# Vyhodnocování, reakce a odpovědnost pracovníků DPPC na příchozí události PPC

Bc. Tomáš Krejčí

Diplomová práce
2020



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

# Univerzita Tomáše Bati ve Zlíně

## Fakulta aplikované informatiky

### Ústav elektroniky a měření

Akademický rok: 2019/2020

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Tomáš Krejčí** |
| Osobní číslo: | **A18699** |
| Studijní program: | **N3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **Kombinovaná** |
| Téma práce: | **Vyhodnocování, reakce a odpovědnost pracovníků DPPC na příchozí události PPC** |
| Téma práce anglicky: | **The Evaluation, Response and Responsibility of DPPC Staff to Incoming PPC Events** |

## Zásady pro vypracování

1. Vypracujte literární rešerši zaměřenou na technickou část bezpečnostních systémů.
2. Popište možné způsoby komunikace bezpečnostních zařízení s dohledovým a poplachovým přijímacím centrem (DPPC).
3. Zdokumentujte možné typy příchozích událostí na DPPC.
4. Vytvořte pracovní postupy vyhodnocení a reakce na příchozí události DPPC.
5. Určete odpovědnost jednotlivých pracovních pozic DPPC.

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:


1. IVANKA, Ján, 2014. Systemizace bezpečnostního průmyslu I. Vyd. 5. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978?80?7454?410?1.
2. DRGA, Rudolf a LAUCKÝ, Vladimír, 2012. Speciální technologie komerční bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-146-9.
3. VALOUCH, Jan. 2015. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-557-3.
4. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I-V. Zlín: VeRBuM, 2011
5. ČSN EN 50131-1 ed. 2/A1/Z2. Poplachové systémy ? Poplachové zabezpečovací a tísňové systémy. Část 1: Systémové požadavky. Praha: Český normalizační institut, 2007.
6. ČSN EN 50518 -3 ed.2. Dohledová a poplachová přijímací centra – Část 3: Pracovní postupy a požadavky na provoz. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
7. HRUŠKA, Ivan. 2014. Dohledové a poplachové přijímací centrum a jeho specifika v sektoru soukromé bezpečnosti. Zlín. Dostupné také z: http://digilib.k.utb.cz/handle/10563/29929. Diplomová práce. Univerzita Tomáše Bati.


Vedoucí diplomové práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**


L.S.

**doc. Mgr. Milan Adámek, Ph.D.**
děkan

**Ing. Milan Navrátil, Ph.D.**
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13. 8.2020 Tomáš Krejčí, v. r.

## ABSTRAKT

Na dohledová a poplachová přijímací centra (dále jen „DPPC“) přichází poplachové, stavové, poruchové, ale i jiné události ze zabezpečovacích, případně integrovaných poplachových systémů. Těžká úloha operátorů DPPC je příchozí události kvalifikovaně, ale hlavně dobře, vyhodnotit s následnou reakcí na vzniklou situaci. Předpokladem kvalitní reakce DPPC je správné nastavení jednotných firemních standardů (postupů) reakce na jednotlivé příchozí události.

Cílem diplomové práce je vytvořit a popsat možné případy vyhodnocení a reakce na příchozí události z bezpečnostních systémů na DPPC. Zároveň také určit odpovědnost jednotlivých pracovníků, podílejících se na řádném provozu dohledového centra.



Klíčová slova: dohledové a poplachové přijímací centrum (DPPC), poplachový zabezpečovací a tísňový systém (PZTS), akční plán, operátor, vyhodnocení.



## ABSTRACT

The Monitoring and alarm receiving centers (further in the work only referred to as „DPPC") receive alarm, status, fault and other events from alarm or integrated alarm systems. The difficult role of DPPC operators is to assess incoming events in a qualified way, but most importantly to evaluate them properly with the subsequent response to the situation. A prerequisite for a good DPPC response is the correct setting of uniform corporate standards (procedures) for responding to individual incoming events.

The aim of this thesis is to create and describe possible cases of evaluation and response to incoming events from security systems at DPPC. Additionally, the thesis aims to determine the responsibilities of individual personnel involved in the proper operation of the Monitoring center.



Keywords: Monitoring and alarm receiving centre (DPPC), Intrusion and hold-up alarm system (PZTS), action plan, operator, evaluation.

Na tomto místě bych chtěl poděkovat svému vedoucímu práce panu Ing. Jánu Ivankovi za trpělivé, nekonečné rady a připomínky během celé doby vypracovávání diplomové práce. Velice si vážím jeho přístupu, schopností, a především chuti předávat své znalosti. V neposlední řadě děkuji za značnou dávku shovívavosti.

Z poděkování nemůžu vynechat celou svou rodinu za veškerou podporu, kterou mi věnovala po celou dobu mého studia, a stejně tak děkuji zaměstnavateli za vyhrazení časového prostoru při zdokonalování profesní kvalifikace.

# OBSAH

# ÚVOD

Každý z nás potřebuje mít pocit bezpečí, ať už se jedná o náš život, zdraví nebo majetek. Je jenom na nás, jak si budeme vše potřebné chránit. Každé preventivní opatření vedoucí ke snížení rizika jakékoliv újmy na nejnižší možnou úroveň je v našich životech velice cenné. Hodnotu preventivních opatření bychom měli volit i s ohledem na hodnotu chráněné oblasti. Velmi obtížně se dá vyčíslit hodnota lidského života nebo zdraví. Můžeme si dovolit tvrdit, že tyto hodnoty jsou vlastně nevyčíslitelné. Co se týká majetku, lze předpokládat, že nabyté majetkové hodnoty mají svojí určitou cenu. Nesmíme ovšem zapomenout také na osobní duševní hodnotu určitých věcí, které vlastníme a o které bychom mohli velice snadno přijít.

Jednou z mnoha možností zavedení preventivních opatření je instalace a využívání bezpečnostních systémů nebo i systémů jiných než bezpečnostních, které dokáží generovat poplachové události. Aby tyto systémy sloužily ke svému účelu je nutné, aby návrh, projektovou dokumentaci, instalaci a údržbu prováděly odborně způsobilé a v oboru vzdělané osoby. Jen tak může být zajištěn bezproblémový provoz instalovaných zařízení. Technologický pokrok v dnešní době je nezadržitelný a výrobci vyvíjejí stále nová, dokonalejší nebo sofistikovanější zařízení pro zvýšení úrovně zabezpečení různých oblastí zájmu.

Aby instalované zařízení plnilo svou funkci ještě lépe, je v nabídkách firem poskytujících bezpečnostní služby provozování dohledových poplachových a přijímacích center, kam je možnost zařízení připojit a zprávy událostí přenášet na monitory operátorů. Ti pak kvalifikovaně reagují na příchozí události a dle operačních postupů vyvolávají akce protiopatření na snížení dopadu škodícího účinku.

Operátoři, ale také supervisoři nebo administrátoři jsou přímými účastníky podílející se na provozu DPPC. Dobře nastavené procesy, srozumitelně sepsané postupy, jasně definovaná pravidla a odpovědnost jsou základními předpoklady správné funkční činnosti dohledového centra.

Diplomová práce si klade za úkol vytvořit možný návod nastavení procesů pro spolehlivý chod dohledového centra. Diplomová práce může sloužit jako návod při tvorbě standardních operačních postupů při určování odpovědnosti jednotlivých pracovních pozic a obsah pracovních činností. Převážná část práce je věnována činnosti a reakci pracovníků v pozicích operátorů.

Úvodní část diplomové práce se zabývá přiblížením funkční a normativní problematiky zařízení poplachových a přijímacích center a popisuje základní funkční principy vybraných zařízení, které jsou montovány u zákazníků.

Praktická část diplomové práce pak naznačuje možné provozní řešení dohledových center s ohledem na normativní požadavky. Jsou popsány technologie a zařízení pro zajištění bezpečnosti dohledového centra, včetně přístupových úrovní a nouzového postupu. Standardní operační postupy naznačují možné služby nabízené agenturami provozující dohledová centra a popisují možné reakce operátorů na příchozí události ze systémů zákazníků. Nedílnou součástí provozu každého podniku jsou postupy popisující poruchové stavy zařízení a reakcí. V závěru jsou uvedeny příklady vyhodnocení příchozích událostí.

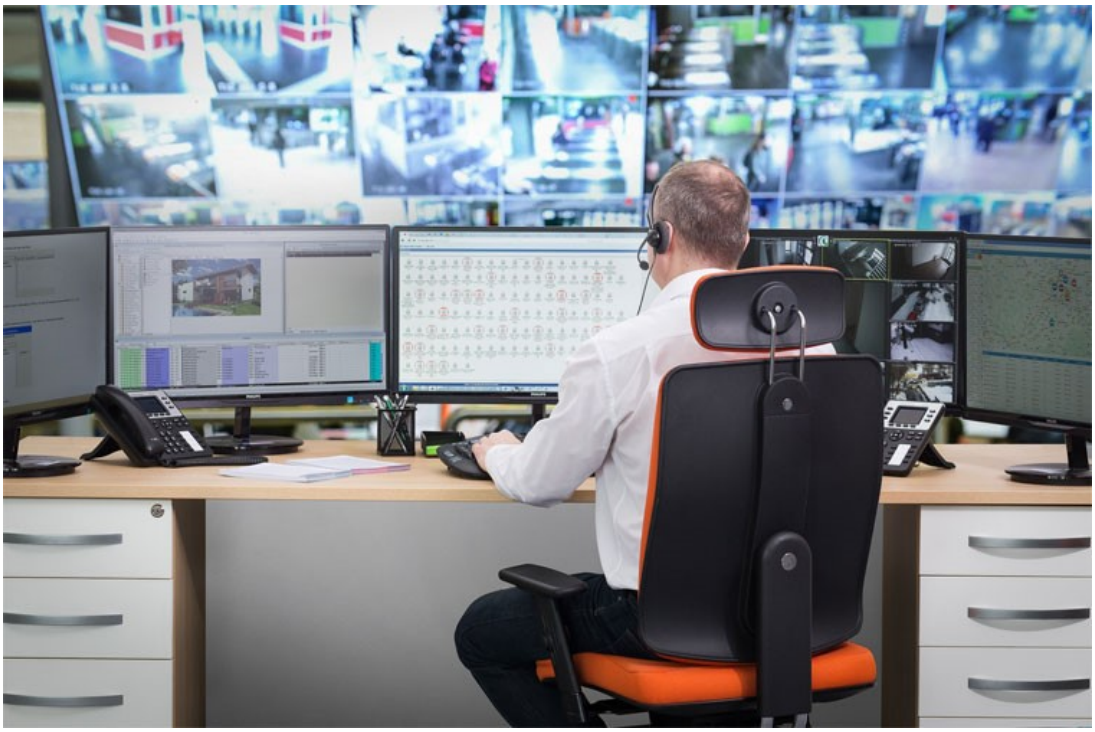
Jenom bezpečnostní agentury, které mají pevně nastavené procesy a vyžadují jejich dodržování, mohou nabídnout svým zákazníkům služby na té nejvyšší úrovni. Administrátoři si musí uvědomit při sestavování akčního plánu se zákazníkem, že jakýkoliv nestandardní postup může snížit účinnost preventivního opatření. Operátor musí mít pevně stanovená pravidla pro vyhodnocování a reakci na příchozí události ze systémů zákazníka.

# I. TEORETICKÁ ČÁST

# 1 DOHLEDOVÉ A POPLACHOVÉ PŘIJÍMACÍ CENTRUM

## 1.1 Obecně

Dohledová a poplachová přijímací centra (DPPC), stále ještě dnes označovaná také jako pulty centralizované ochrany (PCO), nebo anglicky Alarm receiving center (ARC), přijímají signály a informace z různých technologických systémů s využitím nejmodernějších technologií. Operátoři (přímí pracovníci dohledového centra) vyhodnocují a reagují na příchozí události dle nastavených scénářů, postupů a svých zkušeností. Agentury provozující DPPC nabízejí zákazníkům své služby pro zvýšení úrovně bezpečnosti jejich zdraví, životů nebo majetků.



Obr. 1: Ukázka pracoviště operátora dohledového centra [1]

Technologické systémy jsou instalovány v objektech zákazníků DPPC a vyhodnocují mnoho různých veličin, na které je nutné požadovaným způsobem reagovat. Jak se vyspělé moderní technologie vyvíjejí, je nutností, aby i firmy poskytující služby v oblasti bezpečnostních systémů, nebo firmy provozující bezpečnostní agentury reagovaly inovací svých technologií, ale také zvýšením úrovně znalostí svých zaměstnanců. Dohledová centra a všichni jejich pracovníci nejsou v tomto směru výjimkou. Na techniky bezpečnostních systémů, administrátory, supervisory a v neposlední řadě na operátory jsou kladeny čím dál větší požadavky. Je nutností, aby všichni odpovědní pracovníci znali svoje pracovní povinnosti a kompetence.

Již není pravdou, že se na DPPC připojují objekty pouze z bezpečnostního hlediska, ale náročtí zákazníci žádají „střežení“ všech možných veličin, které jsou důležité, např. pro jejich ekonomickou činnost. Práce operátora dohledového centra se stává náročnou na znalost všech možných technologií, alespoň z pohledu reakce na vzniklou událost. Operátor tak musí mít přehled, z jaké technologie příchozí zpráva pochází a k čemu slouží. V opačném případě není možné, aby operátoři kvalifikovaně reagovali.

## 1.2 Normativní požadavky

Tab. 1: Příklady technologií připojitelných na DPPC

| | Označení | Technologie |
|---|---|---|
| **Poplachové systémy** | PZTS<br>(EZS) | Poplachové zabezpečovací a tísňové systémy<br>soubor ČSN EN 50 131 |
| | VSS<br>(CCTV) | Dohledové videosystémy<br>ČSN EN 62 676 |
| | SAS | Systémy přivolání pomoci<br>EN 50 134 |
| | EKV<br>(ACS) | Elektronické systémy kontroly vstupu<br>ČSN EN 60 839-11 |
| | AVDES | Audio a video dveřní vstupní systémy<br>ČSN EN 50486 a ČSN EN 62 676 |
| **Jiné systémy než poplachové** | EPS | Elektrické požární signalizace<br>ČSN 34 2710 nebo soubor norem EN 54 |
| | SIE | Systémy inteligentní elektroinstalace<br>řada ČSN EN 50 090 a ČSN 33 2000 |
| | ostatní | Systémy pro sledování a vyhledávání (např. vozidel)<br>Dohledová zařízení nad telekomunikačními systémy<br>Obchůzkové systémy<br>např. ČSN CLC/TS 50136-7 a ČSN CLC/TS 50398 |

V lednu 2020 byla přeložena a zveřejněna evropská norma EN 50 518:2019 – Monitoring and alarm receiving centre (dále jen „MARC“, resp. „ARC“[1]), v české verzi tedy ČSN EN 50 518 - Dohledová a poplachová přijímací centra.

Do 6. 2. 2022 bude tato norma souběžně platit s ČSN EN 50 518-1 ed.2, ČSN EN 50 518-2 ed.2 a ČSN EN 50 518-3 ed.2 ze září 2014. Nové normy reagují na rozšíření technologií, které jsou schopné předávat informace o stavech a událostech na DPPC, a neomezují je pouze na příjem, zpracování a odezvu od systémů generované poplachovými zabezpečovacími a tísňovými systémy. Pod pojem „Poplachové systémy“ (normy zpracovávané technickou komisí CLC/TC 79) jsou v této normě, kromě poplachových zabezpečovacích a tísňových systémů (PZTS nebo I&HAS), zařazena také zařízení pro dohledové videosystémy, systémy přivolání pomoci, systémy kontroly vstupu a audio a video dveřní vstupní systémy. ARC jsou schopny přijímat, zpracovávat a iniciovat odezvy také na příchozí události generované i jinými systémy jako jsou elektrické požární signalizace, systémy pro sledování a vyhledávání (osob nebo vozidel) nebo dohledová zařízení nad telekomunikačními systémy [2].

I když stále není v platnosti zákon o soukromých bezpečnostních službách, tak se odpovědné osoby bezpečnostních agentur provozující dohledová centra snaží přizpůsobit svoje prostory i technologie na budoucí certifikaci DPPC dle aktuálně platných norem, a tím mít možnost získat licenci Ministerstva vnitra dle připravovaného zákona.


Obr. 2: Příklady monitorovaných zařízení [1]

[1] Zkratka MARC popisuje úplný funkční rozsah dohledového poplachového a přijímacího centra (DPPC). Pro dosažení konzistence terminologie je v ČSN EN 50 518 i v tomto dokumentu používaná zkratka ARC (DPPC), kde MARC je ekvivalentní ARC [2].

Norma pro DPPC stanovuje požadavky na návrh, konstrukci, zabezpečení, integritu a provoz pro dvě kategorie ARC, kde ARC kategorie I bude na vyšší úrovni než ARC kategorie II. Dle [2] (ČSN EN 50 518) je kategorizace závislá na typu přijímaných a zpracovávaných událostí a rozděluje jí následujícím způsobem.

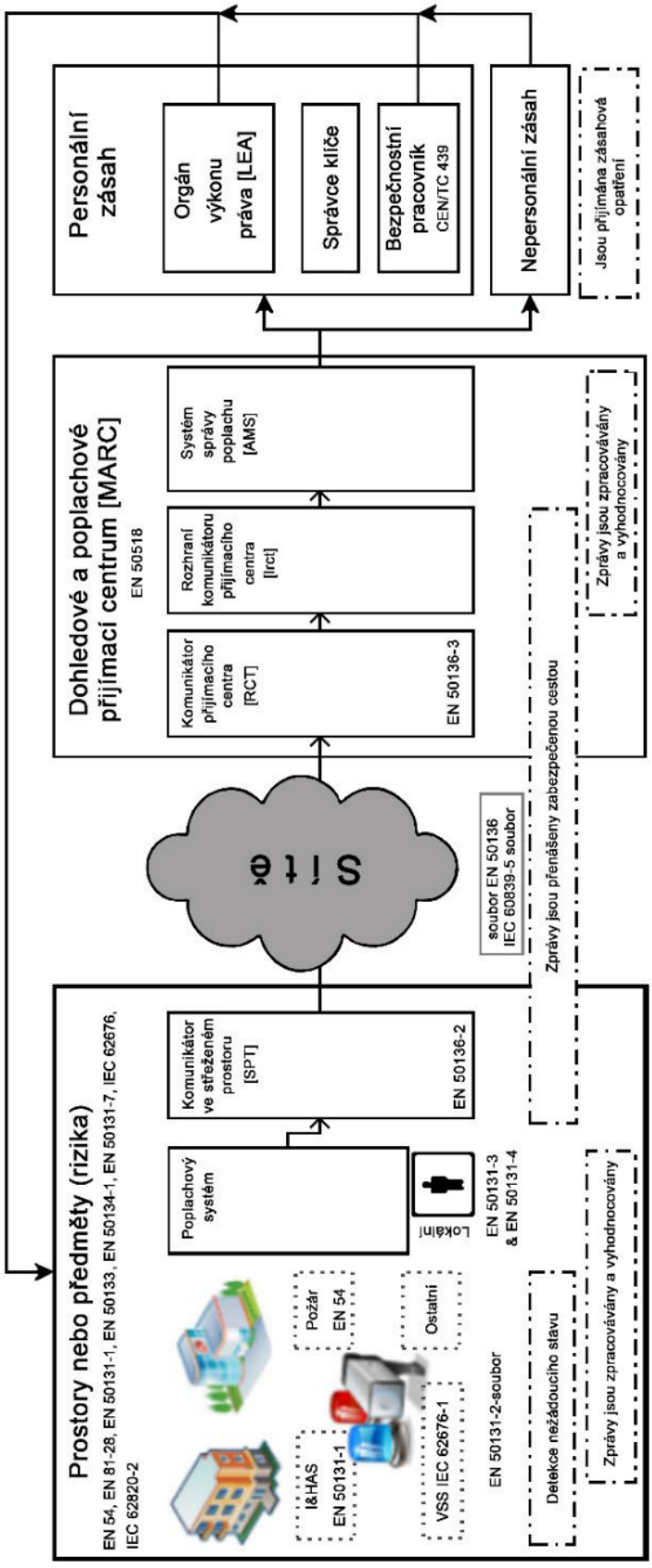
*Kategorie I: ARC zpracovávající zprávy z bezpečnostních aplikací:*

- *I&HAS,*
- *systém kontroly vstupu,*
- *VSS v bezpečnostních aplikacích, které vyžadují reakci na mimořádnou událost,*
- *monitorování lidí, osamělých pracovníků a systémy pro sledování objektů pro bezpečnostní aplikace,*
- *poplachové zprávy zpracované podle ARC kategorie II,*
- *kombinace výše uvedených systémů.*

*Kategorie II: ARC zpracovávající zprávy z jiných než bezpečnostních aplikací:*

- *elektrická požární signalizace,*
- *stabilní hasící zařízení,*
- *systémy přivolání pomoci,*
- *audio/video systémy vstupu dveří,*
- *VSS v jiných než bezpečnostních aplikacích,*
- *monitorování lidí, osamělých pracovníků a systémy pro sledování objektů pro jiné než bezpečnostní aplikace,*
- *systémy nouzových výtahů,*
- *kombinace výše uvedených systémů.*

Celý princip poplachového procesu, včetně následných vazeb, vyjádřili tvůrci předpisu v grafické podobě řetězcového diagramu na *Obr. 3*.




Obr. 3: Řetězcový diagram celkového poplachového procesu [2]

# 2 VYBRANÁ ZAŘÍZENÍ PŘIPOJITELNÁ DO DPPC

## 2.1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Účelem montáže poplachových zabezpečovacích a tísňových systémů je pro majitele různých objektů zvýšit bezpečnost svého majetku nebo bezpečnost přítomných osob (referenčního objektu). Tyto systémy jsou tvořeny souborem bezpečnostních prvků, jako jsou ústředny, napájecí zdroje, ovládací prvky, různé typy detektorů (mnoho výrobců i dodavatelů označuje nesprávně čidla), výstražná zařízení nebo komunikátory (přenosová zařízení). Celý systém má pak za úkol, v případě zjištění narušení, napadení, technického poplachu nebo poruchového stavu, informovovat o vzniku události majitele nebo oprávněnou obsluhu na předem určených místech, např. zvukově (sirénou), opticky (majákem) nebo notifikací na mobilní telefon. Kvalitní montáži bezpečnostního zařízení by mělo předcházet bezpečnostní posouzení zabezpečovaného prostoru. Postup pro návrh, montáž i servis PZTS je zakotven v ČSN CLC/TS 50131-7 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace.

Tab. 2: Stupně zabezpečení PZTS dle ČSN 50 131-1 [3]

| | |
|---|---|
| **Stupeň 1:** | **Nízké riziko** |
| | Předpokládá se, že vetřelec nebo lupič mají malou znalost I&HAS a mají k dispozici omezený sortiment snadno dostupných nástrojů. |
| **Stupeň 2:** | **Nízké až střední riziko** |
| | Předpokládá se, že vetřelec nebo lupič mají omezené znalosti I&HAS a používání běžného nářadí a přenosných přístrojů (např. multimetr). |
| **Stupeň 3:** | **Střední až vysoké riziko** |
| | Předpokládá se, že vetřelec nebo lupič jsou obeznámeni s I&HAS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení. |
| **Stupeň 4:** | **Vysoké riziko** |
| | Používá se tehdy, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopní nebo mají možnost vypracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů I&HAS. |

Asociace technických bezpečnostních služeb Grémium Alarm z.s. (dále jen „AGA“) ve spolupráci s Ministerstvem vnitra ČR vypracovala v roce 2018 dokument STANOVENÍ ÚROVNĚ ZABEZPEČENÍ OBJEKTŮ A PROVOZOVEN PROTI VLOUPÁNÍ PODLE EVROPSKÝCH TECHNICKÝCH NOREM, který pak vydala Česká agentura pro standardizaci (dále jen „ČAS“). Dokument představuje přehled a pravidla pro aplikaci PZTS, společně s využitím mechanických zábranných systémů (dále jen „MZS“) a umožňuje optimalizaci zabezpečení majetku.


Obr. 4: Instituce podílející se na vzniku dokumentu – Stanovení úrovně zabezpečení objektů a provozoven [4]

Majitelé objektů také často využívají služby DPPC a své objekty a jejich bezpečnost svěřují kvalifikované obsluze bezpečnostních agentur. Operátoři dohledových center po přijetí události, dle připraveného scénáře, v ČSN EN 50 518 označován jako *standardní operační postup* (dále jen „SOP“), vyhodnotí vzniklou událost a provedou veškeré možné úkony k zabránění nebo zmírnění škodícího účinku (hrozby) na referenčním objektu [5].

Poplachové zabezpečovací a tísňové systémy (PZTS), často v technických dokumentacích a normách Intrusion and hold-up alarm systems (dále jen „I&HAS“), jsou stále označovány laickou, ale i odbornou veřejností jako systémy elektrické zabezpečovací signalizace (EZS) a operátoři se také mohou setkat s hovorovým označením *zabezpečovačka*.

