Příloha 1a Smlouvy

TECHNICKÉ SYSTÉMY FYZICKÉ OCHRANY

- TECHNICKÁ SPECIFIKACE -

AKCE:	**Modernizace bezpečnostních systémů areálu MV ČR Nad štolou 936/3**
Investor:	Zařízení služeb pro Ministerstvo vnitra Přípotoční 300, 101 01 Praha 10, IČ: 67779999
Účel:	Pro vnitřní potřebu
Vypracoval:	Ing. Tomáš Mikula Valdecká 82 268 01 Hořovice www.tmproject.cz
Datum zpracování:	04/2015

SEZNAM ZMĚN

č. změny	Předmět změny	Platnost od	Schválil
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Obsah

ÚVOD

Tento dokument je podkladem projektu „Modernizace bezpečnostního systému MV-ČR Nad štolou“. Předmětem je *technická specifikace* (dále jen TS) požadavků na *technické systémy fyzické ochrany* (dále jen TSFO). **TS slouží jako závazný výchozí podklad pro následnou fázi projektových prací. TS je nedílnou součástí zadávací dokumentace.**

POJMY, DEFINICE A ZKRATKY

Aplikace	dle ČSN CLC/TS 50398 označení pro jednotlivé TSFO
Bezpečnost	je stav, kdy velikost všech rizik v organizaci je na přijatelné (akceptované) úrovni, tj. rizika jsou optimalizována
Bezpečnostní systém	je nástroj k zajištění bezpečnosti v organizaci
Falešný poplach	poplach, jehož příčinu nelze jednoznačně určit
Interoperabilita	schopnost různých systémů a aplikací vzájemně spolupracovat, komunikovat, poskytovat si služby a dosáhnout vzájemné součinnosti
Kompatibilita	schopnost různých zařízení pracovat dohromady, zařízení mají shodná rozhraní pro vzájemné propojení
Planý poplach	poplach, u kterého je známa příčina, ale nebyl vyvolán vloupáním nebo pokusem o vloupání/vniknutí do střeženého prostoru
Shoda	Stav úplného souladu dle daných kritérií
Standard	Označení pro parametrický standard TSFO v této TS
Systém	dle ČSN CLC/TS 50398 označení pro celý IPS, součástí Systému jsou jednotlivé Aplikace
Threat levels	Označení funkce řízení ACS dle aktuální úrovně ohrožení, funkce umožňuje autorizovanému operátorovi jednoduše a rychle změnit (přepnout) chování celého systému ACS nebo jeho určitých částí v reakci na změnu bezpečnostní situace, tj. jsou předpovězeny nebo dokonce detekovány jiné hrozby s cílem útoku na chráněné osoby a/nebo aktiva

ACS	Systém kontroly vstupu (elektronický)
AR	Analýza rizik
ARC	Poplachové přijímací centrum
ATE	Poplachové přenosové zařízení
ATS	Poplachový přenosový systém
BOZP	Bezpečnost a ochrana zdraví při práci
CCTV	Původní označení pro VSS
ČSN	Česká technická norma
DNS	Dokumentace návrhu/studie stavby dle VF 2
DPS	Dokumentace pro provádění stavby (stupeň PD dle SZ)
DSP	Dokumentace pro stavební povolení (stupeň PD dle SZ)
DVR	Zařízení pro digitální záznam analogového obrazu
EPS	Elektrická požární signalizace (PBZ)
EZS	Původní označení pro PZTS

FOV	Zorné pole kamery VSS (Field of view)
H.264	Video kodek, standard ISO ITU-T MPEG-4 Part 10
iLIDS	Knihovna videozáznamů pro testování/certifikaci VCA pro vládní účely UK (imagery Library for Intelligent Detection Systems)
IP	Internet Protocol (síťový protokol vrstvy OSI L3)
IPS	Integrovaný poplachový systém
JPEG	Expertní sdružení pro fotografii (Joint Photography Experts Group)
LP	Ochrana před bleskem (Lightning Protection)
MJPEG	Video kodek, standard ISO IEC (Motion JPEG)
MPEG4	Kodek pro proudové video sdružení filmových expertů (Moving Picture Experts Group)
MZP	Mechanické zábranné prostředky
MZS	Mechanické zábranné systémy
MVČR	Ministerstvo vnitra České republiky
N/A	Neaplikovatelné (funkce, vlastnost, kritérium)
nePBZ	označení pro zařízení, které nesplňují podmínky PBZ
neTSFO	označení pro systémy, které nespadají pod TSFO
NVR	Síťové zařízení pro záznam digitálního obrazu
OOÚ	Ochrana osobních údajů
PBZ	požárně bezpečnostní zařízení (vyhrazená požární zařízení dle předpisů požární ochrany)
PČR	Policie ČR
PD	Projektová dokumentace
PIDS	Perimetrický detekční systém
PO	Požární ochrana
PTZ	Polohovatelná (pan/tilt) a zoomovací (zoom) kamera VSS
PZTS	Poplachový zabezpečovací a tísňový systém (I&HAS)
RDS	Realizační (dodavatelská) dokumentace stavby
REX	Zařízení žádosti o uvolnění místa přístupu (Request-to-exit device)
RTP	Síťový protokol pro přenos videa (Real-time Transport Protocol)
RTSP	Síťový protokol pro přenos videa (Real Time Streaming Protocol)
ŘJ	Řídící jednotka
SDO	Organizace pro vývoj standardů/norem (Standards Developing Organization)
SPD	Soupis prací a dodávek dle VF 6
STP	Stavebně technický průzkum dle metodiky ZSMV
STS	Studie stavby (stupeň PD, také pod označením DNS)
SZ	Stavební zákon (z. č. 183/2006 Sb., ve znění pozdější předpisů vč. prováděcích vyhlášek)
TSFO	Technický systém fyzické ochrany (poplachový systém k ochraně života a zdraví osob a zvířat, k ochraně majetku a prostředí/environment)
ÚOOÚ	Úřad pro ochranu osobních údajů
VCA	Objektová analýza v obraze (Video Content Analysis)
VF x	Výkonová fáze Standardu profesních výkonů ČKAIT
VSS	Video dohledový systém (dříve CCTV)
ZOOÚ	Zákon o ochraně osobních údajů, v platném znění

ZOV	Zásady organizace výstavby
ZSMV	Zařízení služeb pro Ministerstvo vnitra, IČ: 67779999

1. SOUČASNÝ STAV

V současné době se v objektu nachází technicky zastaralé TSFO jak z pohledu technického stavu, tak z pohledu bezpečnosti. Některé části systému jsou dokonce nefunkční. Současný stav TSFO v objektu spolu se zvýšenými nároky na bezpečnost objektu vyvolal potřebu komplexní modernizace všech stávajících TSFO.

2. POŽADOVANÉ ŘEŠENÍ

Cílem projektu je vedle nezbytné modernizace také využití nejmodernější techniky k docílení komplexního integrovaného poplachového systému (IPS).

3. KVALITATIVNÍ POŽADAVKY

Veškeré projekční a dodavatelské činnosti/práce budou v souladu s právním řádem ČR a touto TS**. Investor požaduje**, aby kvalita veškerých služeb a výstupů byla v souladu:

- s řádnou praxí v daném oboru;
- s platnými právními předpisy ČR;
- s propozicemi a instrukcemi výrobců a distributorů jednotlivých materiálů, hmot a zařízení;
- s technickými normami včetně doporučených ČSN v jejich posledních vydáních (edicích);
- metodikou ČKAIT pro projektování staveb, tj. Standardů profesních výkonů (verze 06/2014)
- se Standardy ZSMV.

<u>Veškeré projekční práce musí být:</u>

- Kompletní
- Jednoznačné
- Srozumitelné
- **Ve standardu BIM** (úroveň/stupeň/podrobnost/technologii stanoví investor, resp. jím pověřený BIM manažer)

4. POŽADAVKY NA ROZSAH

Konkrétní požadavky na rozsah nasazení (instalace) jednotlivých TSFO budou řešeny v rámci DNS a upřesněny v DPS.

5. FUNKČNÍ POŽADAVKY

Funkční požadavky jsou klíčovým dokumentem pro projektanty a návrháře. Definují představy (potřeby, odůvodnění a účel) zákazníka, jak má systém pracovat. Definice funkčních požadavků vede k jasnému názoru na **co, kde, kdy, kým a** zejména **proč bude systém použit**. V příslušných vývojových etapách (VF) je nutné provádět kontroly, aby se zabezpečilo, že navrhovaný systém bude vyhovovat funkčním požadavkům, tj. svému účelu.
Funkční požadavky nevznikly na základě předem vypracované analýzy rizik nebo jejího auditu, ale na základě konkrétních požadavků kompetentních zástupců investora. To znamená, že tato TS není výsledkem analýzy ochranných opatření, ale omezuje se na definici technického rámce projektu, resp. části projektových prací.
Dále uvedené **funkční požadavky jsou pro celý rozsah projektu závazné**. Funkční požadavky neobsahují požadavky na rozsah aplikací/systémů, bude předmětem DNS a finálně upřesněno v DPS. Veškeré případné odchylky budou diskutovány a prokazatelně odsouhlaseny investorem.

5.1. FUNKČNÍ POŽADAVKY - MECHANICKÉ TSFO

Funkční požadavky na MZP/MZS upřesní investor.

