

## Obsah:

1.	VŠEOBECNÁ ČÁST .....	1
1.1.	Všeobecné údaje.....	1
1.2.	Výchozí podklady.....	1
2.	TECHNICKÉ ŘEŠENÍ.....	2
2.1.	KAMEROVÝ SYSTÉM (VSS) .....	2
2.1.1.	Požadavky na systém .....	2
2.1.2.	Technické řešení .....	5
2.1.3.	Rozmístění kamer .....	6
2.1.4.	Rozvody .....	6
2.1.5.	Aktivní prvky.....	7
2.1.6.	Měření kabeláže .....	7

## 1. VŠEOBECNÁ ČÁST

### 1.1. Všeobecné údaje

Název stavby:	Rekonstrukce výpravní budovy v žst. Tábor
Investor:	Správa železnic, státní organizace Dlážděná 1003/7, 110 00 Praha 1
Projektant části:	Michal Eibich
Název PS:	D.1.2.4 Poplachové zabezpečovací a tísňové systémy, žst. Tábor, videodohledové systémy

### 1.2. Výchozí podklady

Pro zpracování této zprávy bylo použito následujících podkladů:

- Půdorysné podklady dodané GP
- Koordinace s ostatními profesemi
- Projekt Požárně bezpečnostního řešení PBR
- Konzultace s investorem a projektanty ostatních profesí

Všeobecné

ČSN 34 2300 ed.2 - Předpisy pro vnitřní rozvody sdělovací vedení

STRUKTUROVANÁ KABELÁŽ

ČSN EN 50173-1 ed.2 - Informační technologie - Univerzální kabelážní systémy –  
Část 1: Všeobecné požadavky

ČSN EN 50174-1 ed.2 - Informační technologie - Instalace kabelových rozvodů –  
Část 1: Specifikace a zabezpečení kvality

ČSN EN 50174-2 ed.2 - Informační technika - Kabelové rozvody - Část 2: Plánování instalace  
a postupy instalace v budovách

CCTV

ČSN EN 62676-1-2 - Dohledové videosystémy pro použití v bezpečnostních aplikacích –  
Část 1-2: Systémové požadavky - Výkonové požadavky na video přenos

ČSN EN 62676-4 - Dohledové videosystémy pro použití v bezpečnostních aplikacích  
Část 4: Pokyny pro aplikaci

## 2. TECHNICKÉ ŘEŠENÍ

Tento projekt řeší slaboproudé technologie (kamerový systém VSS). Ve stávajícím objektu (před rekonstrukcí) je instalován kamerový systém VSS ve správě SŽ, jsou instalovány zastaralé rozvody strukturované kabeláže neodpovídající současným trendům a zvyklostem. S ohledem na stavební úpravy a zpřísnění nároků na kvalitu záznamu z kamer, je navrženo stávající kamery demontovat a nahradit za nové. V rámci tohoto projektu je navržen nový kamerový systém v IP provedení.

### 2.1. KAMEROVÝ SYSTÉM (VSS)

#### 2.1.1. Požadavky na systém

V budově (uvnitř i na plášti budovy) budou instalovány IP kamery. Záznam z IP kamer bude ukládán na záznamové zařízení s kapacitou záznamu na cca 7 dní s nejméně 4 sloty pro instalaci harddisků a minimálně 1 síťovým rozhraním 1Gbps. Systém navržený v tomto projektu bude sloužit pro fyzickou ochranu objektu. Navržený systém VSS neslouží pro řízení dopravy. Obsluha systému VSS bude prováděna pomocí stávajícího monitorovacího softwaru. Všechny instalované systémy musí splňovat pokyn SŽDC PO-21/2017.

S ohledem na zajištění jednotnosti a kompatibility instalovaných prvků v rámci SŽ musí dle požadavku investora kamery, videomanagement systémy i videoanalytické systémy umožňovat integraci do monitorovacího a řídicího systému kompatibilního s centrálním řešením Správy železnic, s.o. a zároveň splňovat požadavky dané směrnicí NIS2, zákonem o kybernetické bezpečnosti s příslušnými vyhláškami a akceptovat doporučení NÚKIBu v oblasti kritické informační infrastruktury.