Dle stupně zabezpečení (*Tab. 2*), které definuje norma ČSN EN 50131-1 ed.2 včetně změn, jsou základními funkčními požadavky na systémy PZTS detekovat, zaznamenat, vyhodnotit a předat zejména stavy uvedené v *Tab. 3*. Pro odpovědnou práci operátora DPPC je znalost typu vstupů PZTS bezpodmínečně nutná, jelikož příchozí zprávy na monitorech jednotlivých vyhodnocovacích softwarů pak plně korespondují právě s typem vstupu, resp. s typem příchozí události.

Manažeři DPPC na základě podrobné znalosti normativních požadavků, bezpečnostních systémů, montážních postupů a zejména svých zkušeností sestavují a do praxe uvádějí SOP pro

spolehlivý chod DPPC. Manažeři a následně operátoři si také musí uvědomit prioritu příchozích událostí, a to při své náročné práci vždy pečlivě vyhodnotit a zohlednit.

Tab. 3: Funkční požadavky na vstupy PZTS dle ČSN EN 50 131-3

| Typ vstupu | Popis |
|---|---|
| Narušení | Prostředky pro detekci, vyhodnocení a předání událostí typu poplach, narušení (např. detektor pohybu, magnet. kontakt). |
| Tísňové | Prostředky pro přivolání pomoci při tísňovém (ohrožujícím) stavu přítomných osob ve střeženém objektu (např. tísňový hlásič). |
| Sabotážní | Prostředky pro rozpoznání narušení fyzické celistvosti systémů PZTS (např. narušení krytů detektorů, ústředen, koncentrátorů nebo vedení). |
| Poruchové | Prostředky pro vyhodnocení poruchových stavů systémů PZTS (např. vadná baterie, výpadek napětí, chyba komunikace apod.). |
| Vstup / výstup uživatelů | Prostředky k přijetí a zpracování informací z uživatelských zařízení pro ovládání systémů PZTS (např. klávesnice, ovladač nebo čtečka). |
| Zakrytí, maskování | Prostředky pro rozpoznání úplného zakrytí detektorů a zabránění detekce narušení ve střeženém prostoru detektorem. |
| Snížení rozsahu pokrytí | Prostředky pro rozpoznání snížení rozsahu pokrytí detektorů. V určitých případech shodné se zakrytím, maskováním. |
| Nepoplachové (technické) vstupy | Prostředky pro vyhodnocení nepoplachových technických stavů měřených veličin. Tyto vstupy nesmí ovlivnit funkci bezpečnostních aplikací systému PZTS. |

### 2.1.1 Ústředna

Řídící jednotka neboli ústředna je centrální prvek PZTS, který je schopen dle interního programu vyhodnocovat a reagovat na příkazy a stavy ovládacích prvků, vstupních obvodů nebo měřených veličin pomocných obvodů.

Do vstupů ústředny (tzv. zón) se pak sbíhají všechny signály od detektorů, hlásičů, tísňových prvků nebo prostředků pro vyhodnocení různých technických stavů a veličin. Laickou, ale bohužel i odbornou veřejností jsou globálně tyto prvky často nazývány *čidly*. Všechny

poplachové stavy, které přichází na monitory operátorů v DPPC, jsou následkem reakce (vyhodnocení) prvků, které jsou připojeny právě na vstupy ústředen[2].

Základní desky systémů PZTS mají omezenou kapacitu počtu přímých vstupů. Pro rozšíření kapacity vstupních zón, v závislosti na velikosti střeženého objektu, se používají rozšiřující moduly, které nazýváme koncentrátory nebo expandéry.

Důležitou součástí pro chod systému PZTS je zálohovaný napájecí zdroj. Jelikož se jedná o bezpečnostní systém, je normativní podmínkou[3], aby ústředna uměla průběžně kontrolovat a měřit chod napájecí soustavy. Musí umět vyhodnotit přítomnost, poruchu nebo ztrátu napájecího napětí, nabíjení akumulátoru a zároveň také jeho stav. Zdrojová část je ve většině případů přímo integrována na základní desku ústředny PZTS, ale často se setkáváme i se zdrojem externím (přídavným), který může být umístěn kdekoliv v rámci instalace PZTS.


Obr. 5: Externí zdroj a ústředna PZTS v plechovém boxu [vlastní zdroj]

Na základní desce, případně na rozšiřujících modulech, jsou také umístěny výstupní obvody pro ovládání sirén, majáků nebo ovládaných zařízení (např. zamlžovací generátory, rolety, žaluzie nebo topení). Tyto výstupy jsou zpravidla volně programovatelné (dále jen „PGM“) a nastavuje je technik při montáži PZTS, dle požadavků projektové dokumentace nebo

[2] Přímý vstup označujeme u PZTS zónou, do které je připojen jeden nebo více detektorů, a v tom případě použijeme termín smyčka. Zóny jsou přiřazovány do bloků (sekcí nebo oblastí), které pak lze ovládat samostatně.

[3] V současné době se jedná o normu ČSN EN 50 131-6 ed.3: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 6: Napájecí zdroje.

zákazníka. Obvody PGM výstupů umožňují monitorovat jejich stavy, nežádoucí účinky nebo poruchy a předávají veškeré informace do řídících jednotek.

Tab. 4: Příklady výrobců PZTS a příklady jejich ústředen

| Značka | Příklady PZTS ústředen a systémů |
|---|---|
| Satel | Polský výrobce, např. CA, Integra, Perfecta |
| DSC | Kanadský výrobce, např. 1832, 1864, PowerNeo, PowerSeries Pro |
| Honeywell | Mezinárodní společnost (UK), např. Galaxy Flex, Dimension |
| Paradox | Kanadský výrobce, např. Digiplex, Spectra/Magellan |
| Jablotron | Český výrobce, např. JA 100, 100+ |
| Siemens | Německá společnost, např. Sintony IC60, Intrunet SPC |

### 2.1.2 Ovládací prvky

Systémy PZTS je nutné ovládat uživatelem, např. zamknout (zakódovat, zastřežit) nebo odemknout (odkódovat, odstřežit), ale k dispozici jsou také různé režimy chování systémů nebo povely pro ovládaná zařízení (např. spustit topení, klimatizaci). Moderní doba dovoluje neomezené množství designového řešení ovládacích prvků, ale také nepřeberné množství technologických možností.

Ovládat PZTS může uživatel zadáním číselné kombinace (kódu) na klávesnici, přiložením přístupové karty ke čtečce nebo např. bezdrátovou klíčenkou. PZTS umožňuje integraci s jinými systémy (SIE, ACS nebo např. VSS), které zároveň mohou sloužit také k ovládání zabezpečovacího systému. Nejmladším zástupcem ovládání jsou mobilní aplikace[4] výrobců konkrétního zabezpečovacího zařízení. Uživatel může velice komfortním způsobem ovládat celý svůj systém PZTS.

Ovládací prvky, stejně jako rozšiřující moduly, se připojují k základním deskám, resp. řídícím jednotkám pomocí datové sběrnice systému. Komunikace mezi ústřednou a prvkem je

[4] Ověření přístupu řeší nově norma EN 50710 – Guidelines and requirements for Remote Services for fire safety and security systems – Pokyny a požadavky na vzdálené služby pro systémy požární bezpečnosti a zabezpečení vydané CEN/CENELEC v březnu 2020.

obousměrná a zároveň je komunikace dohledovaná. Na klávesnicích, tablech nebo v aplikacích je možné vyčíst veškeré funkční stavy systému nebo jeho historii. Uživatel je tak plně informován o proběhlém poplachu nebo poruše.


Obr. 6: Přístupový modul se čtečkou karet a LCD klávesnice [vlastní zdroj]

### 2.1.3 Detektory

Prvky systému PZTS, které na základě změny fyzikálních vlastností okolí vyhodnocují případné narušení a předávají tyto stavy do vstupů ústředny, nazýváme všeobecně detektory. Jaký typ detektoru, co bude detekovat (neboli účel použití), je v plné kompetenci bezpečnostního projektanta na základě vyhodnocení bezpečnostního posouzení objektu. Projektant musí zhodnotit okolí (vlivy prostředí) a veškeré požadavky na funkčnost jednotlivých detektorů. Zvláštní pozornost musí věnovat nežádoucím vlivům, které by mohly ovlivnit detekci, a tím vyvolávat plané poplachy ve střeženém prostoru. Z praxe víme, že vybavení prostor se postupem času mění (např. v létě otevřené okno), tím dochází také často ke změně nežádoucích účinků a detektory začnou vyhlašovat plané poplachy.

Pro práci operátora je velmi důležité znát a umět si přestavit jaký typ detektoru, pro jaké účely je v daném místě umístěn a jakou fyzikální veličinu daný prvek v systému vyhodnocuje. Operátor si musí uvědomit, jakou část daný detektor střeží (v jaké části objektu byl poplach vyvolán, např. perimetr, plášť atd.) a dle SOP[5], vlastních zkušeností nebo nedávné historie událostí přijmout veškerá možná opatření k zamezení nebo minimalizování škod na chráněném majetku nebo zdraví a životě lidí nebo zvířat.

[5] SOP – Standardní operační postup je předmětem praktické části diplomové práce.

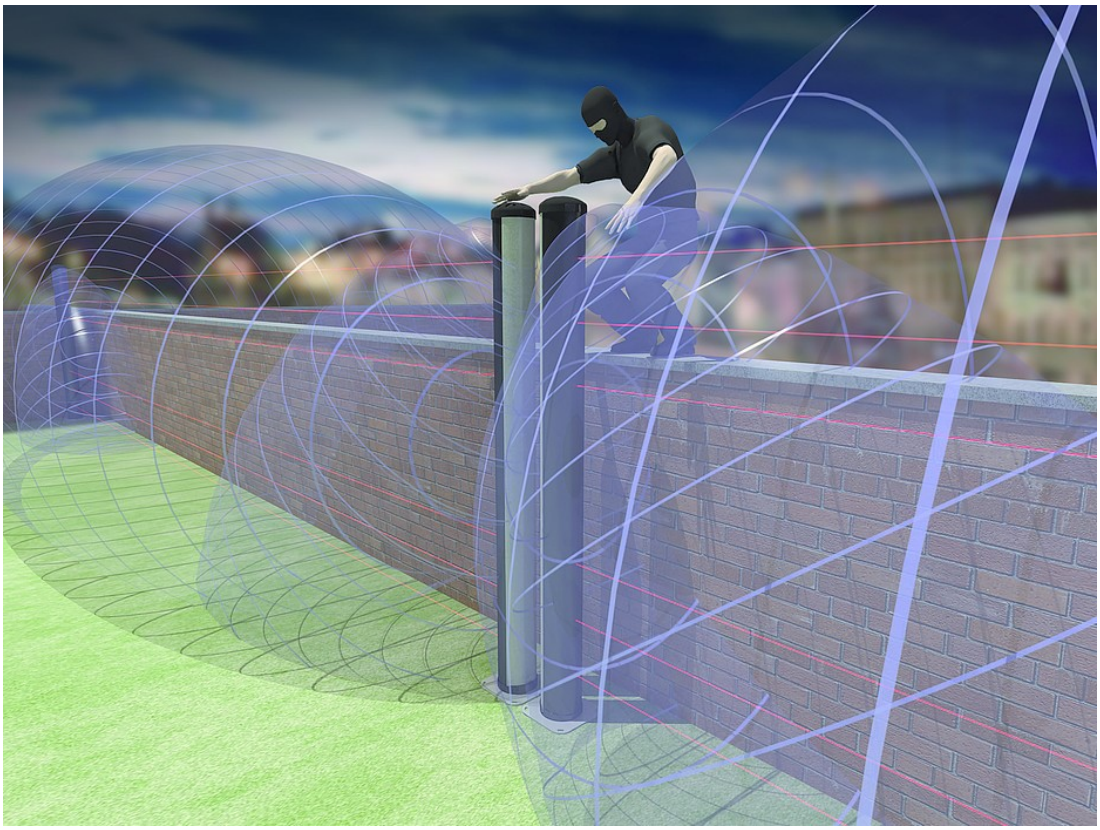
**Perimetrická ochrana**

Tab. 5: Příklady detektorů pro ochranu perimetrickou

| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| IR závora (bariéra) | Systém vysílače a přijímače infračerveného světla, který reaguje na přerušení paprsku. | Sníh, déšť, mlha, sluneční paprsky. |
| Plotový detekční systém | Systém instalovaný na oplocení, např. ve formě mikrofonního drátu nebo otřesových (akceleračních) detektorů, které reagují na pohyb oplocení. | Vítr, zvěř, krupobití, akustické pole (např. projíždějící auto). |
| Mikrovlnná bariéra | Systém vysílače a přijímače, kde vzniká elektromagnetické pole s reakcí právě na jeho změnu. | Hustý sníh, déšť, krupobití, vysoké teploty. |
| Zemní štěrbinový kabel | Jedná se o systémy skryté detekční technologie na principu dvou kabelů, vyzařování a vyhodnocení elektromagnetického pole a jeho změn. | Zvěř, souběžná podzemní kabeláž, potrubí apod. |
| Venkovní pohybový detektor | PIR nebo duální PIR+MW detektor pro vyhodnocení pohybu ve venkovním krytí. Jedná se o nejzákladnější prvky vyhodnocení pohybu. | Sníh, déšť, mlha, sluneční paprsky, vítr, vysoké teploty. |
| Laserový detektor | Pracující na principu vyhodnocení odrazu rozptýleného infračerveného laserového paprsku. | Velmi hustý sníh, déšť, mlha, krupobití. |

V případě, že zákazník vyžaduje nebo je mu bezpečnostním posouzením doporučeno střežit venkovní prostory objektu, může využít obvodové ochrany. Perimetrické detektory většinou pokrývají pouze určitou linii chráněného prostoru, proto jsou často montovány po obvodu pozemku, nebo jako příčná past v předem vytipovaném místě pravděpodobného pohybu nežádoucích osob. Obvodové ochrany je nejčastěji využito v případech zabezpečení fotovoltaických elektráren, pískoven nebo např. sběren barevných kovů. Detektory mívají dlouhý dosah střežené linie (desítky až stovky metrů) ve venkovním prostředí a jsou velmi často náchylné na vnější podněty okolí, proto jsou častým zdrojem falešných poplachů. Ve většině případů jsou chráněné prostory doplněny podpůrnými prostředky k omezení falešných zpráv, např. v podobě kamerového systému (VSS). Výrobci zařízení se snaží o eliminaci falešných

poplachů implementací moderních technologií a sofistikovanějších algoritmů při vyhodnocování detekce [6].



Obr. 7: Příklad perimetrické ochrany – kombinace laser + MW bariéry [6]

**Plášťová ochrana**

Pro detekci neoprávněného vstupu do chráněné budovy (nebo její části) slouží plášťová ochrana. Detektory mohou střežit pouze stavební otvory zájmové oblasti nebo i celé stěny. Detektory plášťové ochrany patří k základním typům zabezpečení systémem PZTS a jsou vyžadovány i při nejnižším stupni zabezpečení (viz Tab. 2: Stupně zabezpečení PZTS dle ČSN 50 131-1 Tab. 2). Prvky plášťové ochrany by měly být montovány na každém objektu, kde je systém PZTS vyžadován.

Nejjednodušší detekce spočívá ve vyhodnocení otevřených vstupních dveří nebo detekce rozbití okna. Tento typ detekce bývá nejméně náchylný na falešné poplachy v systému. Samozřejmostí tohoto tvrzení je bezvadná montáž jednotlivých komponent a proškolená obsluha, která dbá provozních náležitostí a podmínek používání.

V případě použití infrazávor, bariér se jedná o vyspělejší detekci plášťové ochrany, která je hůře překonatelná pachatelem, ale také je více náchylná na plané poplachy díky přírodním vlivům, stejně jako prvky perimetrické ochrany.

Tab. 6: Příklady detektorů pro plášťovou ochranu

| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Magnetický kontakt | Jazýčkové relé ovládané permanentním magnetem. Signalizace otevřených dveří, vrat, oken nebo např. mříží. | Nesprávná montáž, vůle zavřených křídel, ale také uživatel. |
| Detektor tříštění skla | Vyhodnocení zvuku tříštění skla pomocí mikrofonu v detektoru, nebo vyhodnocení tlakové vlny. | Rušivé akustické pole, např. ohňostroj. |
| Vibrační detektor | Det. reaguje na otřesy při překonávání mechanických překážek, např. vybourání zdi, staveb. otvorů | Přilehlá komunikace, nežádoucí otřesy. |
| IR záclona | Specifický PIR detektor s charakteristikou záclony pro střežení průchodu např. dveřmi nebo oknem. | Sluneční paprsky, průvan, hmyz. |
| IR bariéra | Systém vysílače a přijímače infračervených paprsků tvořících bariéru. Reaguje na přerušení paprsků. Zohledňuje velikost nežádoucího objektu. | Povětrnostní vlivy, sluneční paprsky, ptactvo. |

Obr. 8: Detektor tříštění skla, pohybu a magnetický [vlastní zdroj]

### Prostorová ochrana

Jak vyplývá z názvu, jedná se o ochranu vnitřního prostoru zabezpečeného objektu. Na případného pachatele po překonání překážek v plášti objektu jsou nastraženy další prvky, které mají za úkol detekovat a upozornit na jeho pohyb uvnitř objektu. Touto detekcí by měly být vybaveny všechny prostory, kde se předpokládá pohyb narušitele, a všechny prostory s cenným majetkem.

Nejčastěji používanými prvky jsou detektory vyhodnocující pohyb pasivním nebo naopak aktivním způsobem detekce. Výrobci detektorů využívají a zlepšují detekci svých výrobků implementací nejmodernějších technologií a algoritmů vyhodnocování. U starších instalací se můžeme setkat s častějším výskytem falešných poplachů, zapříčiněných nevhodnou volbou místa instalace, pohybem hmyzu, pavouků v blízkosti detektorů, ale také provozem zařízení ovlivňujících detekci pohybu detektorem (např. pohyb kapaliny v rozvodech topení, záclony apod.).

Jedná se o nejčastěji používanou formu zabezpečení systémem PZTS, která dokáže informovat uživatele nebo zasahující skupinu o pohybu narušitele po jednotlivých částech střežené budovy (objektu). Bohužel ale s častou absencí prvků plášťové ochrany je vyhodnocení události náročnější a často vede k planým výjezdům zásahových jednotek.

Tab. 7: Příklady detektorů pro prostorovou ochranu

| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| PIR detektor - montáž na stěnu, nebo strop | Detekce vychází z principu vyhodnocení změn ve vyzařování infračerveného záření v zorném poli detektoru. | Světlo, slunce, rychlé změny teplot, průvan, hlodavci apod. |
| Duální PIR+MW detektor | Je PIR doplněn o mikrovlnou část, která pracuje na principu vyhodnocení Dopplerova jevu a poplach je vyvolán kombinací obou částí. | Domácí zvířata, špatné nastavení citlivosti senzorů. |
| Ultrazvukový detektor | Vyhodnocuje změny vyslaných ultrazvukových vln od odražených předmětů nebo těles ve střeženém prostoru. | „Vidí“ skrze stěny a může detekovat objekty i za zdí. |

Obr. 9: Detektor pohybu – PIR, PIR a hlásič kouře [vlastní zdroj]

**Předmětová ochrana**

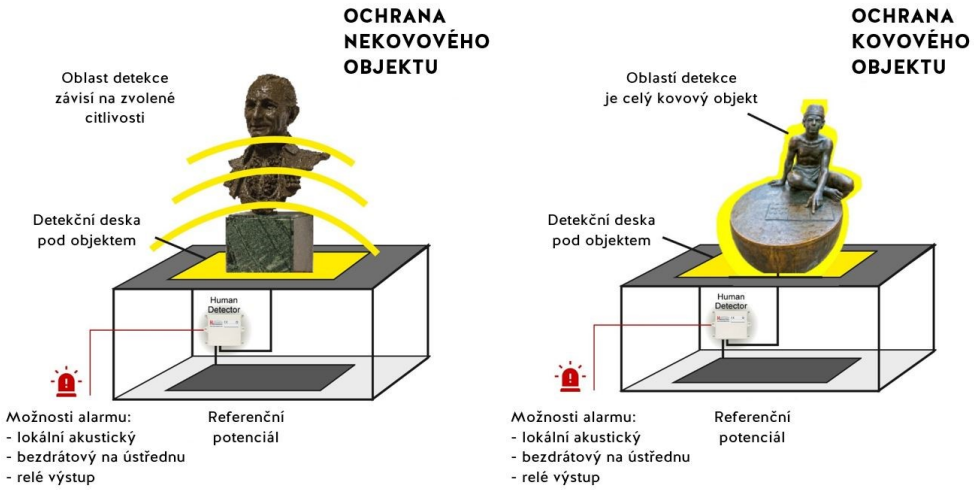
V případech potřeby lépe zabezpečit konkrétní cenný předmět ve střeženém prostoru (případně mimo přímo střežený prostor) může uživatel využít doplnění svého bezpečnostního systému o prvky předmětové ochrany. Jedná se o zařízení, která přímo vyhodnocují manipulaci s chráněným předmětem (např. trezor, obraz, socha).

Tab. 8: Příklady detektorů pro předmětovou ochranu

| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Mechanický kontakt | Nejjednodušší detekce na principu sepnutí/rozepnutí mikrospínače. | Mechanická část, případně sabotáž. |
| Závěsné detektory | Systém lanka a zavěšení předmětu na něj s vyhodnocením tažné síly na senzoru. | Průvan, únava materiálu. |
| Detektor přemístění | Reaguje na změnu své polohy pomocí akceleračních nebo náklonových senzorů. | Rušení bezdrátového přenosu, akumulátor. |
| Kapacitní detektor (Human Detector) | Speciální detekce založená na snímání pouhého doteku na chráněný předmět. | Dle výrobce neexistují rušivé vlivy. |

Řada detektorů, výše zmíněných, může také sloužit k ochraně předmětů (např. mag. kontakt, otřes. detektor nebo IR/laser bariéra). Projektant systému musí vždy dobře zhodnotit vhodnost použitého prvku detekce s ohledem na konkrétní podmínky. Existuje celá řada

speciálních a přímo určených technologií na vyhodnocení narušení bezpečnosti cenných předmětů. Vhodným doplňkem, nebo v dnešní době i detektorem, může být i kamerový systém.



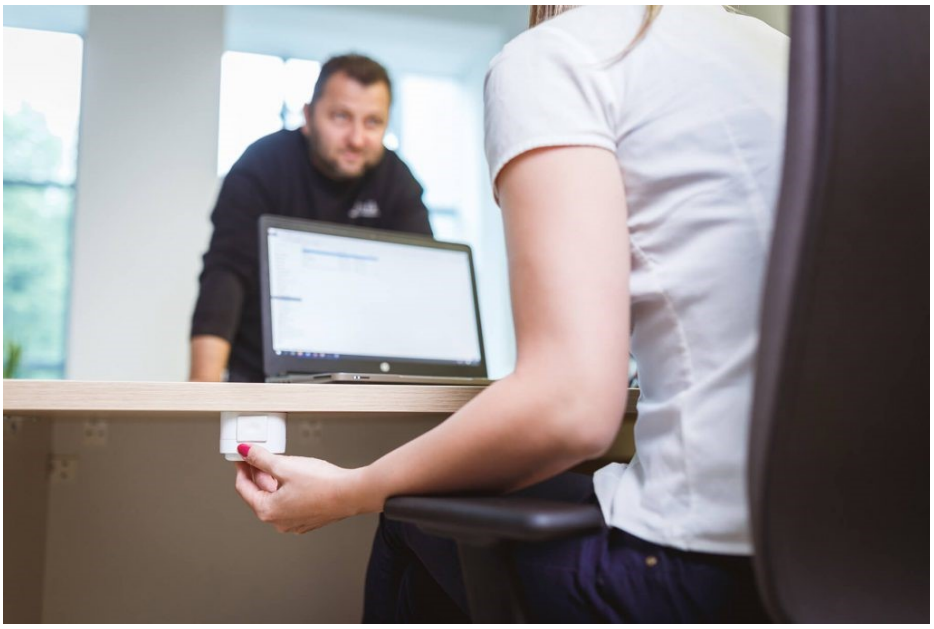

Obr. 10: Systém Human Detector [7]

**Prostředky pro přivolání pomoci**

Bezpečnostní systémy neslouží pouze pro zvýšení ochrany majetku, ale vyrábí a používají se prostředky, které při aktivaci vyvolají reakci pro přivolání pomoci. Může se jednat o situaci ohrožující zdraví nebo život přímo monitorovaných osob (asistenční služba), ale také osob přítomných v určitém rizikovém prostředí (např. přepážky bank, pošt). Hlásiče přivolání pomocí mohou být pevně montovány, nebo se setkáváme s přenosnými panikovými tlačítky. Výbava těchto hlásičů může také obsahovat např. GPS přijímač a přenos na DPPC pomocí GPRS, v tom případě operátor může ohroženou osobu přesněji lokalizovat.