Předpokládají se následující typy MZP/MZS:

- Road blocker (vjezd do garáží)
- Výplně otvorů na plášti budovy objektu (okna, dveře, brány, vrata apod.)
- Vjezdové závory

5.2. FUNKČNÍ POŽADAVKY - ELEKTRONICKÉ TSFO

5.2.1. Integrovaný poplachový systém (IPS)

Integrovaný poplachový systém (IPS) integruje všechny navržené TSFO do jednotné integrační platformy.
Cíle, jichž má být dosaženo integrací:

- zvýšení bezpečnosti objektu díky jednotné, přehledné a flexibilní integrační platformě sdružující všechny TSFO, a to jak nePBZ tak PBZ (tj. vč. EPS apod.)
- možnost integrovat/kombinovat TSFO s neTSFO
- možnost optimalizace manuálních a zautomatizovaných operací mezi jednotlivými TSFO
- vyšší efektivita práce ostrahy – uživatelsky orientované prostředí
- efektivní prioritizace činností a obsluhy
- bezprostřední informovanost kompetentních pracovníků
- možnost vzájemné verifikace poplachů z jednotlivých TSFO
- zjednodušení administrace a přehledu o všech TSFO
- možnost flexibilní delegace povinností
- redukce dodavatelů
- jednotná a komplexní dokumentace
- garance cen budoucích rozšiřování
- pomoc při vypracování směrnic

Následující funkční požadavky vychází z těchto oborových technických norem:

ČSN CLC/TS 50398:2009	Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky

ČSN CLC/TS 50398

- musí být provedena **volba typu konfigurace** vč. vypracování základního integračního schéma dle normy, a to vč. PBZ (EPS atd.) a ostatních neTSFO správy budovy požadovaných investorem (MaR, výtahy atd.)
- pro TSFO musí být použity oborové technické normy uvedené v požadavcích jednotlivých aplikací této TS
- ATS nepatří/nejsou zahrnuty do této normy – nejsou součástí IPS
- společná zařízení, která nejsou obsažena v aplikačních normách, musí splňovat tuto normu
- definice provozních podmínek pro celý IPS, zejména povelové řízení a posouzení dopadů/vlivů při nesprávné činnosti/poruchách bude součástí akceptačních testů provedených při výběru technologie na demo sestavě
- prioritizace signalizace dle čl.5.3.3 normy
- jsou-li k TSFO připojena zařízení, která nesplňují aplikační normy, tak nesmí TSFO ovlivňovat
- jsou zpracovány jen signály povolené normou a jsou chráněny proti sabotáži, pokud si to stav žádá
- mají být prověřeny/zkontrolovány zvlášť jednotlivé systémy a zvlášť IPS jak v normálním stavu, tak poruchovém - akceptační testy
- přenosové trasy v rámci každého TSFO musí splňovat normy
- porucha společného zařízení nebo prvku musí být indikována ve všech dotčených aplikacích
- napájecí zdroje společných zařízení, tras a vyhodnocovacích prvků nesmí ohrozit požadavky dle příslušných aplikačních norem
- musí být vypracovány školící manuály pro obsluhu IPS a znalosti pravidelně přezkušovány
- směrnice pro montáž, provoz a spolehlivost viz příloha A normy

Ostatní funkční požadavky:

- základem IPS vícevrstvá architektura klient-server (multiple client)
- otevřená systémová architektura umožňující integrovat systémy třetích stran

- IPS musí být provozován na technickém vybavení běžně dostupném v obchodní síti
- podpora průběžné replikace databáze pro případ obnovení provozu po výpadku
- IPS nesmí být nijak nepříznivě ovlivněn nefunkčností jednoho nebo více TSFO
- podpora redundance jakékoli části systému
- podpora libovolného počtu aktivních signalizačních prvků
- IPS bez omezení z hlediska počtu současných výstražných událostí (poplachů, poruch atd.)
- operátor IPS musí mít možnost, dle nastavených přístupových práv, ovládat z IPS všechny TSFO
- podpora min. 3 úrovní Threat levels
- administrace/správa společné přenosové trasy (sítě) z IPS výhodou, nikoli podmínkou
- IPS musí poskytovat grafické uživatelské rozhraní, umožňující jeho přizpůsobení dle potřeb jednotlivých pracovišť a uživatelů
- veškeré výstražné signalizace musí být zobrazovány na interaktivních mapách objektu
- IPS musí umožňovat import grafických map v různých souborových formátech
- IPS musí umožňovat propojení několika map různých lokalit/provozů/budov
- podpora libovolného počtu úrovní priorit výstražných signalizací
- výstražná signalizace musí umožňovat automatické otevření příslušné (propojené) mapy v dané lokalitě
- výstražná signalizace musí umožňovat automatickou aktivaci zobrazení videosignálu z předem určených kamer VSS
- IPS musí vyžadovat odbavení výstražné signalizace potvrzením události s poznámkami operátora
- výstražnou signalizaci musí být možné dočasně vypnout (např. během údržby)
- podpora vícemonitorového zobrazení
- IPS musí být vybaven funkcí samokontroly a generovat hlášení o jakékoli závadě na záložních nebo primárních součástech
- objekty by mělo být možné organizovat do několika struktur, umožňujících tyto objekty seskupovat podle různých kritérií (funkčních, fyzických, logických)
- podpora libovolného počtu uživatelských úrovní vč. skupinování
- při přihlašování do IPS povinnost ověření práv uživatele (autorizace)
- IPS musí zaznamenávat do protokolu veškerou výstražnou signalizaci
- IPS musí zaznamenávat do protokolu veškerou činnost operátora IPS
- s žádnými záznamy v protokolu ani s videozáznamy v rámci IPS nesmí být možné neoprávněně manipulovat
- podpora přímého přehrávání videozáznamů spojených se zaprotokolovanými událostmi a výstražnými signalizacemi
- databáze uživatelů musí být jednotná a samostatná pro IPS (pouze TSFO), případná db komunikace s neTSFO bude řešena v DNS a upřesněna v DPS

5.2.2. Poplachový zabezpečovací a tísňový systém (PZTS)

Následující funkční požadavky vychází z těchto oborových technických norem:

ČSN EN 50131-1 ed.2:2007	Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky
ČSN CLC/TS 50131-7:2011	Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace

TNI 33 4591-1:2012	Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - Část 1: Návrh systému PZTS – Komentář k ČSN CLC/TS 50131-7:2011

Výše uvedené normy vychází ze stejné řady a **platí pouze pro PZTS instalované v budovách** (vč. venkovních doplňkových ovládacích zařízení a akustických výstražných zařízení). **Neplatí vně budov**, např. pro PIDS nebo jiné venkovní detekční systém, byť jsou instalovány v těsné blízkosti budovy (na fasádě apod.).

ČSN EN 50131-1 ed.2

- zvolený systém, jeho komponenty a rozsah nasazení musí prokazatelně odpovídat danému stupni zabezpečení (st. 1 až 4) dle čl.6 normy
- **Standardem** pro komponenty a rozsah nasazení **je 3. stupeň zabezpečení** (přímý požadavek investora)
- zvolené komponenty musí pro správnou a spolehlivou práci prokazatelně splňovat požadavky dané třídy prostředí (I až IV) dle ČSN EN 50130-5
- zvolené komponenty musí prokazatelně splňovat výrobkové normy, pokud existují (ČSN EN 50131-2 až -6)
- systém musí umožňovat signalizaci a rozpoznání poruch následujících typů/zařízení bez závislosti na daném stupni zabezpečení: detektory vniknutí, tísňové prostředky, základní napájecí zdroj, náhradní napájecí zdroj, propojení, ATS/ATE, výstražné zařízení
- pro stupně zabezpečení 3 a 4 musí být detektory pohybu vybaveny detekcí zakrytí/maskování
- pro jednotlivé funkce systému musí odpovídat úroveň přístupu dle čl. 8.3.1 normy (úrovně: 1 – přístup pro kohokoli, 2 – přístup pro uživatele typu obsluha, 3 - přístup pro uživatele typu servis, 4 - přístup pro uživatele typu výrobce zařízení), přístupové úrovně k jednotlivým funkcím viz tab.2 normy
- požadavky na kódy oprávnění ve vztahu k úrovní přístupu a stupni zabezpečení musí odpovídat tab.3 normy
- systém musí být navržen tak, aby byla minimalizována možnost vyvolání planého poplachu uživatelem
- při návrhu musí být věnována zvláštní pozornost minimalizaci vzniku falešných poplachů (poplachy bez zjevné příčiny)
- zpracování signálů/zpráv vniknutí, tísně, sabotáže, poruchy a zakrytí musí odpovídat tab.7 normy
- stav tísně, vniknutí, sabotáže a poruchy musí být hlášeny pomocí ATS a/nebo akustickým výstražným zařízením dle tab. 10 a tab.11 normy
- akustické výstražné zařízení musí být v činnosti po dobu nejméně 90s, nejdéle 15min
- hlášení poruchy základního napájecího zdroje může být zpožděno max. o 1h
- je-li součástí systému ATS/ATE, musí splňovat ČSN EN 50136 (ATS1 až ATS6)
- požadavky na detekci sabotáže komponentů dle tab.12 a tab.13 normy
- detekce sabotáže musí být ve všech stupních zabezpečení účinná ve stavu střežení i klidu
- nespecifická/sdílená propojení (např. TCP/IP over ethernet) musí splňovat požadavky čl. 8.8 normy
- všechny napájecí zdroje musí splňovat ČSN EN 50131-6 ed.2, primárně požadavek na využívání zdroje typu A (výjimečně typ C, typ B nepřípustný)
- požadavky na náhradní zdroj dle tab.23 a tab.24 normy
- všechny komponenty systému musí splňovat z pohledu EMC normu ČSN EN 50130-4

ČSN CLC/TS 50131-7

- **Návrh** systému bude splňovat požadavky čl. 7 normy, předmětem je: vnější vlivy – uvnitř/vně, volba a umístění jednotlivých zařízení/komponent, propojení, princip uvádění do stavu střežení a klidu, příchodové a odchodové trasy, indikace, sdružování detektorů, hlášení poplachu, napájení, odezva na poplachové a poruchové hlášení, prováděcí/realizační dokumentace
- **Montáž** systému bude splňovat požadavky čl.8 a čl.9 normy, předmětem je: doporučení výrobce(ů) komponent, ověření správnosti STP, výrobní dokumentace
- **Kontrola a funkční zkouška** bude splňovat požadavky čl. 10 normy, předmětem je: finální prohlídka, funkční zkouška, předání uživateli, zkušební provoz, dokumentace skutečného provedení
- **Provoz a údržba** bude splňovat požadavky čl. 11, čl. 12 a čl. 13 normy, předmětem je: předávací dokumentace, provozní kniha, servisní smlouva, program údržby, pravidelné funkční zkoušky
- V rámci daného STP bude posouzení budovy dle přílohy C normy
- V rámci daného STP bude posouzení vnějších vlivů na systém s původem uvnitř střežených prostor dle přílohy D normy
- V rámci daného STP bude posouzení vnějších vlivů na systém s původem vně střežených prostor dle přílohy E normy
- V rámci daného STP bude posouzení komponentů systému dle přílohy H normy
- Standardem rozsahu/úrovně střežení podle jednotlivých stupňů zabezpečení je tab F.1 normy

Vzít v úvahu	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	O+P	O+P
Okna		O	O+P	O+P
Ostatní otvory		O	O+P	O+P
Stěny				P
Stropy nebo střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předmět (vysoké riziko)			S	S
Legenda O = otevření P = průnik (tj. dohled na stavební komponenty pro detekci narušení nebo pokusu o narušení) S = objekt, vyžadující zvláštní pozornost T = past (tj. dohled ve vybraných prostorech, v nichž je vysoká pravděpodobnost detekce)				

Tab.1 Úrovně střežení pro jednotlivé stupně zabezpečení; zdroj: tabulka F.1 normy

- Provozní kniha systému bude vypracována/pořízena v rozsahu dle doporučení přílohy I normy
- Servisní smlouva bude obsahovat požadavky na provádění pravidelných funkčních zkoušek dle přílohy J normy

TNI 33 4591-1
- montáž a údržba systému bude v souladu s TNI 33 4591-2 a TNI 33 4591-3
- vzorové zabezpečení objektu pro jednotlivé stupně zabezpečení dle přílohy B,C,D,E normy

Ostatní funkční požadavky
- interoperabilita se zvolenou technologií integrační platformy IPS
- v odůvodněných případech přípustná varianta přenosu poplachových smyček detektorů do ústředny PZTS přes společnou přenosovou síť
- interoperabilita rozhraní RS485 a digi I/O s vybranou technologií společné přenosové trasy ve funkci nespecifického propojení
- připojení detekce na úrovni perimetru vnějšího pláště budovy objektu (viz PIDS)

5.2.3. Perimetrický detekční systém (PIDS)

Perimetrický detekční systém (PIDS) není v současné době v objektu provozován. Nicméně v rámci koncepce IPS je nutné s PIDS počítat jako s dalším TSFO, který bude možné v budoucnu nově nasadit a v rámci IPS provozovat.
V současné době nejsou k dispozici žádné technické normy (SDO), podle kterých by bylo možné stanovit základní normativní funkční požadavky. Existují pouze speciální/účelové certifikace a podnikové normy/standardy výrobců. Vzhledem k rozmanitosti a proprietárnosti jednotlivých PIDS řešení a technologií, se omezíme pouze na základní požadavek integrace s vybranou technologií IPS.
Nicméně byly identifikovány požadavky investora na částečnou (úsekovou) detekci na úrovni perimetru vnějšího pláště budovy objektu. Tuto detekci se předpokládá připojit na úrovni poplachových smyček do PZTS.