Instalace a SW nastavení dohledového video systému musí splňovat požadavky specifikované v interním dokumentu „Základní technické požadavky na kamerové systémy“, č. j.: 18453/2018-SŽDC-014, požadavky na EMC pro eliminaci rušení rádiových systémů. Infrastruktura kamerového systému musí splňovat požadavky, které jsou specifikovány v Pokynu generálního ředitele č. 21/2017, č. j.: 48729/2017-SŽDC-GR-014 – Opatření a omezení pro dodávky technologických celků s dopadem na síťovou infrastrukturu SŽ. Dále musí být zajištěna připravenost na připojení VSS do systému DDTS. Při instalaci VSS a jeho následném provozu jsou dodržovány požadavky platných technických norem řady ČSN EN 62676. Systém VSS musí splňovat požadavky na stupeň zabezpečení minimálně 3: střední až vysoké riziko dle ČSN EN 62676-1-1. Všechny komponenty použité při instalaci a následném provozu musí být schváleny v souladu se Směrnicí SŽDC č. 34, změna č. 1, č. j.: S 53542012-OAE – Směrnice pro uvádění do provozu výrobků, které jsou součástí sdělovacích a zabezpečovacích zařízení a zařízení elektrotechniky a energetiky, na železniční dopravní cestě ve vlastnictví státu státní organizace Správa železnic.

Dohledový videosystém ve správě SŽ musí umožňovat modulární výstavbu tak, aby VSS bylo možno libovolným způsobem doplňovat a rozšiřovat. Rovněž musí být schopný nastavení a rozdělení funkcionalit dle uživatelského prostředí. Veškerá použitá zařízení musí být kompatibilní s otevřeným protokolem ONVIF a musí umožňovat přenos videosignálu minimálně s kodekem H.264.

Záznamové zařízení VSS musí vyhovovat nasazení v prostředí třídy II – vnitřní – všeobecné, tj. v rozsahu teplot -10 °C až +40 °C při střední relativní vlhkosti přibližně 75 % bez kondenzace. Operační systém záznamového zařízení musí být umístěn na jiném médiu než pořízené záznamy (tj. vyhrazený pevný disk, flash disk apod.).

Systém musí spolupracovat v rámci integrovaného řídicího systému s PZTS a EACS, tzn. umožnit automatické směřování a zapínání kamer dotčených definovanými incidenty.

Pro správné využívání instalovaných VSS je nutné zpracování projektové dokumentace skutečného provedení specifikující typ, rozsah a způsob současné instalace VSS. Tato dokumentace musí být aktualizována na základě změn a úprav, ke kterým může v provozních podmínkách docházet.

Dodaný a instalovaný systém bude dále odpovídat Požadavkům na kamerové systém ve Správě železnic, s.o. (č.j. 56576/2024-SŽ-GR-O30):

#### *Minimální technické požadavky pro software pro správu videa (VMS)*

Řešení bude plně vyhovovat požadavkům Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a splňovat požadavky Zákona o kybernetické bezpečnosti pro kritickou informační infrastrukturu respektive pro regulovanou službu v režimu vyšších povinností (dle nového Zákona o kybernetické bezpečnosti).

*SW umožní zaznamenávání logů pro:*

- jednoznačnou identifikaci uživatele
- přihlašování a odhlašování ke všem účtům včetně neúspěšných pokusů
- činností provedených administrátory
- úspěšné i neúspěšné manipulace s účty, oprávněními a právy
- neprovedení činností v důsledku nedostatku přístupových práv a oprávnění
- činností uživatelů, které mohou mít vliv na bezpečnost dodávaného systému
- zahájení a ukončení činností technických aktiv (*Technické aktivum = komunikační prostředky a programové vybavení SW*)
- kritických a chybových hlášení technických aktiv
- přístupů k záznamům o událostech, pokusy o manipulaci s nimi a změny nastavení nástrojů

SW je schopen odesílání výše požadovaných událostí do SIEM provozovaného v SŽ.

#### *Parametry VMS pro využití v působnosti KS SŽ:*

Požadované rozlišení	HD, FullHD
Podporovaná rychlost snímání	8-30 snímků za vteřinu
Podporované formáty videosouboru	.AVI, .MKV, .MPEG4, .MOV, .WMV, .DVR, .ASF, .RT4, .DIVX, .264, .GE5, .TS, .3GP, .MP4, .FLV
Podporované kodeky	H.264, H.265/HEVC, MPEG-4
Přihlášení (SSO)	Microsoft Active Directory, LDAP a LDAPS, včetně uživatelských skupin a SAML protokol
Rozpoznání obličejů	Minimální velikost obličeje 24x24 pixelů
Podporované jazyky	Čeština, angličtina
Podporované prohlížeče	Microsoft Edge nebo Google Chrome Desktop

#### *Podporovaná zařízení*

VMS musí podporovat více než 10.000 různých typů a značek zařízení.