Reakce ústředny na vyvolaný poplach je závislá na nastavení typu vstupu (zóny), kdy poplachy tísňového charakteru (např. přepadení) nesmí upozornit na tísňové hlášení pachatele trestného činu. Proto se programují a na DPPC zobrazují jako tichá tíseň. Operátor v tomto případě musí správně vyhodnotit, jestli je vhodné kontaktovat oprávněného uživatele telefonicky pro verifikaci poplachu. Upřednostňuje se vyslání výjezdové skupiny (případně jednotku PČR) s ohledem na akční plán objektu. Bohužel v praxi (i vzhledem ke skryté montáži) je tento typ ochrany častým zdrojem planých poplachů při nechtěném spuštění obsluhou. Hlasitá tíseň je naopak dobře využitelná pro přivolání pomoci, např. při zdravotních

problémech hlídané osoby a operátor se ve většině případů spojuje dle akčního plánu s kontaktní osobou.



Obr. 11: Umístění tísňového tlačítka [8]

Tab. 9: Příklady tísňové ochrany

| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Tísňové tlačítko | Princip mikrospínače, manuální stisk. | Opotřebení, obsluha. |
| Bezdrátové tísňové hlásiče | Princip mikrospínače, mohou obsahovat akcelerometry apod. | Baterie, bezdrátový dosah, rušení, obsluha. |
| Detektor poslední bankovky | Mikrospínač a šachta, v níž je bankovka, při vysunutí spustí poplach. | Opotřebení, namáhané kabelážní systémy. |

**Ostatní aplikace**

Poplachové systémy ve své podstatě jsou schopny vyhodnocovat a přenášet události z jakéhokoliv detektoru nebo hlásiče jakékoliv fyzikální veličiny. Podstatou správného přenosu a následného vyhodnocení operátorem je správná konfigurace ústředny na poplachový vstup.

V praxi se často využívá např. při hlídání teplot v prostorách (serveroven, drůbežáren, odchoven prasat) nebo činnosti klimatizačních jednotek, vodních čerpadel apod.

Zvláštní pozornost vyžadují požární hlásiče připojené na systém PZTS, kdy je vyžadována lokální detekce kouře. V žádném případě tyto systémy nenahrazují elektrickou požární signalizaci, kterou předepisuje PBŘ na základě požadavku norem a operátor k hlášení typu požár musí použít verifikační proces, než oznámí událost na operační středisko HZS.

Tab. 10: Příklady ostatních detektorů a hlásičů připojitelných do PZTS

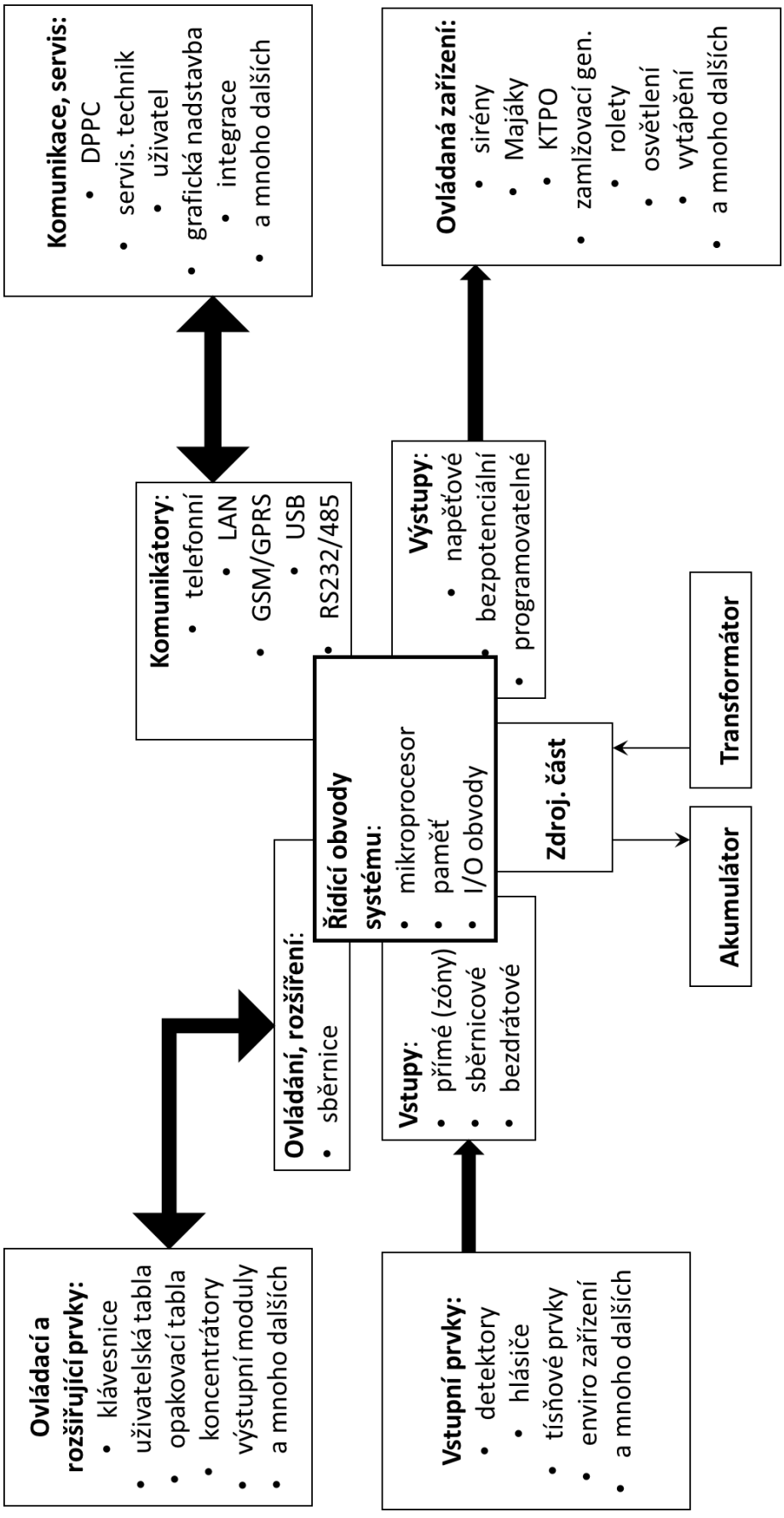
| Detektor | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Kouřový hlásič požáru | Detekce zakouření prostoru. | Teploty, pára, prach, špatné umístění. |
| Teplotní hlásiče požáru | Detekce maximální nebo diference teploty. | Průvany, prach, špatné umístění. |
| Plynové detektory | Detekce úniku plynů (např. zemní plyn, CO) | Zanesení senzoru. |
| Záplavový det. | Zjištěna hladina vody (např. pod pračkou) | Obsluha. |
| Měření teplot | Minimální nebo maximální teplota. | Minimální. |
| Chod el. zařízení | Hlášení poruch el. zařízení (např. čerpadlo) | Obsluha. |

**Sabotážní ochrana**

Pod tímto pojmem rozumíme ochranu samotného systému proti neoprávněnému zásahu nebo neúmyslného poškození, které by mohlo znemožnit správnou funkci aplikovaného řešení ochrany majetku nebo osob. Sabotáže systému vyhodnocují ústředny nezávisle na režimu, ve kterém se nacházejí (zamčeno/odemčeno), a při vyhodnocení situace sabotáže je nutné okamžitě reagovat na vzniklou událost. Může se jednat o přípravnou akci narušitelů bezpečnosti, nebo také o poruchový stav některých z komponent. Sabotážní smyčka prochází napříč celým systémem a v detektorech se připojuje na svorky tamperového kontaktu[6].

Samostatným oddílem sabotáže systému můžou být detekce zakrytí, maskování nebo snížení rozsahu pokrytí detektoru. Tato funkce detekce a vyhodnocení je vyžadována u všech prvků, které jsou montovány do vyšších stupňů zabezpečení (3, 4 st.), a nazýváme ji antimasking.

[6] Tamper – ochranný kontakt detektoru, ústředny nebo ostatních modulů bezpečnostního systému.




Obr. 12: Všeobecné blokové schéma systémů [vlastní zdroj]

## 2.2 Elektrická požární signalizace

Primárním účelem systémů EPS je včasné varování a evakuace přítomných osob ve střeženém prostoru pomocí vyhlášení *VŠEOBECNÉHO POPLACHU* o vznikajícím nebezpečí v podobě požáru. V první fázi je informována proškolená obsluha a ta má za úkol provést veškeré možné kroky k odvrácení nebezpečí. Pokud to již není možné a dochází k nekontrolovatelnému rozvoji požáru, je zapotřebí evakuovat přítomné osoby a přivolat pomoc hasičské jednotky (dále jen „JPO“).

Na rozdíl od PZTS a ostatních bezpečnostních systémů, je povinnost instalace, provozu a údržby v určitých objektech dána zákonnými předpisy[7]. Na základě požadavků schváleného požárně bezpečnostního řešení stavby (dále jen „PBŘ“) projektant provede návrh systému EPS dle platných norem a pokynů výrobce zařízení. EPS patří k vyhrazeným požárně bezpečnostním zařízením, a proto projektování, montáž, údržbu a zkoušky může provádět pouze osoba, která splňuje zákonné předpisy dle vyhl. 246/2001 Sb. §10.

Provoz EPS může být v objektu obsluhovaný, tzn. dvoučlenná obsluha 24 hodin 7 dní v týdnu, nebo může být využito připojení a přenosu zpráv na operační středisko KOPIS HZS příslušného kraje. Přenosové trasy poskytují firmy, které mají s krajským oddělením HZS podepsanou smlouvu o spolupráci a zároveň také splňují podmínky pro připojení provozovatele zařízení dálkového přenosu a PCO[8] (dle přílohy č.1 smlouvy o spolupráci s HZS). Objekty, které mají být připojeny na PCO HZS musí bezpodmínečně splňovat veškeré technické podmínky pro připojení EPS na PCO příslušného krajského oddělení HZS (dále jen „TP HZS“).

### 2.2.1 Ústředna

Stejně jako u ostatních systémů, je základním řídícím prvkem EPS ústředna, která obsahuje zdrojovou část, část zálohování napájení, komunikační rozhraní, vstupní a výstupní obvody. Ústředny EPS jsou také plně konfigurovatelné a rozšiřitelné pomocí přídavných modulů

[7] Zákon o požární ochraně č. 133/1985 Sb., který definuje podmínky pro účinnou ochranu života a zdraví osob a majetku, vyhláška o požární prevenci č. 246/2011 Sb. a vyhl. 23/2008 Sb. o technických podmínkách PO staveb. Těmito zákonnými prostředky se určité normy pro návrh, provoz, kontroly, údržby a opravy EPS stávají závaznými. Např. ČSN 73 0875 (PBŘ), ČSN 34 2710 (návrh, provoz, kontroly, údržby a opravy EPS) nebo soubor norem EN 54 (výrobní normy).

[8] HZS ve svých dokumentech, smlouvách nebo technických podmínkách využívá pouze označení PCO.

a periferií. Vnitřní program ústředny vyhodnocuje hlášení a stavy veškerých hlásičů nebo ostatních periferií (např. požární klapky) a dle nastavení instalačního technika vyvolává reakci systému na vzniklou událost.

V případě, že je EPS přepnuta do režimu DEN[9] (obsluha je přítomna) a dojde k vyhlášení poplachu typu požár, spustí ústředna čas T1 (max. 1 minuta) a bzučákem upozorní obsluhu o vzniku události. Obsluha v čase T1 musí na table ústředny odbavit událost a zahájit kontrolu místa hlášení, a to v době, kterou nazýváme čas T2 (max. 6 minut). Kontrola musí proběhnout do skončení času, včetně znovunastavení ústředny. Pokud z nějakého důvodu obsluha nestihne odbavit poplach v daném čase (T1 nebo T2), přejde ústředna k vyhlášení *VŠEOBECNÉHO POPLACHU*. V případě zjištění požáru je obsluha povinna potvrdit poplach použitím požárního tlačítka, kdy ústředna vyhlásí poplach okamžitě. V opačném případě, kdy ústředna je v režimu NOC (neobsluhovaná EPS), dojde k vyhlášení *VŠEOBECNÉHO POPLACHU* při první poplachové zprávě [9].

### 2.2.2 Hlásiče

Vstupní, detekční prvky (hlásiče) se připojují na kruhovou linku do vstupů linkové karty ústředny. Kruhová linka se využívá především z důvodu zajištění komunikace hlásičů s ústřednou i v době požáru a určitá část vedení nemusí být tak plně funkční. Každý vstupní prvek má svou jedinečnou adresu[10], a tím je možné získat přesné označení místa hlášení události. Hlásiče se programově přiřazují do zón (sekcí nebo oblastí), dle odpovídající části budovy a toto nastavení pak přímo ovlivňuje chování ovládaných zařízení.

Jelikož požáry doprovází různé jevy (kouř, teplo) vznikající při hoření látek, je důležitou součástí instalace EPS vhodná volba hlásičů na konkrétní místo instalace.

Hlásiče dělíme do dvou základních skupin:

- hlásiče manuální – tlačítkové,
- hlásiče automatické [10].

---

[9] Nastavení režimu DEN/NOC a časy T1, T2 musí být stanoveny v rámci návrhu PBŘ a EPS. Po schválení PD HZS není možné toto nastavení svévolně měnit.

[10] TP HZS již neumožňují připojení na PCO HZS neadresný systém EPS, proto v diplomové práci nebude uváděn.

U tlačítkových hlásičů je zřejmé, že k vyhlášení události dojde po manuálním zásahu obsluhy, nebo jiné osoby v objektu, která zpozorovala požár. Události z manuálních hlásičů přímo vyvolávají všeobecný poplach, spouští sirény, ovládají jiná požárně bezpečnostní zařízení (např. evakuační výtah, požární klapky apod.) a aktivují přenos na PCO HZS.


Obr. 13: Tlačítkový hlásič [11]

U automatických hlásičů očekáváme samočinnou detekci podnětné události a předání informace ústředně EPS k dalšímu vyhodnocení a upozornění obsluhy. Automatické hlásiče dělíme do skupin dle velikosti střežených úseků na:

- bodové – střeží většinou kruhový prostor pod sebou (např. Obr. 9),

Tab. 11: Příklady bodových hlásičů požáru

| Hlásič | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Opticko-kouřový | Založen na principu zachycení odrazu světelného paprsku v kouřové komoře hlásiče. | Vodní páry, prudké změny teplot (mlžení). |
| Teplotní | Reaguje na maximální nastavenou teplotu, nebo rychlou změnu teploty v prostoru. | Prudké změny teplot. |
| Ionizační | Dnes již nepoužívaný, princip ionizace vzduchu radioaktivním prvkem. | Téměř bez rušivých účinků. |
| Plamenný | Detekce založena na vyhodnocení přítomnosti UV a IR projevů při hoření. | Sluneční záření, přímé osvětlení. |
| Multisenzorový | Obsahuje kombinaci různých typů detekce. | Eliminuje fal.poplach. |
| CO | Zachycení zplodin vzniklých při hoření. | Dopravní prostředky. |

- lineární – střeží celou linii prostoru (např. skladové haly).

Tab. 12: Příklady lineárních hlásičů požáru

| Hlásič | Stručný popis | Rušivé účinky, např. |
|---|---|---|
| Kouřový lineární | Princip vysílače – přijímače IR paprsků a vyhodnocení snížení překážky v dráze. | Vodní páry, prudké změny teplot (mlžení). |
| Lineární teplotní kabel | Reaguje na maximální nastavenou teplotu, nebo rychlou změnu teploty v prostoru. | Prudké změny teplot. |
| Nasávací (i ve variantě bod. det.) | Pro náročné aplikace, nasávání vzduchu do trubic, detekce ve vyhodnocovací jednotce. | Prach, ucpaní nasávacích otvorů. |

### 2.2.3 Ovládací prvky

Jako u každého systému je i u EPS nutné ovládání nebo zobrazení hlášení o poplaších a poruchách. Zařízení k tomu určená nesou všeobecně název tabla. Umístění může být přímo na ústředně (pokud je v dosahu vstupu a obsluhy) nebo jsou montovány u vstupů do objektu a v případě obsluhovaného pracoviště i u obsluhy EPS (zároveň bývá i ohlašovnou požárů). Na tablech jsou zobrazována veškerá hlášení EPS, včetně spuštění časů T1 nebo T2 a obsluha stiskem příslušného tlačítka vyvolá další reakci.

### 2.2.4 Obslužné pole požární ochrany


Obr. 14: Klávesnice PZTS, OPPO, DZP a ovládací tablo EPS [vlastní zdroj]

Obslužné pole požární ochrany (dále jen „OPPO“) a jeho montáž je dána požadavkem ČSN 73 0845 a ČSN 34 2710 v případech, kdy je nutné objekty vybavit zařízením dálkového přenosu (dále jen „ZDP“ - odst.3.2) s připojením EPS na PCO HZS příslušného kraje. Certifikované OPPO slouží ke standardizovanému obsluhování systému EPS jednotkami požární ochrany HZS. Umístění by mělo být vždy do 5 m od vstupu do objektu přeurčeného pro JPO HZS.

### 2.2.5 Klíčový trezor požární ochrany

Dalším doplňujícím zařízením při požadavku připojení na PCO HZS je klíčový trezor požární ochrany (dále jen „KTPO“), v němž je uložen generální klíč od všech prostor střežených systémem EPS. Ústředna v případě vyhlášení všeobecného poplachu vydává povel k otevření prvních dvířek certifikovaného KTPO, tento stav je zároveň přenášen na DPPC agentury provozující přenosovou trasu ZDP. Umístění je v místech předpokládaného nástupu JPO HZS.


Obr. 15: Příklad umístění KTPO, [12] upravil Krejčí 2020

## 2.3 Dohledové videosystémy

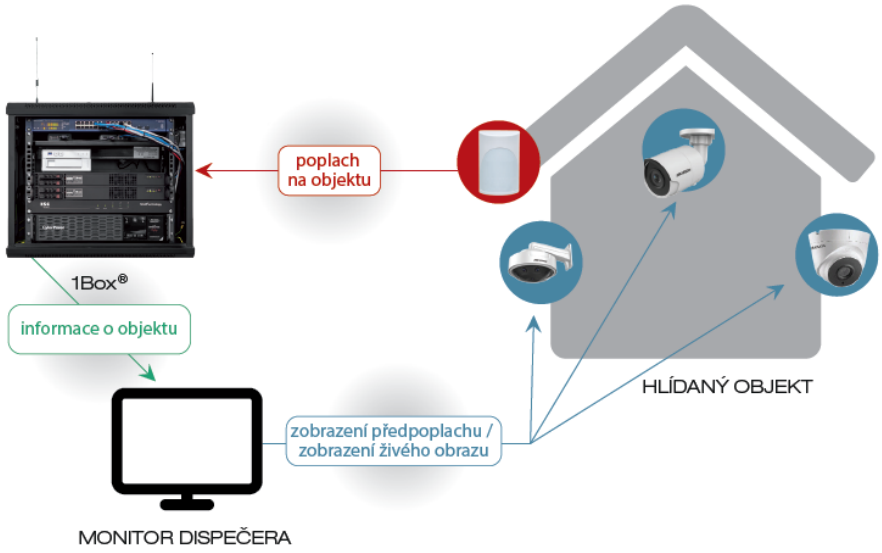
Za nejrychleji se rozvíjející bezpečnostní zařízení se dají označit dohledové videosystémy (dále jen „VSS“), které známe většinou pod označením kamerové systémy (CCTV). VSS jsou velmi žádaným doplňkovým zařízením pro zvýšení bezpečnosti střežených prostorů. Systémy velice dobře plní funkci preventivního opatření, i když jejich primární funkce je

přenos obrazu na dohledové pracoviště (místně nebo vzdáleně) uživatele a archivace pořízených záznamů. Díky rozvíjejícím se technologiím je obraz z kamerových systémů více kvalitnější, ve větším rozlišení, ale také je umožněno rychlejší předávání snímků pomocí datových sítí k uživateli. Stále častěji se setkáváme s implementací různých detekčních a vyhodnocovacích algoritmů přímo do jednotlivých kamer, ať se jedná o detekci opomenutého zavazadla, narušení vyhrazeného prostoru, měření teploty lidského těla nebo např. ztráta předmětu v detekční zóně. Mnoho různých aplikací pak směrují výrobci na alarmové výstupy kamer, aby včas upozornili obsluhu na vznikající možnost narušení bezpečnosti. Je otázkou času, kdy kamerové systémy budou přímo připojovány na běžná dohledová centra a přímo budou spouštět poplachové akce, včetně videoverifikace.

V současnosti jsou VSS připojovány na DPPC jako podpůrný prostředek pro verifikaci příchozí události z monitorovaného objektu jiných zařízení. Operátor má tak možnost, resp. povinnost, pokud je takový systém instalován a zpřístupněn, připojit se vzdáleně do VSS a zkontrolovat dění v objektu pomocí kamerového systému (existují systémy, které automaticky pořizují a zasílají sekvence obrazů na monitory operátorů).

Řada zákazníků také žádá tzv. službu videodohledu, kdy se operátorům na monitorech střídají obrazy z různých kamer a je jejich povinností sledovat případné narušení bezpečnosti. Ovšem bez kvalitní videoanalýzy a následného upozornění se jedná o zjištění čistě náhodné a je třeba tuto službu brát čistě jako doplňkovou.

Operátor při verifikaci kamerovým systémem si musí uvědomit a dodržovat pravidla související s ochranou osobních údajů a nařízení GDPR.




Obr. 16: Komunikační schéma 1Box video [13]

# 3 KOMUNIKACE ZAŘÍZENÍ A PPC

Nejenom každé z výše zmíněných zařízení je schopné předávat informace o svých vyhodnocených stavech na servery PPC (ARC). Komunikace mezi koncovým zařízením a serverem PPC probíhá v kódované formě předávání. V dnešní době je kladen důraz na bezpečnost těchto informací v době přenosu, a k tomu je využíváno ověřování a šifrování. Ovšem tuto možnost mají pouze modernější technologie a navzájem kompatibilní periferie. Každá přenosová soustava nese svoje specifikace spolehlivosti, odolnosti, ale také finanční náročnosti [3].

## 3.1 Komunikační trasy

Řídící jednotky předávají informace o svém stavu pomocí interních komunikátorů na periferie určené pro komunikaci s PPC. ČSN EN 50 518 definuje všeobecně pojmem *poplachové přenosové zařízení (ATE)*. Komunikační schéma je patrné z Obr. 3.

**Telefonní komunikace**

Je nejstarší technologie přenosu informací z ústředen PZTS, ale stále ještě používaná zvláště u starších, původních instalací. Interní komunikátory PZTS jsou připojeny přímo na přípojky JTS a pomocí hovorového pásma předávány na zařízení sloužící pro příjem a dekódování telefonních zpráv. Bezpečnostní agentury se tento typ komunikace snaží nahradit jinou, rychlejší a bezpochyby bezpečnější přenosovou cestou i u dlouholetých zákazníků.

**Internetová komunikace**

Dnes již téměř všichni výrobci zařízení a systémů umožňují využití nejmodernější komunikační prostředků koncových zařízení s dohledovými centry. Ať již přímo integrovanými komunikátory na základních deskách, nebo pomocí externích komunikátorů se přepojují zařízení zákazníků přes celosvětovou síť internetu k přijímačům PPC. Koncové prvky komunikační trasy mohou využít pevných přípojek od poskytovatelů služby internetu, nebo mohou využít datových služeb mobilních operátorů. Internetová komunikace mezi zařízeními se dá zařadit mezi velice spolehlivé a dnes i nejčastěji používané. Zákazník, který chce mít větší jistotu přenosu zpráv, využívá zálohovaných komunikátorů s připojením pevného internetu a zároveň pomocí datových služeb mobilního operátora, nebo kombinaci GPRS se záložní SMS. Výhodou internetové komunikace je její téměř neomezená šířka pásma, proto připojená zařízení mohou předat více informací o svých stavech.

**Komunikace pomocí GSM**

Byla hodně rozšířenou alternativou přenosu po telefonních linkách, kdy se využívalo hovorového pásma, nebo k přenosu zpráv z vysílače do přijímače GSM pomocí šifrovaných SMS zpráv [3]. V dnešní době se SMS zprávy využívají především jako záložní kanál pro GPRS přenos.

**Rádiová komunikace**

Patří bezesporu k nejbezpečnějším formám komunikace mezi zařízeními, ovšem klade na provozovatele, ale i zákazníka nejnáročnější finanční požadavky. Systém přenosu je založen na vysílači zpráv, retranslačních stanicích a přijímače v PPC. Celý systém využívá vyhrazeného frekvenčního rozsahu přiřazeného provozovateli Českým telekomunikačním úřadem. Vzhledem k pořizovacím i provozním nákladům je dnes tato přenosová trasa vytlačována internetovou komunikací.