Funkční požadavky
- interoperabilita se zvolenou technologií integrační platformy IPS
- přípustná jak varianta připojení PIDS pod PZTS (tj. jako poplachové smyčky) nebo přímo do společné přenosové sítě (I/O síťového zařízení – přepínače)
- v rámci STP budou u vybrané technologie PIDS výrobcem dodány/určeny parametry, které budou za součinnosti investora posouzeny:
    - **Pd** (Probability of detection) – pravděpodobnost detekce [%]
    - **NAR** (Nuisance Alarm Rate) – četnost planých poplachů [#/time]
    - **FAR** (False Alarm Rate) – četnost falešných poplachů [#/time]
    - **Vd** (Vulnerability to defeat) – pravděpodobnost/zranitelnost překonání

- v případě použití detekce pomocí VCA (z kamer) je požadována certifikace **iLIDS** (Sterilní zóna) nebo obdobná oborově uznávaná zkouška založená na testování pomocí testovacích video smyček

5.2.4. Video dohledový systém (VSS)

Následující funkční požadavky vychází z těchto oborových technických norem:

ČSN EN 62676-1-1:2014	Video dohledové systémy pro využití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně
ČSN EN 62676-1-2:2014	Video dohledové systémy pro využití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky – Výkonové požadavky na video přenos
ČSN EN 62676-2-1:2014	Video dohledové systémy pro využití v bezpečnostních aplikacích – Část 2-1: Video přenosové protokoly – Obecné požadavky
ČSN EN 50132-7 ed.2:2013	Poplachové systémy – CCTV dohledové systémy pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace

V době vypracování docházelo k postupnému přechodu/nahrazování norem řady ČSN EN 50132 řadou ČSN EN 62676. Toto je současný stav. Norma ČSN EN 50132-7 ed.2 bude nahrazena normou ČSN EN 62676-4. Stejně tak bude ČSN EN 50132-5-3 nahrazena ČSN EN 62676-3 (Analogové a digitální video rozhraní). V rámci revizí tohoto dokumentu budou normativní požadavky upraveny dle aktuálního stavu norem.

ČSN EN 62676-1-1

- zvolený systém, jeho komponenty a funkce musí prokazatelně odpovídat danému stupni zabezpečení (st. 1-4) dle čl.5 normy
- **Standardem** pro komponenty a funkce systému **je 3. stupeň zabezpečení** (přímý požadavek investora), požadované odchylky od standardu jsou vyjádřeny v tab.2

Funkce VSS	Požadovaný stupeň zabezpečení
Vzájemná propojení	3
Ukládání (tab.1 normy)	4
Archivace a zálohování (tab.2 normy)	4
Systémové logy (tab.3 normy)	3
Zálohování a obnova systémových dat	3
Oznámení opakujících se selhání	3
Sledování zdroje napájení pro zařízení ke zpracování obrazu	4
Čas přídrže obrazové vyrovnávací paměti (bufferu)	3
Monitorování propojení (tab.4 normy)	4
Detekce narušení (tab.5 normy)	3
Ochrana kamerových krytů proti neoprávněné manipulaci	3
Požadavky na autorizační kódy (tab.7 normy)	3
Časová synchronizace	3
Autentizace dat	3
Autentizace exportu/kopie	3
Označování dat (tab.11 normy)	3
Ochrana před manipulací s daty	4

Tab.2 Funkce VSS a požadavky na stupeň zabezpečení

- zvolené komponenty musí prokazatelně splňovat výrobkové normy, pokud existují
- jednotlivé funkce VSS mohou použít různý stupeň zabezpečení, stejně tak ochrana proti sabotáži (čl. 6.3.2.3 normy)
- požadavky na zpracování obrazu a exportu snímků dle čl. 6.1.3.5 až 6.1.3.12 normy
- požadavky na správu událostí dle čl. 6.2.2.3 normy
- přesné a kompletní systémové logy musí být udržovány po dobu 6 měsíců
- všechny systémové bezpečnostní požadavky definované v čl. 6.3 normy musí být dodrženy i v případech, kdy je VSS přístupný a řízený jiným systémem; jiný systém musí být vnímán jako systémový uživatel s definovanými přístupovými právy
- VSS nebo jeho logická část se stupněm zabezpečení 3 a 4 musí být schopen zálohovat a obnovit veškerá systémová data
- VSS nebo jeho logická část musí být schopen regulérně ukončit provoz v definované proceduře bez ztráty uložených dat; pro stupně zabezpečení 3 a 4 nesmí být snímky uloženy ve vyrovnávací paměti po dobu delší než 5 vteřin bez zápisu na paměťové médium
- pro stupně zabezpečení 3 a 4 musí VSS zvládnout selhání zařízení tak, že indikuje jakékoliv selhání základních funkcí do 100 sekund od selhání
- povinné detekce narušení pro stupeň zabezpečení 3 a 4: změna pozice kamery, zasprejování
- zařízení snímající obraz (např. kamery) ve stupni zabezpečení 3 a 4 musí být chráněny proti narušení; kamery by měly být umístěny mimo dosah a fixační šrouby krytů musí být odolné proti neoprávněné manipulaci za účelem zamezení neautorizovaného přemístění kamer
- zařízení snímající obraz, nabízející ochranu proti vandalismu, musí splňovat následující minimální kritéria:

1. Minimální IP stupeň 44 v souladu s normou IEC 60529;
2. Kladivové testy v souladu s IEC 60068-2-75
   Údery musí být směřovány na hlavní části, jako je kryt, objektiv apod. Při testech odolnosti proti fyzickému napadení musí být pro všechny testy zařízení namontováno dle instrukcí výrobce na pevném podstavci definovaném v IEC 62262. Každý test musí být proveden jednou osobou.
3. IK stupeň 07;
4. Odolnost minimálně po dobu 1 minuty proti:
   - uvolnění zařízení povolením fixačním šroubů;
   - vytažení zařízení;
   - útoku s jednoduchým nástrojem, jako je šroubovák o průměru 4 až 7 milimetrů a 60 až 200 milimetrů dlouhém;
   - útoku jednoduchým nástrojem, jako jsou kleště;
   - útoku zapalovačem aplikací tepla

5. Odolnost proti útoku politím sladkokyselým nápojem za použití 0,3 l komerčního nealkoholického nápoje. Polovinou obsahu se polije zařízení a zbytek se nastříkání na spodní stranu zařízení.
6. Po všech testech musí zařízení nadále normálně pracovat.

- požadavky na úroveň přístupu: Pro každý VSS musí přístup k obsluze a datům být řízen autorizačním schématem (úroveň 1 – pro jakoukoli osobu, úroveň 2 – pro jakéhokoli uživatele, úroveň 3 – pro administrátora(y) systému, úroveň 4 – pro servis nebo výrobce), a to dle čl. 6.3.2.4 normy; to zahrnuje také přístup skrze vzdálenou pracovní stanici nebo skrze externí systém integrovaný do VSS
- pro stupně zabezpečení 3 a 4 musí být přesnost nastavení času pro různé prvky VSS v rozmezí $\pm$ 10 sekund od UTC
- VSS nebo jeho logická část ve stupni zabezpečení 3 a 4 musí za účelem ověření integrity snímků a jiných dat, poskytovat metodu k ověření snímků, metadat a jejich identity (např. vodoznak, kontrolní součet, otisk prstu)
- VSS nebo jeho logická část ve stupni zabezpečení 3 a 4 musí poskytovat metodu k ověření autentičnosti kopírovaných a exportovaných dat; použitá autentizační metoda musí být specifikovaná v dokumentaci systému
- VSS nebo jeho logická část ve stupni zabezpečení 4 musí poskytovat metodu (např. šifrování) k zamezení prohlížení snímků a jiných dat neautorizovanými osobami bez povolení; VSS nebo jeho logická část ve stupni zabezpečení 4 musí také poskytovat metodu k ochraně důvěrnosti kopírovaných a exportovaných dat; metoda použitá k ochraně důvěrnosti dat musí být specifikována v dokumentaci systému
- zvolené komponenty VSS musí pro správnou a spolehlivou práci prokazatelně splňovat požadavky dané třídy prostředí (I-IV) dle ČSN EN 50130-5
- zvolené komponenty VSS musí pro správnou a spolehlivou práci prokazatelně splňovat požadavky EMC čl. 6.4.2 normy
- požadavky na kvalitu obrazu: VSS musí používat prvky, které prokazatelně prošly testování dle ISO 12233 za účelem zjištění jejich maximální rozlišovací schopnosti

ČSN EN 62676-1-2
- různé funkce systému mohou mít různé třídy výkonností; výkonnostní třídy jsou nezávislé na bezpečnostních třídách
- hodiny reálného času (RTC) ve video-přenosovém zařízení by měly být synchronizovány s časovým normálem dle doporučení RFC 2030 protokolem SNTP verze 4
- přesnost časových služeb pro transportní video-stream ve třídě T3 dle tab.1 normy
- čas navázání spojení pro každý nový požadavek na video-stream ve třídě I4 dle tab.2 normy
- síťová zařízení (přepínače) ve sdílené síti musí nabídnout prostředky pro konfiguraci ve třídě C3 dle tab.3 normy
- síťová zařízení (přepínače) ve sdílené síti musí nabídnout prostředky pro prioritizaci ve třídě P3 dle tab.4 normy
- přenosová síť musí používat nástroje pro minimalizaci jitteru jak u živého streamu, tak i u streamů ze záznamu (dostatečná šířka pásma, vyrovnávací paměť)
- pro streamování videa a zobrazování streamu požadována třída S3 dle tab.5 normy

- jiter paketů video-streamu ve třídě M4 dle tab.6 normy
- monitorování propojení požadováno ve 4 stupni zabezpečení dle tab.7 normy
- požadovaná spolehlivost bude dosažena v IP video přenosové síti využitím zařízení a sítí se zálohováním, rozdělením zátěže a sdílení pomocí vhodného výběru z těchto řešení:

- Redundantní (zálohovaný) hardware
- Redundantní připojení k síti
- N + n redundance (zálohování)
- Schopnost výměny jednotky za provozu (hot-swap)
- Schopnost zotavit se po poruše u všech složek (fail-over)
- N + 1 fail-over schopnost pro jednu z N stejných dílů
- Žádný bod selhání (SPOF), s výjimkou kamer a kódování
- Duální síťový port zdrojového video zařízení, např. v IP kamerách nebo enkodérech
- Konfigurace, software a firmware, který se může změnit a aktualizovat bez provozního výpadku

- přenosová síť pro VSS musí splňovat požadavek na střední dobu mezi poruchami MTBF min. 16 000 hodin
- řídicí data a video data musí být možné posílat s využitím protokolu TCP/IP dle STD 7 RFC 793 nebo protokolu UDP/IP dle STD 6 RFC 768, tj. podpora UDP a TCP; primárně upřednostňován protokol TCP
- VSS musí podporovat následujících specifikace videostreamování z důvodů kompatibility:
    - JPEG přes RTP
    - MPEG - 4 ve shodě s ISO / IEC 14496-2
    - H.264 ve shodě s ISO / IEC 14496-10
    - ČSN EN 62676-2-2 (shodné s PSIA specifikacemi)
    - ČSN EN 62676-2-3 (shodné s ONVIF specifikacemi)
- podpora správy síťových zařízení pomocí protokolu SNMP v2
- pro VSS používána vyhrazená vlastní informační základna MIB 31373
- požadavky na SNMP správce a agenta čl. 11.3 až čl. 11.5 normy

ČSN EN 62676-2-1

- VSS bude navržen s plnou podporou provozu IP videa dle normy
- Obecné požadavky IP interoperabilitu video přenosových zařízení dle čl. 7.1 normy
- Video přenosové zařízení musí poskytovat prostředky pro:
    - IP připojení v souladu s čl. 7 normy
    - streamování videa v souladu s čl. 8 normy
    - řízení video streamu v souladu s čl. 8 normy
    - přehrávání videa v souladu s čl. 9 normy
    - vyhledání zařízení a jejich popis v souladu s čl. 10 normy
    - upozorňování na událost v souladu s čl. 11 normy

ČSN EN 50132-7 ed.2

- Provozní požadavky (čl. 5.3 normy):
  - *základní účel/funkčnost* – na vybraných místech areálu monitoring pracovníky operačního střediska v reálném čase s cílem přehledu o bezpečnostní situaci vč. vizuální podpory nahlášených událostí (narušení); záznam hrozeb ohrožujících osoby, majetek a prostředí; video verifikace (ex post ze záznamu) poplachových (příp. poruchových) událostí vzniklých z ostatních TSFO (PZTS, ACS)
  - *definice omezení dohledu* – definice předmětem DNS/upřesnění v DPS
  - *definice sledovaných míst* – konkrétní definice sledovaných míst (ROI – region of interest) není na žádost investora předmětem této specifikace, konkrétní posouzení/definice ROI jak uvnitř objektu tak na perimetru vnějšího pláště objektu (vč. střechy) je požadováno provést v rámci DNS/upřesnění v DPS, definice ROI bude provedena pomocí grafického vyjádření (ve výkresové části) vč. textového popisu, perimetrem vnějšího pláště objektu je zde myšlen koridor do max. vzdálenosti cca 100m od pláště budovy
  - *definice sledovaných aktivit* – obecně se jedná o aktivity spojené s neoprávněným vstupem do střeženého/zakázaného prostoru/stavby/provozu, krádeže a vandalismus aktiv, vstupem/výstupem osob do/z areálu, vjezdem/výjezdem vozidel do/z objektu, reakcemi na podněty vyvolané externími událostmi (událostní scénáře), mimořádnými událostmi (bezpečnostního charakteru), konkrétní definice v rámci DNS/upřesnění v DPS
  - *funkční vlastnosti systému/obrazu* – v rámci DNS/upřesnění v DPS bude řešen stupeň rozlišení sledovaného cíle (osoba, předmět, zařízení, technika apod.); v případě osob bude definice provedena dle čl. 6.7 normy; požadavek na funkce analýzy obrazu (VCA) nebyl identifikován
  - *doba provozu* – je požadován provoz VSS v režimu 24/7/365
  - *místní podmínky* – podmínky jako osvětlení scén, potenciální překážky v zorném poli kamer a ostatní vnější vlivy prostředí budou předmětem konkrétního posouzení v rámci DNS/upřesnění v DPS
  - *schopnost za nepříznivých podmínek* – je požadováno kompletní zálohování napájení VSS vč. přenosových tras (dedikovaných i společných), požadované doby zálohy budou předmětem konkrétního posouzení v rámci DNS/upřesnění v DPS
  - *monitorování a ukládání obrazu* – monitorování v reálném čase obsluhou operačního střediska a ostatními oprávněnými klienty; práce se záznamem obrazu pouze oprávněnými pracovníky; definice dob(y) záznamu obrazu bude předmětem DNS/upřesnění v DPS, po uplynutí této doby budou systémem VSS automaticky vymazány; v případě záznamu na základě události (interní/externí) bude v rámci DNS/upřesnění v DPS definována doba záznamu před a po události; nakládání s obrazovými záznamy a daty bude v souladu s předpisy/směrnicemi správce VSS a ZOOÚ; v rámci DNS/upřesnění v DPS bude provedena definice základního schéma provozování streamů z kamer (počet streamů, účel použití, kodek, obrazové rozlišení, snímková frekvence)
  - *export obrazového záznamu* – export záznamu obrazu smí provádět pouze oprávnění pracovníci; definice způsobu(ů) exportu obrazového záznamu bude předmětem DNS/upřesnění v DPS
  - *rutinní činnosti* – definice předmětem DNS/upřesnění v DPS

- *provozní odezva* – provozní odezvy na události jsou spojeny zásadně s pracovištěm operačního střediska a jsou dány dotčenými směrnicemi/předpisy
- *vytížení obsluhy* – definice počtu obrazovek, které má obsluha sledovat bude předmětem DNS/upřesnění v DPS a bude v souladu s návrhem velínu operačního střediska; ostatní klienti VSS budou přistupovat k VSS ze svých pracovních PC; počet poplachových událostí, které má obsluha zvládat odbavit za jednotku času bude předmětem DNS/upřesnění v DPS (tomu bude odpovídat počet pracovníků obsluhy VSS)
- *výcvik* – požadavky na výcvik obsluhy budou předmětem DNS/upřesnění v DPS
- *rozšiřování systému* – výstavba celého VSS vč. jeho rozšiřování bude předmětem etapizace

- Provozní kritéria systému (čl. 5.4 normy):
  - automatizace (ovládání pomocí poplachu, ext. událostí, časových událostí, manuálně):
    - přepínání obrazu – manuálně obsluhou nebo automaticky na základě události
    - přednastavení kamer – automatické přepínání den/noc
    - monitoring zařízení, kontrola správné činnosti – plně automatizováno systémem VSS vč. hlášení poruchy obsluze
    - analýza obrazu – není požadováno; pokud k tomu dojde, tak automaticky pomocí inteligentní SW VCA se spouštěním dle konkrétních požadavků
    - ukládání obrazu – žádné další požadavky na záznam, pro záznam definovat stream
  - odezva na poplach:
    - indikace poplachu musí mít prioritu před všemi ostatními událostmi
    - definice manuálního převzetí ovládání systému obsluhou po poplachu bude předmětem DNS/upřesnění v DPS
    - prezentace poplachových obrazů na určených obrazovkách (spot, fullscreen)
    - manipulace při souběžných poplachových stavech – předmětem DNS/upřesnění v DPS
    - volba kritérií pro ukládání – předmětem DNS/upřesnění v DPS
  - doby odezvy systému (definice akceptovatelných dob)
    - doba mezi generováním poplachu a jeho indikací obsluze – do 0,2s
    - odezva systému musí být v rozmezí od 0 do 0,2s (např. ovládání PTZ kamer)
    - reakční doba pro obsluhu ve velínu k potvrzení příjmu poplachu – do 5s
    - přednastavení PTZ kamer – do 3s
    - změna z průběžného režimu do poplachového režimu záznamu – do 0,5s

- výběr zařízení a funkčních vlastností VSS provést dle čl.6 normy
- požadavky na prezentaci obrazu dle čl.7 normy
- konfigurace řídícího pracoviště (velínu) VSS dle čl.12 normy

Ostatní funkční požadavky

- provoz VSS v souladu se ZOOÚ
- interoperabilita se zvolenou technologií integrační platformy IPS
- pro přenosovou síť VSS bude využito shodné technologie jako u společné přenosové trasy celého IPS, tj. standardu průmyslového ethernetu
- je přípustná platforma NVR jak PC based + SW, tak proprietární HW s tím, že budou splněny požadavky prostředí (vnější vlivy) a schopnost automatického restartu po obnovení napájení po

předchozím výpadku bez nutnosti zásahu obsluhy (tj. do stejného provozního stavu jako před výpadkem napájení)

- Systémové požadavky:
  - dimenzování systému: unlimited cameras, unlimited servers/NVRs, unlimited users
  - teoretický maximální počet kamer v objektu: předmětem DNS/upřesnění v DPS
  - teoretický minimální počet současně připojených klientů: předmětem DNS/upřesnění v DPS
  - česká lokalizace SW
  - licencování po jedné kameře, nelicenovaní (neplacení) klienti
  - podporované video formáty: dle ČSN EN 62676-1-2
  - podpora Mpxls a HD kamer
  - nastavování parametrů systému per kamera
  - podpora ONVIF kompatibilních zařízení (aktuálně Profile S)
  - podpora mobilních klientů: Android, iOS, Windows Mobile
  - podpora archivace na síťové uložiště (NAS)
  - podpora aktivních vrstvených vektorových mapových podkladů
  - podpora failover recording servers (redundance)
  - multistreaming (min. 3 streamy)
  - podpora video data encryption
  - podpora VCA (embeded v kamerách, na serveru)
  - podpora unicast, multicast, QoS
  - video stěna
  - časové sekvence
  - vyhledávání v záznamu pomocí časové osy (timeline) v zobrazení multiscreen
  - VMD zónová analýza záznamu
  - podpora virtuální matice
  - podpora vícemonitorového zobrazení
  - zabezpečení proti poruše paměťového média záznamového zařízení (např. RAID 5 nebo 1 nebo přepnutí na jiné záložní zařízení)
  - autorizace uživatelů/klientů
  - podpora detekce a rozpoznávání RZ vozidel
  - podpora šifrování AES
  - plná podpora PTZ a HW joysticků
  - současné přehrávání z různých NVR/serverů
  - podpora digitálního podpisu záznamu
  - alarmové hlášení SMS, email, SNMP trap
  - automatická aktualizace systému
  - správa událostí
  - centrální správa systému

5.2.5. Systém kontroly vstupu (ACS)

Následující funkční požadavky vychází z těchto oborových technických norem:

ČSN EN 60839-11-1:2014	Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty
ČSN EN 50133-7:2000	Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Pokyny pro aplikace

V době vypracování docházelo k postupnému přechodu/nahrazování norem řady ČSN EN 50133 řadou ČSN EN 60839-11. Toto je současný stav. Norma ČSN EN 50133-7 bude nahrazena normou ČSN EN 60839-11-2. V rámci revizí tohoto dokumentu budou normativní požadavky upraveny dle aktuálního stavu norem.