#### *Obecné požadavky společné pro všechny kamery*

- Kamery musí být oficiálním výrobkem výrobce a určená pro nepřetržité průmyslové použití.

- Kamery musí podporovat známé standardy a osvědčené technologie využívající otevřené a zveřejněné protokoly.
- Musí splňovat následující normy v jednotlivých uvedených oborech.

#### *Technické normy*

##### *Síť:*

- IEEE 802.3af/802.3at (napájení přes Ethernet)
- IEEE 802.1AR
- IEEE 802.1x (EAP-TLS, PEAP-MSCHAPv2) (ověřování)
- IPv4 (RFC 791)
- IPv6 (RFC 2460)
- QoS - DiffServ (RFC 2475)
- NIST SP500-267

##### *Kybernetická bezpečnost:*

- ČSN EN ISO 303 645 V2.1.1

##### *Zkoušení vlivů prostředí:*

- ČSN EN 60068-1 ED2

##### *Elektromagnetická kompatibilita (EMC)*

- ČSN EN 61000-6-2 ED2 - Část 6-2: Kmenové normy - Odolnost pro průmyslové prostředí

#### *Ochrana soukromí:*

- Kamery musí být navrženy v souladu s rámcem „Privacy by default“. Bezpečnostní kamery musí obsahovat možnost video a audio analytických funkcí, které jsou prováděny přímo v procesoru kamery tak, aby analyzované video a zvuk nemusely opustit kameru a minimalizovaly tak možnost úniku osobních dat.
- Kamery určené pro sledování dopravy mohou mít parametry požadované příslušnými odbornými zaměstnanci a nemusejí umět video a audio analýzu, pokud není požadována.
- Kamery, které slouží pro sledování drážní dopravy a zároveň pro bezpečnost, musejí obsahovat možnost video i audio analytických funkcí.
- Kamery musí obsahovat funkce umožňující anonymizaci a pseudonymizaci statickou i dynamickou, a to jak v živém obraze v reálném čase, tak i následně v exportovaném záznamu.
- Kamery musí obsahovat funkci pro stanovení aktuálního rozlišení pro možnost stanovení třídy technických a organizačních opatření podle Metodiky ÚOOÚ.
- Všechny kamery musejí mít možnost „vymaskovat“ definovaný prostor

#### *ONVIF profily*

Kamera musí podporovat ONVIF Profile G, ONVIF Profile M, ONVIF Profile S a ONVIF Profile T dle specifikace na adrese [onvif.org](http://onvif.org). Není možné kamery připojovat pomocí RTSP streamingu.

Opatření pro kybernetickou bezpečnost a vestavěné kyberneticko-bezpečnostní funkce (pro soulad se směrnicí NIS2 a souvisejícími právními normami)

- Dodavatel HW popř. SW musí být certifikován v souladu s normou ČSN ISO/IEC 27001 pro systém řízení bezpečnosti informací (ISMS)
- Dodavatel musí bezodkladně odstraňovat všechny relevantní zranitelnosti, které se vztahují k SW a HW a které mají hodnocení zranitelností založené na systému CVSS (Common Vulnerability Scoring System) vyšší než 8.0, a to včetně 8.0