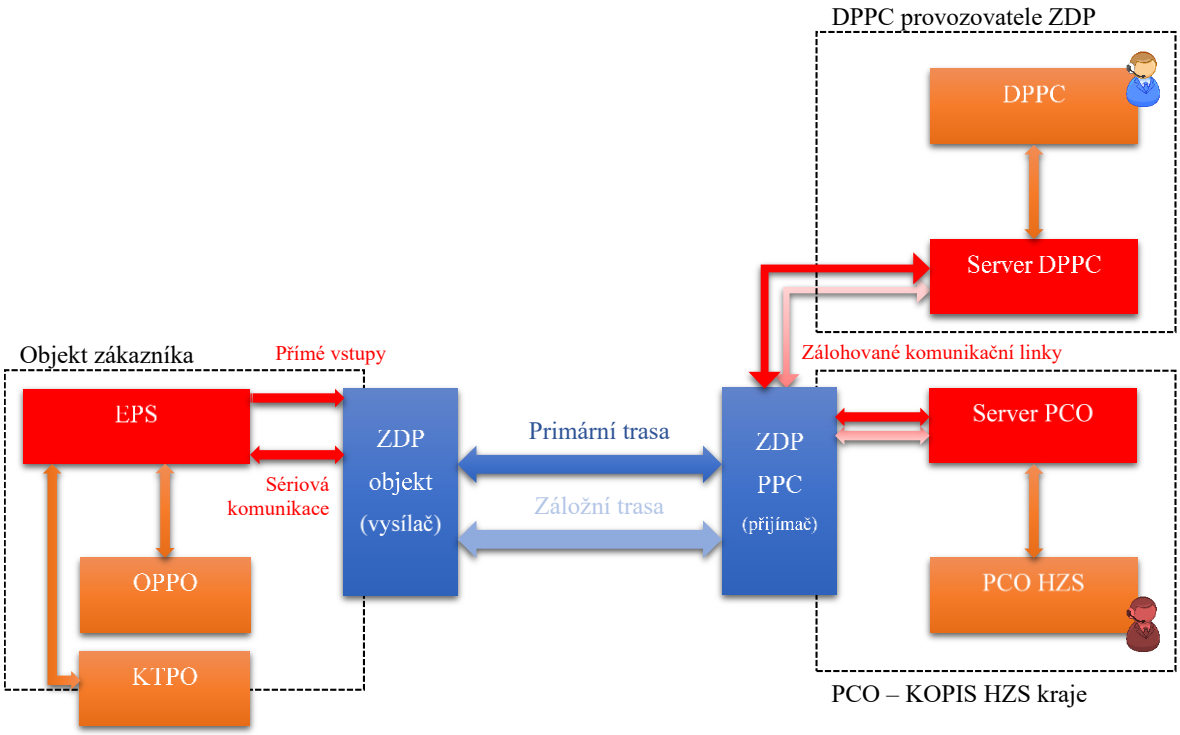
## 3.2 Zařízení dálkového přenosu

Samostatnou přenosovou soustavou jsou zařízení dálkového přenosu (ZDP). Jak bylo výše zmíněno, v případech, kdy je na objektu předepsaná nutnost instalace a provoz EPS a není zajištěna trvalá obsluha, musí být systém EPS trvale připojen na PCO HZS pomocí ZDP. Přenosové trasy ZDP zajišťují soukromé subjekty (bezpečnostní agentury) v rámci spolupráce s krajským sborem HZS ČR. Povinností provozovatele přenosové trasy je také současně provozovat obsluhované dohledové pracoviště, kde operátoři vyhodnocují veškerý provoz systémů EPS, ZDP a přijímací části PCO HZS a v případě poruch nebo poplachů (verifikovaných falešných a planých) musí náležitě reagovat.

ZDP využívají ke své komunikaci mezi vysílačem a přijímačem tyto druhy přenosových tras:

- radiová komunikace,
- GPRS,
- Internet
- nebo SMS.

Podmínkou pro připojení EPS k PCO HZS je použití certifikovaného ZDP typově schváleno generálním ředitelství HZS ČR a umožňuje přenos minimálně dvěma nezávislými poplachovými přenosovými cestami [14].




Obr. 17: Zjednodušené komunikační schéma ZPD [vlastní zdroj]

Komunikace mezi EPS a ZDP probíhá po sériových linkách, kde jsou přenášeny veškeré provozní stavy a upřesňující informace:

- RS 232, 485,
- nebo TTY.

Výstupy z EPS jsou přímo propojeny na smyčky ZDP a samočinně se musí přenést informace z EPS na PCO HZS:

*a) signál „VŠEOBECNÝ POPLACH“ (viz čl. 3.19 ČSN 34 2710),*
*b) signál porucha (bez rozlišení druhu poruchy) a*
*c) informaci o adrese vysílacího místa* [14].

# 4 SHRNUTÍ TEORETICKÉ ČÁSTI

V předchozích kapitolách věnovaných stručnému přiblížení principu a normativních požadavků na DPPC, vybraných technických zařízení v podobě PZTS, EPS, VSS a na závěr komunikačních tras, včetně zařízení dálkového přenosu se především operátoři dohledových center (ale i ostatní čtenáři) mohli seznámit s příklady bezpečnostních opatření souvisejících s nabízenými službami DPPC.

Předchozí kapitoly nenabízí kompletní ani konečný přehled všech technologií připojitelných na dohledová centra, ale ve své podstatě z výše uvedeného je zřejmý princip ostatních bezpečnostních i jiných než bezpečnostních zařízení.

Operátorům, supervisorům, ale především administrátorům je doporučeno neustále sledovat vývoj technologií a účastnit se i technických školení v oblasti bezpečnostních zařízení. Technický pokrok jde stále kupředu a jsou vyvíjena další a další zařízení, která nám v budoucnu umožní ještě lépe chránit svůj, ale i zákazníkův život, zdraví a majetek.

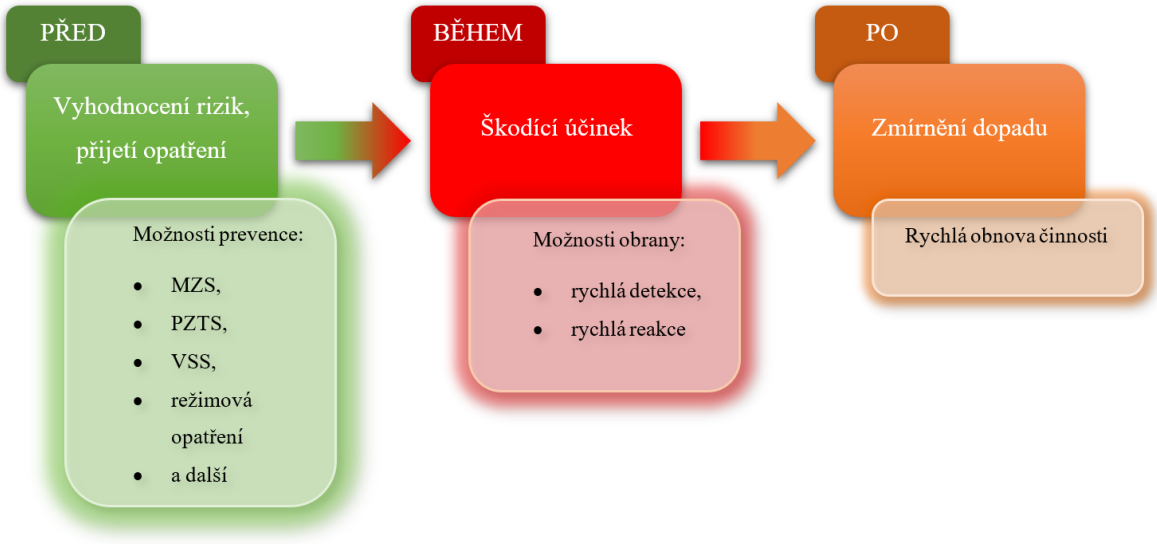
Každý zákazník, každý uživatel musí být náročný a požadovat po firmách zabezpečujících technické služby to nejmodernější, a pro své účely určené, zařízení. Každé elektrické zařízení vyžaduje odbornou montáž, servis a kontroly. Jen řádně udržované a obsluhované zařízení plní funkční požadavky, tak jak se od něj předpokládá, tak jak bylo projektováno.

# II. PRAKTICKÁ ČÁST

# 5 BEZPEČNOSTNÍ OPATŘENÍ

Pocit bezpečí je pro každého člověka velice cenný. Pocit bezpečí ovlivňuje náš každodenní život. Bezpečnostní opatření lze chápat jako činnost, která vede ke zmírnění dopadu případného škodícího účinku na referenčním objektu[11] na minimální přijatelnou úroveň [5].

Každý pracovník v soukromých bezpečnostních službách má svou určitou pozici a důležitost při zavádění bezpečnostních opatření. Systém může fungovat pouze jako celek a jeho nejslabší článek bude určovat výsledný efekt přijatých bezpečnostních opatření. Uvědomění všech zúčastněných stran (od zákazníka až po člena zásahové jednotky, v případech poskytování soukromých bezpečnostních služeb) může vést k minimalizaci případných škod při naplnění hrozby.




Obr. 18: Příklad možností opatření a možný průběh incidentu [vlastní zdroj]

[11] Definice dle [5]:

- ***Referenční objekt*** *představuje celek (entitu) usilující o zajištění bezpečnosti (o zamezení vzniku újmy nebo negativního dopadu) – stát, firma, úřad, osoba.*
- ***Hrozba*** *představuje skutečnost (jev, událost se škodícím účinkem), která se svým působením projevuje na určitém celku negativně. Může mu v případě expozice způsobit újmu nebo na něj mít negativní dopad – krádež, nehoda, útok viru.*
- ***Aktivum*** *představuje celek (skutečnost, entitu), který referenční objekt považuje z určitého důvodu za existenciálně důležitý – život, zdraví, území, čest.*
- ***Riziko*** *je veličina, charakterizující očekávané negativní dopady, vyjádřená součinem pravděpodobnosti vzniku újmy a její předpokládané velikostí.*
- ***Újma*** *představuje vnímatelný negativní/nežádoucí projev na aktivech či zájmech referenčního objektu (který lze vyjádřit kvantitativně).*
- ***Negativní dopad*** *představuje vnímatelný negativní projev na aktivech či zájmech referenčního objektu, jehož velikost nelze spolehlivě vyčíslit.*

# 6 NÁVRH PROVOZNÍHO ŘEŠENÍ DPPC

## 6.1 Vymezení účastníků při provozu DPPC

Termíny a definice vycházejí z normativních požadavků a zažitých zvyklostí. Účelem je konkretizovat, ujasnit si užité termíny pro účely přehlednosti použitých terminologií v tomto dokumentu.

### 6.1.1 Pracovníci DPPC

Všichni pracovníci (zaměstnanci) podílející se na provozu DPPC musí podstoupit bezpečnostní prověření a lustraci[12], ale také musí projít výcvikem pro činnost bezpečnostní pracovník/strážný pro získání minimální kvalifikace pracovníka dohledového centra. Národní soustava kvalifikací (NSK) uvádí tento kvalifikační standard pod kódem 68-003-H [15], včetně podmínek pro získání kvalifikace. Všem pracovníkům DPPC je zakázáno podávat jakékoliv informace jiným než kontaktním osobám zákazníka.

**Operátor** – osoba, která je odpovědná za správné vyhodnocení a reakci na příchozí události předané do PPC. Na operátory jsou taky kladeny požadavky v rámci SOP, řízení přístupu do dohledového centra, ale také dohled nad technologiemi podílejícími se na celkovém chodu DPPC. Normou [2] je vyžadována v DPPC přítomnost minimálně dvou operátorů, kteří jsou schopni provádět veškeré provozní postupy.

**Supervisor –** je osoba odpovědná za správné funkční technické prostředí systému PPC jako celku. Supervisorovi také náleží povinnost vést a spravovat veškerou agendu související s připojenými objekty na PPC (zákaznické účty nebo objektové karty), kontrolovat a hodnotit evidenci řešených událostí a deník závad. Na začátku každého měsíce provede report o činnosti DPPC a výsledky předá administrátorovi. Od supervisora se očekává větší technická znalost v oblasti bezpečnostních systémů a informačních technologií. Pozice supervisora vyžaduje 24hodinovou pohotovostní připravenost.

**Administrátor –** je osobou odpovědnou za veškerý provoz DPPC, dbá a kontroluje dodržování stanovených SOP nebo dodržování pravidel BOZP a PO. Vede a vyhodnocuje na základě výsledků z evidence řešených událostí a deníku závad klíčový ukazatel

[12] Bezpečnostní prověření a lustraci definuje ČSN EN 15602.

výkonnosti DPPC. Neustále kontroluje a reviduje nastavené SOP a reaguje na možné změny související s rozvojem technologií, nebo zákonné a tržní požadavky. Na základě reportu o činnosti provede měsíčně její vyhodnocení a předá na mzdové a účetní oddělení podklady pro mzdy a fakturace. Administrátor je členem managementu agentury provozující DPPC, který se mimo jiné věnuje správě rizik a výjimečných situací, správě informací (např. bezpečnost IT, GDPR), správě výkonnosti, vyřizování stížností, správě portfolia služeb a správě personálu, zákazníků, obchodních partnerů, tak jak vyžaduje [2].

### 6.1.2 Zákazník

Je fyzická nebo právnická osoba, která má s DPPC uzavřenou smlouvu o připojení a monitorování svého bezpečnostního nebo jiného než bezpečnostního systému.

**Uživatel –** je osoba, která má přístup do chráněného prostoru zákazníka a může ovládat monitorované zařízení.

**Kontaktní osoba –** je osobou zmocněnou zákazníkem, která má právo komunikovat (např. odvolávat plané oplachy) s operátorem dohledového centra. Pro zvýšení bezpečnosti je nutné, aby kontaktní osoby bylo možné ověřit pro komunikaci, např. ověřením telefonního čísla, nebo sjednaným heslem. Pořadí kontaktních osob určuje zákazník v akčním plánu.

### 6.1.3 Výjezdová skupina

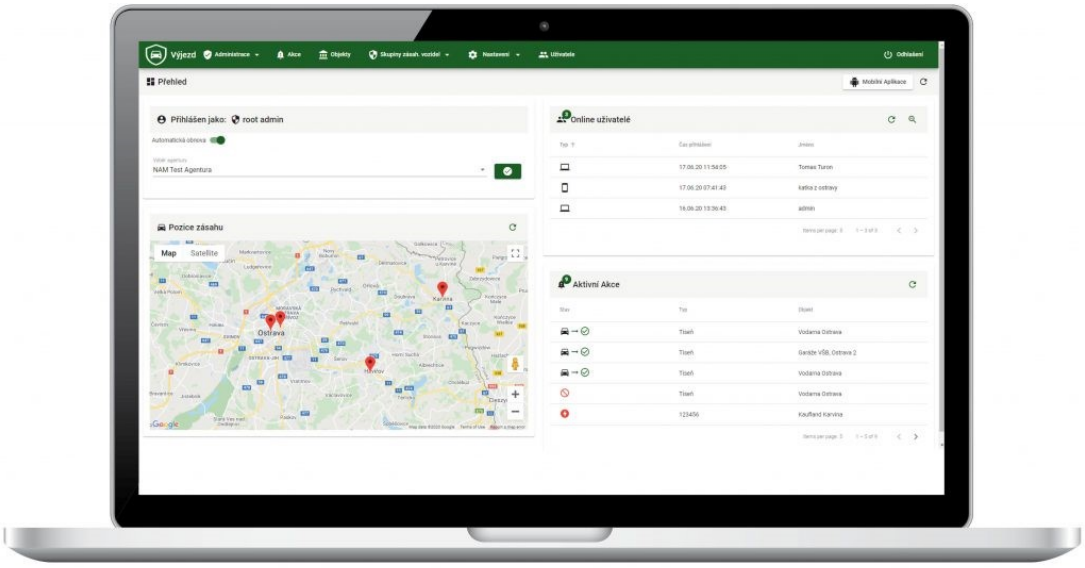
Je tvořena zaměstnanci bezpečnostní agentury poskytující zásahové služby. Každá výjezdová skupina (VS) má určené stanoviště, odkud provádí vyžádaný zásah operátorem. Dojezdové časy zásahu musí být stanoveny i s ohledem na stanoviště, vzdálenost, silniční provoz nebo další ovlivňující vlivy (např. dopravní uzly, počasí apod.). Výjezdová skupina má od DPPC k dispozici objektovou specifikaci, kde jsou uvedeny základní údaje o střeženém objektu. Objektová specifikace obsahuje především:

- jedinečné komunikační číslo objektu,
- název a stručný popis objektu,
- adresu, včetně GPS souřadnic,
- popis příjezdové trasy (v obtížných podmínkách včetně fotografií),
- upozornění na rizikové oblasti,
- povinné kontrolní body

- a další doplňující nebo upřesňující informace.

**Komunikace**

Operátor po vyhodnocení příchozích událostí má možnost (dle SOP a akčního plánu objektu) vyslat k zásahu nebo kontrole výjezdovou skupinu pomocí telefonního hovoru, radiostanice (pokud je VS v dosahu radiostanice) nebo datové komunikace (aplikace vyvíjené k tomuto účelu a pokud jí využívají obě strany). Struktura oznámení výjezdové skupině probíhá v definované formě dle objektové specifikace.




Obr. 19: Náhled aplikace pro organizaci výjezdových skupin [16]

### 6.1.4 Integrovaný záchranný systém

*Integrovaný záchranný systém (IZS) je **efektivní systém vazeb, pravidel spolupráce a koordinace** záchranných a bezpečnostních **složek**, **orgánů** státní správy a samosprávy, fyzických a právnických **osob** při společném provádění záchranných a likvidačních prací a přípravě na mimořádné události.*

***Základní složky IZS:***

- *Hasičský záchranný sbor České republiky,*
- *Jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany,*
- *poskytovatelé zdravotnické záchranné služby,*
- *Policie České republiky* [17].

V situacích, kdy se člověk ocitne v nouzi a potřebuje pomoc hasičů, záchranářů nebo policistů (nejsou dotčeny ostatní složky IZS), má vždy možnost využít tísňových linek jednotlivých subjektů integrovaného záchranného systému. Stejnou možnost má i kdokoliv jiný, kdo není přímo v ohrožení, ale stal se svědkem mimořádné události. Může se jednat např. o nahlášení požáru, žádost o zdravotnickou pomoc pro někoho dalšího nebo oznámení trestné činnosti. Ve všech případech komunikace se složkami IZS platí zásady zachování klidu, slušného vystupování a věcného odpovídání na případné dotazy operátora tísňové linky.

Volající by měl vždy dodržet základní komunikační model (příklady v závorkách):

- **jméno, příjmení** a případně pracoviště volajícího (Dobrý den, tady je Adam Novák, výjezdová skupina Vaše bezpečí Naše Město),
- **popis události** (chtěl bych oznámit narušení objektu vypáčenými vstupními dveřmi),
- co nejpřesnější **místo události** (jedná se rodinný dům ve městě Vaše Město v ulici Uliční 158),
- **zda událost probíhá, nebo proběhla** (je pravděpodobné, že pachatel je stále uvnitř domu),
- zda jsou **zranění** a případně **kolik** (nevidím žádné zraněné),
- upozornění na **potencionální nebezpečí** (ulice z Náměstí je neprůjezdná),
- odpovědět na **další otázky operátora,**
- **dodržet postup** dle instrukcí operátora,
- a v případech, kdy **se situace změní,** je nutné znovu zavolat na tísňovou linku a **předat nové skutečnosti** [18].

Tísňové linky se směrují na nejbližší operační středisko místa, odkud ohlašovatel volá. Proto, v případech nutnosti použití tísňové linky pracovníkem bezpečnostních služeb, je doporučeno, aby událost oznámil člen výjezdové skupiny přímo z místa.

Bezdůvodné použití volání na tísňovou linku je zakázáno a zneužití tísňové linky je trestné:

- **112 - jednotné číslo tísňového volání –** obsluhuje operační informační středisko HZS ČR (OPIS) v příslušném kraji (KOPIS), stejně jako
- **150 –** tísňovou linku **Hasičského záchranného sboru ČR,**
- **155** – je tísňová linka **Zdravotnické záchranné služby,**
- **158 –** je tísňová linka **Policie ČR,**
- **156 –** je jednotná linka **Městské (Obecní) policie.**

### 6.1.5 Servisní organizace

Jsou firmy poskytující technické služby v oblasti bezpečnostních i jiných než bezpečnostních systémů. Je dobrým zvykem, že zákazník při stanovování akčního plánu předá kontaktní údaje na servisní organizace svých připojovaných zařízení. Operátor má pak možnost konzultace, nebo nahlášení poruchy, přímo u technické podpory daného systému.

### 6.1.6 Dodavatelé zařízení PPC

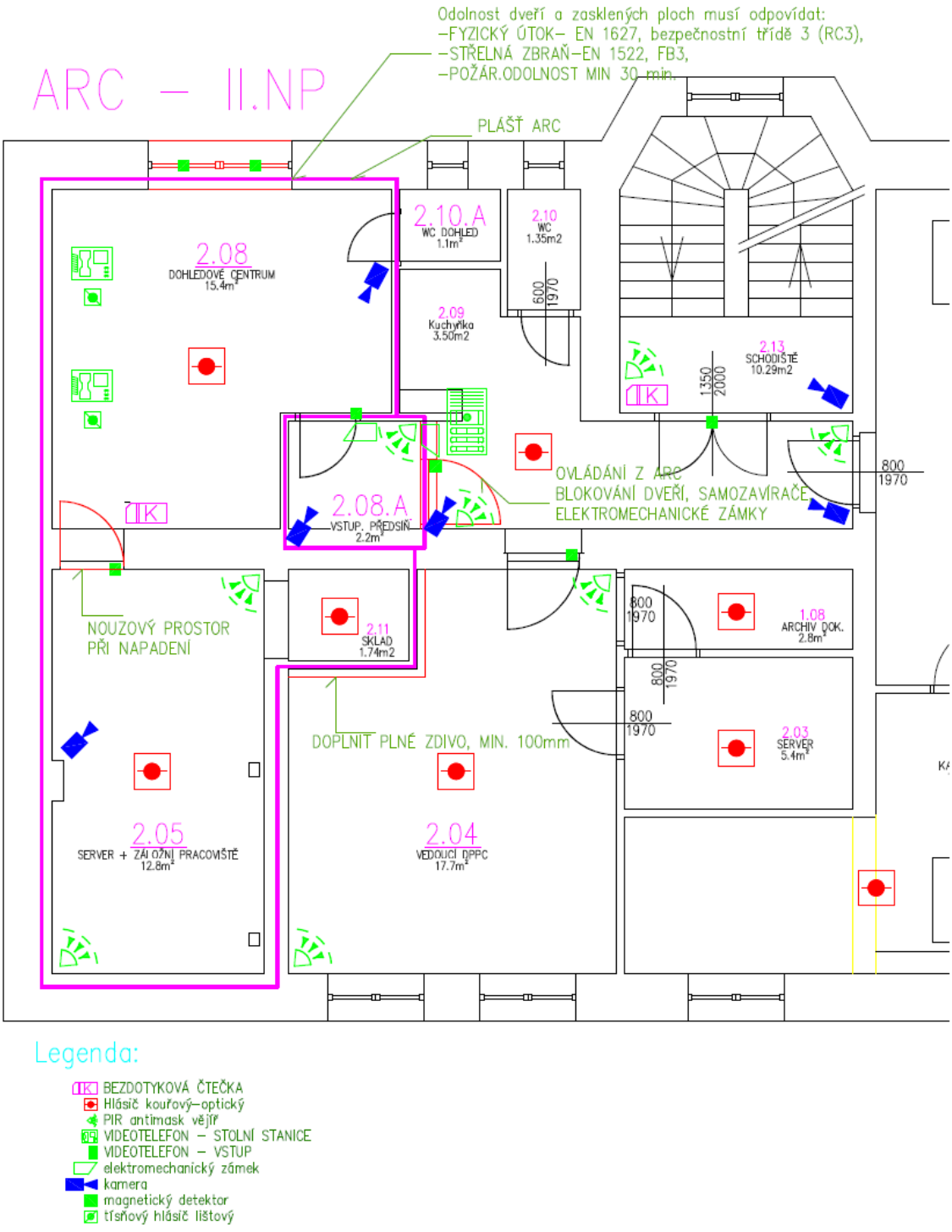
Společnosti na vývoj, výrobu, distribuci a servis komponent pro dohledová centra jsou velice specializovaní odborníci v tomto oboru. Na zaměstnance těchto společností je kladen nelehký úkol, aby veškeré dodávané komponenty, bezchybně a bezpečně spolu komunikovaly. V dnešní době je požadavek ještě zvýšen o implementaci protokolů pro komunikaci třetích stran. Serverové části PPC musí mít strukturu databází značně propracovanou, aby nedocházelo k dlouhým odezvám při provozu DPPC a operátorské prostředí musí být srozumitelné a uživatelsky příjemné. Na veškeré komponenty systémů PPC je kladen požadavek certifikací a schválení příslušnými orgány a zkušebními laboratořemi.

Společnosti provozující DPPC by měly mít (dle doporučení [2] musí mít) podepsanou servisní smlouvu pro nepřetržitou podporu a případný rychlý servis. Některé dodavatelské společnosti v ČR mají i ve své nabídce vzdálený 24hodinový dohled nad zařízeními svých zákazníků a jsou schopny odhalit vznikající problém dříve než operátor na dohledovém centru.

