přenosům. Takovou technologií je MPLS, nejen že tyto požadavky plní ale je schopna i v případě postupné migrace z legacy rozhraní na Ethernet, připojit tyto legacy rozhraní a transparentně jejich provoz přenést. Právě možnostem připojení stávajících technologií a možnostem jejich přenosu v implementované MPLS síti je věnována tato část studie.



OBR. 9 – OBECNÁ STRUKTURA MPLS

Provoz je od koncových zařízení, připojených do zařízení CE rozhraním Ethernet, přenášen ze zařízení CE protokolem IP do zařízení PE. Směrovač PE přidělí na vstupu do páteřní MPLS sítě příchozímu IP paketu obvykle dvě značky. Vnější a vnitřní značku. Vnější slouží pro směrování IP paketu v prostředí MPLS páteřní sítě a vnitřní slouží k identifikaci VRF (Virtual Routing and Forwarding) na cílovém PE směrovači. Podle vnější značky jsou potom přepínány pakety na P směrovačích. Cílový směrovač PE potom díky vnitřní značce, kterou po její použití zahodí, předá paket do adekvátního VRF, odkud se paket dostává na správné CE zařízení a odtud následně na cílové koncové zařízení.

Samostatnou kapitolou jsou legacy rozhraní jako je např. E1, které jsou připojeny přímo do zařízení PE. Zde je jejich provoz zabalen a opatřen MPLS značkou a přenášen MPLS sítí.

3.2.1 DOVYBAVENÍ STÁVAJÍCÍCH LOKALIT

V tuto chvíli je v některých stávajících lokalitách SPoF (Single Point of Failure - jeden prvek sítě, při jehož nefunkčnosti by byla vyřazena celá lokalita) v podobě jediného PE routeru. Z důvodu zvýšení zabezpečení provozu je nutné dovybavit následující lokality PE routery:

- Praha – Perneroва, Praha – U2, Pardubice, Olomouc, Plzeň, Ústí n. Labem, Ostrava, Brno.

3.2.2 SEGMENTACE PROVOZU DO VRF

V textu je zmíněno VRF, které umožňuje vytvoření vlastní směrovací instance v rámci směrovací tabulky směrovače. Díky použití VRF je možné zajistit vzájemnou izolaci provozů, to znamená např. při požadavku dvou provozů, které mají být součástí jednoho směrovače a mají být vzájemně od sebe izolovány, stačí každý z těchto provozů přiřadit do vlastního VRF.

Různorodost požadavků uživatelů aplikací a správců systému i navazujících procesů uživatele vyžaduje výkonné prostředky pro segmentaci sítě jako základní prostředek řízení informačních toků v jejím rámci (viz kapitola 7.6.1). S použitím VRF je možné zajistit vzájemnou izolaci provozů, to znamená např. při požadavku dvou provozů, které mají být součástí jednoho směrovače a mají být vzájemně od sebe izolovány, stačí každý z těchto provozů přiřadit do vlastního VRF.

3.2.2.1 Vyčlenění externích organizací do oddělené sítě

V současné době mají do přenosové sítě SŽDC přístup externí subjekty (např. ČD, ČD Cargo, ČD IS a další) za účelem správy údržby nasazených zařízení a aplikací. V dalších krocích rozvoje přenosové sítě a také s ohledem na zákon č. 181/2014 Sb., o kybernetické bezpečnosti je nutné provést vyčlenění externích subjektů do samostatné oddělené sítě s řízeným prostupem, umístěním za Firewall do přidělené VPN.

TAB. 6 – NÁVRH SEGMENTACE PROVOZŮ DO VRF

OZNAČENÍ VRF	DRUH PROVOZU
VOIPTS	VOIP TECHNOLOGICKÉ SÍŤE (DISPEČERSKÁ KOMUNIKACE)
VOIPSS	VOIP SLUŽEBNÍ SÍŤE
KAMS	KAMEROVÉ SYSTÉMY
ISIC	INFORMAČNÍ ZAŘÍZENÍ
ROZ	ROZHLASOVÉ ZAŘÍZENÍ
EZS	ELEKTRONICKÁ ZABEZPEČOVACÍ SIGNALIZACE
EPS/ZPDP	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE/ZAŘÍZENÍ PRO DETEKCI POŽÁRU
ASHS	AUTONOMNÍ SAMOZHÁŠECÍ SYSTÉM
EOV	ELEKTRICKÝ OHŘEV VÝMĚN
OSV	OSVĚTLENÍ
ENERGETIKA	
DRT	DISPEČERSKÁ ŘÍDÍCÍ TECHNIKA
DDTS	DÁLKOVÁ DIAGNOSTIKA TECHNOLOGICKÝCH SYSTÉMŮ ŽDC
ENE_KAMS	KAMEROVÉ SYSTÉMY
ENE_EZS	ELEKTRONICKÁ ZABEZPEČOVACÍ SIGNALIZACE
ENE_EPS/ZPDP	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE/ZAŘÍZENÍ PRO DETEKCI POŽÁRU
ENE_ASHS	AUTONOMNÍ SAMOZHÁŠECÍ SYSTÉM

OSTATNÍ	
INTRA	INTRANET
INET	INTERNET
MGMT	INTERNÍ MANAGEMENT
EXTERNÍ SUBJEKTY	
EXT_XXX	EXTERNÍ SUBJEKTY

3.2.3 VARIANTY PŘIPOJENÍ LOKALIT DO MPLS

Pro potřeby studie byly v rámci sítě SŽDC vytipovány 4 typové lokality (Železniční stanice, zastávky, energetické objekty a další) podle Tab. 7, na kterých budou dále modelovány varianty typového zapojení aktivních zařízení do sítě MPLS.

TAB. 7 – TYPICKÉ OBSAZENÍ LOKALIT V SÍTI SŽDC

LOKALITA	POČET SMĚRŮ	VLÁKEN NA SMĚR	ETHERNET PORTY*	E1*	MÍSTNÍ L2L3 CE	MÍSTNÍ MPLS PE	VZDÁLE NÁ MPLS PE
BTS GSM-R	2	2	1	2	-	1	2
NAPÁJECÍ STANICE / MĚNÍRNA	1 / 2	12 / 4	12	-	1	-	1 / 2
NAPÁJECÍ STANICE / MĚNÍRNA (S E1)	1 / 2	12 / 4	12	1	1	1	1 / 2
ZASTÁVKA	2	4	3-8	-	1	-	2
ZASTÁVKA (S GSM-R)	2	4	3-8	2	1	1	2
STANICE (S/BEZ GSM-R)	2	12	49-50	2 / 4	1+	1 / 2	2
UZLOVÁ STANICE (S/BEZ GSM-R)	2+	12	51 - 100	2 / 4	1+	1 / 2	2

* Orientační hodnoty

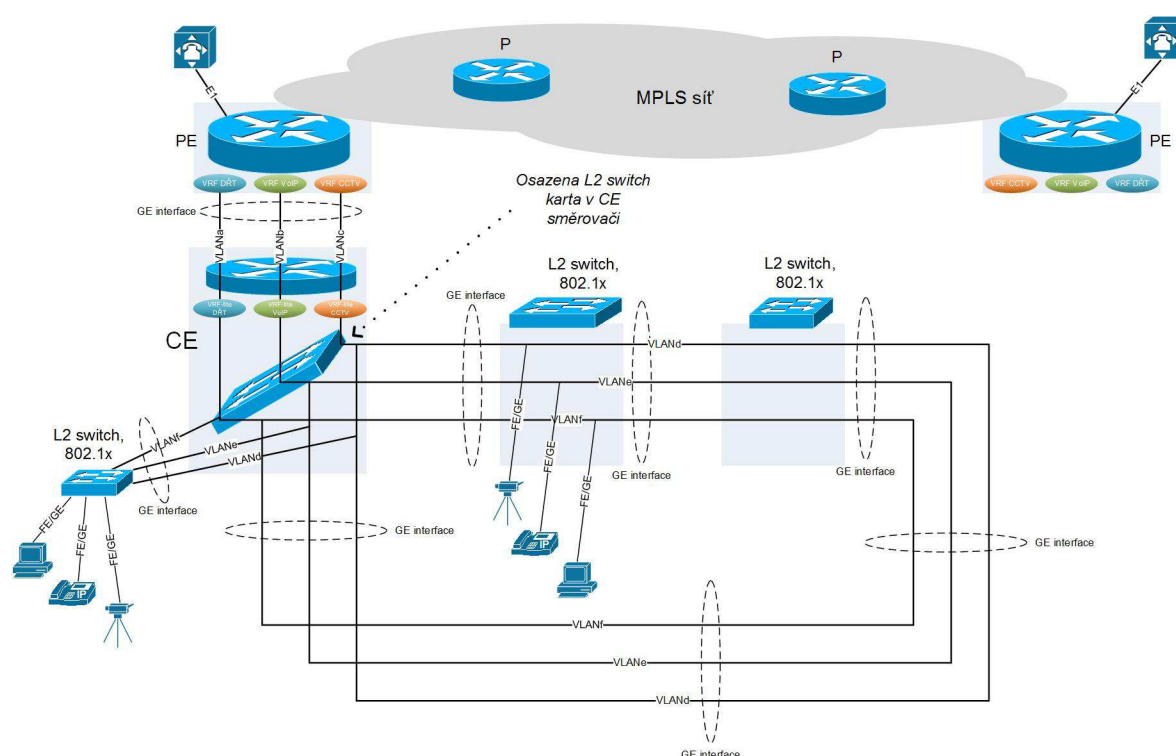
3.2.3.1 Varianta č.1 – Varianta připojení ŽST a ZAST pomocí PE, CE a L2 přepínači

Připojení koncových zařízení (Obr. 10) s Ethernet rozhraním do MPLS sítě lze realizovat ve třech bodech:

- Přímou na směrovač CE, pokud je směrovač osazen L2 switch kartou (podpora 802.1x);
- Na předřazený L2 switch k CE směrovači;
- Na L2 switch zapojené v kaskádě;

Zařízení jsou potom přes VLAN konfiguračně připojena do příslušné VRF v CE zařízení. Připojení koncových zařízení s legacy rozhraním jako je rozhraní E1 lze realizovat pouze na směrovačích PE a jejich provoz neprochází přes vytvořenou L2 topologii. Na vytvořené L2 kruhu musí být spuštěn protokol pro zabránění vytváření logických smyček. Pokud nebude možné osadit CE směrovač L2 switch kartou, je možné:

- Před CE směrovač předsadit samostatný switch, ve kterém bude začínat a končit vytvořená L2 topologie;
- Před CE směrovač předsadit dva switche zapojené ve stacku (logicky se chovají jako jeden switch). L2 kruh pak bude začínat v jednom z dvojice L2 switchů ve vytvořeném stacku a končit ve druhém z dvojice switchů ve vytvořeném stacku.



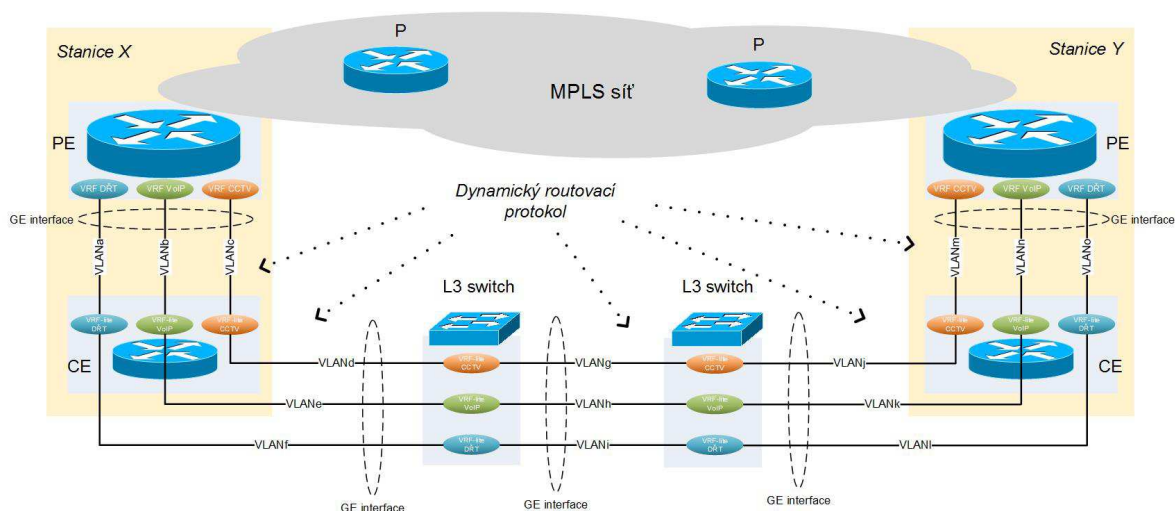
OBR. 10 – PŘIPOJENÍ KONCOVÝCH ZAŘÍZENÍ S L2 PŘEPÍNAČI

Jedná o jednoduché, méně robustní a i finančně méně náročné řešení, které nabízí pouze rozhraní typu Ethernet, nikoliv E1. Toto řešení je vhodné méně důležité regionální tratě. Vytvořená L2 topologie nesmí být záložně propojena do dalšího CE nebo PE směrovače.

Řešení kaskády L3 switchů připojené na koncích k PE směrovačům-obecné zásady

Pro případy, kdy je nutné zajistit pro koncová zařízení záložní prostup do sítě MPLS nebo když bude mezi dvěma lokalitami s PE směrovači nutné na mezilehlých stanicích připojit další koncová zařízení, jsou nutné následující záležitosti (Obr. 11):

- PE směrovače musí být propojeny sítí MPLS nezávisle na propojení přes mezilehlé switche.
- Všechny switche musí být s podporou dynamického směrování (minimálně OSPF). Switche pouze s L2 funkcionalitou k řešení této záležitosti nestačí.
- Všechny switche musí podporovat vytváření směrovacích instancí VRF-lite.
- Na celé kaskádě switchů včetně propojení PE-CE musí být provozován dynamický směrovací protokol.



OBR. 11 – PŘIPOJENÍ KASKÁDY L3 SWITCHŮ

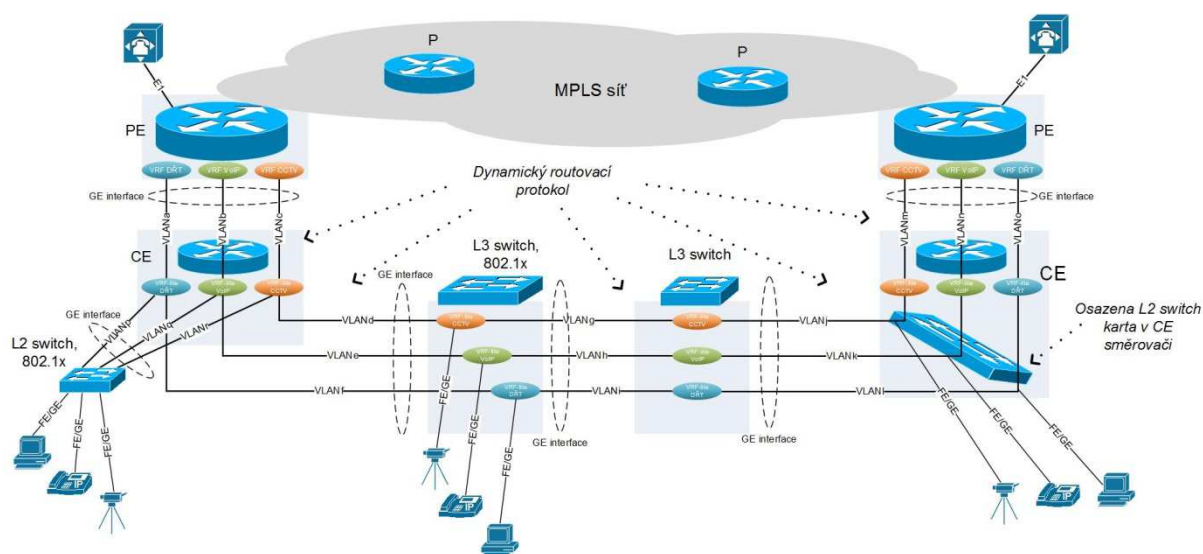
K CE směrovačům a L3 switchům nelze připojit zařízení s legacy rozhraním jako je rozhraní E1.

3.2.3.2 Varianta č.2 – Varianta připojení ŽST a ZAST pomocí PE, CE a L3

Připojení koncových zařízení (Obr. 12) s Ethernet rozhraním do MPLS sítě lze realizovat ve třech bodech:

- Přímě na směrovač CE, pokud je směrovač osazen L2 switch kartou (podpora 802.1x);
- Na předřazený L2 switch k CE směrovači;
- Na L3 switche zapojené v kaskádě mezi dvojicí CE směrovačů.

Zařízení jsou potom přes VLAN nebo přes fyzický interface konfiguračně připojena do příslušné VRF. Připojení koncových zařízení s legacy rozhraním jako je rozhraní E1 lze realizovat na směrovačích PE a jejich provoz nikdy neprochází přes zařízení CE a vytvořenou kaskádou L3 switchů.



OBR. 12 – PŘIPOJENÍ KONCOVÝCH ZAŘÍZENÍ (L3)

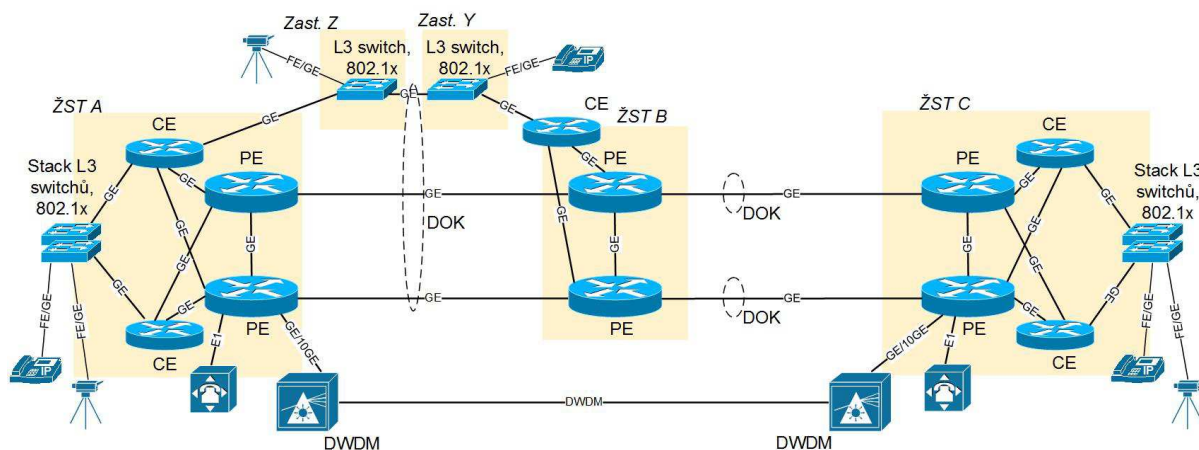
3.2.3.3 Varianta č.3 – Varianta připojení ŽST a ZAST v redundantním řešení

ŽST je z důvodu redundance (Obr. 13) řešeno v zálohovaném provedení 2xPE, 2xCE a 2xL3 switch zapojený ve stacku. Zastávky, protože nevyžadují připojení legacy rozhraní jako je E1 a redundanci, jsou osazeny L3 switchi.

Připojení koncových zařízení s Ethernet rozhraním do MPLS sítě lze realizovat na předřazených L3 switchích. Připojení koncových zařízení s legacy rozhraním jako je rozhraní E1 lze realizovat pouze na směrovačích PE a jejich provoz neprochází přes vytvořenou kaskádu L3 switchů.

Pokud vyvstane v tomto řešení požadavek připojení legacy rozhraní např. E1 na zastávce, musí být:

- buď celá kaskáda L3 switchů nahrazena v každé zastávce PE směrovačem a CE směrovačem s předřazeným L2 switchem s podporou 802.1x nebo PE směrovačem a CE směrovačem s osazenou L2 switch kartou s podporou 802.1x;
- nebo daná zastávka musí být osazena PE směrovačem, který bude mít vlastní optické spoje na PE v sousedních ŽST. Pokud na dané zastávce bude potřeba připojit další zařízení s rozhraním Ethernet, je nutné tato zařízení do místního PE opět připojit přes L2 switch s podporou 802.1x a místní CE směrovač.



OBR. 13 – ZÁLOHOVANÉ ŘEŠENÍ ŽST

Příklad tohoto zapojení na konkrétní trati je uveden příloze č.1.

Popis a využití optických vláken ve variantě č.3

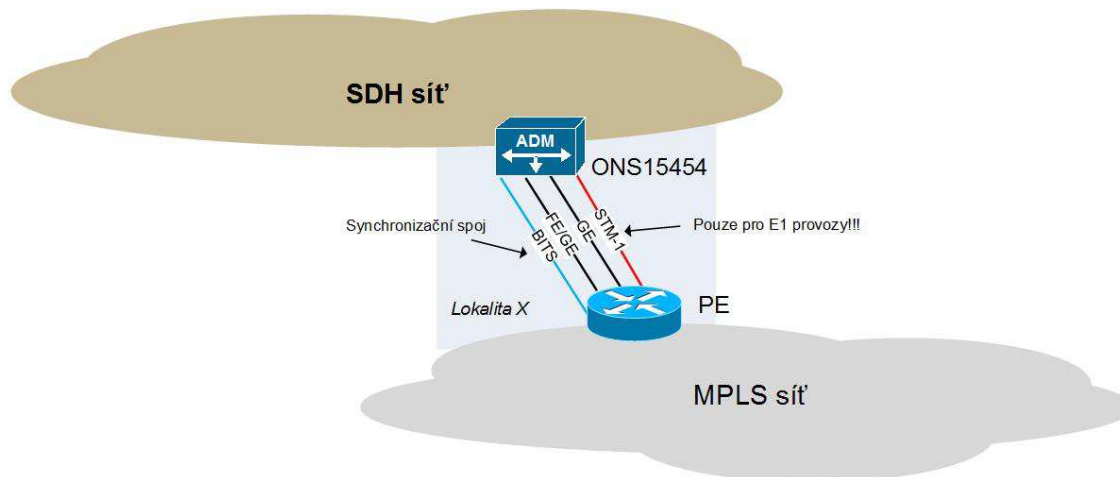
- Všechny lokality kromě jednou cestou připojených napájecích stanic/měření nutno zapojit redundantně do dvou PE;
- Pro služby přes E1 je nutné lokální MPLS PE;
- CE vždy připojeno do jednoho nebo dvou místních nebo vzdálených PE;
- Železniční stanice se doporučuje se dvěma PE;
- CE se nikdy neřetězí;
- CE není L2, ale vždy L3L2 s podporou multi-VRF nebo L3;
- Oddělení PE a CE nutné kvůli konfiguračním zásahům různých týmů
- V případě nedostatku vláken je možné řetězení PE mezi stanicemi a případně osazení některé zastávky PE;
- Je možné při nedostatku vláken využívat jedno-vláknových transceiverů – pro 1GE pro vzdálenost až do 80km.

3.2.4 VZÁJEMNÉ PROPOJENÍ SDH A MPLS SÍTĚ

Na Obr. 14 je vyobrazeno vzájemné propojení MPLS a SDH sítě v rámci jedné lokality. Sítě je důležité propojit na rozhraních:

- BITS, pro vzájemnou synchronizaci obou sítí, která je důležitá pro přenos provozů z legacy rozhraní (např. E1) připojených do sítě MPLS. V této souvislosti je potřeba zmínit, že pro bezchybné přenosy TDM provozu, je nutné samozřejmě zajistit i synchronizaci TDM sítě s SDH a MPLS sítí.
- FE nebo GE, pro vzájemné předávání provozu jako jsou kamery, VoIP, DŘT, DDTS, intranet, internet a interního managementu. To znamená obecně řečeno IP provozu segmentované do VLAN, které jsou v současné době přenášeny SDH kontejnery a VLANami.
- GE pro případ řešení záložního propojení MPLS sítě přes síť SDH.

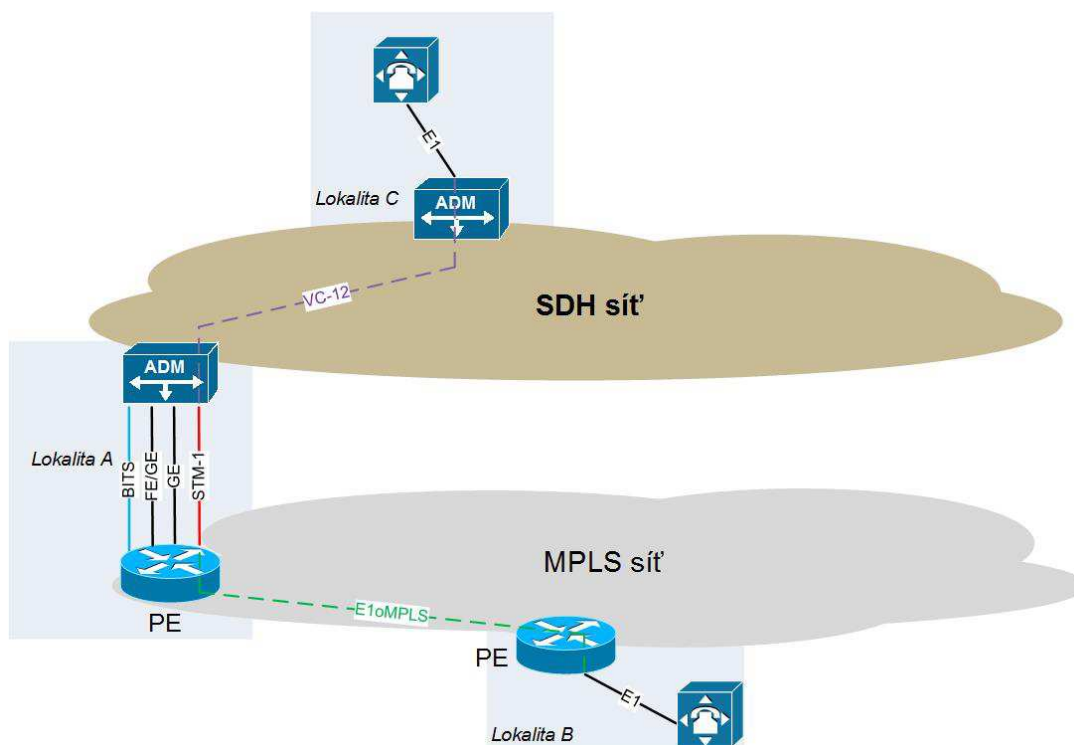
- STM-1, pro přenos E1 provozů mezi oběma sítěmi. Viz Obr. 15, kde je znázorněn přenos E1 z lokality B na lokalitu C.



OBR. 14 – PROPOJENÍ MPLS A SDH SÍTĚ

3.2.5 MOŽNOSTI ZÁLOŽNÍHO PŘENOSU E1 PRO PŘÍPAD ZÁLOŽNÍHO PROPOJENÍ MPLS A SDH SÍTĚ

Níže uvedené scénáře předpokládají v síti MPLS implementaci aplikací rychlé detekce výpadku linky a rychlého překlopení na záložní linku, tak aby časové nároky byly srovnatelné s technologií SDH. Zároveň je důležité poznamenat, že tyto aplikace je nutné provozovat společně s realizovaným QoS v síti MPLS.

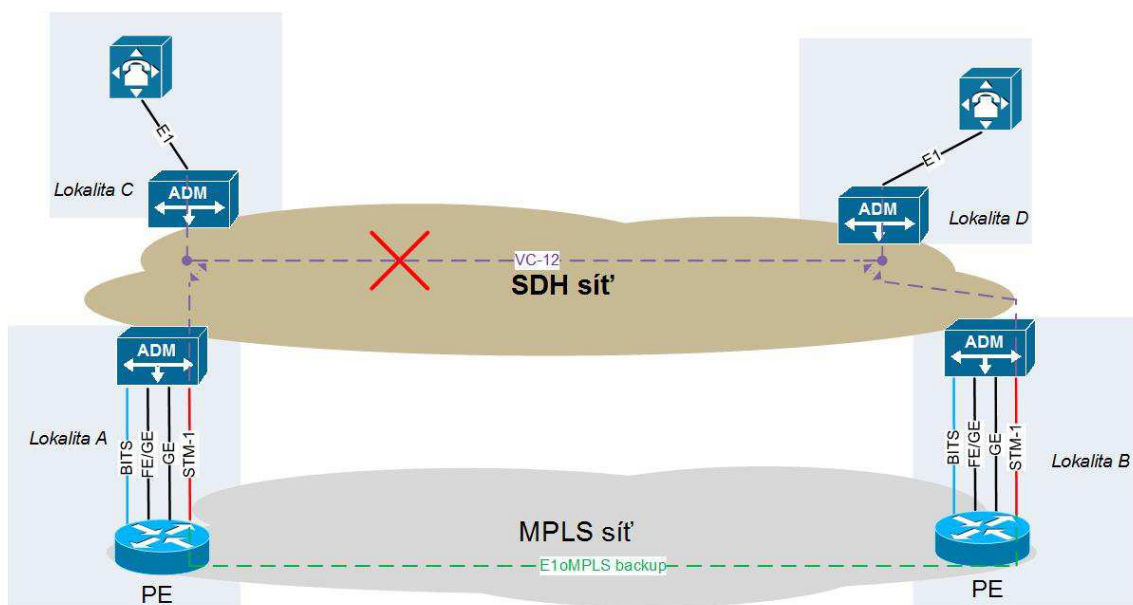


OBR. 15 – PŘENOS E1 MEZI SDH A MPLS SÍTÍ

Scénáře je nutné před každým nasazením nové softwarové verze MPLS směrovačů ověřit.

3.2.5.1 Zálaha E1, která začíná a končí v SDH

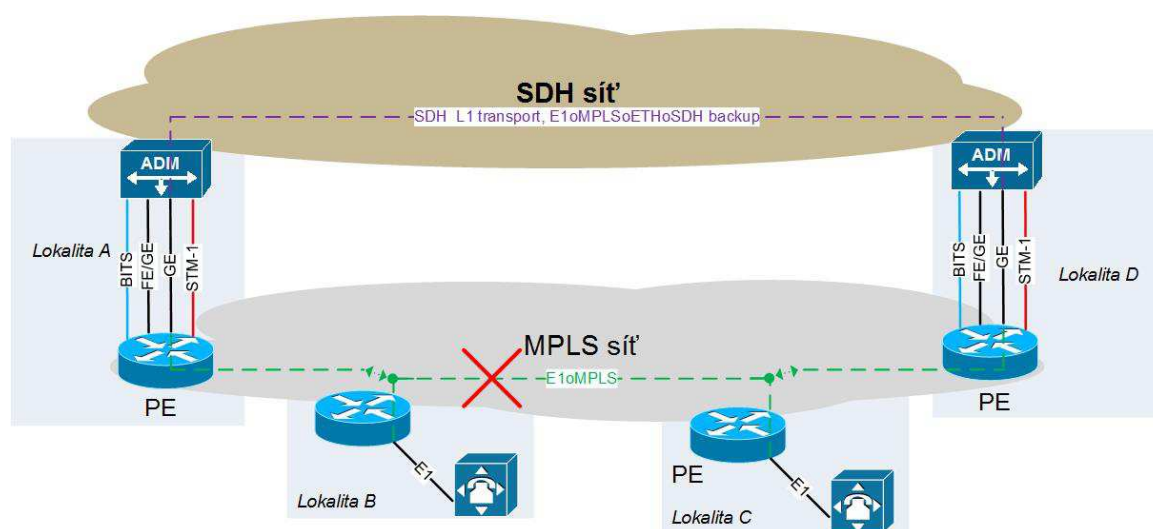
Na Obr. 16 je zobrazen přenos E1 která je přenášena primární cestou SDH sítě to znamená, začíná a končí v SDH síti. Pokud dojde k výpadku na cestě mezi koncovými prvky SDH, přesměruje zálohovací SDH mechanismus tuto E1 na hraniční SDH prvky mezi sítí MPLS a SDH, kde je E1 předána do sítě MPLS rozhraním STM-1, jako jeden z E1 příspěvků. Na vstupu do sítě MPLS je E1 zabalena do MPLS a transportována z jednoho hraničního PE směrovače na druhý hraniční PE směrovač.



OBR. 16 – PŘENOS E1 V SDH A ZÁLOŽNĚ MPLS SÍTÍ

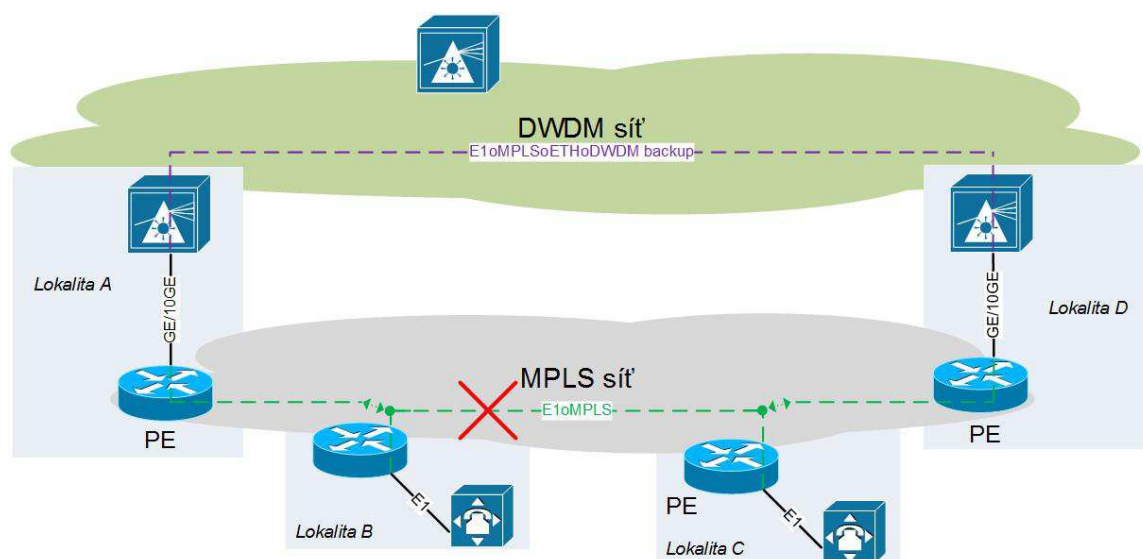
3.2.5.2 Zálaha E1, která začíná a končí v MPLS

Na Obr. 17 je zobrazen přenos E1, která je přenášena primární cestou MPLS sítě (E1oMPLS) to znamená, začíná a končí v MPLS síti. Pokud dojde k výpadku na cestě mezi koncovými směrovači MPLS, přesměruje zálohovací MPLS mechanismus tuto E1 na hraniční MPLS prvky mezi sítí MPLS a SDH, kde je E1 předána přes rozhraní GE (případně FE) do sítě SDH. E1 na tomto přechodu není ale z MPLS vybalena, ale MPLS je přenášeno transparentně společně s Ethernetem sítě SDH. V SDH je využita služba L1 transportu.



OBR. 17 – PŘENOS E1 V MPLS A ZÁLOŽNĚ SDH SÍŤÍ

Zálohu lze samozřejmě také provést přes síť DWDM viz Obr. 18. V přechodových bodech je propojení mezi směrovačem MPLS a DWDM prvkem realizováno na rozhraní GE nebo 10GE. Při výpadku sítě MPLS mezi oběma koncovými body E1 je provoz E1 přesměrován na přechodové PE směrovače a odtud přenášen přes Muxponder nebo Transponder kartu DWDM sítě jako E1 zabalená v MPLS a Ethernetu.

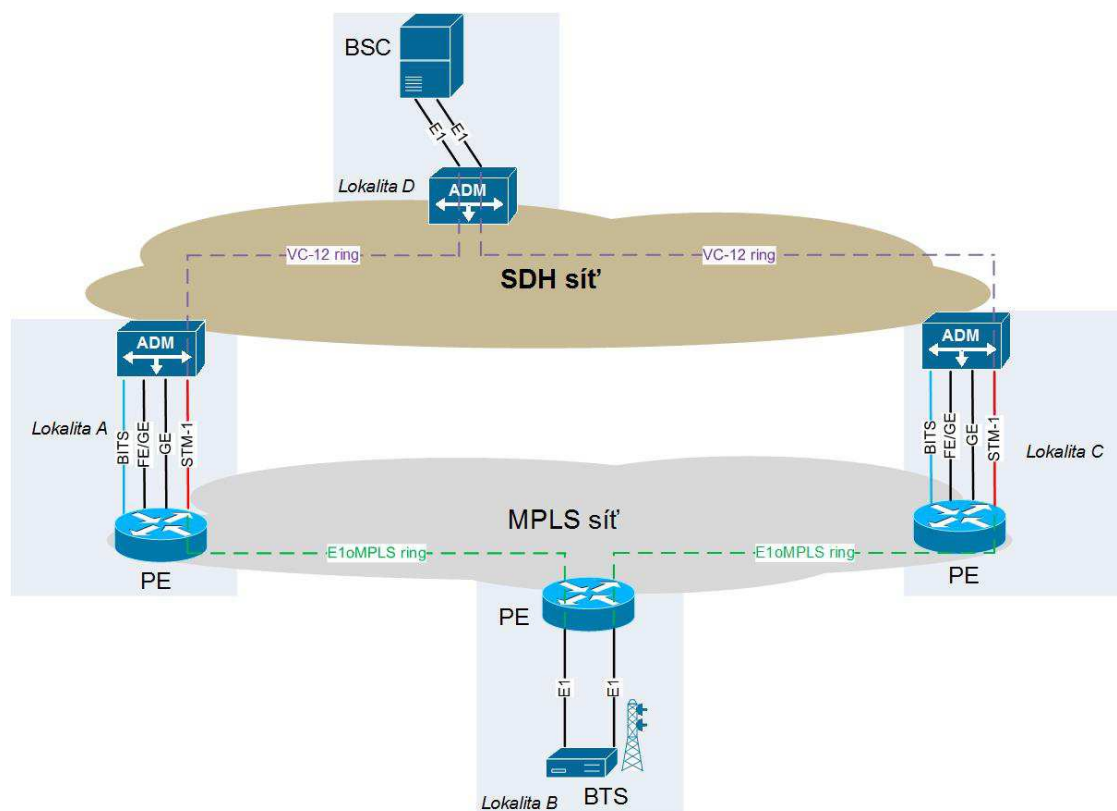


OBR. 18 – PŘENOS E1 V MPLS A ZÁLOŽNĚ DWDM SÍŤÍ

3.2.5.3 Zálohované připojení GSM-R BTS s rozhraním E1 do sítě MPLS

Na Obr. 19 je uvedeno připojení GSM-R BTS s rozhraním E1 do sítě MPLS. GSM-R BTS je do sítě MPLS připojena oběma rozhraními E1, čímž zachovává kruhovou topologii připojení GSM-R BTS k technologii GSM-R BSC. Pokud dojde k výpadku v jedné polovině E1 kruhu, GSM-R BTS výpadek spojení na E1 zaregistruje detekcí alarmu na E1 např. LOF a začne provoz směřovat druhou částí

kruhu. Důležité je pro přenos E1, mezi sítí SDH a MPLS v obou přechodových lokalitách, využít rozhraní STM-1.



OBR. 19 – PŘIPOJENÍ GSM-R BTS V SÍTI MPLS

3.3 Synchronizace přenosového systému a TDS

3.3.1 VYUŽITELNOST DATOVÉ SÍTĚ A MOŽNOSTI JEJÍ OPTIMALIZACE

Pro přenos TDM služeb přes PSN (např. MPLS WAN síť) je nutnou podmínkou distribuce frekvenční a fázové složky synchronizace uzlům WAN sítě, a to i v případě, kdy pro podporu služeb stačí *Network-synchronous operation* model dle standardu G.8261/Y.1361, který předpokládá zcela synchronní síť včetně koncových zařízení. Ve složitějších případech:

- Může být potřebné šíření časové složky (TOD), a to především pro koncová zařízení, vyžadující přesnost vyšší, než poskytují samostatné obecné protokoly, např. NTP (dostačující pro management přenosu);
- Může být požadováno šíření dalších plesiochronních signálů (tj. s definovaným malým limitem odchylky přenosové rychlosti), např. pro aplikaci ostatních modelů dle standardu G.8261/Y.1361 pro vybraná koncová zařízení (KZ) nebo pro tunelování okruhů TDM cizích sítí.

Pro zmíněné aplikace musí systém šíření frekvenční a fázové složky splňovat minimálně tyto výsledné parametry:

- Jitter a wander obnoveného taktu a stability autonomních taktů splňují požadavky ITU-T G.823/G.824, v obecném případě i úrovně pro šíření synchronizace;
- Rozsah zachycení synchronizace je v případě plesiochronních TDM toků alespoň ± 50 ppm (při šíření synchronizace fyzickou vrstvou vyžadující model DCR - *Differential Clock Recovery*),
- Tolerance alespoň 5% ztrátovosti bez degradace kvality obnovy taktu;
- Podpora mechanismů automatického přepnutí do autonomního (*hold-over*) režimu a následného vyhledání náhradní synchronizační reference v případě ztráty normální provozní konektivity (spoje) v PSN.

Protože šíření potřebných složek je nutnou podmínkou funkčnosti příslušných služeb, je šíření synchronizace důležitým aspektem z hlediska bezpečnosti systémů a proto, v technologických sítích zejména, má být zajištěno vlastními síťovými prostředky, ne pomocí lokálního využití cizích synchronizačních systémů, jejichž funkčnost a provozuschopnost není provozovatel sítě schopen ovlivnit (příkladem je dnes často využívaný satelitní systém GPS, provozovaný US DOD).

Z hlediska plánování a návrhu je potřeba rozlišovat systémy (protokoly) šíření po fyzické vrstvě („klasické“) a systémy využívající paketové toky.

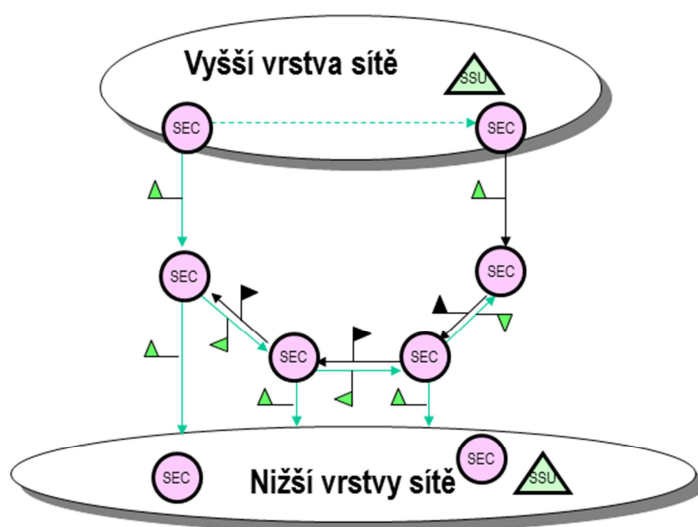
3.3.2 SYSTÉMY S ŠÍŘENÍM PO FYZICKÉ VRSTVĚ

Hlavním reprezentantem klasického schématu je šíření mezi uzly systémů SDH, které má následující charakteristiky:

- frekvenční složka synchronizace je šířena hop-by-hop přímo fyzickou vrstvou sítě, rámcovanou strukturou linkového signálu;
- z topologického hlediska je schéma tvořeno řetězy (polokruhy) synchronizovaných uzlů se standardy omezenou délkou kvůli omezení kumulace odchylek (viz obrázek);
- které se v rámci sítě skládají v řídkou mesh-strukturu, zajišťující redundanci při poruše uzlu/linky;
- Redundance řízena jednoduchým signalizačním protokolem, vázaným na shora popsané topologie.

Nástupcem popsaného schématu v PSN je SyncE (*Synchronous Ethernet*), převádějící jeho principy do prostředí Ethernet:

- Využívá fyzickou vrstvu Ethernetu (1GE a výše), jejíž rámce jsou vysílány v definovaném časovém rastru, kterou přenáší frekvenční složku synchronizace;
- Rovněž logické topologie synchronizace jsou odvozeny od SDH sítí, včetně shodné aplikační vrstvy signalizačního protokolu;
- SyncE musí podporovat všechna zařízení po cestě (stejná podmínka u SDH byla automaticky splněna, v technice Ethernet toto už neplatí, protože SyncE je dodatečným rozšířením protokolu).



OBR. 20 – ZAČLENĚNÍ POLOKRUHU SEC (EEC) MEZI VRSTVY ŠÍŘENÍ SYNCHRONIZACE (PRAPORKY SYMBOLIZUJÍ ZPRÁVY ŘÍDICÍHO PROTOKOLU QL/SSM)

V obou případech použitý signalizační protokol vede při nedodržení topologických podmínek na nestabilitu synchronizačních cest a nemá integrované prostředky ani pro ověření dalších funkčních podmínek. To vede na potřebu detailního návrhu síťové synchronizace, který je typicky nutné zajistit v projekční fázi na samostatných nástrojích (managementové nástroje typicky správu synchronizace v síťovém měřítku nepodporují). Návrh musí vycházet z následujících zásad:

- fyzická topologie sítě, obvykle předem daná, musí být rozdělena na polokruhové segmenty s možnou referencí z obou konců (z důsledného uplatnění této zásady vychází i požadavek na dva geograficky rozdílné synchronizační zdroje sítě),
- segmenty musí být rozčleněny do vrstev, např. analogicky členění provoznímu (páteří, regionální, lokální segmenty),
- pro signalizaci QL/SSM (u SyncE) musí být zvolen vhodný profil s ohledem na aplikaci a mezi vrstvami musí pro ni být zajištěn řízený přístup (případný průnik může způsobit vznik nestabilních zakázaných topologií).
- Nedílnou součástí návrhu je kontrola délky¹ synchronizačních cest v navrženém schématu proti limitům příslušných standardů, a to nejen v plně provozním stavu, ale minimálně i ve stavu jedné poruchy (ve vrstvě, segmentu).
- Výsledkem analýzy přípustných délek může být stanovení lokalit pro dodatečnou instalaci distribučních prvků s vyšší stabilitou generovaných signálů (SSU).
- Ve všech krocích návrhu je nutné zohlednit známá funkční omezení² provozovaných nebo plánovaných zařízení.