- Dodávané řešení musí využívat nástroj pro centrální správu přístupových účtů
- CVE Numbering Authority (CNA) v rámci domény MITRE
- Výrobce použitých kamer má zavedena minimálně tato opatření na řešení kyber bezpečnostních incidentů tzn. prevence, odhalování a reakce na incidenty a jejich hlášení: Služba upozornění na zabezpečení (Security Notification Service) a Zásady správy zranitelnosti (Vulnerability Management Policy)
- Výrobce použitých kamer má ve svých produktech standardně minimálně tyto funkcionality zajišťující požadavek na opatření vyžadované NIS2: „Bezpečnost sítí a informačních systémů a používání kryptografie“
  - Digitálně podepsaný firmware - kontrola integrity FW – spustí se pouze s autorizovaným firmwarem
  - Zabezpečený kryptografický výpočetní modul dle ČSN EN IEC 62443-4-1 Bezpečnost pro systémy průmyslové automatizace a řízení
  - ID zařízení - digitální pas, jedinečný pro každou jednotku zařízení po celou dobu životního cyklu produktu.
  - Podepsané video, které zajistí, že video důkazy lze ověřit jako nezfalšované a nemanipulované
  - HTTPS šifrování defaultně zapnuto – při spouštění zařízení musí být automaticky zapnuto HTTPS šifrování s vlastním podepsaným certifikátem = bezpečná úvodní konfigurace včetně nastavení hesla. V SŽ je vybudována interní certifikační autorita s požadovanými parametry.
- Výrobce použitých kamer poskytuje zdarma centralizovaný management nástroj pro správu všech svých zařízení v síti provozovatele – monitoring jejich stavu a zdraví, centrální nástroj pro správu prvků, dávkový upload bezpečnostních updatů a patchů, bezpečnostních certifikátů a nastavení a monitoring funkcí kybernetického zabezpečení.
- Poskytovatel je povinen informovat Objednatele o všech událostech, které mají charakter KBU nebo KBI.
- V případě likvidace dat musí být dodržena pravidla pro likvidaci dat v závislosti na klasifikaci těchto dat.
- Výrobce dodávaných kamer poskytuje možnost updatů firmware formou Long-Term Support FW track pro zajištění maximální stability informačního systému při zachování maximální kybernetické bezpečnosti.
- Ve smlouvě je nutné využít ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele.

Dodaný systém bude odpovídat i ostatním požadavkům uvedeným v Požadavcích na kamerové systém ve Správě železnic, s.o. (č.j. 56576/2024-SŽ-GŘ-O30).

### 2.1.2. Technické řešení

IP kamery budou monitorovat vstupy do objektu, plášť objektu, prostor odbavovací haly, výtah v prostoru podchodu a kabinu výtahu (viz výkresová část). Pro přenos videosignálu budou využívat IP prostředí a protokol Ethernet. Kamery budou napájeny s využitím technologie PoE. Kabelové rozvody od přípojných míst pro VSS systém budou v 19" rozvaděči ukončeny na modulárním patch panelu 24xRJ45 CAT.6 UTP. Do integračního koncentrátoru Dálkové diagnostiky technologických systémů DDTS bude připojeno záznamové zařízení NVR přes datovou síť/strukturovanou kabeláž. Projektová dokumentace DDTS je řešena v části D.1.2.10.

Systém VVS bude připojen na dohledové pracoviště. Umístění tohoto dohledového pracoviště však není ze strany SŽ určeno. Nepředpokládá se, že dohledové pracoviště bude u soukromé bezpečnostní agentury.

V budově bude umístěna PC pracovní stanice s monitorem 27" pro práci se systémem VVS (pro práci v on-line i se záznamem). Přesné umístění PC sestavy bude určeno před realizací.

19" rozvaděč VVS bude umístěn v rozvodně slaboproudu A.1.3.03. Rozvaděč bude půdorysného rozměru 800x800mm o výšce 47U, bude uzamykatelný a bude vybaven dveřním kontaktem připojeným do systému DDTS.

IP kamery budou ve zodolněném venkovním provedení. Kamery budou disponovat rozlišením min 4MPx. Kamery budou vybaveny motorzoom objektivem s ohniskovou vzdáleností minimálně 2,8÷10mm a IR osvětlením.

### 2.1.3. Rozmístění kamer

Pro výpravní budovu je tímto projektem navrženo instalovat celkem 27 kamer.

K.01-K.04 – Kamery umístěny na fasádě budovy. Budou sledovat prostor ulice před budovou a zároveň fasádu budovy vč. vstupů do výpravní budovy.

K.05 – Kamera umístěna na fasádě objektu, bude sledovat prostor před vstupem do pasáže D.1.0.01 a podchodem

K.06 – kamera umístěna na fasádě, bude sledovat fasádu objektu a stojany s jízdními koly

K.07-K.11 – kamery umístěny na fasádě, budou sledovat prostory nástupiště před budovou

K.12 – kamera umístěna na stropě, bude sledovat prostor podchodu a výstup z výtahu

K.13 – kamera umístěna na stropě, bude sledovat prostor před vstupem do pasáže a vstup do výtahu

K.14 – umístěna v kabině výtahu, bude sledovat prostor kabiny výtahu

K.15 – umístěna na stropě, bude sledovat celý prostor pasáže D.1.0.01 vč. výdejních boxů

K.16, K.17 – umístěny na stěně, budou sledovat prostor pasáže B.1.0.01

K.18, K.19 – umístěny na stěně, budou sledovat celý prostor odbavovací hala C.1.0.01