Tab. 13: Příklady dodavatelů technologií pro PPC

| Společnost | Software a připojitelné systémy | Kontakt |
|---|---|---|
| RADOM, s.r.o.<br>Pardubice | WRS32, Radomnet II<br>PZTS, EPS, VSS, SAS, SIE a další. | +420 466 414 211<br>www.radom.eu |
| NAM system, a.s.<br>Havířov | NET-G<br>PZTS, EPS, VSS, SAS, SIE a další. | +420 603 493 885<br>www.nam.cz |
| JABLONET s.r.o.<br>Jablonec n. Nisou | (CLOUD PCO) JABLONET PRO<br>PZTS, VSS, SAS a další. | +420 725 190 629<br>www.jablonetpro.com/ |

## 6.2 Prostory DPPC




Obr. 20: Návrh stavebního řešení DPPC v II.NP, včetně rozmístění bezpečnostních prvků [vlastní zdroj]

Pro potřeby střežení PZTS (ostatní systémy jsou pak zahrnuty) musí být dohledové centrum zamýšleno do kategorie I. ČSN EN 50 518 přesně definuje požadavky na konstrukci pro jednotlivé části DPPC. Na Obr. 20 je návrh možného řešení umístění a úprav konstrukční

části DPPC, včetně bezpečnostních prvků PZTS, VSS, EKV a EPS. Každý z pracovníků musí být seznámen s jednotlivými prostory a umístění komponent systému PPC, zároveň si každý musí být vědom a nést odpovědnost za plnění svěřených úkolů na dané pracovní pozici.

## 6.3 Poplachové systémy DPPC

Každé pracoviště DPPC dle požadavku [2] musí být vybaveno elektronickými detekčními a dohledovými zařízeními provozovanými dle příslušných norem, předpisů výrobce a postupů provozovatele. Poplachové stavy musí být signalizovány přímo na dohledovém pracovišti a zároveň musí být přenášeny na jiné DPPC. Systémy slouží k včasné detekci možného nebezpečí a pouze řádně obsluhované zařízení může plnit svou funkci.

V případě podezření na možné narušení bezpečnosti musí každý pracovník upozornit operátora na dohledovém centru (např. vyvoláním poplachu tísně, použití požárního tlačítka) na vznikající riziko a učinit veškeré možné kroky v zabránění možného narušení bezpečnosti a chodu DPPC.

Povinností operátorů je neustále sledovat a vyhodnocovat bezpečnostní systémy instalované v budově DPPC a v případě pouhého podezření na možné nebezpečí upozornit kompetentní osoby (např. vrátného, výjezdovou skupinu, administrátora apod.) na nutnost kontroly a případného opatření.

Ve chvíli, kdy operátor vyhodnotí narušení bezpečnosti v prostorách, kde je provozováno DPPC, okamžitě koordinuje veškeré možné kroky k odvrácení nebezpečí (např. oznámení situace na jiné DPPC, tísňové volání na HZS, PČR, Městskou policii apod.). V dalších krocích je potřeba postupovat dle vývoje situace a nouzového plánu.

**PZTS**

Je instalován ve všech částech budovy a operátor je upozorněn na narušení bezpečnosti poplachem. Část budovy, kde je umístěno dohledové centrum, zařízení PPC a náhradní generátor (veškeré části související s provozem DPPC), v případě detekce narušení jsou poplachové stavy přenášeny také na jiné DPPC.

Povinností každého pracovníka DPPC je zodpovědný přístup k ovládání poplachových systémů, dodržovat předepsaný postup přístupu do jednotlivých prostor a v případě zjištění jakéhokoliv nedostatku sjednat okamžitou nápravu.

### Dohledový videosystém

Dohledový videosystém (VSS) je instalován na každém možném vstupu do budovy a celá příchodová trasa ke vstupní předsíni dohledového centra, je také pod kamerovým systémem.

Pro přesnou identifikaci osob, které mají oprávnění vstoupit do prostor dohledového centra, technologického úseku zařízení PPC (serveru) nebo náhradního generátoru, slouží jednotlivé kamery umístěné přímo na pláštích příslušného úseku.

Operátor je povinen sledovat a vyhodnocovat obraz celého videosystému, pro který má vyhrazen prostor ve videostěně a v žádném případě ho nesmí ničím jiným nahradit.

### Elektrická kontrola vstupu

Terminály elektrické kontroly vstupu (dále jen „EKV“) jsou osazeny u každých dveří v budově (kromě sociálního zázemí). Práva na přístup do jednotlivých prostor přiděluje administrátor DPPC jednotlivým pracovníkům dle pracovních pozic. Jsou hlídány stavy dlouho otevřených dveří po celé přístupové trase k dohledovému centru a upozornění dostávají operátoři zvukovým i optickým signálem.


Obr. 21: DS-K1T671 – Pro Face Access Terminal [19]

U dveří vstupní předsíně jsou instalovány prvky pro identifikaci vstupující osoby a vstup i výstup musí být autorizován osobou zevnitř dohledového centra (vyjma případů nouzového otevření). Dveře jsou blokovány tak, aby nebylo možné, během standardního vstupu nebo výstupu, otevřít oboje současně. Autorizovaný vstup osobou uvnitř DPPC je také požadován do prostor, kde jsou umístěny komponenty PPC nebo náhradní generátor.

**Elektrická požární signalizace**

V celém objektu je instalován a provozován systém elektrické požární signalizace (dále jen „EPS“). Ústředna, respektive ovládací tablo EPS, je instalováno v prostorách dohledového centra, kde jsou dle požadavku [2] přítomni minimálně dva pracovníci, kteří tvoří obsluhu EPS.

Postup vyhodnocování událostí ze systému EPS odpovídá postupu pro vyhodnocování bezpečnostních systémů instalovaných v DPPC. Operátoři jsou seznámeni a prokazatelně proškoleni na obsluhu EPS dle požadavku ČSN 34 2710.

## 6.4 Přístup do prostor DPPC

Do prostor dohledového centra, technologického úseku PPC (serverovny) a prostor náhradního generátoru je povolen vstup pouze oprávněným osobám.

Zástupcům dodavatelských společností (např. při servisní činnosti), stejně jako případným návštěvníkům, může být umožněn vstup do prostorů DPPC pouze v případě, že jsou doprovázeny jinou oprávněnou osobou a mají protokolovaný souhlas supervisora nebo administrátora.

Za oprávněné osoby se považují:

- operátoři,
- supervisoři
- a administrátor.

## 6.5 Nouzové postupy

Nelze vyloučit situaci, kdy bude potřeba evakuovat veškeré prostory budovy, kde se DPPC nachází (např. požár, hrozba výbuchu apod.). V této situaci nemůžou být operátoři výjimkou a budou muset přerušit veškerou svou činnost. Pro tyto případy je nutné okamžitě vyrozumět partnerské DPPC, případně dodavatele PPC, aby okamžitě převzali pomocí vzdáleného dohledu kontrolu nad připojenými objekty. Povinností operátorů v této situaci je neprodleně kontaktovat administrátora nebo supervisora pro zajištění výše zmíněné činnosti.

Pro případy totálního vyřazení DPPC z provozu je administrátorem a supervisorem zpracován krizový SOP. Operátoři musí okamžitě, pokud možno v první fázi zjištění problému, předat informace administrátorovi nebo supervisorovi (např. využitím tísňových prostředků

připojených na partnerské DPPC). Následuje svolání a jednání krizového managementu společnosti, které určí další postup. O obnově provozu a návratu do standardního stavu rozhodne krizový management společnosti.

## 6.6 Zařízení PPC

Veškeré technologie, které jsou součástí příjmu a zpracování dat jsou umístěny v serverovně, která je součástí (v plášti) dohledového centra.

Operátoři (následně supervisor, administrátor nebo dodavatel systému) DPPC nesou odpovědnost za veškerá zařízení umístěná v prostoru dohledového centra na úrovni:

- zabezpečení přístupu pouze oprávněných osob,
- bezporuchový stav všech komponent systému,
- dodávky elektrické energie,
- dodržování pravidel BOZP a PO,
- a ostatní faktory zajišťující provoz zařízení PPC.

V případě vzniku jakékoliv poruchy nebo nestandardní události na jakékoliv části zařízení PPC jsou operátoři povinni učinit veškerá nápravná opatření, nebo v případě, že nejsou schopni vlastními silami nebo prostředky zabezpečit nápravu sami, předají okamžitě odpovědnost (podají zprávu) prokazatelným způsobem dalším odpovědným osobám, kteří mají povinnost zabezpečit nápravu, nebo postoupit další odpovědné osobě.

Obr. 22: PCO 1Box® [20]

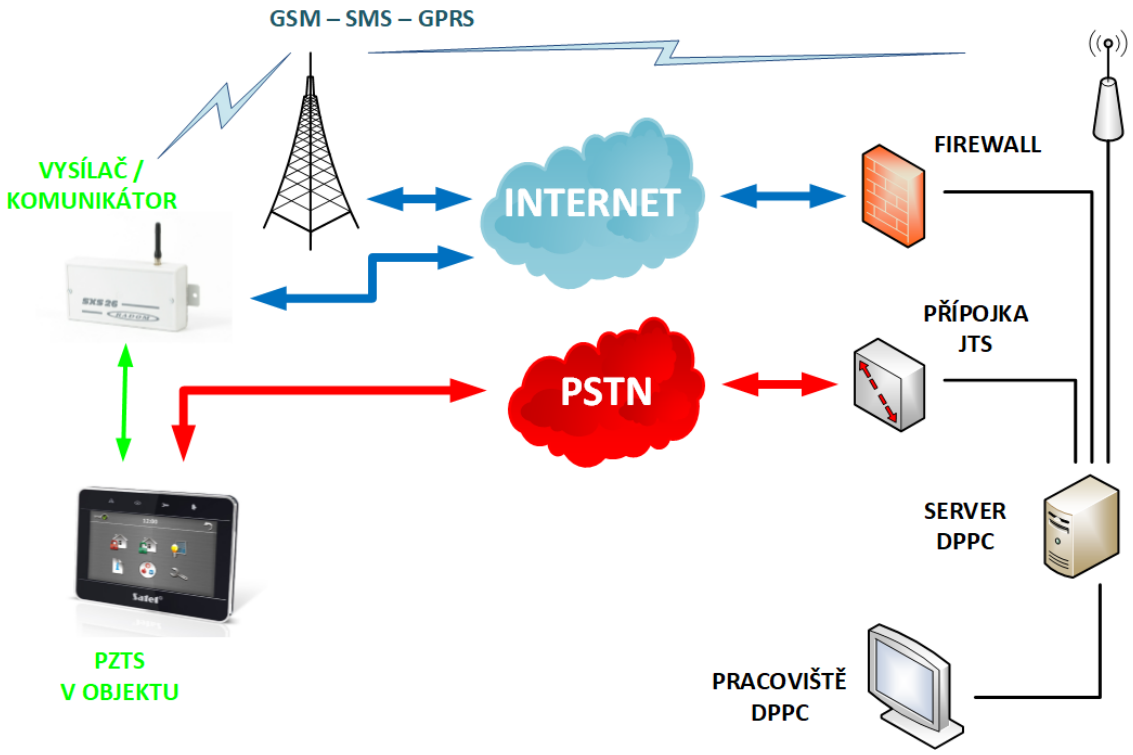
Tab. 14: Typy zařízení PPC umístěná v DPPC dle [2]

| Zařízení | Stručný popis | Příklady poruch |
|---|---|---|
| RCT | Komunikátor přijímacího centra – přijímače jednotlivých výrobců zařízení – např. ZPD přijímač. | Napájení, akumulátory, prach atd. |
| $I_{RCT}$ | Prostředky (HW i SW), které zprostředkovávají komunikaci mezi RCT a AMS – např. převodníky, konektory, rozhraní. | Napájení, chyba běhu programu (restart), chyba sítě. |
| AMS | Servery systému správy poplachu (databáze, uložiště) – servery umístěné v RACKu. | Napájení, při jiné poruše předat další os. |
| Telefonní ústředna | Komunikační zařízení, včetně záznamu hovorů a datového uložiště. | Napájení, chyba běhu programu (restart). |
| LAN/WAN | Vnitřní ukončení přístupového bodu poskytovatele internetových služeb. | Nedostupnost internetu. |
| Síťové prvky | Aktivní (routery, switche), ale i pasivní prvky počítačové sítě. | Napájení, chyba běhu programu (restart). |
| UPS | Záložní bateriový zdroj napájení při výpadku síťového napájení. Provoz min. 10, max. 30 minut. Automatické přepínání, signalizace na DPPC. | Napájení, stav akumulátorů. |
| | | |
| Generátor umístěn vně DPPC | Pohotovostní generátor při výpadku síťového napájení trvající více než 5 minut. Automatický start, signalizace na DPPC. | Gen. nenaskočí do 5 minut okamžitě předat další os. |

## 6.7 Komunikační trasy

Komunikační prostředky, jednotlivé komunikační trasy a formáty přenosu zpráv popsal autor v bakalářské práci [3] *Řešení přenosových tras a protokolů dohledového a poplachového přijímacího centra* v roce 2018. Obsahem práce bylo také přiblížení překladu příchozích zpráv pomocí překladových tabulek, které v nastavení každého PPC tvoří nezbytnou část pro správnou funkci. Každý výrobce, každá agentura má možnost volby k přístupu a překladu dle vlastního uvážení, respektive nastavení přenosových firemních standardů.

Jelikož objektová zařízení komunikují přes různé hlavní, případně i záložní trasy, je nezbytnou součástí znalostí operátorů mít přehled (supervisorů a administrátorů podrobně) o všech možnostech komunikace, pravidel přenosu, poruch tras a reakcí na vzniklou situaci.




Obr. 23: Zjednodušené schéma komunikačních tras [3]

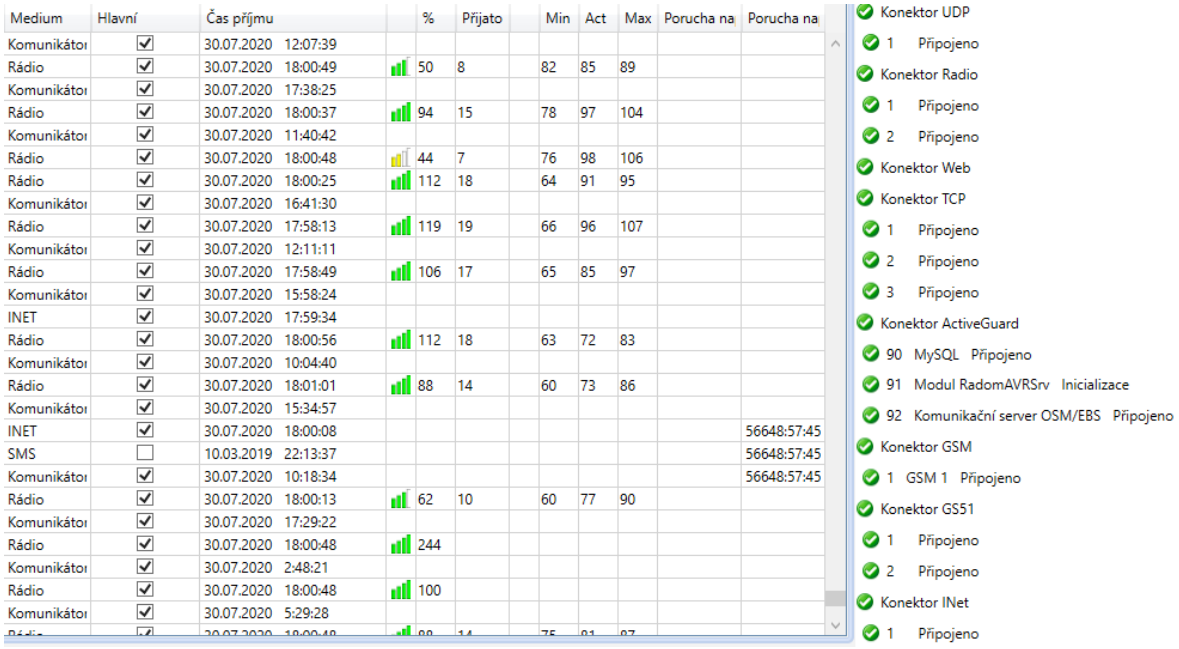
### 6.7.1 Internet

Poskytovatelé internetu připojují do svých sítí provozovatele DPPC pomocí routerů a rozhraní WAN. Jedná se o zařízení, přes které prochází veškeré události z objektů zákazníků (připojených přes datové linky). Dalšími zařízeními, které jsou připojovány do vnitřních sítí (LAN) dohledových center, jsou tzv. switche, které řídí (přepínají) provoz jednotlivých připojených zařízení při komunikaci mezi sebou a internetem. Na grafických rozhraních jednotlivých PPC se zobrazují stavy jednotlivých komunikačních tras. Operátor má tak přehled, který přenosový kanál pracuje bezchybně, nebo který vykazuje poruchu.

Server každého PPC je přímo připojen přes strukturovaný kabelážní systém do switche.

O bezpečnost datové komunikace se starají specialisté IT oboru. Je na nich, aby zabezpečili bezproblémový chod a v případě problémů, co nejrychleji našli řešení nápravy. Internetová konektivita musí být zásadně redundantní, nelze spoléhat pouze na jeden přenosový kanál, aby byla zabezpečena obnovitelnost závad dle ČSN 50 518.

Operátoři, supervisoři, ale i administrátoři musí být obezřetní a jakákoliv anomálie od běžného provozu v internetové komunikaci musí být řádně prošetřena pracovníky IT oddělení. Může se bohužel jednat o kybernetický útok, kterými jsme svědky každý den.




Obr. 24: Výřez obrazovky přehledu komunikace sw Radomnet II [21]

Tab. 15: Příklady internetových kanálů a zařízení

| Komunikace | Zařízení PPC (RCT) | Připojitelná technologie |
|---|---|---|
| TCP | WAN, LAN, SurGuard, SMET -256 | PZTS, EPS, ACS, SIE |
| UDP | WAN, LAN | PZTS, EPS |
| Web | WAN, LAN | Aplikace uživatelů |
| I-NET | WAN, LAN | Komunikátory RADOM |
| ActiveQuard | WAN, LAN, GPRS | Obchůzkové systémy AQ |
| NSG | WAN, LAN, GPRS | PZTS, EPS, ACS, GPS |
| SIA, Videofield | WAN, LAN, GPRS | PZTS, VSS |

### 6.7.2 GSM – SMS

Příchozí i odchozí služby jsou uskutečňovány přes mobilní operátory. Je nutné komunikační zařízení na straně PPC a v něm aktivní SIM karta. Využívá se zároveň jako odchozí brána pro přeposílání SMS zákazníkům.

Komunikační zařízení GSM je připojeno do serveru pomocí sériového rozhraní RS232, nebo pomocí převodníku RS232/LAN do počítačové sítě a softwarový sériový port.

Tab. 16: Příklady komunikace a zařízení GSM – SMS

| Komunikace | Zařízení PPC (RCT) | Připojitelná technologie |
|---|---|---|
| GSM | SRX10G | PZTS s CID komunikací |
| SMS1 | 1Box NAM Technology | PZTS s CID komunikací |

### 6.7.3 Rádio komunikace

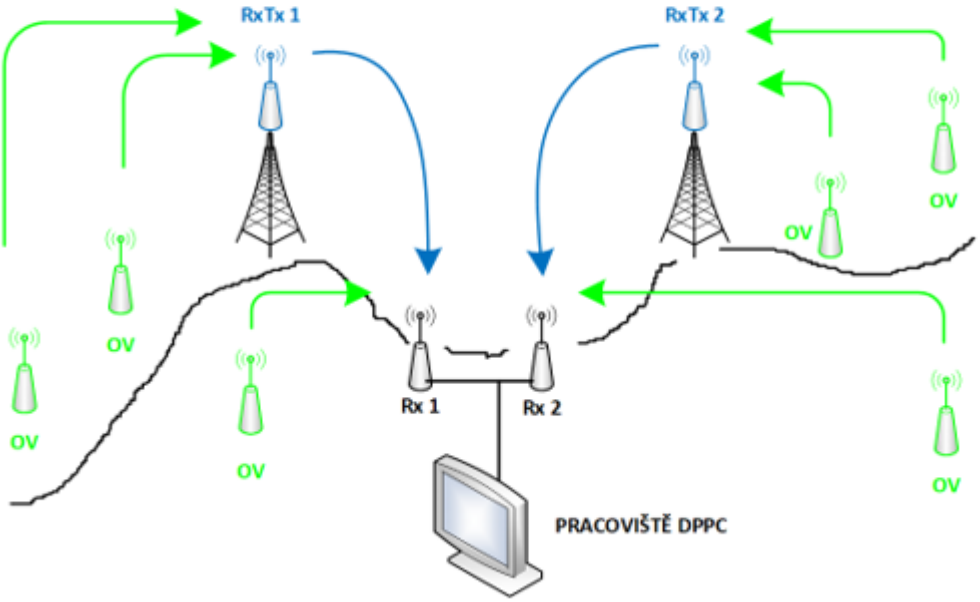
Vyžaduje instalaci vyhrazených zařízení pro rádiovou komunikaci jak na straně zákazníka, tak na straně PPC. Na přijímací straně je systém retranslačních stanic a přijímače. U zákazníka je osazen vysílač. Komunikace je znázorněná na Obr. 25. Přenos signálů je závislý na přenosovém frekvenčním pásmu, které může být ovlivněno vnějšími vlivy, jako je např. počasí, zástavba, stromy apod.

Přijímací zařízení jsou také vybavena výstupem pro sériovou komunikaci a do serveru se připojují pomocí RS232, nebo převodníků na LAN.

Tab. 17: Příklady rádio vysílačů a zařízení

| Komunikace | Zařízení PPC (RCT) | Připojitelná technologie |
|---|---|---|
| Radio | STX23/400 | PZTS, EPS |
| REGGAE RT | GLOBAL, Global2 | 1Box NAM technology |

- OV – objektový vysílač,
- RxTx – retranslační stanice,
- Rx – koncové přijímače PPC.




Obr. 25: Princip rádiové komunikace, [3] upravil Krejčí 2020

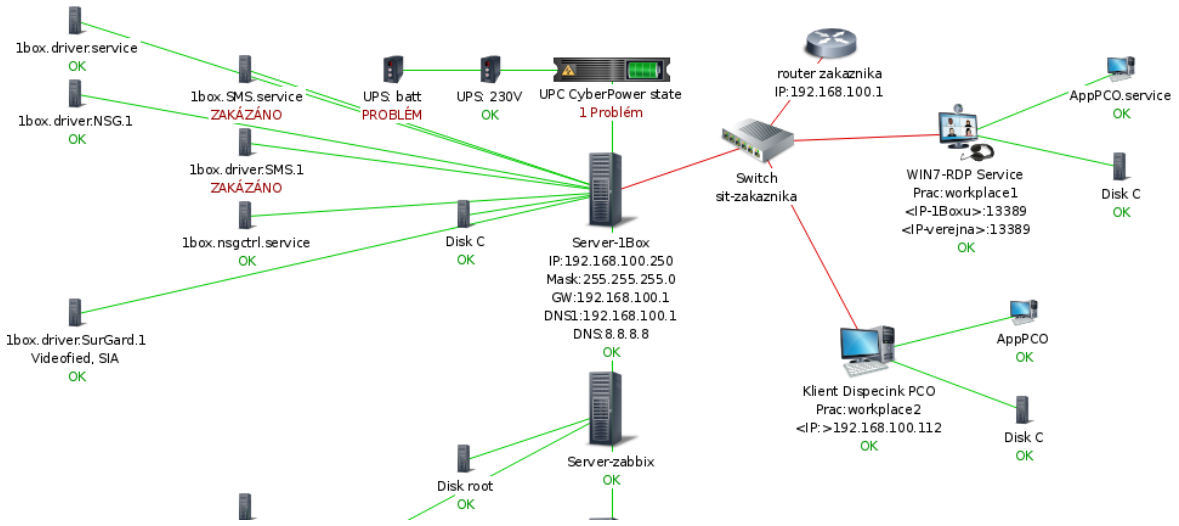
### 6.7.4 Telefonní komunikace

Zařízení, která komunikují prostřednictvím pevných telefonních linek, vytáčejí příchozí linky PPC, které jsou vyvedeny do převodníků telefonních linek (telefonní karty) na sério-vou komunikaci. Jednotlivé karty jsou osazeny vícevstupním modulem.

Komunikace se serverem je možná pomocí USB, nebo sériovým výstupem RS 232.

Tab. 18: Příklady telefonní komunikace a zařízení

| Komunikace | Zařízení PPC (RCT) | Připojitelná technologie |
|---|---|---|
| GS51 | telefonní karta GS51 + USB Box | PZTS |
| NSG | telefonní karta TF 98P | PZTS |




Obr. 26: Výřez obrazovky přehledu komunikace sw NET-G [22]

## 6.8 Monitorování a testování zařízení PPC

Každé el. zařízení podílející se na provozu DPPC musí být kontrolováno, testováno nebo monitorován jeho stav. Na každou z těchto činností musí být vystaven dokument (nebo digitální záznam) s výsledkem kontroly. Normou je přímo vyžadováno:

- **každodenní testování**, resp. monitorování všech zařízení, která zpracovávají veškeré komunikační cesty, až na monitory operátorů. V případě zjištění jakékoliv závady je **operátor** upozorněn **poruchovou zprávou**, kterou musí okamžitě vyhodnotit a přistoupit k nápravným krokům,
- **měsíční testování** je vyžadováno pro **všechna napájecí zařízení** a vlastní poplachové systémy. Povinností **supervisora** je 1x za měsíc testem vyzkoušet všechny bateriové náhradní zdroje a ručně spustit pohotovostní generátor. Zároveň je jeho povinností zkontrolovat, případně doplnit provozní kapaliny (palivo, olej nebo chladící směs) tak, aby byl zabezpečen kompletní chod DPPC v případě výpadku síťového napětí po dobu 24 hodin,


Obr. 27: Náhradní generátor [23]

- **roční testování** spočívá ve vypnutí hlavního napájecího zdroje od všech zařízení v rámci PPC. V té chvíli musí samočinně napájení dodávat náhradní bateriové zdroje do všech zařízení v rámci DPPC bez rozdílu, včetně nouzového osvětlení[13]. Do 5 minut od vyřazení síťového napájení musí být ověřen automatický start a chod náhradního generátoru. Generátor bude testován a kontrolován dle návodu výrobce, ale chod při plné zátěži minimálně po dobu 1 hodiny. Kontrola a doplnění provozních kapalin zůstává samozřejmostí ihned po skončení testování.