ČSN EN 60839-11-1

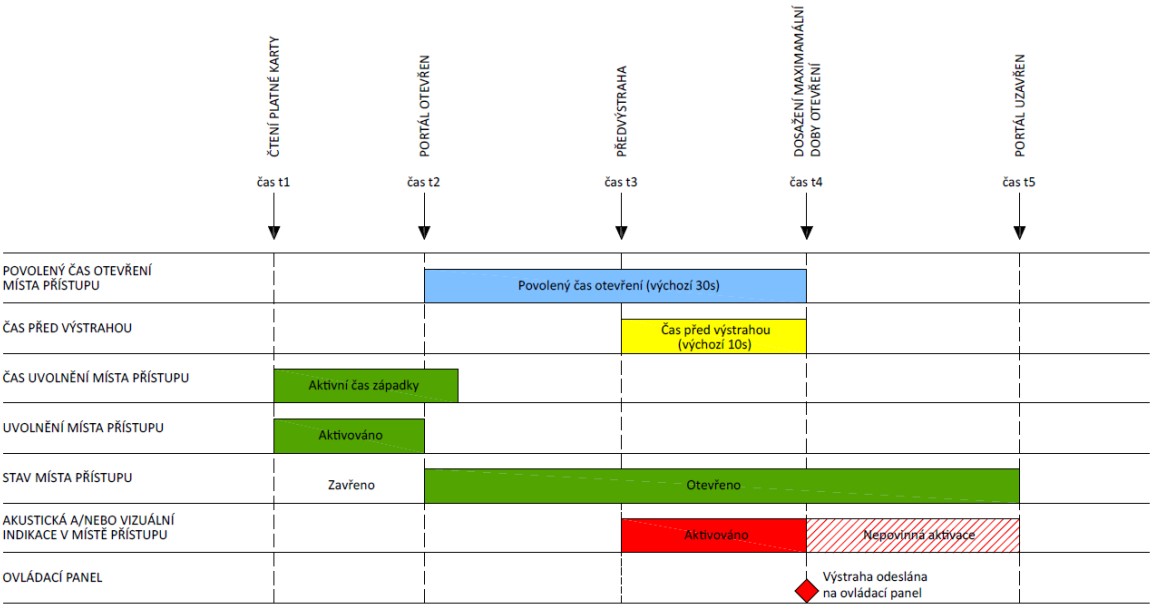
- každé přístupové místo (portál) musí prokazatelně odpovídat danému stupni zabezpečení (st. 1 až 4) dle čl.6.1, tab.1 normy
- **Standardem je 3. stupeň zabezpečení** (přímý požadavek investora)
- klasifikace stupně zabezpečení může být individuálně řešena pro každé přístupové místo
- řídící prvky/funkce celého ACS musí splňovat nejvyšší stupeň zabezpečení z přístupových míst

	Požadavky na rozhraní místa přístupu	**Stupeň zabezpečení**			
		1	**2**	**3**	**4**
	A – Doba uvolnění				
1	Doba uvolnění musí být definována systémem	V/N	V/N	N	N
2	Doba uvolnění musí být pro jednotlivé portály konfigurovatelná	V/P	V/P	P	P
3	Je-li doba uvolnění definována systémem, nesmí být povolená doba kratší než 3 s	P	P	N/A	N/A
4	Je-li doba uvolnění konfigurovatelná, mohou hodnoty pro jednotlivé portály souviset s přístupovými oprávněními systému	V	V	V	V
	B – Kontrola přístupu				
5	Umožnění přístupu pro vstup do chráněného (kontrolovaného) prostoru	P	P	P	P
6	Umožnění přístupu pro odchod z chráněného (kontrolovaného) prostoru	V	P	P	P
7	Zábrana proti opakovanému průchodu s následným zamítnutím přístupu	V	V/P	P	P
8	Výstraha při nerespektování zábrany proti opakovanému průchodu	V	V/P	V/P	V/P

Požadavky na rozhraní místa přístupu		Stupeň zabezpečení			
		1	**2**	**3**	**4**
9	Globální zábrana proti opakovanému průchod**u**	V	V/P	V/P	P
10	Překonání/vyřazení zábrany proti opakovanému průchodu	V	V	V/P	P
11	Časově závislá zábrana proti opakovanému průchodu	V	V	V	P
12	Podmíněný přístup do data účinnosti/platnosti	V	V	P	P
13	Podmíněný přístup podle platnosti oprávnění (blokované, pozastavené, neplatné)	P	P	P	P
14	Přístup pro doprovázenou osobu	V	V	V	V
15	Režim dohlížitele	V	V	V	V
16	Dvojnásobná přítomnost (kontrola přítomnosti dvou nebo více osob)	V	V	V	V
17	Dvojnásobný přístup (přístup dvou osob)	V	V	V	P
18	Singularizace/zamezení následného průchodu více osobami	V	V	V	V
19	Kontrola výtahu	V	V	V	V
	C – Monitorování místa přístupu				
20	Místo přístupu/stav musí být monitorován	V	P	P	P
21	Přípustná doba otevření místa přístupu musí být definována systémem (doporučená doba nemá být menší než 10 s)	V/N	V/N	N	N
22	Doba otevření místa přístupu musí být konfigurovatelná pro jednotlivé portály	V/P	V/P	P	P
23	Jsou-li konfigurovatelné, mohou být přípustné doby otevření spojeny s přístupovými právy pro jednotlivá místa přístupu	V	V	V	V
	D – Vstupní signály				
24	Musí být zpracovávány digitální vstupní signály (tj. jiné než komunikační signály) s aktivní periodou přesahující 400 ms	V	P	P	P

Požadavky na rozhraní místa přístupu	Stupeň zabezpečení			
	1	2	3	4
POZNÁMKA Zkratky používané v tabulce jsou následující: N = nepovoleno normou V = volitelné normou i projektem P = povinné normou V/N = volitelné normou / nepovoleno projektem V/P = volitelné normou / povinné projektem N/A = neaplikovatelné				

Tab.3 Požadavky na rozhraní místa přístupu; zdroj: tab.2 normy



Obr.2 Diagram požadavku normy na časování; zdroj: Příloha A, obr. A.1 normy

Požadavky na indikaci a hlášení		Indikace			Stupeň zabezpečení			
					1	2	3	4
	A – Portál (místní indikace)							

1	Požaduje se vizuální a/nebo akustická indikace, jestliže je povolen přístup	•			P	P	P	P
2	Požaduje se vizuální a/nebo akustická indikace, jestliže je přístup odmítnut	•			P	P	P	P
3	Vizuální a/nebo akustická indikace stavu uzamčení portálu dokud není přístup povolen	•			V	V	V	V
4	Vizuální a/nebo akustická indikace je požadována pro poslední časový interval (doba před výstrahou) maximální povolené doby otevření portálu jestliže portál zůstane otevřen, pro varování uživatele (uživatelů), že uplyne doba otevření portálu. Zanikne, je-li portál uzavřen. Doba otevření musí být v celém systému definovaná, nebo konfigurovatelná u jednotlivých portálů (doporučená doba: 10 sekund)	•			V	V	P	P
	B – Ovládací panel (hlášení)							
		Zobrazení	Výstraha	Záznam				
5	Požaduje se vizuální informace, je-li přístup povolen	•			V/P	V/P	V/P	V/P
6	Požaduje se záznam, je-li přístup povolen			•	V/P	V/P	P	P
7	Požaduje se vizuální informace, výstraha a záznam při stavu nátlaku	•	•	•	V/P	V/P	V/P	P
8	Počitadlo použití karty	•		•	V	V	V	V
9	Požaduje se vizuální informace, výstraha a záznam při zamítnutí přístupu v důsledku pokusu o použití identifikačního prostředku, jehož platnost vypršela	•	•	•	V/P	V/P	V/P	P
10	Požaduje se vizuální informace, výstraha a záznam, při zamítnutí přístupu z důvodu překročení konfigurovatelného počtu pokusů o použití identifikačního prostředku s neplatnou uloženou informací. Není-li počet pokusů konfigurovatelný, musí být omezen na 5°	•	•	•	V	V	V/P	P
11	Požaduje se vizuální informace, výstraha a záznam, při zamítnutí přístupu z důvodu překročení konfigurovatelného počtu následných pokusů použít neplatnou zapamatovanou informaci (např. použití PIN pouze pro identifikaci). Není-li počet pokusů konfigurovatelný, musí být omezen na 5 následných pokusů v rámci 30 sekund každého z nich	•	•	•	V	V	N	N

12	Vizuální indikace míst výstrahy v půdorysu střežených prostorů	•			V/P	V/P	V/P	P
13	Po poplachu musí být následně zobrazena instrukce	•			V/P	V/P	V/P	P
14	Transakce			•	V	P	P	P
15	Vizuální hlášení a záznam pro otevřený stav portálu poté, co byl povolen přístup. Může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•		•	V	V	P	P
16	Vizuální hlášení, výstraha a záznam pro stav, že portál zůstal v uzavřeném stavu poté, co byl odepřen přístup. Může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•	•	•	V	V	V	P
17	Přístup odepřen, může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•	•	•	V/P	V/P	P	P
18	Příčina odepření přístupu. Může být konfigurovatelné podle portálu a/nebo příčině odepření v souladu s požadavky stupně	•	•	•	V	V	V/P	P
19	Plánovaná nebo manuální změna stavu portálu			•	V	V	P	P
20	Porucha primárního zdroje napájení	•	•	•	V	V/P	P	P
21	Obnova primárního zdroje napájení	•		•	V	V/P	P	P
22	Stav problému záložního zdroje napájení (nízké napětí baterie a chybějící baterie)	•	•	•	V	V	P	P
23	Vstup a opuštění režimu konfigurace	•		•	V/P	V/P	P	P
24	Ztráta komunikace mezi řídicí jednotkou a ovládacím panelem	•	•	•	V/P	P	P	P
25	Kontrola přítomnosti	•		•	V	V	P	P
26	Portál uzavřen následně po násilném otevření nebo příliš dlouho otevřený portál	•		•	V	V/P	P	P
27	Veškeré události musí být identifikovány podle typu, místa a data kdy k nim došlo	•		•	V	V/P	P	P
28	Výstrahy musí obsahovat indikaci jejich priority,	•		•	V	V	P	P

	jestliže systém určení úrovní priority umožňuje							
29	Souběžně přijaté výstrahy musí být zobrazeny podle priority, jestliže systém určení úrovní priority umožňuje	•			V	V	P	P

Požadavky na indikaci a hlášení		Indikace			Stupeň zabezpečení			
					1	2	3	4
	B – Ovládací panel (hlášení)							
		Zobrazení	Výstraha	Záznam				
30	Detekce sabotáže	•	•	•	V	P	P	P
31	Násilně otevřený portál	•	•	•	V	P	P	P
32	Vizuální hlášení, výstraha a záznam pro uplynutí povolené doby otevření (příliš dlouho otevřený portál)	•	•	•	V	P	P	P
33	Sledování karet	•		•	V	V	V	P
34	Sledování čteček	•		•	V	V	V	P
35	Off-line stav čtečky	•	•	•	V	V	V	P
36	Abnormální stav uzamykacího zařízení	•	•	•	V	V	V/P	P
37	Hlášení dosažení limitu 90 % od maxima kapacity prostoru pro záznam	•	•	•	V	V	P	P
38	Maximální zpoždění signálů přicházejících na ovládací panel (90 s, 45 s a 15 s)	•	•	•	V	90 s	45 s	15 s
39	Maximální zpoždění pro zobrazení instrukcí následujících výstrahu poté co na ovládací panel došla výstraha (5 s)	•	•		V	V	V/P	P
40	Maximální zpoždění obrázku a/nebo grafiky poté co na ovládací panel došla výstraha (6 s)	•	•		V	V/6s	V/6s	6 s
41	Systém musí umožňovat určení úrovní priority pro určité události výstrahy	•			V	V	P	P
42	Výstrahy přijaté na ovládacím panelu vyžadují potvrzení příjmu operátorem	•	•	•	V/P	V/P	P	P
43	Požaduje se vizuální hlášení, výstraha a záznam jestliže nebyly respektovány podmínky	•	•	•	V	V	V	V

	dvojnásobné/vícenásobné přítomnosti (není přítomen minimální počet osob)							
44	Musí být zaznamenávány všechny operátorem iniciované změny včetně typu, identifikace operátora, čas a datum kdy nastaly			•	V	V	V/P	P
45	Operátorovy komentáře k výstrahám musí být zaznamenány s identifikací operátora, času a data příchodu záznamu komentáře. Musí být identifikovány specifické komentované výstrahy	•		•	V	V/P	V/P	P
46	Přístup k zaznamenaným informacím pro jejich vyvolání (událostí tj. zobrazení, tisk, export) musí být zaznamenán s identifikací operátora, času a data příchodu kdy se přístup uskutečnil			•	V	V/P	P	P
47	Záznamová kapacita minimálního počtu zaznamenávaných systémových událostí v průměru na čtečku			•	V	200	500	1 000

POZNÁMKA Zkratky používané v tabulce jsou následující:
N = nepovoleno normou
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.4 Požadavky na indikaci a hlášení; zdroj: tab.3 normy

Požadavky rozpoznávání		**Stupeň zabezpečení**			
		1	**2**	**3**	**4**
	A – Přístupové úrovně				
1	Vestavěné hodiny reálného času musí mít přesnost ±10 s za týden a umožňovat nastavení letního času a přestupného roku	V/P	P	P	P
2	Systém musí umožňovat více časových pásem	V	V	V	V
3	U systémů s více propojenými řídicími jednotkami musí být hodiny synchronizovány s hlavními hodinami nebo jiným spolehlivým zdrojem synchronizace nejméně jednou za 24 hodin	V/P	V/P	P	P

Požadavky rozpoznávání		Stupeň zabezpečení			
		1	**2**	**3**	**4**
4	Synchronizace hlavních hodin systému s úředním časem	V	V/P	V/P	P
5	Hodiny reálného času musí být po uvedenou minimální dobu v provozu v případě úplné ztráty napájení (s výjimkou ztráty energie baterie pro uchovávání dat)	V	24 h	120 h	120 h
6	Minimální počet uživatelských přístupových úrovní	1	8	16	64
7	Minimální počet konfigurovatelných časových úseků	0	4	8	16
8	Minimální rozpoznávání pro čas v rámci přístupových úrovní zahrnující den v týdnu, hodinu a minutu denního času	N/A	P	P	P
9	Minimální rozpoznávání pro čas v rámci přístupových úrovní zahrnující den v měsíci, měsíc a rok	N/A	V	V	P
10	Systém musí být schopen zvládnout určitý počet konfigurovatelných dní (např. státní svátky, speciální pracovní dny a dny pracovního klidu)	N/A	2	16	24
11	Systém má umožňovat přidělení přístupových oprávnění skupině oprávněných jedinců	V/P	V/P	V/P	V/P
12	Systém má být schopen měnit přístupová práva skupině přístupových oprávnění v návaznosti na bezpečnostní podmínky	V/P	V/P	V/P	V/P
	B – Zařízení a způsoby identifikace				
13	Systém musí přidělit jedinečnou identifikaci každému oprávněnému uživateli	V	P	P	P
14	Systém musí používat pouze zapamatovanou informaci (PIN)	V	V/N	N	N
15	Systém musí používat buď jen biometrii, nebo v kombinaci s dalšími způsoby rozpoznávání	V	V	V	V
16	Systém musí používat identifikační prostředky (karta, čip)	V	V	V	V/N
17	Systém musí používat zapamatovanou informaci a identifikační prostředky (PIN+karta/čip)	V	V	V	V
18	Přístup musí být odmítnut po každém pokusu o získání přístupu s použitím identifikačního prostředku s neplatnou zapamatovanou informací a po předdefinovaném počtu neúspěšných pokusů o získání přístupu s identifikačním prostředkem s přístupovými oprávněními pozastavenými na přednastavené trvání. Počet pokusů může být konfigurovatelný. Není-li konfigurovatelný, musí být počet pokusů omezen na 5	V	P	P	P

	Požadavky rozpoznávání	Stupeň zabezpečení			
		1	2	3	4
19	Přístup musí být odmítnut po každém pokusu o získání přístupu jen s neplatnou zapamatovanou informací. Přístup musí být vyloučen po 5 následných nesprávných zadání v rámci přednastaveného časového úseku	V/P	V/ N/A	N/A	N/A
20	Při použití biometrie nesmí FAR_{eff} překročit limit stanovený pro každý stupeň. POZNÁMKA 1 $FAR_{eff} = FAR$ (četnost falešných přijetí) je-li prováděno porovnávání 1:1 (např. biometrická verifikace identity potvrzená zapamatovanou informací nebo identifikačním prostředkem) nebo $FAR_{eff} = FAR \times n$ je-li prováděno porovnávání 1:*n* a *n* = počet uložených vzorků (např. biometrická verifikace identity bez použití zapamatované informace nebo identifikačního prostředku). POZNÁMKA 2 Hodnoty *FAR* jsou založeny na přehledu údajů ve výrobcem přiložené dokumentaci.	1 %	0,3 %	0,3 %	0,1 %
21	Minimální poměr mezi počtem možných uživatelských kódů a počtem přidělených kódů musí být nejméně 1 000 ku 1, je-li systém používán k rozpoznávání uživatelů pouze zaznamenanou informací, např.: do 10 uživatelů – 4 číslice, do 100 uživatelů – 5 číslic, do 1 000 uživatelů – 6 číslic; atd.	P	P	N/A	N/A
22	Pro systémy používající rozpoznávání uživatelů zapamatovanou informací v kombinaci s identifikačním prostředkem nebo biometrií vyžaduje zapamatovaná informace nejméně 4 číslice	V/P	V	P	P
23	V normálním provozním režimu musí systém pro identifikaci používat kompletní informaci identifikačního prostředku (kód objektu a číslo karty, nebo jedinečné číslo karty)	P	P	P	P
24	Podpora pro vícenásobné kódy objektů, jestliže systém používá kódy objektů	V	V	V	P
25	V degradovaném režimu činnosti může systém pro identifikaci používat částečnou informaci identifikačního prostředku (např. pouze kód objektu).	V	V	V/N	N
26	Nesmí být používány identifikační prvky se strukturou kódovacího systému viditelnou pouhým okem	P	P	P	P
27	Identifikační číslo identifikačního prostředku nemá být přímou reprezentací celého kódování	P	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
N = nepovoleno normou
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.5 Požadavky na rozpoznání; zdroj: tab.4 normy

Požadavky na signalizaci nátlaku		Stupeň zabezpečení			
		1	2	3	4
1	Aktivování funkce signalizace nátlaku musí být konfigurovatelné	V/P	V/P	V/P	P
2	Výstraha nátlaku na ovládacím panelu má být odlišná od ostatních výstrah	P	P	P	P
3	Činnost iniciačního zařízení výstrahy nesmí vyvolat signál, který by mohl být slyšitelný nebo viditelný v místě, kde byla signalizace nátlaku vyvolána	P	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.6 Požadavky na signalizaci nátlaku; zdroj: tab.5 normy

- další požadavky na signalizaci nátlaku:
    - signál nátlaku přijatý na ovládacím panelu musí obsahovat identifikaci umístění, času a data, kdy k nátlaku došlo
    - signál nátlaku přijatý na ovládacím panelu musí obsahovat identifikaci uživatele

	Požadavky na překonání/přemostění	Stupeň zabezpečení			
		1	**2**	**3**	**4**
1	Poskytnutí jednoho volného přístupu, jeden portál	V	V	P	P
2	Poskytnutí volného přístupu pro celý systém	V	V	V	V
3	Poskytnutí volného přístupu do příštího systémového příkazu, jednotlivý portál nebo skupina portálů	V	V	V	V
4	Poskytnutí plánovaného/časově definovaného volného přístupu, jednotlivý portál nebo skupina portálů	V	V	V	V
5	Elektronický systém kontroly vstupu nesmí zamezit volný odchod povolený jinými nouzovými systémy (např. požární, environmentální)	P	P	P	P
6	Blokování portálu do dalšího systémového povelu, jednotlivý portál nebo skupina portálů	V	V	V	V
7	Plánované/časové blokování portálu, jednotlivý portál nebo skupina portálů	N/A	V	V	V

POZNÁMKA Zkratky používané v tabulce jsou následující:
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.7 Požadavky na překonání/přemostění; zdroj: tab.6 normy

- další požadavky na přemostění/překonání:
  - všechny příkazy překonání musí být zaznamenány s časem a datem, kdy se uskutečnily
  - zaznamenaná informace musí obsahovat typ příkazu k překonání a identifikaci operátora.

- požadavky na komunikaci čl. 6.7
  - výpadek a/nebo obnovení komunikačního kanálu pro zařízení stupně zabezpečení 2, 3 a 4 nesmí mít za následek uvolnění portálů
  - ověření komunikace (časování) musí být realizováno jako součást finální instalace a musí pro tuto instalaci splňovat požadavky tab.4, řádek 38
  - zařízení stupně zabezpečení 2, 3 a 4 musí umožňovat autonomní provoz po přerušení komunikace s ovládacím panelem; zařízení musí umožňovat provádění veškerých funkcí s výjimkou těch, které jsou ztrátou komunikace ovlivněny

- zařízení stupně zabezpečení 4 musí garantovat integritu komunikací mezi všemi komponentami elektronického systému kontroly vstupu vysílajících nebo přijímajících data vztahující se na poskytnutí přístupu, včetně například: komunikace mezi identifikačními prostředky/kartami a uživatelskými rozhraními, uživatelskými rozhraními a ovládacími zařízeními kontroly vstupu a mezi ovládacími zařízeními kontroly vstupu a ovládacím panelem
- integrity komunikace musí být dosaženo dohledem nad komunikačním kanálem (tab.8, řádek 9) a bezpečností přenášených informací.
- bezpečnost informací musí být zajištěna prostředky zamezujícími neoprávněnému čtení a modifikaci přenášené informace

- požadavky na vlastní ochranu systému dle čl. 6.8 normy

	Požadavky na vlastní ochranu systému	**Stupeň zabezpečení**			
		1	**2**	**3**	**4**
	A – Prevence				
1	Informace uložené v paměti (nastavení) musí být v případě úplné ztráty napájení (s výjimkou ztráty energie baterie pro uchovávání dat) zachována minimálně po uvedený časový úsek	10 min	2 týdny	2 týdny	2 týdny
2	Po úplné ztrátě napájení je po obnovení primárního zdroje napájení požadován automatický restart systému kontroly vstupu	P	P	P	P
3	Nelze-li po automatickém restartu obnovit plnou funkčnost řídicí jednotky kontroly vstupu (došlo k poškození nebo ztrátě dat), musí být ohlášen problémový stav	P	P	P	P
4	Možnosti přístupu k vnitřním prvkům komponent systému kontroly vstupu musí vyžadovat použití nástroje	P	P	P	P
5	Otevření krytu uživatelského rozhraní určeného k instalaci vně kontrolovaného prostoru musí vést k detekci sabotáže, může-li manipulace s vnitřními prvky způsobit stav povoleného vstupu. K detekci sabotáže musí dojít dříve, než může být mechanismus detekce sabotáže vyřazen z činnosti	V	P	P	P
6	Zařízení určená k instalaci vně kontrolovaného prostoru nebo mohou být dostupná z vnějšku kontrolovaného prostoru, musí detekovat odstranění z montážního místa, jestliže by to umožnilo přístup k vnitřním prvkům, jejichž manipulace může způsobit stav povoleného vstupu	V	V/P	P	P
7	Kryty komponent EACS dosažitelné z vnějšku kontrolovaného prostoru musí splňovat požadované hodnocení IP a IK	IP4X IK04	IP4X IK04	IP4X IK04	IP4X IK04

8	V případě ztráty komunikace mezi řídicí jednotkou (jednotkami) a ovládacím panelem musí řídicí jednotka umožňovat ukládaní a následné vyslání po obnovení komunikace minimální počet událostí na jeden portál	N/A	V/500	500	1000
9	Komunikace mezi řídicí jednotkou a komponentami EACS musí být monitorována. Ztráta komunikace po uvedenou dobu trvání musí mít za následek výstrahu na ovládacím panelu	N/A	V/10min	10 min	2 min
10	Administrace systému včetně konfigurace musí být logicky přístupná s použitím platného oprávnění (např. heslo, identifikační prostředek)	N/A	P	P	P
11	Musí existovat oddělené úrovně přístupu, kategorizující schopnost operátorů provádět v systému různé funkce. Minimální počet logických přístupů je:	1	1	2	4
12	Minimální počet požadovaných znaků požadovaných pro logický přístup prostřednictvím zapamatované informace musí být pouze, tak jak je uvedeno (C=číslicový/A-alfanumerický)	4C	5C	6A	8A
13	Jsou-li pro logický přístup zapamatovanou informací používány číslicové kódy, není povoleno používat postupně rostoucí nebo klesající číslice a není povoleno používat tutéž číslici více než dvakrát	V	V/ N/A	P	P
14	Pro logický přístup použít při kombinaci s indikačním prostředkem nebo s biometrií minimálně čtyřcifernou zapamatovanou informaci (generovanou systémem nebo administrátorem systému)	V/P	V/P	P	P
15	Logický přístup může být oprávněnému přidělen pouze administrátorem systému	V	V	P	P
16	Musí být možnost přepsat výrobcem přednastavené hodnoty pro logický přístup	V	V	P	P
17	Minimální doba zachování dat pro zaznamenané události uložené v řídicí jednotce systému pro kontrolu vstupu během provozní ztráty napájení (v důsledku ztráty komunikace s ovládacím panelem) musí odpovídat uvedeným hodnotám	V	24 h	120 h	120 h
18	U veřejně sdílených sítí (např. internet) se požaduje šifrování komunikačních signálů mezi komponentami EACS	V	V/P	P	P
19	Informace uložené na identifikačním prostředku musí být chráněny proti neoprávněné modifikaci nebo kopírování	V/P	V/P	P	P
20	Porucha nebo obnovení komunikačního kanálu nesmí mít za následek uvolnění místa přístupu	P	P	P	P
21	Porucha komunikace s ovládacím panelem nesmí přerušit proces rozhodování	P	P	P	P

	o přístupu				
22	Procesní pravidla uložená ve čtečce místa přístupu nesmí být pro uživatele systému viditelná	P	P	P	P
23	Světelné nebo zvukové indikátory aktivace stisku kláves klávesnice nesmí být přímou reprezentací skutečných kódů, ale musí mít stejnou výšku tónu a trvání	P	P	P	P
24	Komunikace mezi čtečkami a řídicími jednotkami musí umožňovat šifrování s autentizací	V	V	V	P
25	Návod k obsluze musí obsahovat podrobné montážní požadavky pro mechanickou ochranu omezující přístup ke komunikačním spojům mezi čtečkami a řídicí jednotkou systému kontroly vstupu	V	V	V	V
	B – Detekce a podávání zpráv				
26	Změna stavu digitálního vstupu detekčního obvodu (otevřeno, zavřeno, sabotáž (rozpojení nebo sepnutí sabotážního kontaktu)) musí být výrobcem konstruován tak, že se tolerance pro každý stav vstupního obvodu nesmí překrývat se sousedním stavem	V/P	V/P	P	P
27	Validace systému vstupu dat. Systém musí poskytovat hlášení na ovládacím panelu, jestliže byla v průběhu konfiguračního režimu vložena neplatná data.	P	P	P	P
28	Přístup ke konfiguračnímu režimu se musí přerušit po překročení přednastavené doby nečinnosti	P	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.8 Požadavky na vlastní ochranu; zdroj: tab.7 normy

	Požadavky na napájení	Stupeň zabezpečení			
		1	2	3	4
1	Řídicí jednotka systému kontroly vstupu musí být vybavena záložním zdrojem napájení, schopným zajistit provoz systému a jeho příslušenství ve stavu specifikovaného plného zatížení po uvedenou dobu. (Podmínky zatížení nezahrnují ovládací panel nebo aktivační prvky přístupových míst)	V	V/2h	2 h	4 h
2	Po delším výpadku primárního zdroje napájení (nastalo přerušení činnosti systému) a obnovení napájení musí být baterie dobity na 80 % jmenovité kapacity během 24 hodin a na 100 % jmenovité kapacity během 72 hodin	P	P	P	P
3	Výpadek primárního zdroje napájení nebo jeho obnovení nesmí negativně ovlivnit normální činnost systému.	V	V/P	P	P
4	Jestliže je zajištěn záložní zdroj napájení, musí být možné monitorovat jeho následující stavy: nízké napětí a baterie není přítomna (akceptovatelné je společné hlášení obou stavů)	V	V/P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
V = volitelné normou i projektem
P = povinné normou
V/N = volitelné normou / nepovoleno projektem
V/P = volitelné normou / povinné projektem
N/A = neaplikovatelné

Tab.9 Požadavky na napájení; zdroj: tab.8 normy

- další požadavky na napájení dle čl. 6.9 normy
- aplikovatelné zkoušení odolnosti proti vlivům prostředí každého komponentu musí být prováděno v souladu se způsoby popsanými v IEC 62599-1
- aplikovatelné zkoušení odolnosti EMC každého komponentu musí být prováděno v souladu se způsoby popsanými v IEC 62599-2
- zkoušky/testy komponentů ACS musí být provedeny dle čl. 8 normy

ČSN EN 50133-7

- kromě požadavků uvedených v předchozí části (ČSN EN 60839-11-1), je nutné při návrhu nutné vzít v úvahu ještě u každého přístupového místa:
  - četnost průchodu (spolehlivost portálu)
  - safety požadavky – požární cesta, únik, panika atd.
  - konkrétní provedení prostředků na hlášení a indikaci – displej, ukládání dat, výstraha
  - charakter prostředí (vandalismus apod.)
  - umístění zařízení, mechanická pevnost místa instalace

- snadnost obsluhy (ovládání)
- nezbytnost zajištění průchodu pouze jedné osoby – anti-tailgate (turniket apod.)
- způsob návratu přístupového místa do stavu uzavření (samozavírač apod.)
- kabeláž (topologie, trasy, uložení, ochrana)
- vhodnost identifikačního zařízení (životnost, četnost průchodů, prostředí)
- provozní uspořádání pro přístupové místo (bezrizikový režim při poruše, zabezpečení proti poruše)
- opatření pro tělesně postižené, zavazadla, zásilky
- správa/ovládání/programování systému
- detekce sabotáže
- anti-passback logický, časový, prostorový
- provedení poplachu pod nátlakem
- kontrola přítomnosti min. nebo max. počtu osob
- správa návštěv
- vjezd vozidel

Ostatní funkční požadavky
- interoperabilita se zvolenou technologií integrační platformy IPS
- distribuovaná architektura
- min. 3 úrovně Threat levels
- pro přenosovou síť VSS bude využito shodné technologie jako u společné přenosové trasy celého IPS, tj. standardu průmyslového ethernetu
- propracovaný modul správy návštěv
- v maximální míře snaha vyhnout se bezdrátovému propojení na úrovni přenosové trasy
- zvážit podporu bezdrátových čtecích terminálů, bezproblémový/spolehlivý provoz v rádiovém prostředí v místech nasazení
- standardní identifikace uživatele pomocí bezkontaktní ID karty, v rámci DNS/upřesnění v DPS dojde k revizi požadavku na definici stávající technologie/standardu ID karet, příp. bude definován nový standard
- nadstandardní identifikace uživatele (investorem určené portály) pomocí ID karta+PIN nebo jiná volitelná kombinace v souladu s požadavky normy na daný stupeň zabezpečení

5.2.6. Elektrická požární signalizace (EPS)

Není předmětem projektu. Jediný požadavek se vztahuje na možnost integrace (zajištění interoperability) stávající(ch) EPS v objektu do IPS. Tento požadavek musí být zohledněn při výběru technologie (platformy) IPS. Vlastní integrace EPS do IPS není požadována, předpokládá se v následných projektech týkajících se PBZ.

5.2.7. Přenosový systém

Pro přenosový systém IPS bude v souladu s ČSN CLC/TS 50398 navržena **společná přenosová trasa** s následujícími požadavky a parametry:

- společná přenosová trasa fyzicky vyhrazená (dedikovaná) pouze pro nePBZ aplikace TSFO v rámci IPS
- interoperabilita se zvolenou technologií integrační platformy IPS
- společný TCP/UDP/IP přenosový systém na bázi (over) Industry ethernet
- topologie optický ring
- podpora 10/100/1000BASE-T
- rekonfigurovatelnost při 1 poruše do 30ms
- SM/MM univerzální optické porty s WDM
- podpora TSFO aplikací (splnění aplikačních norem) - přenos proprietárních RS485/422/232 a I/O over IP (NO,NC,EOL,DEOL,TEOL)
- event management – http příkazy, IP relé, SNMP traps, email notification
- podpora PoE (IEEE 802.3af), PoE+ (IEEE 802.3at)
- ochrana proti sabotáži dle aplikačních norem provozovaných (přenášených) TSFO
- podpora unicast, multicast
- podpora VLANs, SMTP, IGMPv3, SNMPv3, SNTP, 802.1p/q, QoS
- administrace přenosového systému prováděna dodavatelem/integrátorem IPS
- integrovaná funkce IP Watchdog
- redundantní napájení aktivních prvků
- odolnost dle IEC 61643-11, EN 61000-4-X
- certifikace dle ČSN EN 50131-1 ed.2, ČSN EN 50130-4, ČSN EN 60065, ČSN EN 60529, ČSN EN 55022
- kabeláž přenosových tras bude dle ČSN EN 50174, ČSN EN 50173 a ČSN EN 50310

5.2.8. Operační středisko, velín

Dispoziční řešení stávajícího operačního střediska je nevyhovující. V rámci DNS/upřesnění v DPS bude dle požadavků investora provedena kompletní úprava dispozice celého operačního střediska. Stávající velín je požadováno situovat dále od pláště budovy. Úpravy operačního střediska budou provedeny dle požadavků investora. Operační středisko bude nově navrženo dle souboru ČSN EN ISO 11064. Ergonomie velínu bude navržena dle ČSN EN ISO 11064-3 a ČSN EN 50132-7 ed.2 čl.7.2, čl.12 (VSS).
V objektu je požadováno vybudování záložního velínu. Prostor záložního velínu bude sloužit zároveň jako datové uložiště IPS. Parametry záložního velínu definuje investor.

5.2.9. Vztah k ostatním neTSFO

Všeobecné základní požadavky pro všechny neTSFO:

- sjednocení ID prostředků (zapamatovaná informace, identifikační prostředek, biometrie)
- využití databáze uživatelů společné s TSFO pouze na základě požadavku investora

6. POŽADAVKY NA ZAJIŠTĚNÍ INŽENÝRSKÝCH, PROJEKČNÍCH A DALŠÍCH ČINNOSTÍ

Investor požaduje vypracovat projektovou dokumentaci vč. činností souvisejících dle metodiky ČKAIT pro projektování staveb, tj. Standardů profesních výkonů (verze 06/2014) a Standardů ZSMV.

Investor požaduje generální dodávku všech nezbytných inženýrský, projekčních a dalších prací a činností souvisejících generálním projektantem. Generální projektant je povinen v případě zjištění (ve VF2) přizvat k sobě další nezbytné profese (např. stavební, silnoproud, VZT/CHL, MaR, BOZP, PO apod.) k účasti na projekčních pracích a všech činností souvisejících. Tento požadavek se předpokládá hlavně v případě integrovaného návrhu operačního střediska.

Investor požaduje zajistit následující činnosti a výstupy - výkonové fáze (VF):

- **VF2** (dokumentace návrhu/studie stavby – **DNS**/STS)
- **VF3** (dokumentace pro územní rozhodnutí - **DUR**) – nepředpokládá se, nicméně povinná v případě požadavku (vyplyne z VF2)
- **VF4** (dokumentace pro stavební povolení – **DSP**) – předpokládá se v části operačního střediska, nicméně povinnost vč. rozsahu vyplyne z předchozích VF
- **VF5** (dokumentace pro provádění stavby – **DPS**)
- **VF6** (soupis prací a dodávek – **SPD**)

Všechny VF budou zpracovány v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, v platném znění.

Následují konkrétní požadavky na rozsah a obsah jednotlivých VF.

DNS – standardní činnost provést **dle požadavků VF 2.** Kromě standardních činností budou v rámci DNS dodány následující **nadstandardní činnosti:**

- Použití metody BIM
- Provedení STP vč. zdokumentování výsledků dle metodiky ZSMV
- Návrh etapizace výstavby vč. stanovení odhadu nákladů na výstavbu
- V součinnosti s investorem vypracovat dokument popisující pravidla funkce *Threat Level Management*, tj. popis chování celého IPS vč. režimových opatření za různých

bezpečnostních situací (stavech ohrožení, poruchové a krizové stavy). Investor požaduje 3 úrovně Threat Levels

- Součinnost a profesní účast na paralelně probíhajícím samostatném projektu rekonstrukce hlavního vstupu do objektu (nová budova)

DUR – standardní činnost provést **dle požadavků VF 3, tj. dle vyhlášky 499/2006 Sb., ve znění vyhlášky č. 62/2013 Sb.**

DSP - standardní činnost provést **dle požadavků VF 4, tj. dle vyhlášky 499/2006 Sb., ve znění vyhlášky č. 62/2013 Sb. (příloha č. 5)**. Kromě standardních činností budou v rámci DSP dodány následující **nadstandardní činnosti:**

- Použití metody BIM
- Koordinační výkresy profesí
- Návrh etapizace výstavby vč. stanovení odhadu nákladů na výstavbu
- Protokol o určení vnějších vlivů

DPS – standardní činnost provést **dle požadavků VF 5, tj. dle vyhlášky 499/2006 Sb., ve znění vyhlášky č. 62/2013 Sb. (příloha č. 6)**. Kromě standardních činností budou v rámci DPS dodány následující **nadstandardní činnosti:**

- Použití metody BIM
- Koordinační výkresy profesí
- Návrh Zásad organizace výstavby
- Návrh etapizace výstavby vč. stanovení odhadu nákladů na výstavbu
- Návrh a vypracování akceptačních kritérií a soupisu akceptačních testů pro výběr technologií IPS. Provedení akceptačních testů bude v DPS požadováno provést po zhotoviteli na demo sestavě při úvodním výběru konkrétních technologií v rámci zpracování realizační dokumentace RDS. Pozitivní výsledek akceptačních testů, tj. akceptace ze strany investora, je nezbytnou podmínkou dopracování RDS a následné zhotovení díla.
- Zapracovat do DPS komplexní návrh interiéru operačního střediska vč. záložního velínu
- Zapracovat do DPS požadavek na vypracování RDS (zhotovitelem díla) vč. stanovení nezbytného rozsahu a obsahu RDS.

- Zapracovat do DPS požadavek na vypracování dokumentace skutečného stavu (zhotovitelem díla) vč. stanovení nezbytného rozsahu a obsahu této dokumentace.
- DPS bude obsahovat veškeré rozhodné návrhové výpočty.
- Zapracovat do DPS požadavek na vypracování migračního plánu (zhotovitelem díla) přechodu na nové technologie.
- Zapracovat do DPS předpis pro zpracování migračního plánu (formální vzor rozsahu a obsahu).

SPD – standardní činnost provést **dle požadavků VF 6**. Kromě standardních činností budou v rámci SPD dodány následující **nadstandardní činnosti:**

- Použití metody BIM
- Sestavení kontrolního rozpočtu

7. ETAPIZACE

Součástí všech VF projekčních prací bude vypracování návrhu etapizace výstavby díla. V každé VF bude v rámci návrhu etapizace sledován **požadavek investora na rozsah 5 až 10 mil. Kč na každou jednu etapu**. Z každé etapy je požadován nový ucelený hmatatelný užitek, který bude odsouhlasen investorem. Prioritou výstavby, tj. i etapizace, je modernizace VSS, a to přednostně VSS perimetru vnějšího pláště budovy.
Návrh etapizace bude v každé VF odsouhlasen investorem. Formu a podrobnost návrhu etapizace každé VF určí investor.

8. ODHAD NÁKLADŮ

Odhad investičních nákladů na zajištění projekčních prací a prací souvisejících je 1-3mil.Kč.

9. MIGRAČNÍ PLÁN

Součástí zhotovitelské RDS bude vypracování migračního plánu dle předpisu DPS. Migrační plán bude akceptovat návrh etapizace výstavby IPS.

10. SOUČINNOST INVESTORA

Součinnost investora se v průběhu projekčních prací předpokládá standardní dle VF.

PŘÍLOHY

1. Dokumentace skutečného stavu objektu MVČR Nad štolou – stavební část

Poznámka: Dokumentace skutečného stavu objektu MVČR Nad štolou – stavební část bude poskytnuta vybranému uchazeči po podpisu Smlouvy o dílo.