K.20 – umístěna na stěně, bude sledovat halu s přepážkami prodeje jízdenek

K.21 – umístěna na stěně, bude sledovat předsíň vstupu do objektu A

K.22 – umístěna na stěně, bude sledovat chodbu vč. vstupu do výtahu

K.23 - umístěna na stěně, bude sledovat chodbu a vstupy do rozvoden

K.24 – umístěna na stropě, bude sledovat především vstup do prostoru sklepa A.0.3.01

K.25 – umístěna na stropě, bude sledovat především vstup do prostoru technické místnosti A.0.1.03

K.26 - umístěna na stropě, bude sledovat sklep B.0.2.03 a především vstup do prostoru kolektoru C.0.0.01

K.27 – umístěna na stropě, bude sledovat především vstup do prostoru sklepa B.0.2.05c

K.28 – umístěna na stěně nade dveřmi, bude sledovat turniket na vstupu do WC

### 2.1.4. Rozvody

Metalické rozvody ke kamerám budou provedeny nestíněným kabelem U/UTP 4x2x0,5 CAT.6. Kamery, které jsou od 19" rozvaděče vzdálenější než 90m budou napojeny přes PoE Extender pro prodloužení dosahu. Kamery připojené přes PoE extender budou napájeny ze zdroje s minimálně 14 výstupy 1,1A jištěnými pojistkami a se záložním akumulátorem 17Ah (viz výkresová část). Napájecí zdroj bude umístěn v 1.PP ve sdělovací místnosti B.0.2.05c.

Všechny kamery namontované na fasádě objektu budou do NVR připojeny přes přepětové ochrany.

Kabelové trasy budou v místnostech s podhledy vedeny nad podhledem ve svazkových držácích, svody z podhledu ke kamerám budou v ohebných trubkách pod omítkou. V místnostech bez podhledu budou kabely v ohebných trubkách pod omítkou. Při souběhu kabelů kamerového systému VSS se silovými rozvody musí být zachována minimální vzdálenost 20cm, při souběhu kratším než 5m lze odstup snížit na 6cm a při křížování vedení nejméně 1cm. Prostupy všemi požárními stěnami a stropy je nutné požárně utěsnit na požární odolnost PROSTUPUJÍCÍ KONSTRUKCE. Každá požární ucpávka bude označena identifikačním štítkem.

### 2.1.5. Aktivní prvky

V 19" rozvaděči bude namontován switch s podporou napájení PoE s možností vložení až 4 SFP modulů.

Veškeré aktivní prvky musí být navrženy v souladu s Pokynem generálního ředitele č. 21/2017 (dálková konfigurace, dohled, bezpečnost...). Musí být použita buď zařízení téhož typu jako zařízení provozovaná v současnosti, nebo zařízení jiného schváleného typu, splňující podmínku plné kompatibility se stávajícím řídicím a dohledovým systémem a se stávajícími zařízeními.

Typ PoE switchů pro kamerový systém je nutné nejprve nechat schválit od budoucího správce.

### 2.1.6. Měření kabeláže

Po ukončení montáže bude dodavatelem provedeno měření metalické kabeláže. Kamery budou očíslovány a toto číslování bude popsáno také na patch panelu. Toto označení musí korespondovat s konečnou projektovou dokumentací předávanou uživateli systému. Stejně označení bude použito i na měřících protokolech.

Po ukončení montáže bude dodavatelem provedeno měření metalické kabeláže. Kabeľy s konektory RJ45 u kamer musí být označeny kódem, podle kterého lze jednoznačně určit příslušnou pozici na patch panelu v příslušném rozvaděči. Toto označení musí korespondovat s konečnou projektovou dokumentací předávanou uživateli systému. Stejně označení bude použito i na měřících protokolech.

Po provedení veškerých instalačních prací je třeba prověřit funkčnost celého systému certifikovanými měřeními. Měřit je nutné následující parametry:

- mapa linky
- stejnosměrný odpor
- délka
- kapacita
- útlum
- dual next (útlum přeslechu na blízkém a vzdáleném konci)
- ACR (minimální odstup)
- ztráty odrazem
- impedance
- zpoždění vlivem šíření

Protokol měření musí obsahovat identifikaci měřeného bodu, u každého měřeného parametru limitní a naměřenou hodnotu, viditelně označený výsledek testu, originální otisk razítka firmy, která měření prováděla a podpis pracovníka, který měření provedl. Protokoly o měření budou dokladem o správném zapojení jednotlivých komponentů.