[13] Testování systémů PPC nenahrazuje zkoušky a kontroly provozuschopnost dle vyhl. 246/2001Sb. ani revize elektrických zařízení dle ČSN 33 1500, které mohou vykonávat pouze osoby k tomu odborně způsobilé.

# 7 STANDARDNÍ OPERAČNÍ POSTUPY OPERÁTORŮ

## 7.1 Vymezení činnosti a pojmů DPPC

**Akční plán –** je předem stanovený postup vyhodnocování a reakce operátorů, včetně stanovení výkonnostních kritérií – zpracování zpráv stanovené požadavkem 9.2 [2], dle dohody zákazníka a administrátora (managera) DPPC. Akční plán je povinnou přílohou každé smlouvy o poskytování služeb. Supervisor je odpovědný za zanesení požadavků akčního plánu do objektové karty v rámci PPC.

**Poplachový stav –** je stav systému, kdy jedna nebo více komponent, vyvolá odezvu na přítomnost nebezpečí.

**Zaznamenaný poplach** – je poplachový stav předaný pomocí komunikačních zařízení do PPC.

**Planý poplach** – je poplach vyvolaný podnětem na detektor (hlásič), který správně reaguje na vzniklou událost vyhlášením poplachového stavu, ale tento stav není způsoben narušením bezpečnosti monitorovaného objektu. Např. poplach je vyvolán špatnou obsluhou objektu, průvanem, zvířaty apod.

**Falešný poplach –** naopak není způsoben obsluhou nebo podobným podnětem, ale může se jednat o nespecifikovanou závadu na systému, kterou je nutné odstranit servisním zásahem.

**Ostrý poplach –** je poplachový stav, kdy došlo k detekci a signalizaci skutečným narušením bezpečnosti monitorovaného objektu.

**Všeobecný poplach –** je vyhrazeným pojmem pro zařízení elektrické požární signalizace, kdy dochází k vyhlášení požárního poplachu ústřednou EPS, spouští se sirény a ovládaná zařízení v objektu a jsou přenášeny poplachové informace na PCO HZS (výjezd JPO HZS).

**Verifikace poplachu** – je proces ověření poplachového stavu zařízení, kdy jsou vyhodnoceny doplňující informace příchozích událostí, a kdy je možné zvýšit pravděpodobnost vyhodnocení, zda došlo k ostrému poplachu.

**Rušivá událost** – je jakákoliv nežádoucí událost (přírodní nebo umělá), která může zapříčinit omezení, nebo přerušení standardních činností DPPC (např. požár, poruchy zařízení, kyberútok apod.).

**Kontrola objektu –** operátor vyšle výjezdovou skupinu ke kontrole objektu za účelem verifikace příchozích událostí. Výjezdové skupině je operátor povinen sdělit veškeré dostupné informace o příchozích událostech i v průběhu kontroly objektu (např. další příchozí poplachová událost). Po skončení kontroly je operátorovi sdělen výsledek, včetně podrobností a zaslána fotodokumentace pořízená výjezdovou skupinou.

**Bezpečnostní zásah** – je prováděn a vyžadován v případech, kdy operátor má verifikované příchozí události tak, že došlo k narušení bezpečnosti monitorovaného objektu. Přednostně operátor oznámí událost složkám integrovaného záchranného systému a sdělí veškeré zjištěné podrobnosti. Ve výjimečných případech může operátor požádat o zásah výjezdovou skupinu.

**Dostřežení napadeného objektu –** spočívá ve fyzické přítomnosti bezpečnostního pracovníka – strážného bezpečnostní agentury zajišťující výjezdové služby u napadeného objektu, do doby předání odpovědnému zástupci zákazníka. Operátor objednává dostřežení dle SOP a akčního plánu objektu u člena výjezdové skupiny, který oznámil zjištění narušení bezpečnosti.

**Předání napadeného objektu –** je stav, kdy se k napadenému objektu dostavila odpovědná osoba zákazníka, nebo jednotka integrovaného záchranného systému, s kterou společně s výjezdovou skupinou i operátorem si vzájemně potvrdí převzetí objektu a ukončení zásahu výjezdové skupiny.

**Patrolace –** je činnost výjezdových skupin, kdy se po dohodě s operátorem v definovaných časech provádí preventivní kontrola objektu (např. při ztrátě komunikace nebo poruše monitorovaného zařízení).

**Deník událostí –** je jakýkoliv záznam do databáze PPC na úrovni příchozích událostí, poruchových stavů, činnosti operátora nebo automatických akcí PPC, včetně data a časového razítka.

**Rozbor události –** je podrobný zápis operátora do deníku událostí přiřazený objektové kartě PPC, kde operátor slovně popíše veškerou činnost a zjištění při řešení příchozích událostí monitorovaného objektu.

**Evidence řešených událostí –** slouží k vyhodnocování řešených událostí DPPC administrátorovi a je podkladem pro ekonomickou činnost společnosti. Evidenci zapisuje operátor po každé ukončené události (v některých PPC označováno akcí).

**Deník závad –** slouží k evidenci a přezkoumání řešených závad komponentů PPC. Operátor je povinen zapsat veškeré zjištěné závady, včetně řešené opravy. Zároveň deník slouží k vyhodnocení měsíční dostupnosti všech zařízení podílejících se na příjmu událostí.

## 7.2 Možné typy nabízených služeb zákazníkům

Každý zákazník má jiné potřeby a každý připojený systém má svoje specifika. Je nutné rozlišit, jakou prioritu má příchozí událost v konkrétním případě a jakou službu zákazník využívá. Administrátoři, supervisoři a operátoři musí mít jasně stanovená pravidla pro připojování objektů a vyhodnocování přijatých událostí. Všichni zúčastnění si musí dobře uvědomit, jaký je rozdíl v připojení poplachových nebo jiných než poplachových systémů (vyjma připojení EPS).

Elektrické požární signalizace jsou zvláštní kapitolou ze souboru jiných systémů, které generují poplachové informace [2] a připojení na DPPC zprostředkovatele přenosové trasy a PCO HZS místě příslušného kraje se řídí předpisy a normami o požární ochraně[14]. Nutnost instalace a připojení na PCO HZS kraje pak stanovuje schválené požárně bezpečnostní řešení stavby (PBŘ).

### 7.2.1 Dohled

Dohled je nejnižší úroveň služby, kterou agentura provozující DPPC může nabídnout zákazníkům, ale uživatel získává alespoň minimální komfort při ochraně střeženého majetku. Zákaznické systémy (bezpečnostní i jiné než poplachové) jsou připojeny na DPPC s automatickým zpracováním události (např. poplachu, poruchy) a reakce probíhá dle nastaveného scénáře supervisorem v objektové specifikaci samočinně (např. odeslání SMS nebo emailu uživateli o poplachu v objektu). Dle [2] scénář koresponduje s akčním plánem dohodnutým se zákazníkem, který je nedílnou součástí smlouvy o připojení objektu.

Operátor vyhodnocuje a reaguje pouze na události typu ztráty spojení s objektem nebo neúspěšného automatického zpracování události. O těchto událostech je operátor informován prostřednictvím poruchových zpráv.

[14] Např. zákon č.133/1985 Sb. o požární ochraně, vyhláška 246/2001 Sb. o požární prevenci, vyhláška 23/2008 Sb. o technických podmínkách požární ochrany staveb nebo řada norem ČSN 73 xxx, které řeší požární bezpečnost staveb.

Zákazník nebo autorizovaný uživatel[15] má vždy možnost se telefonicky spojit s dohledovým centrem a konzultovat s operátorem další postup na vzniklou událost (např. jednorázové vyslání výjezdové skupiny ke kontrole objektu).

### 7.2.2 Střežení

Základní typ služby, kterou DPPC nabízejí svým zákazníkům pro zvýšení ochrany bezpečnosti jejich objektů pomocí prostředků připojitelných prostřednictvím komunikačních zařízení na PPC, sloužící k ochraně osob, zvířat, technologií, životního prostředí nebo majetku.

Operátor vyhodnocuje, reaguje na veškeré příchozí události dle SOP (přednostně odst. 7.3) a postupuje dle akčního plánu zadaného supervisorem v objektové specifikaci. Operátor zohledňuje zákaznickou prioritu příchozích událostí a je jeho povinností řešit přednostně události s nejvyšší důležitostí tak, jak si určil zákazník v akčním plánu (např. tíseň, požár, zaplavení, narušení střežených prostor atd.).

Jelikož se jedná o základní formu nabízených služeb a ve většině případů je výjezd ke kontrole objektu výjezdové skupiny zpoplatněn, jsou zákazníkům nabízeny dvě varianty tarifu střežení:

- **střežení A** – operátor vyhodnotí příchozí události a telefonicky kontaktuje osobu dle pořadí uvedeného v objektové specifikaci (kontaktní osoby), které sdělí výsledek vyhodnocení příchozích událostí a dále operátor postupuje dle dohody s kontaktní osobou (např. zásah výjezdové skupiny, kontaktování servisní organizace apod.). V případech, kdy se není možné z jakéhokoliv důvodu spojit s žádnou z kontaktních osob, operátor při vyhodnocení poplachové události okamžitě vyšle ke kontrole objektu výjezdovou skupinu a zákazníkovi odešle informaci o probíhající kontrole výjezdovou skupinou (SMS nebo email), pokud není v akčním plánu stanoveno jinak.
- **střežení B** – pro verifikaci poplachové události nebo přímo k bezpečnostnímu zásahu operátor může využít výjezdovou skupinu ke kontrole střeženého objektu bez předchozího odsouhlasení kontaktní osobou.

[15] Uživatel, který je zadán do objektové specifikace na základě písemné žádosti zákazníka, jako kontaktní osoba objektu.

### 7.2.3 Komfort

Služba je určená pro náročnější klientelu, která nemůže být vždy dostupná ke komunikaci s operátorem nebo chce mít vyšší komfort a nemít starost s řešením bezpečnostního opatření v podobě zásahu výjezdové skupiny (např. banky, zastavárny nebo rekreační objekty). Hlavní rozdíl oproti službě střežení spočívá v tom, že výjezdy na poplachové události jsou řešeny zcela automaticky a jsou již zahrnuty v ceně měsíčního paušálu za připojení objektu (zařízení).

Tento typ služby je možné nabízet pouze zákazníkům, kteří dbají o pravidelné kontroly, servis svých zařízení a uživatelé jejich systémů jsou zodpovědní k užívání. Plané nebo opakující se falešné poplachy (od 10 a více za měsíc) s následným výjezdem bývají obvykle zpoplatněny částkou za neoprávněný výjezd.

Technické, poruchové stavy zařízení nebo ztráty spojení komunikace jsou i v tomto případě řešeny s kontaktní osobou operátorem, pokud není v akčním plánu sjednáno jinak.

### 7.2.4 Exklusive

Úplně nejvyšší úroveň služeb nabízí tarif pro nejnáročnější zákazníky, kteří si přejí, aby se bezpečnostní agentura plně postarala o bezpečnost jimi svěřených hodnot. DPPC a veškerý personál má za úkol vyřešit veškeré bezpečnostní i provozní situace související s dohledávaným zařízením.

Operátoři vyhodnocují a reagují na všechny příchozí události obdobným způsobem jako na poplachové události u služby komfort, ale s tím rozdílem, že výjezdová skupina má umožněn vsup do střeženého objektu k verifikaci nebo zásahu na veškerá příchozí hlášení z DPPC. Operátor ve spolupráci s výjezdovou skupinou, případně supervisorem, zajistí vše potřebné k zajištění bezpečnosti střežených hodnot. Může se jednat např. o objednávku instalatérských služeb, opravu elektroinstalace nebo služeb sklenářů.

Ve většině případů agentura zajišťuje také běžnou kontrolní a servisní činnost na připojených zařízeních. Ceny a akční plán pro tento typ služby je zcela individuální záležitostí domluvy zákazníka a manažera, nebo administrátora DPPC.

**Společné pro služby zmíněných tarifů**

V případech, kdy dojde k potvrzení narušení bezpečnosti střeženého subjektu, operátor nebo člen výjezdové skupiny oznámí incident na tísňové lince 112 Integrovaného záchranného systému (pokud došlo ke zranění osob), na tísňové lince 158 Policie ČR (v případech

trestného činu) nebo na linku 150 operačního střediska HZS (když je zjištěn požár). Operátor informuje kontaktní osoby o nastalé situaci a vyžádá jejich přítomnost na místě incidentu k součinnosti a předání objektu. Pokud kontaktní osoba požádá, nebo se s ní operátor z jakéhokoliv důvodu nedokáže spojit, zajistí operátor u organizace zajišťující výjezdové služby dostřežení objektu až do doby, kdy bude možné narušený objekt předat oprávněné osobě.

Po zpětném hlášení výsledku kontroly (výjezdovou skupinou nebo kontaktní osobou) provede operátor rozbor celé události a podrobně jej zapíše do deníku událostí k příslušnému objektu a zároveň vytvoří záznam do elektronické evidence řešených událostí, včetně výsledku.

### 7.2.5 Služby pro objekty připojené na PCO HZS

Zákazníci, kteří podléhají povinnosti instalace, a tím i provozu EPS, mohou využít připojení na PCO HZS příslušného kraje pomocí smluvních provozovatelů ZDP (místo obsluhované EPS). Seznam provozovatelů ZDP je veden na webových stránkách HZS ČR dle krajské příslušnosti. Provozovatel EPS, pokud instalace systému odpovídá veškerým zákonným a normativním požadavkům, včetně TP HZS, může podat žádost o připojení EPS na PCO HZS na příslušném krajském ředitelství HZS. Veškeré postupy a požadavky TP HZS musí být splněny, aby bylo možné EPS připojit (např. předepsané dokumentace v aktuálních stavech, osazení objektu generálním klíčem nebo dostupnost provozní knihy EPS a návodů).

Administrátor DPPC společně s odborně způsobilou osobou požární ochrany (dále jen „OZO PO“) zkontroluje stav celého systému EPS zákazníka, včetně veškerých dokumentací, které jsou vyžadovány TP HZS. Dále zajistí vypracování projektové dokumentace pro zřízení ZDP, včetně projednání a schválení na místním oddělení HZS (v místech instalace EPS). Administrátor vydá písemné potvrzení o možnosti připojení EPS a zákazník odešle společně s žádostí o připojení EPS na příslušné krajské ředitelství HZS.

Pokud je vše schváleno a přijato ze strany HZS (došlo k podpisu smlouvy), dojde k uzavření smlouvy o připojení EPS pomocí ZDP, mezi provozovatelem EPS a provozovatelem ZDP.

Na rozdíl od jiných bezpečnostních systémů jsou služby DPPC v těchto případech předepsány dohodou o spolupráci provozovatele ZDP a HZS ČR. Zákazník tak má možnost pouze využít nebo nevyužít nabízených služeb připojení EPS.

Veškeré události z EPS jsou přenášeny na DPPC provozovatele. Všeobecný poplach, upřesnění poplachů a celková porucha jsou současně přenášeny na PCO HZS. Při hlášení události

*VŠEOBECNÝ POPLACH* jsou ze strany HZS vysílány JPO k zásahu na střeženém objektu. Provozovatel EPS a operátor DPPC mají možnost, v případě planého (falešného) poplachu, odvolat planý výjezd JPO přes operátora KOPIS HZS do 2 minut od vyhlášení všeobecného poplachu.

Poruchy EPS řeší operátor DPPC společně s provozovatelem EPS nebo servisní organizací zákazníka v nejbližším možném termínu od zjištění závady (např. při poruchách neovlivňujících zásadně činnost, může kontaktovat zákazníka až v ranních hodinách, pokud porucha nastala v noci).

Součástí provozu ZDP jsou povinné půlroční kontroly funkčnosti a jednoroční kontroly provozuschopnosti prováděné technickým oddělením DPPC (OZO PO musí být přítomen při kontrole provozuschopnosti).

## 7.3 Reakce na příchozí události


Obr. 28: Základní postup řešení každé poplachové události [vlastní zdroj]

Rychlé a přesné vyhodnocení příchozích událostí na DPPC je nejtěžší úloha operátora. Na prvotní reakci a na následujících krocích je závislý výsledek uskutečněných protiopatření vedoucích ke zmírnění dopadu škodícího účinku na střeženém objektu.

Základním pravidlem je, že každá poplachová událost musí být verifikována. Neexistuje žádná poplachová zpráva, která by nevyžadovala pozornost operátora. Neexistuje poplachová událost, která by nebyla vyvolána na základě vyhodnocení měřené fyzikální veličiny, určenou pro detekci narušení bezpečnosti střeženého objektu.

Operátor při vyhodnocování poplachové události si musí být naprosto jist všemi okolnostmi, než označí danou událost za planou nebo falešnou. Musí si být jist, že se nejedná

o připravovanou sabotážní akci bezpečnostního systému případným pachatelem. Operátor důkladně znovu přehodnotí veškeré zjištěné skutečnosti, než přistoupí k následujícím krokům. Aby bylo zamezeno nadměrnému objemu planých nebo falešných poplachových zpráv, operátor vyřadí (provede bypass[16]) chybující část v objektové kartě. O této skutečnosti musí být okamžitě a prokazatelně informován zákazník (pokud akční plán vyžaduje, tak i servisní organizace zákazníka) a zároveň operátor zapíše tuto skutečnost do evidence řešených událostí.

Vyřazení (bypass) celého střeženého objektu operátorem je možné pouze s prokazatelným souhlasem supervisora. Jedná se o krajní řešení situace, která by bránila kvalifikovanému vyhodnocování dalších příchozích událostí. Zákazníka informuje o vyřazení celého střeženého objetu prokazatelným způsobem supervisor. Součástí zápisu do evidence řešených událostí bude předpokládaný termín zpětného uvedení do provozu, získaný od zástupce zákazníka.

V případech, kdy se jedná o střežení systémů EPS, je nutné postupovat dle technických podmínek HZS příslušného kraje.

Jak je zřejmé z Obr. 29, je operátor limitován časem $T_{REAKCE}$, který musí být uveden v objektové kartě střeženého objektu, dle akčního plánu. Jedná se o maximální možný čas, kdy musí být operátorem zahájena první akce po příchodu řešené události.

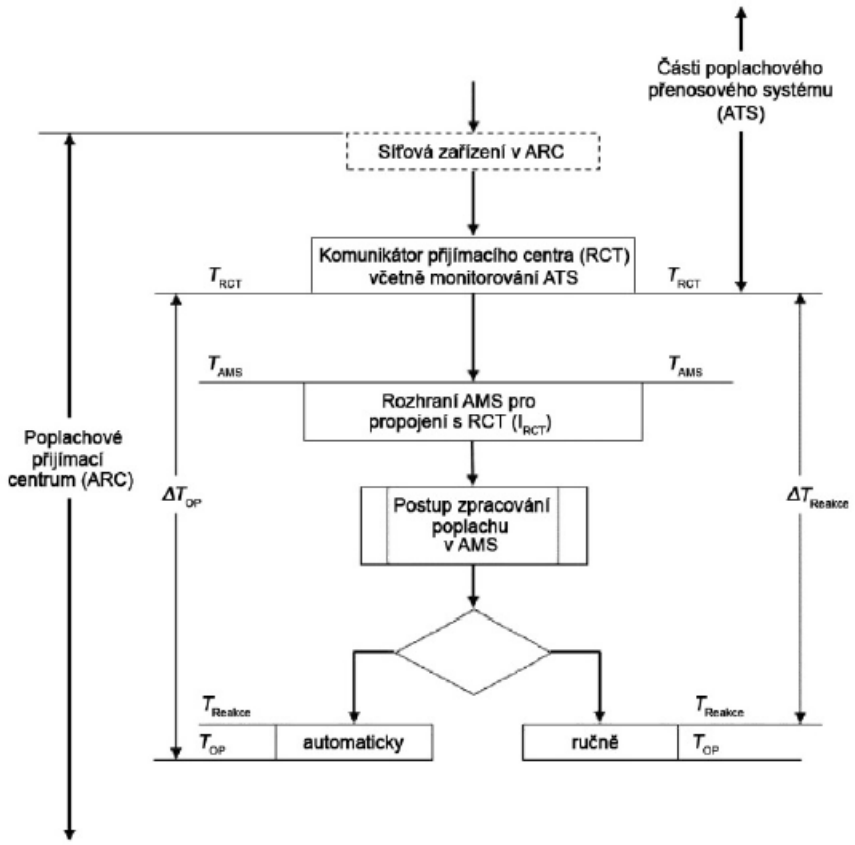
Operátor musí postupovat dle sjednaného akčního plánu pro daný objekt a pomoci mu může všeobecný postup, kde níže uvedené jednotlivé kroky vyhodnocení, reakce a iniciace akcí jsou pouze doporučené a operátorovi slouží jako vodítko reakce na daný typ příchozí události.

Administrátor DPPC by měl vzít v potaz standardy a co nejvíce se držet doporučených postupů při sestavování akčního plánu se zákazníkem. Jen v nutných případech, kdy se není možné držet doporučeného plánu, administrátor a zákazník schválí vlastní postupy vyhodnocování a detailně je popíší do akčního plánu objektu. Především administrátor si musí

[16] Bypass – vynechání, resp. vyřazení určité části ze střežení. Systémy na vyřazenou část nereagují, používá se např. při závadách nebo opravách. Bypass je možné provést přímo na řídících jednotkách uživatelem nebo v nastavení objektové karty v PPC. Ve většině případů se bypass nastavuje na určitou dobu nebo do dalšího cyklu střežení.

uvědomit, že jakákoliv odchylka od doporučených postupů vede ke zdržení operátora ve vyhodnocování vzniklé události a o této skutečnosti zákazníka prokazatelně poučit.

ČSN EN 50518




**Legenda**

| | |
|---|---|
| $T_{RCT}$ | čas výstupní zprávy z RCT |
| $T_{AMS}$ | čas přijatých zpráv na AMS |
| $T_{Reakce}$ | čas poskytnutí informací operátorovi nebo zahájení automatické akce |
| $\Delta T_{Reakce}$ | doba, která uplyne mezi okamžikem výstupu poplachové zprávy z RCT a začátkem automatického nebo manuálního zpracování poplachu v AMS ($\Delta T_{Reakce} = T_{Reakce} - T_{RCT}$) |
| $T_{OP}$ | čas první akce zahájené operátorem ARC nebo AMS podle akčního plánu dohodnutého se zákazníkem |
| $\Delta T_{OP}$ | doba, která uplyne mezi okamžikem výstupu poplachové zprávy z RCT a okamžikem první akce iniciované operátorem ARC nebo AMS ($\Delta T_{OP} = T_{OP} - T_{RCT}$) |

Obr. 29: Posloupnost příchozích událostí [2]

Dohledové videosystémy instalované v prostorách střeženého objektu mohou pomoci operátorovi k upřesnění situace, zvláště v případech, kdy je nutná komunikace se složkami integrovaného záchranného systému. Operátor je povinen, pokud je takový systém instalován, okamžitě vyhodnotit snímky z videosystému a přizpůsobit reakci vyhodnocené situaci.

### 7.3.1 Metody ověření poplachu

**Sekvenční poplach –** je stav, kdy příchozí poplachové zprávy vykazují sekvenci hlášení o narušení dvou a více detektorů (hlásičů) ze střeženého objektu. Systémy PZTS mohou být programovány na automatickou verifikaci, a v tom případě příchozí události obsahují zprávy o potvrzeném (verifikovaném, křížovém apod.) poplachu.

**Audio verifikace –** je možná, pokud je ve střeženém objektu společně s bezpečnostním systémem (nebo jiným) instalováno zařízení snímání zvuku, které je zároveň schopno přenášet zvukovou stopu na DPPC.

**Video (foto) verifikace –** může být automatická přímo z bezpečnostního systému nebo s využitím přístupu do dohledového videosystému instalovaného u zákazníka. Bezpečnostní systém při vyhlášení poplachu může být osazen prvky, které zaznamenají a přenesou na DPPC snímky, sekvence snímků nebo přímo videozáznam, před počátkem i během poplachové situace. Stejně tak jako dohledový videosystém, PZTS s videoverifikací umožňuje živý náhled do střeženého prostoru (online).

**Verifikace očitým svědkem –** lze využít v případech ověření vyslanou výjezdovou skupinou, přítomnou kontaktní osobou nebo přímo zákazníkem.