¹Analýza cest je úloha složitosti N^2 , z toho plyne i zmíněná potřeba rozčlenění sítě do samostatně řízených vrstev a segmentů.

3.3.3 ŠÍŘENÍ PAKETOVÝMI TOKY

PSN dovolují, na rozdíl od techniky TDM, využívat při srovnatelné kvalitě šířené synchronizace i techniky nepřímé, kdy synchronizační informace je šířena s menšími nebo většími rozšířeními proti spolu s uživatelskými daty standardními forwardovacími / směrovacími mechanismy. Představiteli těchto technik jsou protokol IEEE 1588v2 (PTP, *Precision Time Protocol*) a techniky ACR (*Adaptive Clock Recovery*).

Protokol IEEE 1588v2 (PTP, *Precision Time Protocol*)

- je vybaven pro distribuci frekvenční složky i jednotného času (časová složka, TOD),
- při synchronizaci se využívá kontinuálního toku synchronizačních paketů nebo rámců,
- výkonnostní profily definují konkrétní komunikační média, protokoly, funkční podmnožiny a parametry pro jednotlivé aplikace, konkrétně např. transport UDP/IP nebo přímo Ethernet (specifický *Ethertype*), režim obsluhy QL/SSM značek, apod.
- dovoluje na jednom segmentu PSN provozovat několik domén PTP se vzájemným překryvem (rozlišení adresováním) pro záložní účely nebo pro distribuci cizího taktu (při tunelování plesiochronních signálů TDM cizích sítí),
- zařízení po cestě ale (při dodržení limitů, typicky pro transport UDP/IP) nemusí nutně protokol (funkce) PTP podporovat.

Techniky ACR (*Adaptive Clock Recovery*) zatím nejsou plně standardizovány.

- Umožňují minimálně synchronizaci frekvenční (fázové) složky stejně jako klasické techniky,
- při synchronizaci se využívá pakety uživatelských nebo režijních relací CES,
- obvykle využívají transport UDP/IP s minimem specifických požadavků na využívanou L2/L3 službu,
- funkce ACR jsou implementovány zásadně jen na začátku a konci synchronizačního skoku, zařízení po cestě nemusí funkce ACR podporovat.

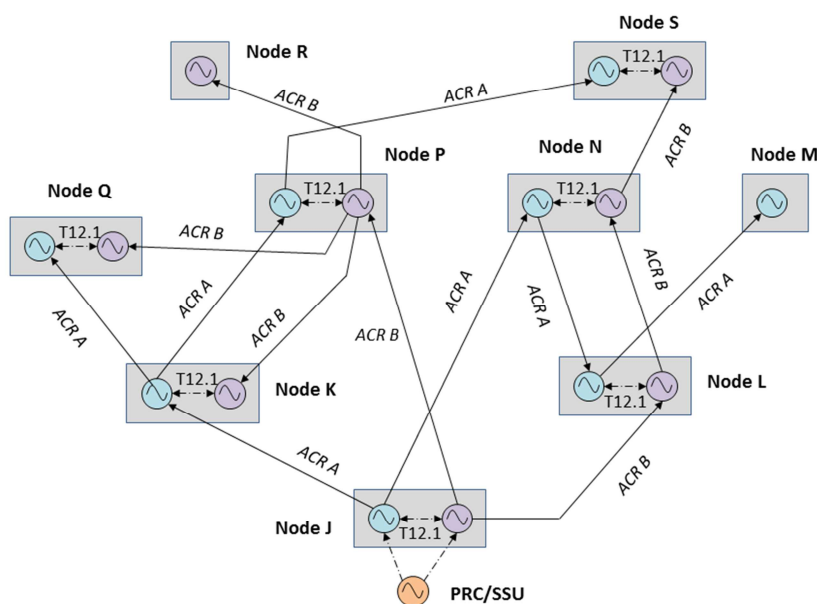
Obě jmenované techniky nepřímého šíření odvozují frekvenční složku filtračními technikami z četnosti doručení paketů / rámců a často započítávají specifickými postupy zjištěná transportní zpoždění, kvalita je proto silně ovlivněna PDV (Packet Delay Variation) a dynamickými změnami v síti (rerouting). Vyžadují specifická schémata šíření synchronizace v síti, výrazně odlišná od klasického schématu pro technologie SDH a SyncE, popsaného v odst.3.3.2. Zásadní rozdíly jsou následující:

- uvnitř segmentu (domény) se synchronizace mezi uzly šíří end-to-end ve více hvězdicových nebo stromových logických topologiích, které jsou synchronizovány ze společného primárního zdroje taktu.

² Zařízení renomovaných výrobců vykazují různá omezení v podpoře QL na některých interface, vyhodnocení provozního stavu interface z hlediska synchronizace, problémy při zavěšování na záložní referenční vstup nebo omezení typů interface definovatelných jako záložní reference.

- Topologie se ve vybraných uzlech překrývají, a protože jejich fázové odchylky v normálním stavu splňují odpovídající požadavky, jsou si schopné v případě poruchy synchronizaci vzájemně předat bez fázových skoků, narušujících provoz.
- Záloha synchronizace, realizovaná těmito protokoly, je zásadně vratná – po obnově přenosu relace se postižený strom vrací do normálního provozního stavu.

Příklad takové logické topologie - dvojitého stromu ACR o hloubce 4, ukazuje obrázek (stromy A a B jsou barevně odlišené, lokální vazby označené T12.1 jsou specifikou použité přenosové technologie).



OBR. 21 – PŘÍKLAD SCHÉMATU ACR S PŘEKRÝVAJÍCÍMI SE STROMY

Stejně jako klasická schémata, i schémata nepřímého šíření vyžadují detailní návrh v rozsahu sítě. Zásady návrhu se od klasických v detailech liší:

- Fyzická topologie sítě musí být optimálně segmentována na (překryvné) domény šíření synchronizace end-to-end (pátevní, regionální, lokální, záložní, pro plesiochronní provoz, apod.),
- pro signalizaci QL/SSM musí být zvolen vhodný profil s ohledem na aplikaci a mezi segmenty musí pro ni být zajištěn řízený přístup.
- Optimalizace segmentace vychází z odpovídajících funkčních omezení provozovaných nebo plánovaných zařízení (adresování, potřebnou licenční výbavu zařízení, apod.)
- Součástí návrhu je opět kontrola délky synchronizačních cest v navrženém schématu proti limitům příslušných standardů v plně provozním stavu a vybraných poruchových stavech, včetně případně lokalizace prvků s vyšší stabilitou generovaných signálů (SSU).

Výše uvedenou kapitolu je nezbytné realizovat s nejvyšší prioritou, neboť od synchronizace celé přenosové sítě (TDM, PSN) včetně telefonních ústředí a GSM-R se odvíjí další její rozvoj. V dalších částech Studie je řešeno jako samostatné investiční akce.

4 DOHLEDOVÝ MANAGEMENT SÍTĚ

V návaznosti na *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti* je nutné zařadit všechny aktivní prvky datové sítě SŽDC pod dohledové servery, umožňující sledovat stav dohledovaných zařízení až na úroveň jednotlivých interface, portů a služeb. Tam, kde to koncové zařízení neumožňuje, je nutné naplánovat náhradu zařízení. V případě úzce specializovaných zařízení technologické datové sítě je nutné obnovu posuzovat a plánovat individuálně, případně budou jednotlivá zařízení nahrazena novějšími při generační obnově celého technologického celku.

Tato kapitola obsahuje potřebné teoretické části (kapitoly 4.1.1, 4.1.2, 4.1.3, 4.1.4), obecné závěry a doporučené postupy (4.1.2.4, 4.2) pro další řešení koncepce managementu jednotlivých sítí a centrálního managementu, včetně naznačení možných vazeb.

4.1 Teoretické předpoklady

Obecně návrh dohledu (monitoringu) ICT infrastruktury vyžaduje stanovit pro infrastrukturu jako celek, nebo pro její záměrně vydělené části:

- Architekturu komunikace mezi řízenými ICT prvky a dohledovými (monitorovacími) aplikacemi, resp. navzájem mezi aplikacemi, typicky ve vícevrstvé hierarchii (z hlediska funkcí a rozsahu monitorovaných prvků, blíže kapitola 4.1.1), ovlivněnou členěním dohledovaných ICT prostředků na administrativní domény (diktované spíše využívajícími procesy, než technologickými hledisky);
- Základ modelu správy poruch (*Fault Management*, FM) pro vrcholový (*umbrella*, nejvyšší ve stanovené hierarchii) management, kde jsou služby (zde v **ICT smyslu** jako typy konektivit, resp. aplikací IT využívaných nějakým procesem) klasifikovány a obrazy jednotlivých technologií unifikovány na základě vytvořeného *modelu služeb*. Model zahrnuje mj. i klasifikaci zařízení podle jeho vlivu na sledovaný provoz (traffic-affecting, pro ICT služby, resp. hlavní procesy);
- Mapu uživatelských oprávnění (zejména, bude-li uplatněna uživatelská informovanost o incidentech) na základě provedené analýzy organizačních útvarů³, spravujících určitý proces nebo jeho část a využívajících definované ICT služby (v předchozím smyslu).

V případě návrhu dohledu (monitoringu) již existující ICT infrastruktury nebo infrastruktury již v nějakém schématu monitorované musí uvedeným krokům předcházet audit (detailní analýza) stávajícího stavu, včetně případných již schválených rozvojových záměrů pro nástroje dohledu, nejméně v rozsahu níže blíže popsané v kapitole 4.2.

4.1.1 ARCHITEKTURY KOMUNIKACE S MONITOROVANÝMI PRVKY

Informace z monitorované technologie jsou často zpracovávány v různých monitorovacích nástrojích, vyhrazených např. pro monitoring, správu konfigurací, výkonnosti, apod. Mezi

³ Zjištěné organizační struktury jsou často rovněž nazývané „služby“, zde v **organizačním smyslu**.

různými způsoby současného napojení těchto nástrojů můžeme identifikovat dvě základní architektury:

- **U paralelní architektury** jsou data z konkrétního prvku sbírána **paralelně** na více cílových systémech. Prvky jsou jednotlivými nástroji monitorovány v podstatě nezávisle. Změny, které musí být **promítnuty do každé vazby zvlášť**, představují nastavení cíle spontánní komunikace na straně prvku, zavedení odpovídajícího informačního modelu (MIB) na straně nástroje. Informační modely přitom mohou být vůči jednotlivým nástrojům podle jejich účelu stejné, nebo různé (podmnožiny obecnějšího modelu). Udržení konzistence těchto vazeb je věcí nástroje nebo procesů *provisioningu* sítě;
- **U hierarchické architektury** jsou data z konkrétního prvku sbírána pouze na primární monitorovací nástroj (obvykle nástroj spravující rovněž jejich konfiguraci). Primární nástroj pak data v původním, nebo předzpracovaném rozsahu poskytuje systémům dalším. Může tak vzniknout i hierarchie víceúrovňová. Časté je přepracování informace na logické úrovni na **společný informační model** (datové popisy a syntaxi zpráv a atributů). Pro vytvoření vazby primárního nástroje na prvek nového typu pak stačí pouze přidání nové instance již existujících typů objektu, které jsou pro vysokou úroveň abstrakce aplikovatelné i na nově přidáný typ;

Obě architektury vykazují odlišnosti a mají svá charakteristická omezení, a proto jsou v praxi často kombinovány (např. spontánní komunikace hierarchicky, doplňující *polling* paralelně).

4.1.2 MODEL MANAGEMENTU SLUŽEB

Základem monitoringu každého procesu je odpovídající model, který odráží rozhodující vztahy mezi komponenty procesu nebo systému a dovoluje z dílčí informace odvozovat informaci obecnější, popisující abstraktní komponenty procesu nebo systému. Vrstvený model monitoringu, využívaný převážně pro ICT, který vychází ze standardizovaných dohledových rámců, ukazuje následující obrázek Obr. 22.

Model zahrnuje tři základní vrstvy, lišící se stupněm zobecnění dohlížených prostředků, ale především cílovou skupinou uživatelů v hierarchii organizační struktury podniku, které každá z vrstev poskytuje obraz stavu komunikační sítě ve struktuře a hloubce potřebné pro jejich práci (vykonávané procesy). Obrázek paralelně znázorňuje hierarchii monitoringu IC i IT prostředků.

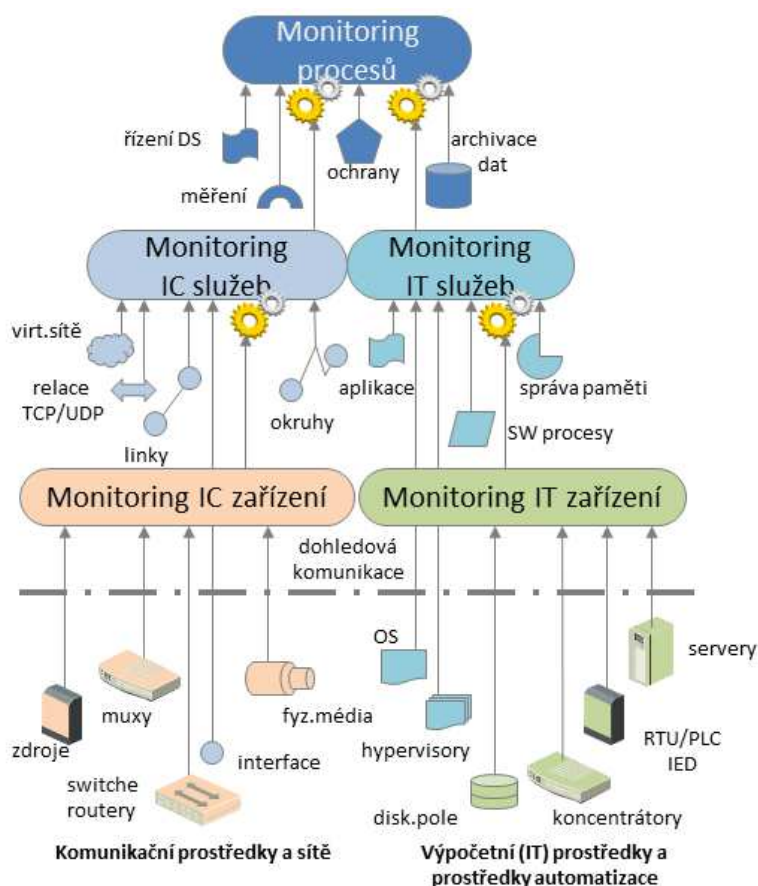
- **Monitoring procesů** svými výstupy primárně slouží pro manažerskou úroveň řízení a dává celkový přehled o stavu ICT podpory základních procesů, jejichž příklady jsou v obrázku uvedené. Obsahuje model těchto procesů z hlediska jejich podpory ICT systémem, jako logických objektů, jejichž stav je generován korelací dat z nižší vrstvy.

Monitoring služeb je primární úroveň pro výměnu informace mezi jednotlivými uživateli ICT podpory a jejím poskytovatelem (poskytovateli)⁴, sloužící operativnímu řízení (on-line

⁴ Vztah uživatel – poskytovatel v ICT prostředí může být obousměrný. IC prostředky typicky poskytují komunikační kanály pro IT prostředky. Některé subsystémy komunikační sítě (typicky právě subsystémy pro dohled a monitoring) jsou naopak realizovány IT prostředky, které mohou být zajištěny sdílenou službou a spravovány (částečně) týmem IT.

monitoring), plánování a vyhodnocování (reporting), případně je podkladem pro platby, je-li vztah uživatel-poskytovatel nastaven jako komerční. Logické objekty tvořící model představují hierarchicky modelované funkce (soubory funkcí) komunikačních a výpočetních systémů podporující procesy DŘ, v komunikačním prostředí typicky nazývané

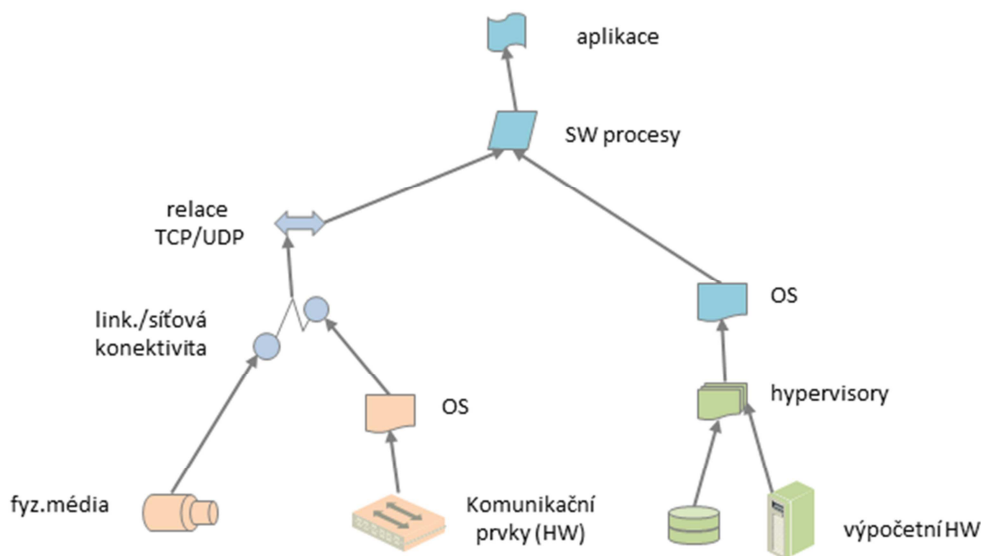
- „služby“. Provozní stavy těchto logických objektů jsou získány buď přímým sběrem relevantních dat z monitorů na koncových bodech služby (viz end-to-end model odst. 4.1.2.2), nebo korelací dat z nižší vrstvy (korelační model, odst. 4.1.2.1). Vrstva může být horizontálně členěná na monitorovací systémy specializované na jednotlivé druhy ICT prostředků (IC, IT, prostředky okruhové vs. paketové komunikace, apod.).
- **Monitoring fyzických prvků (zařízení)** je primární úroveň monitoringu pro správce (IC nebo IT)⁴ prostředků. Model vrstvy obvykle tvoří přímé mapování datových položek v systému na hierarchicky uspořádané subsystémy komunikačních a výpočetních prostředků, jejichž provozní stavy jsou získány sběrem dat přes nativní dohledové protokoly. Vrstva je typicky horizontálně členěná na dohledové systémy specializované na jednotlivé druhy ICT prostředků a/nebo na ICT prostředky jednotlivých dodavatelů.



OBR. 22 – MODEL MANAGEMENTU SLUŽEB

ICT služby jsou typicky představovány aplikací běžící na výpočetních prostředcích (HW, SW), propojenými vzájemně komunikačními prvky (HW, SW), využívajícími komunikační média a

poskytujícími různé úrovně konektivity. Rozpad ICT služby na jmenované komponenty a vazby mezi nimi ukazuje obrázek Obr. 23.

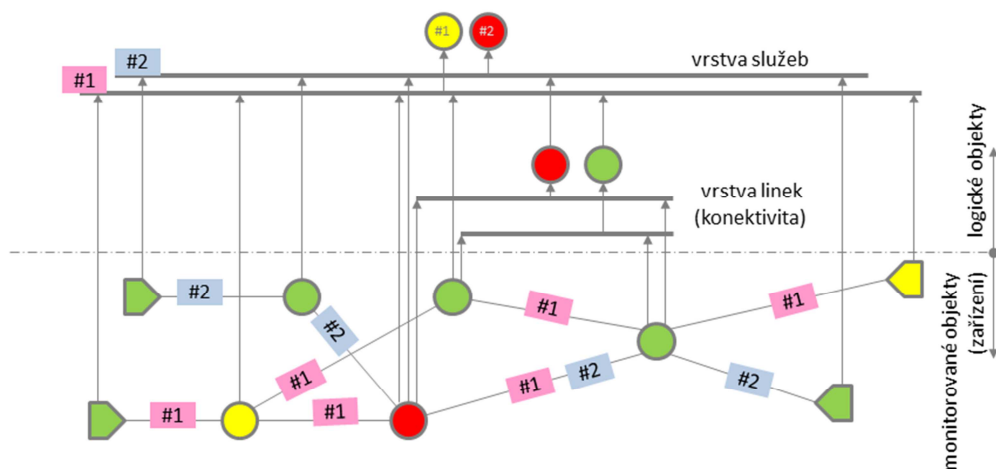


OBR. 23 – ROZPAD ICT SLUŽBY NA KOMPONENTY A VAZBY MEZI NIMI

Vazby tvoří mezi komponenty hierarchickou strukturu podmiňující funkčnost vyšší úrovně úrovní nižší. Hierarchie dobře odpovídá přiřazení jednotlivých komponent vrstvám monitoringu z předchozího obrázku a představuje nejhrubší dostupný model pro vyhodnocování funkčnosti. Detailnějším modelům, reprezentujícím různé způsoby vyhodnocování, jsou věnovány následující odstavce.

4.1.2.1 Korelační model

Model vychází z obecných modelů sítí a jejich vyšších úrovní (síťové, služeb), využívaných často i jako popisný aparát pro účely standardizace. Ilustrační schéma tohoto modelu ukazuje obrázek, znázorňující průchod dvou služeb (#1 a #2) mezi předávacími body přes různé síťové prostředky s možností alternativní cesty (#1) nebo bez ní (#2):

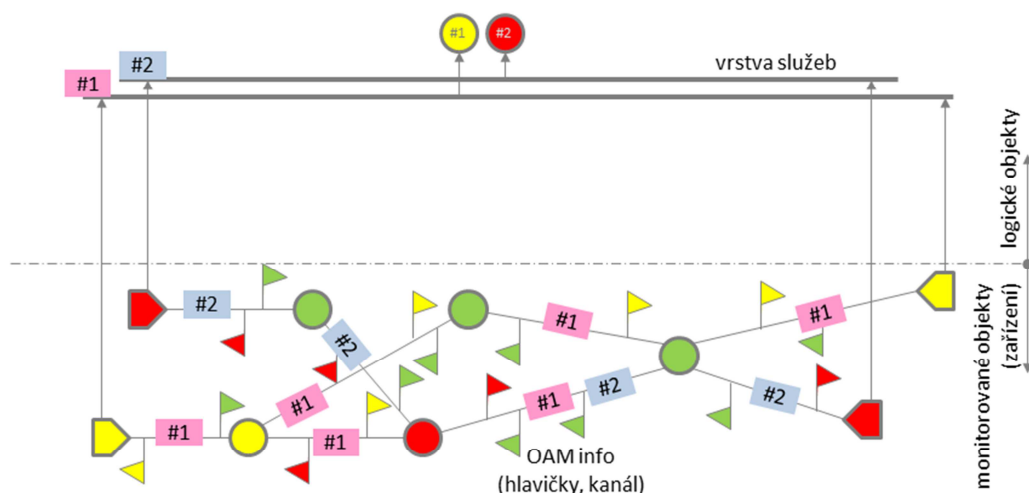


OBR. 24 – KORELAČNÍ MODEL

Síťové prostředky jsou vybaveny schopností rozlišit lokálně provozní a neprovozní stav jednotlivých svých funkčních a signalizovat tento stav v dohodnutém objektovém modelu monitorovacího systému (vyznačeno barevně ve škále zelená - plná provozuschopnost, žlutá / červená - různé stupně degradace). Pouze některé stavy, obvykle označovány jako *traffic affecting*, mají v korelačním schématu na výslednou službu reálný vliv. Nad síťovými prostředky je vytvořen model služby, představovaný souborem pravidel, podle kterých se stav prostředků promítá do stavu služby - logické entity. I logické entity se sekundárně vyhodnocovanými stavy mohou být hierarchicky členěné do vrstev, odpovídajících tomu kterému síťovému modelu (např. *linky* jako speciální typ *konektivity*),

4.1.2.2 End-to-end model

Tento alternativní model vychází z rozšířených funkcí monitoringu na úrovni vlastních prostředků, které již nejsou pouze lokální, ale jsou schopny stav služby přímo vyhodnotit. Ilustrační schéma tohoto modelu na stejné infrastruktuře a souboru služeb ukazuje obrázek:



OBR. 25 – END TO END MODEL

Síťové prostředky typu *port / interface* jsou u tohoto modelu vybaveny dodatečnou monitorovací funkcí, která je schopna s dodatečnou přesností aproximovat chování zakončené *konektivity* (obecně ICT funkce) vůči uživatelským datům. To se obvykle děje pomocí dodatečné služební (systémové) informace, doplňované k uživatelským datům ve formě záhlaví, nebo služebního (přidruženého) kanálu (v obrázku znázorněno praporky, postupujícími směrem své špičky). Každý prostředek, účastník komunikace, modifikuje obsah služební informace podle svého aktuálního stavu, opět pouze ty stavy, u kterých se očekává vliv na službu (*traffic affecting*). Model služby nad síťovými prostředky je prostá množina těchto koncových monitorů, na které jednoduchým pravidlem (logickým součtem) vyhodnocován stav služby.

4.1.2.3 Specifika dohledu hlasových služeb

Základním prvkem, modelujícím hlasový systém pro účely monitoringu je *ústředna* – prvek schopný komutovat hlasové spoje mezi lokálně obsluhovanými KZ (přípojky, *extension lines*) a/nebo propoji na jiné komutační prvky (*trunk*y). KZ jsou v tomto modelu telefonní přístroje a další zařízení, zakončující hovorový spoj (dispečerské konzole, záznamové jednotky), jejichž provozní stav je indikován nepřímo přes stav přípojky. Infrastruktura přenosu dat, propojující tyto prvky hlasového systému je servisní vrstvou, pro model neviditelnou.

V nejčastějším prostředí monitoringu protokoly SNMP je model opět rozdělen do různě zobecněných stupňů:

- Úroveň modelu nezávislá na (výrobci) konkrétního systému je SNMP DIAL-CONTROL-MIB (IETF RFC2128), patřící do skupiny MIB-2 *transmission* (21), administrované US DOD. Dohlíženým elementem je především *hovorové spojení* (*call*), jehož atributy se vztahují k propojovacím trunkům mezi peer-ústřednami (end-to-end model kapitola 4.1.2.2). Model nerozlišuje typy KZ (přípojek) ani typy ústředen, které nejsou nijak hierarchicky uspořádané (*peer-to-peer*).
- Firemní MIB spojovacích systémů (příkladem jsou i firemní MIB prvků řešení Cisco UC, např. CISCO-CCM-MIB nebo SNMP výbava Cisco UBE – SW implementace GW/SBC na ISR G2+) tento model rozšiřují o vnitřní struktury *ústředen*, např. jejich logická propojení do *clusterů*, explicitní registraci peer-ústředen i KZ a jejich rozdělení do skupin s přiřazením unifikovaných konfigurací, dovolující zavést zálohovací mechanismy, účinnější zabezpečení, apod., oddělení identifikace KZ a *přípojky*, dovolující jejich dynamickou asociaci a správu poruch vlastních KZ (vázané ale obvykle na firemní protokoly mezi ústřednou a KZ), podrobnější statistiky, rozšířený soubor notifikací (trapů), soubor atributů dovolujících konfigurovat tyto rozšířené funkce.
- Samostatné MIB obsahují informace k HW/SW k prostředkům platformy (server nebo SW směrovač), hostující dohlížený prvek hlasového systému s obvyklým generickým obsahem (stav a využití CPU, paměti, DSP, správu SW image, správu interface apod.).

Správa hlasových systémů v prostředí SNMP ale ani tak není tak komplexní, jako u komunikačních prvků datové sítě (přepínače, směrovače). V mnoha implementacích hlasové aplikace chybí podpora SNMP notifikací (trapů) a pro SW prostředí (aplikace, procesy, OS) typicky chybí podpora SNMP úplně. Sběr provozních stavů a statistik je v těchto případech nutné zajistit příjmem a vyhodnocováním *syslog* zpráv, některé funkce notifikace lze suplovat pomocí skriptovacích nástrojů (např. TLC skripty EEM na platformách Cisco).

4.1.2.4 Výběr modelu

Identifikace primárně využívaného modelu služeb je principiální otázkou komplexního monitoringu, významně ovlivňující uživatelský i administrátorský komfort (výsledně se promítající do provozních nákladů) i náklady na pořízení systému. Během výběru je nutné zhodnotit následující faktory:

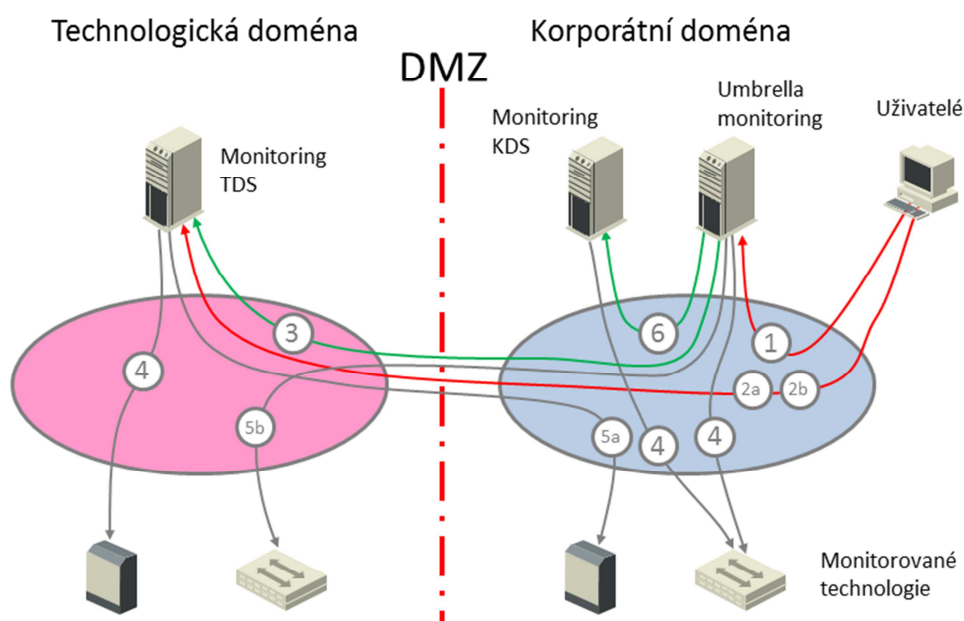
- Nakolik lze u provozovaných technologií zajistit **konzistenci** mezi souborem **vyhodnocujících pravidel**, a skutečným vlivem prostředků na stav služby. Kromě řídkých případů, kdy takovou konzistenci ani zajistit nelze je hlavním problémem udržení této konzistence při změnách služeb. Ve většině reálně provozovaných sítí je objem signalizovaných stavů a pravidel takový, že konzistence musí být zajištěna dalším automatickým prostředkem – nástrojem pro *provisioning* (zřízení) služby. Některé dopady toho jsou diskutovány v kapitole. 4.1.3.
- Nakolik je **komplexita pravidel** pro korelační model zvládnutelná manuálně, případně automatickými systémy. Komplexita roste zejména s dynamikou síťových systémů (dynamické směrování, zálohy). Zatímco staticky definovaný model historicky plošně uplatňovaný u TDM techniky vystačil plně s korelačním pravidlem logického součtu vstupních stavů, dynamické směrování vyžaduje pravidla dynamicky modifikovaná signalizovanými stavy (např. obsahy směrovacích tabulek).
- Nakolik je na koncovém rozhraní zařízení zajištěna **podpora** nebo možná **implementace monitorovacích prostředků pro end-to-end** monitoring (není automaticky splněno u všech síťových zařízení).
- Nakolik používané **nástroje provisioningu** dovolují **asociaci a parametrizaci** těchto prostředků (protější koncový bod, typ monitorovacích signálů, apod.), které jsou obvykle funkční option, v krajním případě aplikace třetí strany.
- Nakolik je pro využití monitorovacího nástroje nutný **drill-down na poruchy**, které jsou příčinou indikovaného stavu. Ten u end-to-end modelu není možný, protože síťové prostředky kromě koncových bodů nejsou ke službě asociovány.
- Nakolik jsou ve zvoleném hierarchickém (kapitola 4.1.1) prostředí unifikované interní datové modely (např. generické SNMP MIB, dostupné pro import do daného nástroje), a nakolik jsou dostupné a implementovatelné „překladače“ objektů (*Object Brokers*), které struktury a syntaxe upravují do podoby cílového systému - implementace je typicky složitá a nákladná a ne všechny nástroje jsou pro ni dostatečně otevřené.

4.1.3 VLIV BEZPEČNOSTNÍCH DOMÉN

Nezanedbatelným kritériem pro volbu architektury vrcholového (*umbrella*) systému monitoringu jsou podmínky přístupu, dané bezpečnostními politikami a rozdělením ICT systému na bezpečnostní domény. V případě SŽDC se jedná o rozdělení prvků a systémů

- mezi jednotlivé technologické sítě a intranet;
- oddělení jednotlivých technologických sítí mezi sebou;
- rozdělení intranetu na intranety SŽDC, jednotlivých přepravek, případně dalších subjektů;
- případně oddělení nativních technologických sítí od jejich částí řešených VPN v intranetu.

Obrázek ukazuje příklad jednoduchého schématu rozdělení na dvě domény a možné interakce prvků monitorovacího systému mezi nimi:



OBR. 26 – ROZDĚLENÍ NA DVĚ DOMÉNY S MOŽNÝMI INTERAKCEMI PRVKŮ MONITOROVACÍHO SYSTÉMU

- Komunikace **uživatelů se servery** umbrella monitorovacího systému se odehrává jen v rámci KDS (1);
- Komunikace **uživatelů se servery** specializovaných systémů přístupem z KDS do TDS se může odehrávat **tenkými klienty (2a)** nebo **tlustými klienty (2b)**, využívajícími specifické porty TCP a uzavřené protokoly;
- Komunikace hierarchicky výše postavených **monitorovacích (umbrella) systémů na systémy specifické**, kde je z hlediska bezpečnosti opět důležitá komunikace mezi systémy v KDS a TDS (3);
- Komunikace monitorovacího (obecně dohledového) systému **na monitorované prostředky** je převážně v rámci vlastní domény (4). Některá schémata však využívají přímou paralelní komunikaci mezi vrcholovým (umbrella) monitorovacím systémem a monitorovanými prostředky. Lze očekávat hlavně komunikaci systémů v KDS na prostředky v TDS (5b), opačná (5a) je méně pravděpodobná.

Pro výběr schématu jsou důležité následující aspekty:

- **stupeň oddělení sítí**, obecně praktikovaný ve dvou úrovních - firewallem, který povoluje komunikační toky s určitými charakteristikami (adresy, TCP/UDP porty, apod.), nebo DMZ, která všechny datové relace ukončuje na aplikační úrovni (klient/server dané relace je uvnitř DMZ) a transversální komunikaci zásadě nepovoluje;
- **charakter komunikačních protokolů** - komunikace buď otevřenými protokoly po omezeném souboru portů (např. uživatelská HTTPS port 443, SNMP port 160/161), nebo uzavřenými protokoly se specifickými porty, využití otevřených protokolů jako tunelů pro

jiné druhy komunikace (např. HTTP/HTTPS pro SOAP, typicky vyžaduje nasazení IDS na aplikační úrovni), resp. komunikace přes dynamicky otevírané (privátní) porty TCP;

- **počty komunikačních protějšků** v cizí doméně (např. uživatelů, monitorovaných zařízení, často s roztríštěnými adresovými prostory), které zvyšují objem bezpečnostních pravidel.

4.1.4 NÁVAZNOST NA PROCESY

4.1.4.1 Standardy ITIL

Procesním zajištěním provozu ICT prostředků se zabývá mimo jiné standardizace ITIL. Oblasti ITIL, relevantní ke studované problematice jsou

- řízení incidentů (*Incident Management*);
- případně řízení změn (*Change Management*).

ITIL (případně ISO 20000) rozlišuje **incident** ve dvou významech:

- 1) **Neplánované** přerušení služby nebo snížení její kvality – obvykle hlavní úroveň pro informovanost
- 2) Jakákoli **událost** mimo normální provozní režim, která **může způsobit** přerušení služby nebo snížení její kvality – úroveň pro informovanost správců, On-line informování uživatelů služeb o incidentech v této úrovni, kdy korektivní akce má preventivní charakter (k přerušení služby nebo snížení její kvality zatím nedošlo), není obvyklá. Na zvážení je pouze informovanost uživatelů, ve které fázi procesů řízení problémů a změn se řešení incidentu nachází. O technických prostředcích pro podporu takových procesů pojednává kapitola 4.1.4.2.

Významný vliv na rozsah i technické parametry systému monitoringu má rozhodnutí o uživatelských skupinách (rolích), které budou pro jednotlivé úrovně (významy) incidentu informovány:

- **Správci** dotčených systémů, zodpovědní za patřičnou reakci, která nedovolí stavu eskalovat na úroveň prvního významu, budou informováni v obou případech. V rámci ITIL je reakce představovaná navazujícími procesy řízení problémů a změn (*Problem Management, Change Management*), které jsou náplní administrátorů systému a jejich specializovaných útvarů.
- **Uživatelé služby** – pracovníci na službu navazujících útvarů, mohou být v případě 1) informováni on-line, častější je informovanost uživatelů, ve které fázi procesů řízení problémů a změn se řešení incidentu nachází. O technických prostředcích pro podporu takových procesů pojednává kapitola 4.1.4.2. Rozsahem zpřístupnění výsledků jsou uživatelé velká skupina, definovaná obvykle nepřímými rolmi v navazujících procesech. Informování uživatelů služeb o incidentech v úrovni 2), kdy korektivní akce má preventivní charakter (k přerušení služby nebo snížení její kvality zatím nedošlo), není obvyklé.

4.1.4.2 Technické prostředky řízení procesů

Technickým prostředkem pro řešení incidentů a změn v ICT (obecně jakýchkoli technických) prostředcích v návaznosti na obsluhované procesy (uživatele) jsou systémy *ServiceDesk*. Primární úlohou tohoto prostředku je automaticky i poloautomaticky přijímat požadavky procesů (uživatelů) a evidovat je pro podporu jejich následného řešení.

Při rozhodování o podobě nově budovaných, nebo úrovni propojení existujících systémů *ServiceDesk* je potřeba vzít v úvahu následující faktory:

- bude-li *ServiceDesk* využíván jako další vstup pro *Incident Management* pro sledování kvality vlastních služeb přes párování technicky zaznamenaných incidentů a reklamací od uživatelů⁵;
- nakolik bude veden a uživatelům zpřístupňován *log* následných pracovních kroků spojených s řešením incidentu nebo změny (viz kapitola 4.1.4.1);
- bude-li začleněna evidence řešitelské kapacity, její přidělení k jednotlivým případům a podíl na řízení jejich činností (např. svolávání, výstupy na evidence pracovních výkazů, evidenci a povolování výluk, vazby do ŘS předmětných technologií přes dispečinky, apod.);
- jaká data budou poskytována pro do reportingu / dokladování (reakčních dob, objemů prací, apod.);

4.1.5 OBECNÉ POŽADAVKY NA CÍLOVÝ UMBRELLA-SYSTÉM

Z rozborů podmínek nasazení monitorovacích systémů v kapitolách 4.1.1 až 4.1.4 plynou některé obecné požadavky, které mohou být podle tam zmíněných kritérií dále konkretizovány.

Klíčový pro schopnost funkce monitorovacího systému na úrovni zobecněných služeb je otevřený informační model, schopný pracovat s dostatečnou granularitou s logickými objekty a alespoň minimálním aparátem korelačních pravidel:

- Systém musí být schopen **práce s logickými objekty** dodefinovanými nad rámec MIB monitorovaných zařízení.
- **Granularita informačního modelu.** Má-li dotčený systém pracovat s rozlišením na úrovni jednotlivé služby, musí při monitorování fyzických prostředků dovolovat rozlišení až na fyzické, resp. různé typy virtuálních portů a v případě IT i na služby OS, procesy a aplikace, které se na konkrétní službě podílejí. Objekty v této granularitě musí samostatně vstupovat do individuálních korelačních vztahů. Systémy, které takové rozlišení nativně neposkytují, budou složité rozšiřitelné o logické modely služeb a schémata přístupových práv k nim (viz kap.), pokud takové rozšíření bude vůbec možné.
- **Obecná schopnost korelace** je pro budování modelů služeb (viz kapitola 4.1.2) zásadní, nicméně více než soubor pravidel uplatňovaný v základní konfiguraci monitoringu

⁵ Praktické uplatnění tohoto modelu však vyžaduje selektivní informovanost skupin uživatelů a správců. Při společném informování obou skupin hrozí zkreslení prováděné klasifikace a zvyšují se nároky (rychlost odezvy, resp. rozsah) a tím i jednostranně náklady na korektivní akce na straně správců.

prostředků tolik rozhodující není. Minimální požadavky jsou odvislé od použitého korelačního modelu, kdy end-to-end model klade nároky minimální, korelační model naopak velmi vysoké co do elementárních funkcí a pružnosti uplatňovaných pravidel.

Dalším klíčovým souborem funkcí je **správa uživatelských oprávnění**.

- Pro pokrytí potenciálních uživatelů komplexního monitoringu je nutné **odstupňování oprávnění** především **po typech dat**, z nichž většina jsou typy dat dodefinované v rámci rozšíření informačního modelu o logické objekty. Klíčová je proto flexibilita systému oprávnění v tomto směru s rozlišením minimálně po typech, optimálně však i po instancích objektů (definovaných pro každého uživatele výčtem – selekce stejných služeb poskytovaných pro jiný účel nebo v jiném místě).
- Naopak nároky na **funkční odstupňování** oprávnění jsou u studovaného monitoringu služeb minimální, omezené na zobrazování dostupné informace. Tyto požadavky mohou plnit i systémy s fixními rolemi. Výrazné zvýšení nenastává ani, pokud je systém monitoringu spojen s aktivní poloautomatickou správou služeb, kdy jsou funkční oprávnění rozšiřována jen o modifikace, případně zřizování a rušení objektů a pravidel.

Požadavky jsou rovněž kladeny stavový model služby a jeho zobrazení na UI.

- Za **minimální standard** je stejně jako u dohledu fyzických prostředků považován **alarmový záznam** s plnou identifikací zdrojového objektu (k rozlišení zdrojů viz výše), typu anomálie, aktuálního stavu a časového údaje poslední změny, který tvoří minimum pro úspěšnou dodatečnou korelaci v čase i síťových vazbách.
- Mělo by být implementováno **stavové** (*stateful*) schéma alarmů, které jediné může stabilně indikovat výsledky korelací, prosté bezstavové (*stateless*) chronologické řazení signalizovaných změn (*events*) obvykle hrozí vznikem neřešitelných inkonzistencí.
- Ostatní parametry alarmového záznamu (počet stavů, úrovně urgency) nejsou pro služby významné. Pro vyhlášení incidentu služby je rozhodující klasifikace poruch nižších úrovní (fyzická, síťová) z hlediska narušení služby – příznak *traffic affecting*. Tato klasifikace je prakticky permanentní a je součástí korelačních pravidel monitorovaných prostředků na dotčenou službu. Ostatní klasifikace ve vrstvě prostředků (URG/NURG, ...) mají význam pouze tam a určují naléhavost (prioritu) preventivního korekčního zásahu.
- Pokud má monitoring pracovat s grafickým (mapovým nebo stromovým) zobrazením stavu služeb, musí GUI podporovat základní logické objekty typu linek (obecněji mnohabodové konektivity) a kontejnerů a musí mít schopnost přiřadit tyto typy grafických objektů logickým objektům rozšiřujícím informační model.

Mimo požadavky na vlastní monitorovací systém naopak stojí jinak klíčové požadavky na udržení konzistence korelačních pravidel (*change management* ITIL, kapitola 4.1.4.1), která je předmětem navázaných (polo)automatických systémů nebo procesů *provisioningu* služeb.

4.2 Inventura dohledového prostředí

Stanovení strategických cílů a postupů dohledu / monitoringu ICT technologií v prostředí SŽDC musí předcházet důkladný audit celého prostředí, sestávající ze dvou úrovní auditovaných skutečností:

- audit vlastností provozovaných zařízení z hlediska dohledovatelnosti, podrobněji rozvedeno v kapitole 4.2.1;
- audit provozovaných, případně plánovaných dohledových systémů úrovně EML/NML pro skupiny výše uvedených ICT zařízení z hlediska jejich způsobilosti poskytnout stavová data pro úspěšnou korelaci na poskytované služby (jejich modely viz kapitola 4.1.2) a případné schopnosti administraci služeb případně převzít, podrobněji rozvedeno v kapitole 4.2.2;

a následně podle výsledků musí být provedena klasifikace „služeb“ v obou používaných smyslech slova, popsanych v úvodu kapitoly 4.1.

4.2.1 AUDIT DOHLEDOVANÝCH TECHNOLOGIÍ

Pro každý typ (*class*) dohlíženého prvku (NE) takový audit konkrétně zahrnuje zjištění:

- výrobce, typu, rozsahu aktuálně řízených verzí;
- dohledový protokol a využívaný režim snímání stavů (*events/traps, polling* vč. intervalu a počtu NE na segmentu), způsob identifikace NE (adresování);
- agent dohledového protokolu (u komunikačních zařízení obvykle nativní integrovaný v OS);
- granularita zdroje stavové signalizace v rámci NE (NE – modul – port – kanál/VI);
- podpora indikace standardních alarmových stavů (IS/OOS, *up/down, operation/administrative*, apod.) a konzistence alarmových stavů po jednotlivých typech modulů a interface;
- podpora urgency alarmu (fixní, konfigurovatelné nebo dynamické schéma);
- koincidence monitorovaných rozhraní NE s předávacími službami;
- hodnocení z hlediska možnosti nasazení volitelných nástrojů end-to-end monitorování služeb přímo na zařízení.

a též specifické údaje k aplikaci těchto zařízení:

- příslušnost k jednotlivým „sítím“ (technologickým nebo VPN Intranetu jednotlivých subjektů), kde zařízení může být sdíleno i několika sítěmi, v krajním případě i bezpečnostními doménami;
- klasifikace zařízení podle vlivu na monitorované služby (*traffic-affecting*).

Objem prací, reprezentující tuto fázi, bude relativně značný. Podle předběžných podkladů je u SŽDC cca 13500 evidovaných zařízení 247 technologických rodin, z nichž je zatím pouze 73 identifikovaných jako monitorovatelných přímo nebo nepřímo (přes proxy, např. telefony přes ústřednu), u 167 rodin (představujících téměř 50% zařízení) je to teprve potřeba podle detailních podkladů zjistit.

4.2.2 AUDIT DOHLEDŮ SÍTÍ

Pro posouzení dohledových systémů z hlediska jejich výše uvedených způsobilostí takový audit konkrétně zahrnuje zjištění:

- výrobce, typ dohledového systému;
- u existujících systémů instalovaná verze, její stáří a podporovatelnost;
- soubor volitelných komponent (je-li - nainstalované komponenty / doplňkové nástroje, licence, apod.), u existujících systémů instalované komponenty pro NBI/API a/nebo export dat;
- existující / plánovaná platforma HW/OS a její funkční / výkonová rezerva;
- způsob zpracování stavové informace (events/alarms – *statuful/stateless...*) na úrovni EML a NML (je-li), formát a atributy zobrazovaných poplachových stavů, *drill-down* mezi úrovněmi;
- využití DB při sběru stavové informace (přímá komunikace s NE vs. průběžně plněná stavová DB, historické záznamy, apod.);
- podpora urgency alarmu – fixní schéma, konfigurovatelná, dynamická podle pravidel, apod.;
- systém uživatelských oprávnění, počet úrovní přístupu, uživatelské role, prostředky pro *partitioning* sítě a možnost externí správy uživatelů a ID;
- možné metody přístupu k interním datům systému (protokolový nebo souborový NBI/API, přístup do DB, apod.), případně možnosti volání komponent EMS/NMS z jiné aplikace;
- podporovaný soubor funkcí FM (PM a diagnostiky), u existujících systémů též skutečně operátory využívaný.

5 KOMUNIKACE DŘT, DDTS ŽDC V ENERGETICKÝCH OBJEKTECH

V rámci sítě SŽDC jsou v energetických objektech provozovány řídicí systémy, které zpracovávají vstupní informace a pomocí datové komunikace v reálném čase je přenášejí do oblastních elektrodispečinků (dále jen ED) do systému dispečerské řídicí techniky (dále jen DŘT), dálkové diagnostiky technologických systémů železniční dopravní cesty (dále jen DDTS ŽDC). Dále jsou přenášeny přímé povely pro dálkové ovládání silových prvků (např. ochrany mezi napájecími stanicemi, ochrany distribuční sítě). Veškerá komunikace probíhá oběma směry, ve směru od energetického objektu do ED mají data většinou informační charakter, data z ED směrem do energetických objektů přenášejí přímé povely pro dálkové ovládání silových prvků.

Pro přenos těchto informací do nadřazených systémů a pro dálkové ovládání silových prvků je nutné vytvořit v přenosové síti SŽDC takové podmínky, aby přenos těchto informací byl co nejspolehlivější, s garantovanou přenosovou rychlostí. Nutno říci, že problematika přenosů a stanovení kvalitativních podmínek je natolik rozsáhlá, že je vhodné zpracování samostatné studie, řešící tuto problematiku samostatně. Doporučuje se při zpracování samostatné studie vycházet z metod analýzy a návrhů dle skupiny norem ČSN EN 61968 Integrace aplikací v energetických společnostech - Systémová rozhraní pro řízení dodávky elektrické energie a ČSN EN 61850 Komunikační sítě a systémy pro automatizaci v energetických společnostech. K jednotlivým bodům studie uvádějícím definice a rozsahy kvalitativních požadavků doplnit jednoznačné přiřazení a určení konkrétních hodnot přenosových parametrů vztahujících se k jednotlivým typům přenášených dat.

Parametry pro přenosovou síť vychází zejména z níže uvedených řad norem, ve kterých se stanovují kvalitativní požadavky pro výše systémy (DŘT, DDTS ŽDC, ochrany napájecích stanic, distribuční sítě). Tyto kvalitativní požadavky vycházejí především z norem řady:

- ČSN IEC 870-x a ČSN EN 60870-x – Systémy a zařízení pro dálkové ovládání.
- ČSN EN 61850-x-x – Komunikační sítě a systémy pro automatizaci v energetických společnostech
- ČSN EN 60834-1 – Zařízení pro přenos povelů ochrany elektrizační soustavy
- ČSN 33 4690-2 – Provoz a zkoušení zařízení dálkových ochrany elektrizační soustavy

Uvedené řady norem definují parametry, časové odezvy přenosové sítě pro spolehlivý přenos informací. Doporučuje se v rámci přenosové sítě SŽDC tyto parametry respektovat.

5.1 Normy, předpisy

5.1.1 KLASIFIKACE PROVOZNÍCH PARAMETRŮ DLE ČSN IEC 870-4

Provozní parametry jsou definovány normou ČSN IEC 870-4 *Systémy a zařízení pro dálkové ovládání – Část 4: Požadavky na vlastnosti*. Tato část se zabývá takovými charakteristikami, které ovlivňují vlastnosti systémů dálkového ovládání a uvádí vztah charakteristik a aplikačních funkcí a funkcí zpracování dat. Tato část stanovuje soubor pravidel, která lze použít ke stanovení a upřesnění požadavků na vlastnosti systémů dálkového ovládání.

Klasifikace provozních parametrů je definována v Kapitole 3: Klasifikace provozních parametrů, která zahrnuje ty vlastnosti, které ovlivňují vlastnosti systémů dálkového ovládání.

- **Bezporuchovost** – je definována jako schopnost zařízení nebo systému plnit jeho určenou funkci v daných podmínkách a v daném časovém intervalu. Vyjadřuje pomocí „střední doby mezi poruchami“ v hodinách (MTBF). Třídy bezporuchovosti R1, R2, R3 s MTBF \geq 2000h, 4000h, 8760h.
- **Pohotovost** – charakterizuje její schopnost plnit požadovanou funkci v kterémkoliv časovém okamžiku. Hodnoty, pokud není stanoveno jinak, vztahují k pohotovosti jednotek celkového systému. Třídy pohotovosti A1, A2, A3 s $A \geq 99\%$, 99,75%, 99,95%.
- **Udržovatelnost** – je schopnost systému nebo zařízení při podmínkách určených pro jeho používání obnovit po zjištění poruchy plně svoji činnost a udržovat ji během normální provozní činnosti. Udržovatelnost je vyjádřena pomocí „střední doby na opravu“ („střední doby do obnovení“) v hodinách (MTTR).
- **Bezpečnost** – lze definovat jako jeho schopnost zabránit, aby se řízený systém dostal do eventuálního nebezpečného nebo nestabilního stavu
- **Nenarušitelnost dat** – je definována jako neměnnost informačního obsahu mezi zdrojem a místem určení informace. V systémech dálkového ovládání se nenarušitelnost dat vztahuje ve směru sledování k pravděpodobnosti nezjištěných chyb, které mají za následek nesprávné informace o okamžitých stavech procesu, nebo ve směru ovládání k pravděpodobnosti nezamýšlených činností.
- **Časové parametry** – jsou takové parametry, které se týkají vlastností systémů dálkového ovládání, včetně přenosu a zpracování informace. Pro oblast dálkového ovládání obsahuje nejdůležitější časový parametr dobu nezbytnou pro přenos informace ze zdroje do místa určení.
- **Celková přesnost** – je definována jako odchylka hodnoty v místě určení od zdrojové hodnoty, vyjádřená v procentech maxima jmenovité hodnoty. Toto se použije pro všechny informace, u nichž mezi zdrojem a místem určení dochází k převodu z analogového zobrazení na digitální či naopak. Zpracování celkové přesnosti vyžaduje uvažovat jednotlivé úseky informační cesty od zdroje do místa určení.

5.1.2 KLASIFIKACE KVALITATIVNÍCH POŽADAVKŮ DLE ŘADY ČSN EN 61850-X-X

Soubor IEC 61850 je poskytován za účelem zajištění interoperability mezi všemi zařízeními systémů automatizace v energetických objektech. Definuje komunikační síť a systémy pro automatizaci v energetických objektech a zvláště komunikační strukturu podřízených systémů.

Jedním z hledisek souboru IEC 61850 je zajištění automatických funkcí v podřízených stanicích pomocí komunikace s (počet jističů viz obrázek):

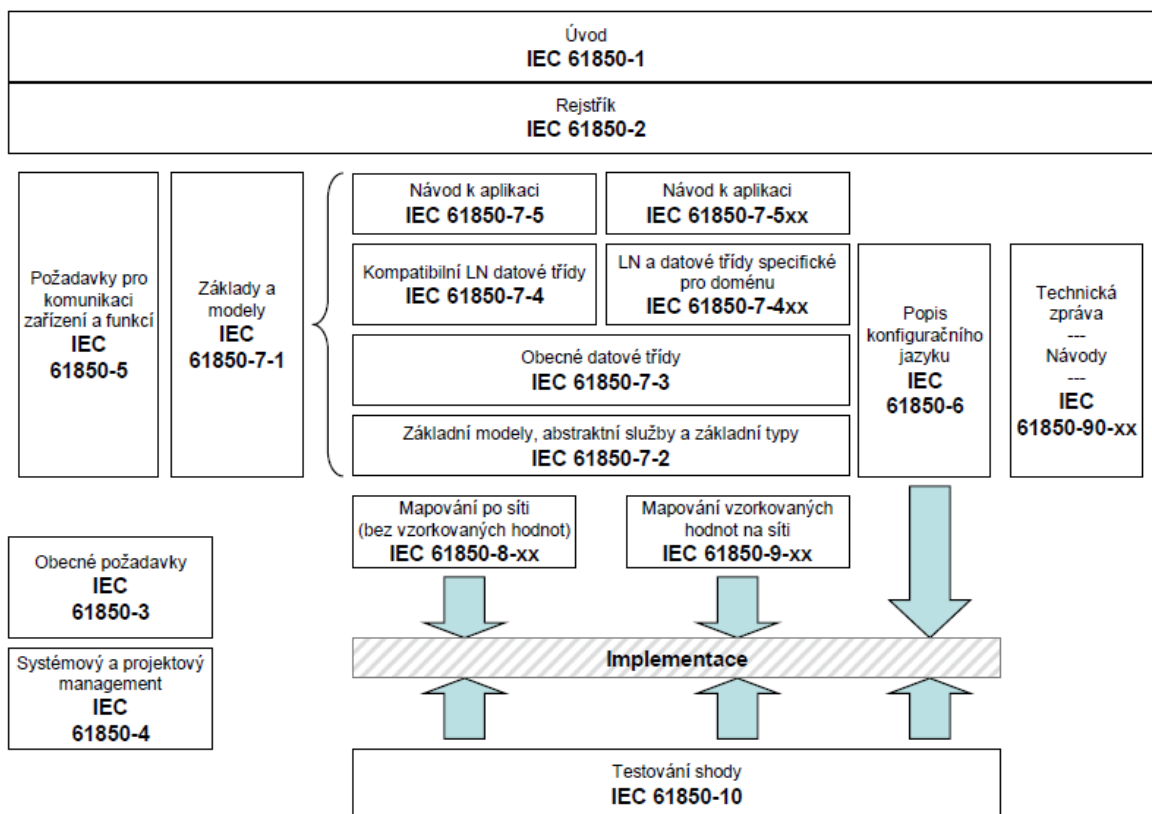
- Výměnou vzorkovaných hodnot u Transformátoru proudu a Transformátoru napětí;
- Rychlou výměnou I/O dat pro chránění a řízení;
- Řídicími signály;
- Vypínacími signály;

- Technickou údržbou a konfigurací;
- Sledováním a kontrolou;
- Komunikací mezi řídicími centry;
- Časovou synchronizací;

Zajištění ostatních funkcí, například měření, sledování podmínek a řízení aktiv (kmenového majetku) se provádí stejně.

Mnoho funkcí je realizováno v inteligentních elektronických zařízeních (IED). V jednom IED může být realizováno několik funkcí, nebo může být jedna funkce realizována v jednom IED a další funkce může být obsažena v jiném IED. IED (tj. funkce obsažené v IED) komunikují s funkcemi v jiných IED pomocí mechanismů výměny informací z této normy. Lze tak implementovat funkce rozložené na více než jednom IED.

Pro oblast ochrany distribučních rozvodů elektrické energie (6kV a 22 kV) se doporučuje vycházet z ČSN EN 61850-7-1 ed.2, kapitoly 5 *Přehled koncepce souboru IEC 61850*. Na Obr. 27 – Vztahy mezi modelováním a mapováním částí souboru IEC 61850 jsou přehledně znázorněny informace o souvislostech, vztazích a ustanovení jednotlivých norem souboru. V rámci SŽDC se předpokládá použití diferenciální ochrany a srovnávacích ochrany vedení.



OBR. 27 – VZTAHY MEZI MODELOVÁNÍM A MAPOVÁNÍM ČÁSTÍ SOUBORU IEC 61850

Každá část IEC 61850 definuje specifické hledisko IED v rozvodně.

Pro oblast ochrany distribučních rozvodů elektrické energie (6kV a 22kV) lze vycházet z ČSN EN 61850-61850-5 ed. 2 a ČSN EN 61850-7-1 ed.2, Kapitoly 5: Přehled koncepce souboru IEC 61850.

- 1) Část IEC 61850-5 specifikuje požadavky na komunikace funkcí, provozovaných v automatizačních systémech energetiky a modely přístrojů. Definuje všechny známé funkce a jejich požadavky na komunikace.
- 2) Část IEC 61850-7-1 ed. 2 zavádí metody modelování, zásady komunikace a informační modely, které se používají. Účelem je umožnit – z koncepčního hlediska – pochopit základní pojmy modelování a metody popisu pro:
 - Informační modely stanic pro automatizované systémy energetické společnosti;
 - Funkce zařízení použitého k účelům automatizace energetické společnosti;
 - Komunikační systémy zajišťující funkční spolupráci energetické společnosti.

Systémové požadavky vychází IEC 61850-5, Kapitola 10: popis systému a systémové požadavky a Požadavky na výkon definuje Kapitola 11: Požadavky na výkon.

Čas a synchronizace času – zařízení kompatibilní s IEC 61850 od různých prodejců lze nalézt nejen v rozvodnách, ale také kdekoli jinde v napájecí soustavě. Proto musí všechna tato zařízení používat pro časové značení stejný systém. Musí být možné porovnat sled událostí v systému pro libovolný druh analýzy událostí. Výsledný požadavek je takový, aby čas mezi IED respektive hodiny ve všech těchto IED byly synchronizovány pro souvislou časovou zónu s patřičnou přesností.

Specifické požadavky na model a formát čas jsou uvedeny v Kapitole 11.1.1.2: Čas a synchronizace času pod body a) až j).

Specifické požadavky na synchronizaci času jsou následující:

- 1) Čas pro synchronizaci času musí být snadno odvozen z globálního časového referenčního systému (například GPS).
- 2) Přesnost je vždy vyjádřena rozdílem mezi hlavními hodinami (GPS) a podřízenými hodinami v zařízení (IED)

Přenosový čas – celkový přenosový čas t je specifikován jako celkový čas přenosu zprávy včetně zpracování na obou koncích (vysílač, přijímač). Čas se počítá od okamžiku, kdy vysílač umístí obsah aplikačních dat na vrchol svého přenosového zásobníku (kódování a vyslání) až do okamžiku, kdy přijímač extrahuje data ze svého přenosového zásobníku (příjem a dekódování). Kódovací a dekódovací procesy mohou být zajištěny buď hlavním procesorem, nebo vyhrazeným komunikačním procesorem (mimo rozsah platnosti této normy). Tento požadavek je nezávislý na zásobníku vybraném v ostatních částech tohoto souboru.

Typy zpráv a třídy výkonu – typem přenosu je podle normy zpráva. Zpráva obsahuje typicky jednoduchá binární data, povely nebo jednoduché zprávy například „Vypnutí“, „Sepnutí“, „povel Opětovného sepnutí“, „Start“, „Stop“, „Blokovat“, „Odblokovat“, „Spustit“, „Uvolnit“, „Změna stavu“ a pro některé funkce také „Stav“. Přijímající IED bude obvykle po přijetí tohoto typu zprávy nějakým způsobem okamžitě jednat pomocí příslušné funkce, protože jinak by nebylo zapotřebí rychlé zprávy. Všechny takové rychlé zprávy se týkají funkcí, jako jsou právě ochrany, kde je čas

kritický. Spínání, blokování, uvolnění a podobné signály pro sousedící rozvodnu patří do této třídy. Pro tyto zprávy uvnitř rozvodny nebo jakéhokoli jiného místního systému je typická třída výkonu P1, pro zprávy mezi nimi třída výkonu P2.

- **Vypnutí** – je nejdůležitější zprávou v rozvodně. Proto má tato zpráva náročnější požadavky v porovnání se všemi ostatními rychlými zprávami. Stejný výkon může být vyžadován pro blokovací podmínky, strhávání ochran a logickou hierarchii ochran.

TAB. 8 – TŘÍDY VÝKONU

TŘÍDA VÝKONU	POPIS POŽADAVKŮ	PŘENOSOVÝ ČAS		TYPICKÉ PRO ROZHRANÍ (IF ⁶)
		TŘÍDA	MS	
P1	CELKOVÝ PŘENOSOVÝ ČAS MUSÍ BÝT ŘÁDOVĚ NIŽŠÍ NEŽ ČTVRTINA CYKLU (5 MS PRO 50 HZ, 4 MS PRO 60 HZ).	TT6	≤ 3	3,5,8
P2	CELKOVÝ PŘENOSOVÝ ČAS MUSÍ BÝT ŘÁDOVĚ NIŽŠÍ NEŽ POLOVINA CYKLU (10 MS PRO 50 HZ, 8 MS PRO 60 HZ).	TT5	≤ 10	2,3,11

Třídy přenosových časů pro řízení a ochrany – jsou definovány ČSN EN 61850-5 ed. 2: Kapitola 11.1.3.1. Použití diferenciací ochrany a srovnávacích ochrany vedení. To odpovídá Třídě výkonu P1, přenosovému času třídy TT6 menším nebo rovném 3 ms a přenosovému času třídy TT5 menším nebo rovném 10 ms (viz Tab. 9)

TAB. 9 – TŘÍDY PRO PŘENOSOVÉ ČASY

TŘÍDA PŘENOSOVÉHO ČASU	PŘENOSOVÝ ČAS [MS]	PŘENOS
TT0	>1000	SOUBORY, UDÁLOSTI, OBSAHY LOGŮ
TT1	1000	UDÁLOSTI, ALARMY
TT2	500	POVELY VYDANÉ OPERÁTOREM
TT3	100	POMALÉ AUTOMATICKÉ INTERAKCE
TT4	20	RYCHLÉ AUTOMATICKÉ INTERAKCE
TT5	10	UVOLŇOVÁNÍ, ZMĚNY STAVŮ
TT6	3	VYPÍNÁNÍ, BLOKOVÁNÍ

Třídy synchronizace času – pro zajištění správného sledu událostí napříč různými místy v napájecí soustavě musí být poskytovány časové značky s přesným globálním časem. Z toho důvodu musí

⁶ Dle normy ČSN EN 61850-5 ed. 2: IF2 datová výměna ochrany mezi úrovní pole a vzdálenou ochranou (například ochranou vedení); IF3 datová výměna v rámci úrovně pole; IF5 datová výměna řízení mezi úrovní procesu a pole; IF8 přímá datová výměna mezi poli týkající se zejména rychlých funkcí jako jsou blokovací podmínky; IF11 datová výměna řízení mezi rozvodnami.

být příslušná zařízení s požadovanou přesností synchronizována. Běžná hodnota u událostí je 1 ms.

Podle normy ČSN EN 61850-5 ed. 2 čl. 11.1.3.3: *Třídy synchronizace času* (Tab. 10, Tab. 11) je pro ochrany podle typu je nutné uvažovat hodnoty pro třídy T4 a T5. Různé požadavky mohou být seřazeny v třídách, viz Tab. 10.

TAB. 10 – TŘÍDY SYNCHRONIZACE ČASU PRO SYNCHRONIZACI IED

TŘÍDA SYNCHRONIZACE ČASU	PŘESNOST	PŘESNOST FÁZOVÉHO ÚHLU PRO 50 HZ	PŘESNOST FÁZOVÉHO ÚHLU PRO 60 HZ	PŘESNOST LOKALIZACE PORUCHY B
TL ⁷	> 10 000	>180	>216	NENÍ
T0	10 000	180	216	NENÍ
T1	1 000	18	21,6	7,909
T2	100	1,8	2,2	0,780
T3	25	0,5	0,5	0,195
T4	4	0,1	0,1	0,031
T5	1	0,02	0,02	0,008

Třídy synchronizace času mohou být přiřazeny také k typickým aplikačním funkcím, které potřebují synchronizaci času, viz Tab. 11.

TAB. 11 – POUŽITÍ SYNCHRONIZACE ČASU PRO ČASOVÉ ZNAČKY NEBO VZORKOVÁNÍ

TŘÍDA SYNCHRONIZACE ČASU	PŘESNOST [μS] SYNCHRONIZAČNÍ CHYBA	POUŽITÍ
TL	> 10 000	NÍZKÁ PŘESNOST SYNCHRONIZACE ČASU – RŮZNÉ
T0	10 000	ČASOVÉ ZNAČKOVÁNÍ UDÁLOSTÍ S PŘESNOSTÍ 10 MS
T1	1 000	ČASOVÉ ZNAČKOVÁNÍ UDÁLOSTÍ S PŘESNOSTÍ 1 MS
T2	100	ČASOVÉ ZNAČKY PŘEKROČENÍ NULY A DAT PRO DISTRIBUOVANÝ SYNCHROCHECK. ČASOVÉ ZNAČKY PODPORUJÍCÍ SPÍNÁNÍ V DANÉM BODĚ VLNY
T3	25	RŮZNÉ
T4	4	ČASOVÉ ZNAČKOVÁNÍ VZORKŮ RESPEKTIVE SYNCHRONIZOVANÉ VZORKOVÁNÍ
T5	1	VYSOCE PŘESNÉ ČASOVÉ ZNAČKOVÁNÍ VZORKŮ RESPEKTIVE VYSOKÉ SYNCHRONIZOVANÉ VZORKOVÁNÍ

Požadované parametry ze skupiny norem ČSN EN 61850 musí být prokázány zkouškou shody, ale i dlouhodobě garantovány správcem sítě.

⁷ TL znamená pro synchronizaci času „nízká“.

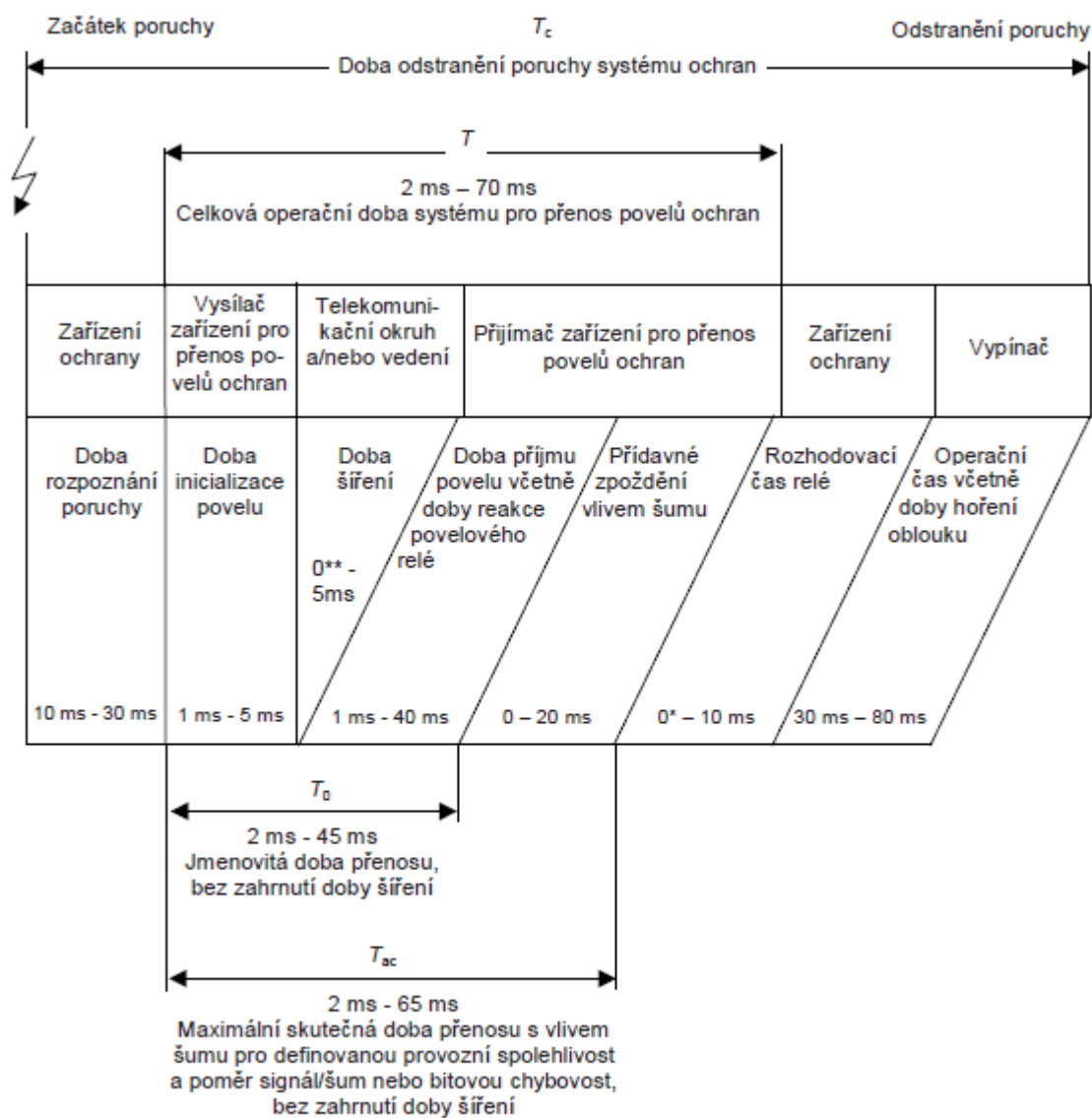
5.1.3 POŽADAVKY NA SYSTÉMY PRO PŘENOS POVELŮ OCHRAN DLE ČSN EN 60834-1

Oblast přenosů povelů ochrany jsou požadavky definovány normou ČSN EN 60834-1 *Zařízení pro přenos povelů ochrany elektrizační soustavy – Provoz a zkoušení – Část 1: Povelové systémy v Kapitole 3 - Požadavky na systémy pro přenos povelů ochrany*. Požadavky se týkají rozhraní mezi zařízením ochrany a zařízením pro přenos povelů ochrany a rozhraní mezi zařízením pro přenos povelů ochrany a telekomunikačním systémem. V případě SŽDC se především týká povelů vazeb napáječů soustavy 3 kV DC. Zde je potřeba zohlednit všechny normou uvedené požadavky zejména pak:

- **Celkový operační čas systémů pro přenos povelů ochrany (včetně telekomunikačního okruhu)** – Celkový operační čas T je čas, který uběhl mezi okamžikem změny stavu na povelovém vstupu a okamžikem odpovídající změny stavu na povelovém výstupu, včetně doby šíření a přídavného zpoždění vlivem šumu. Celkový operační čas systému pro přenos povelů ochrany ovlivňuje dobu odstranění poruchy.
- **Doba přenosu (bez telekomunikačního okruhu)** – doba přenosu v systému pro přenos povelů ochrany je doba, která uběhla mezi okamžikem změny stavu na povelovém vstupu a okamžikem odpovídající změny stavu na povelovém výstupu bez doby šíření.

Norma stanovuje i další požadavky na časovou synchronizaci, jitter, dostupnost, chybovost, nenarušitelnost apod.

Požadavky na systémy pro přenos povelů ochrany jsou definovány v *Kapitole 3: Požadavky na systémy pro přenos povelů ochrany*. Požadavky se týkají rozhraní mezi zařízením ochrany a zařízením pro přenos povelů ochrany a rozhraní mezi zařízením pro přenos povelů ochrany a telekomunikačním systémem.



* Může se použít dálkové vypínání (zařízení pro přímé dálkové vypínání)

** Používá se při spojení zařízení v malé smyčce (back to back)

OBR. 28 – TYPICKÉ PROVOZNÍ DOBY PRO SYSTÉMY OCHRAN VE SPOJENÍ SE ZAŘÍZENÍM PRO PŘENOS Povelů OCHRAN

Z uvedeného Obr. 28 je patrné, že doba přenosu musí být menší nebo rovna 5ms. Požadavek na přenosy diferenciálních a srovnávacích ochran (ČSN EN 61850-5 ed. 2, Třídy pro přenosové časy TT6 a TT5) a přenosy povelů ochran je 5ms podle ČSE EN 60834-1.

Použití vyhrazených optických vláken je tedy možné pouze v případě, že požadovaných časových parametrů (doba zpoždění přenosu) není možné dosáhnout technologickou datovou sítí. Proto se doporučuje tyto časy při realizaci vždy prověřit a následně provádět tato měření v pravidelných intervalech. V případě, že tyto parametry doby přenosu a časové synchronizaci nebude možné splnit, se doporučuje přenos po samostatných optických kabelech v režimu point-to-point (viz 5.2.2).

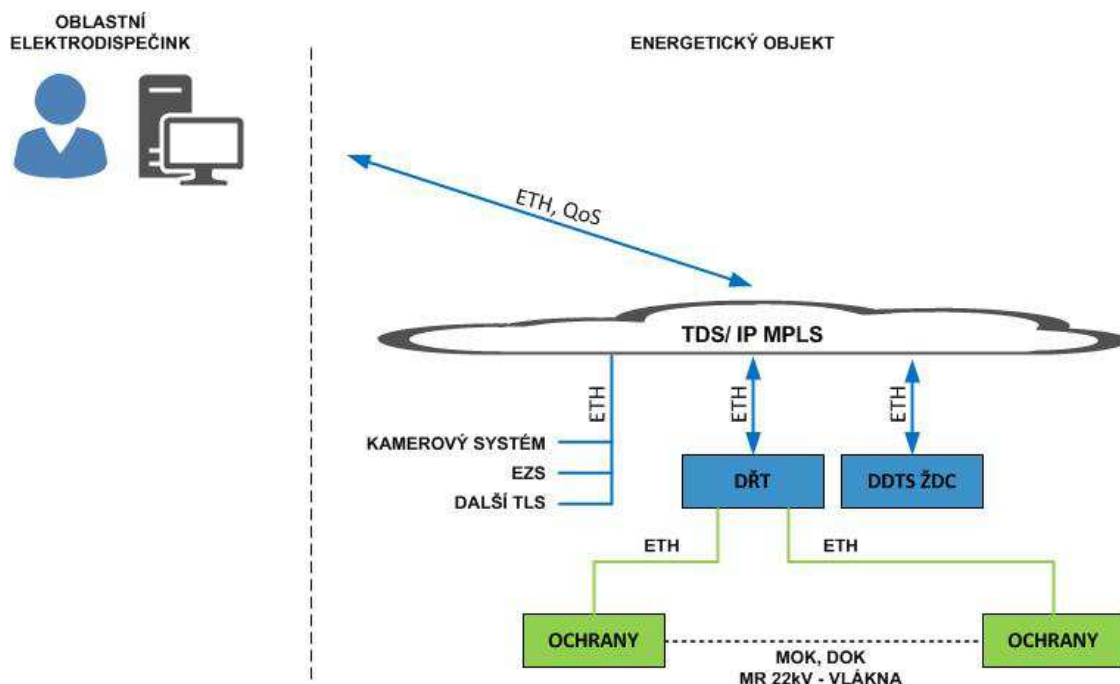
Na základě výše uvedeného se doporučuje mezi energetickými objekty do nadřazených systémů a pro dálkové ovládání silových prvků následující komunikace.

5.2 Komunikace dispečerských systémů v přenosové síti SŽDC

5.2.1 KOMUNIKACE NA ÚROVNI ENERGETICKÝCH OBJEKTŮ

Pro přenos dat a informací se předpokládá se v rámci jiných investičních akcí pokračování ve výstavbě a rozšiřování přenosového systému DWDM a IP/MPLS v síti SŽDC v souladu s kapitolou 3, která navrhuje přenos veškerého datového provozu (VoIP, Kamery, Intranet atd.) vyjma zabezpečovacího zařízení. Stávající přenosový systém SDH (PDH) se navrhuje postupně v následujících letech utlumovat a nahrazovat právě zařízením IP /MPLS.

Pro komunikaci z energetických objektů (TM, SpS, TS atd.) a zejména systémů DDTS ŽDC, DŘT, dálkového odečtu elektroměrů ve směru do nadřazeného řídicího systému v ED příslušného Oblastního ředitelství (dále jen OŘ) se i nadále bude využívat stávající technologická datová síť (TDS) v technologii IP/MPLS v nově realizovaných a rekonstruovaných energetických objektech a železničních stanicích. U těchto nově realizovaných a rekonstruovaných objektů se navrhuje definovat a zajistit dostatečnou propustnost (viz kapitoly výše) a také určenou náhradní variantu přenosu v případě výpadku některého z aktivních prvků přenosové sítě. Navrhuje se primárně využívat dvě služby, a to spojení L2 bod – bod a L3 VPN.



OBR. 29 – TOPOLOGIE KOMUNIKACE DŘT, DDTS ŽDC, OCHRAN A OSTATNÍCH APLIKACÍ

Navrhuje pro potřeby systémů DDTS ŽDC, DŘT a dálkového odečtu elektroměrů realizovat datové přenosy informací o stavu zařízení a prvků v energetických objektech pomocí přenosového

systému IP/MPLS a CE směrovače s potřebným počtem portů (počet portů vzejde vždy z konkrétního řešení a požadovaných přenosů). V přenosovém systému IP/MPLS budou pro zmíněné systémy vytvořeny samostatné VRF z koncového bodu (z energetického objektu) až do příslušného ED OŘ. V žádném přenosovém bodu (lokalitě) v celé přenosové cestě nesmí dojít ke sloučení VRF s jinými provozy (VoIP, Intranet atd.), tak aby byly dodrženy předepsané časové odezvy.

U nově realizovaných nebo rekonstruovaných energetických objektů se jednoznačně navrhuje výstavba pouze zařízení IP/MPLS. V rámci výstavby je nutné důsledně dodržovat (a to zejména pro „kritické aplikace“) oddělení provozu a zajištění požadované šířky pásma (QoS).

U stávajících energetických objektů zůstane zachován stávající stav, který se bude postupně nahrazován výše popsaným řešením. V tomto případě výměnou přenosového zařízení (SDH, PDH), vyčleněním provozu do samostatné VRF a rekonfigurací přenosové sítě.

5.2.1.1 Zabezpečený způsob výměny mezi DŘT, DDTS ŽDC a jinými systémy

Pro zvýšení síťové bezpečnosti na úrovni propojení segmentů jednotlivých OŘ a mezi energetickými objekty se doporučuje zabezpečení veškerých prostupů mezi jednotlivými VLAN-TDS (DDTS ŽDC, DŘT, kamery, EZS a další) a Intranetem pomocí zařízení Firewall. Navrhuje se pro každý správní celek (OŘ) nasadit dva New Generation Firewally s funkcionalitami AVC, IPS, AMP. Tyto firewally budou mít za úkol kontrolovat a sledovat provoz jak v rámci celku, tak i mezi nimi a provádět centrálně řízené politiky v souladu s vnitřními předpisy (Navrženo jako samostatná investiční stavba v části D. *Soubor možných investičních akcí na doplnění topologie sdělovací sítě využívané SŽDC*).

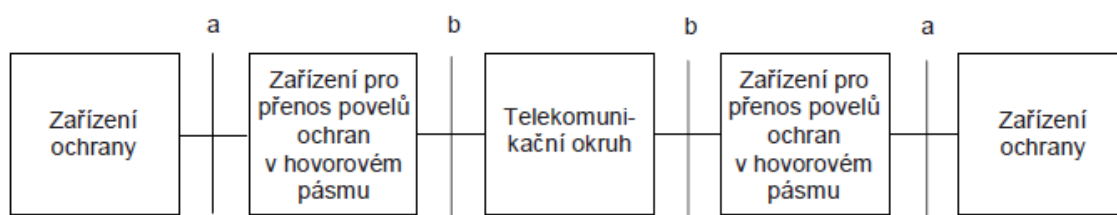
Uvedené řešení přinese výhody jak výhody segmentace společných sítí (technologická síť a intranet) na aplikační úrovni, tak i zvýšenou kontrolu přístupů a prostupů mezi sítěmi.

5.2.2 KOMUNIKACE NA ÚROVNI OCHRAN DISTRIBUČNÍCH ROZVODŮ

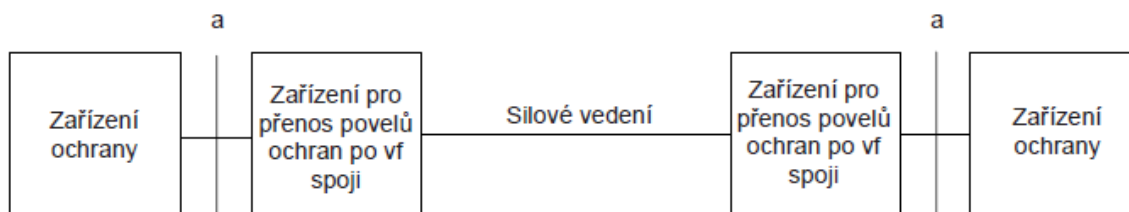
Pro komunikaci na úrovni ochran distribučních rozvodů elektrické energie se doporučuje na základě kapitoly 5.1 propojení IED point-to-point přímo bez dalších aktivních prvků po optickém kabelu v provedení Single Mode a to pouze v případě, že nebude možné dosáhnout požadovaných časových parametrů (doba zpoždění přenosu) technologickou datovou sítí. Na obrázcích Obr. 30 - Obr. 33 jsou uvedeny možné způsoby komunikace dle normy ČSN EN 60834-1.

V případě použití vyhrazených vláken může tato komunikace probíhat po diagnostickém optickém kabelu (DOK) a místních optických kabelech (MOK).

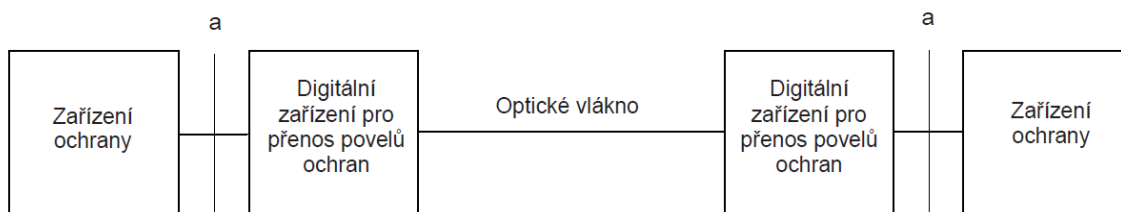
Komunikace mezi ochranami distribučních rozvodů elektrické energie musí být řazena do úrovně LTDS.



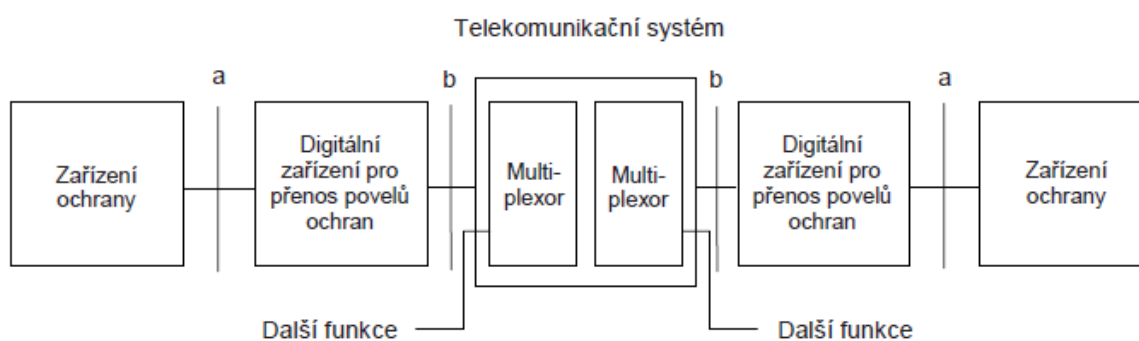
OBR. 30 – KONFIGURACE ZAŘÍZENÍ PRO PŘENOS POVELŮ OCHRAN V HOVOROVÉM PÁSMU



OBR. 31 – KONFIGURACE ZAŘÍZENÍ PRO PŘENOS POVELŮ OCHRAN PO VF SPOJI PO SILOVÝCH VEDENÍCH



OBR. 32 – PŘÍMO PROPOJENÁ DIGITÁLNÍ ZAŘÍZENÍ PRO PŘENOS POVELŮ OCHRAN



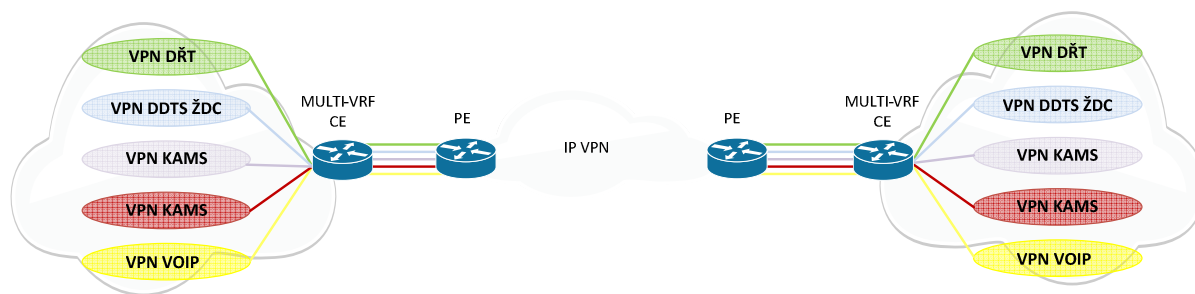
OBR. 33 – DIGITÁLNÍ ZAŘÍZENÍ PRO PŘENOS POVELŮ OCHRAN PŘES KOMUNIKAČNÍ SYSTÉM

K výše uvedenému je nutné uvést, že je k dispozici stanovisko SŽDC, O14 č.j. 19493/2017 které dané řešení v určitých případech umožňuje. Nutno zdůraznit, že vyhrazená vlákna nebudou sloužit pro datové přenosy systémů DŘT, DDTS ŽDC, ale pouze pro systémy chránění a to jak v rámci stanic pro například diferenciální ochrany kabelů, kde se jedná o propojení jednotlivých TS a dané komunikace se dají zahrnout dle stanoviska jako aplikace s kritickou časovou odezvou.

Alternativou k DOK, MOK bude možné využít kabelu magistralního rozvodu 22kV, který bude umožňovat využití optických vláken, kterou jsou jeho součástí (vychází ze v současné době zpracovávané studie „Metodika zásad projektování a provozu lokální distribuční sítě SŽDC 22kV“) a který bude možné použít pouze pro komunikaci mezi ochranami rozvodu 22kV. Dále bude toto řešení možné využít i pro ochranné funkce vazby napáječů.

5.2.3 KOMUNIKACE OSTATNÍCH TECHNOLOGICKÝCH CELKŮ

V tomto případě se jedná zejména o komunikaci kamerových systémů, elektronické zabezpečovací signalizace (EZS), elektrické požární signalizaci (EPS), případně dalších aplikací. Vzhledem k tomu, že se nejedná o aplikace s kritickou časovou odezvou, navrhuje komunikace výhradně v TDS v prostředí IP/MPLS s opětovným vyčleněním do samostatných VRF (např. VRF_Kamery_Energetika, VRF_EZS_EPS_Energetika).



OBR. 34 – VYČLENĚNÍ PROVOZŮ DO SAMOSTATNÝCH VRF

6 HLASOVÁ A TELEFONNÍ SÍŤ

Hlasové a multimediální komunikační služby (zkráceně služby UCC) jsou uživatelům dostupné obvykle podle jejich pracovního a funkčního zařazení. V prostředí podporované mobility to znamená, že služby jsou dostupné primárně plošně a uživatelé mohou služby využívat na svých přidělených zařízeních (dotykových terminálech či telefonech) nebo na společných sdílených terminálech (videokonferenční místnosti) v rozsahu a s oprávněními podle jejich identity, resp. souvisejícího profilu (např. funkčního zařazení) a technických možností konkrétního terminálu.

6.1 Druhy služeb a druhy zařízení

K výše uvedeným selektivně autorizovaným službám patří:

- Hlasové služby - telefonní hovory a služby speciální telefonie
- Video a videokonference – různé režimy, počty účastníků, apod.
- Faxová a modemová spojení
- Voicemail
- IM & presence
- Adresářové služby, plánování schůzek
- Nástroje pro sdílení dokumentů, aplikací a pracovní plochy
- Atd.

Terminály, pro které by měl být přístupový mechanismus ke službám UCC podporován jsou minimálně:

- Dispečerská a spojovatelská pracoviště na bázi VoIP
- IP telefony
- Analogové telefony
- MB telefony
- Tablety, Smartphony
- Mobilní telefony
- Videokonferenční terminály
- Faxmodemové přístroje

6.2 Architekturní požadavky na služby UCC

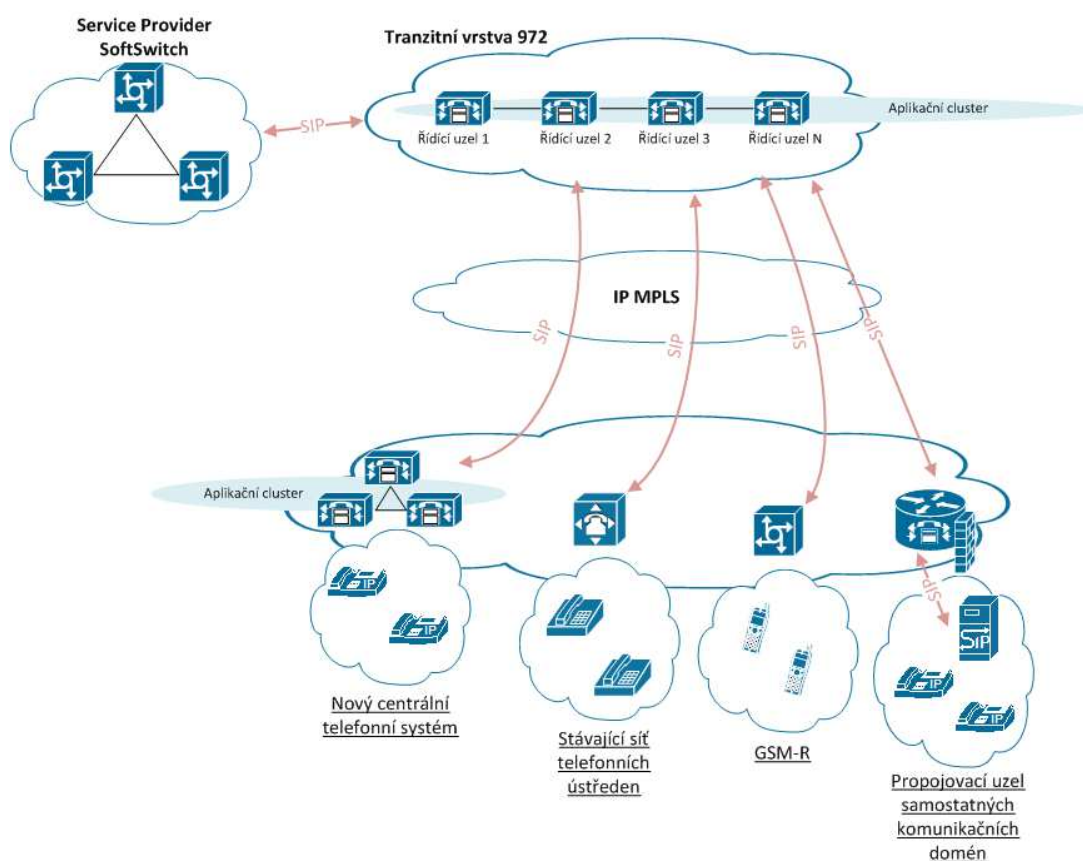
Infrastruktury poskytující služby UCC ve větším rozsahu (počet uživatelů, sortiment služeb, terminálů, oprávnění, apod.) mohou vyžadovat hierarchickou architekturu. Pro zajištění její spolehlivé funkce, rozšiřitelnosti a spravovatelnosti je třeba požadované řešení omezit dalšími architekturními požadavky, jako je:

- Členění, oddělující minimálně tranzitní vrstvu (propojení jednotlivých komunikačních domén s možností implementace kontrolních mechanismů směrování hovorů) a přístupovou vrstvu (řízení hovorů na úrovni jedné komunikační domény, implementace uživatelských služeb a tříd oprávnění);

- Požadavky na hraniční prvky (funkční bloky zajišťující propojení komunikačních domén s rozdílným stupněm bezpečnostního zařazení), hlasové brány (propojení rozdílných komunikačních prostředků využívající technologie TDM a IP) a modifikace media-dat (RTP transcoding a transrating pro hlas i video);
- Požadavky na strukturu číslovacích plánů a IP adresního plánu;
- Požadavky na překlad číslovacích plánů (ITU-T E.164) a překlad IP adresního plánu (IP NAT);
- Zajištění determinismu v přidělování prostředků infrastruktury (správu přenosového pásma a kapacity) obecným mechanismem Call Admission Control.

6.3 Navrhovaná architektura UCC

UCC cluster technologické hlasové sítě je tvořen celkem sedmi instancemi IP telefonní ústředny, kdy publisher je umístěn v Praze a šest subscriberů je geograficky rozděleno v rámci ČR (Praha, Brno, Přerov, Ústí nad Labem, Plzeň, České Budějovice). Toto rozdělení je optimální i pro stav do budoucna, je však doporučeno provést zastřešení clusteru technologické hlasové sítě a i dalších hlasových sítí nadstavbovou vrstvou.



OBR. 35 – NAVRHOVANÁ ARCHITEKTURA UCC

Základní myšlenkou navrhované architektury UCC je umístit nad stávající i nově budované komunikační entity společnou nadstavbovou tranzitní vrstvu, která by umožnila jednotnou správu UCC v celém drážním prostředí, zejména pak:

- jednotnou správu číslovacího plánu
- snadno realizovatelnou přenositelnost čísel
- centrální tarifkaci
- další nově požadované služby

Tato tranzitní vrstva, tvořená nadřazeným aplikačním clusterem, má za úkol kromě výše uvedených funkcionalit týkajících se správy sítě zajistit i vlastní propojení z celé drážní sítě směrem k operátorovi.

Připojení tranzitní vrstvy k podřazeným, doposud samostatně řízeným částem UCC, je předpokládáno přes SIP trunky přenášené skrze MPLS síť.

6.4 Správa uživatelů, uživatelských služeb a komunikačních zařízení UCC

Množství koncových uživatelů, rozmanitost používaných zařízení a (multimediálních) služeb obvykle vyžaduje podporu automatizace správy a modifikace konfigurací. Pro design by měl být požadován automatizovaný service provisioning jednotlivých uživatelů na základě tříd:

- přidělených zařízení (jedno nebo více), jejich typů;
- seznamu autorizovaných služeb UCC vázaných na uživatelskou roli / profil;
- vazba služeb UCC na komunikační infrastrukturu LAN/WAN.

Součástí nástrojů provisioningu by mělo být schvalovací workflow na základě hierarchie pracovního, funkčního zařazení.

6.5 Údržba systému – upgrady

Všechny softwarové i hardwarové součásti systému je nutné udržovat pravidelně aktualizované. Důvodem je kromě zcela samozřejmého udržování aktuálních vlastností a podpory aktuálních protokolových standardů zejména důraz na bezpečnost řešení, jíž je pravidelná aktualizace jak HW tak i SW nedílnou součástí. Dalším faktorem vstupujícím do hry a přinášejícím nutnost pravidelné aktualizace je i kompatibilita s ostatními zařízeními a systémy, leckdy svázaná právě s již zmíněnou podporou protokolových standardů.

6.5.1 ÚSTŘEDNY / CLUSTER

Co se týče telefonní ústředny, je plánováno ponechat stejnou platformu, tedy CUCM. V souladu s výše uvedeným doporučením je optimální SW vybavení upgradovat, nejlépe po dohodě s dodavatelem či výrobcem, aby byl nalezen vyvážený kompromis mezi bezpečností a funkčností systému a častostí nasazování nových verzí.

6.5.2 TERMINÁLY

Dotykovým terminálům je věnována v rámci této studie zvláštní kapitola, zde se omezíme pouze na konstatování, že uprady HW i SW dotykových terminálů jsou nedílnou součástí udržování systému aktuálního jako celku.

6.5.3 TELEFONY

I pro IP telefony platí výše uvedené. Výrobci dnes již nabízejí nové řady telefonů, které je vhodné použít. Jeden z velice důležitých směrů, který je třeba sledovat, je přechod protokolových standardů telefonů z proprietárních protokolů (např. SCCP) na univerzální standardy, zejména na protokol SIP. Tomu by měl být přizpůsoben výběr nových telefonů a licencování vůči ústředně.

6.5.4 HLASOVÉ BRÁNY

I technologie směrovačů podporujících hlas, na nichž jsou postaveny hlasové brány, podléhá inovacím. Od doby prvního nasazení došlo již k několika generačním obměnám. Nové typy hlasových směrovačů podporují technologie containerů, dokáží oddělit fungování aplikací uvnitř směrovače tak, aby se navzájem neovlivňovaly. Výkonnější typy směrovačů mají oddělenou datovou a ovládací část (data-plane a control-plane) a dávají tím možnost stále pracovat konfiguračně se směrovačem, který je pod plnou datovou zátěží. Samozřejmým přínosem při uprady směrovačů na nové typy je i zvýšení výkonu a propustnosti.

6.6 Telefonní síť

6.6.1 SLUŽEBNÍ TELEFONNÍ SÍŤ SŽDC

Služební telefonní síť SŽDC slouží primárně k hlasové komunikaci účastníků. Jedná se o neveřejnou, korporátní (dříve podnikovou) telekomunikační síť, jejímiž účastníky jsou především zaměstnanci SŽDC, dále pak organizace spolupracující se SŽDC, případně mimodrážní účastníci, kteří využívají tuto síť na základě pronájmu telefonních poboček.

Služební telefonní síť je propojena s veřejnou telefonní sítí a dále s korporátními telefonními sítěmi sousedních železničních správ. Není určena pro řízení dopravy, její účel spočívá v zajištění komunikace mezi jednotlivými účastníky, komunikace bez přímé vazby na řízení dopravy. Rozsah přístupu jednotlivých účastníků je daný přiděleným oprávněním. Pro řízení dopravy je určena dopravní síť, která tvoří víceméně samostatnou strukturu, ale v určitých bodech je HW propojena se sítí služební.

Dříve se jednalo o hlavní komunikační prostředek v drážní infrastruktuře, v současné době při zavádění jiných komunikačních možností je její význam nižší, především v hlavních uzlech a oblastech dráhy. Nicméně v některých, zvláště méně významných regionálních tratích, se stále jedná o hlavní drážní komunikační prostředek.

Možnosti rozšiřování a modernizace telekomunikační sítě zcela závisí na fyzické a přenosové vrstvě, tj. na existenci kabelové sítě, především optické a na existenci kapacitně odpovídajících

přenosových prostředků. V současné době je absence kabelových sítí hlavní překážkou rozvoje korporátní telekomunikační sítě SŽDC.

6.6.2 STÁVAJÍCÍ STRUKTURA TELEFONNÍ SÍTĚ

Stávající hierarchická struktura telefonní sítě vychází z původního konceptu tří, resp. čtyř úrovní sítě, který dominoval do konce minulého století. Nejvyšší úroveň tvořily hlavní resp. hlavní a uzlové ústředny, následovala úroveň koncových ústředen, doplněná podružnými ústřednami. Jedná se o koncept typický pro analogovou síť.

Nástupem digitální technologie se začala budovat telefonní síť dvouúrovňová, horní – tranzitní úroveň představují dříve hlavní a uzlové ústředny, dolní úroveň představují dříve koncové a podružné ústředny. Dolní úroveň je zapojena jako kaskáda účastnických uzlových bodů na traťovém úseku, jejíž koncové body se připojují na tranzitní uzly sítě.

V současné době je telefonní síť tvořena kombinací hierarchického uspořádání jak původního – analogového uspořádání, tak novějšího konceptu dvouúrovňové digitální sítě. Starší způsob hierarchického uspořádání sítě je používán hlavně v severní části a v severozápadní části dráhy. Jedná se o oblasti, kde je absence kvalitního kabelového propojení a přenosových systémů. Telefonní ústředny jsou v těchto oblastech propojeny analogovými nf okruhy po starších metalických kabelech s mnohdy špatnou kvalitou.

Tranzitní úroveň sítě je v současné době již plně digitalizovaná systémem MD110 a vybrané uzly této tranzitní úrovně jsou doplněné bloky MX-One, které umožňují přes tzv. call managery telefonii v ethernetovém prostředí v IP síti. Pobočky zapojené do tohoto prostředí se využívají především pro dopravní telefonní síť.

Číslovací plán sítě je založený na šestimístním číslování poboček vlastní sítě, toto šestimístné číslo je doplněné korporátním prefixem 972, který určuje přechod z veřejné telefonní infrastruktury do sítě SŽDC. Komplexní číslo pobočky je devítimístné 972 zy xxxx, kde zy vyznačuje tranzitní uzel a xxxx číslo pobočky tranzitního uzlu. V obvodu tranzitního uzlu je možné volat zkrácenou volbou yxxxx, mezi tranzitními uzly je volání možné pouze celým devítimístným znakem.

Volání na IP pobočky lze uskutečnit prostřednictvím tranzitního uzlu kde je pobočka zaregistrovaná pod call managerem, který zajišťuje přepočítání volaného čísla na IP adresu a převod volání do IP sítě. Na této úrovni dochází k HW propojení služební a dopravní sítě.

Stávající stav telefonní sítě v jednotlivých úrovních je uveden v přílohách 2, 3 a 4.

6.6.3 IP TELEFONIE

Rozvoj klasických telefonních sítí obecně zaostal a to i celosvětově za rozvojem datových sítí, které do sebe v současné době integrují hlasové služby. Stávající telefonní sítě včetně služební telefonní sítě SŽDC jsou založeny hlavně na TDM kanálech (kanál s časovým multiplexem, který vytváří hovorové spojení v jednotlivých slotech časového rámce). Nejedná se o přenos hovoru v reálném čase jako u analogových okruhů, ale zpoždění je nepatrné, konstantní a probíhá na

stejném, předem vytvořeném okruhu. (U vyšších přenosových rychlostí a při vysokém hovorovém zatížení se u veřejných systémů využívá i sdílení kanálů resp. přepínání kanálů).

Sítě s IP protokolem jsou provozované v ethernetovém prostředí, ve kterém se šíření datové informace šíří prostřednictvím paketů. Princip přenosu se neděje v reálném čase a dochází ke zpoždění, které je vyvolané vlastním zpracováním a přenosem paketu. Není vytvořena pevná přenosová cesta, pakety se od zdroje k cíli dostávají v různém čase podle toho, jakou cestou byl zajištěn jejich přenos. Zpoždění paketů může být různé a může kolísat. Pro zajištění kvalitního přenosu, který je možné využít pro přenos hovorových signálů, je nutný základní předpoklad tím je datová síť s rychlostí přenosu okolo 1Gb/s.

VoIP (Voice over IP) telefonie umožňuje přenos hovorových signálů tak, že digitalizovaný signál rozdělí do menších paketů, doplní je adresou a dopraví do cíle, kde dojde k jeho opětovnému sestavení. Jedná se o stejný princip, který využívá ostatní datový přenos na internetu. Hlavní rozdíl oproti ostatním datovým přenosům spočívá v jeho prioritě. Jedná se o data, u kterých nemůže dojít k většímu zpoždění tak, aby byla zachována srozumitelnost hovoru, pro dobrou kvalitu nesmí být zpoždění paketu větší jak 150ms. K dalšímu zpoždění dochází při vyrovnávání rozdílných dob doručování jednotlivých paketů (jitter) přes tzv. buffer.

V současné době je na trhu mnoho technologických zařízení pro provozování telefonie na bázi IP. Jednotlivé články spojovacího, přenosového a účastnického řetězce musí umožňovat poskytování služeb ve vysoké kvalitě, tak aby výsledek spojení odpovídal požadavkům uživatele. Jedním z parametrů pro výběr zařízení je tzv. QoS (Quality of Service), jehož koncept zahrnuje velkou škálu parametrů a veličin, které je nutné splnit pro dosažení kvalitní služby. Jedním z předpokladů zavedení telefonní sítě na bázi VoIP u SŽDC je vytvoření nástrojů QoS pro potřeby SŽDC.

Architekturu sítě na bázi VoIP je možné řešit dvojím způsobem:

- Centralizovaně – řízení hovorů, dohled nad sítí a její řízení je zřízeno z jednoho místa. Jedná se o obdobu architektury používané u klasických telefonních sítí.
- Distribuovaně – „intelligence“ sítě je rozprostřena blíže koncovým bodům nebo přímo do koncových bodů sítě. Řídící uzly jsou distribuované, koncové body jsou tvořené zařízením, které je schopné iniciovat, sestavit a ukončit hovor tj. VoIP bránami, IP telefony, media servery PC s potřebným SW apod. Tento systém je používán v datových sítích.

Základním prvkem telefonní sítě je tzv. Call Manager - správce volání. Call Manager spravuje síťovou konfiguraci a směřuje hovory v rámci telefonní sítě. Obsahuje adresářovou strukturu a umožňuje tak zadávat a ukládat informace o uživateli na jednom místě. Call Manager může být aplikovaný jako software, běžící na serveru nebo jako specializované hardwarové zařízení. Situování Call Manageru je možné volit následujícím způsobem:

- Centralizovaně – Call Manager je umístěn pouze v jednom centru – vhodný způsob pro skupiny situované v jedné, prostorově omezené lokalitě;
- Distribuovaně – každá lokalita je vybavena vlastním Call Managerem;
- Kombinovaně – Call Manager je distribuovaný do více míst – cca 5-10, ostatní zbylé lokality nemají vlastního Call Managera – jedná se o systém vhodný pro SŽDC.

Ve VoIP telefonii se využívají dva druhy protokolů - komunikační a signalizační protokol.

Komunikační protokol slouží k vlastnímu přenosu hlasu – používané jsou protokoly RTP (Real-time Transport Protocol) protokol pro přenos dat a RTCP (RTP Control Protocol), který je určen pro řízení toku dat.

Signalizační protokol slouží k navázání spojení, jeho řízení a ukončení. Těchto protokolů je více druhů, pro potřeby SŽDC je vhodný protokol SIP (Session Initiation Protocol) určený pro distribuovanou architekturu sítě. SIP je signalizační protokol pro sestavení, dohled a rozpad spojení mezi dvěma nebo více účastníky komunikace.

Koncovým zařízení SIP sítě jsou tzv. User Agents (UA), v podstatě účastníci sítě nebo přenašeče (analogie s klasickou sítí), což mohou být jednak HW zařízení – IP telefony, koncové brány do jiného prostředí anebo aplikační SW na PC, který je vybavený pro zprostředkování hovoru (sluchátky, mikrofon apod.).

Obdobou klasického spojovacího pole jsou ve VoIP síti servery, jejichž úkolem je zprostředkování kontaktu mezi dvěma koncovými zařízeními (mezi dvěma UA).

Identifikace účastníků v síti VoIP probíhá odlišně od klasické telefonní sítě. Telefonní číslo je převedeno na IP adresu, pro jejíž identifikaci se využívá identifikační protokol URL (Universal Resource Locator), pomocí kterého lze identifikovat účastníka kromě telefonního čísla i např. podle jeho e-mailové adresy.

IP telefony jsou koncová účastnická zařízení, která zajišťují hovorová spojení, stejně jako klasické telefony. Dále mohou mít podle vybavení i další funkce, umožňující provoz textově a obrazově orientovaných aplikací. IP telefon může být také prezentovaný jako aplikační software na klientských PC.

Hlasové brány – Voice Gateway (VoGW) umožňují spojení mezi klasickou telefonní sítí a paketovou sítí. Tyto brány dovolují spojení mezi stávajícím prostředím a novou VoIP sítí. Jedná se o velmi důležitý prvek, který umožní snadnou implementaci nové technologie do stávajícího prostředí. Pro migraci nové technologie do stávající telefonní sítě SŽDC představují vhodné hlasové brány důležitou součást sítě.

6.6.4 NÁVRH NOVÉ STRUKTURY

Nová architektura IP služební telefonní sítě je založena na dvouúrovňové síti:

- Tranzitní úroveň;
- Koncová úroveň.

Tranzitní úroveň budou tvořeny tranzitními uzly, umístěnými do bodů sítě, ve kterých se stýká více tratí. Tranzitní uzly budou zajišťovat spojení do koncových uzlů, zapojených kaskádně na traťovém úseku. Část tranzitních uzlů se vybaví Call Managerem. V návrhu sítě se vycházelo ze stávajícího stavu, ze stávajících tranzitních uzlů, kde jsou již některé uzly doplněné IP blokem MX-One. Celkem je v návrhu počítáno s následujícími tranzitními uzly s Call Managerem – Praha, Ústí nad Labem, Plzeň, České Budějovice, Hradec Králové, Brno, Přerov, Ostrava, tj. celkem 8 uzlů. Další tranzitní uzly by byly situované následovně – Karlovy Vary, Chomutov, Cheb, Strakonice,

Veselí nad Lužnicí, Benešov, Jihlava, Havlíčkův Brod, Liberec, Kolín, Pardubice, Česká Třebová, Břeclav, Olomouc, Bruntál, Opava, Valašské Meziříčí – celkem 17 uzlů. Návrh tranzitních uzlů vycházel z údajů o stávajícím stavu, jedná se o lokality bývalých uzlových ústředen, lokality, které zajišťují spojení do nižší úrovně sítě, a ve kterých bude nutné řešit přechody mezi novou a stávající sítí do doby plného přechodu na IP síť. Návrh zapojení tranzitní úrovně je znázorněna na příloze č.5.

Koncová úroveň bude zajišťovat spojení na konkrétních traťových úsecích. Jedná se o obdobu stávající druhé úrovně sítě, která má spojovací uzly v každé ŽST a je propojena kaskádně. V IP síti by se jednalo opět o kaskádní propojení těchto uzlů, tyto uzly by však z ekonomických důvodů nebyly situovány do všech ŽST. na traťovém úseku, ale jen ve větších lokalitách. Účastnická úroveň by se dále distribuovala pomocí koncových zařízení (User Agent – UA), tj. IP telefonů, účastnických bran, SW apod. Návrh zapojení koncové úrovně je znázorněna na příloze č.6.

IP uzly tranzitní úrovně musí být podle potřeby vybaveny bránami pro připojení stávajících systémů, které budou po nějakou dobu ještě v provozu a jejich plná náhrada nebude v daném okamžiku možná (chybějící kabelizace, přenosové prostředky, ekonomické důvody apod.).

6.6.5 ZPŮSOBY IMPLEMENTACE

Implementaci nové IP sítě do stávajícího prostředí je možné aplikovat dvěma základními způsoby, a to překryvně nebo postupnou migrací. Vzhledem k tomu, že implementace IP technologie zcela závisí na technickém vybavení prostředí – optická kabelizace, přenosové systémy apod., tak v síti SŽDC je možný pouze způsob postupné migrace. Překryvným způsobem je možné vyřešit pouze tranzitní úroveň sítě. Rozhodování o postupné migraci IP sítě se bude opírat o tři základní hlediska – technické a ekonomické a časové.

Z technického hlediska je nutné postupně nahrazovat ty části stávající sítě, kde jsou v provozu staré analogové systémy a systémy, které jsou na hranici životnosti, a nelze již pro ně zajistit odpovídající servis. Jedná se většinou o oblasti, kde nejsou k dispozici optické kabely a je nutné současně řešit i otázku odpovídající kabelizace a doplnění přenosových systémů.

Z ekonomického hlediska je nutné posuzovat stav a užitnost stávajících systémů. V telefonní síti je v současné době v provozu mnoho systémů, které byly vybudované v nedávné době, jejich stav je dobrý a zajišťují požadované služby v odpovídající kvalitě. Není v podstatě jiný důvod než systémový, tento stav v dohledné době řešit.

Z časového hlediska je nutné řešit otázku provázanosti sítě. Nemá smysl řešit koncovou úroveň sítě, pokud nebude v dané oblasti vyřešena tranzitní část, resp. odpovídající tranzitní uzel, který zajistí návaznost na IP síť.

Při zvážení výše uvedených hledisek je vhodný následující postup migrace IP telefonní sítě:

- 1) Vybudování tranzitní úrovně v IP prostředí a to jak uzlů s call managery, tak i ostatních tranzitních uzlů. V této úrovni je v podstatě již k dispozici propojení optickými kabely, podmínkou by bylo doplnit přenosovou síť. Práce spojené s touto přestavbou by se týkaly vnitřních technologií, odpadají složitá jednání ohledně správních řízení, problémy ohledně

povolovacích procesů a majetkoprávních vztahů. U tranzitních uzlů je možné postupovat metodou doplňování stávajících systémů IP bloky nebo výměnou celých uzlů případně kombinovaně. Odhad celkové doby pro přestavbu tranzitní úrovně je 1-2 roky včetně přípravy.

- 2) Postupná přestavba stávajících systémů na druhé úrovni sítě, výběr tratí pro přestavbu by vyhodnotili jednotlivé OŘ ve spolupráci se správcem telefonní sítě. Jednalo by se převážně o stavby, které by kromě telefonní sítě musely přednostně řešit kabelizaci a přenosové systémy. Vzhledem k tomu, že tyto stavby by zahrnovaly i venkovní technologie, podléhající správním řízení a řešení majetkoprávních vztahů, doba na jejich přípravu a realizaci je delší, odhadem cca 2-3 roky na jednu trať. Tyto stavby je nutné dále koordinovat s jinými stavbami SŽDC.

Tranzitní úroveň sítě by měla být řešena v jednom zcela kompatibilním systému. Koncová úroveň by měla být na trati opět navzájem plně kompatibilní, celý úsek trati by měl být ve stejném systému. Z hlediska staveb se jedná o to, aby spojovací systémy na stejné trati se řešily současně pro celou trať. Tento požadavek může narazit u staveb, jejichž předmětem je např. modernizace traťového úseku a stavbou jsou dotčeny pouze některé ŽST. bez technologické návaznosti na zbylé úseky tratě. Jednou z možností, jak tento problém řešit je řešit sdělovací technologii jako samostatnou stavbu, případně zpracovat podmínku řešení síťové sdělovací technologie nad rozsah stavební části stavby, tj. pro celou předmětnou trať.

6.7 Bezpečnost služební sítě

Z hlediska bezpečnosti je vhodné zabránit neautorizovanému přístupu do telefonní sítě, ve které se IP telefony nacházejí. Jako vhodná technologie se jeví protokol IEEE 802.1X v plném rozsahu, případně alespoň částečně.

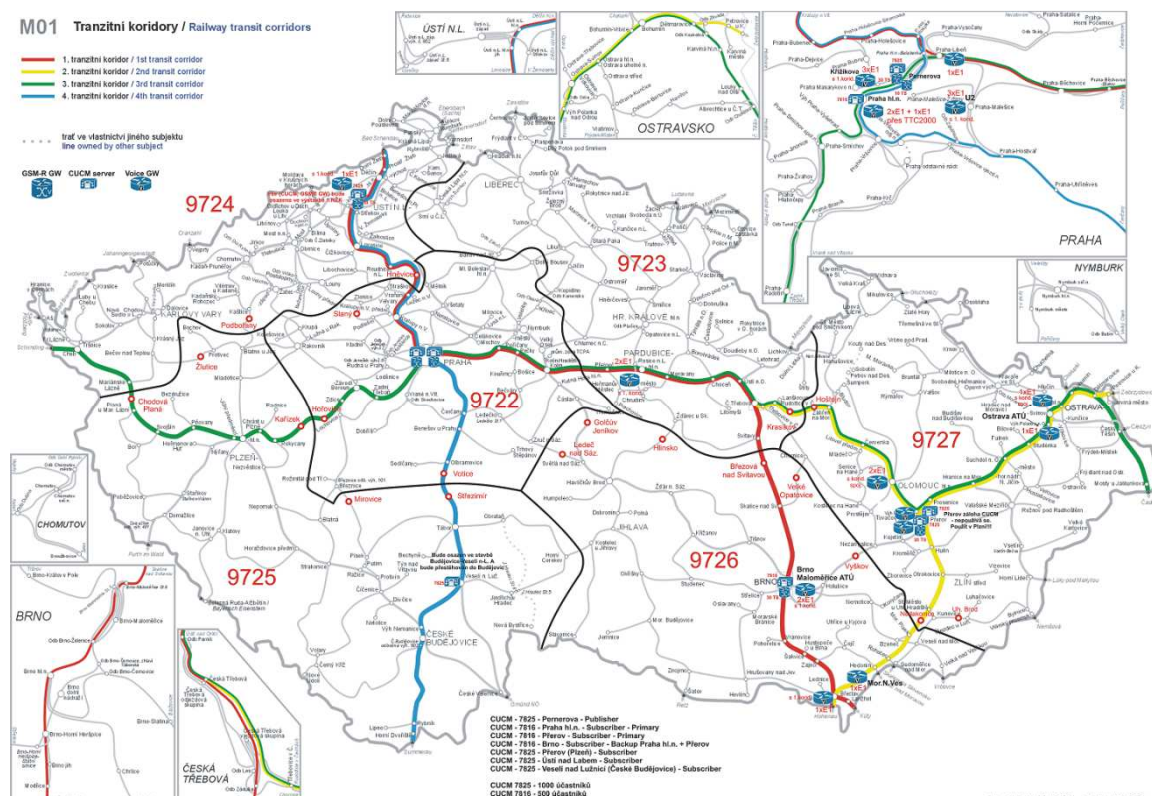
Stávající telefony pokud to umožňují nastavit pro využívání protokolu IEEE 802.1x v plné míře nebo alespoň částečně. Nevyhovující telefony postupně nahrazovat.

7 DOTYKOVÉ TERMINÁLY A ZAPOJOVAČE

V rámci produktů dispečerského řešení SŽDC se vyskytuje několik typů dotykových terminálů od několika výrobců. Tyto terminály byly dodány v různém časovém období, jsou na nich různé SW verze. Terminály odpovídají technické specifikaci SŽDC TS 6/2010-S, která popisuje jejich chování a je sjednocujícím prvkem.

7.1 Dopravní síť

Dotykové terminály a zapojovače jsou součástí dopravní sítě. Dopravní síť tvoří cluster CUCM. Tyto zapojovače jsou k CUCM připojeny buď přímou SIP registrací, nebo pomocí SIP trunku. V rámci této sítě je potřeba zajistit aktuálnost verze a podporu prvků CUCM v dopravní síti pro zajištění plné funkčnosti a bezpečnosti sítě.



OBR. 36 – SCHÉMA CLUSTERU CUCM DOPRAVNÍ SÍTĚ

7.2 Konsolidace terminálů

Terminály dispečerského řešení jsou dodávány v rámci jednotlivých staveb a je na nich tedy různá verze software odpovídající aktuálně platné technické specifikaci SŽDC TS 6/2010-S. Jelikož se požadavky na terminály v čase mění a tyto změny jsou postupně zapracovávány do specifikace, je potřeba zajistit sjednocení sw všech terminálů v provozu. Proto je nutné najít mechanismus, jak udržovat v terminálech stále aktuální sw odpovídající aktuálnímu znění specifikace.

V rámci udržování aktuálního stavu sw je potřeba v první fázi zajistit tyto úkony:

- Upgrade centrálních prvků;
- Upgrade HW dotykových terminálů;
- Upgrade SW všech terminálů na aktuální verzi.

Ve druhém kroku je pak potřeba zajistit mechanismus udržování aktuálního softwaru na všech prvcích dispečerského řešení:

- Zajištění aktuálního SW centrálních prvků;
- Zajištění podporovaného HW dotykových terminálů;
- Zajištění aktuálního SW všech terminálů dle aktuálně platné směrnice.

Poznámka

Dle směrnice SŽDC č.34 je potřeba každou změnu SW podrobit příslušnému schvalovacímu procesu (pouze schválení, akceptační testy nebo ověřovací provoz). A po každé změně SW v terminálu je třeba tento přezkoušet.

Jednotliví výrobci terminálů musí zajistit možnost vzájemného ovládání (ovládání terminálů z dispečerského pracoviště na tratích vybavených terminály různých výrobců).

7.3 Prostupy mezi služební a dopravní sítí

Dotykové terminály a zapojovače jsou připojeny do dopravní sítě, kterou tvoří cluster CUCM. Tyto zapojovače jsou k CUCM připojeny buď přímou SIP registrací, nebo pomocí SIP trunku.

Služební síť tvoří hybridní ústředny MX-ONE. Propoje mezi služební a dopravní sítí jsou realizovány pomocí E1 příček. Do budoucna se předpokládá nahrazení E1 příček za SIP trunky tam, kde to bude možné.

7.4 Číslovací plán

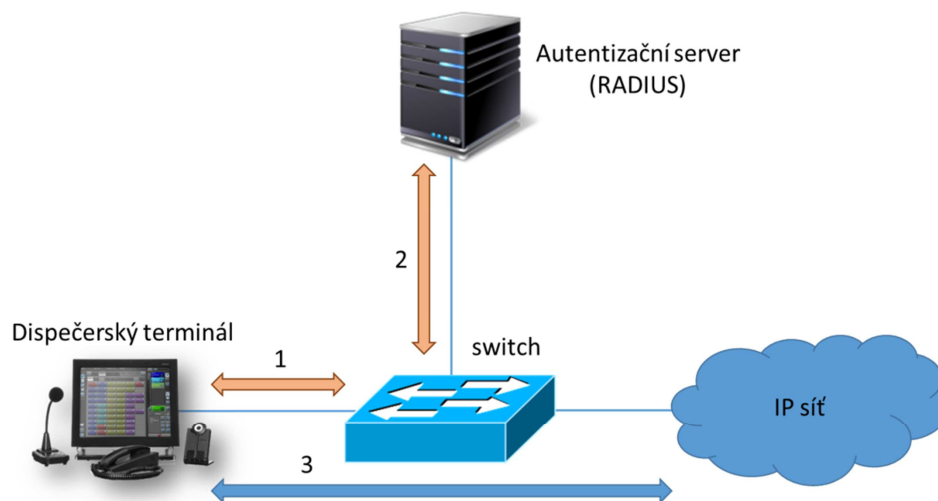
Stávající číslovací plán dopravní sítě je v devítimístném tvaru 9720xxxxx, což umožní bezproblémové směrování čísel mezi služební telefonní sítí a dopravní sítí. Tuto koncepci číslování doporučujeme zachovat.

Dále doporučujeme sjednotit přístup ke globálnímu telefonnímu seznamu SŽDC pro oba systémy, tedy služební telefonní síť a dopravní síť tak, aby uživatelé obou sítí mohli využívat překladů čísel na jména a volbu z globálního telefonního seznamu přes rozhraní LDAP. V souvislosti s tímto bodem bude nutné stanovit správce globálního telefonního seznamu.

7.5 Bezpečnost dispečerské sítě

Z hlediska bezpečnosti je vhodné zabránit neautorizovanému přístupu do počítačové sítě, ve které se dotykové terminály nacházejí. Jako vhodná technologie se jeví protokol IEEE 802.1X. Pokud se počítač či terminál připojí k přípojnému bodu (do portu switchu), je po něm pomocí protokolu 802.1X vyžadována autentizace. Přípojný bod blokuje veškerý ostatní datový provoz klienta do té doby, než je úspěšně autentizován.

Pro řízení autentizace je u klienta používán suplikant. Tento suplikant je nutné implementovat do dotykových terminálů. Z hlediska přípojného bodu je nutné, aby tento bod daný protokol podporoval.



OBR. 37 – PRINCIP AUTENTIZACE 802.1X

7.6 Síťová bezpečnost

Bezpečnost komunikační infrastruktury by se měla v požadavcích na návrh řešení odrážet minimálně v následujících skupinách požadavků:

- Segmentace a další architekturní požadavky na síť;
- Ochrana důvěrnosti a integrity přenášených dat;
- Zabezpečení přístupu do sítě;
- Podpora subsystémů kybernetické bezpečnosti a potenciál ke splnění aktuálních nebo budoucích legislativních požadavků.

7.6.1 SEGMENTACE INFRASTRUKTURY

Různorodost požadavků uživatelů aplikací a správců systému i navazujících procesů uživatele vyžaduje výkonné prostředky pro segmentaci sítě jako základní prostředek řízení informačních toků v jejím rámci. V rámci aktuálních trendů zajištění odpovídající segmentace znamená minimálně:

- Použití robustní technologie MPLS (*MultiProtocol Label Switching*), pro vytváření a provozování bezpečně oddělených a nezávislých virtuálních privátních sítí pracujících na třetí nebo druhé vrstvě modelu ISO/OSI;
- V případě L3 MPLS VPN dle standardu RFC 2547bis, požadavky na dostatečnou škálovatelnost a flexibilitu i s ohledy na budoucí perspektivy (růst společnosti, organizační změny, apod.) – minimální počet zřiditelných VPN, možnost definovat VPN sítě se sdílenými datovými zdroji a s konektivitou typu any-to-any nebo hub-and-spoke;

- Možnost vytvářet i L2 MPLS VPN pro transparentní propojení vybraných lokalit, podporu spojnic bod-bod i multipoint, typů Ethernet, Frame Relay, pevná linka apod. s diferencovanými a garantovatelnými QoS;
- Komunikační infrastruktura musí umožnit poskytovat síťové služby uvnitř jednotlivých VPN samostatně za individuálních podmínek (přístupové politiky, adresní plány včetně možného překryvu IPv4 adres, apod.).

7.6.2 OCHRANA DŮVĚRNOSTI A INTEGRITY PŘENÁŠENÝCH DAT

Jednou z nejdůležitějších služeb komunikační infrastruktury je ochrana důvěrnosti a integrity dat přenášných v rámci její LAN i WAN infrastruktury. Komunikační infrastruktura musí

- Zajistit šifrování aplikačního provozu ve vybraných MPLS VPN sítích, a to nejen **šifrování provozu mezi hraničními zařízeními komunikační sítě, ale podporovat rovněž** šifrování aplikačního provozu až do úrovně koncových stanic a serverů s využitím standardizovaných šifrovacích technologií;
- Pro šifrování aplikačního provozu nad MPLS VPN infrastrukturou musí být dostupné šifrovací metody, které umožní šifrovat aplikační provoz dynamicky, tj. bez předem definovaných bod-bod tunelů;
- Nedílnou součástí služeb komunikační infrastruktury zajišťujících ochranu důvěrnosti a integrity přenášných dat je i implementace PKI infrastruktury, která bude sloužit pro vydávání certifikátů jednotlivým zařízením a systémům připojeným do komunikační sítě.

7.6.3 ZABEZPEČENÍ PŘÍSTUPU DO SÍTĚ

Kromě standardního zajištění přístupu uživatelů a administrátorů do aplikací pomocí používání nástrojů pro ověření identity uživatelů a administrátorů - pomocí uživatelského jména a hesla - je žádoucí používat další prostředky pro ověření přístupu do sítě ještě před zahájením aktivit uživatelů či administrátorů. Jedním z doporučených způsobů autentizace je využití protokolu 802.1X, kdy je vyžadována autentizace hned po připojení zařízení do sítě, ať již kabelem nebo bezdrátově. Tímto způsobem je možno blokovat neautorizovaná zařízení či osoby v síti, případně namísto blokace je možné neautorizovaná zařízení soustředit do samostatné VLAN s řízeně omezeným přístupem ke zbytku sítě.

Pro řízení autentizace je u klienta používán suplikant. Z hlediska přípojného bodu je nutné, aby tento bod daný protokol podporoval.

Pokud není u klienta suplikant k dispozici (starší zařízení, nepodporující 802.1X atd.), je možné provést ověření alternativním způsobem, například pomocí MAC adresy. 802.1X je tedy možné implementovat postupně, zahrnout i starší zařízení tento standard nepodporující a postupně je pak nahrazovat zařízeními novými, které již podporována budou.

Pro řízení zabezpečení přístupu je vhodné použít specializovanou platformu pro NAC (Network Admission Control), která sjednotí a automatizuje mechanismus vynucovaného ověřování zařízení v síti.

7.6.4 PODPORA SUBSYSTÉMŮ KYBERNETICKÉ BEZPEČNOSTI

Komunikační infrastruktura musí být maximálně odolná proti bezpečnostním útokům. Z tohoto důvodu musí být nedílnou součástí komunikačních prvků:

- Robustní bezpečnostní mechanismy, které zajistí nejen ochranu přenášených dat, ale rovněž i ochranu samotných komunikačních prvků (ACL, firewall systémy, IDS/IPS systémy atd.);
- Nástroje pro aktivní monitorování datových toků pro účely detekce bezpečnostních incidentů včetně možnosti zasílání monitorovaných dat na centrální systémy, které zajistí kontinuální vyhodnocování bezpečnostních událostí včetně vazby na bezpečnostní systémy (pracoviště CIRC);

Uvedené komponenty připravují nově budovanou KI i na požadavky kybernetické ochrany dané nastupující evropskou a současnou národní legislativou, jejíž plná účinnost se očekává během životního cyklu dnes budovaných systémů. Jedná se zejména o Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, (dále jen „ZKB“), který ukládá řadě subjektů, mezi něž se svou důležitostí řadí i drážní prostředí, povinnost zavedení a dodržování bezpečnostních opatření a povinnost hlášení bezpečnostních incidentů. Implementované bezpečnostní prvky proto musí realizovat nebo alespoň musí být rozšiřitelné na plnou podporu požadovaných nástrojů dle ZKB, ke kterým patří:

- fyzická bezpečnost;
- ochrana integrity komunikačních sítí - HW, SW;
- ověřování identity uživatelů včetně přístupu administrátorů;
- řízení přístupových oprávnění včetně přístupu administrátorů;
- ochrana před škodlivým kódem;
- zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců;
- detekce kybernetických bezpečnostních událostí;
- sběr a vyhodnocení kybernetických bezpečnostních událostí;
- zajištění aplikační bezpečnosti;
- kryptografické prostředky;
- zajišťování úrovně dostupnosti informací;
- bezpečnost průmyslových a řídicích systémů.

Systémy pro administraci by navíc měly obsahovat podporu i pro organizační opatření podle §5 zákona, zejména:

- systém řízení bezpečnosti informací;
- řízení aktiv a rizik;
- bezpečnostní politika;
- organizační bezpečnost;
- stanovení bezpečnostních požadavků na dodavatele;

- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému;
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému;
- akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů;
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů;
- řízení kontinuity činností;
- kontrolu a audit kritické informační infrastruktury a významných informačních systémů.

V neposlední řadě by požadavky měly zahrnovat i služby KI pro podporu subsystémů víceúrovňové bezpečnosti a služby KI pro podporu systémů fyzické bezpečnosti.

Správce kritické komunikační nebo informační infrastruktury dle § 3 písm. c) a d) ZKB i správce významného informačního systému dle § 3 písm. e) ZKB jakožto orgán či osoba, které se ukládají povinnosti v oblasti kybernetické bezpečnosti, může po dodavateli technologií vyžadovat, aby prokázal, že výrobce nabízených aktivních síťových prvků má při vývoji svých produktů implementován tzv. "SDP - secure development lifecycle", tedy opakovatelný a měřitelný proces, navržený pro zvýšení odolnosti a spolehlivosti výrobků) a rovněž má k dispozici tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty, který spolupracuje se zdrojem zprávy pro potvrzení údajů o zranitelnosti výrobku, shromažďuje potřebné technické informace a zajišťuje vhodná nápravná opatření. Po skončení vyšetřování jsou pak výsledky doručeny tomu, kdo incident nahlásil spolu s plánem pro řešení a následné zveřejnění.

8 RÁDIOVÉ SYSTÉMY

Rádiové sítě provozované v prostředí SŽDC se dělí na dvě základní skupiny. Do první skupiny rádiových systémů náleží rádiové systémy liniového (stuhového) charakteru. Mezi tyto rádiové systémy patří evropský rádiový systém GSM-R (*Global System for Mobile communications – Railway*) pracující v kmitočtovém pásmu 900 MHz, národní rádiový systém TRS pracující v kmitočtovém pásmu 450 MHz, poloduplexní rádiový systém ASCOM pracující rovněž v kmitočtovém pásmu 450 MHz a simplexní národní rádiový systém SRV pracující v kmitočtovém pásmu 150 MHz.

Druhou skupinu rádiových systémů, resp. sítí tvoří rádiové systémy místního charakteru, tzv. místní rádiové sítě (MRS) pracující v kmitočtovém pásmu 150 MHz. Mezi místní rádiové sítě provozované u SŽDC patří např. SMV (*Síť manipulace vlaků*), TOS (*Technologická operativní síť*), VOS (*Všeobecná operativní síť*) a další.

8.1 Rozvoj stávajících rádiových systémů

Rozvoj a výstavba rádiových systémů v síti SŽDC jsou limitovány technickými specifikacemi pro interoperabilitu subsystémem řízení a zabezpečení transevropského konvenčního železničního systému, tzv. TSI CCS, k jejichž implementaci se Česká republika, resp. SŽDC zavázala vstupem do Evropské unie. V TSI je v současnosti uvedena **povinnost budovat jako první rádiový systém na železnici pouze a jedině evropský rádiový systém GSM-R**. Povinnost se týká jak drah zařazených do tzv. celoevropského železničního systému TEN-T (Trans-European Transport Network), tak i ostatních celostátních a regionálních drah. Tato povinnost byla potvrzena také dopisem 1. náměstka Ministerstva dopravy generálnímu řediteli SŽDC, s. o. ze dne 19. září 2016.

Výstavba jiných rádiových systémů, než evropského rádiového systému GSM-R, je tedy přípustná pouze jako doplněk k evropskému rádiovému systému. Vzhledem k výše uvedenému je výstavba doplňkových, převážně liniových národních rádiových systémů (TRS, SRV) značně neekonomická a nedoporučuje se jejich další rozvoj a výstavba.

Jistou výjimku může tvořit výstavba místních rádiových systémů, které lze v opodstatněných případech a na základě schválení generálního ředitelství SŽDC budovat ve velkých železničních uzlech a významných železničních stanicích především tam, kde na hlavní železniční trať pokrytou rádiovým systémem GSM-R navazují odbočné tratě pokryté národním rádiovým systémem TRS.

8.2 Údržba stávajících rádiových zařízení

Stávající rádiové systémy liniového charakteru (TRS, SRV, ASCOM), nebudou nadále již rozšiřovány, ale pouze udržovány. Údržba systému bude spočívat v zachování funkčnosti daného rádiového zařízení do doby, než budou nahrazeny novou technologií. Podmínkou pro údržbu je tedy dostatek náhradních dílů a technická podpora pro daná zařízení. Do údržby stávajících rádiových sítí bude dále nutné postupně zařadit taktéž problematiku zvyšování zabezpečení s ohledem na *zákon 181/2014 Sb., Zákon o kybernetické bezpečnosti* a o změně souvisejících zákonů v platném znění, a to přímo v samotných stávajících rádiových systémech, pokud to bude

technologicky možné, v opačném případě předřazením nových systémů, a to vždy s přiměřenými pořizovacími a provozními náklady (logování uživatelů, kontrola přístupů, ...).

Nad rámec běžné údržby je možno umísťovat nové základnové radiostanice TRS a SRV na železničních tratích pokrytých těmito rádiovými systémy pouze v případě, že nový systém nemění funkci nebo výkonnostní charakteristiky subsystému. Výstavba těchto nových základnových radiostanic musí být v souladu s platnými TSI.

8.2.1 TRAŤOVÝ RÁDIOVÝ SYSTÉM

Traťový rádiový systém provozovaný u SŽDC byl dodáván v současnosti dvěma výrobci. Těmito dvěma výrobními variantami jsou analogový systém výrobce T-CZ, a. s. a digitální rádiový systém TRS IP od výrobce DCom, spol. s r. o. Součinnost výrobců při údržbě rádiového systému TRS je samozřejmou nutností. V případě nahrazování rádiového systému TRS novějším rádiovým systémem GSM-R doporučujeme uchovávat výzisky pro budoucí využití právě při servisu daného zařízení.

8.2.1.1 Postup migrace a souběhu rádiových systémů TRS a GSM-R

Při výstavbě infrastruktury rádiového systému GSM-R budou prioritně touto technologií vybavovány tratě ve vazbě na jejich důležitost. Je vhodné, aby instalace GSM-R v rámci jedné stavby byla prováděna na poměrně dlouhém úseku (cca 100 km a více), jak bylo zmíněno výše.

Je předpoklad, že touto technologií budou vybaveny v první řadě celostátní tratě. To znamená, že pokud na trati bude nově nasazen rádiový systém GSM-R, zůstane původní rádiový systém v provozu souběžně nejvýše po dobu dvou měsíců (nebude-li stanoveno jinak) od data uvedení systému GSM-R do rutinního provozu. Konkrétní datum zahájení provozu rádiového systému GSM-R, resp. ukončení provozu původního vlakového rádiového zařízení bude oznámeno na portálu SŽDC to nejméně šest měsíců před provedením změny. Hnací vozidla musí být ale i nadále vybavena duálním rádiovým systémem, protože je předpoklad, že některé typy vozidel budou přejíždět do obvodu obou rádiových systémů. Na tratích se přechody mezi jednotlivými technologiemi budou signalizovat příslušnou návěstí („radiovníky“), aby byl strojvedoucí upozorněn na změnu rádiového systému.

Přechod z rádiového systému TRS na GSM-R je podmíněn řadou předpokladů. Vzhledem k tomu, že z železničních uzlů vycházejí tratě různých kategorií a s rozdílnou prioritou výstavby GSM-R, musí být vždy v dané oblasti po určitou dobu vybudovaná infrastruktura pro oba systémy. **Důležitým prvkem v postupném přechodu z TRS na GSM-R je vybavenost hnacích vozidel radiostanicemi schopnými pracovat v obou systémech (duální stanice).**

Migrační strategie u systému GSM-R vychází z využití duálního vybavení na vozidlech umožňujícími současně provoz v GSM-R i v národním analogovém systému TRS pro zajištění přechodu vozidel na trať, jejichž vybavení systémem GSM-R bude reálné až v delším časovém horizontu.

Je možné definovat několik přechodových procesů pro implementaci rádiového systému GSM-R. Prvním přechodovým procesem je vybavení všech hnacích vozidel, se kterými je uvažováno pro jízdu na železničních tratích vybavených systémem ERTMS/ETCS L2.

Druhým přechodovým stavem je vybavit stávající tratě systémem ERTMS/ETCS L2 (tj. i rádiovým systémem GSM-R). Jakmile budou všechny vybrané tratě systémem ERTMS/ETCS L2 vybaveny, může dojít k samotnému vybavení hnacích vozidel systémem GSM-R a následně může dojít k demontáži stávajícího traťového rádiového systému TRS.

Pokud by oba přechodové procesy probíhaly samostatně, je zřejmé, že migrace mezi oběma rádiovými systémy by trvala neúměrně dlouhou dobu. Proto se jeví jako optimální, kombinace obou přechodových procesů, tj. postupné zavádění systému GSM-R na vybraných železničních tratích a zároveň k souběžnému vybavování hnacích vozidel. Tento způsob je optimální jak z hlediska časového harmonogramu nasazování celého systému ERTMS/ETCS L2, tak i z praktického hlediska.

8.2.2 SRV

„Síť radiodispečerská vlaková (dále jen SRV)“ je druh traťového rádiového systému pracující v simplexní režimu, který byl zpravidla již v 70. letech budován jako základní rádiové spojení v kmitočtovém pásmu 150 MHz na železničních tratích provozovaných zpravidla podle předpisu SŽDC D3 společností Tesla Pardubice, na některých částech jako systém Tesla Selectic tzn. se selektivní volbou vždy pomocí kombinace dvou tónů ze tří (A, B, C). Při údržbě tohoto rádiového systému doporučujeme postupovat obdobně jako u rádiového systému TRS. Dodavatelem a výrobcem tohoto rádiového systému na české železnici byla převážně společnost DCom, spol. s r. o.

8.3 Rádiový systém GSM-R

Výstavba rádiového systému GSM-R byla na území České republiky zahájena pilotním projektem v roce 2004. Od té doby až do současnosti se neustále pracuje na jeho rozšíření. Rádiový systém GSM-R je budován na základě systémových SRS (*System Requirements Specification*) a funkčních požadavků FRS (*Functional Requirements Specification*) standardu EIRENE (*European Integrated Railway radio Enhanced Network*), které vydává a reviduje mezinárodní železniční unie – UIC (*International Union of Railways*). Aktuální platná verze je v případě SRS verze 16.0.0. a v případě FRS verze 8.0.0.

Předními výrobci a dodavateli technologie GSM-R byla potvrzena podpora technologií GSM-R minimálně do roku 2030. Podpora zahrnuje dodávky komponent, náhradních dílů a celkové technické podpory systému. Tato podpora byla potvrzena zástupci GSM-R Industry Group na 2nd UIC GSM-R Světové konferenci konané dne 15-16. 9. 2015 v Paříži.

8.3.1 ROZVOJ GSM-R

Stávající základnové radiostanice BTS (*Base Transceiver Station*) rádiového systému GSM-R jsou s nadřazeným kontrolérem BSC (*Base Station Controller*) a dále s ústřednou MSC (*Mobile Switching*

Center) propojeny pomocí téměř výhradně prostřednictvím přenosové technologie SDH s příslušnou redundancí. Konkrétně se jedná o multirámce digitálních přenosových systémů 1. generace, tzv. E1. Pouze v některých specifických případech (např. absence optického kabelu) je možno zvolit jiný, alternativní způsob připojení (např. modemy SHDSL na stávajícím metalickém kabelu, rádioreléový spoj, atd.). **Vzhledem k postupnému přechodu veškeré sdělovací technologie na protokol IP, bude přenos informací v rádiovém systému GSM-R nahrazován právě tímto protokolem.** Přechod na protokol IP s sebou ovšem nese problém kybernetické bezpečnosti a napadnutelnosti jednotlivých technologií, pracujících s tímto protokolem. Přechodu na protokol IP u technologie GSM-R musí tedy předcházet důkladná analýza rizik a technologická opatření k zamezení neoprávněného přístupu k přenášeným datům. V případě ústřednové části systému GSM-R SŽDC, s. o., tzv. NSS (*Network Switching Subsystem*) byla již v nedávné době provedena migrace technologie do IP prostředí.

Využívání jednotlivých možností nabízených systémem GSM-R (hlasové, datové a řídicí funkce) bude upravováno dle aktuálních požadavků správce a provozovatele systému.

8.3.2 VÝSTAVBA GSM-R

Výstavba nových úseků sítě GSM-R musí probíhat v úzké návaznosti na již pokryté úseky železničních tratí. V současné době jsou systémem GSM-R pokryty převážně národní železniční koridory (I., II., III., a částečně IV. TŽK) a důležité objízdné trasy koridorů (např. trať Kolín – Havlíčkův Brod – Brno). Z tohoto důvodu je nezbytné v případě další výstavby systému GSM-R navazovat na uvedené úseky a budovat další ucelené úseky rádiové sítě GSM-R. **Za zcela neracionální a dopravně nepřijatelné je považována výstavba tzv. „ostrovů“, tj. krátkých úseků pokrytých signálem GSM-R, které na žádné straně nenavazují na stávající traťovou část systému GSM-R.** V takovém případě by bylo nutno zbytečně mezi sebou přepínat používané sítě, např. TRS / GSM-R / TRS. Z tohoto důvodu je nutno v připravovaných stavbách SŽDC, které nejsou primárně zaměřeny pouze na budování sítě GSM-R (tj. např. stavby optimalizací, modernizací a racionalizací železničních tratí) důsledně vyžadovat, aby byl navržen nezbytný přesah rádiového systému nad rámec samotné stavební části stavby, jako je tomu v současnosti například při budování optické a metalické kabelizace, přenosových systémů a zabezpečovacího zařízení.

Také na úsecích tratí s tzv. úsekovým ovládáním zařízení ÚOZ (1 výpravčí v určené ŽST na trati ovládá 1-3 neobsazené dopravní na tuto řídicí dopravnu přiléhající) nebo začleněním těchto úseků do dálkového ovládání zařízení DOZ z CDP je nutné budovat nebo upravovat vlakové rádiové systémy pro komunikaci se strojvedoucím tak, aby došlo ke sjednocení typu rádiové technologie (analogového nebo digitální GSM-R) do jednoho typu vždy v celém úseku trati s ÚOZ nebo DOZ a ne jen v úseku dotčeném komplexní novou výstavbou nebo revitalizací, protože hrozí při nárůstu specifických povinností při řízení drážní dopravy pochybením lidského faktoru (strojvedoucího), který uvnitř UOU nebo DOZ nepřepne u návěsti platné pro rádiový provoz typ vlakového rádiového systému z toho plynoucí nebezpečí nemožné rádiové komunikace včetně možnosti nouzového zastavení vlaku pomocí nadstavbové funkce vlakového rádiového systému „G-STOP“.

V připravovaných stavbách, které budou řešit výstavbu traťové části systému GSM-R, je nezbytně nutné již během zpracování přípravné dokumentace při samotném návrhu rozmístění a situování základnových stanic BTS vycházet nejenom z hlediska rádiového plánování, které je samozřejmě při návrhu primární, ale rovněž z hlediska požadavků budoucích uživatelů systému GSM-R, tj. z požadavků řízení provozu a zajištění provozuschopnosti dráhy. Z tohoto pohledu je žádoucí, aby v případě nového návrhu situování jednotlivých BTS byly základnové stanice primárně umísťovány do obvodu železničních stanic a na tyto pevné body sítě byly dále navazovány další BTS v zastávkách, příp. na širé trati. Tímto řešením bude zajištěno, že obvod dotčené železniční stanice bude pokryt pouze signálem z jedné BTS a budou tak v budoucnu eliminovány problémy při následném definování oblastí volání, skupinových hovorů atd.. Z výše uvedeného je patrné, že samotné handover musejí být přednostně v mezistaničních úsecích.

Za alternativní způsob výstavby rádiového systému GSM-R může být považováno rozdělení digitálního modulu – DM (Digital Module) s umístěním ve vnitřních prostorách, popřípadě ve vnější přístrojové skříni společně s napáječem a výkonového modulu RRH (*Remote Radio Head*) s umístěním ve vnějších prostorách přímo na stožáru. Mezi výhody tohoto řešení patří:

- Možnost připojení více RRH s rozdílným umístěním na jeden DM;
- Eliminace použití koaxiálních kabelů s velkými poloměry ohybu a snížení útlumu při přenosu vf energie mezi RRH a anténním systémem na minimum;
- Jedna BTS může pokrýt signálem GSM-R až cca 30 km žel. trati.

Vzhledem k dosavadnímu způsobu zadávání a postupu budování systému GSM-R u SŽDC (tzn. vždy po jednotlivých traťových úsecích), vyvstaly drobné nedostatky spočívající v nedokonalém pokrytí určených vnitřních prostor drážních budov signálem GSM-R. Tento stav je důsledkem budování systému GSM-R striktně dle specifikace EIRENE pro ETCS L2, která definuje pouze úroveň pokrytí samotných železničních tratí signálem GSM-R pro HV s VR a externí anténou, a tudíž neřeší možné problémy při komunikaci drážních zaměstnanců v síti GSM-R v budovách atd. Postupným připojováním jednotlivých základnových stanic BTS ke kontrolérům BSC a dále k ústředně MSC docházelo k ne zcela vhodnému zapojování jednotlivých BTS do smyček E1 v přenosovém traktu. To se projevilo například při dostavbě nových BTS, které zajišťují vstup do oblasti ETCS (*European Train Control System*). Z těchto důvodů navrhujeme provést analýzu a následně optimalizaci stávajícího rádiového systému GSM-R, která by napravila výše zmíněné nedostatky a optimalizovala tak stávající provozovanou síť GSM-R SŽDC.

V případě využití BTS, umožňující rozdělení digitálního DM a výkonového modulu RRH, by bylo vhodné v rámci této optimalizace uvažovat i s náhradou původně instalovaných repeaterů. Repeatery by byly nahrazeny právě těmito novými typy BTS, resp. jejich výkonovými částmi. Z velké části by byla využita stávající infrastruktura (přípojný optický kabel, přípojka NN, anténní nosič...).

Vzhledem k budoucímu rozvoji sítě GSM-R a k nemožnosti budovat jiný rádiový systém, doporučuje tato Studie provést celosíťové rádiové plánování, které by zmapovalo možnost pokrytí zbývajících železničních tratí rádiovým systémem GSM-R. Tento materiál by pak byl závazný pro všechny připravované stavby SŽDC, jejichž součástí by byla výstavba rádiového

systému GSM-R (např. modernizace, optimalizace, elektrizace, revitalizace atd.). V rámci těchto staveb by tedy byly v návaznosti na tento materiál připraveny určené lokality, a to buď vytvořením nezbytné technické přípravy pro budoucí možnost výstavby BTS (např. dimenze napájení, pokládka HDPE trubek, resp. sdělovacích a NN kabelů, vytipování a rezervování potřebné plochy pro výstavbu BTS...) nebo přímo výstavbou této základnové stanice. Zároveň by tento materiál dal investorovi nahlédnout do složitosti a náročnosti pokrývání nových traťových úseků systémem GSM-R.

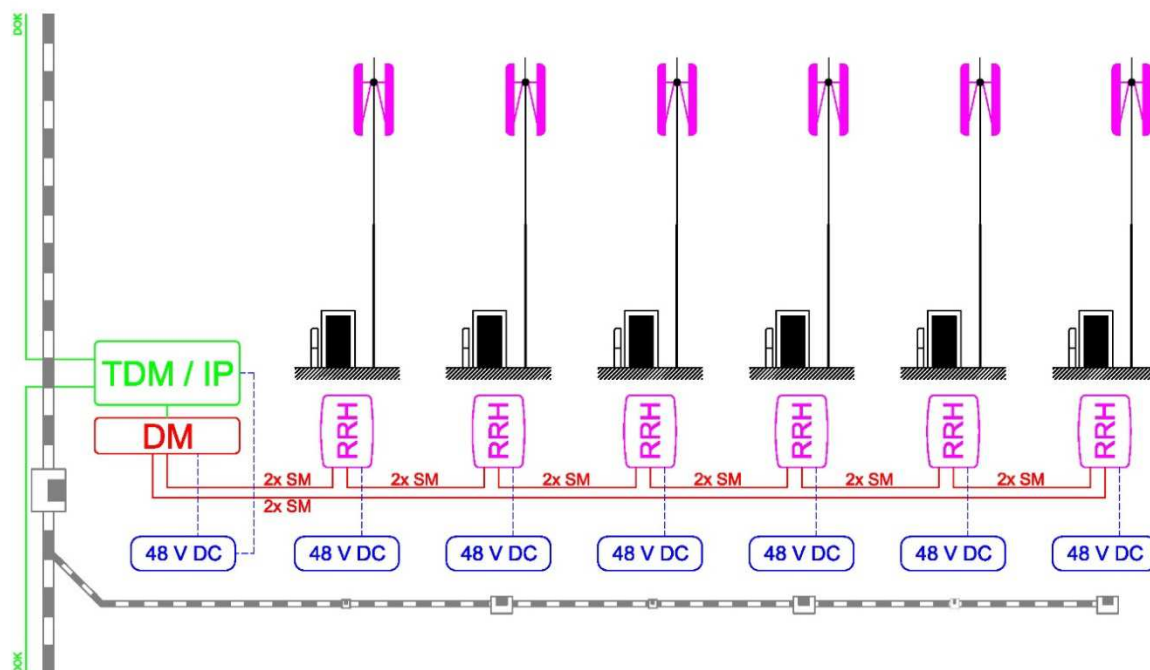
8.3.3 FUNKCIONALITA GSM-R STOP

Funkcionalita GSM-R STOP je nástavbou rádiového systému GSM-R a je popsána v technické specifikaci systémů, zařízení a výrobků číslo TS 3/2014-S. Tato funkcionalita, která není náhradou za systém ETCS, ale bude výrazným zvýšením bezpečnosti všude tam, kde je již rádiová síť GSM-R vybudovaná a aktivní, ale systém ETCS dosud není vybudovaný, se začíná postupně uplatňovat a do budoucna bude její implementace v rámci výstavby systému GSM-R povinností. Hlavním důvodem je samozřejmě zvýšení bezpečnosti na provozované dopravní cestě. Například v součinnosti s kamerovými systémy a celým systémem videomonitoringu tak vznikne velmi účinný podpůrný nástroj pro prevenci mimořádných událostí.

8.3.4 GSM-R JAKO NÁHRADA RÁDIOVÝCH SÍTÍ TRS SRD A TRS SRV

Vzhledem k výše uvedeným faktům a novým technologickým možnostem se nabízí možnost výstavby rádiového systému GSM-R i v tzv. režimu náhrady sítí TRS SRD a TRS SRV. Rádiový systém GSM-R by na méně frekventovaných železničních tratích, především tratích regionálního charakteru, nemusel být budován s vidinou budoucí implementace evropského zabezpečovacího systému ETCS ve verzi level 2, ale ve verzi nižší, resp. bez systému ETCS. Tento režim výstavby by ve spojení s aplikací GSM-R STOP mohl vést ke zvýšení bezpečnosti na regionálních tratích a mohl by částečně nahradit národní traťový rádiový systém TRS, který již nebude možno nadále budovat jako základní rádiový systém.

Tento způsob řešení (Obr. 38) by spočíval ve výstavbě nižších typizovaných stožárů s menšími anténami a s umístěním výkonových vysílacích částí BTS (RRH) přímo na stožárech. Na jeden řídicí digitální modul BTS (DM) by tak mohlo být připojeno až 6 rádiových bodů. Podmínkou výstavby rádiového systému GSM-R v tomto režimu ovšem zůstává nutnost přípravy napájení pro jednotlivé rádiové body a nutná přítomnost optického kabelu s dostatečnou volnou kapacitou na dané žel. trati. Každý oddálený výkonový modul RRH je nutno připojit pomocí dvou optických SM vláken. Alternativou připojení RRH k DM je připojení prostřednictvím modemů nasazených na ev. stávajícím metalickém kabelu dálkovém, resp. traťovém. Vzhledem k technickému stavu těchto metalických kabelů na regionálních tratích, způsobu jejich uložení (mnohdy s uložení na povrchu u paty kolejnice) a především absenci kvalitních přenosových parametrů kabelových prvků je však taková možnost využití metalických kabelů spíše teoretická.



OBR. 38 – VÝSTAVBA RÁDIOVÉHO SYSTÉMU GSM-R JAKO NÁHRADA SÍTÍ TRS SRD A TRS SRV

8.4 Místní rádiový systém MRS

Místní rádiový systém MRS v kmitočtovém pásmu 150MHz není interoperabilní a bude dále využíván především jako rádiový systém pro umožnění provádění technologie (posun, údržba ZZ...) vedle primárního systému GSM-R. Jeho budování (popř. údržba) bude prováděno pouze ve zcela výjimečných případech, jejichž schvalování spadá pod generální ředitelství SŽDC, a to především ve velkých železničních uzlech a v dopravně významných železničních stanicích, kde jsou zaústěné odbočné tratě vybaveny národním traťovým rádiovým systémem TRS, který nelze pro dorozumívání zaměstnanců při posunu používat.

8.4.1 VÝSTAVBA MRS

Podmínkou výstavby nových základnových radiostanic MRS je schválení takové výstavby generálním ředitelstvím SŽDC.

V případě, že bude schválena výstavba nové základnové radiostanice MRS, doporučujeme pro výstavbu využívat v maximální míře infrastrukturu rádiového systému GSM-R, tedy technologické objekty, stožáry atd. Nové základnové radiostanice doporučuje tato studie budovat v IP provedení a umísťovat je do 19" skříní, napájení pak realizovat ze zálohovaných zdrojů 48 V DC, které jsou budovány v rámci výstavby rádiového systému GSM-R a přenosové technologie. Ovládání těchto základnových radiostanic doporučujeme integrovat do IP dotykových terminálů a vyvarovat se umísťování analogových ovládacích souprav, pro jejichž umístění je nutno dodržet maximální délku propojovacího kabelu.

8.5 Budoucnost rádiových systémů pro železnici

Jelikož v současnosti se teprve připravuje specifikace pro nový rádiový systém, který by nahradil rádiový systém GSM-R, nelze prozatím počítat s jinými alternativami k systému GSM-R. Diskutovaným nástupcem rádiového systému GSM-R byl systém LTE-R (*Long Term Evolution – Railway*). Tento systém ovšem nemá v současné době zpracovány funkční ani systémové specifikace (FRS a SRS) a s ohledem na složitý a zdoluhavý proces jejich vytvoření.

V současné době se na půdě UIC zahajují práce na základech specifikace zcela nového mobilního rádiového systému využitelného pro potřeby železniční dopravy, který by v budoucnu systém GSM-R nahradil. Největší perspektivu má pravděpodobně specifikace vyvíjená v rámci projektu Shift2Rail na bázi 3GPP s možností nasazení jak na LTE, tak na 5G.

8.6 Železniční bezdrátová síť

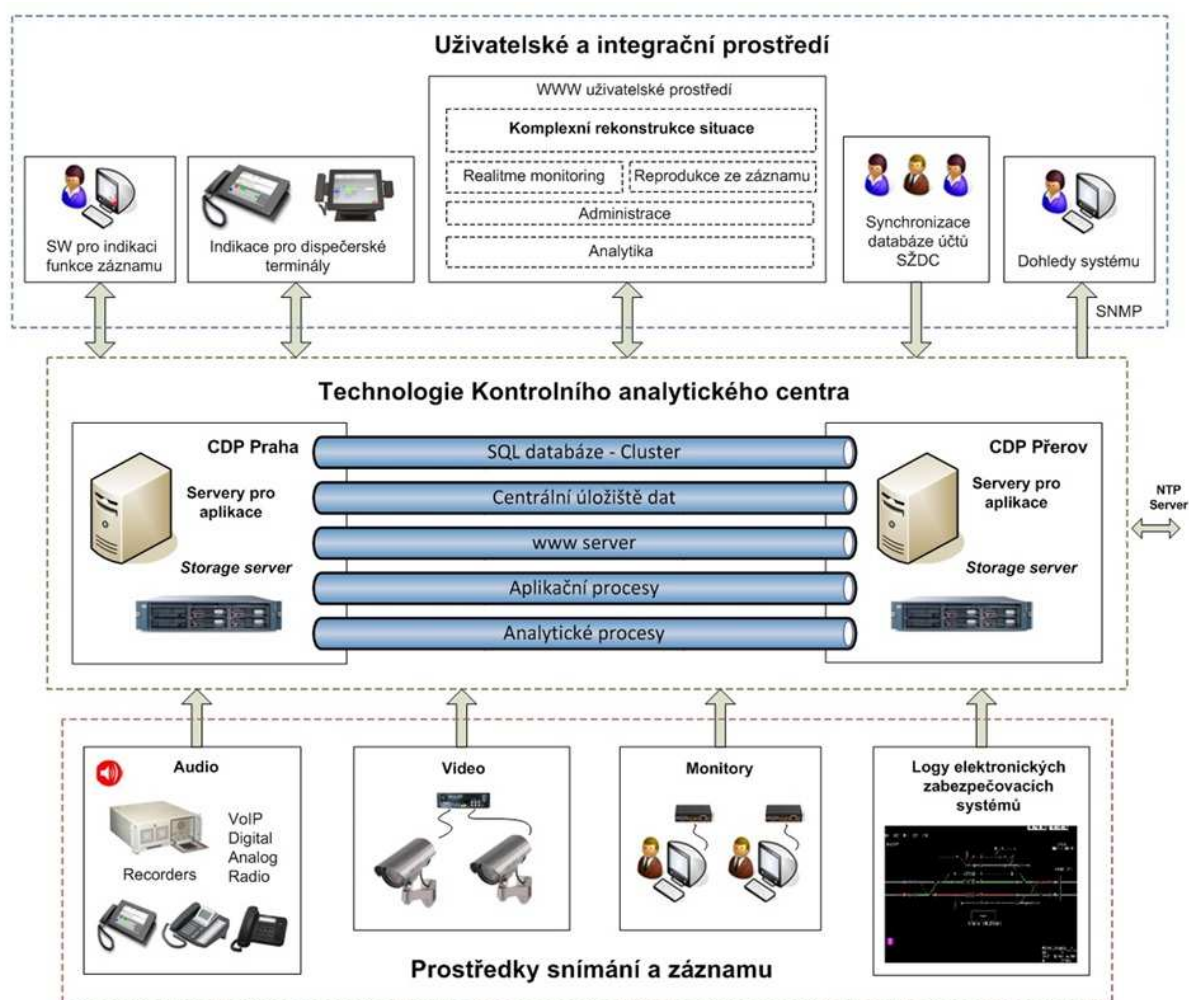
Mezi standardní vybavení železničních tratí by mělo patřit i kvalitní celoplošné pokrytí železniční infrastruktury technologií veřejné bezdrátové komunikace typu GSM jako služby pro cestující veřejnost, kde GSM se v širším slova smyslu myslí nejen hlasové služby, ale především vysokorychlostní datové služby 3G-4G a LTE. Nicméně lze očekávat, že zájem o pokrytí datovými službami budou mít zejména operátoři osobní dopravy, aby mohli datové služby poskytovat cestujícím na palubě prostřednictvím WLAN. Garance takové služby však nepřísluší provozovateli dráhy, nýbrž je záležitostí veřejných poskytovatelů telekomunikačních služeb. Pro eliminaci možných rizik spojených s posilováním GSM služby (např. v podobě negativních vlivů na železniční sdělovací systémy apod.) musí před nasazením služby do provozu proběhnout ověřovací a zkušební provoz, který ověření možnosti rušení sdělovacího a zabezpečovacího zařízení zejména pak rádiového systému GSM-R.

Aplikace této technologie **umožňuje realizaci řady telematických služeb** (odbavování cestujících, informační systémy pro cestující, sledování zásilek, telemetrie a diagnostika vozidel atd..) a rovněž **umožní výrazně zatraktivnit železniční dopravu**. Pokrytí celé tratě je důležité pro zajištění celosíťovosti železniční dopravy, tím její dostupnosti a atraktivity, a zároveň umožňuje řešit integrované dopravní systémy v území s využitím železniční dopravy jakožto rychlého, bezpečného, spolehlivého a atraktivního módu dopravy.

Zároveň se ukazuje jako technická nutnost, provést opatření na straně kolejových vozidel. Kolejová vozidla z principu konstrukce skříně (kovová uzavřená skřín) vyžadují pro optimální pokrytí signálem GSM instalovat uvnitř vozidel technologie pro zesílení/převod signálu GSM. Pro optimální provedení by však byla vhodná standardizace a sjednocení těchto technologií v rámci segmentu ITS, aby kvalita a dostupnost těchto služeb mohla být garantována ve všech vozidlech a na celé železniční síti.

9 KONTROLNĚ ANALYTICKÉ CENTRUM ŘÍZENÍ DOPRAVY

Kontrolně analytické centrum (KAC) v současné době poskytuje funkcionality komplexní rekonstrukce situace vztažné k řízení a organizování drážního provozu ze záznamu (Obr. 39). Situace je rekonstruována časově synchronní reprodukcí záznamů hlasové komunikace, video záznamů, obrazovek monitorů a logů činnosti zabezpečovacích zařízení z vybrané lokality resp. uzlu řízení provozu (např. CDP, ŽST.). Dále je podporována funkce přenosu aktuální reálné situace (video monitoringu) z vybrané lokality do nadřízeného centra a to s minimálním časovým zpožděním.



OBR. 39 – STÁVAJÍCÍ FUNKCIONALITA A STRUKTURA APLIKACE KAC

Uživatelské funkce jsou poskytovány prostřednictvím internetového prohlížeče. Je kladen důraz na jednoduchost a přehlednost prostředí, zvláště pro rutinní funkce pro nejnížší úroveň oprávnění pracovníků v přímém výkonu řízení dopravy. Z hlediska ovládání, KAC centralizuje a soustřeďuje konfiguraci, správu a dohled funkčnosti integrovaných prostředků snímání a záznamů.

První etapa KAC zajistila a předala do provozování robustní centralizovaný systém pro monitoring, záznam a analýzu činností při řízení dopravy, který slouží:

- Dispečerům a výpravčím pro:
 - akutní ověřování faktů z komunikace;
 - indikaci funkčního a probíhajícího záznamu;
- Pracovníkům vykonávající kontrolní činnost:
 - dohled a prověřování výkonu dopravní služby dispečerů a výpravčích ze záznamu a online;
 - dostávají systém pro evidenci nálezů a jejich řešení včetně systému reportingu
- Pro pracovníky účastníci se šetření mimořádností:
 - systém jim poskytuje „od stolu“ dostupná data jako informace před vlastním řešením v terénu;
 - nástroj pro evidenci provozních dat a dalších dokumentů k mimořádným událostem
- Pro analytické pracovníky:
 - dostupná data z provozu pro posuzování souvislostí a výjimek, synchronní reprodukce vzájemně souvisejících dat.

9.1 Rozšiřování funkcionalit a možností aplikace KAC

Studie předpokládá rozšiřování a zapojování dalších stávajících zařízení SŽDC do aplikace KAC. Tím jsou míněna typová zařízení, která již do aplikace KAC data poskytují (zařízení pro záznam hlasu, kamerové systémy, diagnostikovaná data ze zabezpečovacích zařízení, EZS a EPS systémy, DVI-D sondy). V rámci tohoto tématu doporučujeme provést analýzu, která všechna zařízení podporovaného typu v síti SŽDC mají být připojena do KAC, a tento rozsah realizovat. V případě překročení licence na počet zařízení určitého typu je nutné počítat s dodatečnými náklady na licenční krytí.

V rámci analýzy by měla být zachycena potřeba rozvoje aplikace po funkční stránce - zda současné funkce zabezpečí všechny budoucí potřeby zaměstnanců SŽDC od tohoto SW. Pokud ne, budou z analýzy vytvořeny požadavky na další vývojové práce."

Studie dále uvažuje aplikaci KAC jako hlavní konsolidační prostředek nejrozličnějších kontrolních analytických a monitorovacích prostředků sloužících k řízení provozu. Doporučuje ve spolupráci s gestorem řízení provozu (SŽDC, Odborem O12) provést analýzu potřeby zapojení jiných typů zařízení, než jaké aplikace KAC v současné době podporuje. V rámci analýzy by měla být zachycena potřeba rozvoje aplikace po funkční stránce.

9.1.1 ROZŠIŘOVÁNÍ STÁVAJÍCÍCH FUNKCIONALIT KAC

V nejbližší etapě rozšíření systému KAC by mělo být následující:

- Úpravy uživatelských funkcí KAC a začleňování nových funkcí podle poznatků z provozování

- rozšíření systému přístupových práv, zavedení systému překrývajících a paralelních hierarchických struktur (organizace GŘ - OŘ - ... – stanice versus GŘ – CDP ... a versus GŘ – struktura inspekce, ...);
- úpravy mapových podkladů dle požadavků uživatelů;
- požadavky na úpravy reportů a workflow e-mailových notifikací;
- a další funkce z námětů z provozu KAC;
 - funkce požadované uživateli na různých úrovních;
 - funkce podporující správu a servis celého systému.
- **Připojení dalších stávajících zařízení do aplikace KAC stávajících zařízení, které je nutné připojit do KAC**
 - Integrace dalších kamerových systémů určených pro řízení provozu;
 - Integrace dalších záznamových zařízení;
 - Integrace dat ze zabezpečovacího zařízení;
 - Doplnění dalších železničních stanic do systému KAC;
 - Rozšíření systému monitoringu obrazového videa na zabezpečovací zařízení, zajištění požadované úrovně zabezpečení SIL ve spolupráci s dodavateli zabezpečovacích zařízení.
- **Rozšíření podpory aplikace KAC o další typy zařízení v síti SŽDC**
 - Doplnění ovladačů pro nové typy např. kamery, EPS, EZS a další.
- **Analýza požadavků vyplývajících z nového zákona o kybernetické bezpečnosti na technologii KAC a návrh na zabezpečení těchto požadavků**

9.1.2 NOVÉ FUNKCIONALITY APLIKACE KAC

V dalších etapách by měl být systém KAC rozšířen o další nové funkcionality a měla by být vytvořena užší integrace s dalšími systémy. Jedná se zejména:

- **Začlenění dalších typů informací ze systémů DDTS ŽDC a těsnější provázání**
 - Začlenění elektrického ohřevu výměn, osvětlení včetně nouzového osvětlení a dalších informací z DDTS ŽDC⁸.
- **Integrace se systémem GSM-R, poloha vlaku**
 - zavedení geografického oprávnění podle pozice vozidla v době;
 - zobrazení pozice vozidla v mapě podle polohových údajů ze sítě GSM-R (BTS, směrník, vzdálenost) na začátku a konci hovoru pro možnost posuzování okamžiku přijetí informace;
 - zobrazení dostupných GSM-R terminálů v inkriminované oblasti v mapě – jako jedna z posledních možností zabránění mimořádnosti při nedostupnosti vozu.
- **Těsnější integrace aplikací zabezpečovacího zařízení (synchronnost při rekonstrukci situace)**

⁸ Ve smyslu ČSN EN 1838:2015 Světlo a osvětlení - Nouzové osvětlení je předpoklad, že nově instalované NO bude kontrolováno a provozováno i v souladu s ČSN EN 50172 Systémy nouzového únikového osvětlení resp. ČSN EN 62034 ed. 2 Automatické zkušební systémy pro nouzové únikové osvětlení napájené z baterií.

- přechod na www prostředí klienta a jeho plná integrace do prostředí KAC.
- **Začlenění indikátorů horkoběžnosti a plochých kol**
 - pozice vlaku na kontrolních bodech, integrace základní výstupů uvedených systémů pro korelaci s dispečerskými daty.
- **Integrace se systémem integrovaného technologického systému správce železniční infrastruktury**
- **Rozšíření a doplnění algoritmů pro zpracování hlasové komunikace (audio záznamů)**
 - Doplnění algoritmů zpracování audio záznamů o systém vyhodnocování kvality signálu s ohledem na srozumitelnost jako podklad pro hodnocení pokrytí rádiovým signálem a stavu rádiových sítí;
 - Rozšíření kapacit systému pro přepis hlasové komunikace do textu pro rozšíření působnosti nástroje pro kontrolu hovorové kázně dle předpisu D1 a pro plnou možnost vyhledávání komunikace podle klíčových slov a frází;
 - Zasiťování ReDatů, které nejsou dostupné pro KAC a nahrazování zbývajících starých systémů záznamu hlasu na bázi PC za řešení záznamů typu „black box“.
- **Centrální zastřešení kamerových systémů na přejezdech, video analytika výskytu překážek a vozidel v době výstrahy včetně rozlišení druhu vozidla a případně SPZ, obecný reporting, automatizace podkladů pro činné orgány**
 - KAC bude zastřešovat různé typy kamerových systémů od různých výrobců určených pro provoz, z tohoto hlediska se jedná o rozšíření systému;
 - KAC bude mít vyřešen systém přístupu k datům, který bude schválen z hlediska legislativy;
 - KAC bude poskytovat vstup také externím organizacím podle jasně definovaných pravidel a oprávnění, lze umožnit přístup např. policii s odpovídající úrovní zabezpečení
 - KAC bude mít systém pro vyšetřování mimořádností schválený O30 a používaný inspekcí, nabízí se rozšíření o zpracovávání předpokladů k mimořádnostem z přejezdů;
 - KAC obsahuje prostředky a bude provozovat algoritmy pro analýzu záznamů, bude připraven pro rozšíření o algoritmy zpracování videa pro rozpoznávání objektů na přejezdech;
 - KAC umožňuje vytvořit systém e-mailových notifikací pro orgány pověřené šetřením těchto incidentů a systém reportovacích výstupů;
 - Integrace na systému o stavu přejezdů a přechodů.
- **Systém pro monitorování hlukového pozadí a dokladování dodržování hygienických požadavků a odhalování „nekompaktních“⁹ vozidel**
 - analýza způsobů, norem a metodik měření hluku, analýza kde hluk v drážní dopravě měřit;
 - výběr možností řešení a realizace zvukových sond a zabezpečení datového přenosu do KAC pro snímání zvuku a detekci úrovně hluku;

- zavedení systému pro kalibraci úrovně zvuku a vyhodnocování úrovně;
- umístění prostředků do mapy, zabezpečení možnosti korelace se stavem dopravy, polohou vozidel;
- realizace pilotního projektu řešení, rozmístění soud, zavedení do KAC, dodání úprav uživatelských funkcí pro vyhodnocování, vytvoření systému přístupových práv, vytvoření a konfigurace reportovacích sestav.

V budoucnosti je možné směřovat k větší centralizaci okruhů v síti SŽDC tzn., směřování nahrávání VoIP komunikace, resp. komunikace směřované po IP do center KAC (redundantně) bez nutnosti provozování záznamových zařízení v bodech řízení dopravy a postupně nahrazovat stávající záznamová zařízení pro záznam analogových a TDM signálů za hlasové gateways.

⁹ Vozidla nesplňující předepsané parametry, normy atd.

10 INFORMAČNÍ MANAGEMENT ŽELEZNIČNÍ INFRASTRUKTURY

10.1 Dálková diagnostika technologických systémů železniční dopravní cesty

Přenesení obsluhy zabezpečovacího zařízení většího počtu železničních stanic do dispečerských pracovišť vyžaduje, aby byly soustředěny i další informace ze souvisejících technologických systémů železniční dopravní cesty (TLS) pro zajištění provozuschopnosti železniční dopravní cesty (ŽDC). Z tohoto důvodu byl v rámci sítě SŽDC vytvořen systém dálkové diagnostiky technologických systémů železniční dopravní cesty (DDTS ŽDC). Do systému DDTS ŽDC jsou dnes přenášeny TLS zejména pak:

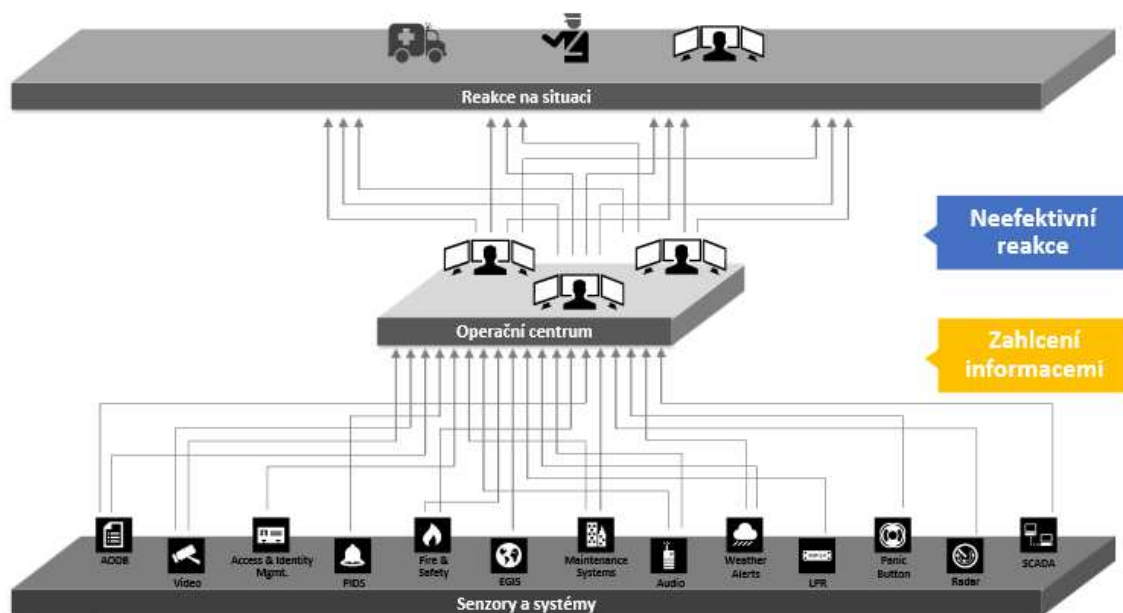
- Elektrický ohřev výměn (EOV);
- Osvětlení železničních stanic a zastávek (OSV);
- Autonomní samočinný hasicí systém;
- Zařízení pro detekci požáru;
- Elektronická zabezpečovací signalizace;
- Informační systémy pro cestující (ISC);
- Kamerové systémy (KAMS);
- Elektrická předtápěcí zařízení (EPZ);
- Odečet spotřeby elektrické energie;
- Eskalátory;
- Výtahy.

Informace z TLS jsou přenášeny přes integrační koncentrátoři (InK) na integrační servery (InS). InS soustřeďuje diagnostické informace z TLS a poskytuje data klientským pracovištím. Veškeré přenosy a sběr dat jsou navrženy v souladu s technickou specifikací TS 2/2008-ZSE „Dálková diagnostika technologických systémů železniční dopravní cesty“ v platném znění a gestorského výkladu k Technickým specifikacím 2/2008 – ZSE, č.j. 5641/2016-SŽDC-O14 ze dne 8.2.2016 (GVTS 2/2008-ZSE).

Díky rychlému vývoji technologií a možnosti získávání informací z různých zdrojů přicházejí i možnosti, jak tato data využít i v oblasti ochrany života, zdraví a majetku. Tradiční dohledová a přijímací centra sice poskytují základní možnosti ochrany, nicméně dnešní prostředky již nabízejí firmám a organizacím komplexnější řešení. Jedná se o souhrn HW a SW prostředků, který integruje nezávislé bezpečnostní aplikace a zařízení do jednoho funkčního celku a ovládá je pomocí centrálního komplexního uživatelského rozhraní. Shromažďuje a vyhodnocuje události z existujících různorodých bezpečnostních zařízení a informačních systémů (video, řízení přístupu, senzory¹⁰, analytika, sítě, systémy budov, atd.) a identifikuje a aktivně řeší nastalé situace. Oproti

¹⁰ Přednostně musí být sledována smysluplnost (účelnost) nasazování senzorů, kamer a dalších obdobných prvků. Nasazování značného množství prvků, které se stávají zdroji dat a následné hledání nástrojů pro zvládání jejich zpracování je sice současným trendem (platí obecně, nejen pro železniční dopravu), nelze je však z dlouhodobého hlediska považovat za udržitelné, v konečném důsledku povede ke snižování spolehlivosti železničního systému.

stávajícím integračním a vizualizačním nadstavbovým systémům přináší dvě nové základní vlastnosti, a to informační management a situační analýzu.



OBR. 40 – OBECNÉ SCHÉMA NADSTAVBY DDTS ŽDC

Množství informací, které denně proudí z technologických systémů SŽDC je obrovské. Informace přicházejí z různých technologií a technologických celků – kamery, zabezpečovací zařízení, řízení přístupu, automatické rozpoznávání registračních značek, RFID, GIS, HVAC, počasí, alarmy, požární systémy, IP systémy a další. Důležité je pak jak s těmito daty dále pracovat. Při řešení nastalé situace je klíčové dostat relevantní informace zainteresovaným lidem ve správný čas tak, aby byli schopni efektivně reagovat. V oblasti bezpečnosti a provozu může být každý okamžik klíčový pro ochranu lidí, majetku a obchodní činnosti. Proto je důležité mít k dispozici znalosti, být připraven a mít přehled o situaci.

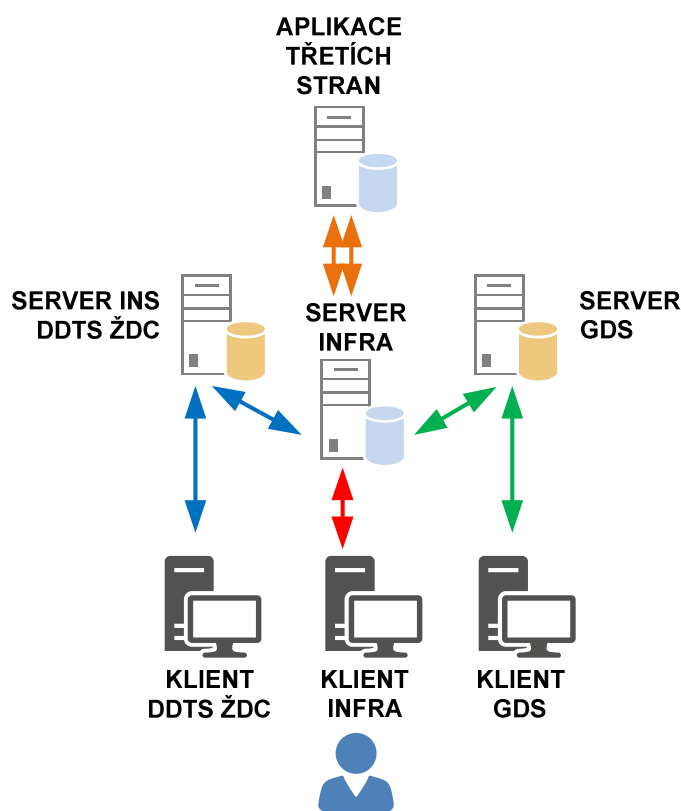
V současné době existuje v oblasti správy a údržby železniční infrastruktury množství informačních systémů. Inteligentní dopravní systémy nabízí široké spektrum aplikací pro správce infrastruktury, dopravce i uživatele dopravy. Realizací projektu „**Vytvoření integrovaného technologického systému správce železniční infrastruktury**“ bude umožněno správci železniční infrastruktury optimálně alokovat prostředky a kapacity s cílem zvýšit bezpečnost a plynulost prací na železniční síti, zajistit optimální parametry provozuschopnosti pro využívání jednotlivých částí infrastruktury s přihlédnutím ke stávajícím i výhledovým potřebám provozu. Vazba této připravované aplikace na provoz usnadní a zefektivní plánování vlakové dopravy, výlukovou činnost a včasnou indikaci a omezení nepravidelných a havarijních zákroků na infrastruktuře, což umožní celkové snížení zpoždění a nepravidelností v železničním provozu.

Současně budou vytvořeny podmínky a rozhraní pro využití aplikací založených na družicových systémech (GPS, EGNOS, Galileo) pro monitorování bezpečnosti železniční dopravní infrastruktury, pro předvídání vlivu povětrnostní situace, sesuvů a poklesů půdy, záplav a povodní apod.

10.2 Základní topologie systému

Operátorský systém umožní evidenci poruch a stavů zařízení, podporu jejich řešení a reporting provedených oprav. Architektura je založena na aplikaci Klient/Server a musí být postavena na výkonných serverech, což umožňuje implementaci široké škály pracovišť. Na následujícím Obr. 41 je vyobrazena architektura systému.

Systém bude pomáhat organizaci/objednateli snížit bezpečnostní a provozní rizika tím, že zachycuje, analyzuje a koreluje smysluplné informace z mnoha zdrojů a poskytují komplexní situační přehled. Zabezpečuje celý bezpečnostní životní cyklus – vylepšuje celkový přehled, řízení, reakce, plánování a prevenci. Software je navržen a vytvořen tak, aby umožnil bezproblémovou a rychlou integraci se všemi řídicími systémy, senzory a dalšími zařízeními.



OBR. 41 – ZÁKLADNÍ ARCHITEKTURA SYSTÉMU

Mezi klíčové vlastnosti systémů musí patřit:

- **Otevřená platforma** – poskytuje snadnou integraci různých systémů a Zařízení, aby bylo možné zajistit obousměrnou komunikaci systému. Definované rozhraní bude navrženo zhotovitelem a odsouhlaseno objednatelem.
- **Normalizace dat** – poskytuje možnost transformovat agregovaná data Z různých zdrojů do jednotného tvaru tak, aby byla možnost data vzájemně významově porovnávat (korelovat) a stanovit jejich prioritu. Datová sktruktura bude navržena zhotovitelem a odsouhlasena objednatelem.

- **Korelace** – poskytuje schopnost porovnávat události a alarmy z více systémů a integrovat je společně s dalšími informacemi, jako jsou čas, geografické údaje, údaje z privátních databází aj. Na základě těchto výsledků se automaticky identifikuje vzniklá situace, která se dynamicky aktualizuje podle skutečného vývoje.
- **Dynamické mapování na zařízení** – možnost zobrazení situací a alarmů relevantním osobám na fixních i mobilních zařízeních. Ukazuje, co se děje v reálném čase v rámci dané situace, nebo globálně napříč všemi situacemi.
- **Prohlížeč** – Webové rozhraní: Umožňuje snadný přístup a spolupráci mezi pracovníky a organizacemi a podporuje koncová mobilní zařízení (systém Android) stejně jako terminály v dispečerském centru.
- **Scénáře** – představují standardní operační postupy provozovatele, spolu s informacemi, nástroji v rámci jediného uživatelského rozhraní. SW má sadu snadno použitelných vizuálních nástrojů pro generování politik a scénářů, které jsou automaticky importovány do systému pro použití při identifikaci a řešení situací.
- **Reporting** – Shromažďuje všechny informace (alarmy, audio), přijatá opatření a výsledky do jedné složky přístupné operátorům. Umožňuje zpětnou analýzu situace a podklady pro zlepšení procesů či školení.

10.2.1 STRUKTURA SYSTÉMU

Spodní úroveň „technologie, systémy“ zobrazuje vstupy, které přicházejí do systému DDTS ŽDC a Globálního diagnostického systému (GDS). Těmi mohou být události z různých technologií, senzorů, tak i informace vkládaných obsluhou. Vyšší vrstva „Korelační jádro“ tyto vstupní informace koreluje mezi sebou, informace lokalizuje a ze všech vstupů vytváří relevantní informaci, která se pak zobrazí na pracovišti dispečera. Zde se provádí „Optimalizace odezvy na situaci“ tak, že s touto informací je pracováno podle předem definovaných postupů, ať již plně automatických, poloautomatických či v kompetencích dispečera. Na situaci je tak relevantně reagováno s minimalizací času odezvy a možnosti vzniku chybné reakce. Po vyřešení vzniklé situace následuje reporting a možnost zpětného prověření průběhu jejího řešení tak, aby se mohl celý proces dále optimalizovat a zdokonalovat.

Vlastní realizace SW integrovaného systému správce železniční infrastruktury se předpokládá postupně v také dalších odvětvích SŽDC jako např. traťové hospodářství. Současně budou vytvořeny podmínky a rozhraní pro využití aplikací založených na družicových systémech (GPS, EGNOS, Galileo) pro monitorování bezpečnosti železniční dopravní infrastruktury, pro předvídání vlivu povětrnostní situace, sesuvů a poklesů půdy, záplav a povodní apod.

10.3 Hlavní zdroje dat

Hlavními zdroji dat vhodnými pro analýzu a vyhodnocování situace jsou:

- Hovorová technologie – dotykové terminály, telefonie, MRS, TRS, GSM-R;
- Video – kamerové systémy;
- Obrazovky – obslužná pracoviště;

- Data dálkové diagnostiky PZTS;
- Zabezpečovací zařízení;
- Zařízení pro požární signalizaci (EPS apod.);
- Systémy MaR;
- Systémy technologií budov (výtahy, klimatizace, topení);
- Informace o poloze;
- Systémy technické ochrany;
- Senzory;
- IT systémy;
- Informace o počasí;
- Mapové podklady;
- Jízdní řády;
- Atd.

10.4 Možnosti využití dat z technologických systémů

MIMOŘÁDNÉ UDÁLOSTI (nehody na přejezdech, pády do kolejíště, srážka vlaků, požár ve stanici)

- Možnost predikce incidentů;
- Výrazné zkrácení doby získání přehledu o situaci;
- Řízení situace;
- Zkrácení doby přerušení provozu a tím i nákladů s nimi spojených;
- Možnost zlepšování pracovních postupů, simulace a nacvičení mimořádné události;
- Ochrana cestujících.

PORUCHY INFRASTRUKTURY

- Výrazné zkrácení doby získání přehledu o situaci;
- Predikce poruch;
- Možnost monitoringu běžné údržby;
- Snížení nákladů na údržbu a na případné zpoždění, které porucha způsobí;

OBJEKTOVÁ BEZPEČNOST – ZABEZPEČENÍ DRÁŽNÍCH OBJEKTŮ, VZDÁLENÝ MONITORING

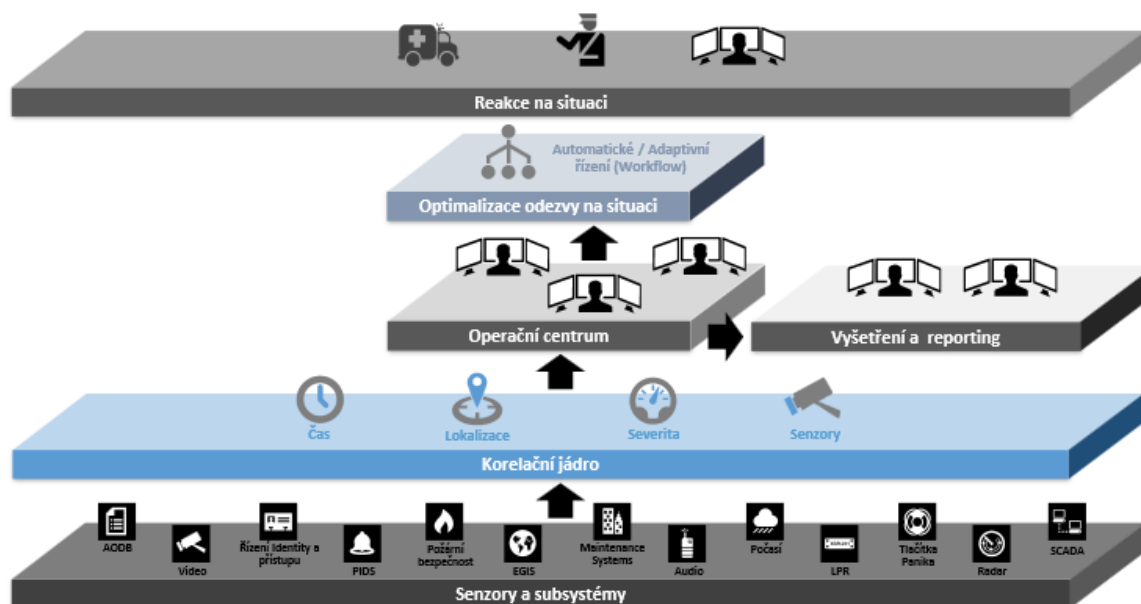
- Snížení počtu krádeží, vandalismu;
- Dálkové zamykání/odemykání čekáren a jiných prostor;
- Ochrana perimetru;
- Správa objektů pod jedním pracovištěm.

DYNAMICKÉ HODNOCENÍ ODOLNOSTI INFRASTRUKTURY

- Predikce proti krádežím, zničení majetku a omezení poskytovaných služeb, tedy i nákladů;
- Zvýšení bezpečnosti – eliminaci rizik plynoucích z hrozeb na co nejnižší úroveň.

10.5 Informační management

Z pohledu koncepce železnice v České republice a možných bezpečnostních situací, které je a bude nutné řešit, je využití sofistikovaného systému informačního managementu provozní bezpečnosti značným přínosem. V rámci komplexnosti řešení je možné systém využít na řešení **Mimořádných událostí**, predikce a odstraňování **Poruch infrastruktury**, zabezpečení jednotlivých **Objektů** ve správě železnice a **Hodnocení odolnosti infrastruktury** ve smyslu kritické infrastruktury.



OBR. 42 – STRUKTURA INFORMAČNÍHO MANAGEMENTU

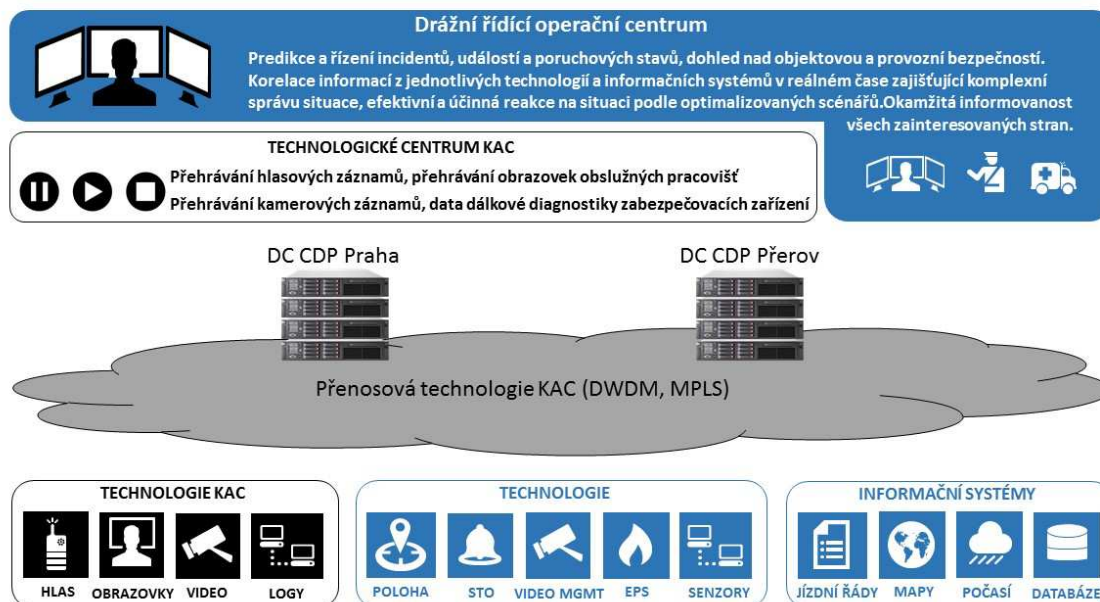
Spodní vrstva Obr. 42 zobrazuje vstupy, které přicházejí do systému. Těmi mohou být události z různých technologií, senzorů, tak i informace vkládaných obsluhou. Vrstva „Korelační jádro“ tyto vstupní informace koreluje mezi sebou, informace lokalizuje a ze všech vstupů vytváří relevantní informaci, která se pak zobrazí v operačním centru. Zde je s touto informací pracováno podle předem definovaných postupů, ať již plně automatických, poloautomatických či v kompetencích operátora. Na situaci je tak relevantně reagováno s minimalizací času odezvy a možnosti vzniku chybné reakce. Po vyřešení vzniklé situace následuje reporting a možnost zpětného prověření průběhu jejího řešení tak, aby se mohl celý proces dále optimalizovat a zdokonalovat.

10.6 Začlenění do systému KAC

Kontrolně Analytické Centrum KAC nyní řeší záznam dat hovorové komunikace, záznam kamer sledování provozu, záznam obrazovek obslužných pracovišť a logování dat dálkové diagnostiky a zabezpečovacího zařízení.

Rozšířením funkcí KAC o principy a možnosti informačního managementu umožní získat plnohodnotné drážní řídicí operační centrum, které bude zajišťovat:

- Predikci a řízení incidentů, událostí a poruchových stavů;
- Dohled nad objektovou a provozní bezpečností;
- Korelaci informací z jednotlivých technologií a informačních systémů v reálném čase zajišťující komplexní správu situace;
- Efektivní a účinné reakce na situaci podle optimalizovaných scénářů;
- Okamžitou informovanost všech zainteresovaných stran.



OBR. 43 – ZAČLENĚNÍ DO SYSTÉMU KAC

10.7 Přínosy řešení

Informační management provozní bezpečnosti nabízí železnici kompletní správu událostí. Ať už se jedná o mimořádné události, poruchy infrastruktury, objektovou bezpečnost, hodnocení odolnosti infrastruktury nebo rutinní postupy, reporty a hlášení, včetně distribuce různým složkám. Systém IMPROB je připraven tyto činnosti v různých rolích zastávat.

Z hlediska **mimořádných událostí** tento systém poskytuje výrazné zkrácení doby získání přehledu o situaci a umožňuje automatické nebo poloautomatické cílené reakce na situaci.

Z hlediska **poruch** umožňuje systém do jisté míry predikovat poruchy, a tak předcházet výpadku důležité technologie, která by způsobila škody většího rozsahu. I při řešení běžných poruch nebo vykonávání rutinních oprav či revizí, dokáže systém výrazně snížit dobu tohoto řešení.

Zapojení tohoto informačního managementu do **objektové bezpečnosti** vede ke snížení počtu krádeží a vandalismu v železničních objektech a zároveň umožňuje automatizaci různých rutinních činností, které se dosud musí vykonávat lokálně.

V případě hodnocení **odolnosti infrastruktury** umožňuje upozornit správu infrastruktury na slabá místa, která v budoucnu mohou způsobit újmu nebo mohou znamenat finanční náklady.

Výše zmiňované aspekty se výrazně odráží v úspoře finančních prostředků. Dalším přínosem je pohodlné a jednotné pracoviště pro obsluhu, včasné vyrozumění všech zúčastněných při řešení mimořádných událostí nebo poruch, stanovení jasných postupů při práci pod stresem a komplexní reporting o událostech.

11 KAMEROVÉ SYSTÉMY

11.1 Kamerové systémy v železničních stanicích a zastávkách

11.1.1 STÁVAJÍCÍ STAV

Stávající kamerové systémy v síti železničních drah SŽDC byly v převážné míře vybudovány nezávisle na sobě jen v některých železničních stanicích. Tyto systémy jsou zpravidla analogové. Sloužily a slouží jen pro lokální obsluhu (výpravčího nebo operátora železniční stanice, obsluhu staveb apod.), měly a mají za úkol sledovat jen vybraná a exponovaná místa v kolejišti, v podchodech pro cestující, na nástupištích a ve vestibulech. Takový kamerový systém byl zpravidla sestaven z následujících komponent: videoústředna (uniplexer, duplexer...) s ovládací soupravou, sada několika monitorů CRT (v závislosti na počtu kamer), kabelová vedení (zpravidla koaxiální kabely, kroucené linky v metalických kabelech apod.), linkové přenosové zařízení, kamery, videorekorder. Všechny komponenty kamerového systému musely být napájeny ze stejného zdroje z důvodu nutné synchronizace obrazu. Zpracování obrazu je zajištěno zpravidla dle standardu PAL.

Výjimku představují pouze některé tratě, které jsou řízeny centrálně z lokálních dispečerských pracovišť anebo z CDP Praha a CDP Přerov. Na těchto tratích byly zejména v posledních letech v rámci staveb typu „Modernizace“, „Elektrizace“, Revitalizace“ a zejména „DOZ“ (dálkové ovládání zabezpečovacího zařízení) vybudovány digitální kamerové systémy, pracující s protokolem TCP/IP a jednotlivá zařízení takového kamerového systému mají své nezaměnitelné IP adresy. Zpravidla jsou takové kamerové systémy sestaveny z následujících zařízení: videosever, záznamové zařízení nebo datové uložení, monitory LCD, zařízení pro přenos videa, dat a hlasu po optických vláknech, optické kabely, kamery. Přenos videa, dat a hlasu je zpravidla zajišťován po optických vláknech s ohledem na minimalizaci nežádoucích rušivých vlivů od zdrojů elektromagnetického vlnění (napájecí trakce, vedení VVN, apod.).

11.1.2 NAVRHOVANÝ STAV

V rámci další výstavby kamerových systémů v železničních stanicích v jednotlivých připravovaných stavbách doporučuje tato Studie pokračovat v budování IP kamerových systémů v souladu se „Základními technickými požadavky na kamerové systémy“ a to bezvýhradně ve všech železničních stanicích. Účelem těchto systémů je jednoznačně sledování nástupištních hran z důvodu bezpečnosti dopravy. Předmětem této Studie není rekapitulace podrobného znění uvedených ZTP.

Vzhledem ke skutečnosti, že předmětné kamerové systémy byly doposud budovány především v železničních stanicích, doporučuje tato Studie budovat v přiměřeném rozsahu a se stejnými komponentami dle uvedených ZTP tyto kamerové systémy i v železničních zastávkách s větší frekvencí cestujících. V rámci budování přenosových cest jsou vytvářeny postupně i v těchto železničních zastávkách podmínky pro plnohodnotné zapojení kamerových systémů zastávek do videomonitoringu dopravní cesty SŽDC. V případě, že nebudou kamerové systémy na zastávkách, ale i na přejezdech a v dalších exponovaných lokalitách budovány přímo v rámci konkrétních

staveb, bude žádoucí připravit alespoň odpovídající podmínky pro jejich bezproblémové doplnění v budoucnu (tedy např. výpichy příslušných optických vláken případně alespoň rezervy na sdělovacích kabelech pro budoucí výpich, rezervace místa v technologických skříních, resp. objektech, rezerva v napájecích rozvaděcích apod.).

Obecně musí mít kamery možnost nastavit rozdílnou rozlišovací schopnost při neměnném obraze a při dynamické změně obrazu nebo v nastavené oblasti zájmu sledování, aby nedocházelo k vyčerpání zdánlivě velkého přenosového pásma.

11.2 Traťové kamerové systémy (kamerové systémy na přejezdech)

Pod pojmem traťové kamerové systémy se rozumí pro účely této Studie zejména kamerové systémy na přejezdech, i když takové systémy lze budovat i na jiných exponovaných či jiným způsobem ohrožených místech železničních tratí (např. tam, kde je železniční trať vedena pod skalním masivem, či ve skalnatém zářezu apod.). Velmi dobře představitelná je i přechodná (časově omezená) možnost nasazení obdobných kamerových systémů, např. při náročnějších stavebních činnostech (opravy silničních nadjezdů, železničních mostů apod.) při současném zachování železničního provozu na exponovaných tratích neumožňujících delší výluky.

Ve smyslu technické specifikace SŽDC TS 1/2014-SZ Vydání I. (účinnost od 16.4.2014) jsou kamerové systémy na přejezdech určeny zejména pro dokumentování nehodových událostí na železničních přejezdech z pohledu ochrany osob a majetku. Kamerový systém zajistí uložení záznamu situace na přejezdu, pořízeného v době výstrahy, a to se stanoveným časovým přesahem před začátkem této doby a po jejím skončení, zpravidla 30 s. Způsob ukládání záznamu (kontinuální, resp. samplovaný versus záznam mimořádné události) z kamer bude předmětem případného předpisu SŽDC. Přenosová cesta k příslušnému úložišti dat musí být dimenzována na obě varianty.

S využitím analýzy obrazu (tj. prostřednictvím analytického SW záznamového zařízení nebo kamer) budou zaznamenány i další události ve sledovaném prostoru přejezdu mimo dobu výstrahy, např. setrvání osoby nebo vozidla po dobu delší než stanovenou, odložení předmětu atd.

Zpracování osobních údajů podle těchto technických specifikací musí být v souladu s právními předpisy upravujícími ochranu osobních údajů, včetně Směrnice SŽDC č. 97 o ochraně osobních údajů státní organizace Správa železniční dopravní cesty „...a **musí být realizováno i s přihlédnutím k NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).**“

Jedná se o strategický předpis EU v předmětné oblasti, jehož zavedení do podmínek SŽDC bude muset být provedeno.

Záznamy budou uloženy jen po dobu nezbytně nutnou k účelu jejich zpracování. Protože účelem zpracování osobních údajů v případě kamerových systémů na PZS je především ochrana majetku, rozumí se dle stanoviska ÚOOÚ nezbytnou dobou lhůta maximálně pěti kalendářních dnů, u SŽDC

pak 7 dnů (168 hodin). Toto omezení na 7 dnů znamená, že informace z takového systému musí být kontinuálně předávány příslušným pracovníkům, nestačí jejich pravidelné měsíční stahování při kontrole technologie přejezdu. To klade větší požadavky na konektivitu daného systému a kapacitu přenosových cest.

11.2.1 STÁVAJÍCÍ STAV

Traťové kamerové systémy se v doposud realizovaných stavbách SŽDC (stavby typu „Modernizace“, „Elektrizace“ či „Revitalizace“) navrhovaly spíše výjimečně i s ohledem na menší četnost mimořádných událostí na přejezdech, která si budování takových kamerových systémů nevynucovala a rovněž s ohledem na doposud budovanou přenosovou infrastrukturu s nedostatečnou šířkou přenosového pásma pro náročnější přenosy od kamer u jednotlivých přejezdů k místům koncentrace a jejich částečnému zpracování (analýza, případně záznam) těchto videosignálů a jejich případnému transferu do vyšších úrovní přenosové sítě k přenosu na nadřazená pracoviště.

11.2.2 NAVRHOVANÝ STAV

Vzhledem ke stále narůstajícímu počtu mimořádných událostí (většinou s fatálními následky) na chráněných i nechráněných železničních přejezdech a rovněž s ohledem na fatální události při rekonstrukci umělých staveb nad žel. tratí (viz např. ŽST Studénka) se jednoznačně doporučuje traťový kamerový systém v rámci připravovaných staveb navrhovat a realizovat. U připravovaných staveb typu VRT se nepředpokládá nutnost instalace takového kamerového systému (nebudou budovány přejezdy). Požadavek na realizaci takového systému se musí uplatnit již v zadávacích podmínkách připravovaných staveb.

Je však nutno mít na zřeteli i skutečnost, že budování traťových kamerových systémů neznamena pouze jejich zřízení, ale následně je nutno zajišťovat také jejich pravidelnou údržbu. Nasazení těchto systémů proto musí být pečlivě zdůvodněno, rozhodně nelze uvažovat o zcela běžném a plošném zřizování.

Technické aspekty budování takových systémů poměrně jednoznačně vymezuje a specifikuje výše uvedená technická specifikace SŽDC TS 1/2014-SZ Vydání I. (základní prvky kamerových systémů, požadované umístění a základní vlastnosti kamerového systému, připojení a napájení kamerových systémů, požadavky na jednotlivé komponenty...). Není účelem této Studie rekapitulovat podrobně obsah uvedené TS.

11.3 Kamerové systémy a Kontrolně analytické centrum řízení dopravy

V roce 2015 a první polovině roku 2016 došlo k vybudování první etapy aplikace KAC. Tato první etapa zahrnovala vybudování a zprovoznění vlastní technologie KAC, začlenění a integraci prostředků pro snímání a záznam dat a doplnění dalších prostředků, které uvedený záměr vyžadoval.

KAC poskytuje funkcionality komplexní rekonstrukce situace vztažné k řízení a organizování drážního provozu ze záznamu. Situace je rekonstruována časově synchronní reprodukcí záznamů

hlasové komunikace, video záznamů, obrazovek monitorů a logů činnosti zabezpečovacích zařízení z vybrané lokality, resp. uzlu řízení provozu. Dále je podporována funkce přenosu aktuální reálné situace (monitoringu) z vybrané lokality do nadřízeného centra, a to s minimálním časovým zpožděním.

Do systému KAC jsou redundantně přenášeny informace z obou centrálních dispečerských pracovišť (CDP) v Praze a Přerově a řízených oblastí zaústěných do těchto CDP. Tyto dvě lokality jsou navzájem plně zálohovány. Do systému KAC jsou přenášeny informace ze stávajících (i budoucích) regionálních dispečerských pracovišť (RDP).

Jednou z významných komponent systému KAC jsou i „Systémy pro video monitoring objektů souvisejících s řízením dopravy“.

Pro zabezpečení přenosu předpokládaného masivního objemu dat u SŽDC byly v rámci stavby KAC ŘD vybudovány na síti stávajících optických kabelů SŽDC, s.o., resp. ČD-Telematika, a.s.:

- přenosový systém DWDM
- přístupové routery MPLS
- Core routery MPLS
- agregační (sběrná) vrstva přenosových bodů MPLS, ve kterých je/bude prováděn sběr příspěvkových signálů systému KAC z navazujících tratí.

Výše uvedené vrstvy přenosové sítě SŽDC umožní společně s výkonným a kapacitním přenosovým zařízením nižších úrovní (úroveň jednotlivých tratí) postupné nasazování výše uvedených kamerových systémů pro přenos videosignálů od jednotlivých kamer k agregačním bodům na jednotlivých tratích, kde dojde k sekundárnímu zpracování těchto videosignálů (SW analýza, prvotní záznam). Dále přenosová síť umožní přenos upravených (analyzovaných a filtrovaných) i neupravených (kompletních) dat z kamerových systémů do regionálních agregačních bodů a jejich prostřednictvím pak dále finálně do systému KAC ŘD (kompletní data) a na videodispečinky SŽDC (analyzovaná a filtrovaná data).

Způsob lokálního ukládání záznamu z kamer zůstane zachován. Do systému KAC budou přenášeny záznamy z kamer, které budou ukládány v CDP (tj. v KAC) pouze 24 hodin a poté budou opět přemazány. V lokálním úložišti zůstane zachována stávající délka záznamu, případně může být prodloužena na dobu respektující platné zákony ČR, tj. maximálně 168 hodin. K lokálnímu úložišti kamerového systému bude možné přistoupit přes systém KAC v rámci přidělených přístupových práv.

Vzhledem k tomu, že za nakládání s pořízenými daty odpovídá správce zařízení, je nutno nalézt technická opatření, aby byla jednoznačně prokazatelná zodpovědnost při poskytování dat jiným složkám SŽDC v rámci projektů KAC a CDP.

11.4 Systém automatické výstrahy ohrožení provozu (SAVOP)

11.4.1 STÁVAJÍCÍ STAV

V rámci SŽDC jsou k dnešnímu dni nainstalovány stovky kamer, které monitorují kolejiště, nástupištní hrany a další prostory železniční stanic, souvisejících přímo s bezpečností dopravní cesty. Přenosy obrazu z těchto kamer jsou ve většině případů přenášeny na lokální video pracoviště, situované zpravidla u některého z pracovníků, jehož hlavní činnost souvisí s řízením provozu. Tento zaměstnanec však nemůže nad rámec svých běžných pracovních povinností sledovat a vyhodnocovat v reálném čase videomonitoring, což může v současné době dle složitosti železniční stanice představovat 4 - 20 přenosů z kamer. Kamerový systém je pro pracovníky přímo řídicí provoz pouze pomocným prostředkem, neboť se jedná o únavnou činnost s velkou pravděpodobností přehlédnutí mimořádné události, způsobeného negativním vlivem lidského faktoru, a to i v případě, že by byl pracovník vyčleněn pouze pro takovou činnost. Kamerový systém musí umět zobrazit video na požádání, případně automaticky zobrazovat příslušný videosignál dle aktuální obsluhy zabezpečovacího zařízení. V návaznosti na budování traťových kamerových systémů náročnost vyhodnocení videomonitoringu ještě dále vzroste na zcela neúnosnou míru. Rovněž v souvislosti s narůstající traťovou rychlostí (modernizace tratí, VRT...) se zkracuje pod kritickou mez reakční doba nutná pro provedení účinného zásahu pro zamezení mimořádné události s fatálními důsledky. Záznamy z kamer jsou zpravidla ukládány na lokální krátkodobá úložiště a po cca 5 - 7 dnech (dle zákona o Ochráně osobních údajů a směrnic SŽDC) jsou přemazány novými záznamy, případně jsou nebo budou přenášeny do systému KAC ŘD (viz výše).

Přes relativně velké množství kamer nasazených v posledních letech v rámci modernizačních, resp. optimalizačních staveb, jsou tyto kamery využívány především pro dokazování a dokládání incidentů a nikoli pro reálné zvýšení bezpečnosti dopravní cesty.

V současné době je možno z výstupů kamerových systémů reálně použít pro odvrácení nehody pouze vyhodnocení úvinnutí vozidla na přejezdu v době, kdy není výstraha (resp. v době výstrahy pro snížení následků nehody). Tento alarm ale musí být indikován u pracovníka, který aktuálně řídí dopravu v daném úseku a jako jediný je oprávněn použít STOP v traťovém rádiovém systému. Případná možnost řešení případu úvinnutí vozidla při uzavření přejezdu znamená podstatné zásahy do zabezpečovacího zařízení, v současné době se ověřuje a není tedy předmětem této studie.

11.4.2 NAVRHOVANÝ STAV

Vzhledem k výše uvedenému je jednoznačným požadavkem vybudování efektivního, tj. zcela automatizovaného systému videomonitoringu železniční dopravní cesty. Většina kamerových systémů instalovaných u SŽDC již dnes umožňuje další zpracování obrazu a automatické předvyhodnocení vybraných krizových dějů přímo ohrožujících bezpečnost železničního provozu a cestující veřejnosti. Navíc současné algoritmy pro zpracování obrazu nejsou příliš náročné na kvalitu rozlišení a ani na počet snímků. Podobně výpočetní náročnost algoritmů není náročná jako dříve a je tedy možné zpracovávat na jednom systému i více obrazů současně. Automatické

vyhodnocování událostí v obraze je dnes již běžná praxe s danou úspěšností s danou četností falešných poplachů. Využití takového systému pak může významně zvýšit aktivní bezpečnost tím, že upozorní na definované události lokální obsluhu, případně obsluhu regionálního, resp. centrálních videodispečinků (ideálně na CDP Praha a CDP Přerov), která vyhodnotí, zda se jedná o reálné ohrožení bezpečnosti a na základě toho může aktivně zasáhnout. Vybudování všech úrovní videodispečinků vč. nezbytného HW a SW vybavení tato Studie jednoznačně doporučuje.

Místo toho, aby příslušný pracovník na všech úrovních videomonitoringu sledoval nepřetržitě či namátkou na všech nebo jen některých kamerách, zda např. uvízlo auto na přejezdu apod., dostane včasnou informaci, že analytika tuto možnost vyhodnotila a nabídne mu zvětšený obraz z kamery, která tuto událost zachytila. Bude tak mít relativně dostatek času k efektivnímu zásahu např. v součinnosti se systémem GSM-R STOP. Na přítomnost osoby v kolejišti není možno přiměřeně reagovat, navíc takových alarmů by bylo mnoho. Ochránit bezpečnost osob např. na úrovňových přechodech v ŽST je nutno jinými prostředky.

11.5 Kamerové systémy a funkcionality GSM-R STOP, resp. generální STOP TRS

Na koridorových tratích je k dnešnímu dni vybudován rádiový systém GSM-R. Tento systém se dále rozšiřuje a postupně nahradí i na dalších, nekoridorových tratích stávající traťový rádiový systém (TRS). TRS je vybaven od počátku nasazení tohoto systému funkcí „generální stop“, která umožní zastavit veškerý železniční provoz v dané oblasti, případně i konkrétní vlakovou soupravu. Pro zajištění účinnosti uvedené funkce je však nutno splnit řadu podmínek, její zaúčinkování není garantováno (ve smyslu přístupu uvažovaného v případě zabezpečovacího zařízení) nelze ji proto v žádném případě považovat za náhradu vlakového zabezpečovacího zařízení.

V roce 2017 bude implementována v síti GSM-R SŽDC funkcionality GSM-R STOP, umožňující podobně jako rádiový systém TRS, dálkově zastavit vlak pomocí nadstavby rádiového zařízení. Oprávněno k podobnému zásahu je pouze plně vybavené pracoviště, tedy pracoviště vybavené tzv. dotykovým terminálem pro funkci výpravčí, traťový (úsekový, dirigující dispečer) nikoliv provozní dispečer nebo dispečer ŽDC. Ve spojení se stávajícími i nově budovanými kamerovými systémy v železničních stanicích, zastávkách, ale i traťovými kamerovými systémy představuje tato funkcionality velmi účinný nástroj pro zvýšení rychlosti adekvátní reakce příslušného zaměstnance.

11.6 Videodispečinky (CDP)

Vzhledem k výše uvedenému navrhuje tato Studie budování komplexního systému videodispečinků. První úroveň vytvoří lokální pracoviště, a to zejména na tratích bez dálkového dispečerského řízení. Tato pracoviště základní analýzy obrazu budou dislokována ve vybraných železničních stanicích. Druhou úroveň vytvoří tzv. regionální videodispečinky, pod které bude spadat vždy příslušná oblast s železničními tratěmi nezapojenými do systému dálkově dispečersky řízených tratí. Nejvyšší úroveň by vytvořily dva centrální videodispečinky (doporučuje se CDP Praha a CDP Přerov). K centrálním videodispečinkům budou přímo připojeny železniční tratě dálkově dispečersky řízené z těchto CDP.

Ve všech úrovních by byla videodispečerská pracoviště vybavena kromě nezbytných HW komponent kamerových systémů a souvisejícího SW pro analýzu obrazu i plnohodnotnými dotykovými terminály, funkcionality GSM-R STOP však bude příslušet pouze zaměstnancům řídícím provoz.

Současně bude nutno zajistit dostatečnou kapacitu datových úložišť na jednotlivých videodispečincích a zejména v centrech KAC (CDP Praha, CDP Přerov), pro spolehlivé ukládání kompletních dat z kamerových systémů v příslušné oblasti, resp. rámci celé SŽDC.

U tratí nezapojených do systému DOZ (tedy lokálně obsluhovaných) vytvoří nejjednodušší 1. úroveň videomonitoringu samotná inteligentní kamera, která je schopna prvotní analýzy obrazu (na principu nastavení jednotlivých zón alarmu v obraze) a dá potřebný impuls k vynucenému sledování obrazu této kamery na monitoru pracovníka pověřeného řízením provozu. Nutno podotknout, že ne všechny stávající kamery u SŽDC vykazují takovou funkcionality, u připravovaných investičních akcí by ale nasazení takových inteligentních kamer mělo být striktně vyžadováno. U větších železničních stanic, či stanic, ve kterých se navíc soustřeďuje i videosignál kamer ze sousedních menších železničních stanic, případně zastávek (a v budoucnu i z kamer traťového kamerového systému) již bude nutno provádět současnou analýzu obrazu všech připojených kamer prostřednictvím sofistikovaného HW a SW, a to v reálném čase. Obraz kamery (případně více kamer) zabírající mimořádnou událost se tak opět vynuceně dostane s příslušným alarmem (např. akustickým) na monitor pracovníka pověřeného řízením provozu, vybaveného potřebnými HW prostředky pro efektivní zásah (rozhlasové zařízení, generální STOP TRS, GSM-R STOP...).

Jiná situace bude u tratí zapojených nebo postupně zapojovaných do systému DOZ, tedy tratí řízených dálkově. Ty jsou podle své důležitosti připojovány buď na centrální dispečerská pracoviště (CDP Praha, CDP Přerov) nebo k regionálním dispečerským pracovištím (RDP). I zde bude nejdůležitějším prvotním článkem videomonitoringu inteligentní kamera se schopností prvotní analýzy obrazu, potřebný impuls k vynucenému sledování obrazu této kamery bude směřován jednak na monitor případné lokální obsluhy (bude-li doprava z nějakého důvodu dočasně obsazena) a současně do místa zpracování a souběžné analýzy videosignálů všech připojených kamer prostřednictvím sofistikovaného HW a SW, a to opět v reálném čase. Tato analytická pracoviště musí být zcela automatizovaná a mohou být dislokována ve vhodných agregačních bodech (dle konkrétní topologie železničních tratí v dané oblasti), které se mohou případně kryt i s pracovištěm RDP. Po příslušné analýze videosignálů bude pak obraz mimořádné události s příslušným alarmem vynuceně zobrazen na monitoru pracovníka videodispečinku RDP, resp. pracovníka pověřeného řízením provozu (dispečera), vybaveného opět potřebnými HW prostředky pro efektivní zásah.

Obdobně bude řešena distribuce videosignálu z kamer instalovaných na železničních tratích, zapojených k CDP Praha, resp. CDP Přerov. Obraz z inteligentní kamery s přenosem na lokální pracoviště, paralelně na místo agregace a souběžné analýzy videosignálu všech kamer v připojené oblasti a po vyhodnocení odeslání vybraného obrazu kamery/kamer, sledujících mimořádnou událost, na videodispečera CDP.

Je zřejmé, že takto složitý proces nemůže a nebude probíhat zcela v reálném čase, neboť k dopravnímu zpoždění mezi kamerou a koncovým článkem celého řetězce distribuce videosignálu bude docházet vlivem přenosové rychlosti budovaných přenosových cest a časem nutným pro samotnou analýzu videosignálů. Vhodnou topologií celého řetězce lze však zpoždění minimalizovat na přijatelnou míru, která neohrozí efektivní zásah pověřených pracovníků v případě mimořádné události.

Rychlost zásahu pracovníků řídících provoz bude záviset na rychlosti předání informací z kamerového systému, přenos obrazové informace prostřednictvím přenosové sítě SŽDC však nebude mít podstatný vliv na rychlost a efektivitu zásahu. Ty budou závislé především na samotném vyhodnocení situace a aktivním zásahu pracovníků řídících provoz (např. vybavení funkce GSM-R STOP), obojí je pochopitelně zatíženo lidským, tedy subjektivním faktorem.

Nutno zdůraznit, že výše popsaný systém, kdy se k pověřeným pracovníkům přenáší pouze obraz z vybraných kamer, nesouvisí nijak se systémem ukládání kompletní obrazové informace (ať už lokálně nebo do systému KAC).

Agregační body, resp. RDP jsou dle projektu KAC dislokovány v následujících lokalitách:

Česká Lípa ATÚ, Liberec ATÚ, Stará Paka VB, Hradec Králové VB (ATÚ), Týniště nad Orlicí ATÚ, Jihlava VB (ATÚ), Havlíčkův Brod ATÚ, Břeclav ÚS, Šumperk VB, Valašské Meziříčí ATÚ, Český Těšín DB, Staré Město u Uherského Hradiště ATÚ, Mladá Boleslav VB (ATÚ), Nymburk VB, Čerčany TB, Zdice ATÚ, Kralupy, Klatovy VB, Tábor TKB, Chomutov ATÚ, Most VB (ATÚ).

Na závěr je nutno zdůraznit uvážený přístup při budování kamerových systémů, zejména s ohledem na zajištění jejich provozuschopnosti (udržovatelnosti) a dlouhodobé udržitelnosti systému jako celku.

12 INFORMAČNÍ SYSTÉMY PRO INFORMOVÁNÍ CESTUJÍCÍCH

Na úvod této kapitoly je nutno uvést, že současný stav informačního systému pro informování cestujících (ISIC) v železničních stanicích a na zastávkách pro cestující, který slouží cestující veřejnosti, je neuspořádaný a nemá standardizovaný obsah. Z důvodu chybějící příslušné legislativy dochází v posledních letech k roztříštěnosti a nejednotnosti v této oblasti.

V časovém období vznikaly různé druhy orientačního systému tak, jak je tvořili jednotlivé společnosti a organizace. Tyto systémy byly vytvářeny v nejednotném vizuálním stylu, umístění a v různých velikostech. Elektronické informační systémy, které postupně v tomto období vznikaly, mají nejednotný rozsah pro zaznamenávání základních informací, často dochází k neúplnému zobrazení těchto informací, případně jsou často nepřehledné. Přetrvávají nedořešené otázky a problémy, které je nutné popsat, sjednotit a aktualizovat do jednoho nařízení a předpisu. Je nutné unifikovat a zkvalitnit tyto systémy tak, aby orientace cestujících byla v prostorách nástupišť, železničních stanicích, zastávkách a následných společných terminálech zjednodušena a standardizována.

Pro vytvoření zásad projektování a využívání informačního zařízení je nutné provést analýzu stávajícího stavu a následně určit kritéria pro nasazení zařízení. Tato studie jednoznačně podporuje a navrhuje, aby výše uvedený dokument (směrnice, technická specifikace) byl zpracován a na jeho základě došlo k postupnému sjednocování a standardizaci informačního zařízení.

12.1 Standardizace informačního zařízení

Standardizace a sjednocení zobrazovaných informací povede nepřímo i k standardizaci rozměrů informačních systémů, což může v konečném důsledku vést ke snížení výrobních nákladů.

Kromě výše popsané nutnosti definovat rozsah zobrazovaných informací je také nutné zhodnotit vhodnost a dostupnost technologií, díky kterým se požadované informace cestující veřejnosti prezentují. Směr, kterým se budou informační systémy resp. zobrazovací panely technologicky vyvíjet. Jelikož se jedná o velice dlouhodobý časový horizont, musí mít uvažovaná technologie dlouhou morální životnost, podporu a dlouhodobý rozvoj. Dodavatel tedy musí být schopen, dodávat náhradní díly dokonce v horizontu desítek let.

To je hůře splnitelné u komerčních LCD obrazovek. V současné době se ve všech ohledech nejlépe osvědčuje technologie průmyslových LCD panelů (LCD displej podsvětlený LED, složený do požadované matice a velikosti). Jedná se o téměř bezúdržbové a energeticky úsporné řešení. Oproti textovým LED panelům, jsou mnohem lépe čitelné, cenově výhodné, fungují za mnohem vyšších teplot a jsou konstrukčně jednodušší. Nevýhodou je vždy jedna barevná kombinace (např. bílé písmo na modrém pozadí, které již nelze změnit). Pro některé speciální aplikace jsou také vhodné průmyslové LCD obrazovky, různých renomovaných výrobců. Tyto LCD obrazovky ovšem nejsou vhodné do exteriérů, nelze je ani z důvodu nízké morální životnosti doporučit do soustav (matic), (např. velká odjezdové tabule). Jsou vhodné do menších železničních stanic, čekáren pro

cestujících jako samostatné odjezdové tabule v ochranných ventilovaných krytech, nebo jako směrové LCD monitory, doplňkové informační kiosky pro železniční stanice.

Datové spojení jednotlivých prvků systému se do budoucna dá očekávat po optických kabelech, jelikož tyto technologie se stále zlevňují. Tím by se dosáhlo velkých datových přenosů na velké vzdálenosti, bez vlivů okolního rušení.

Moderní informační systém musí být modulární, v budoucnu snadno rozšiřitelný o nové prvky, jako jsou informační panely nebo LCD obrazovky za předpokladu, že nedojde ke ztrátě funkčnosti stávajících prvků. Musí umožnit centrální správu a provádění datových a programových aktualizací ISIC, aby byl zajištěn dlouhodobý rozvoj a podpora.

Nedílnou součástí moderních informačních systémů musí být podpora pro handicapované. Moderní informační panely musí být schopny informaci o spoji nejen zobrazit, ale i přečíst. Případně informovat nevidomé o mimořádných událostech.

Je nutné, aby vývoj informačního systému směřoval neustále k vyššímu uživatelskému komfortu a lepší zpětné vazbě ke koncovému uživateli.

12.2 Centrální správa informačního systému

V současné době jsou jednotlivá nasazení informačních systémů koncipována jako samostatné oddělené jednotky bez možnosti centrální správy a aktualizace. Tento stav sebou přináší narůstající problémy, jak z hlediska časové náročnosti provádění datových a programových aktualizací informačního systému, tak omezené možnosti pro dohled a údržbu všech integrovaných zařízení. Vzhledem ke stále rostoucím požadavkům na spolehlivost informačních systémů pro cestující a na rychlost odezvy na požadavky provozovatele zařízení (SŽDC) je potřebné tento koncept změnit a všechna jednotlivá nasazení propojit do jednotného centrálního systému.

12.2.1 NÁVRH ARCHITEKTURY A DEFINOVÁNÍ KONCEPCE CENTRÁLNÍ SPRÁVY

Navrhovaná architektura využívá již vybudovanou infrastrukturu a stávající informační zařízení v železničních stanicích a zastávkách, ponechává jim jejich existující roli, přebírá roli přípravy, spravování a distribuce dat, administraci včetně potřebného zálohování, podporu uživatelů systému a technickou podporu.

Centrální správa ISIC (tvořená centrálním aplikačním a databázovým serverem) je navržena tak, aby umožnila zapojení již existujících nasazení ISIC, které splňujících základní parametry pro integraci do centrální správy (zejména připojení do sítě SŽDC a novější platformu operačního systému Windows 7 a vyšší verze)¹¹.

¹¹ Součástí studie je rovněž přehled všech nasazení ISIC. V daném přehledu jsou rozlišena nasazení, která jsou již vzhledem k datu jejich realizace technicky i morálně zastaralá, jsou z hlediska možnosti integrace do centrální správy nevyhovující a je doporučena jejich modernizace z hlediska hardware i software.

12.2.2 CENTRÁLNÍ SPRÁVA ISIC

Aplikace Centrální správa ISIC se navrhuje jako internetová aplikace pro dohled, centrální správu a provádění datových a programových aktualizací ISIC.

Aplikace je postavena může být realizována na operačním systému Windows server 2012 R2 a vyšší a SQL serveru verze 2012 a vyšší. Z důvodu předpokládaného objemu ukládaných dat v řádu desítek až stovek gigabajtů je vyžadována verze SQL serveru Standard nebo Enterprise¹².

K provozování na straně uživatele je zapotřebí standardní internetový prohlížeč.

Každý uživatel využívající aplikaci Centrální správa ISIC se musí autorizovat přiděleným přihlašovacím jménem a heslem (případně vyšším zabezpečením viz zákon o kybernetické bezpečnosti). Na základě přihlašovacího jména a hesla je každému uživateli přidělena úroveň přístupových oprávnění. Tato přístupová oprávnění řídí dostupnost jednotlivých níže uvedených funkcí aplikace pro přihlášeného uživatele.

12.2.2.1 Dostupné funkce

Aplikace Centrální správa ISIC se skládá z následujících modulů:

- **Evidence** – v Centrální správě ISIC jsou zaevidována všechna nasazení informačních systémů s popisem jednotlivých prvků daného nasazení a jejich konfiguračních parametrů. Provozovatel informačního systému pro cestující má tedy vždy k dispozici aktuální přehled všech stanic, kde je informační systém nasazen včetně kompletního seznamu všech zaintegrováných zařízení (řídící PC, servery, rozhlasové ústředny, informační tabule, informační monitory). Ke každému zařízení jsou vedeny podrobné údaje včetně dodavatele zařízení, jeho verze a přístupových údajů pro jeho administraci. Dále jsou v evidenci uvedeny IP adresy přidělené jednotlivým zařízením.
- **Datová aktualizací základna** – Centrální správa ISIC zajišťuje správu a automatizovanou distribuci aktualizací datových a programových souborů do jednotlivých lokálních informačních systémů. Systém přehledně informuje, jaká data a kdy byla na lokální informační systém distribuována a jaká ještě čekají na distribuci. Distribuci aktualizací programových komponent lokálních informačních systémů je možno provádět buď jednotlivě na jednotlivá lokální nasazení informačního systému, nebo hromadně výběrem příslušných nasazení. Je tak umožněno rychle a efektivně nasazovat a aktualizovat jak nové verze řídicího software ISIC napříč všemi lokálními systémy, tak případné hromadné datové změny a úpravy.
- **Záloha IS** – Centrální správa ISIC udržuje aktuální obraz každého lokálního nasazení informačního systému a umožňuje jeho zpětné obnovení v případě nutnosti nebo výměny HW. V případě havárie lokálního řídicího PC nebo severu servisní technik provede výměnu vadného PC za nové předkonfigurované PC a po nastavení přidělené IP adresy a autorizaci vůči Centrální správě ISIC dojde k automatizované obnově daného nasazení ze zálohy.

Tímto způsobem lze dosáhnout podstatného zkrácení doby opravy v případě poruchy lokálních informačních systémů v jednotlivých stanicích a minimalizovat negativní dopady poruchy informačního zařízení vůči cestujícím.

- **Archiv** – Centrální správa ISIC zajišťuje archivaci logů o provedených hlášeních a vypsaných informacích na informačních tabulích z jednotlivých informačních systémů. Na základě tohoto centrálního archivu je možno zpětně dle potřeby centrálně dohledat informace o hlášení a informačních textech zpětně k požadovanému datu, stanici a vlaku. Vzhledem k centrálnímu uchovávání informací z jednotlivých lokálních systémů na jednom místě je zajištěna dostupnost těchto informací pro všechny pověřené pracovníky SŽDC bez nutnosti vytvářet vždy nové samostatné prostupy do technologických datových sítí na jednotlivá nasazení. Je tímto také eliminována možnost ztráty dat z těchto logů, ke které nyní může v případě havárie lokálního informačního systému docházet.
- **On-line dohled ISIC** – Centrální správa ISIC v on-line režimu komunikuje s lokálními informačními systémy v jednotlivých stanicích a zpětně předává informace o stavu jednotlivých zařízení včetně upřesnění případných chybových stavů jednotlivých prvků informačního systému. Na základě těchto informací je schopen proškolený pracovník provozovatele přesněji identifikovat příčinu poruchy a žádost o servisní zásah již směřovat na konkrétního dodavatele zařízení v poruše. Díky této okamžité a cílené diagnostice chybových stavů je možno předpokládat i zkrácení samotné doby, kdy je zařízení v poruše. Všechny chybové stavy z jednotlivých lokálních systémů jsou zaznamenávány a archivovány v databázovém systému Centrální správy ISIC. Na jejich základě je možné operativně vytvářet sestavy s přehledem aktuálních nebo již vyřešených problémů či přehledy poruch k jednotlivým nasazením nebo zařízením a identifikovat tak problémová či poruchová zařízení. Doporučuje se zasílání chybových stavů do systému DDTS ŽDC.

12.2.3 LOKÁLNÍ INFORMAČNÍ SYSTÉM STANICE

Lokální informační systémy stanice budou k Centrální správě ISIC připojeny prostřednictvím technologické datové sítě.

Každý lokální systém obsahuje vlastní databázi informací a hlasových vzorků.

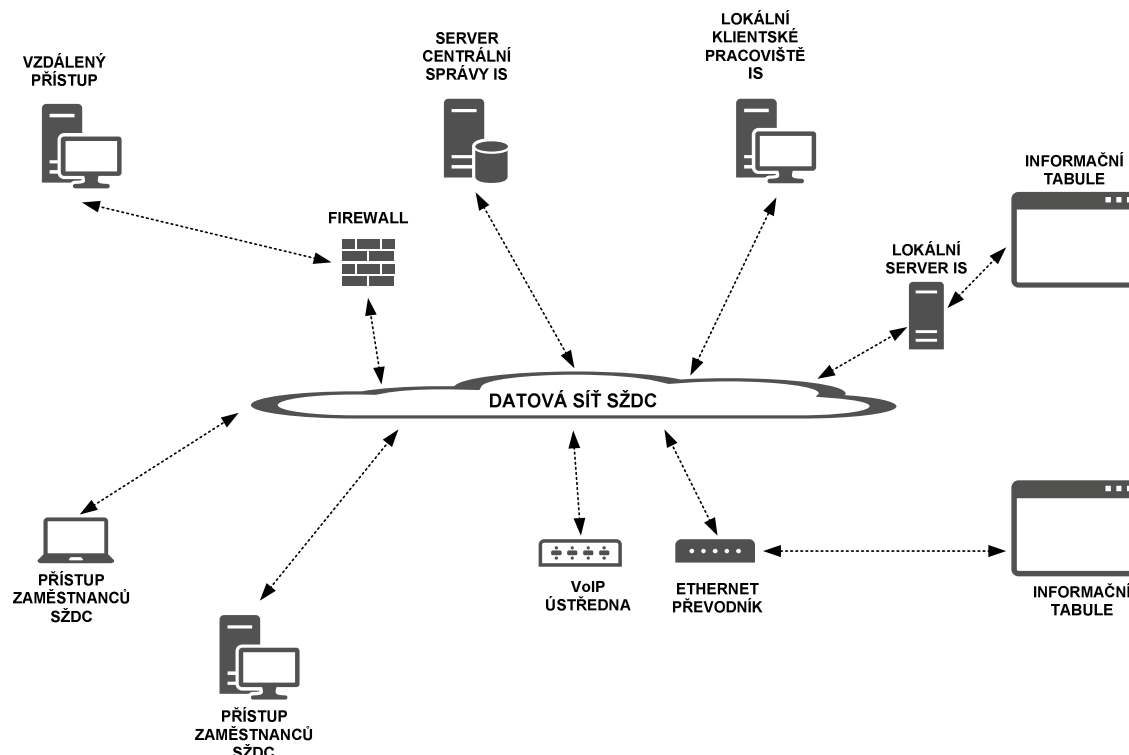
Aktualizace dat lokálních informačních systémů mohou probíhat několika způsoby:

- **Plánované** – lokální systém se dotazuje Centrální správy ISIC na nové aktualizace. V případě pozitivní odpovědi jsou aktualizace následně staženy do lokálního systému a dle zadaného data a času instalovány.
- **Operativní** - Centrální správa ISIC zasílá aktualizaci okamžitě.

Lokální systémy jsou navrženy tak, aby mohly pracovat v režimech online i offline (s dostupným/nedostupným připojením Centrální správě ISIC). V případě výpadku spojení jsou

¹² Konkrétní operační a databázový systém bude vybrán provozovatelem na základě provedené analýzy a při zpracování již konkrétního zadání.

všechny informace ukládány lokálně a po obnovení spojení jsou přeneseny na server Centrální správy ISIC.



OBR. 44 – PŘEHLEDOVÉ SCHÉMA CENTRÁLNÍ SPRÁVY ISIC

12.2.4 TECHNICKÉ PARAMETRY CENTRÁLNÍ SPRÁVY ISIC

12.2.4.1 Centrální server

Centrální server bude koncipován jako databázový a aplikační server. Vzhledem k požadavku na zajištění vysoké dostupnosti doporučujeme provozovat daný server buď na virtualizační platformě provozovatele systému nebo na samostatném serveru v konfiguraci splňující tento požadavek (duální napájení, hot-swap disky a ostatní komponenty vyměnitelné za běhu serveru). K dosažení vysoké dostupnosti je doporučeno v obou variantách (virtualizační platforma nebo samostatný server) umístění do obou CDP (Praha, Přerov).

Jako databázový server je možné buď využít stávající licence provozovatele informačních systémů, případně pořídit licenci novou.

12.2.4.2 Lokální systémy ISIC

Vzhledem k technické a morální zastaralosti některých nasazení informačních systémů ve stanicích (stáří PC cca 8-10 let, OS Windows XP) již toto hardwarové a softwarové vybavení nesplňuje požadavky pro provozování aktuální programové vybavy a jejich začlenění do centralizovaného systému. Je doporučeno při výměně těchto zařízení uvažovat s postupným budoucím začleňováním těchto stanic do DOZ a nasazovat v nejvyšší možné míře samostatně

ovládané síťové prvky (např. ethernetové převodníky pro řízení informačních tabulí nebo VoIP rozhlasové ústředny).

13 ROZHLASOVÉ ZAŘÍZENÍ

Ve většině železničních stanic se dnes nachází rozhlasové zařízení pro cestující. Železniční zastávky jsou vybaveny rozhlasovým zařízením v menším rozsahu. Vybavené jsou především zastávky na koridorových tratích nebo železničních tratích, které prošly v poslední době modernizací nebo výstavbou DOZ. Jedná se o různé typy i provedení od dříve nasazovaných analogových systémů po dnes nasazované digitální systémy v IP provedení. Ovládání nově nasazovaných rozhlasových zařízení je převážně dálkové z dispečerského pracoviště CDP Přerov / CDP Praha, nebo z nadřazené železniční stanice.

13.1 Navrhovaný stav

Požadavek na vybavení železničních stanic a zastávek hlasovým informačním systémem je zakotven přímo v *zákoně č. 266/1994 Sb., o dráhách* a také ve *směrnici SŽDC č.16/2005 Zásady modernizace a optimalizace vybrané železniční sítě České republiky*.

Studie tento požadavek plně respektuje. V rámci studie se navrhuje dodržet stávající trend v nasazování rozhlasových systémů tvořených ústřednou v IP provedení se 100V rozvodem. Použitá rozhlasová ústředna by měla umožnit osazení do 19" rámu (skříně). Všechny prvky rozhlasového zařízení musí být v provedení ve dvojité izolaci.

Ozvučování budou prostory i nadále nástupiště, podchody pro cestující, prostory pro cestující veřejnost (čekárny a jiné plochy určené k tomuto účelu). U větších železničních stanic se navrhuje ozvučit i prostory náhradní dopravy (doporučuje se vždy řešit samostatnou rozhlasovou větví).

Nově nasazované rozhlasové systémy by měly umožňovat přepínání režimů den/noc dle astrálního času. Nové rozhlasové systémy by měly zajistit stejnou úroveň hlasitosti výstupního hlášení při hlášení z různých zdrojů. Toto přispěje k minimalizaci rušení veřejnosti nadměrným hlukem.

Hlášení do rozhlasových ústředěn bude probíhat přes rozhraní Ethernet s VoIP protokolem umožňující hlášení z dispečerských pracovišť ze systému automatického hlášení s vazbou na zabezpečovací zařízení. Tento systém hlášení také umožní případný lokální, nebo vzdálený přístup pomocí VoIP telefonie pro případ nutnosti nouzových hlášení. Rozhlasová ústředna zároveň musí umožnit dálkový dohled stavů, vzdálenou konfiguraci a záznam provozní historie.

Napájení rozhlasového zařízení navrhujeme ve stanicích ze zálohovaných zdrojů, na zastávkách bez záložního napájení.

13.1.1 ROZHLAS PRO POSUN

V současné době rozhlas pro posun je ve stádiu dožívání. Pro potřeby posunu i údržby infrastruktury se již používají jiné technologie (MRS, GSM-R), proto se s dalším budováním rozhlasu pro posun neuvažuje. Naopak ve stavbách při jakémkoliv jeho dotčení bude, především z důvodu požadavku MŽP na snižování zvukového zatížení ze železničního prostředí, rušen.

13.1.2 EVAKUAČNÍ ROZHLAS

Evakuační rozhlas nesmí být spojován s drážním rozhlasem pro informování cestujících, i když umožňuje i zde poskytování jistých služeb. Evakuační rozhlas či jiné nouzové sdělovací zařízení bude instalováno jako požárně bezpečnostní zařízení tj. jako samostatný systém pouze ve výjimečných případech, když jeho instalování bude požadováno požárně bezpečnostním řešením stavby (PBŘ). V případě složitých podmínek pro provedení evakuace osob (odbavovací haly osobních nádraží apod.) bude využíváno k organizování evakuace rozhlasové zařízení v návaznosti na zpracovanou dokumentaci požární ochrany. Riziková místa, kde lze předpokládat použití nouzového sdělovacího zařízení pro usměrnění pohybu osob, jsou zejména prostory s větší koncentrací osob a případně jiná místa se zvýšeným rizikem dopadu mimořádných událostí, jako jsou např. tunely v délce nad 1km a dlouhé mosty s přihlédnutím k jejich dostupnosti a možnostem jejich opuštění.

14 ZABEZPEČOVACÍ A PROTIPOŽÁRNÍ SYSTÉMY

14.1 Autonomní samočinný hasicí systém

Autonomní samočinný hasicí systém (ASHS) je zařízení, které umožňuje v případě požáru provést vyhodnocení nebezpečí vzniku požáru a provést hasicí zásah bez přítomnosti lidské obsluhy.

Instalace zařízení ASHS musí být vždy posouzena a navržena v návaznosti na technické požadavky požární bezpečnosti staveb s přihlédnutím k zajištění přiměřené míry ochrany dotčených prvků kritické infrastruktury. Návrhy zařízení ve vztahu k chráněným prostorům jsou nedílnou součástí požárně bezpečnostního řešení stavby (PBŘ), kde bude stanovena nutnost instalace ASHS, EPS a koordinace s ostatními instalovanými požárně bezpečnostními zařízeními.

Z hlediska instalace zařízení ASHS je nutné v rámci SŽDC vytvořit závaznou směrnici pro výběr, projektování a užívání autonomních samočinných hasicích systémů v prostorách sdělovacích a zabezpečovacích technologií, která stanoví kritéria pro nasazování zařízení ASHS. Účelem této směrnice je sjednocení základních požadavků na autonomní samočinné hasicí systémy, tj. na jejich rozdělení, rozsah, provedení, kvalitu, druhy, komunikace s jinými technologiemi.

Pro vytvoření zásad projektování a využívání zařízení ASHS je nutné provést analýzu rizik a následně určit kritéria pro nasazení zařízení.

14.2 Elektrická požární signalizace

Elektrická požární signalizace (EPS) se v prostředí SŽDC také nazývá zařízení pro detekci požáru (ZPDP). Jedná se v podstatě o systém EPS s tím rozdílem, že pro tato schválená zařízení není nutný certifikovaný přenos do dohledového centra (HZS, HZS SŽDC). Potřebu výstavby EPS případně ZPDP určuje vždy požárně bezpečnostní řešení (PBŘ) příslušné stavby.

Stávající stav systémů EPS resp. ZPDP je velmi různorodý a některé typy ústředí jsou již za hranicí životnosti a jejich údržba je velmi problematická, neboť výrobci již na tyto systémy neposkytují žádná školení pro zajištění právním předpisem požadovaných pravidelných zkoušek činnosti, kontrol a revizí a také nejsou výrobci podporovány. Z výše uvedeného důvodu je nutné tato zařízení nahradit za nové systémy včetně hlásičů a kabeláže. Dalším důvodem proč tato zařízení nahrazovat je jejich nekompatibilita a nemožnost integrace do systému DDTS ŽDC.

Signalizované stavy z nově realizovaných systémů EPS je doporučeno integrovat nejenom do systému DDTS ŽDC, ale tyto stavy zasílat na dohledové centrum HZS SŽDC (operační a informační středisko příslušné JPO HZS SŽDC) a to minimálně ve formě signalizačního tabla EPS. Těchto HZS SŽDC je v současné době 14 lokalit.

Doporučuje se pokračovat také v integraci stavů do aplikace KAC prostřednictvím systému DDTS ŽDC a integračních serverů (InS). V rámci pokračování integrace do aplikace KAC je také nutné, aby systém EPS/ZPDP tvořil samostatnou VRF pro snadnější integraci.

14.3 Elektronická zabezpečovací signalizace

Elektronická zabezpečovací signalizace (EZS)¹³ v síti SŽDC je určena zejména pro ochranu majetku zejména pak objektů (technologické budovy, výpravní budovy a další). Systémem EZS se chrání vybrané místnosti zejména pak místnosti s technologií, dopravní kanceláře, pokladny a nově i technologické objekty přejezdů. Přístupy do jednotlivých místností jsou řešeny pomocí přístupové klávesnice s pinem nebo pomocí čteček karet. Zde doporučujeme využívat ve větší míře čtečky karet, které budou kompatibilní se čtečkami karet zaměstnanců SŽDC a systém EZS bude provázán s personální aplikací SŽDC pro správu uživatelů.

I zde platí stejné doporučení jako u systému EPS/ZPDP na náhradu starších nepodporovaných systémů EZS včetně využití multisenzorových hlásičů a detektorů, vzhledem k novým normativním požadavkům řady ČSN EN 54 popř. řady ČSN EN 50131 a souvisejících.

Doporučuje se pokračovat také v integraci stavů do aplikace KAC prostřednictvím systému DDTS ŽDC a integračních serverů (InS). V rámci pokračování integrace do aplikace KAC je také nutné, aby systém EZS tvořil samostatnou VRF pro snadnější integraci.

¹³ Systémy EZS mají dle platných norem řady ČSN 50131 Poplachové systémy - Elektrické zabezpečovací systémy, označení PZTS - poplachové zabezpečovací a tísňové systémy.

- Orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),
- **Správce informačního systému kritické informační infrastruktury,**
- **Správce komunikačního systému kritické informační infrastruktury a**
- **Správce významného informačního systému.**

15.1 Legislativní rámec

Zákon č. 181/2014 o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

- Kybernetická špionáž: Činnost využívající zranitelnosti systémů, sbírání datových toků atd. k provádění špionáže pro externí národní či nadnárodní žadatele o informace vhodné pro různé využití.
- Kybernetický terorismus: Činnost vedoucí k následkům v extrémních případech srovnatelných s fyzickými teroristickými útoky se srovnatelnými následnými materiálními a lidskými ztrátami.
- Nedostupné služby: Nedostupnost služeb může způsobit zastavení dopravy, nedostupnost informací pro cestující, atd.

Datová síť SŽDC splňuje ve vybraných jejích částech podmínky pro zařazení do kritické nebo významné informační infrastruktury podle Kybernetického zákona 181/2014 Sb. a prováděcích vyhlášek v pozdějším znění.

15.2 Navazující vyhlášky

Nařízení vlády č. 315/2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vyhláška č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Vyhláška č. 317/2014 o významných informačních systémech a jejich určujících kritériích

15.3 Definice pojmů

Sítí elektronických komunikací rozumíme přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace. (§ 2 písm. h) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích))

Významnou sítí rozumíme síť elektronických komunikací, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé propojení ke kritické informační infrastruktuře. (§ 2 písm. g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Kritickou informační infrastrukturou je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. (§ 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací (narušení důvěrnosti, dostupnosti a integrity) může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. (§ 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. (§ 21 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)) **Nouzovým stavem** se rozumí stav, kdy je bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně. (viz. čl. 2 odst. 1, ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.)

15.4 Povinnosti osob a orgánů dle ZKB

Povinnosti osob a orgánů dle ZKB jsou uvedeny např. na www.govcert.cz.

15.5 Doporučení pro komplexní prostředí více dodavatelů – bezpečnostní opatření dle ZKB

- Systém řízení bezpečnosti informací;
- Řízení rizik;
- Bezpečnostní politika (ISO 27000).

Organizační bezpečnost – interní opatření SŽDC

- Manažer kybernetické bezpečnosti;
- Architekt kybernetické bezpečnosti;
- Auditor;
- Garant aktiv.

Stanovení bezpečnostních požadavků pro dodavatele

- Řízení aktiv;

- Bezpečnost lidských zdrojů;
- Řízení provozu a komunikací KII/VIS;
- Řízení přístupu ke KII/VIS;
- Akvizice, vývoj a údržba KII/VIS;
- Zvládání KBU/KBI;
- Řízení kontinuity činností;
- Kontrola a audit KII a VIS;
- Fyzická opatření;
- Nástroj pro ochranu integrity komunikačních sítí;
- Nástroj pro ověřování identity uživatelů;
- Nástroj pro řízení přístupových oprávnění;
- Nástroj pro ochranu před škodlivým kódem;
- Nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů, administrátorů;
- Nástroj pro detekci KBU;
- Nástroj pro sběr a vyhodnocení KBU;
- Aplikační bezpečnost;
- Kryptografické prostředky;
- Nástroj pro zajišťování úrovně dostupnosti informací;
- Bezpečnost průmyslových a řídicích systémů.

15.6 Celoevropská směrnice NIS (Network and Information Security)

NIS přijata 6. 7. 2016, publikována 19. 7. 2016, platnost od 8. 8. 2016.

Nově zaváděné povinnosti:

- Státy musí přijmout národní strategii pro bezpečnost sítí a informačních systémů
- Státy musí určit vnitrostátní příslušné orgány pro oblast regulace, jednotná kontaktní místa a týmy CSIRT;
- Státy musí určit provozovatele základních služeb (PZS) – do 9. listopadu 2018;
- Směrnice přímo definuje poskytovatele digitálních služeb (DSP) – povinnost zapracovat do právního řádu;
- PZS s DSP budou muset přijmout a zavést bezpečnostní opatření a hlásit incidenty;
- Směrnice dále ustavuje síť skupin pro reakci na incidenty (CSIRT) a skupinu pro spolupráci na úrovni EU;
- ČR musí přijmout úpravu do 21 měsíců od vstupu směrnice v platnost – tedy nejpozději do května 2018;
- Nutno novelizovat ZKB;
 - Nyní probíhá vypořádání připomínek;
 - Plán: 4. Q/2016 – předložení transpozičních právních předpisů PS.

Směrnice zavádí dva druhy povinných subjektů:

- Provozovatelé základních služeb (PZS) – podobné KII – jsou zde ale rozdíly (PZS orientovány na vnitřní trh x KII na bezpečnosti státu);
- Poskytovatelé digitálních služeb (DSP) – vyhledávače, on-line tržiště, cloud computing – povinnosti jsou mírnější než u PZS.

Provozovatel základní služby (PZS) – definice:

- Základní služba = služba, jejíž poskytování je závislé na sítích nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví: 1. energetika, 2. doprava, 3. bankovníctví, 4. infrastruktura finančních trhů, 5. zdravotnictví, 6. dodávky a rozvody pitné vody, 7. digitální infrastruktura, 8. chemický průmysl;
- Informační systém základní služby = systém, na jehož fungování je závislé poskytování základní služby;
- Provozovatel základní služby = orgán nebo osoba, která je odpovědná za poskytování základní služby a která je určena Národním bezpečnostním úřadem;
- Určování provozovatelů – kritéria – doprava jedno z postižených odvětví;
- PZS budou určování opatření obecné povahy vydaným NBÚ;
- Určující kritéria stanoví prováděcí vyhláška k ZKB;
- Vyhláška zatím není zpracována – zveřejněny pouze teze vyhlášky;
- Odvětví budou kopírovat NIS, dopadová kritéria budou respektovat požadavky směrnice a zohledňovat národní podmínky;
- Pro určení bude nutné naplnit jak dopadová tak odvětvová kritéria;
- Doprava bude jedno z postižených odvětví, ale definováno jako pododvětví Silniční doprava – silniční orgány a provozovatelé inteligentních dopravních systémů.

Provozovatel základní služby (PZS) – povinnosti

NIS stanovuje následující okruhy povinností pro PZS:

- Přijmout technická a organizační opatření k řízení rizik;
- Přijmout opatření k předcházení incidentům narušujícím bezpečnost;
- Oznamovat incidenty včetně případných přeshraničních dopadů;
- Poskytovat národní regulační autoritě informace pro posouzení bezpečnosti včetně bezpečnostní politiky;
- Provádět nápravu zjištěných nedostatků;
- Povinnosti jsou stejné jako u KII – rozsah povinností bude stejný (KII má navíc povinnosti vyplývající z krizového zákona).

PZS bude regulována jako samostatná kategorie – nebude zahrnuta pod krizový zákon.

Do konce roku 2017 by měl vstoupit v platnost nový právní předpis EU, který upravuje informační bezpečnost a ochranu dat:

- **GDPR** (General Data Protection Regulation) - nařízení o obecné ochraně údajů v KII (Nařízení GDPR – platí pro všechny společnosti v EU);

KYBERNETICKÁ BEZPEČNOST a plnění zákona č. 181/2014 Sb., o kybernetické bezpečnosti musí být prioritou SŽDC. Doporučuje se z hlediska bezpečnosti bránit neautorizovanému přístupu do sítě a nasazovat pouze prvky a zařízení, které splňují požadavky na kybernetickou bezpečnost. Bezpečnost celé komunikační infrastruktury by se měla v požadavcích na návrh řešení odrážet minimálně v následujících skupinách požadavků:

- Segmentace a další architekturní požadavky na síť;
- Ochrana důvěrnosti a integrity přenášených dat;
- Zabezpečení přístupu do sítě;
- Podpora subsystémů kybernetické bezpečnosti a potenciál ke splnění aktuálních nebo budoucích legislativních požadavků.

16 SYNCHRONIZACE ČASU SDĚLOVACÍHO ZAŘÍZENÍ V SÍTI SŽDC

Jedním z velkých problémů v síti SŽDC je různorodý čas sdělovacích technologií (kamerové systémy, informační zařízení, hodinová zařízení, a další ...). Rozdíly mezi technologiemi jsou i v řádu několika minut. Podobná situace je i z hlediska synchronizace času mezi sdělovacími a zabezpečovacími zařízeními.

Z výše popsaného důvodu je nutné, alespoň v první fázi zajistit vytvoření centrálního zdroje času pro všechna sdělovací zařízení v síti SŽDC, mimo zabezpečovacích systémů. Předpokladem je zavedení interního NTP serveru / serverů do významných uzlů technologické datové sítě a následné připojení veškerých sdělovacích zařízení. Konkrétní způsob nasazení musí určit podrobnější analýza možností řešení. Možné externí referenční zdroje času pro nový NTP server je např.:

- GNSS (GPS/GLONASS/GALILEO) a PZF.
- Synchronizace času přes Ethernet
- Radiosignál DCF 77

Ve druhé fázi je pak nutné zajistit jednotný čas i mezi sdělovacím a zabezpečovacím zařízením.

Z pohledu použití se jeví jako nejvýhodnější použití některého ze systému globálního družicového polohového systému (GNSS). Oba současné systémy (GPS a GLONASS) jsou vojenské a ani jeden z provozovatelů nedává záruku, že ve výjimečných situacích budou systémy plně funkční pro civilní využití. Pokud by na jejich využívání byla založena některá z dopravních služeb, mělo by dočasné zhoršení výkonu systému nebezpečné důsledky pro její uživatele.

Naopak systém Galileo má největší potenciál především v dopravě (letecká, silniční, železniční, námořní a říční, městská, atd.), přesto však nabízí široké využití i v dalších oblastech, kde zvýší bezpečnost, přesnost a komfort (energetický průmysl, bankovníctví, zemědělství, civilní ochrana, životní prostředí, stavebnictví atd.). Otázkou zůstává pouze jeho plnohodnotné zprovoznění pro tyto potřeby.

16.1.1 SYNCHRONIZACE ČASU POMOCÍ GPS

Systém je tvořen 24 družicemi NOVASTAR GPS (3 slouží jako záložní) kroužícími na přesně specifikovaných oběžných drahách asi 20 tisíc km nad zemí. Družice jsou vybaveny přijímačem, vysílačem, atomovými hodinami a dalšími přístroji pro navigaci a speciální účely. Každá družice vysílá kódované informace o přesném čase, své poloze ve vesmíru a přibližné poloze ostatních družic systému. Pro příjem a zpracování vysílaných signálů byly vyvinuty speciální přijímače.

Výhody pro uživatele:

- Celosvětový dosah;
- Vysoká spolehlivost příjmu;
- Vyšší přesnost časové informace.

16.1.2 SYNCHRONIZACE ČASU POMOCÍ SIGNÁLU DCF 77

Vysílač DCF 77 Mainflingen je nejpoužívanějším evropským systémem svého druhu. Jeho vysílání je využíváno nejen ve složitých průmyslových zařízeních, ale i v běžných výrobcích spotřebního charakteru. Vysílač DCF 77 je umístěn v Mainflingenu, 24 km jihovýchodně od Frankfurtu nad Mohanem. Vysílač pracuje na dlouhých vlnách s frekvencí 77,5 kHz a svým výkonem 50 kW pokrývá oblast o poloměru přibližně 2000 km.

Tak jako každý radiopřijímač, podléhá i přijímač DCF 77 rušivým vlivům. Příjem radiosignálu DCF 77 ovlivňují následující faktory:

- Kovové obložení budov a místností, kovové stavební prvky (nosníky, armatury, střechy);
- Silné stěny a izolace, suterénny a sklepní prostory;
- Atmosférické poruchy, bouřky;
- Neodrušené elektrospotřebiče;
- Televizory a počítače, umístěné v blízkosti radiopřijímače DCF 77.

Z výše uvedeného doporučujeme se touto problematikou zabývat v samostatné Technicko-ekonomické studii, která bude řešit technické řešení (vhodná technologie, umístění a další) centrálního jednotného zdroje času pro všechna sdělovací zařízení v síti SŽDC.

17 PROSTORY PRO SDĚLOVACÍ ZAŘÍZENÍ V PROSTŘEDÍ SŽDC

Požadavky na prostory pro sdělovací zařízení v železničních stanicích ve výpravních budovách jsou definované v TNŽ 73 4955 – Výpravní budova a budovy zastávek ČSD z 19.5.1992. Plochy pro zabezpečovací a sdělovací zařízení jsou definované v kapitole 5.2.3. Předpokládá se umístění v samostatné sdělovací místnosti ve výpravní budově nebo v samostatném dopravním pavilonu. Předmětná TNŽ se dále odvolává na související stavební normy a předpisy.

Předmětná TNŽ a související normy jsou v současné době v mnoha ohledech zastaralé a v souvislosti s novými požadavky a strukturálními změnami v organizaci práce, provozu a servisu nevyhovující. Od doby uvedení TNŽ do praxe došlo k mnoha organizačním změnám z hlediska kompetencí ve vztahu k různým částem sdělovacího zařízení, k rozdělování a opětovnému slučování místností a distribuci sdělovací technologie do těchto místností. TNŽ a související předpisy rovněž **nerespektují nové požadavky moderních technologií na prostředí, klimatické podmínky, prostory, napájení, vazby na další technologické vybavení (zabezpečovací technologie, silnoproudé technologie) atd.** Velká část stávajících prostor nevyhovuje z hlediska vybavení, volného prostoru, klimatizace, přístupu k zařízení, mnoho místností je zaplněné nefunkčním zařízením, předměty, které nemají se sdělovací technologií nic společného, starými konstrukcemi a odpojenými kabely. Tato situace dále ovlivňuje schopnost správce a servisu zajistit tyto prostory po stavební stránce, údržbové stránce, hygieně práce apod.

V rámci této studie jsou dále navrženy určité postupy a doporučení při přípravě nových prostor v rámci probíhajících a připravovaných staveb. Problémem velké části staveb je ten, že se sice počítá s doplňováním sdělovacích zařízení, ale už méně se dbá na souvisejících stavebních úpravách, pokud se přímo nejedná o výstavbu nové budovy nebo objektu, případně celkovou rekonstrukci stávající budovy nebo rekonstrukci nové sdělovací místnosti. Vzhledem k ceně technologického vybavení je cena za stavební úpravy poměrně okrajovou záležitostí.

V rámci doplňování nového sdělovacího zařízení do stávajících sdělovacích prostor se doporučuje vždy posoudit stav těchto prostor z následujících hledisek:

- Stavební stav – podlaha, malby, okna, dveře, prostupy, žlaby, stoupačky, kabelové šachty;
- Elektroinstalace – NN rozvaděč, osvětlení, rozvod NN, uzemnění;
- Konstrukce – stojany a jejich obsazení, možnost demontáže prázdných starých konstrukcí, rošty;
- Stávající nefunkční zařízení – rekapitulace nefunkčního zařízení, odpojených kabelů a možnosti demontáže tohoto zařízení;
- Stávající funkční zařízení – možnosti jejich přemístění a jiného uspořádání;
- Jiné – klimatizace, EZS, EPS/ZPDP;

Cílem tohoto přístupu by měla být lepší udržitelnost těchto místností a zamezení náhodnému umísťování nového zařízení na „první volné místo na stěně“, zamezení doplňování dalších vzájemně se křížujících instalačních lišt na stěně, tvorbě náhodných kabelových svazků, instalaci vzájemně si překážejícím skříním apod. V neposlední řadě je nutné dodržet průkaznou evidenci a

popis instalovaného zařízení, která by byla přístupná přímo na místě (obsazení rozvaděčů, kabelové štítky, popis patchcordů apod.).

V případě výstavby nových prostor je situace lepší, ale není ideální. **Doporučuje se vypracovat směrnici, která by stanovila základní stavební a technické požadavky na velikost a vybavení místností, na způsob rozmísťování rozvaděčů a řad, ukončování kabelů, kabelových rezerv.**

Jako vodítko pro zpracování můžou sloužit níže uvedené zásady pro sdělovací místnosti, které lze kategorizovat následovně:

- I. kategorie - Sdělovací místnost ve velkém železničním uzlu
- II. kategorie Sdělovací místnost ve střední železniční stanici
- III. kategorie Sdělovací místnost v menší železniční stanici
- IV. kategorie Sdělovací místnost v železniční zastávce
- V. kategorie Venkovní skříně pro sdělovací zařízení

Zcela samostatnou kategorií je výstavba místností pro datová centra a center jako takových (kapitola 18).

17.1 Sdělovací místnost ve velkém železničním uzlu

Sdělovací místnosti ve velkých železničních uzlech je nutné řešit vždy individuálně, předpokládaná plocha pro tyto místnosti cca 27-37m², případně rozdělení na více vzájemně propojených místností. Výška místnosti se předpokládá cca 3,2m. Mezi stavební a technické požadavky patří:

- Samostatný podružný NN rozvaděč;
- Klimatizace, temperování;
- Antistatická PVC podlaha;
- Volitelně zdvojená podlaha;
- Volitelně nouzové osvětlení;
- EZS, EPS/ZPDP;
- Eliminace technických rozvodů budovy v místnosti (voda, odpad, dešťové svody, plyn, topení);
- Průstupy do dalších technologických místností (protipožárně ošetřené);
- Kabelový vstup do sdělovací místnosti – kabelová komora, kabelový žlab apod.

Předpokládá se osazení 19“ vnitřními rozvaděči v počtu cca 6-12ks s následujícími parametry:

- Rozměry (šířka x hloubka v mm): 600x600, 800x800, případně rozváděče o hloubce až 1000mm. Doporučuje se osazování 19“ rozvaděčů o velikosti 800x800;
- Výška v jednotkách U (U=44,45mm): 45U, 47U. Doporučuje se rozměr 45U, který má většina výrobců standardně k dispozici, rozměr 47U je většinou na objednávku s delší dodací lhůtou;
- Vybavení vnitřního rozvaděče: Konstrukční vybavení pro montáž zařízení do 19“ rámu, servisní zásuvkový panel, uzemňovací sběrnice;

- Dveře pro přístup do rozvaděče: Dveře pro přístup do rozvaděče: Prosklené nebo plechové perforované, Rozvaděče musí mít zajištěný pasivní odvod tepla, zadní panel musí umožňovat snadný přístup do rozvaděče, případně je možné druhou stranu opět vybavit dveřmi;
- Boční strana rozvaděče: Rozvaděč musí být vybaven odnímatelnými boky pro možné propojení více rozvaděčů do jednoho celku;
- Doporučuje se vybavovat novou místnost rozvaděči s prostorovou rezervou min. 30% - 40% pro další doplňování a zajištění jednotnosti;

Rozmístění rozvaděčů musí umožnit přístup z obou stran (přední a zadní přístup). Doporučená vzdálenost jednotlivých řad od sebe je 1000mm (min. 850mm). Před 1. řadou se doporučuje vzdálenost min. 1200mm. Vzdálenost boční strany rozvaděče od stěny z jedné strany je 1000mm (min. 850mm), z druhé strany může být řada přisunuta ke stěně místnosti.

Předpokládá se osazení dalšími konstrukcemi:

- Samostatná konstrukce pro ukončování HDPE trubek a plášťů metalických kabelů (může být ve společné nebo samostatné místnosti);
- Konstrukce a kryty pro kabelové rezervy optických kabelů (může být ve společné nebo samostatné místnosti);
- Doporučuje se použít samostatný otevřený nebo uzavřený rozvaděč pro kabelové rezervy optických kabelů;
- Hlavní uzemňovací sběrnice;
- Kabelové rošty – vodorovné, stoupací.

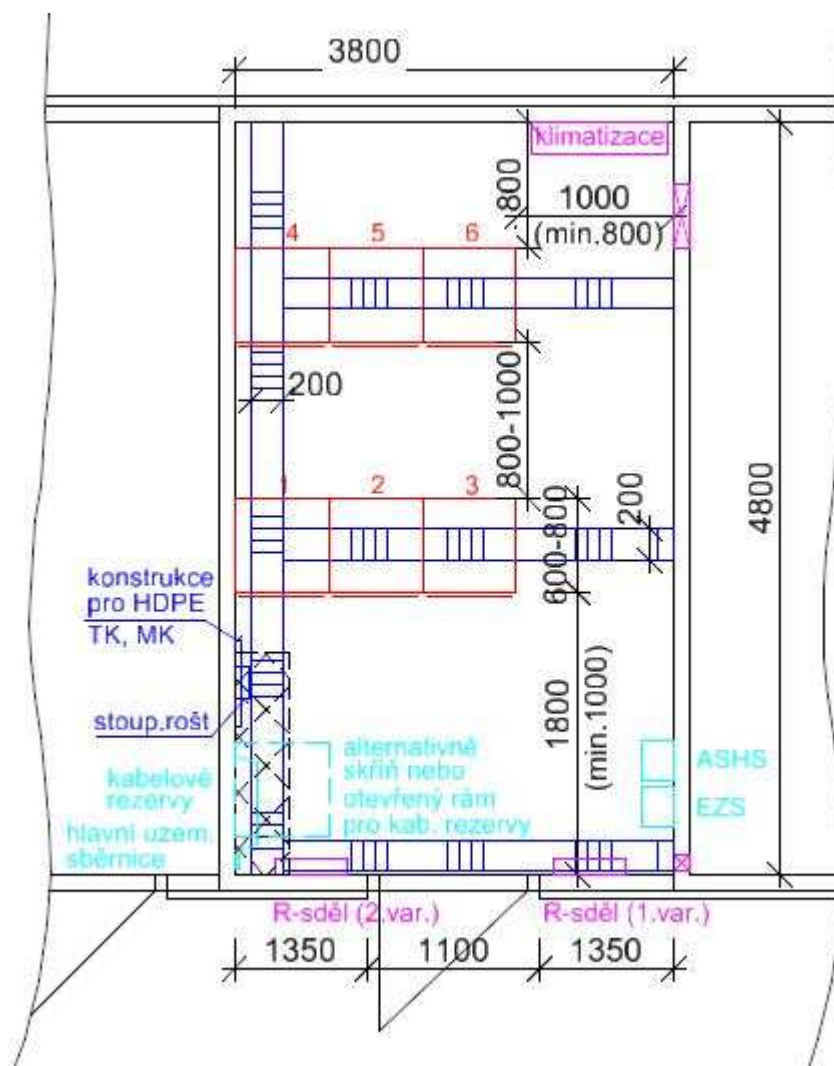
17.2 Sdělovací místnost ve střední železniční stanici

Pro tuto sdělovací místnost platí v přiměřené míře stejné stavební a technické požadavky jako u velké ŽST. Předpokládaný prostor je 14-18m², výška místnosti 3,2m. Návrh na uspořádání zařízení v místnosti je uvedený na Obr. 46.

Předpokládá se osazení 19" vnitřními rozvaděči v počtu cca 4 - 6ks s následujícími parametry:

- Rozměry šířka x hloubka v mm: 600x600, 800x800, 800x1000;
- Výška v jednotkách U (U=44,45mm): 45U, 47U;
- Vybavení vnitřního rozvaděče: Konstrukční vybavení pro montáž zařízení do 19" rámu, servisní zásuvkový panel, uzemňovací sběrnice;
- Dveře pro přístup do rozvaděče: Prosklené nebo plechové perforované, Rozvaděč musí mít zajištěný pasivní odvod tepla, zadní panel musí umožňovat snadný přístup do rozvaděče;
- Boční strana rozvaděče: Rozvaděč musí být vybaven odnímatelnými boky pro možné propojení více rozvaděčů do jednoho celku;
- Doporučuje se vybavovat novou místnost rozvaděči s prostorovou rezervou min. 30% - 40% pro další doplňování a zajištění jednotnosti.

Zásady pro umísťování rozvaděčů jsou stejné jako u velké ŽST.



OBR. 46 – NÁVRH NA USPOŘÁDÁNÍ ZAŘÍZENÍ V MÍSTNOSTI – STŘEDNÍ ŽST

Předpokládá se osazení dalšími konstrukcemi:

- Samostatná konstrukce pro ukončování HDPE trubek a plášťů metalických kabelů;
- Konstrukce a kryty pro kabelové rezervy optických kabelů;
- Doporučuje se použít samostatný otevřený nebo uzavřený rozvaděč pro kabelové rezervy optických kabelů;
- Hlavní uzemňovací sběrnice;
- Kabelové rošty – vodorovné, stoupací.

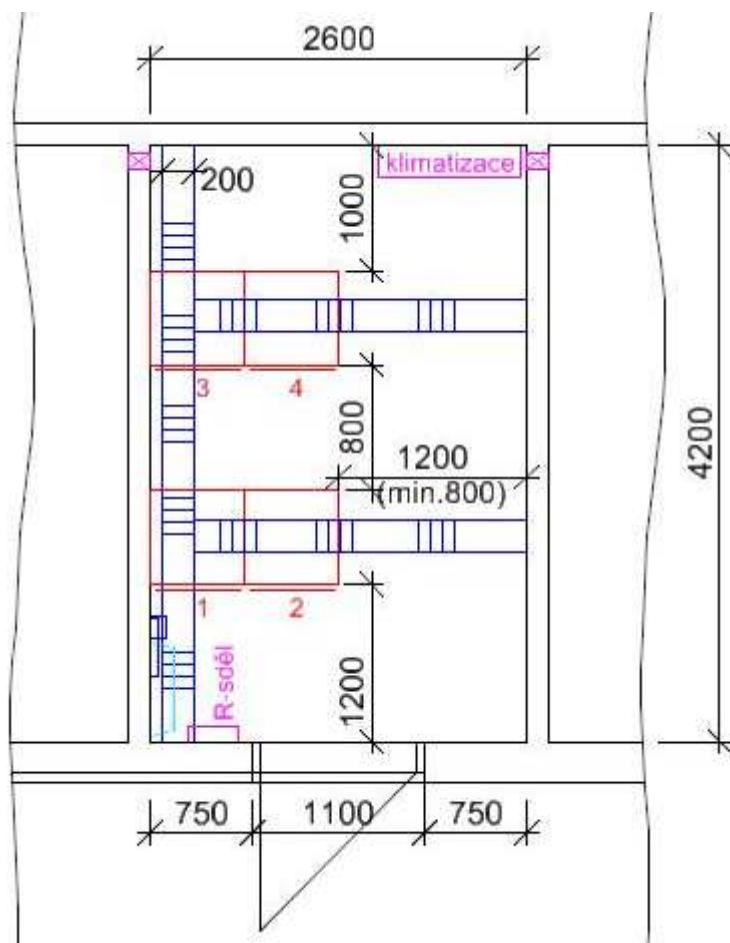
17.3 Sdělovací místnost v menší železniční stanici

Pro sdělovací místnost platí v přiměřené míře stejné stavební a technické požadavky jako u střední ŽST. Předpokládaný prostor je 9-11m² (zcela výjimečně 6-8m²), výška místnosti 2,8 - 3,2m. Návrh na uspořádání zařízení v místnosti je uvedený na Obr. 47.

Předpokládá se osazení 19" vnitřními rozvaděči v počtu cca 3 - 4ks s následujícími parametry:

- Rozměry šířka x hloubka v mm: 600x600, 800x800;
- Výška v jednotkách U (U=44,45mm): 45U, 47U;
- Vybavení vnitřního rozvaděče: Konstrukční vybavení pro montáž zařízení do 19" rámu, servisní zásuvkový panel, uzemňovací sběrnice;
- Dveře pro přístup do rozvaděče: Prosklené nebo plechové perforované, Rozvaděč musí mít zajištěný pasivní odvod tepla, zadní panel musí umožňovat snadný přístup do rozvaděče;
- Boční strana rozvaděče: Rozvaděč musí být vybaven odnímatelnými boky pro možné propojení více skříní do jednoho celku;
- Doporučuje se vybavovat novou místnost skříněmi s prostorovou rezervou min. 30% - 40% pro další doplňování a zajištění jednotnosti.

Pro umisťování rozvaděčů se doporučují stejné zásady jako u střední ŽST.



OBR. 47 – NÁVRH NA USPOŘÁDÁNÍ ZAŘÍZENÍ V MÍSTNOSTI – MALÁ ŽST

Předpokládá se osazení dalšími konstrukcemi:

- Samostatná konstrukce pro ukončování HDPE trubek a plášťů metalických kabelů;
- Konstrukce a kryty pro kabelové rezervy optických kabelů;
- Hlavní uzemňovací sběrnice;

- Kabelové rošty – vodorovné, stoupací.

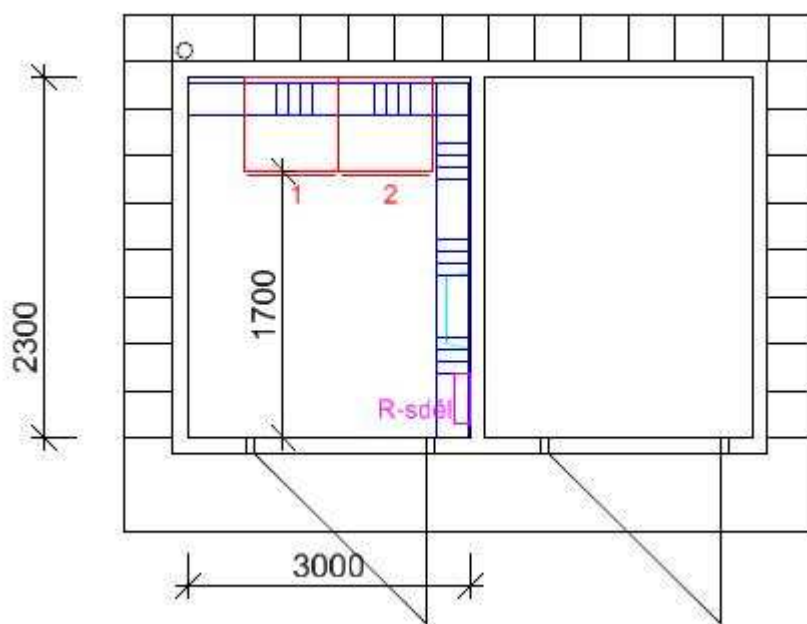
17.4 Sdělovací místnost v železniční zastávce

Pro sdělovací místnost v železniční zastávce platí v přiměřené míře stejné stavební a technické požadavky jako u ŽST. Předpokládaný prostor je 3-5m² (u významnějších lokalit 6-8m²), výška místnosti 2,8m. Návrh na uspořádání zařízení v místnosti je uvedený na Obr. 48.

Předpokládá se osazení 19" vnitřními rozvaděči v počtu max. cca 2ks (výjimečně až 4ks) s následujícími parametry:

- Rozměry šířka x hloubka v mm: 600x600, 800x800;
- Výška v jednotkách U (U=44,45mm): 32U, 42U, 45U;
- Vybavení vnitřního rozvaděče: Konstrukční vybavení pro montáž zařízení do 19" rámu, servisní zásuvkový panel, uzemňovací sběrnice;
- Dveře pro přístup do rozvaděče: Prosklené nebo plechové perforované, rozvaděč musí mít zajištěný pasivní odvod tepla, zadní panel musí umožňovat snadný přístup do skříně.

Předpokládá se umístění rozvaděčů zadní stranou ke stěně, vzhledem k omezenému počtu sdělovacího zařízení není nutný přímý přístup do zadní části rozvaděče.



OBR. 48 – NÁVRH NA USPOŘÁDÁNÍ ZAŘÍZENÍ V MÍSTNOSTI – ZASTÁVKA

Doporučuje se v maximální míře osazovat pouze 19" vnitřní rozvaděče o minimální velikosti 800x800 a minimální výšky 45U vybaveny horizontálními vyvazovacími kanály. Vnitřní rozvaděče umísťovat vždy přístupné ze dvou stran pro všechny ŽST, vyjma železničních zastávek. Sdělovací místnost dimenzovat vždy minimálně s 30% - 40% rezervou pro budoucí rozšíření. Dle potřeby osadit do kliky rozvaděče bezklíčový systém (viz kapitola 17.5)

Pro ukončení optických kabelů se doporučuje se použít samostatný otevřený nebo uzavřený rozvaděč pro kabelové rezervy optických kabelů, který může být součástí stojanové řady.

17.5 Venkovní rozvaděče pro sdělovací zařízení

Pro umístění sdělovacího zařízení v některých lokalitách je možné v případě nedostatku nebo nemožnosti vybudování stavebního objektu využít venkovní rozvaděč. Jeho použití se předpokládá především v železničních zastávkách. Venkovní Rozvaděč je možné doplnit ochrannou ocelovou klecí pro zvýšení ochrany proti vandalismu. Nicméně se doporučuje používat odolnou konstrukci odolávající povětrnostním vlivům a vandalismu. Návrh rozvaděče je uvedený na Obr. 49.



OBR. 49 – PŘÍKLAD VENKOVNÍ KLIMATIZOVANÉ SKŘÍNĚ (ANTIVANDAL PROVEDENÍ)

Pro volbu venkovní skříňe by měly být dodrženy následující požadavky:

- Venkovní rozvaděč min. rozměry 700x650x600mm s řízením vnitřním teploty
- 19" rám, min. 14U (možno větší dle místních podmínek);
- Upevnění na betonovém podstavci;
- Umožnění kabelových vstupů;
- Důkladná antikorozi úprava;
- Ochrana proti UV zařízení s vysokou životností;
- Ochrana proti vniknutí nepovolaným osobám (dálkový dohled);
- Dvouplášťové provedení zajišťující vyšší odolnost a přirozenou cirkulaci vzduchu;
- IP krytí min. 65 proti prachu a stříkající vodě pro standardní provedení a IK10 mechanickou odolnost;
- Možnost aktivního i pasivního chlazení (doporučuje se aktivní);

- Temperování;
- Vnitřní konstrukce pro upevnění zařízení do 19" rámu.

Doporučuje se venkovní rozvaděče vybavit vzdáleným monitoringem a řízením vnitřního prostředí (teplota, vlhkost, zatopení, vniknutí, detekce kouře, siréna a signalizační světlo). V případě potřeby uzavřený elektronický zamykací systém pomocí čtečky karet, což zjednodušuje „bezklíčový“ vstup do venkovního rozvaděče. Tento uzavřený elektronický zamykací systém lze uložit do těla kliky jak venkovního, tak i vnitřního rozvaděče (Obr. 50). TOTO ŘEŠENÍ JE S VÝHODU MOŽNÉ POUŽÍT PRO ROZVADĚČE, DO KTERÝCH JE UMÍSŤOVÁNO ZÁZNAMOVÉ ZAŘÍZENÍ KAMEROVÉHO SYSTÉMU.



OBR. 50 – PŘÍKLAD UMÍSTĚNÍ BEZKLÍČOVÉHO VSTUPU DO KLIKY

17.6 Kabelový management

Obecně velkým problémem ve sdělovacích místnostech je správná organizace kabelového vedení, které je vždy nedílnou součástí každé instalace ve sdělovacích místnostech. Současný stav není uspokojivý ani v nově realizovaných sdělovacích místnost. Proto je nutné dbát zvýšené pozornosti na přesnou organizaci kabeláže uvnitř rozvaděčů nebo otevřených rámu při **dodržení poloměrů ohybů** moderních datových kabelů. Nutno používat taková řešení, která zajistí bezpečné vedení optických a metalických.

V rámci zpracování projektových dokumentací a následně při realizaci staveb je důležité důsledně používat kabelové managementy, které zajistí přehlednost v celém rozvaděči. Vnitřní rozvaděče musí být vybaveny horizontálními vyvazovacími kanály (toto platí pro rozvaděč od velikosti 800x800), vyvazovací kanály pro vertikální vedení kabelů v rozvaděčích (Obr. 51).



OBR. 51 – PŘÍKLAD KABELOVÉHO MANAGEMENTU ROZVADĚČE

18 DATOVÁ CENTRA

Datové centrum lze definovat jako **prostor pro uložení počítačových technologií a přidružených technologií** jako jsou telekomunikační a centralizovaná úložiště, ať už fyzické nebo virtuální, pro skladování, řízení a šíření údajů a informací.

Budování datových center je obecně komplikovaná činnost zahrnující ve většině případů specifické stavební řešení objektu až po koordinaci všech podsystémů zajišťujících životaschopnost datového centra.

18.1 Právní požadavky na datová centra

Při výstavbě a navrhování datových center je nutná respektovat a řídit se právními předpisy a normami, které definují základní požadavky datových center.

Základní požadavky datových center jsou již dnes specifikovány normami jako např. ANSI-TIA/EIA 942A a dalšími vztahujícím se k datovým komunikacím a systémům. Datové centrum ať v malém či velkém provedení **řeší hlavně dostupnost uložených dat a výpočetní kapacity pro uživatele**.

Níže je uveden stručný přehled právních předpisů vztahujících se k datovým centrům.

18.1.1 PRÁVNÍ PROSTŘEDÍ ČR

- **Zákon č. 181/2014 Sb.** o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- **Vyhláška č. 316/2014 Sb.** o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);
- **Nařízení vlády č. 315/2014 Sb.** o kritériích pro určení prvku kritické infrastruktury.

18.1.2 PRÁVNÍ PROSTŘEDÍ EU

Do konce roku 2017 by měly vstoupit v platnost dva nové právní předpisy EU, které upravují informační bezpečnost a ochranu dat:

- **NIS** (Network and Information Security) - směrnice o bezpečnosti sítí a informací (Směrnice NIS je určena pro subjekty poskytující služby v KI);
- **GDPR** (General Data Protection Regulation) - nařízení o obecné ochraně údajů v KII (Nařízení GDPR – platí pro všechny společnosti v EU);

18.1.3 NADNÁRODNÍ NORMY

- **EN 50600-2-5** Informační technologie – Zařízení a infrastruktury datových center – Část 2-5: Systémy zabezpečení;
- **EN 50600-2-6** Informační technologie – Zařízení a infrastruktury datových center – Část 2-6: Informace o správě a provozu;
- **ANSI-TIA/EIA 942A** Telecommunications Infrastructure Standard for Data Centers;

- **ANSI/NECA/BICSI 002-2014** Data Center Design and Implementation Best Practices;
- **ISO/IEC 24764** Information technology — Generic cabling systems for data centres;
- **ISO/IEC 14763-2DC** Cabling Installation;
- **TIA 606-A** Labelling and Documentation;
- **IEC 61000** Electromagnetic compatibility (EMC).

Za stěžejní normu je považována nadnárodní ANSI/NECA/BICSI 002-2014.

18.1.4 ZÁKLADNÍ NADNÁRODNÍ NORMY

- **ČSN EN 50600-1** Informační technologie – Zařízení a infrastruktury datových center – Část 1: Obecné pojmy;
- **ČSN EN 50600-2-1** Informační technologie – Zařízení a infrastruktury datových center – Část 2-1: Výstavba budov;
- **ČSN EN 50600-2-2** Informační technologie – Zařízení a infrastruktury datových center – Část 2-2: Rozvody napájení;
- **ČSN EN 50600-2-3** Informační technologie – Zařízení a infrastruktury datových center – Část 2-3: Úprava okolního prostředí;
- **ČSN EN 50600-2-4** Informační technologie – Zařízení a infrastruktury datových center – Část 2-4: Infrastruktura telekomunikační kabeláže.

18.2 Základní požadavky na datová centra

Budování datových center je velmi komplexní činnost vyžadující znalosti z dalších oborů, chladicí systémy, napájení a záložní systémy, bezpečnost přístupu k zařízením, monitoring, dohled a další.

Důležitým a nedílným krokem je výběr místa pro stavbu datového centra, a to z důvodu nutnosti neustálé obsluhy datového centra. Právě výběr vhodné lokace je prvním krokem k budoucí bezpečnosti. Při návrhu datového centra je potřeba vzít v potaz mnoho faktorů jako například informace ohledně výkonových možností elektrického a datového připojení. Mezi další faktory patří vhodnost lokace při zohlednění možných rizik a možných omezení, jako například zatížitelnost podlahy, hluk, výfukové zplodiny, požární ochrana a rozšiřitelnost.

Základní požadavky na datové centrum jsou již specifikovány ve standardech jako například ANSI TIA/EIA 942A a dalších standardech pro komunikaci a systémy. Datová centra ať už velká anebo malá reflektují schopnost ukládat data a nabízet uživatelům výpočetní kapacitu. To shrnuje článek 1 až 4, které definují nabízené služby mezi 99.671 % a 99.995 % času (Tier 1 - 4).

V rámci zpracování studie proveditelnosti je nutné provést analýzu výběru lokality, zhodnotit aktiva datového centra, jejich strukturu (dat, software, hardware). Jednotlivá aktiva lze rozdělit:

1) Data

- Datová aktiva – Data veřejná
- Data interní – (intranet – standardní dokumenty)
- Data důvěrná – (účetní, výrobní, zákaznická)

- Data tajná – (smlouvy, strategie, finanční)
- Jiná datová aktiva – data jiné společnosti (zákazníka) v datovém centru

2) Aplikační aktiva (Software)

- Aplikační aktiva – Aplikace veřejné (www stránky)
- Aplikace interní – (intranet)
- Aplikace kritické – (SCADA,...)
- Aplikace strategické a tajné
- Jiná aplikační aktiva – aplikace společnosti (zákazníka) v datovém centru

3) Fyzická aktiva (hardware)

- Serverová platforma
- Síťová infrastruktura lokální
- WAN infrastruktura
- Datová úložiště
- Zálohovací knihovny, zařízení
- Objekt, budova, prostory
- Bezpečnostní zařízení CCTV, ACS
- Poplachové zařízení PZS, EPS
- Stabilní hasící zařízení
- Komunikační systémy
- Přenosová zařízení poplachových systémů
- Systémy primárního napájení
- Systémy záložního napájení
- Motorgenerátory
- Vzduchotechnika, klimatizace

4) Služby

- Přístup k IS
- Přístup k datům
- Přístup k aplikacím
- Dohled

V rámci této studie doporučujeme se otázku výstavby datového centra v prostředí SŽDC diskutovat. Doporučujeme zpracování studie proveditelnosti pro výstavbu datového centra, která bude sloužit jako základní rozhodovací materiál pro jeho výstavbu a specifikaci dle výše popsaných bodů.

19 ZÁVĚREČNÁ SHRNUÍ A DOPORUČENÍ

19.1 Kabelizace

Studie jednoznačně doporučuje postupné převedení provozu ze stávajících metalických DK do přenosového zařízení provozovaného po DOK, případně do nověji budovaných traťových kabelů a tím i zcela opuštění těchto DK. Dojde tak k úspoře provozních nákladů na údržbu těchto kabelů i úspoře investičních nákladů ve stavbách při jejich drahých překládkách. Převedení provozu musí být řešeno jako součást příslušné investice, která buduje novou kabelizaci.

Vzhledem k plánovanému přechodu na střídavou trakční soustavu již do budoucna navrhujeme budovat pouze traťovou kabelizaci v provedení TCEPKPFLEZE XN0,8. Pouze na tratích, u kterých se elektrizace jednoznačně neplánuje a nevyskytují se v oblasti vlivů střídavé trakční soustavy nebo indukčních vlivů vedení VVN s hodnotou ovlivnění přesahující normou povolené meze, lze budovat kabely v provedení TCEPKPFLEY XN0,8. Výhledově je ekonomicky vhodné sledovat možnost snížení dimenze traťových kabelů na 10XN0,8, což pro nastávající období považujeme za minimum (v odůvodněných případech doložených obsazovacím plánem je možno použít i vyšší dimenzi).

Z důvodu úspory nákladů za zemní práce vždy řešit kabelizaci komplexně. Při jakýchkoli zemních pracích zajistit pokládku dvou HDPE trubek a traťového kabelu.

Pokračovat v postupném budování optické kabelizace. Přednostně je třeba dobudovat úseky optické kabelizace, které jsou potřebné pro zaokružování vysokorychlostního přenosového systému, nebo kde vznikne propojení na stávající ostrovy optické kabelizace, případně kde nová kabelizace umožní zaokružování stávajících okruhů a tím dojde ke zvýšení bezpečnosti a spolehlivosti datového provozu.

U dálkových optických kabelů z pohledu životnosti kabelů a snížení nákladů na postupné navyšování dimenzí až v případě potřeby, budovat rovnou DOK s dostatečnou rezervou tj. 72 vláken. Pouze v případě koncových tratí, kde nelze uvažovat se zaokružováním provozu, bude použit kabel 48 vláken. Výhodou tohoto řešení je i zachovávání volné rezervní trubky pro případné odstraňování poruchových stavů.

Veškeré optické kabelizace i místní budovat pouze s jednovidovými vlákny (single mode provedení).

Doporučujeme aktualizovat směrnici SŽDC o ukončování a obsazování optických kabelů, a ve stavbách dbát na její dodržování z důvodu jednotnosti sítě. Nebudou tak vznikat úzká hrdla, která omezují možnosti provozu. Součástí staveb, které zasahují do stávající sítě, by měla být provedena i optimalizace obsazení okruhů a případné převaření ukončení kabelů, tak aby ukončení kabelů bylo standardizované. Tyto úpravy by měli být vždy součástí příslušné investiční akce, která zasahuje do kabelizace.

Doporučuje aktualizovat předpisy SŽDC týkající se železničního spodku a přímo v tělese trati vytvořit systémové místo pro ukládání kabelizací z důvodu usnadnění pokládky, údržby a výměny a úspory vstupů na cizí pozemky.

19.2 Přenosová síť SŽDC

Přenosový systém a technologická datová síť v prostředí SŽDC je a v budoucnu i bude klíčovým aspektem efektivního zavádění rozsáhlých propojitelných systémů ITS v dopravě. Tyto systémy vyžadují dostatečně dimenzovanou a v jakémkoliv okamžiku dostupnou přenosovou síť. **Doporučuje se pokračovat v současném trendu realizace přenosové sítě DWDM a po doplnění optických tras připojit další významné lokality.** V konečném důsledku by v budoucnu vzniklo osm kruhů zahrnující všechny významné lokality. **Přenosovou síť IP/MPLS v železničních stanicích a ostatních lokalitách se navrhuje řešit variantně vždy v závislosti na místních podmínkách pomocí páteřních směrovačů (PE), směrovačů (CE) a L3 přepínačů v ideálně ve variantě s redundantním řešením aktivních prvků z důvodu dosažení vyšší pohotovosti a spolehlivosti.** Různorodost požadavků uživatelů aplikací a správců systému i navazujících procesů uživatele vyžaduje výkonné prostředky pro segmentaci sítě jako základní prostředek řízení informačních toků v jejím rámci (viz kapitola 7.6.1). S použitím VRF je možné zajistit vzájemnou izolaci provozů, to znamená např. při požadavku dvou provozů, které mají být součástí jednoho směrovače a mají být vzájemně od sebe izolovány, stačí každý z těchto provozů přiřadit do vlastního VRF. **Zcela zásadní a nutnou podmínkou funkčnosti přenosové sítě a příslušných služeb, je její synchronizace, která je důležitým aspektem z hlediska bezpečnosti systémů.** Od realizace synchronizace sítě se odvíjí další vývoj přenosové sítě, telefonních ústředěn, rádiového systému GSM-R a dalších. Použití vyhrazených optických vláken pro dálkové ovládání ochrany je možné pouze v případě, že požadovaných časových parametrů (doba zpoždění přenosu) není možné dosáhnout technologickou datovou sítí. V případě, že parametry doby přenosu a časové synchronizaci nebude možné splnit, doporučuje se přenos po samostatných optických kabelech v režimu point-to-point.

Z kapitol popsaných výše dále vyplývá, že zejména v rámci přenosové sítě SŽDC je nutné určit a v rámci projektů vyřešit:

- **Globální architekturu sítě SŽDC**
 - Jejích hlavními cíli by měla být bezpečnost, optimalizace využití přenosové kapacity, podchycení požadavku pro vytvoření dlouhodobé koncepce;
 - Dále pak strukturální úpravy HW, konfigurační úpravy, migrace dat.
- **Rozšiřování prostor kvůli budoucím kapacitám**
 - Je nutné při plánování velikosti a rozšiřování prostor pro umístování sdělovací techniky brát ohled na budoucí stavby.
- **Životní doba zařízení**
 - Je nutné stanovit dobu životnosti pro jednotlivé kategorie zařízení, resp. pro technologie a technologické celky. Před koncem uplynutí definované doby vyvolat jednání o prodloužení životnosti, nebo o obnově dané technologie. Při rozhodování uvažovat EoS (End of Support) a EoL (End of Life) termíny stanovené výrobcem a tedy náklady na servisní podporu a dostupnost náhradních dílů, resp. uvažovat bezpečnostní rizika z tohoto vyplývající.
- **Analýza dalšího rozvoje sítě v pravidelných periodách**

- Je nutné v pravidelných intervalech zahájit aktivitu k plánování dalšího rozvoje sdělovacích technologií a datové sítě. V těchto intervalech by měla být spuštěna analýza, návrh a realizace opatření, vedoucí k udržení vysokého technologického standardu, efektivity a jednotné koncepce v rámci sdělovacích technologií a datové sítě. Je vhodné nastavit kontinuální plánování rozvoje. V další rovině je doporučováno stanovit milník pro strategické vyhodnocení a směřování rozvojových aktivit každých 5 let.
- **Optimalizace sítě v pravidelných periodách**
 - Je nutné v pravidelných intervalech zahájit aktivitu k optimalizaci sdělovacích technologií a datové sítě. V těchto intervalech by měla být spuštěna analýza, návrh a realizace nutných provozních úprav v portfoliu zařízení SŽDC s cílem zvýšit efektivitu fungování sdělovacích technologií a datové sítě, nebo odstranit vzniklé nežádoucí odchylky od globální architektury. Je vhodné nastavit milníky optimalizace na základě potřeb SŽDC, v různých intervalech, dle technologických celků.
- **Dohledy na všechna zařízení**
 - Z výše popsaného je zřejmé, že v návaznosti na Zákon č. 181/2014 o kybernetické bezpečnosti je nutné začlenit všechny aktivní prvky datové sítě SŽDC pod dohledové servery, umožňující sledovat stav dohledovaných zařízení až na úroveň jednotlivých interface, portů a služeb.
 - Tam, kde to koncové zařízení neumožňuje, je nutné provést výměnu za nový aktivní prvek splňující všechny požadované parametry. V případě úzce specializovaných zařízení technologické datové sítě je nutné obnovu posuzovat a plánovat individuálně, případně budou jednotlivá zařízení nahrazena novějšími při generační obnově celého technologického celku.

19.3 Komunikace aplikací DŘT, DDTS ŽDC v energetických objektech

V dohledné době nepředpokládá výstavba samotného přenosového systému pro systémy DDTS ŽDC, DŘT, systémy ochrany a dálkového odečtu elektroměrů ve směru od energetického objektu do ED (data mají většinou informační charakter). Veškerá zařízení v přenosové síti SŽDC včetně koncových zařízení musí splňovat požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Doporučuje se, aby topologie přenosového systému byla řešena následovně:

- Oblastní ED musí být dostupné minimálně ze dvou směrů přístupových optických tras (v geograficky oddělené trase);
- Energetické objekty se doporučuje mít dostupné ze dvou přístupových optických tras (pouze na základě místních podmínek v dané lokalitě a v případě, že je toto možné);
- Přenosová síť SŽDC (TDS) musí zajistit různá spojení z libovolného do libovolného místa s možností záložní trasy;
- Topologii TDS navrhovat tak, aby byla zajištěna maximální spolehlivost a dostupnost.

Použití vyhrazených optických vláken je tedy možné pouze v případě, že požadovaných časových parametrů (doba zpoždění přenosu) není možné dosáhnout technologickou datovou sítí. Proto se

doporučuje tyto časy při realizaci vždy prověřit a následně provádět tato měření v pravidelných intervalech. V případě, že tyto parametry doby přenosu a časové synchronizaci nebude možné splnit, se doporučuje přenos po samostatných optických kabelech v režimu point-to-point (viz 5.2.2).

Vzhledem k tomu, že tato problematika je velice rozsáhlá, navrhuje se zpracování samostatné studie, neboť specifikaci potřebných parametrů nelze kvalifikovaně provést bez podrobné znalosti celého komplexu zpracování dat řízení energetické soustavy od snímacích a akčních členů v rozvodně (energetické stanici), funkce realizované v rámci stanice-rozvodny, funkce distribuované mezi stanicemi/rozvodnami, funkce zajišťované SCADA systémy v řídicím centru (elektrodispečinku) a vzájemné komunikace mezi inteligentními elektronickými zařízeními (IED), stanicemi mezi sebou a IED a stanicemi vůči SCADA řídicím systémům.

Doporučuje se při zpracování samostatné studie vycházet z metod analýzy a návrhů dle skupiny norem ČSN EN 61968 Integrace aplikací v energetických společnostech - Systémová rozhraní pro řízení dodávky elektrické energie a ČSN EN 61850 Komunikační sítě a systémy pro automatizaci v energetických společnostech. K jednotlivým bodům studie uvádějícím definice a rozsahy kvalitativních požadavků doplnit jednoznačné přiřazení a určení konkrétních hodnot přenosových parametrů vztahujících se k jednotlivým typům přenášených dat.

19.4 Telefonní síť

Možnosti rozšiřování a modernizace telekomunikační sítě zcela závisí na fyzické a přenosové vrstvě, tj. na existenci kabelové sítě, především optické a na existenci kapacitně odpovídajících přenosových prostředků. V současné době je absence kabelových sítí hlavní překážkou rozvoje korporátní telekomunikační sítě SŽDC.

Před zahájením implementace nové IP služební telefonní sítě je nutné na základě této studie upřesnit a odsouhlasit navrženou novou architekturu sítě, její úrovně a rozsah jednotlivých uzlů. Vzhledem k tomu, že v současné době se začíná připravovat implementace IP prostředí do nejvyšší úrovně sítě, je vhodné začít připravovat projekty, které budou bezprostředně navazovat na tyto uzly, tj. projekty, které budou tyto tranzitní uzly doplňovat o stávající detašované části uzlu a projekty, které budou do těchto uzlů připojovat navazující tratě, představující 2. úroveň sítě.

V rámci jednotlivých projektů je nutné vyřešit účastnické kapacity jednotlivých lokalit, předpokládané provozní zatížení pro jednotlivé pobočky, kategorizace poboček a jejich oprávnění a způsob propojení jednotlivých uzlů. Dále bude nutné v rámci jednotlivých uzlů vyřešit uzlové části sítě a distribuční části, tj. kde budou instalované jednotlivé části telefonního systému a kde se provede distribuce pomocí datových přenosových sítí.

Předpokládá se postupná migrace telefonní sítě. Z technického hlediska je nutné postupně nahrazovat ty části stávající sítě, kde jsou v provozu staré analogové systémy a systémy, které jsou na hranici životnosti, a nelze již pro ně zajistit odpovídající servis. Jedná se většinou o oblasti, kde nejsou k dispozici optické kabely a je nutné současně řešit i otázku odpovídající kabelizace a doplnění přenosových systémů.

Z ekonomického hlediska je nutné posuzovat stav a užitnost stávajících systémů. V telefonní síti je v současné době v provozu mnoho systémů, které byly vybudované v nedávné době, jejich stav je dobrý a zajišťují požadované služby v odpovídající kvalitě.

Pro implementaci telefonních IP uzlů je nutný předpoklad existence optických kabelů pro jejich propojení. Jednotlivé uzly by se propojily na úrovni optických vláken – uzly by byly vybaveny vlastním optickým linkovým zakončením nebo, v případě existence odpovídajícího přenosového systému, by se propojily přes tento systém.

Navržený postup migrace IP telefonní sítě a další doporučení jsou popsány v kapitole 6.6.5.

19.5 Dotykové terminály a zapojovače

Konsolidace dotykových terminálů pro dispečerské řešení jsou dodávány v rámci jednotlivých staveb a je na nich tedy různá verze software odpovídající aktuálně platné technické specifikaci SŽDC. Jelikož se požadavky na terminály v čase mění a tyto změny jsou postupně zapracovávány do specifikace, je potřeba zajistit sjednocení SW všech terminálů v provozu. Proto je nutné najít mechanismus, jak udržovat v terminálech stále aktuální sw odpovídající aktuálnímu znění specifikace.

V rámci udržování aktuálního stavu SW je potřeba v první fázi zajistit tyto úkony:

- Upgrade centrálních prvků;
- Upgrade HW dotykových terminálů;
- Upgrade SW všech terminálů na aktuální verzi.

Ve druhém kroku je pak potřeba zajistit mechanismus udržování aktuálního softwaru na všech prvcích dispečerského řešení:

- Zajištění aktuálního SW centrálních prvků;
- Zajištění podporovaného HW dotykových terminálů;
- Zajištění aktuálního SW všech terminálů dle aktuálně platné směrnice.

Z hlediska bezpečnosti je vhodné zabránit neautorizovanému přístupu do počítačové sítě, ve které se dotykové terminály nacházejí. Jako vhodná technologie se jeví protokol IEEE 802.1X. Pokud se počítač či terminál připojí k přípojnému bodu (do portu switchu), je po něm pomocí protokolu 802.1X vyžadována autentizace. Připojný bod blokuje veškerý ostatní datový provoz klienta do té doby, než je úspěšně autentizován.

19.6 Kontrolně analytické centrum

Kontrolně analytické centrum v současné době poskytuje funkcionality komplexní rekonstrukce situace vztažené k řízení a organizování drážního provozu ze záznamu. Studie předpokládá rozšiřování a zapojování dalších stávajících zařízení SŽDC do aplikace KAC. Tím jsou míněna typová zařízení, která již do aplikace KAC data poskytují (zařízení pro záznam hlasu, kamerové systémy, diagnostikovaná data ze zabezpečovacích zařízení, EZS a EPS systémy, DVI-D sondy). V rámci tohoto tématu doporučujeme provést analýzu, která všechna zařízení podporovaného typu

v síti SŽDC mají být připojena do KAC, a tento rozsah realizovat. V případě překročení licence na počet zařízení určitého typu je nutné počítat s dodatečnými náklady na licenční krytí. V dalších etapách by měl být systém KAC rozšířen o další nové funkcionality jako např.:

- Začlenění dalších typů informací ze systémů DDTS ŽDC a těsnější provázání
- Integrace se systémem GSM-R, poloha vlaku
- Těsnější integrace aplikací zab. zařízení (synchronnost při rekonstrukci situace)
- Začlenění indikátorů horkoběžnosti a plochých kol
- Integrace se systémem integrovaného technologického systému správce železniční infrastruktury
- Rozšíření a doplnění algoritmů pro zpracování hlasové komunikace (audio záznamů)
- Centrální zastřešení kamerových systémů na přejezdech, video analytika výskytu překážek a vozidel v době výstrahy včetně rozlišení druhu vozidla a případně SPZ, obecný reporting, automatizace podkladů pro činné orgány
- Systém pro monitorování hlukového pozadí a dokladování dodržování hygienických požadavků a odhalování „nekompaktních“ vozidel

Zároveň by měla být vytvořena užší integrace s dalšími systémy zejména pak s Drážním řídicím operačním centrem.

Studie dále uvažuje aplikaci KAC jako jeden z hlavních konsolidačních prostředků nejrůznějších kontrolních analytických a monitorovacích prostředků sloužících k řízení provozu. Doporučuje ve spolupráci s gestorem řízení provozu (SŽDC, odbor O12) provést analýzu potřeby zapojení jiných typů zařízení, než jaké aplikace KAC v současné době podporuje.

19.7 Informační management pro železniční infrastrukturu

DRÁŽNÍ ŘÍDÍCÍ OPERAČNÍ CENTRUM (Informační management pro železniční infrastrukturu) a jeho výstavba povede k efektivnímu řízení a predikci incidentů, událostí a poruchových stavů. Realizací projektu bude umožněno správci železniční infrastruktury optimálně alokovat prostředky a kapacity s cílem zvýšit bezpečnost a plynulost prací na železniční síti, zajistit optimální parametry provozuschopnosti pro využívání jednotlivých částí infrastruktury s přihlédnutím ke stávajícím i výhledovým potřebám provozu. Vazba této připravované aplikace na provoz usnadní a zefektivní plánování vlakové dopravy, výlukovou činnost a včasnou indikaci a omezení nepravidelných a havarijních zákroků na infrastruktuře, což umožní celkové snížení zpoždění a nepravidelností v železničním provozu.

Z pohledu koncepce železnice v ČR a možných bezpečnostních situací, které je a bude nutné řešit, je využití sofistikovaného systému informačního managementu provozní bezpečnosti značným přínosem. V rámci komplexnosti řešení je možné systém využít na řešení **Mimořádných událostí**, predikce a odstraňování **Poruch infrastruktury**, zabezpečení jednotlivých **Objektů** ve správě železnice a **Hodnocení odolnosti infrastruktury** ve smyslu kritické infrastruktury.

19.8 Kybernetická bezpečnost v prostředí SŽDC

Kybernetická bezpečnost a plnění zákona č. 181/2014 Sb., o kybernetické bezpečnosti musí být prioritou SŽDC. Doporučuje se z hlediska bezpečnosti bránit neautorizovanému přístupu do sítě a nasazovat pouze prvky a zařízení, které splňují požadavky na kybernetickou bezpečnost. Bezpečnost celé komunikační infrastruktury by se měla v požadavcích na návrh řešení odrážet minimálně v následujících skupinách požadavků:

- Segmentace a další architekturní požadavky na síť;
- Ochrana důvěrnosti a integrity přenášených dat;
- Zabezpečení přístupu do sítě;
- Podpora subsystémů kybernetické bezpečnosti a potenciál ke splnění aktuálních nebo budoucích legislativních požadavků.

19.9 Rádiové systémy

Stávající rádiové systémy liniového charakteru (TRS, SRV, ASCOM), nebudou nadále již rozšiřovány, ale pouze udržovány. Údržba těchto systémů bude spočívat v zachování funkčnosti daného rádiového zařízení do doby, než budou nahrazeny novou technologií. Podmínkou pro údržbu je tedy dostatek náhradních dílů a technická podpora pro daná zařízení.

Jednoznačně se doporučuje budování pouze interoperabilního rádiového systému GSM-R (případně v následných letech jeho nástupce).

Dále Studie doporučuje:

- 1) Vzhledem k charakteru výstavby a rekonstrukcí železničních tratí je třeba provést rádiové plánování jako základní podklad pro koordinaci staveb pro celé území České republiky.
- 2) Pro regionální tratě, kde se nepředpokládá v blízké budoucnosti nasazení vlakového zabezpečovače, doporučujeme z ekonomických důvodů hledat variantu úsporného řešení staveb GSM-R (kapitola 8.2.1.1). Doporučujeme se na to téma zpracovat Technicko-Ekonomickou studii.
- 3) Zpracovatelský tým studie doporučuje nadále budovat rádiový systém GSM-R, pokud možno v relativně ucelených celcích navazujících na již zprovozněné úseky a omezit budování ostrovů, i když jsme si vědomi skutečnosti, že tohoto stavu nelze zcela dosáhnout. Lze však minimalizovat počet přechodů mezi jednotlivými rádiovými systémy. Tyto přechody způsobují provozní obtíže a zvyšují riziko lidské chyby.
- 4) Současně doporučujeme přednostně budovat rádiový systém GSM-R na tratích, kde doposud není nasazen žádný rádiový systém.
- 5) Součástí každé stavby musí být automaticky nasazení aplikace GSM-R STOP.
- 6) Výstavba nových základnových radiostanic místních radiových sítí v pásmu 150MHz musí vždy podléhat schválení generálním ředitelstvím SŽDC.

ŽELEZNIČNÍ BEZDRÁTOVÁ SÍŤ by měla patřit mezi standardní a kvalitní celoplošné pokrytí železniční infrastruktury technologií veřejné bezdrátové komunikace typu GSM jako služby pro cestující veřejnost, kde GSM se v širším slova smyslu myslí nejen hlasové služby, ale především vysokorychlostní datové služby 3G-4G a LTE. Nicméně lze očekávat, že zájem o pokrytí VRT datovými službami budou mít zejména operátoři osobní dopravy, aby mohli datové služby poskytovat cestujícím na palubě prostřednictvím WLAN. Aplikace této technologie **umožňuje realizaci řady telematických služeb** (odbavování cestujících, informační systémy pro cestující, sledování zásilek, telemetrie a diagnostika vozidel atd..) a rovněž **umožní výrazně zatraktivnit železniční dopravu**. Pokrytí celé tratě je důležité pro zajištění celosíťovosti železniční dopravy, tím její dostupnosti a atraktivity, a zároveň umožňuje řešit integrované dopravní systémy v území s využitím železniční dopravy jakožto rychlého, bezpečného, spolehlivého a atraktivního módu dopravy.

19.10 Kamerové systémy

Kamerové systémy se i nadále doporučuje budovat dle dosavadních zvyklostí ve všech železničních stanicích (bez výjimky), v železničních zastávkách pouze ve zdůvodněných případech (pouze tam, kde je větší pohyb cestujících veřejnosti a dle místních podmínek). Doporučuje se výstavba centrálních dohledových dispečinků ať už na úrovni regionální nebo celostátní. Doporučuje se v současné době použití dostupné IP **technologie s vysokým rozlišením záznamu a nasazování inteligentních kamerových systémů s analytickými funkcemi** (identifikace odložených zavazadel, identifikace cestujících, apod.). Doporučuje se využít IP kamer funkcí detekce pohybu v záběru s API rozhraním a využívání analytického software, který umožní definování prostor pod dohledem kamer s následným automatickým upozorňováním.

V rámci jednotlivých připravovaných staveb budovat **traťové kamerové systémy** pro zajištění bezpečnosti osob a majetku na železničních přejezdech, případně jiných exponovaných místech železničních tratí.

Navrhuje se vybudování komplexního systému dohledové centra:

- V rámci jiné vhodné investiční akce, případně formou samostatné pilotní stavby realizovat výstavbu **regionálního videodispečinku**.
- Na základě vyhodnocení výsledků pilotního ověření stanovit, případně upřesnit technické podmínky pro budování videodispečinků v dalších RDP, tyto videodispečinky postupně dobudovat.
- **Vybudovat centrální videodispečinky** na CDP Praha, resp. CDP Přerov a provést pilotní ověření integrace regionálního a centrálního dispečinku, vyhodnotit zkušenosti;
- Postupně provést integraci všech regionálních videodispečinků a obou centrálních videodispečinků.

19.11 Informační zařízení pro informování cestujících

Doporučuje se začít provádět postupné sjednocování a standardizaci informačního zařízení a sjednocování zobrazovaných informací. Pro možnost evidenci, datovou aktualizací základnu,

zálohu informačních systémů, kompletní archivaci a on-line komunikaci s lokálními informačními systémy se navrhuje výstavba centrální správy informačního systému.

19.12 EPS, EZS, ASHS

U systémů EPS se doporučuje signalizované stavy z nově realizovaných systémů integrovat nejenom do systému DDTS ŽDC, ale tyto stavy zasílat na dohledové centrum HZS SŽDC (operační a informační středisko příslušné JPO HZS SŽDC) a to minimálně ve formě signalizačního tabla EPS. Dále se doporučuje se pokračovat také v integraci stavů do aplikace KAC prostřednictvím systému DDTS ŽDC a integračních serverů (InS).

Z hlediska instalace zařízení ASHS je nutné v rámci SŽDC vytvořit závaznou směrnici pro výběr, projektování a užívání autonomních samočinných hasicích systémů v prostorách sdělovacích a zabezpečovacích technologií, která stanoví kritéria pro nasazování zařízení ASHS. Účelem této směrnice je sjednocení základních požadavků na autonomní samočinné hasicí systémy, tj. na jejich rozdělení, rozsah, provedení, kvalitu, druhy, komunikace s jinými technologiemi. Pro vytvoření zásad projektování a využívání zařízení ASHS je nutné provést analýzu rizik a následně určit kritéria pro nasazení zařízení.

19.13 Datová centra

Budování datových center je obecně komplikovaná činnost zahrnující ve většině případů specifické stavební řešení objektu až po koordinaci všech podsystémů zajišťujících životaschopnost datového centra.

Budování datových center je velmi komplexní činnost vyžadující znalosti z dalších oborů, chladicí systémy, napájení a záložní systémy, bezpečnost přístupu k zařízením, monitoring, dohled a další.

V rámci této studie doporučujeme se výstavbou datového centra v prostředí SŽDC zabývat. Doporučujeme vyhotovení studie proveditelnosti pro výstavbu datového centra, která bude sloužit jako základní rozhodovací materiál pro výstavbu datového centra.