

Schvalovací protokol stavby v přípravě „Segmentace provozu v technologické datové síti“ ve stádiu 2

A. Základní identifikační údaje

Název stavby:	„Segmentace provozu v technologické datové síti“
ISPROFOND/ISPROFIN:	5003520087
Místo stavby:	<p>Stavba se nachází ve stávajících technologických objektech v rámci oblastních ředitelství (OŘ) Praha, Plzeň, Ústí nad Labem, Hradec Králové, Brno, Olomouc, Ostrava ve vybraných železničních stanicích v síti Správy železnic. Stavba se nachází ve stávajících sdělovacích místnostech ve vybraných ŽST a ve sdělovacích místnostech obou CDP</p> <ul style="list-style-type: none">▪ OŘ Praha – Objekt CDP Praha▪ OŘ Plzeň – ŽST Plzeň hl. n. – Ústřední stavědlo triangl▪ OŘ Ústí nad Labem – ŽST ÚNL – Ústřední stavědlo▪ OŘ Hradec Králové – ŽST Pardubice – Provozní objekt▪ OŘ Brno – Brno Maloměřice – objekt/místnost ATÚ▪ OŘ Olomouc – Objekt CDP Přerov▪ OŘ Ostrava – ŽST Ostrava Svinov – objekt/místnost ATÚ
Kraj:	Praha, Ústecký, Plzeňský, Pardubický, Jihomoravský, Moravskoslezský, Olomoucký
Investor:	<p>Správa železnic, státní organizace Dlážděná 1003/7, 110 00 Praha 1 – Nové Město IČ: 70 99 42 34, DIČ: CZ – 70 99 42 34</p> <p>Zastoupená Stavební správou západ, Ke Štvanici 656/3, 186 00 Praha 8</p>
Zpracovatel dokumentace:	<p>SUDOP PRAHA a.s., 208 Středisko elektrotechniky, trakce, sdělovací a zabezpečovací techniky Olšanská 1a, PSČ 130 00 Praha 3</p>
Předpokládaná realizace:	2022 – 2024

B. Posuzovací část

B.1. Účel stavby

Cílem stavby je úprava technologické datové sítě ve vztahu k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a provedení takových úprav, které umožní zajistit vzájemnou izolaci stávajících provozů a případných externích subjektů do samostatné fyzicky nebo logicky oddělené sítě s řízeným přístupem pomocí směrování a TCP/IP komunikačními pravidly.

Ve stavbě bude navržena segmentace provozu v technologické datové síti pomocí VRF/VPN jako základní prostředek pro řízení informačních toků v datové přenosové síti. V rámci segmentace pomocí VRF/VPN bude navržena vzájemná izolace stávajících datových provozů přenosové sítě do samostatných logických celků (VRF/VPN) a to i s výhledem k budoucímu provozu. Dokumentace bude obsahovat návrh designu a rozdělení provozu (VRF/VPN) podle geografické lokality, funkce nebo typu uživatelů.

Pro zvýšení síťové bezpečnosti na úrovni propojení v rámci jednotlivých Oblastních ředitelství (OŘ) bude navržena ochrana a kontrola přístupu na sdílené SW prostředky v síti Správy železnic, která zvýší kontrolu přístupů a přístupů v rámci správní oblasti (např. OŘ, CDP).

Pro každou správní oblast (OŘ a CDP) budou navrženy dva New Generation Firewally s funkcionalitami AVC, IDS, AMP. Tyto firewally budou mít za úkol kontrolovat a sledovat provoz jak v rámci oblasti, tak i mezi nimi a provádět řízení politiky v souladu s vnitřními předpisy Správy železnic. Celý soubor firewallů bude řízen a nastavován z dohledového centra.

B.2. Popis stavby včetně kapacitních údajů

Stavba „Segmentace provozu v technologické datové síti“ řeší bezpečné oddělení jednotlivých typů provozu v technologické datové síti do samostatných logických segmentů. Dále řeší zajištění kontrolovaných přístupů mezi jednotlivými logicky izolovanými segmenty. Logická segmentace zachová rovněž možnost připojit a kontrolovat přístupy z fyzicky oddělených segmentů sítě.

Segmentaci bude realizována na různých vrstvách OSI modelu. Na vrstvě L2 prostřednictvím VLAN, na L3 oddělením do samostatných sítí s využitím technologie VRF (Virtual Routing and Forwarding) v MPLS pak označením jednotlivých typů provozu a oddělením do samostatných VPN (Virtual Private Network).

Segmentace je navržena na rozčlenění technologické datové sítě podle druhu přenášeného provozu, případně je určena technologií nebo typem zařízení pro kterou je daný segment vyhrazen. Tyto logické segmenty určené typem přenášených dat jsou následně segmentovány geograficky podle příslušnosti k OŘ. Další úroveň je hierarchická segmentace, kdy provoz z jednotlivých OŘ přechází do příslušného segmentu páteřní (globální) sítě. Tento princip tak umožňuje minimalizaci L2 segmentů, optimalizaci L3 segmentů a zajišťuje možnost kontroly a řízení provozu mezi jednotlivými segmenty. Z hlediska správy dovolí segmentace při vhodné implementaci řídit provoz v síti na základě relativně malých segmentů, které tak v případě bezpečnostního nebo provozního incidentu nebudou nevhodně ovlivňovat provoz v ostatních segmentech.

S ohledem na předpokládaný rozsah segmentace je nutné, aby byly náležitě dimenzovány síťové prvky přenosové sítě, zejména s ohledem na podporu dostatečného množství VRF, lze očekávat požadavky až v desítkách VRF.

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

- Segmentace provozu v technologické datové síti a další architekturní požadavky na síť;
- Zabezpečení přístupu do sítě;
- Podpora subsystémů kybernetické bezpečnosti a potenciál ke splnění aktuálních nebo budoucích legislativních požadavků.

Základní kapacitní údaje:

Kapacitní údaj	Popis	Měrná jednotka	Předchozí schválené stádium 1	Aktuální stádium 2
Sdělovací zařízení	FireWall	ks	14	14
	Předimplementační analýza, konfigurace, parametrizace	ks	7	7

B.3. Projednání dokumentace

Dokumentace pro územní rozhodnutí (stádium 2) byla v průběhu zpracování projednána elektronicky v rámci Správy železnic, státní organizace se složkami dotčenými stavbou a byla uzavřena 14.05.2021.

DUR byla projednána:

- se SŽ O14 + CTD UŽT-stanovisko č.j. 25305/2021-SŽ-GR-O14 ze dne 08.04.2021
- se SŽO30-stanovisko č.j. 19956/2021-SŽ-GR-O30 ze dne 06.04.2021

Stavba nevyžaduje územní rozhodnutí ani stavební povolení.

B.4. Požadavky pro další přípravu a realizaci

Na realizaci stavby nejsou kladeny žádné zvláštní požadavky. S ohledem na skutečnost, že stavbou je upravováno stávající sdělovací zařízení, je nutné, aby realizace stavby probíhala v úzké spolupráci se správcem zařízení a jeho odbornými složkami.

B.5. Shrnutí posuzovací části

Stavba „Segmentace provozu v technologické datové síti“ je v souladu s koncepčními záměry MD a Správy železnic, státní organizace.

Zpracovaná DUR odpovídá potřebám Správy železnic a požadavkům platné legislativy, zejména zákonu o drahách č. 266/1994 Sb., stavebnímu zákonu č. 183/2006 Sb. a prováděcím vyhláškám k těmto zákonům, vše v aktuálním znění. Odpovídá i požadavkům na DUR podle Směrnice GR č. 11/2006 v platném znění.

Na základě výsledků projednání a posouzení předmětné DUR doporučuje Stavební správa západ stavbu ve stádiu 2 ke schválení.

Zpracovatel posuzovací části:

Monika Škarvadová, M: +420 725 519 543; E: Skarvadova@spravazeleznic.cz

V Praze dne 2. listopadu 2021

Jakub Bazgier
13.12.2021 10:01
Podepsáno elektronicky

Ing. Jakub Bazgier
náměstek ředitele pro techniku