### 7.3.2 Tísňové typy událostí

Události typu tíseň signalizují operátorovi ohrožení zdraví nebo života střežené osoby (např. dohled nad nemocným člověkem) nebo ohrožení osob ve střeženém prostoru (např. zaměstnanci bank). Poplachové stavy typu tíseň jsou automaticky považovány za poplachy ostré.

Postup akcí iniciovaných operátorem je závislý na vyhodnocení příchozích zpráv nebo dalších zjištěných skutečností:

- **vyslání výjezdové skupiny** – okamžitě po přijetí tísňového hlášení,
- **kontrola VSS** – pokud je k dispozici,
- **oznámení události příslušným složkám IZS –** operátor DPPC sdělí operátorovi tísňové linky IZS veškeré podrobnosti a kroky (např. informaci o vyslání výjezdové skupiny) k předmětné události, které zjistil nebo učinil. Je potřeba si uvědomit, že zneužití tísňových linek je zakázáno,
- nebo **oznámení události osobám v pořadí uvedeném v akčním plánu** – pokud akční plán určuje přímo kontaktní osobu pro tísňové události (např. kontakt na ošetřujícího lékaře), oznámí operátor událost dle pokynů v akčním plánu.

Příklady tísňových zpráv: tíseň tichá 24 hod, přepadení, kód pod nátlakem, poslední bankovka, ohrožení života, žádost o lékařskou asistenci apod.

### 7.3.3 Hlášení událostí typu požár

Rozlišujeme, zda se jedná o zprávy ze systémů EPS (předepsané PBŘ) s přenosem signálů na PCO HZS nebo zprávy z hlásičů požáru, které jsou připojeny přes systémy PZTS (nebo obdobné).

V případě **EPS** jsou poplachové zprávy současně přenášeny pomocí ZDP na PCO HZS příslušného kraje (všeobecný poplach, místo hlášení, typ hlásiče apod.). Operátor v případě zjištění poplachové události typu požár:

- **kontaktuje osoby dle pořadí v akčním plánu** a zjistí, zda je poplachový stav ostrý nebo planý (falešný). Pokud mu kontaktní osoba sdělí, že se jedná o planý (falešný) poplach,
- tak okamžitě **spojí operátora KOPIS PCO HZS do konferenčního hovoru** se zástupcem zákazníka a společně si potvrdí, že se jedná o planý nebo falešný poplach. JPO vyjíždějí na hlášení všeobecný poplach do 2 minut od přijetí hlášení,
- nebo v případě potvrzení požáru **postupuje dle pokynů operátora KOPIS PCO HZS** a je nápomocen v komunikaci se zákazníkem.

Příklady zpráv o požáru z EPS: všeobecný poplach, požár, požární hlásič, požární tlačítko atd.

Pokud je na DPPC připojen objekt osazený lokální detekcí kouře (např. hlásiče požáru s PZTS), je DPPC jediný operující příjemce poplachové události. Operátor bez prodlení:

- **verifikuje** přijaté poplachové hlášení všemi dostupnými prostředky (sekvenční ověření, kontrola VSS nebo např. očitý svědek),
- **kontaktuje kontaktní osoby** a dále postupuje dle domluvy se zákazníkem,
- **vyšle ke kontrole výjezdovou skupinu**
- a v případě potvrzení požáru **oznámí požár na tísňové lince HZS.**

Příklady zpráv ze systémů lokální detekce kouře: požární poplach, kouřový (teplotní) hlásič v poplachu, celkový požár apod.

### 7.3.4 Detekce fyzického narušení objektu

Na rozdíl od výše uvedených typů událostí (chráněn převážně lidský život a zdraví) je detekce fyzického narušení bezpečnosti objektu zamířeno na ochranu majetku. Podmínkou funkční detekce a přenosu událostí na DPPC je bezpečnostní zařízení přepnuté do stavu střežení.

Příklady zpráv o zastřežení objektu nebo jeho části: zamčení bloku (objektu) uživatelem, objekt (sekce) zakódován uživatelem, automatické zastřežení, objekt hlídán apod.

Naopak zprávy o vypnutí bezpečnostního systému přenos poplachových zpráv znemožní např.: odemčení bloku uživatelem, odkódováno, automaticky odemčeno nebo objekt vypnut.

Ve chvíli, kdy operátor zaznamená zprávu o narušení (napadení) objektu nebo jeho části, musí si uvědomit, do které ochrany je daný detektor zamýšlen a instalován.

**Narušení perimetrické ochrany**

Tato detekce narušení je nejvíce náchylná na hlášení planých i falešných poplachů. Kvalitní systémy by měly být doplněny o automatické verifikační prvky. Akční plán vyhodnocení narušení perimetru musí být zpracován velice přehledně, detailně a musí odpovídat hodnotám střeženého majetku. Operátor musí být velice pozorný a dodržet následující:

- **postupovat dle akčního plánu,**
- **verifikovat** všemi možnými způsoby (sekvenční poplach, VSS, výjezdová skupina, kontaktní osoba atd.),
- **informovat zákazníka.**

Příklady narušení perimetru: poplach infrazávora, narušení bariéry (MW), detekce pohybu ve venkovním prostoru, zachycen pohyb plotu apod.

**Narušení plášťové ochrany**

Při detekci narušení pláště budovy je pravděpodobnost ostrého poplachu téměř jistá. Operátor vždy dle akčního plánu:

- **verifikuje** hlášenou událost,
- **vyšle výjezdovou skupinu** (v případech potvrzeného narušení oznámí PČR)**,**
- **informuje kontaktní osoby** (případně zajistí vhodná opatření)**.**

Příklady poplachových zpráv o narušení pláště objektu: poplach MK (magnetický kontakt), detekce tříštění skla, narušení plášťové ochrany IR, vibrace zachyceny atd.

**Narušení prostorové ochrany**

Poplachové zprávy signalizují pohyb možného pachatele po vnitřních prostorách střeženého objektu. Prostorová ochrana je bohužel často montována jako primární a jediná. Verifikace poplachové zprávy často není možná bez použití klíčů a přímého vstupu člena výjezdové skupiny do střeženého objektu, nebo bez přítomnosti zástupce zákazníka. Operátor opět respektuje postup uvedený v akčním plánu:

- **verifikuje** hlášenou událost,
- **vyšle výjezdovou skupinu** (v případech potvrzeného narušení oznámí PČR)**,**
- **informuje kontaktní osoby** (případně zajistí vhodná opatření)**.**

Příklady poplachových zpráv o narušení pláště objektu: poplach z detektorů pohybu (PIR, MW, duálního atd.).

**Narušení předmětové ochrany**

V případě, kdy je signalizováno poplachem narušení předmětové ochrany, je téměř jisté, že dochází k neoprávněné manipulaci se střeženým předmětem. Postup vyhodnocení a reakce musí být podrobně uveden v akčním plánu objektu a operátor je povinen dodržet:

- **postup dle akčního plánu,**
- **verifikace** všemi možnými způsoby (sekvenční poplach, VSS, kontaktní osoba atd.),
- **vyslání výjezdové skupiny** (v případech potvrzeného narušení oznámení PČR)**,**
- **informovanost zákazníka** (případně zajištění vhodných opatření)**.**

Příklady narušení bezpečnosti střeženého předmětu: ochranný kontakt rozpojen, detekován pohyb předmětu, poplach Human Detector, poplach trezor apod.).

**Kombinace narušení**

Pokud jsou zároveň nebo postupně narušeny alespoň dva výše uvedené typy ochran, je zřejmé, že se bude s největší pravděpodobností jednat o poplach ostrý. Bohužel ale nemůžeme vyloučit, že se jedná i o poplach planý, vyvolaný nesprávnou obsluhou objektu (závislost na denní době). Operátor okamžitě zahájí akce dle akčního plánu:

- části **postup při ostrém poplachu,**
- **vyšle výjezdovou skupinu** (v případech potvrzeného narušení oznámí PČR)**,**
- **informuje kontaktní osoby** (případně zajistí vhodná opatření)**.**

### 7.3.5 Sabotážní typy hlášení

Sabotážní poplach, resp. hlášení o otevření ochranných kontaktů připojeného zařízení, může znamenat přípravnou akci případného pachatele před útokem na narušení bezpečnosti střeženého objektu, a to i v době odkódování (nestřežení) poplachového systému. V praxi se také setkáváme s případy, že vlivem únavy materiálu, přicházejí na DPPC poplachová hlášení o sabotáži. Operátor nemá jinou možnost, než poplachový sabotážní stav prověřit:

- **kontaktní osobou zákazníka** (případně domluví další postup)**,**
- **servisní organizací**
- **nebo výjezdovou skupinou**.

Příklady sabotážních poplachových stavů: sabotáž, tamper, ochranný kontakt otevřen, klávesnice zablokována, snížení rozsahu detektoru, detektor zakryt, detekce rušičky bezdrátových signálů atd.

### 7.3.6 Technické alarmy

Zákazníci žádají a nechávají připojovat, prostřednictvím bezpečnostních i jiných než bezpečnostních zařízení, na PPC technologické prvky vyhodnocující různé veličiny, které potřebují sledovat a o jejich změně stavu si přejí být informováni operátorem DPPC (pokud není v akčním plánu určeno jinak). Operátor po příchodu technického alarmu:

- **informuje kontaktní osoby** (dle požadavku v akčním plánu)
- nebo **postupuje dle instrukcí v objektové kartě.**

Příklady technických alarmů: vysoká/nízká teplota, detekce plynu, porucha oběhového čerpadla nebo např. signalizace zaplavení.

### 7.3.7 Poruchové stavy zařízení zákazníka

Řídící jednotky střežených systémů informují operátora o možné poruše pomocí poruchových zpráv. Operátor je povinen sledovat další vývoj z objektu oznamujícího poruchu, zvláště pokud se jedná o systémy bezpečnostní. Pachatelé trestné činnosti, často v domněnce vyřazení bezpečnostních systémů z provozu, se pokoušejí např. odpojit přívod elektrické energie nebo přerušit (vyrušit) komunikační trasy. Zařízení mohou pracovat spolehlivě pouze ve stavu bez poruch, nebo s některou poruchou trvající určitou dobu (např. při výpadku energie). Zákazník by si měl určit, o jakých poruchových stavech chce být okamžitě informován, které jsou pro chod systému důležité, a které snesou odkladu okamžitého řešení.

Administrátor poradí zákazníkovi při sestavení akčního plánu důležitost daných hlášení. Operátor po obdržení poruchové zprávy vyhodnotí závažnost poruchového stavu a reaguje dle:

- **pokynů akčního plánu,**
- **informuje kontaktní osoby** (případně servisní organizaci)
- a **neustále sleduje další vývoj** událostí na střeženém objektu**.**

Příklady poruchových stavů: výpadek napájení ústředny, porucha akumulátoru, chyba/výpadek komunikace, porucha externích modulů, generální systémová porucha apod.

### 7.3.8 Informační události

Zákaznické systémy informují PPC o svém stavu pomocí informačních událostí, které se pouze zapisují do deníku událostí (nejsou zvukově ani opticky zvýrazněné). Operátor tak má při vyhodnocování poplachových, ale i jiných událostí, přehled, v jakém stavu se zařízení nachází nebo jak bylo zařízení ovládáno. Např. je patrné, kdy se daný systém uvádí do stavu střežení, odstřežení nebo kdy zařízení posílá testovací zprávy přenosu.

Příklady informačních událostí: test přenosu, odemčeno/zamčeno, odemčeno po poplachu, nastavení systémových hodin, vzdálený downloading, servis povolen apod.

### 7.3.9 Náhlé zvýšení počtu příchozích událostí

Mohou nastat situace, kdy vlivem nestandardní události (např. nepřízeň počasí, výpadek energie nebo komunikačních kanálů, ohňostroje apod.) dojde k náhlému zvýšení počtu příchozích zpráv. V té chvíli musí každý operátor upřednostňovat a v první řadě řešit prioritní poplachové události oznamující ohrožení lidského života (např. tíseň, požár) napříč všemi hlášenými stavy.

Pokud situace není zvládnutelná přítomnými operátory, musí operátor oznámit situaci supervisorovi, který zajistí dočasné zvýšení počtu operujících osob.

Pří náhlém zvýšení příchozích zpráv je na místě ostražitost každého operátora, kdy musí jasně určit příčinu příchozích událostí. Např. při výpadku energie nebo výpadku datových linek lze ověřit u jednotlivých distributorů. Náhlé zvýšení počtu událostí může např. také znamenat kybernetický útok na jakoukoliv část PPC. V situacích, kdy operátor neumí určit jasnou příčinu náhlého zvýšení, oznámí tento stav supervisorovi, který určí další kroky vedoucí k vyhodnocení nastalé situace.

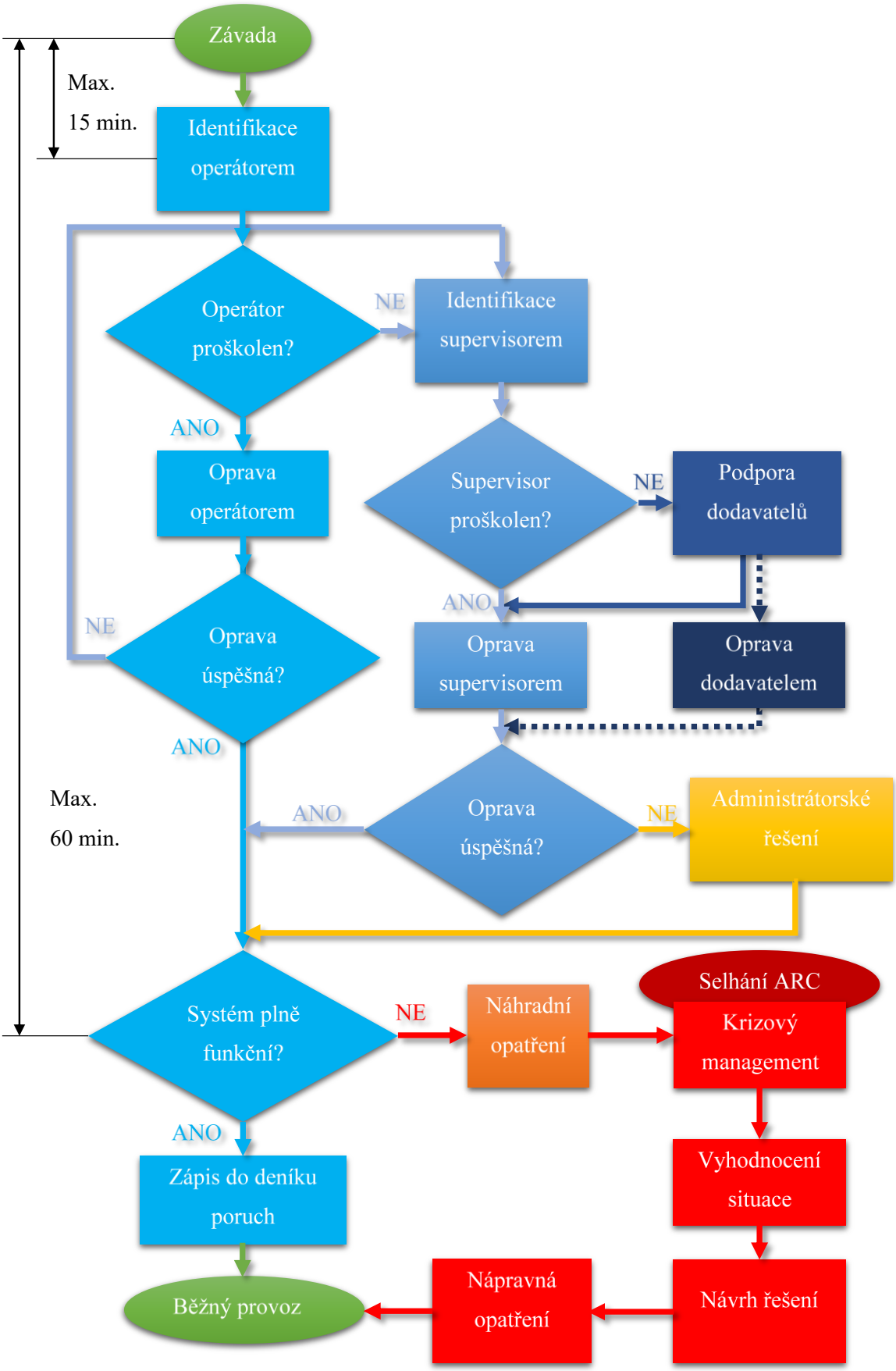
## 7.4 Postupy při zjištění závad zařízení PPC

*Jakákoli součást zařízení zapojená do příjmu, zobrazení nebo dalšího přenosu poplachového signálu, včetně napájení, musí mít záložní zařízení a postup, kterým může být uveden do provozu buď automaticky, nebo dispečerem ARC do 1 h od okamžiku, kdy se dispečer o existenci závady dozví* [2].

Zařízení, která mají automatické redundantní řešení, přejdou na záložní systém samočinně a upozornění se objeví na monitoru operátora, včetně záznamu do deníku událostí. Ostatní zařízení se musí vyměnit fyzicky. Výměnu nebo opravu prvků, které operátor není schopen (není proškolen) zprovoznit sám, zajistí supervisor po prokazatelném oznámení operátora, který je na hlášení závady limitován 15 minutami od zjištění (směrodatný čas je záznam v deníku událostí), viz Obr. 30. Operátor veškeré zjištěné závady zapíše do elektronického deníku závad, včetně řešení opravy, kdo jí vykonal a jak dlouho bylo zařízení mimo provoz.

Tab. 19: Příklady možných závad opravitelných operátorem

| Závada | Příklady zařízení | Primární oprava |
|---|---|---|
| Napájení | Rozvaděč nízkého napětí (jističe), UPS, generátor. U generátoru pouze optická kontrola pomocí VSS. | Kontrola chodu, uvedení do provozu. |
| Periferie operátora | Monitory, klávesnice, myši, reproduktory, telefonní a komunikační aparáty. | Kontrola konektorů, kabely, výměna. |
| Klientské stanice | Počítače, kde jsou instalované nebo provozované klientské aplikace jednotlivých PPC. Redundance na jiné stanici, SW jsou instalovány na všech PC. | Kontrola napájení, restart počítače. |
| Internet | WAN, LAN. Komunikace pomocí datových sítí. | Kontrola PING. Restart síťových prvků. |
| Ostatní komunikace | Přijímače a převodníky jednotlivých výrobců pro příjem zpráv. V klientské aplikaci systém SW konektorů (GS51, GSM, SAMBA apod.). | Napájení, restart konkrétního SW, konektor nebo HW. |




Obr. 30: Návrh postupu při zjištění závady PPC [vlastní zdroj]

Za kompletnost náhradních dílů, ať s automatickým přepínáním nebo manuálně vyměnitelných, nese odpovědnost supervisor. Při výměně jakékoliv části zařízení zajistí přes administrátora nový kus. Náhradní zařízení (vyjma zařízení uvedená v Tab. 19, která jsou určená přímo pro dohledové centrum), která nejsou připojená do systému pro automatickou redundanci, budou v zamčené a střežené skříni (místnosti), od které bude mít klíč supervisor a administrátor. Inventura náhradních zařízení bude probíhat minimálně 1x za 6 měsíců a protokol bude stvrzen podpisem supervisora i administrátora. Kontrola deníku závad a vyhodnocení oprav je každodenní činností supervisora (v rámci běžné pracovní doby).

Tab. 20: Příklady možných závad, které jsou předávány na supervisora

| Závada | Příklady zařízení | Primární oprava |
|---|---|---|
| Internet | Nefunkční internetová komunikace, operátor identifikoval konkrétní nefunkční část. Chyba WAN nebo serveru s firewallem. | Při ztrátě konektivity, kontaktovat tech. odd. providera. |
| LAN | Operátor zjistil chybu vnitřní sítě, switche, konektoru nebo kabelážního systému. | Kontrola konektorů, výměna zařízení. |
| Komunikátory | HW pro příjem zpráv z objektových zařízení a zprostředkovatel komunikace na servery PPC. | Restart a postup dle výrobce zařízení. |
| Servery PPC | Závažná chyba na SW nebo HW serverové části. | Restart, tech. servis dodavatele. |
| Komunikační prostředky | Telefonní ústředna, záznam hovorů. | Restart a postup dle výrobce zařízení. |
| UPS | Záložní bateriový zdroj, vadné akumulátory. | Výměna akumulátorů nebo celé UPS. |
| Generátor | Pohotovostní generátor. | Postup dle výrobce. |

# 8 PŘÍKLADY VYHODNOCENÍ UDÁLOSTÍ OPERÁTOREM DPPC

Následující příklady vyhodnocení nebo následků událostí slouží pouze pro studijní účely. Události pro potřeby diplomové práce byly simulované (dle reálných případů) a znázorňují možné varianty akcí vyvolaných operátorem.

## 8.1 Narušení plášťové ochrany objektu

| | |
|---|---|
| 7:07:26 | Poplach zóny 9 (9 2x MK wc+chodbička) v bloku 2 |
| 4:30:54 | Periodický test ústředny |
| 1:30:32 | POLICIE ZADRŽELA OBČANA ...SKLO VLEVO OD VCHODU LEHCE POŠKOZENO. INFORMOVÁNA pí. |
| 1:27:40 | IP telefonu bylo předáno volání na číslo: +420 |
| 0:53:44 | Odbavení zvukové signalizace |
| 0:53:41 | Obnova zóny 4 (4 AČ prodejna) |
| 0:53:38 | Poplach zóny 4 (4 AČ prodejna) v bloku 1 |
| 0:53:35 | Obnova zóny 4 (4 AČ prodejna) |
| 0:53:33 | Odbavení zvukové signalizace |
| 0:53:32 | Poplach zóny 4 (4 AČ prodejna) v bloku 1 |
| 0:53:30 | Obnova zóny 4 (4 AČ prodejna) |
| 0:53:27 | Poplach zóny 4 (4 AČ prodejna) v bloku 1 |
| 0:48:11 | Odbavení zvukové signalizace |
| 0:48:10 | Obnova zóny 4 (4 AČ prodejna) |
| 0:48:07 | Poplach zóny 4 (4 AČ prodejna) v bloku 1 |
| 0:48:00 | VYSLÁNA HLÍDKA |
| 0:46:11 | Odbavení zvukové signalizace |
| 0:46:11 | Obnova zóny 4 (4 AČ prodejna) |
| 0:46:08 | |
| 0:46:08 | Poplach zóny 4 (4 AČ prodejna) v bloku 1 |
| 20:11:27 | Zamčení bloku 2 uživatelem 5 |
| 20:11:24 | Zamčení bloku 1 uživatelem 5 |
| 7:47:10 | Odemčení bloku 2 uživatelem 5 |
| 7:47:08 | Odemčení bloku 1 uživatelem 5 |

Obr. 31: Posloupnost událostí při narušení pláště objektu [21]

Na Obr. 31 je vidět posloupnost událostí napadeného objektu a velice správná reakce operátora, včetně následného rozboru. Po příchodu poplachové zprávy o narušení bezpečnosti plášťové ochrany (AČ – detektor tříštění skla) operátor okamžitě vyslal výjezdovou skupinu k verifikaci poplachu. Zároveň, dle akčního plánu a požadavku PČR, oznámil podezření na trestnou činnost na tísňové lince PČR (limit času $T_{REAKCE}$ byl splněn, včetně zápisu do deníku událostí).

Chyba operátora spočívá pouze v nezapsání všech akcí prováděných operátorem v rámci řešené události (chybí zápis o oznámení podezření na lince PČR) do deníku událostí.

Následný zásah PČR vedl k dopadení pachatele přímo při konání trestném činu.

## 8.2 Narušení bezpečnosti objektu

| | |
|---|---|
| 0:12:32 | Poplach zóny 7 (7 AČ šatna) v bloku 1 |
| 0:12:34 | Obnova zóny 7 (7 AČ šatna) |
| 0:13:21 | Poplach zóny 7 (7 AČ šatna) v bloku 1 |
| 0:13:24 | Obnova zóny 7 (7 AČ šatna) |
| 0:13:26 | Poplach zóny 7 (7 AČ šatna) v bloku 1 |
| 0:13:29 | Obnova zóny 7 (7 AČ šatna) |
| 0:13:32 | Poplach zóny 7 (7 AČ šatna) v bloku 1 |
| 0:13:35 | Poplach zóny 6 (6 IČ šatna) v bloku 1 |
| 0:13:37 | Potvrzený poplach - křížový alarm |
| 0:13:40 | Obnova zóny 6 (6 IČ šatna) |
| 0:13:43 | Obnova zóny 7 (7 AČ šatna) |
| 0:13:46 | Poplach zóny 6 (6 IČ šatna) v bloku 1 |
| 0:13:48 | Obnova zóny 6 (6 IČ šatna) |
| 0:13:51 | Poplach zóny 6 (6 IČ šatna) v bloku 1 |
| 0:13:54 | Obnova zóny 6 (6 IČ šatna) |
| 0:14:07 | Poplach zóny 3 (3 DČ kancelář u kuchyňky) v bloku 1 |
| 0:14:10 | Poplach zóny 5 (5 MK kancelář vedoucí) v bloku 1 |
| 0:14:13 | Obnova zóny 3 (3 DČ kancelář u kuchyňky) |
| 0:14:16 | Poplach zóny 3 (3 DČ kancelář u kuchyňky) v bloku 1 |
| 0:14:19 | Obnova zóny 3 (3 DČ kancelář u kuchyňky) |
| 0:14:21 | Poplach zóny 3 (3 DČ kancelář u kuchyňky) v bloku 1 |
| 0:14:24 | Obnova zóny 3 (3 DČ kancelář u kuchyňky) |
| 0:14:28 | Poplach zóny 2 (2 AČ kancelář vedoucí) v bloku 1 |
| 0:14:30 | Obnova zóny 2 (2 AČ kancelář vedoucí) |
| 0:14:33 | Poplach zóny 2 (2 AČ kancelář vedoucí) v bloku 1 |
| 0:14:59 | IP telefonu bylo předáno volání na číslo: |
| | |
| 0:43:38 | Automatická událost 'Deaktivace poplachu' |
| 0:44:11 | Automatická událost 'Deaktivace poplachu' |
| 0:44:34 | Automatická událost 'Deaktivace poplachu' |
| 2:19:24 | Napadený objekt předán: POLICII ČR ! |
| 4:44:33 | Ztráta spojení Komunikátor |

Obr. 32: Posloupnost událostí napadení objektu [vlastní zdroj]

I v tomto případě pachatel využil nočních hodin pro napadení objektu. Jak je patrné z Obr. 32, narušení bylo započato útokem na plášťovou ochranu (detekce tříštění skla) a pokračovalo vstupem do střeženého objektu přes detektor pohybu prostorové ochrany (IČ – infračervený detektor). V té chvíli došlo k automatické verifikaci ústřednou PZTS a na PPC byl potvrzen poplach. Pohyb pokračoval přes další detektory (DČ – duální detektor, MK – magnetický kontakt) až do kanceláře vedoucího, kde byla umístěna ústředna PZTS. Poslední zprávy z objektu signalizují zachycení zvuku po úderech kladivem do skříně ústředny, která následně byla vyřazena z provozu.

Operátor v tomto případě reagoval s velkým zpožděním na příchozí události. První akce vyvolaná operátorem byla až za 2,5 minuty, resp. za 1,5 minutu po potvrzeném poplachu, a to telefonickým hovorem s kontaktní osobou uvedenou v akčním plánu. Až poté byla vyslána hlídka výjezdové skupiny, která dalších 15 minut čekala na příjezd kontaktní osoby. Prohlídkou objektu bylo zjištěno napadení, ale pachatel již v objektu nebyl.


Obr. 33: Ilustrativní fotografie napadení objektu [vlastní zdroj]

Ač bylo zřejmé, že se jedná o ostrý poplach, operátor z nepochopitelných důvodů nereagoval včas na příchozí události a namísto okamžitého vyslání výjezdové skupiny (včetně oznámení na tísňovou linku PČR) informoval s prodlením kontaktní osobu. Na obranu operátora se přiklání pouze skutečnost, že zákazník v akčním plánu požadoval veškeré události, a s tím spojené akce, konzultovat s kontaktní osobou. Administrátor se zákazníkem by měli provést revizi akčního plánu, která by reakce na události urychlila, a tím i zvýšila možnost zadržet pachatele při činu.

Operátor v tomto případě hrubě zanedbal povinnost zápisu veškerých prováděných akcí do deníku událostí, a to včetně závěrečného rozboru události.

## 8.3 Vyhodnocení planého poplachu z EPS

Systémy EPS připojené zároveň na PCO HZS musí operátor DPPC řešit hlavně z pohledu planých poplachů, resp. planých výjezdů JPO HZS (JPO vyjíždějí do 2 minut od přijetí hlášení *VŠEOBECNÝ POPLACH*).

Na Obr. 34 je znázorněna posloupnost poplachových událostí ze systému EPS. První zaznamenaná událost znamená otevření prvních dvířek klíčového trezoru (zde je zřejmé špatné naprogramování ústředny, kdy KTPO je otevřeno již v čase T1). Následuje požární poplach hlásiče s popisem umístění (v této době je právě spouštěn čas T1) a na závěr, po vypršení času T1 (obsluha nestihla v definovaném čase deaktivovat bzučák), je vyhlášen *VŠEOBECNÝ POPLACH* (Celkový požár), který je zároveň přenášen na PCO HZS a vyvolává akci pro JPO HZS.

Obsluha ovšem stihla do 2 minut od vyhlášení poplachu zavolat na DPPC, že se jedná o planý poplach. Operátor DPPC okamžitě připojil do konferenčního hovoru operátora KOPIS HZS, kdy si společně všechny zúčastněné strany potvrdily přijetí planého poplachu (JPO nebyla vyslána). Následoval reset ústředny EPS a znovunastavení do stavu střežení.

| | | | | |
|---|---|---|---|---|
| REGGAE Poplach na smyčce | 0003 | Klíčový trezor | 0000 | |
| Vznik akce | | | | |
| Ukončení akce | | | | |
| Požár hlásiče v zóně | 0097 | zóna 151 | 9701 | Prodejna 3 Příjem |
| POŽÁR | FB00 | | 0000 | |
| REGGAE Požár na smyčce | 0001 | Celkový požár | 0000 | |
| Vznik akce | | | | |
| Ukončení akce | | | | |
| Deaktivace bzučáku | 9300 | | 0000 | |
| REGGAE Obnovení smyčky | 0003 | Klíčový trezor | 0000 | |
| Celkový reset ústředny | FB00 | | 0000 | |
| REGGAE Obnova požární smyčky | 0001 | Celkový požár | 0000 | |
| Převzetí akce operátorem | | | | |
| Bypass pro Výjezd aktivován | | | | |

Obr. 34: Příklad vyhodnocení planého poplachu z EPS [22]

## 8.4 Příklady útoků na datové linky PPC

Na Obr. 35 je znázorněn výpis z deníku událostí. Operátor DPPC správně vyhodnotil příchozí události jako nestandardní a dle pokynů SOP informoval supervisora. Společně s administrátorem supervisor vyhodnotil, pomocí logu datové komunikace (Obr. 36), že se jedná o zprávy z neznámých IP adres.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 17.07.2020 | 10:28:4 | | Nepodporovaný formát zprávy. | | 0x53 30 31 30 30 31 5B 23 31 39 33 34 7C 4F 72 69 30 2F 52 50 30 30 33 5D 14 | Chybná data v přijaté zprávě | TCP : 1 |
| 17.07.2020 | 10:28:1 | 1951 | Obnova komunikace s přijímačem 1 PCO | 1951 | 0x59 4B 00 00 01 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:28:1 | | Nepodporovaný formát zprávy. | | 0x53 30 31 30 30 31 5B 23 31 39 35 31 7C 4F 72 69 30 2F 52 50 30 30 33 5D 14 | Chybná data v přijaté zprávě | TCP : 1 |
| 17.07.2020 | 10:28:1 | 1966 | Obnova komunikace s přijímačem 1 PCO | 1966 | 0x59 4B 00 00 01 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:28:1 | 1966 | Porucha v komunikaci s přijímačem 1 PCO | 1966 | 0x59 53 00 00 01 | Informační událost bez upozornění - aktivac | TCP : 1 |
| 17.07.2020 | 10:28:0 | 1951 | Obnova komunikace s přijímačem 1 PCO | 1951 | 0x59 4B 00 00 01 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:28:0 | | Nepodporovaný formát zprávy. | | 0x53 30 31 30 30 31 5B 23 31 39 35 31 7C 4F 72 69 30 2F 52 50 30 30 31 5D 14 | Chybná data v přijaté zprávě | TCP : 1 |
| 17.07.2020 | 10:27:2 | 1980 | Obnova komunikace s přijímačem 1 PCO | 1980 | 0x59 4B 00 00 01 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:27:2 | | Nepodporovaný formát zprávy. | | 0x53 30 31 30 30 31 5B 23 31 39 38 30 7C 4F 72 69 30 2F 52 50 30 30 33 5D 14 | Chybná data v přijaté zprávě | TCP : 1 |
| 17.07.2020 | 10:27:2 | 1980 | Obnova komunikace s přijímačem 1 PCO | 1980 | 0x59 4B 00 00 01 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:27:2 | | Nepodporovaný formát zprávy. | | 0x53 30 31 30 30 31 5B 23 31 39 38 30 7C 4F 72 69 30 2F 52 50 30 30 31 5D 14 | Chybná data v přijaté zprávě | TCP : 1 |
| 17.07.2020 | 10:05:5 | 1989 | Obnova komunikace s přijímačem 3 PCO | 1989 | 0x59 4B 00 00 03 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 10:00:3 | 1971 | Obnova komunikace s přijímačem 0 PCO | 1971 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:55:16 | 1925 | Obnova komunikace s přijímačem 0 PCO | 1925 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:55:00 | 1927 | Obnova komunikace s přijímačem 0 PCO | 1927 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:53:56 | 1947 | Obnova komunikace s přijímačem 0 PCO | 1947 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:53:53 | 1952 | Obnova komunikace s přijímačem 0 PCO | 1952 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:53:47 | 1960 | Obnova komunikace s přijímačem 0 PCO | 1960 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |
| 17.07.2020 | 9:53:41 | 1942 | Obnova komunikace s přijímačem 0 PCO | 1942 | 0x59 4B 01 00 00 | Informační událost bez upozornění - deaktiv | TCP : 1 |

Obr. 35: Výpis z deníku událostí při útoku na datovou linku PPC [21]

```
-SG -01-001-4954-YN-*Invalid Report/Possible Compromise Attempt 103.253.42.53*
-SG -01-001-0000-NR-Network Restoral
-SG -01-001-1910--Nri0/RP0001
-SG -01-001-1910--Nri0/RP0003
-SG -01-001-1971--Nri0/RP00
-SG -01-000-0000-NRR0001-SG-System II v2.12.01.002 Power Up
```

Obr. 36: Výpis z logu dat. komunikace [21]

Podobným způsobem byly také zjištěny útoky na kamerový systém DPPC. Prvotní impuls na kontrolu komunikace byl dán operátorem v době, kdy obrazy z VSS vykazovaly značné zpomalení a vynechávání.

Tab. 21: Seznam nelegálních přístupů do VSS HIKVISION

**Seznam protokolů**

| čas | Hlavni typ | Vedlejsi typ | Místní/vzdálený uživatel | Vzdál. host IP |
|---|---|---|---|---|
| 2020-06-17 07:25:59 | Varování | Nelegal.pristup | admin | 109.173.69.109 |
| 2020-06-20 14:59:38 | Varování | Nelegal.pristup | admin | 45.9.238.21 |
| 2020-06-21 20:53:21 | Varování | Nelegal.pristup | admin | 51.38.36.213 |
| 2020-06-21 23:07:46 | Varování | Nelegal.pristup | admin | 176.65.96.188 |
| 2020-06-23 02:10:10 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-06-23 08:27:35 | Varování | Nelegal.pristup | admin | 192.168.100.147 |
| 2020-06-24 00:02:55 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-06-24 01:09:05 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-06-25 13:22:21 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-06-26 04:21:37 | Varování | Nelegal.pristup | admin | 176.65.96.188 |
| 2020-06-27 00:37:56 | Varování | Nelegal.pristup | admin | 176.65.96.188 |
| 2020-06-27 17:04:41 | Varování | Nelegal.pristup | admin | 176.65.96.188 |
| 2020-06-27 19:54:30 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-06-28 06:47:43 | Varování | Nelegal.pristup | admin | 51.38.36.213 |
| 2020-06-29 04:10:09 | Varování | Nelegal.pristup | admin | 109.173.69.109 |
| 2020-06-29 15:15:03 | Varování | Nelegal.pristup | admin | 109.173.69.109 |
| 2020-06-29 22:37:07 | Varování | Nelegal.pristup | admin | 45.9.238.21 |
| 2020-06-30 10:12:09 | Varování | Nelegal.pristup | admin | 176.65.96.188 |
| 2020-07-01 16:29:26 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-07-02 06:02:56 | Varování | Nelegal.pristup | admin | 192.168.100.147 |
| 2020-07-03 13:47:53 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-07-04 06:08:37 | Varování | Nelegal.pristup | admin | 192.168.100.112 |
| 2020-07-08 09:58:39 | Varování | Nelegal.pristup | admin | 192.168.100.147 |
| 2020-07-08 10:27:20 | Varování | Nelegal.pristup | admin | 192.168.100.147 |
| 2020-07-10 08:48:52 | Varování | Nelegal.pristup | admin | 192.168.100.112 |

Celkem 25 položek 1/1

Dostupným lokalizačním nástrojem Connection Meter určili administrátor a supervisor původ příchozích zpráv z oblasti Asie (Obr. 37).

Následně byl dán požadavek na správce IT struktury k zablokování jakékoliv komunikace na zařízení PPC z rozsahů IP adres jiných než z České republiky.


Obr. 37: Lokalizace podezřelé adresy [24]

# ZÁVĚR

Diplomová práce si klade za cíl pomoci odpovědným osobám bezpečnostních agentur nastavit pevná pravidla a odpovědnost pro bezproblémový provoz dohledového poplachového a přijímacího centra. Žádná společnost nemůže být stejná, a proto diplomová práce může sloužit pouze jako možné vodítko při zpracovávání standardních operačních postupů a školení odpovědných pracovníků administrátorem dohledového centra. Zvláště pak u velkých provozovatelů je nutné přihlédnutí na jejich provozní zvyklosti, větší množství připojených objektů, větší množství operátorů a již nastavených procesů.

Práce vychází z požadavků platných norem na provoz a činnost DPPC a zařízení, ale také z autorových profesních praktických zkušeností, konzultací s profesními komorami a v neposlední řadě ze získaných vědomostí během studia na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně. Autor vychází a v práci uvádí často zjištěné nedostatky, nebo problémy, které provází chod běžných, středně velkých dohledových center. Nejčastější chybou je úplná absence nebo nekompletnost akčního plánu objektu, nestandardizované postupy vyhodnocení a reakcí na příchozí události, a především různorodost schválených požadavků zákazníků obchodním zástupcem bezpečnostní agentury bez předchozí domluvy s osobou odpovědnou za celkový chod dohledového centra. Dalším podstatným nedostatkem je neznalost základních principů funkčnosti technologických zařízení operátory DPPC. Bohužel i trend dnešní doby vede k faktu, že bezpečnostní zařízení instalují osoby bez jakéhokoliv ponětí a znalostí o bezpečnostních systémech. Nezbývá nic jiného než doufat, že zákazník si prověří svou instalační firmu, která bude odpovědná v plném rozsahu za instalaci systémů v jeho objektu, a ta zvolí prvky, které pomůžou zvýšit bezpečnostní opatření objektu.

Diplomová práce se ve svém úvodu věnuje popisu a funkčnosti technologických celků bezpečnostních i jiných než bezpečnostních systémů v podobě vybraných zařízení (PZTS, EPS, VSS a ZDP). Uvedené systémy jsou pouze základními technologiemi, které je možné instalovat u zákazníků a střežit na dohledovém centru. Z výše uvedených systémů lze odvodit funkčnost ostatních připojitelných technologií. Úvodní teoretická část je určená pro začínající pracovníky dohledových center pro základní pochopení funkčnosti bezpečnostních systémů, přenosu událostí a pro snadnější vyhodnocování příchozích událostí na zařízení PPC.

Praktická část diplomové práce se věnuje provozním záležitostem ohledně celkového chodu dohledového poplachového a přijímacího centra. Jsou zde uvedena provozní řešení včetně možného prostorového uspořádání jednotlivých částí DPPC, včetně instalovaných

bezpečnostních systémů pro ochranu samotného dohledového centra. Vymezení účastníků, činností a pojmů při střežení zákaznických systémů je nedílnou součástí standardních operačních postupů. Pracovníkům operačního střediska dohledového centra usnadní práci standardizování postupů a reakcí při vyhodnocování příchozích událostí. Operátoři, supervisoři i administrátoři se zde také mohou dočíst, jak postupovat v případech, kdy zjistí závadu na zařízení PPC. Na závěr praktické části jsou rozebrány příklady vyhodnocení poplachových událostí, které byly simulovány pro potřeby diplomové práce, ale vycházejí z reálných situací při provozu dohledového poplachového a přijímacího centra.

Diplomová práce přináší možnost standardizovat pracovní postupy v rámci činnosti poskytování bezpečnostních služeb pomocí dohledových center. Odpovědní zástupci bezpečnostních agentur mohou dle předložených standardních operačních postupů vytvořit své vlastní postupové směrnice a mohou zároveň vytvořit školící plán operátorů. Supervisoři a administrátoři zde najdou obecný návod odpovědnosti na jednotlivých pracovních pozicích. Operátorům obsah diplomové práce přiblíží a usnadní vyhodnocování příchozích událostí, navede je na optimální reakce po vyhodnocení a celkově usnadní jejich práci. Ostatním čtenářům, resp. zákazníkům autor nabídl náhled do nelehké práce pracovníků bezpečnostních služeb a možná jim pomohl ve výběru budoucích bezpečnostních opatření a výběru bezpečnostní agentury.

# CITOVANÁ LITERATURA

[1] Monitorovací technologie, které pracují za vás. In: *NAM system, a.s.* [online]. [cit. 2020-07-26]. Dostupné z: https://www.nam.cz/

[2] ČSN EN 50518. *Dohledová a poplachová přijímací centra*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020, 44 s. Třídicí znak: 334599.

[3] KREJČÍ, Tomáš. *Řešení přenosových tras a protokolů dohledového a poplachového přijímacího centra*. Zlín, 2018.. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Ján Ivanka.

[4] ASOCIACE TECHNICKÝCH BEZPEČNOSTNÍCH SLUŽEB GRÉMIUM ALARM Z.S. *Stanovení úrovně zabezpečení objektů a provozoven*. Praha: Česká agentury pro standardizaci, 2018.

[5] LUKÁŠ, Luděk. *Teorie bezpečnosti I.* Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.

[6] Fuzzy logika – od pračky po perimetr. *ABBAS* [online]. 2011 [cit. 2020-07-19]. Dostupné z: http://www.abbas.cz/clanky/aktuality/fuzzy-logika-od-pracky-po-perimetr/

[7] Prosíme nesahat! Představujeme systém Human Detector. In: *TSS Group s.r.o.* [online]. 2002-2018 [cit. 2020-07-20]. Dostupné z: https://www.tssgroup.cz/item/prosime-nesahat-predstavujeme-system-human-detector/

[8] Https://1box.cz/co-umi-1box/ochrana-osob-tisnovymi-tlacitky/. In: *NAM system, a.s.* [online]. 2020 [cit. 2020-07-28]. Dostupné z: https://1box.cz/co-umi-1box/ochrana-osob-tisnovymi-tlacitky/

[9] VALOUCH, Jan. *Projektování integrovaných systémů*. Druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015. ISBN 978-80-7454-557-3.

[10] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Vyd. 5. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978–80–7454–410–1.

[11] SOTERIA tlačítkový hlásič s izolátorem. In: *EUROALARM spol. s r.o.* [online]. 2020 [cit. 2020-07-21]. Dostupné z: https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pozarni-signalizace/analogove-systemy/hlasice/tlacitka/sa5900-908apo-s562837274

[12] *Klíčový trezor požární ochrany* [online]. In: . [cit. 2020-07-27]. Dostupné z: https://www.hltrade.cz/modules/tableadmin2/external/imageext_new.php?image=WG9%2BY3N%2BZHNjaTAwMjAuanBnfmdhbGVyaWV%2Bb2JyYXpla19jb3VudGVyfjE4fmdhbGVyaWV%2BMX4zMX5vWQ%3D%3D&TB_iframe=true&width=640&height=480&modal=true

[13] Propojte váš pult s kamerovým systémem Hikvision. In: *NAM system, a.s.* [online]. 2020 [cit. 2020-07-28]. Dostupné z: https://1box.cz/propojeni-s-kamerovym-systemem-hikvision/

[14] KRAJSKÉ ŘEDITELSTVÍ HZS JIHOČESKÉHO KRAJE. *Technické podmínky pro připojení elektrické požární signalizace na pult centralizované ochrany HZS Jihočeského kraje*. 2020.

[15] Pracovník dohledového centra. *Národní soustava kvalifikací* [online]. 2006-2014 [cit. 2020-07-27]. Dostupné z: https://www.narodnikvalifikace.cz/kvalifikace-970-Pracovnik_dohledoveho_centra/revize-1438

[16] Aplikace pro organizaci výjezdových skupin. *NAM system, a.s.* [online]. 2020 [cit. 2020-07-27]. Dostupné z: https://1box.cz/co-umi-1box/aplikace-pro-organizaci-vyjezdovych-skupin/

[17] ŠPAČEK, František. *Integrovaný záchranný systém* [online]. Generální ředitelství Hasičského záchranného sboru ČR, 2009 [cit. 2020-07-29]. Dostupné z: https://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx

[18] *Tísňová volání v České republice* [online]. Generální ředitelství Hasičského záchranného sboru ČR, 2020 [cit. 2020-07-29]. Dostupné z: https://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice.aspx

[19] DS-K1T671. In: *HIKVISION* [online]. 2020 [cit. 2020-07-30]. Dostupné z: https://www.hikvision.com/cz/products/Access-Control-Products/Face-Recognition-Terminals/Pro-Series/ds-k1t671/

[20] 1Box rack. In: *NAM system, a.s.* [online]. 2013-2020 [cit. 2020-07-22]. Dostupné z: https://www.namtechnology.cz/pco_c259523398860899/pco-1box_c259523398860906/1box-rack_p5089

[21] *Systém RADOMNET II pro RADOM SECURITY a RADOM SECURITY FIRE*. 4. Pardubice: Radom, 2016.

[22] NAM SYSTEM, a.s. *Software NET-G*. Havířov, 2020.

[23] ČTYŘ A VÍCE VÁLCOVÉ STROJE. In: *KIPOR*® [online]. IRIUM s.r.o., 2011 [cit. 2020-07-22]. Dostupné z: https://www.kipor.cz/fotogalerie-ctyr-a-vice-valcove-stroje

[24] Lokalizace IP, zjištění polohy zařízení na mapě. *Connection Meter*® [online]. E+P Studio, 2017 [cit. 2020-07-17]. Dostupné z: https://conmet.cz/lokalizace-ip-zjisteni-polohy-zarizeni-na-mape.html?ip_adresa=103.253.42.53#

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| AGA | Asociace technických bezpečnostních služeb Grémium Alarm z.s. |
| AMS | Systém správy poplachu (Alarm management systém) |
| ARC | Alarm receiving centre |
| AVDES | Audio video dveřní vstupní systém (Audio video door entry system) |
| BOZP | Bezpečnost a ochrana zdraví při práci |
| CCTV | Kamerový systém |
| ČR | Česká republika |
| ČSN | Česká státní norma |
| ČSN EN | Česká verze evropské normy |
| DPPC | Dohledové a poplachové přijímací centrum |
| DZP | Dokumentace zdolávání požáru |
| EKV | Elektrická kontrola vstupu |
| EPS | Elektrická požární signalizace |
| EZS | Elektrické zabezpečovací signalizace |
| GDPR | Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation) |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Globální Systém Mobilní komunikace |
| HW | Hardware |
| HZS | Hasičský záchranný sbor |
| I&HAS | Intrusion and hold-up alarm systems |
| IP | Internet Protocol |
| IR | Infračervený detektor (Infrared sensor) |
| IT | Informační technologie |

| | |
|---|---|
| IZS | Integrovaný záchranný systém |
| JPO | Jednotka požární ochrany |
| JTS | Jednotná telefonní síť |
| KOPIS | Krajské operační a informační středisko |
| KTPO | Klíčový trezor požární ochrany |
| LAN | Local Area Network |
| LEA | Orgán výkonu práva (Law Enforced Agency) |
| MARC | Monitoring and alarm receiving centre |
| MK | Magnetický kontakt |
| MW | Mikrovlnný detektor (Microwave sensor) |
| MZS | Mechanické zábranné systémy |
| OPPO | Opakovací tablo požární ochrany |
| OZO PO | Odborně způsobilá osoba požární ochrany |
| PBŘ | Požárně bezpečnostní řešení stavby |
| PCO | Pult centralizované ochrany |
| PČR | Policie České republiky |
| PGM | Programovatelný výstup systému |
| PIR | Pasivní infračervený detektor (Passive infrared sensor) |
| PO | Požární ochrana |
| PPC | Poplachové přijímací centrum |
| PZTS | Poplachový zabezpečovací a tísňový systém |
| RCT | Komunikátor přijímacího centra (Receiving centre transceiver) |
| SAS | Systémy přivolání pomoci |
| SIE | Systémy inteligentní elektroinstalace |
| SMS | Short message service – krátká textová zpráva |
| SOP | Standardní operační postup |

| | |
|---|---|
| SPT | Komunikátor ve střeženém prostoru (Supervised premises transceiver) |
| SW | Software |
| TP HZS | Technické podmínky HZS |
| TTY | Proudová smyčka (TeleTYpewriter) |
| VSS | Dohledové videosystémy |
| WAN | Rozsáhlá síť (Wide Area Network) |
| ZDP | Zařízení dálkového přenosu |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH