Hodnocení účinnosti poplachových zabezpečovacích systémů

Evaluation of Effectiveness of Security Alarm Systems

Bc. Jan Jež

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Jež**
Osobní číslo:	**A12654**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Hodnocení účinnosti poplachových zabezpečovacích systémů**
Téma anglicky:	**An Evaluation of the Effectiveness of Security Alarm Systems**

Zásady pro vypracování:

1. **Analyzujte systémové požadavky na prvky poplachových zabezpečovacích systémů.**
2. **Popište funkční požadavky na prvky poplachových zabezpečovacích systémů.**
3. **Navrhněte hodnotící kriteria posouzení účinnosti poplachových zabezpečovacích systémů.**
4. **Zpracujte návrh metody hodnocení účinnosti poplachových zabezpečovacích systémů.**
5. **Na modelovém objektu aplikujte navrženou metodu hodnocení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.**
2. **VALOUCH, Jan. Projektování integrovaných systémů. [skriptum]. Zlín: UTB, 2013. ISBN 978-80-7454-296-1 152 s.**
3. **LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.**
4. **LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.**
5. **LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4.**
6. **LOVEČEK, Tomáš. REITŠPÍS, Josef. Projektovanie a hodnotenie sytémov ochrany objektov. Žilina: EDIS – vydavateľstvo ŽU, 2011. 281 s. ISBN 978-80-554-0457-8.**

Vedoucí diplomové práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce řeší problematiku hodnocení účinnosti poplachových zabezpečovacích systémů. Teoretická část obsahuje analýzu systémových a funkčních požadavků v souladu s relevantními aplikačními normami v oblasti poplachových zabezpečovacích systémů. Praktická část obsahuje návrh hodnotících kritérii a návrh metody pro potřebu posouzení účinnosti poplachových zabezpečovacích systémů. Uvedené výstupy jsou doplněny o aplikaci navržené metody na modelovém objektu.

Klíčová slova: poplachový zabezpečovací a tísňový systém, hodnocení, účinnost, návrh, kritéria, aplikační norma

ABSTRACT

This thesis addresses the issue of evaluating the effectiveness of security alarm systems. The theoretical part contains an analysis of system and functional requirements in accordance with the relevant application standards in security alarm systems. The practical part contains a draft proposal evaluation criteria and methods for the purpose of evaluating the effectiveness of security alarm systems. The outputs are complemented by the application of the proposed method on a model object.

Keywords: Intrusion and hold system, evaluation, efficiency, design criteria, application standard

Poděkování

Rád bych poděkoval vedoucímu mé dipoomové práce Ing. Janu Valouchovi Ph.D, který mě směroval a pomohl mi při tvorbě této práce.

Rád bych také poděkoval vedoucímu zkušebny Ing. Milanu Zedníkovi z organizace, která mi poskytla materiáli k této diplomové práci.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské 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/bakalářskou 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/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské 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/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské 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 ……

podpis diplomanta

OBSAH

ÚVOD

V současné době působí na trhu mnoho firem, které se zabývají bezpečností a k ní poskytují služby i výrobky v dané oblasti. Pro zákazníka, který není v oblasti přímo znalý je velký problém výběru dodavatele bezpečnostního systému. Nabídky, ohromné spousty firem lákají své zákazníky ve svých reklamách na ucelená portfolia, kde nabízejí bezpečnostní posouzení současného stavu bezpečnosti u zákazníka, tak i analýzy rizika a zjištění možných důsledků ohrožení majetku, lidi i životního prostředí. Dále pak nabízí samotné zpracování analýz a vypracování projektu na bezpečnost v souladu s legislativou a standardy v daném oboru, jednotlivé komponenty bezpečnosti (např. bezpečnostní zámky, magnetické závory, hlásiče kouře, bezpečnostní folie), samostatné subsystémy bezpečnosti (např. přístupový systém, kamerový systém), tak i kompletní integrované systémy, které v sobě mají jednotlivé subsystémy a jsou centrálně ovládané přes ústřednu v místě zákazníka, nebo vzdáleně na dohledovém poplachovém přijímacím centru (DPPC). K těmto službám pak mohou dále nabízet i zásah zásahového výjezdu, servis daného systému, školení zaměstnanců.

Tato práce by měla pomoci při rozhodování o výběru některého z možných bezpečnostních systémů, které jsou v současné době na trhu. Hodnocení a účinnost bezpečnostních a poplachových systémů je specifická oblast, kde se hodnotí možné nedostatky systému, které je potřebné zlepšit, tak aby nebyl ohrožen ochranný zájem. Ukazuje také na ochranná opatření, která jsou po hodnocení shledána jako dostačující a vyhovují současnému stavu bezpečnosti z hlediska ochranného zájmu zákazníka. Zákazník sám pak může posoudit, která bezpečnostní opatření potřebují v jeho zájmu zvýšit a zlepšit, a která bezpečnostní opatření jsou dostačující a nepotřebují tak další finanční krytí.

Cílem této práce je vyhodnocení účinnost poplachového bezpečnostního systému objektu.

V praktické části je řešen projekt bezpečnostního poplachového systému navrženého pro objekt zkušebny výrobku firmy, kdy projekt je řešen v nových prostorech a je potřeba zhodnotit i posoudit kvalitu jeho návrhu s účinností systému.

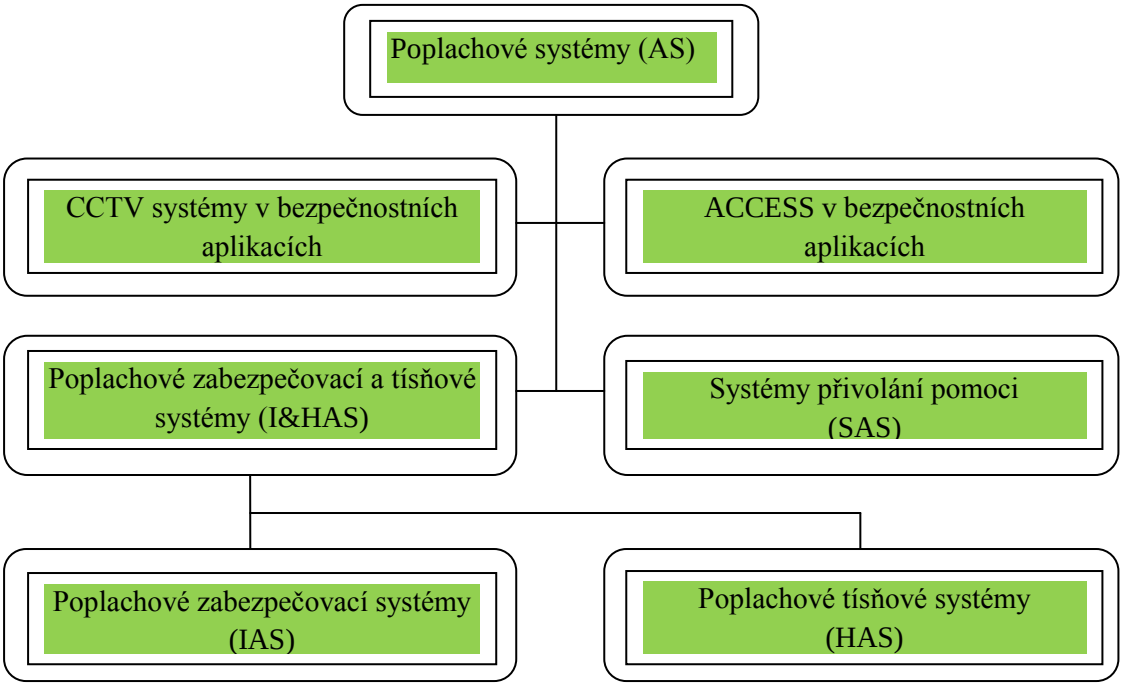
Hodnocení účinnosti systému je činnost, která v sobě zahrnuje minulost (historické souvislosti bezpečnosti), přítomnost (současná bezpečnost) i budoucnost (pravděpodobnost možných bezpečnostních událostí).

Technické normy v oblasti PZTS se ale problematikou hodnocení účinnosti bezpečnostních systémů nezabývají a ani jí neřeší.

I. TEORETICKÁ ČÁST

1 POPLACHOVÉ ZABEZPEČOVACÍ SYSTÉMY

Systémy určené k detekci a signalizaci přítomnosti, vniknutí nebo pokusu o vniknutí narušitele nebo lupiče do střežených prostor. Vydáním nové technické normy ČSN EN 50131-1 (10/2006) byly k poplachovým zabezpečovacím systémům zařazeny i poplachové tísňové systémy (HAS – hold-up alarm systém).[1] Systémy poskytující uživateli možnost úmyslného vyvolání poplachového stavu. Oba systémy se spadají do zabezpečovacích technologií s označením I&HAS = (PZTS) – Poplachové zabezpečovací a tísňové systémy, kde základní technologie vycházejí z platných technických norem, zejména ČSN EN 50131-1(2007) [3] a ČSN CLC/TS 50131-7(2011).[4] Obrázek pod, znázorňuje hierarchii poplachových systémů.



Obr. 1. Klasifikace poplachových systémů

(Zdroj[1]

1.1 Systémové požadavky na poplachové zabezpečovací systémy

Systémové požadavky popisují požadované vlastnosti jako celku. Nejsou tedy specifikovány technologie. Veškeré požadavky jsou stanoveny jako minimální a v rámci návrhu systému je zapotřebí vzít v úvahu:

- charakter objektu
- míru rizika
- nebezpečí pro uživatele a další osoby v objektu[1]

Základní přehled oblastí systémových požadavků

1. Funkce systému
2. Komponenty systému
3. Stupeň zabezpečení
4. Třída prostředí
5. Funkční požadavky
6. Napájení
7. Provozní spolehlivost
8. Funkční spolehlivost
9. Požadavky na prostředí
10. Elektrická bezpečnost
11. Dokumentace
12. Identifikace[1]

1.1.1 Funkce systému

PZTS musí obsahovat následující povinné funkce:

- detekci vniknutí (jako reakce na stav detekující přítomnost nebezpečí),
- a/ nebo aktivaci tísňových prostředků,
- zpracování informací,
- vyhlášení poplachu,
- prostředky k ovládání PZTS.

Další nepovinné funkce (nespecifikované v normě) nesmí negativně ovlivnit funkce povinné. [1]

1.1.2 Komponenty systému

- komponenty PZTS musí být klasifikovány v souladu s jejich odolností vůči

prostředí,

- musí být děleny dle jejich provedení do stupňů zabezpečení,
- v rámci systému musí být komponenty kompatibilní,
- integraci dalších aplikací do PZTS je možná pouze za předpokladu, že tato

negativně neovlivní vlastnosti komponent PZTS. [1]

1.1.3 Stupně zabezpečení

Poplachovému zabezpečovacímu a tísňovému systému musí být přiřazen stupeň zabezpečení, určující jeho provedení, přičemž stupeň zabezpečení systému (subsystému) odpovídá prvku s nejnižším stupněm zabezpečení. [1]

1.1.4 Třída prostředí

V závislosti na předpokládaném místě instalace musí být jednotlivé komponenty PZTS použitelné v jedné z definovaných tříd prostředí I-IV a musí správně pracovat, jsou-li vystaveny stanoveným vlivům. [1]

1.1.5 Funkční požadavky

Funkce systému - I&HAS musí v souladu s jeho konfigurací obsahovat funkce specifikované v normě ČSN EN 50131-1 ed. 2 pro detekci vniknutí a/nebo aktivaci tísňových prostředků, zpracování informací, vyhlášení poplachu – sabotáž a prostředky k ovládání I&HAS.

Vedle povinných funkcí, specifikovaných v normě ČSN EN 50131-1 ed. 2 mohou být v I&HAS obsaženy další funkce za předpokladu, že negativně neovlivní povinné funkce. [3]

Jedním z funkčních požadavků systémů I&HAS je existence rozpoznání poruchy. Poruchový signál nebo zpráva musí být generovány, trvá-li porucha po požadovanou dobu. Doba trvání musí být dostatečně pro uskutečnění komunikace. Specifikace rozpoznání poruchových stavů pro bezpečnostní poplachové a tísňové systémy je uvedena v tabulce pod tímto textem.

Tab. 1. Klasifikace poruchy (Zdroj [3])

Poruchy	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Detektory		P	P	P
Tísňové prostředky	P	P	P	P
Základní napájecí zdroj	P	P	P	P
Náhradní napájecí zdroj	P	P	P	P
Propojení	P	P	P	P
Poplachový přenosový systém	P	P	P	P
Výstražné zřízení	P	P	P	P
Ostatní poruchy	V	V	V	V
Klíč: P= povinné V= volitelné Poznámka – Požadavek na to, aby I&HAS rozeznal poruchy detektoru, tísňového prostředku, poplachového přenosového systému a výstražného zařízení neznamená požadavek specifického poruchového výstupu, například rozpoznání poruchy výstražného zařízení může být odvozeno od poruchy periodické komunikace.				

Je-li u systému I&HAS v závislosti na jeho stupni a volbě varianty přenosu vice než jeden přenosový systém, musí být rozpoznaná porucha každého z nich.

1.1.6 Napájení - napájecí zdroj (power supply)

Základní napájecí zdroj (prime power supply), zdroj napájení PZTS za normálních provozních podmínek. Náhradní napájecí zdroj (alternative power supply), zdroj napájení PZTS schopný napájet systém v případě výpadku základního zdroje po předem stanovenou dobu.

Typy napájení:

Typ A: Energie je dodávána z vnějšího zdroje (např. sítě) a v případě jeho výpadku se energie dodávána z dobíjecího náhradního zdroje (akumulátor), který má automaticky dobíjet z vnějšího zdroje energie.

Typ B: Energie je dodávána z vnějšího zdroje (například sítě), a v případě výpadku se energie dodávána z dobíjecího náhradního zdroje (např. lithiové baterie), který nemá automatické dobíjení z vnějšího zdroje energie.

Typ C: Energie je dodávána pouze z náhradního zdroje, který má v tomto případě základní zdroj energie (např. baterie).

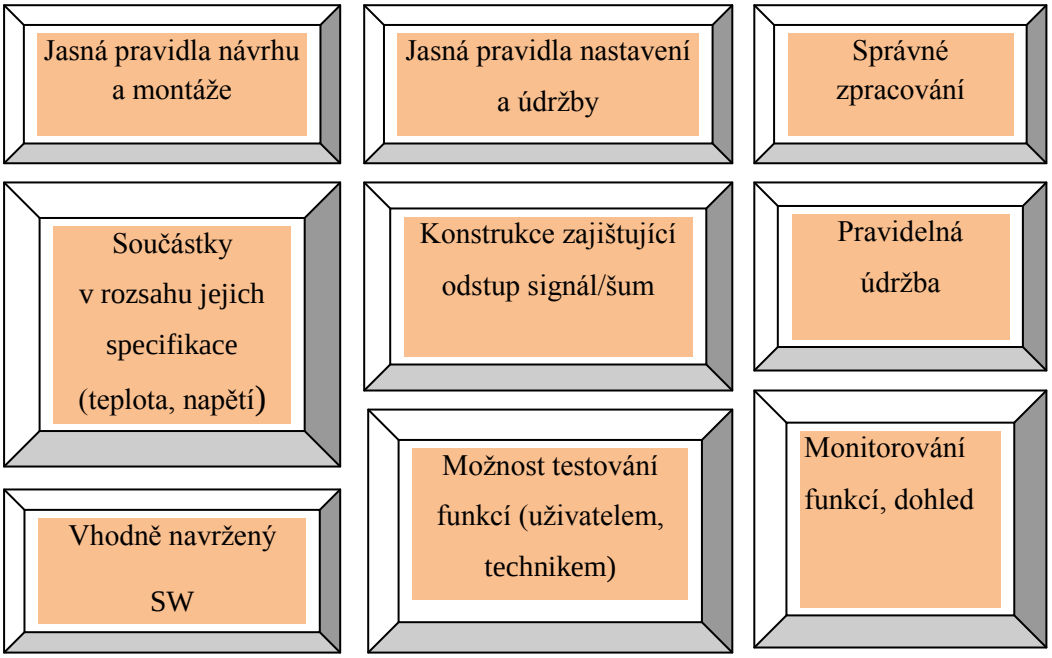
Stanoveny maximální doby dobíjení náhradního napájecího zdroje jsou (72 hodin /pro 1 a 2 stupeň zabezpečení, resp. 24 hodin / pro 3 a 4 stupeň zabezpečení. Dále je stanovena minimální doba napájení náhradním napájecím zdrojem. [1] Tabulka pod specifikuje typy napájení a jejich minimální dobu napájení náhradním zdrojem v jednotlivých stupních zabezpečení.

Tab. 2. Minimální doba napájení náhradním napájecím zdrojem v (hod.) (Zdroj [1])

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Typ A	12	12	60	60
Typ B	24	24	120	120

1.1.7 Funkční spolehlivost

Hlavní zásady zabezpečení funkční spolehlivosti jsou uvedeny v obrázku pod.



Obr. 2. Hlavní zásady funkční spolehlivosti PZTS
zdroj[1]

1.1.8 Provozní spolehlivost

Nutnost aplikace prostředků zajišťujících vyloučení nebo indikaci chyb obsluhy.

Komponenty PZTS musí být jasně a logicky označeny za účelem minimalizace nesprávných činností. [1]

1.1.9 Požadavky na prostředí

Činnost PZTS nesmí být negativně ovlivněna v případě vystavení vlivům prostředí (teplota, vlhkost, EMI atd.) a nesmí dojít ke změnám stavu nebo poškození komponent. Na komponenty PZTS se mohou vztahovat vybrané zkoušky vlivu prostředí. [1]

Prvek I&HAS musí na základě respektování požadavků EN 60950-1 nebo EN 60065

Vniknutí vody	Oxid siřičitý (znečištěné ovzduší)	Solná mlha (koroze chemickými vlivy)
Uder	Volný pád	Vibrace
EMS	Simulované sluneční záření (tepelné vlivy)	Prachotěsnost

poskytovat ochranu proti úrazu elektrickým proudem a souvisícími.[3]

Tab. 3. Přehled zkoušek vlivu prostředí
zdroj[1]

1.1.10 Dokumentace

Dokumentace ke komponentům musí obsahovat název výrobce (dodavatele), popis zařízení, uvedení technické normy, s níž je deklarována shoda, název certifikačního orgánu, stupeň zabezpečení a třída prostředí.[1]

1.1.11 Dokumentace poplachového zabezpečovacího a tísňového systému

Dokumentace vztahující se k I&HAS musí být stručná, kompletní a jednoznačná. Musí být k dispozici dostatečné informace pro montáž, uvedení do provozu, provoz a údržbu I&HAS.

Instrukce vztahující se k provozu I&HAS musí být vytvořeny tak, aby byla minimalizována možnost chybné obsluhy a členěny tak, aby odpovídaly přístupovým úrovním uživatelů. [3]

1.1.12 Identifikace

Na veškerých komponentech I&HAS musí být uveden název, výrobce, typ, datum výroby nebo dodávky, stupeň zabezpečení a třída prostředí.

Veškeré komponenty I&HAS musí být označeny následovně:

- název výrobce nebo dodavatele
- typ
- datum výroby nebo číslo dávky nebo sériové číslo
- stupeň zabezpečení
- třídu zabezpečení

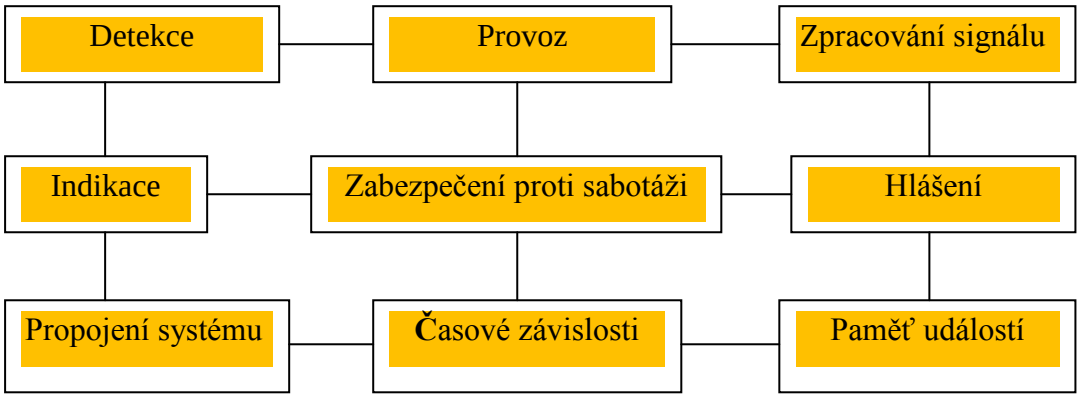
Značení musí být čitelné, stále a jednoznačné. Pokud je na komponentu I&HAS nedostatek místa pro označení, je možno použití kódů s tím, že jsou tyto kódy popsány v přiložené dokumentaci komponentů. Není-li dostatek místa pro kódy, musí mít komponent identifikační znak, který odkazuje na dokumentaci. [3]

Dílčí závěr

Dnešní bezpečnostní situace a vývoj v průmyslu komerční bezpečnosti klade vyšší a vyšší nároky na bezpečnostní systémy a jejich systémové požadavky. Systémové požadavky popisují požadované vlastnosti systému jako celku. Požadavky na systém se mění charakterem objektu, mírou rizika nebo nebezpečím pro uživatele a další osoby v objektu.
Jednotlivé funkce systému musí proto splňovat základní požadavky a to na elektrickou bezpečnost, provozní spolehlivost, stupeň zabezpečení, požadavky na prostředí v jakém má systém pracovat a i na dalších požadavcích specifikovaných v norme ČSN EN 50131-1 ed. 2 pro systémy I&HAS (PZTS).
Vzrůstající nároky na systémy se promítají i na vyšší nároky na dokumentaci těchto systémů a identifikaci komponentů. Závěrem se dá říc, že systémové požadavky určují charakteristiku systému.

2 FUNKČNÍ POŽADAVKY NA PRVKY POPLACHOVÝCH ZABEZPEČOVACÍCH SYSTÉMŮ

Funkční požadavky na I&HAS zahrnují níže uvedené oblasti, ve kterých jsou dále stanoveny podrobné požadavky v závislosti na stupni zabezpečení.



Obr. 3. Klasifikace funkčních požadavků na PZTS
(Zdroj [1])

2.1 Detekce

Detekce je odhalení bezpečnostního rizika v daném čase a umožnuje na riziko reagovat at již formou servisu při poruše funkce systému nebo při samotném fyzickém napadení narušitelem ochranného zájmu či sabotáže.

2.1.1 Detekce vniknutí

I&HAS musí v souladu s konfigurací obsahovat prostředky pro detekci vniknutí, aktivace tísňových prostředků, sabotáž a rozpoznání poruch, nutných pro splnění požadavků normy. Detektory musí být vhodné pro prostředí a předpokládané použití a mohou obsahovat více než jednu technologii. Detektory musí být konstruovány a instalovány tak, aby byla maximalizována detekce skutečného vniknutí a minimalizováno riziko planých poplachů. Signál nebo zpráva o vniknutí musí být generována od aktivace detektoru po požadovanou dobu trvání. Tato doba musí postačovat k uskutečnění komunikace. [3]

2.1.2 Detekce sabotáže

Všechny komponenty I&HAS musí zajišťovat detekci sabotáže, jak je specifikováno v tabulce 5. Signál nebo zpráva o sabotáži musí být generována, trvala-li aktivace sabotážního prvku požadovanou dobu. Tato doba musí postačovat k uskutečnění komunikace. [3]

2.1.3 Rozpoznání poruch

V závislosti na stupni I&HAS musí existovat prostředky k rozpoznání poruchových stavů specifikovaných v tabulce 4. Poruchový signál nebo zpráva musí být generovány, trvá-li porucha po požadovanou dobu. Doba trvání musí být dostatečná pro uskutečnění komunikace. [3]

Tab. 4. Klasifikace poruchy
(Zdroj [3])

Poruchy	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Detektor	P	P	P	P
Základní napájecí zdroj	P	P	P	P
Náhradní napájecí zdroj	P	P	P	P
Propojení	P	P	P	P
Poplachový přenosový	P	P	P	P

systém				
Výstražné zařízení	P	P	P	P
Ostatní poruchy	V	V	V	V
Tísňové prostředky	P	P	P	P

Klíč: P = povinné; V = volitelné

Poznámka – Požadavek na to, aby I&HAS rozeznal poruchy detektoru, tísňového prostředku, poplachového přenosového systému a výstražného zařízení nezaznamená požadavek specifického poruchového výstupu např. rozpoznání poruchy výstražného zařízení může být odvozeno od poruchy periodické komunikace.

Je-li u systému I&HAS v závislosti na jeho stupni a volbě varianty přenosu více než jeden přenosový systém musí být rozpoznána porucha každého z nich.

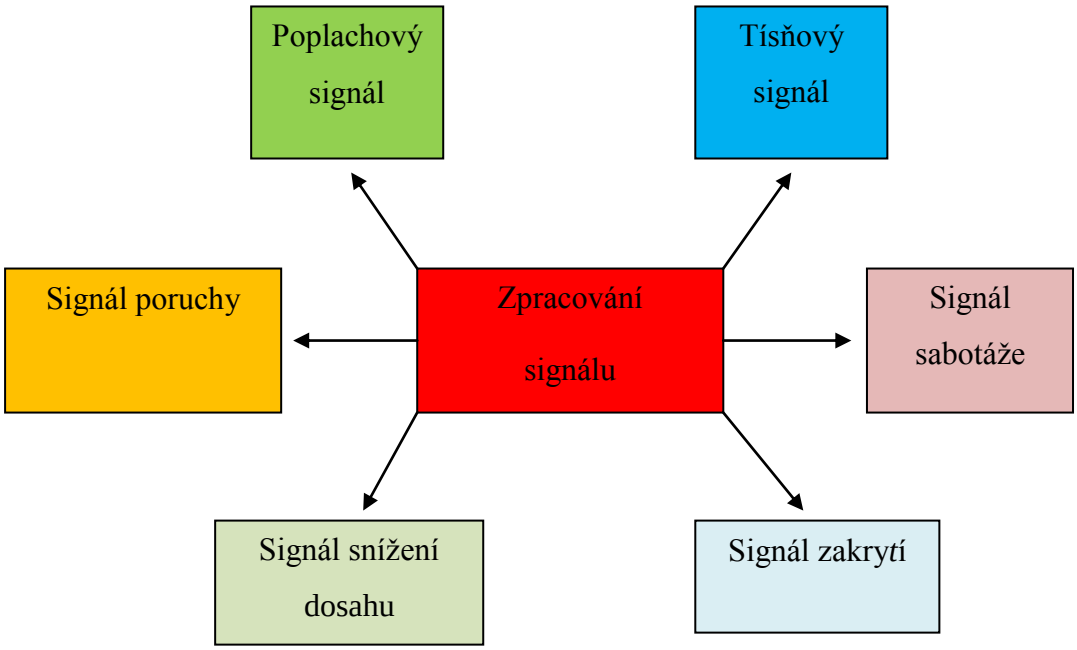
2.1.4 **Tísňový prostředek**

I&HAS musí, je-li to žádoucí, obsahovat tísňové prostředky, vhodné pro dané prostředí a aplikaci. Tísňové prostředky musí obsahovat opatření pro snížení rizika náhodného spuštění. Signál nebo zpráva tísňového poplachu musí být generována, je-li tísňový prostředek v aktivním stavu po požadovanou dobu. Tato doba musí postačovat k uskutečnění komunikace. [3]

Poplachové zabezpečovací a tísňové systémy lze dále dělit na poplachové zabezpečovací systémy postrádající funkci detekce tísňového poplachu neboli detekci přepadení a na poplachové tísňové systémy postrádající funkci detekce vniknutí. [1]

2.2 Zpracování signálu a jejich rozlišení (klasifikace signálu v PZTS)

Zpracování signálu nebo zpráv musí být závislé na stavu, typu signálu nebo zprávy a konfiguraci I&HAS. Jednotlivé detektory mohou být logicky uspořádány tak, aby vyžadovaly generování jednoho nebo více poplachových signálů nebo zpráv z jednoho nebo více detektorů, než dojde ke generování stavu poplachu vniknutí. [3]



Obr. 4. Klasifikace signálu v PZTS [1]

2.3 Indikace

Představuje v rámci systémových požadavků přehled (výčet) jednotlivých stavů povinně/ volitelně indikovaný systémem dle stupně zabezpečení. Není - li možná současná indikace více povinně indikovaných stavů, musí systém zabezpečit sdělení - upozornění na čekající informaci. Veškeré povinné indikace musí být umístěny na jedné ústředně nebo doplňkovém zařízení. PZTS musí indikovat např. stavy střežení, klidu, poplachu, blokování, poruchy, sabotáže, indikace vstupu, neukončení činnosti atd. [1]

Není-li možné realizovat současnou indikaci veškerých povinných informací, tj. povinná informace na indikaci čeká, musí být k dispozici indikaci sdělující další indikace, např. indikátor „čekající informace" [3]

Veškeré požadované povinné indikace musí být umístěny společně alespoň na jedné ústředně nebo doplňkovém zařízení. Další indikace mohou být poskytnuty také na jiných místech. Tam kde je v závislosti na stupni I&HAS vyžadován volitelný přenos hlášení více než jedním poplachovým přenosovým systémem, měl by být osobě nastavující stav střežení indikován stav poruchy kteréhokoli poplachového přenosového systému. [3]

Detektory vniknutí s vyhodnocovací funkcí musí mít individuální prostředky indikace poplachového stavu, v souladu se specifikací. Detektory bez vyhodnocovací funkce mohou sdílet společně prostředky indikace. Společnou indikaci nesmí sdílet více než 10 takovýchto detektorů.

2.4 Hlášení

Stav tísně, vniknutí, sabotáže a poruchy musí být hlášeny prostřednictvím ATS (poplachový přenosový systém) a/nebo WD akustickým výstražným zařízením. Jsou stanovovány požadavky na dobu zvukového signálu, na zpoždění a rovněž na kombinace hlášení v závislosti na stupni zabezpečení.[1] I&HAS musí obsahovat prostředky hlášení splňující, v závislosti na stupni zabezpečení. Činnost výstražného zařízení může být potlačena, např. aby nedošlo k jeho činnosti při aktivaci tísňového prostředku. Jestliže I&HAS obsahuje jak poplachový přenosový systém, tak výstražné zařízení, je povoleno zpozdit činnost výstražného zařízení nejvýše o 10 minut. Činnost výstražného zařízení je povoleno zastavit za předpokladu, že je hlášení přeneseno poplachovým přenosovým systémem do ARC nebo jiného přijímacího místa a je tímto ARC nebo jiným přijímacím místem potvrzeno před uplynutím zpoždění.
Dojde-li k detekci poruchy poplachového přenosového systému, musí být jakékoli zpoždění činnosti výstražného zařízení automaticky zrušeno za předpokladu, jsou-li porucha nebo poruchy detekovány ve všech dostupných přenosových trasách. [3]

Akustické výstražné zařízení musí být v činnosti po dobu nejméně 90 sekund, není-li místními nebo národními předpisy vyžadováno kratší trvání. Maximální doba činnosti nesmí být delší než 15 minut, není-li místními nebo národními předpisy vyžadováno trvání kratší. Hlášení poruchy základního napájecího zdroje napájení muže být zpožděno nejvýše o 1 hodinu. Prostředky hlášení mohou být doplněny nepovinnými prostředky za

předpokladu, že takováto zařízení negativní správnou činnost povinných zařízení, např. siréna se sítovým napájením nebo zařízení zhoršující viditelnost (zamlžovací zařízení). [3]

2.5 Zabezpečení proti sabotáži

Komponenty PZTS musí mít prostředky zamezující přístupu k jejich vnitřním součástkám. Prostředky se liší dle stupně zabezpečení, třídy prostředí a dle technického provedení komponentu. Veškeré svorky a prvky elektronického nastavování musí být umístěny uvnitř krytu. Přístup k vnitřním součástem ústředny, detektorů, ovládacích zařízení - vždy pouze s použitím nástroje. V případě umístění doplňkového ovládacího zařízení vně střeženého prostoru - nutnost zabezpečit proti možnosti jeho záměny, a/nebo proti záměně signálů mezi ústřednou a doplňkovým zařízením. Požadavky na ochranu proti sabotáži se mohou lišit podle stupně I&HAS a podle toho, zda je komponent I&HAS umístěn uvnitř nebo vně střeženého prostoru. Komponenty I&HAS, umístěné vně střežených prostorů, musí mít vhodné prostředky pro ochranu proti sabotáži (např. přídavná ovládací zařízení, výstražná zařízení). Všechny prvky mechanického a elektronického nastavování musí být umístěny uvnitř krytu komponentů I&HAS. Kryty musí být dostatečně robustní, aby nemohlo dojít k nezajištěnému přístupu k prvkům, aniž by došlo k viditelnému poškození krytu. Musí být zamezen neoprávněný přístup k vnitřním prvkům detektorů a tísňových prostředků, normální přístup musí vyžadovat použití nástroje. Přístup k prostředkům určeným k orientaci zorného pole detektoru nesmí být přístupné pro neoprávněné osoby. Komponenty I&HAS specifikované v tabulce 12 musí být vybaveny prostředky pro detekci sabotáže. Tabulka 13 specifikuje typy sabotáže, které je třeba detekovat. Detekce sabotáže musí být ve všech stupních zabezpečení účinná ve stavu střežení i klidu. Doplňkové ovládací zařízení určené k instalaci vně střeženého prostoru, musí obsahovat prostředky zamezující změnu tohoto zařízení a/nebo signálu a zpráv mezi doplňkovým ovládacím zařízením a ústřednou. Tento požadavek nemusí být uplatněn, jestliže jakákoli takováto záměna nemůže ovlivnit správnou činnost I&HAS. [3]

Tab. 5. Detekce sabotáže – komponenty na něž se požadavek vztahuje (Zdroj [3])

Komponenty	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Ústředna /doplňkové ovládací zařízení /poplachový přenosový systém /výstražné zařízení /napájecí zdroj	P	P	P	P
Tísňové prostředky / a	V	P	P	P
Detektory vniknutí / b	V	P	P	P
Rozvodné krabice / c	V	V	P	P
Klíč: V= volitelné P= povinné				
a/ Přenosové tísňové prostředky nemusí vyhovovat požadavkům této tabulky b/ Je akceptováno, že může být problematické realizovat detekci sabotáže u mechanicky nebo magneticky aktivovaných spínačů. U některých stupňů zabezpečení však může být nezbytné chránit magneticky aktivované spínače proti sabotáži pomocí vnějšího magnetického nebo elektromagnetického zdroje. c/ Má-li I&HAS ochranu proti záměně signálů nebo zpráv, není třeba u stupňů 1, 2 a 3 opatřovat rozvodné krabice detekcí sabotáže.				

2.6 Propojení systémů

Propojení musí být vhodné pro daný účel a navrženo tak, aby poskytlo spolehlivý prostředek komunikace mezi komponenty I&HAS.[3] Návrh propojení realizujeme z hlediska minimalizace zpoždění, modifikace, záměny nebo ztráty signálu, přičemž je nutné realizovat monitorování propojení (komunikace). Norma stanovuje např. maximální dobu nedostupnosti spojení, intervaly ověřování spojení nebo ověřování po dobu nastavování střežení.[1]

Specifikace maximální přípustné doby, po níž propojení není dostupné udává norma EN 50131-1 ed. 2 pro I&HAS v tabulce 6 níže tohoto textu.

2.6.1 **Monitorování propojení**

Dojde-li k překročení maximální přípustné doby, musí být generován signál sabotáže nebo poruchy. Jestliže u I&HAS stupňů 1 a 2 překročil interval mezi periodickými komunikacemi 100 s, musí být propojovací médium monitorováno pro stanovení jeho schopnosti přenášet signály nebo zprávy.

Tab. 6. Maximální nedostupnost propojení (Zdroj [3])

	Stupeň 1 s	Stupeň 2 s	Stupeň 3 s	Stupeň 4 s
Max. přípustné trvání nedostupnosti	100	100	100	10
Poznámka: shora uvedený požadavek má za cíl monitorováním komunikačního média zjistit, je-li komunikace možná a zajistit, je-li komunikační cesta schopná přenášet signály nebo zprávy. Monitorování může mít formu odposlechu rušení v případě, kdy je používán radiový přenos, nebo jestliže I&HAS sdílí sběrnicový systém s dalšími aplikacemi zjišťováním, zda tyto aplikace nezískaly trvalou kontrolu nad sběrnicí.				

2.6.2 **Integrita propojení**

Musí být periodicky ověřována v intervalech nepřekračujících hodnoty uvedené v Tabulce 7. Není-li komunikace ověřována podle specifikace v Tabulce 7, musí být signály nebo zprávy generovány následovně:

- když komunikace nelze ověřit z důvodu identifikovatelného stavu, musí být generován poruchový signál nebo zpráva
- když komunikace nelze ověřit, ačkoli neexistuje žádný identifikovatelný důvod, musí být generován signál nebo zpráva poruchy nebo sabotáže. [3]

Tab. 7. Intervaly ověřování (Zdroj [3])

	Stupeň 1 min	Stupeň 2 min	Stupeň 3 min	Stupeň 4 min
Minimální přístupný interval mezi signály nebo zprávami periodické komunikace	240	120	100	10

Tab. 8. Maximální interval od posledního signálu nebo zprávy (Zdroj[3])

	Stupeň 1 min	Stupeň 2 min	Stupeň 3 min	Stupeň 4 min
Maximální přístupný interval od přijetí posledního signálu nebo zprávy	60	20	60	10

2.6.3 **Bezpečnost komunikace**

I&HAS stupně 4 musí obsahovat prostředky k detekci zpoždění, modifikace, záměny nebo ztráty jakýchkoli signálů nebo zprávy, jak je specifikováno v tabulce 8. Maximální přípustná doba pro detekci zpoždění, modifikace, záměny nebo ztráty jakéhokoli signálu nebo zprávy nesmí překročit hodnoty uvedené v tabulce 7 plus 10 s.

Tab. 9. Bezpečnost signálů a zprávy (Zdroj[3])

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Zpoždění, modifikace, záměna nebo ztráta signálu nebo zpráv	V	V	V	P
Klíč: V= Volitelný P= Povinný				

Bylo-li detekováno zpoždění, modifikace, záměny nebo ztráty jakéhokoli signálu nebo zprávy, musí být generován signál nebo zpráva poruchy nebo sabotáže, jak je uvedené v tabulce 9.

Tab. 10. Generované signály nebo zprávy(Zdroj [3])

Požadavky	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
	Signál nebo zpráva	Signál nebo zpráva	Signál nebo zpráva	Signál nebo zpráva
Monitorování propojení (2.6.1)	S nebo P	S nebo P	S	S
Periodická komunikace (2.6.2)	p	P	P	P
Periodická komunikace (2.6.2)	S nebo P	S nebo P	S	S
Bezpečnostní komunikace (2.6.3)	S nebo P	S nebo P	S	S
Klíč: S= sabotáž P= Porucha Generování signálu nebo zpráv je vyžadováno pouze je-li povinné podle článku				

2.7 Časové závislosti

Jsou stanoveny požadavky na signály detekce vniknutí, sabotáže, aktivace tísňového prostředku a rozpoznání poruch z hlediska minimální délky signálu, který musí být zpracován (400ms), maximální doby do které musí být signály vyhlášeny (10 s). Poruchové signály musí být zpracovány, trvají-li déle než 10 s.[1]

2.8 Paměť událostí

V závislosti stupni zabezpečení musí I&HAS zaznamenávat specifikované události. Záznamové prostředky musí být chráněny proti náhodnému nebo úmyslnému zmazání. U I&HAS 2,3 a 4 stupně zabezpečení jsou údaje doplněny datem a časem, kdy událost nastaly. Záznamové prostředky mohou být součásti I&HAS nebo PPC. [1] I&HAS 2,3 a 4

musí mít prostředky pro uložení událostí čekajících na přenos. Prostředky uložení ve vzdáleném místě musí splňovat požadavky tabulky 11. [3]

Tab. 11. Záznam událostí – kapacita paměti (Zdroj[3])

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Kapacitní paměť – min. počet událostí	V	250 událostí	500 událostí	1000 událostí
Min. trvanlivost paměti po výpadku napájení I&HAS	V	30 dní	30 dní	30 dní
Klíč: V= Volitelné				

Ve stupních 3 a 4 musí být zajištěna schopnost průběžného záznamu událostí. Tato schopnost nemusí obsahovat prostředky produkující trvalý záznam. Počet událostí z jakéhokoli zdroje musí být omezen na nejméně 3 a maximálně 10 během jakéhokoli období ve stavu střežení nebo klidu.[3]

Dílčí závěr

Všechny funkční požadavky, které jsou zahrnuty v této kapitole značí, co musí tyto bezpečnostní systémy z funkčních požadavků splňovat, tak aby byla zaručena bezpečnost osob, objektů i majetku na různých bezpečnostních stupních zabezpečení. Projekt bezpečnostního systému musí být navržen tak, aby plnil funkce z hlediska legislativních standardů, tak i funkce a požadavky na systém ze strany zadavatele (uživatele). Legislativní standardy určují limity, kterých se realizace a provoz bezpečnostních poplachových systémů musí držet a které dávají rámec jejich správné funkce.
Mírou funkční bezpečnosti je podle ČSN EN 50131-1ed.2 tzv. integrita bezpečnosti neboli pravděpodobnost, s jakou bude bezpečnostní (nebo řídicí) systém uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu.

II. PRAKTICKÁ ČÁST

3 HODNOTÍCÍ KRITERIA A POSOUZENÍ ÚČINNOSTI POPLACHOVÝCH ZABEZPEČOVACÍCH SYSTÉMŮ

Účinností a efektivností bezpečnostního systému lze určit celkovou úroveň ochrany zabezpečovaného objektu. Záměrem každého subjektu by mělo být přijímání takových ochranných opatření, která sníží velikost rizika na hodnotu nižší, případně rovnu hodnotě akceptovatelného rizika. Jinak řečeno je potřebné přijmout taková bezpečnostní opatření, která sníží celkovou zranitelnost systému na úroveň, která je v daných podmínkách realizovatelná a kterou si může subjekt dovolit financovat. Zranitelnost zahrnuje slabá místa ve fyzické, technické či procesní ochraně, která mohou být zdrojem bezpečnostního rizika a způsobit nepříznivé následky při ochraně ochranného zájmu. [7]

Zranitelnost bezpečnostního systému se dá rozdělit na:

- fyzická zranitelnost (např. okna, dveře, ventilační šachty, kanalizace, tunely, parkovací prostory, přístupové cesty, brány, oplocení, stavební konstrukce, zámky)
- technická zranitelnost (např. telefonní linky, elektroinstalace objektu, akustické vybavení),
- operační zranitelnost (např. lidský faktor).[8]

Zranitelnost je nepřímo úměrná od existujících anebo plánovaných bezpečnostních opatření, patřících do oblasti situační prevence. Situační prevence prostřednictvím mechanické, technické, fyzické a režimové ochrany stěžuje potenciálnímu narušitelovi spáchat trestný čin a zároveň zvyšuje pravděpodobnost jeho odhalení a zadržení. [5]

Hodnocení bezpečnosti lze provést v závislosti od typu bezpečnostních opatření, které používá metody hodnocení systémů a jeho úrovně / stupně ochrany. Navržená kritéria se liší vzhledem posuzované oblasti bezpečnostních opatření.

3.1 Kritéria pro fyzickou ochranu

Fyzická ochrana z hlediska bezpečnosti poplachového systému se může posuzovat na základě technické vybavenosti zásahové jednotky, testu fyzické zdatnosti ostrahy, psychologických testů, osobních prověrek členů jednotky a schopnosti narušitele dosáhnout svého záměru. [9]

Posouzení technické vybavenosti pro zásahovou jednotku je možné a to na základě technického výbavení v poměru vyšší účinnosti zásahu proti narušiteli. Kritéria pro stanovení technické vybavenosti zásahové jednotky lze posuzovat na základě expertního posouzení. **Č**ím vyšší hodnocení jednotlivá vybavení dosáhnou, tím vyšší účinnost zásahu může zásahová jednotka dosáhnout.

Tab. 12. Posouzení vybavenosti zásahové jednotky

Kritérium	Expert A	Expert B	Expert C	Expert D	Hodnocení
Detektory perimetrcké ochrany	Dobré	Dobré	Dobré	Vyhovující	10
Radiové spojení	Vyhovující	Dobré	Dobré	Nevyhovující	7
Mobilita přesunu jednotky	Výborná	Dobrá	Vyhovující	Dobrá	11
Popis: Výborná = 4, Dobrá = 3, Dostatečná = 2, Vyhovující = 1, Nevyhovující = 0					

3.2 Kritéria pro režimovo-organizační opatření

Návrh kritérií pro režimovo-organizační opatření lze posuzovat podle adresného rozdělení zodpovědnosti a pravomocí jednotlivých osob. K tomuto hodnocení můžeme použít

kritéria, která budou hodnotit oprávněnost změny v režimu zabezpečení. Opět lze účinnost systému posuzovat podle kriterií hodnocených expertní skupinou.

Tab. 13. Rozdělení kritérií z hlediska režimovo-organizačních opatření.

Kritérium	Expert A	Expert B	Expert C	Hodnocení
Kibernetická bezpečnost	3	3	2	8
Kriminalita	3	4	3	10
Sabotáž	1	2	1	4
Požární ochrana	4	3	3	10
Popis: Vyhovující = 1, Dostatečná = 2, Nevyhovující = 3, Nedostatečná = 4				

V tabulce je součet hodnot přiřazený experty. Výsledkem jsou pak hodnoty sečtených bodů které udávají, že bezpečnostní opatření v kritériu kriminalita a požární ochrana jsou nedostatečná a mají proto nejvyšší riziko ohrožení. Zatím co bezpečnostní opatření vůči sabotáži jsou vyhovující a skýtají dostatečnou ochranu.

3.3 Kritéria účinnost aktivních a pasivních prvků

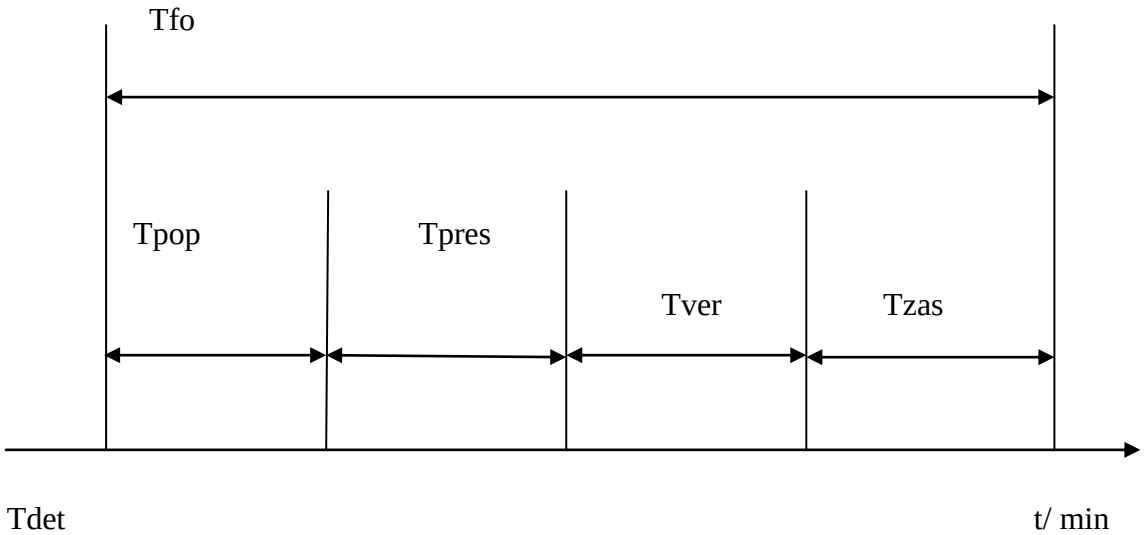
Účinnost systému ochrany objektů je možné vyjádřit jako vztah mezi celkovým časem napadení narušitele a to od času jeho první detekce aktivními prvky ochrany, až po jeho únik ze střeženého prostoru, nebo celkového času prolomení pasivních prvků ochrany v poměru s celkovým časem zásahu zásahové jednotky. Výsledek je pak koeficient účinnosti hodnoceného systému. Kritériem je pak schopnost dopadení narušitele zásahovou jednotkou, nebo aspon jeho zastavení v dalším postupu k ochrnému zájmu.

3.3.1 Detekce vniknutí pomocí aktivních prvků

V případě detekce narušitele pomocí aktivních prvků ochrany, je možné koeficient účinnosti ochranných opatření Qochr definovat pomocí vztahu.

$$Qochr = \frac{Tn}{Tfo} = \frac{Tp + TPRES + Tút + Tn}{Tpop + Tver + Tpres + Tzás} \; pro \; Tn > Tfo \tag{5}$$

$$Qochr = \frac{Tprl}{Tfo} = \frac{Tp + TPRES}{Tpop + Tver + Tpres + Tzás} \; pro \; Tprl > Tfo \tag{5}$$



Obr. 5. Grafické znázornění struktury času fyzické ostrahy Tfo v případě detekce pomocí aktivních prvků (Zdroj [9])

Z hlediska výsledku hodnot tohoto vztahu v bezpečnosti ochrany je pravděpodobnost, že narušitel je detekován všemy aktivními prvky ochrany (PIR detektory) během cesty k ochrnnému zájmu. Hodnota koeficientu je v 1-100%.

V případě detekce narušitele pomocí aktivních prvků ochrany je čas reakce výkonné jednotky Tfo interpretované podle časového grafu (obrázek 5).

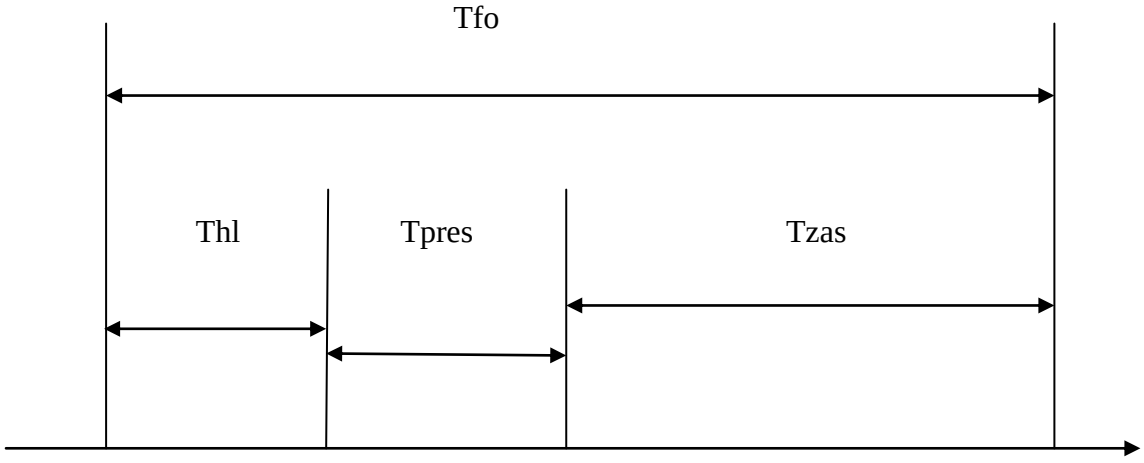
3.3.2 Detekce vniknutí pomocí fyzické ochrany

V případě detekce narušitele pomocí fyzické ochrany je možné koeficient účinnosti ochranných opatření (Qochr) definovat pomocí vztahu.

Detekci narušitele pomocí fyzické ochrany je možné koeficient účinnosti ochranných opatření (Qochr) definovat pomocí vztahu.

$$Qochr = \frac{Tn}{Tfo} = \frac{Tp + TPRES + Tút + Tún}{Thl + Tpres + Tzás} \; pro \; Tn > Tfo \tag{5}$$

$$Qochr = \frac{Tprl}{Tfo} = \frac{Tp + TPRES}{Thl + Tpres + Tzás} \; pro \; Tprl > Tfo \tag{5}$$



Obr. 6. Grafické znázornění struktury času Tfo v případě detekce pomocí fyzické ochrany (Zdroj [9])

Tento vztah v případě účinnosti bezpečnostního systému udává udává koeficient pravděpodobnosti, že zásahová jednotka po správném vyhodnocení napadení objektu narušitelem v ochranném zájmu zadrží narušitele nebo mu znemožní další postup k ochrnnému zájmu. Koeficient se vyjadřuje od 0 výše a uvádí účinnost ochranných

opatření. Pokud by byl koeficient < 1 jsou ochranná opatření bezpečnosti neúčinná a je potřeba ochrnná opatření zvýšit. Pokud je koeficient > 1, je účinnost opatření v rozsahu akceptování bezpečnosti. Či-li, čím je koeficient vyšší, tím je účinnoet ochrnnách opatření také vyšší (účinnost by se měla pohybovat v rozmezí 6 až 12). [9]

Tfo – je celkový čas reakce zásahové jednotky

Skládá se z: Čas vyhlášení poplachu Tpop, času který uplynul od momentu detekce narušitele Tdet, až po vyhlášení poplachového stavu. Čas vyhlášení poplachu Tpop zahrnuje

- čas, který je přednastavený na případné uvedení systému zástavu zastřežení do stavu odstřežení – max. 45s, pokud vznikne poplachový stav v čase tohoto procesu, musí být signalizovaný jen autonomně a až po době 30s může být přenesen přes PPS.
- čas, který je potřebný na uvedení poplachového systému do stavu zastřežení, po opětovném dosažení jmenovité hodnoty napájení po jeho výpadku pro EPS max. 180s
- čas potřebný na změnu poplachového systému ze stavu zastřežení do poplachového stavu
- přenosový čas, který je potřebný pro přenos signálu/ zprávy na stanoviště stálého výkonu služby fyzické ochrany v střeženém prostoru, přenosový čas je úsek od okamžiku, kdy se objeví změna stavu poplachového systému na rozhraní jeho komunikátora a když se objeví změna stavu na rozhraní přenosového poplachového zařízení a indikačního-zobrazovacího zařízení DPPC.

3.3.3 Hodnocení účinnosti bezpečnostního systému

Účinnost je možné vypočítat jako podíl sledované veličiny na výstupu systému k sledované veličině na vstupu systému v stejném časovém intervale. Ideální účinnost je 100%. Za účinný systém bezpečnosti objektů se považuje takový systém, jenž splňuje základní podmínku, a to že čas napadení případně celkový čas prolomení vnitřních a vnějších pasivních prvků ochrany je větší jak čas reakce zásahové jednotky, fyzické ochrany objektu. Systém je účinný pokud, celkový času napadení v poměru s časem zásahu zásahové jednotky je vyší jak jedna. [9] Vztah tohoto poměru je znazorněn pod textem.

Tn > Tfo; Tprl > Tfo (Tn/ Tfo) > 1; Tprl / Tfo > 1 (5)

Celkový čas prolomení pasivních prvků ochrany (Tprl) se skládá z časů prolomení narušitele všech pasivních prvků ochrany Tp předmětových, obvodových, plášťových a to od momentu jeho detekce aktivními prvky ochrany v čase. Důležitý je také časový údaj, který počítá s časem momentu detekce aktivními prvky ochrany při napadnutí narušitele Tdet. Jeden z důvodů proč se výpočet stanový od tohoto času je to, že s určitou pravděpodobností dochází na aktivaci zásahové jednotky. Každý pasivní prvek má svou limitovanou průlomovou odolnost, přičemž prolomení je jen otázka času. K detekci narušitele může dojít vně a nebo před hranicí detekční zóny, v čase prostupu mezi zónami nebo po průniku (vstupu do detekční zóny). V prvním případě se tato hodnota času Tp v rámci celkového času Tprl nemění. V druhém případě je potřeba tento čas vynásobit koeficientem ½ (v případě výpočtu rozptylu náhodné proměnné Tp je potřebné ho vynásobit koeficientem ¼) ve třetím případě je čas rovný 0. To znamená, že průlomová odolnost prvního pasivního prvku se nezapočítává do celkového Tprl.

Na posouzení účinnosti bezpečnostního systému z pohledu pasivních/ aktivních prvků ochrany a prvků fyzické ochrany, je potřebné s výpočtem časů Tprl a Tn stanovit i časy popisující zásah. [5], [10]

Popis:

1. Qochr – koeficient účinnosti ochranných opatření
2. Tn – celkový čas napadení narušitelem od momentu detekce v čase Tdet aktivními prvky ochrany, až po jeho opuštění střeženého prostoru [s]
3. Tprl – celkový čas prolomení pasivních prvků ochrany [s]
4. Tfo – celkový čas reakce zásahové jednotky [s]
5. Tp – čas prolomení všech pasivních prvků ochrany [s]

6. TPRES – celkový čas potřebný na přesun narušitele k ochrannému zájmu a to od momentu jeho detekce aktivními prvky ochrany v čase Tdet [s]
7. Tút – čas útoku narušitele [s]
8. Tún – čas úniku narušitele [s]
9. Tpop – čas vyhlášení poplachu [s]
10. Tver – čas verifikace napadení [s]
11. Tpres – čas přesunu na místo zásahu [s]
12. Tzás – čas zásahu proti narušitelovi [s]
13. Thl – interval mezi dvěma obhlídkami fyzické ostrahy

3.3.4 Kritéria účinnosti detektorů pohybu

Detektor pohybu je v rámci bezpečnostního systému aktivním prvkem ochrany. Čím vyšší počet detektorů je zapojen do systému ochrany, tím vyšší je ochrana chráněnného zájmu. Pokud jsou detektory pohybu zprávně instalovány (pokyny výrobce) a v dostatečném počtu, měly by mít 100% pokrytí chráněnného prostoru. Kritérium je procentuální pokrytí ochraného prostoru.

Tab. 14. Pokrytí chráněného prostoru PIR detektory

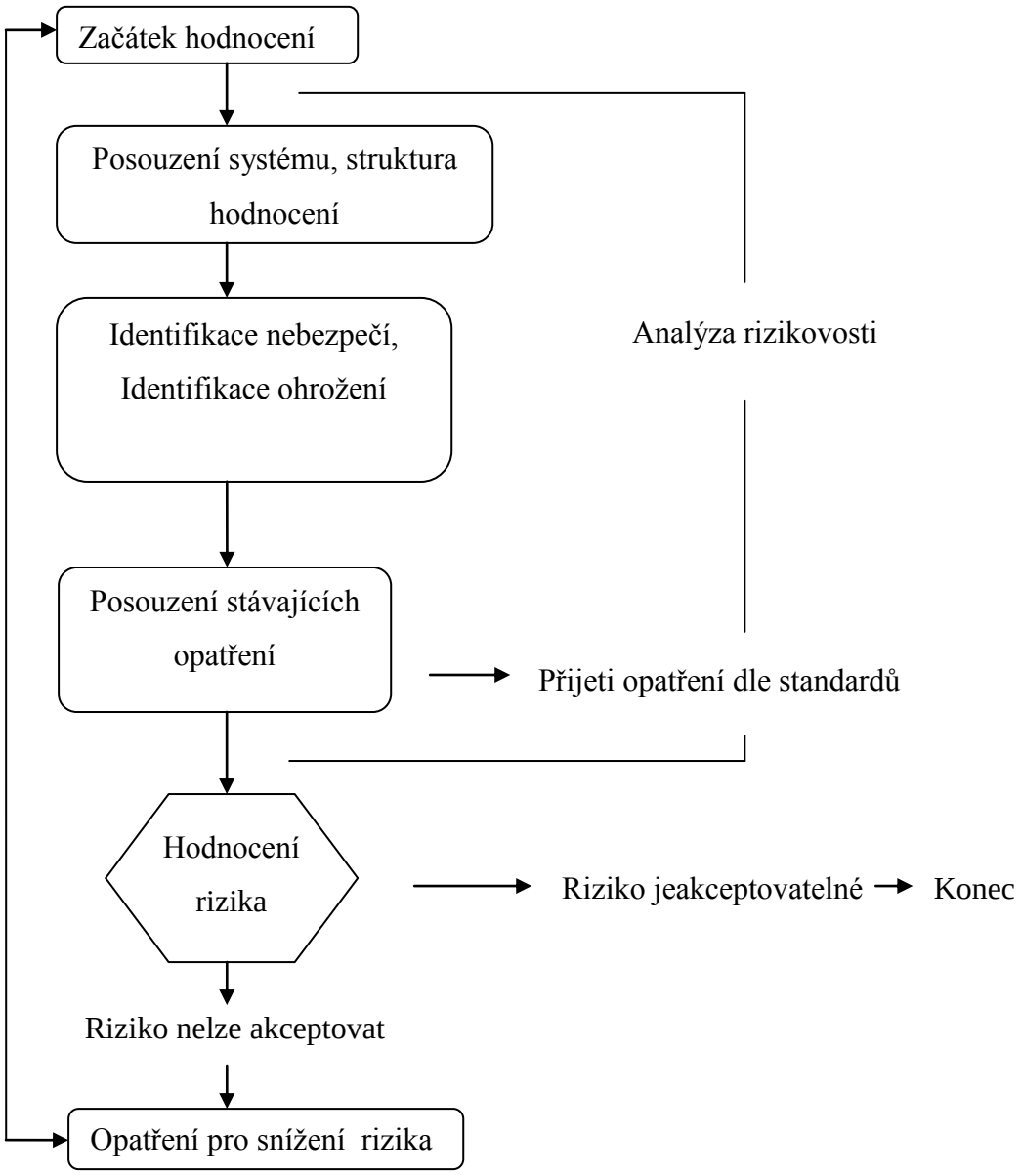
Detektoru (ks)	1	5	6	9	10	11	12
Pokrytí (%)	8,3	41,5	50	74,7	83	91,3	100
Popis: Rozloha objektu = 1200 (m²)							

Dílčí závěr

V této kapitole jsem navrhnul možná kriteria hodnocení bezpečnoatních poplachových systému. Podle definice účinnosti je hodnocení míra odchylky od dosaženého cíle, kterého bychom chtěli dosáhnout. Proto jsem do návrhů kritérií použil expertní hodnocení pro bezpečnost fyzickou i bezpečnost režimovo-organizační. Pro technologickou bezpečnost jsem navrhl kritéria stanovená výpočty koeficientů v poměru časů napadení narušitele a časů zásahu zásahové jednotky. Hodnocení stanovených kritérií je potřebné porovnat se standardy a požadavky pro použité systémy bezpečnosti a z odchylek pak zjistit jejich účinnost a efektivnost.

4 MODELY HODNOCENÍ ÚROVNĚ BEZPEČNOSTI

Pro hodnocení účinnosti bezpečnostního systému je potřebné vytvořit model postavený na požadavcích z hlediska legislativy a funkcí z hlediska provozovatele. Model by měl zahrnovat postup, jak budou získavány informace (vstupy), jaká kritéria budou jednotlivým vstupům přidělena (důležitost informací), jak budou informace dále zpracovány (analýzy), vyhodnocení systému a následná zpětná vazba výsledků hodnocení systému (nová opatření k ochraně zájmu).



Obr. 7. Schéma hodnocení účinnosti bezpečnostních opatření

4.1 Posouzení systému

Cílem bezpečnostní posouzení je nalézt bezpečnostní faktory mající vliv na volbu komponentů (aktivní a pasivní prvky), jejich umístění a stanovení požadovaného stupně zabezpečení dle požadavku.

Definice bezpečnostního posouzení: *Proces analýzy faktorů ovlivnující návrh poplachových systémů.*[1]

Význam bezpečnostního posouzení objektu spočívá v sběru a zpracování informací potřebných k vytvoření návrhu PZTS.

Výstupy bezpečnostního posouzení jsou využitelné zejména v následujících oblastech:

- stanovení rozsahu systému,
- východisko pro volbu komponentů,
- vymezení potencionálních hrozeb,
- charakteristika potencionálního narušitele,
- stanovení stupně zabezpečení,
- stanovení pojistné třídy,
- určení třídy prostředí,
- návrh řešení systému (počty, typy detektorů…),
- umístění komponent v objektu,
- redukce planých poplachů.

Bezpečnostní posouzení má čtyři oblasti zájmů, které musí projekt PZTS brát v úvahu:

- zabezpečované hodnoty,
- budovy,
- vnější vlivy,
- vnitřní vlivy.

Tyto vlivy je pak nutné posuzovat ze dvou pohledů. Jedním z nich je analýza rizik a druhym je posouzení ostatních vlivů na systém.[1]

4.2 Analýza rizik

Analýzy rizik jsou základním prvkém krizového inženýrství. Analýza nabízí varovnou fázy projektu PZTS. Důvodem, proč je důležité zachytit varovné signály je snadnost řešení krizí v brzkém stádiu. Sníží se tím náklady na odstranění následků bezpečnostních událostí a možností předcházet těmto událostem. [11]
Analýza rizik si pokládá tři otázky:

1. *Jaké negativní události se mohou vyskytnot?*
2. *Jaká pravděpodbnost výskytu negativní událostí může nastat?*
3. *Jaké následky vzniknou pokud negativní událost nastane?*

Uvedené otázky spolu úzce souvisí. Nebezpečí je zdroj ohrožení a riziko je bráno jako míra tohoto ohrožení.

4.3 Ostatní vlivy na systém

Tyto vlivvy jsou popisovány jako vnější nebo vnitřní a jsou dalším vstupem do hodnocení bezpečnosti systému s kterým se musí počítat. Získávání hodnot pro výsledné hodnocení účinnosti systému od ostatních vlivů se požívají metody určující velikosti těchto vlivů. K posuzení vnitřních i vnějších vlivů bezpečnosti jsou využívány metody:

- indukce
- dedukce
- porovnávací

4.3.1 Induktivní metody

Induktivní metody se používají v případech, kdy existuje dostatečné množství statistických případů na stanovení pravděpodobnostních veličin. Získávání těchto údajů a stabilita zkoumaného prostředí jsou často omezující faktorem při jejich využívání. Potřebné údaje lze získat a nahradit z expertních odhadů, které však mohou zavádět do celého procesu určitý stupeň subjektivity dotazovaných.

4.3.2 Deduktivní metody

Deduktivní metody využívají hodnocení jevů, které už v minulosti vznikly. Z těchto jevů pak vybíráme zdroje poučení v bezpečnostních procesech budoucnosti. Princip metody spočívá v porovnávání a hledání shody v průběhu určitých událostí, na základě kterých se dá předvídat jejich další vývoj nebo ovlivnit jejich průběh.

K posuzování úrovně bezpečnostních rizika používáme metody kvalitativní nebo kvantitativní.

4.3.3 Kvantitativní metoda

Kvantitativní hodnocení je založené na vyjádření pravděpodobnosti anebo početnosti výskytu negativního jevu a na číselném vyjádření následků. Kvantitativní vyjádření lze posuzovat, pokud známe početnost výskytu všech rizik a početnost výskytu zkoumaného rizika.
Využíváme přitom vztahu:

$$\mathrm{Pi} = \frac{\sum \mathrm{Ri}}{\sum \mathrm{R}}\text{, kde platí že } \sum \mathrm{Pi} = 1 \qquad (12)$$

Při výskytu všech rizik a výskytu jednotlivých rizik je vztah:

$$\mathrm{Pi} = \frac{1}{\sum \mathrm{R}} \qquad (12)$$

kde :

Pi = pravděpodobnost vzniku bezpečnostního rizika [<0, 1>]

∑ Ri = početnost výskytu bezpečnostního rizika [počet]

∑ R = početnost výskytu všech bezpečnostních rizik [počet]

4.3.4 Kvalitativní metoda

Toto hodnocení se v praxi požívá ve vyšší míře a je založené na vyjádření věrohodnosti. Míra rizika se nevyjadřuje matematickým zápisem, ale pomocí expertního hodnocení vyplívajících činitelů (např. hrozba, pravděpodobnost, důsledek). Problém, který může nastat při použití různých kvalitativních metod je, že mohou být vyjádřené různé hodnoty úrovně rizika. Proto závisí od organizace pro kterou metodiku se rozhodne. Její rozhodnutí ovlivňuje účel / podnět, který ji vede k procesu posuzování rizik.

4.4 Identifikace nebezpečí

Identifikace bezpečnostních rizik a posouzení rizikových faktorů zahrnuje činnosti, které mohou ohrozit cíle organizace. Je zaměřena na identifikaci rizika, rizikových faktorů, zpracování scénářů, určení důsledků a pravděpodobností ohrožení. Do rizikových faktorů patří :

1. technologická nebezpečí – energetika, průmysl, komunikace, doprava,
2. ekonomická nebezpečí – globální krize, kolaps peněžních ústavů, trhy,
3. politická nebezpečí – občanské nepokoje, demokratický vývoj, totalitní režim,
4. sociální nebezpečí – obecná kriminalita, speciální kriminalita, nepolitická sabotáž,
5. právní nebezpečí – zákony, normy, soudy, smlouvy,
6. klimatická nebezpečí – změny klimatu, krátkodobé povětrnostní jevy.

Tyto bezpečnostní rizika lze vyjádřit souhrně v analýze SWOT, která zpracovává silné či slabé stránky systému bezpečnosti, ale i příležitosti a hrozby plynoucí z vnitřních a vnějších vlivů působících na systém bezpečnosti.

SWOT Analýza		Analýza vnitřního prostředí	
		Silné stránky	Slabé stránky
Analýza vnějšího prostředí	Příležitosti	Strategie Maximalizace silných stránek, maximalizovat příležitosti	Strategie Minimalizace slabých stránek, maximalizovat příležitosti
	Hrozby	Strategie Maximalizace silných stránek, minimalizovat hrozby	Strategie Minimalizace slabých stránek, minimalizovat hrozby

Obr. 8. SWOT analýza procesu identifikace rizik

4.5 Posouzení stávajících opatření

Tato část modelu hodnocení účinnosti bezpečnostního systému je důležité provést nejlépe ze dvou úhlů pohledu na stávající bezpečnostní opatření. Vnitřní pohled je posouzen vlastními pracovníky provozu, bezpečnostním technikem nebo managementem organizace a vnější pohled je posuzen nezávislou organizací pověřenou vypracováním projektu bezpečnostních opatření v závislosti na podmínkách a míře požadovaného stupně zabezpečení. Posouzení stávajících opatření bezpečnosti souvisí s přijetí opatření podle legislativních standardů.

4.6 Hodnocení rizika

Při hodnocení rizik se můžeme setkat s případy, kdy v daném prostředí existuje vícero bezpečnostních rizik se stejnou úrovní rizika. Proto při hledání vhodných opatření sehrává důležitou roli prioritizace rizik, která je součástí procesu hodnocení rizik.
Pro tyto případy je možné využít metody operační analýzy:

- metoda pořadí
- metoda párového porovnání
- metoda bodového hodnocení

Metody operační analýzy určují míry a významnost bezpečnostních rizik organizace. Porovnávají rizika mezi sebou a přiřazují jim body významnosti, které označují důležitost v bezpečnosti stávajícího systému. Do hodnocení rizik se řadí další metody určující účinnost systémů. Metoda výpočtu koeficientů času zásahu zásahové jednotky v závislosti na celkovém čase napadení objektu narušitelm. Metoda hodnocení počtu detektorů v poměru ku rozloze objektu. Metody pro hodnocení efektivnosti systémů v porvnání s vloženými investicemi do bezpečnostních opatření. Metoda postupu narušitele cestou nejmenšího odporu. Každý model systému ochrany objektů by měl mít své vstupní a výstupní veličiny (kritéria). Při modelování výstupních veličin existují dva způsoby, jakým je možné vyjádřit stupně veličin. Bud´ dané veličiny / časy budeme považovat za konstantní a vyjádří se jejich číselnou hodnotou – deterministický model, nebo jsou považovány za náhodné, proměnné – stochastické modely.

Výstupem hodnocení rizik je rozhodnutí zda riziko je akceptovatelné nebo neakceptovatelné.

Pokud se riziko stane akceptovatelné uzavře se okruh hodnocení bezpečnosti a výsledek učinnosti stávajícího systému je postačující bezpečnostním požadavkům požadovaným organizací či vlastníkem objektu (ochranného zájmu).

Pokud je výsledek hodnocení účinnosti bezpečnostního poplachového systému neakceptovatelný musí se organizace okamžitě vrátit na začátek do bodu posouzení systému a přistoupit k novým opatřením na snížení rizika.

Dílčí závěr

V této kapitole jsem popsal návrh několika metod, které lze použít k hodnocení účinnosti poplachových systémů. Metody musí jasně vyjadřovat k čemu jsou použity a jaké veličiny jsou jejich vystupem např. výpočet koeficientů zásahu, metoda pro zjištění postupu narušitele cestou nejmenšího odporu jsou informační sběr vstupů pro celkovou analýzu hodnocení účinnosti systému. Vstupy jsou kameny skládačy celého obrazu systému s kterým je možné dále pracovat (zlepšení ochranných opatření).

5 HODNOCENÍ ÚČINNOSTI SYSTÉMU

Návrh hodnocení účinnosti bezpečnostních a poplachových systémů jsem aplikoval na objektu nové zkušebny výrobků u výrobní organizace. Objekt zkušebny bude situačně umístěn v areálu firmy, kde vnější perimetr objektu bude chráněn fyzickou ostrahou v podobě strážných v obchůzkovém režimu ochrany areálu podpořenou sledovacím systémem CCTV spojeným s DPPC v místě centra fyzické ostrahy pro detekci narušitele střeženého prostoru/zájmu firmy.

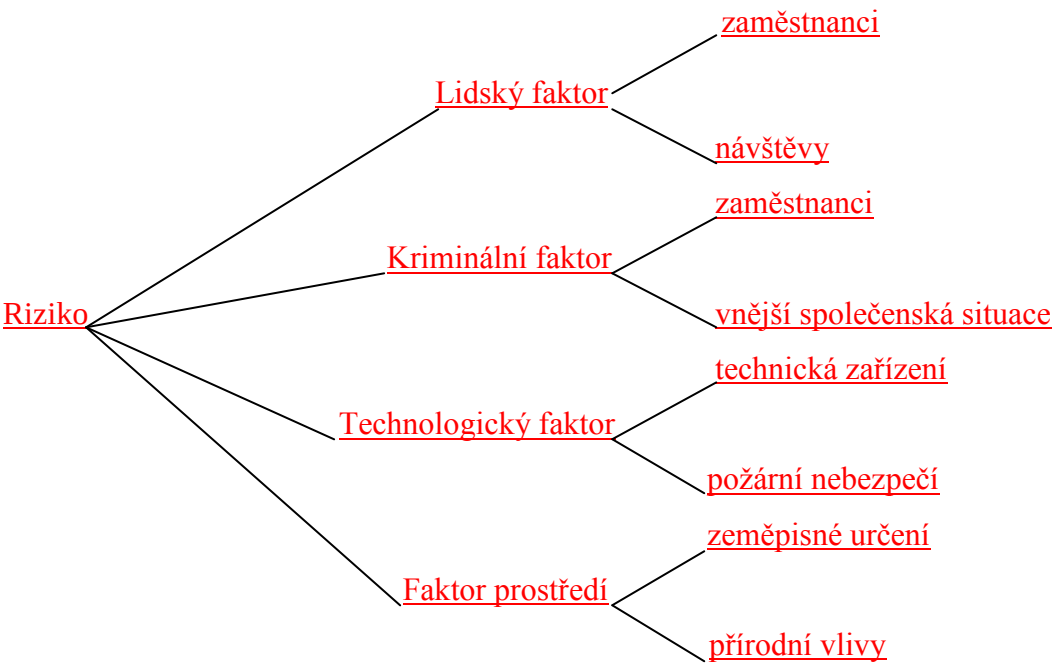
Zkušebna bude samostatně stojící objekt, který bude zahrnovat dvě nadzemní podlaží, plus přízemní prostory. Přízemní část objektu bude z bezpečnostního hlediska vniknutí do objektu nejrizikovější. Do rizikových částí patřit hlavní vchod (vchodové dveře), technický vchod (vrata pro technologická řešení v rámci strojového parku zkušebny), okenní stavební otvory. Prostory přízemí budou střeženy a detekovány pasivními i aktivními prvky objektové ochrany, což představuje detektory tříštění skla, detektory pohybu při zastřeženém objektu snímače zavření či otevření oken i technického vchodu do objektu. Hlavní vchod bude střežen aplikací ACS slouží k řízení kontroly vstupu přístupového modulu zahrnujícího dveřní bezpečnostní zámek, čtečku osobních karet zaměstnanců s volným přístupem nebo přístupem pro hosty s čipovou kartou.

První patro objektu bude chráněno před vniknutím narušitele detektory tříštění skla a detektory pohybu při zastřeženém prostoru. Druhé patro bude chráněno před narušitelem jen detektory pohybu. Okenní výplně nebudou nijak chráněny, protože se nepředpokládá vniknutí narušitele těmito konstrukčními otvory. Všechny komponenty systému budou propojeny s ústřednou PZTS umístěnou v jedné z kanceláří nového objektu (archiv písemností zkušebny).

Celý objekt pak bude také propojen na EPS firmy, který bude spojen na DPPC ostrahy firmy. Ostraha pak bude ověřovat zda signál je čí není chybný a dá povel pro výjezd HZS nebo dobrovolného sboru hasičů firmy.

5.1 Identifikace bezpečnostních rizik objektu

Identifikace bezpečnostních rizik objeku zkušebny je vytvoření seznamu možných negativních událostí, které mohou nastat při provozu zkušebny. Z vyobrazení je vidět, že velkým rizikovým faktorem jsou zaměstnanci. Jsou součástí dvou faktorů, proto je nutné zaměstnancům věnovat zvýšenou pozornost. Mají přístup k utajovaným zájmům i majetkovým aktivům firmy.



Obr. 9. Strom identifikace rizik

Podle identifikace a analýzy rizika jsem se soustředil na nejpravděpodobnější ohrožení bezpečnosti objektu zkušebny na rizika způsobená kriminálním faktorem do níž patří kriminalita z vnějšího prostředí, tak i ze strany zaměstnanců a technologický faktor, kde nejvyšší procentuální zastoupení má hrozba požáru.

5.2 Posouzení stávajícího bezpečnostního systému organizace

Z bezpečnostního rizika je organizace nejvíce ohrožena kybernetickou krádeží (technická řešení výrobků, vývoj nových výrobních programů), Jde o konkurenční boj o nové prodejní trhy. Dalšími bezpečnostními riziky firmy jsou majetková trestná činnost zvenčí i zevnitř, nedbalost zaměstnanců při jejich pracovní činnosti a ohrožení lidí i majetku požárem.

Rovněž hmotný majetek (strojové vybavení) může být v ohrožení ze strany neodborné manipulace zaměstnanců zkušebny tak i ze strany zaměstnanců firmy s přístupem do prostorů zkušebny. Z hlediska historických událostí je vysoké riziko požárního nebezpečí. V minulosti byl již hašen požár na jednom ze zařízení, kde topné těleso vznítilo olejovou náplň vyhřívání.

Jednou z metod, kterou jsem použil pro posouzení rizika je metoda párového porovnání. Spočívá v určení významnosti bezpečnostního rizika postupným pozorováním každého rizika s každým.

Tab. 15. Párové porovnání bezpečnostních rizika

					R1	R2	R3	R4	R5	R6
1	1	1	1	1	3					
2	3	4	5	6			1			1
	2	2	2	2		4				
	3	4	5	6			1	1		
		3	3	3			3			
		4	5	6						
			4	4				1		
			5	6						1
				5					1	
				6						
Celkem					3	4	5	2	1	2

Popis: Riziko R1 = vnější vlivy, Riziko R2 = kriminální čin, Riziko R3 = požár, Riziko R4 = sabotáž, Riziko R5 = nedbalost zaměstnanců , Riziko R6 = vnitřní vlivy

Nejvýznačnější se stává riziko, které má nejvyšší součet v těchto porovnáních. Bezpečnostní rizika se posuzují v tzv. Fullerovu trojúhelníku. Schéma Fullerova trojúhelníku je založeno na zápise dvojic porovnávaných bezpečnostních rizik do dvou řádků pod sebe.

Po sečtení jednotlivých hodnocení rizik vychází jednoduché vyjádření porovnávaných. Za nejzávažnější rizika považuji rizika R3 a R2. Člověk jako riziko bude vždy vnášet nejistotu do bezpečnostních systémů a je jen na každém, zda dodržuje bezpečnostní politiku firmy v rámci své působnosti a pracovní činnosti.

Tab. 16. Hodnocení stupnů pro párové porovnání

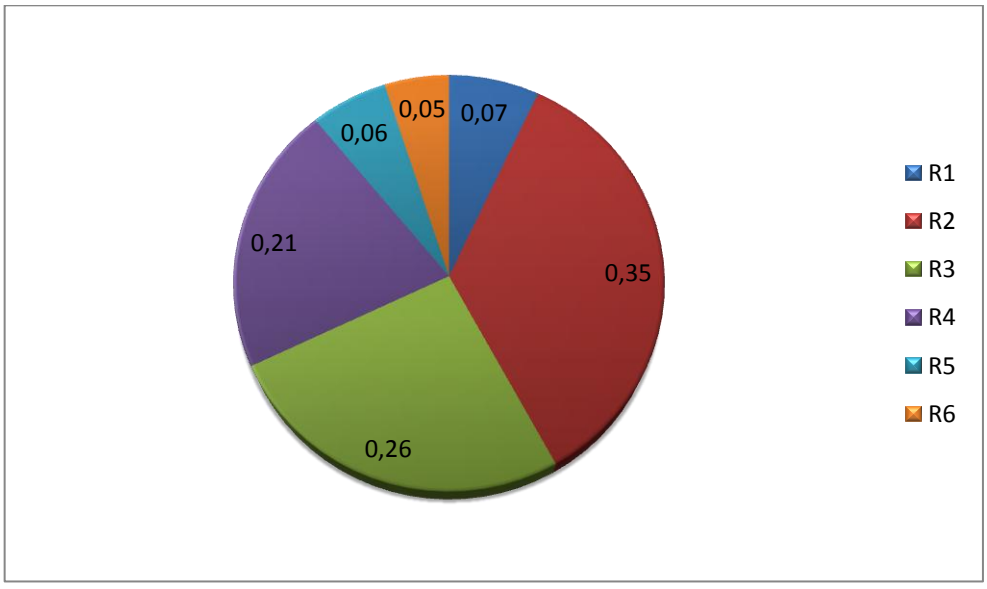
Stupeň hodnocení - w	Porovnání R3 a R5
1	Ra stejně důležité jako Rb
2	Ra silně důležitější než Rb
3	Ra o mnoho silněji důležitější než Rb
4	Ra velmi silně důležitější než Rb
5	Ra extrémně důležitější než Rb

Tabulka hodnocení stupnů párového porovnání slouží k odstranění nerozhodnutých porovnání z tabulky č.15. rizik R4-R6. Porovnáním dvou rizik zjistíme stupeň ohrožení, který budu dál používat pro upřesnění významnosti rizika.

Tab. 17. Porovnání pomocí hodnotících stupňů a váhového koeficientu (Zdroj [5])

Riziko	R1	R2	R3	R4	R5	R6	Suma	Priorita	k
R1		1/5	1/3	1/4	2	1	3,78	4	0,07
R2	5		2	3	4	5	19	1	0,35
R3	3	1/2		4	3	4	14,5	2	0,26
R4	4	1/3	1/4		4	3	11,58	3	0,21
R5	1/2	1/4	1/3	1/4		2	3,33	5	0,06
R6	1	1/5	1/4	1/3	1/2		2,58	6	0,05
Suma							54,77		1,00

Výsledkem parového hodnocení rizik je váhový koeficient rizika k na celkovém riziku organizace. Nejvyší podíl je tedy u rizika kriminálního činu a hned z nim je ohrožení objektu požárem.



Obr. 10. Graf podílu jednotlivých rizik na celkovém riziku

5.3 Hodnocení účinnosti bezpečnostního systému

V tabulce č.18 jsou srovnávací data v bezpečnostním prostředí jen u stupnů 3 a 4 protože stupně 1 a 2 mají v intervalu ověřování spojení podle normy ČSN EN 50131-1 ed. 2 mezi komunikaci aktivního prvku zabezpečení a ústřednou I&HAS min. 240 a 120 minut, což je nevyhovující z hlediska ochrany navrženého projektu.

Tab. 18. Výpočet koeficientu účinnosti ochranných opatření pomocí aktivních prvků

Detekce aktivních prvků	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Qochr. Tn/Tfo	-	-	3,606	7,212
Qochr. Tprl/Tfo	-	-	2,545	5,090
Popis: Tn = 2380(s), Tprl = 1680(s), Tfo = 660(s) 3 stupeň, Tfo = 330(s) 4 stupeň.				

Výpočty koeficientů účinnosti detekce aktivních prvkůProto komponenty a systémy stupně 1 a 2 bezpečnostního prostředí se nehodí pro instalaci bezpečnostního poplachového systému do projektu zkušebny. Z tabulky je možné vyčíst, že koeficienty jsou vyšší jak jedna. Pokud by koeficienty nedosahovali jedné, pak by ochranná opatření systému byla nedostačující a systém by nesplnoval požadavky bezpečnostní ochrany pro případ napadení narušitelem z vnějšího prostředí. Pokud koeficienty naopak vychází nad jedna, má systém vyšší účinnost bezpečnostní ochrany (čím vyšší tím lepší). Odborná literatura uvádí, že koeficient by se měl pohybovat v intervalu <6, 12>.[ ]

$$\mathbf{Tn > Tfo} \qquad (5)$$

$$\mathbf{Tprl / Tfo > 1} \qquad (5)$$

Toto hodnocení nelze využít pro případy, kdy ochranný zájem je napadený ze strany zaměstnanců firmy s přístupem do provozu zkušebny nebo pracovníků samotné zkušebny. Pracovníci v tomto případě mají volný pohyb po prostorách zkušebny a nejsou nijak omezeni v přístupech do jednotlivých zon (systém je odstřežen a nepracuje).

5.4 Detekce vniknutí pomocí fyzické ochrany

K hodnocení účinnosti bezpečnostního poplachového systému pomocí detekce fyzické ochrany jsem použil poměr celkového času napadení objektu narušitelem a času periodické obchůzky fyzické ochrany společně s časem přesunu a zásahu zásahové jednotky. Výsledný poměr udává, jaká je účinnost bezpečnostních opatření vzhledem k fyzické ostraze objektu.

Tab. 19. Výpočet koeficientu účinnosti ochaných opatření pomocí fyzické ochrany

Detekce fyzickou ochranou	
Qochr. Tn/Tfo	0,595
Qochr. Tprl/Tfo	0,420
Popis: Tn = 2380(s), Tprl = 1680(s), Tfo = 4000(s).	

V tabulce č.19 jsou vypočítány koeficienty detekce narušitele pomocí fyzické ostrahy. Čas zásahu zásahové jednotky musí být vždy nižší než čas napadení. Výpočet detekce fyzické ostrahy a následného zásahu jsou nižšší než jedna. Tento výsledek ukazuje, že při daném obchůzkovém režimu fyzické ostrahy objektu není zaručena ochrana objektu. Interval obchůzky fyzickou ochranou je dlouhý a musel by se zkrátit z 3600(s) na čas 1980(s) a méně, aby účinnost této ostrahy byla dostatečná. Vztahy pro výpočet:

Tn > Tfo (5)

Tprl / Tfo > 1 (5)

Zadání pro výpočty koeficientů ochranných opatření pro zkušebnu výrobků.

Tn – celkový čas napadení narušitelem od momentu detekce v čase Tdet aktivními prvky ochrany, až po jeho opuštění střeženého prostoru 2380[s]

Tprl – celkový čas prolomení pasivních prvků ochrany 1680[s]

Tfo – celkový čas reakce zásahové jednotky 660, 330[s]

Tp – čas prolomení všech pasivních prvků ochrany 1500[s]

TPres – celkový čas potřebný na přesun narušitele k ochrannému zájmu a to od momentu jeho detekce aktivními prvky ochrany v čase Tdet 180[s]

Tút – čas útoku narušitele 400[s]

Tún – čas úniku narušitele 480[s]

Tpop – čas vyhlášení poplachu 160(3 stupeň), 20(4 stupeň)[s]

Tver – čas verifikace napadení 100(3 stupeň), 10(4 stupeň)[s]

Tpres – čas přesunu na místo zásahu 180[s]

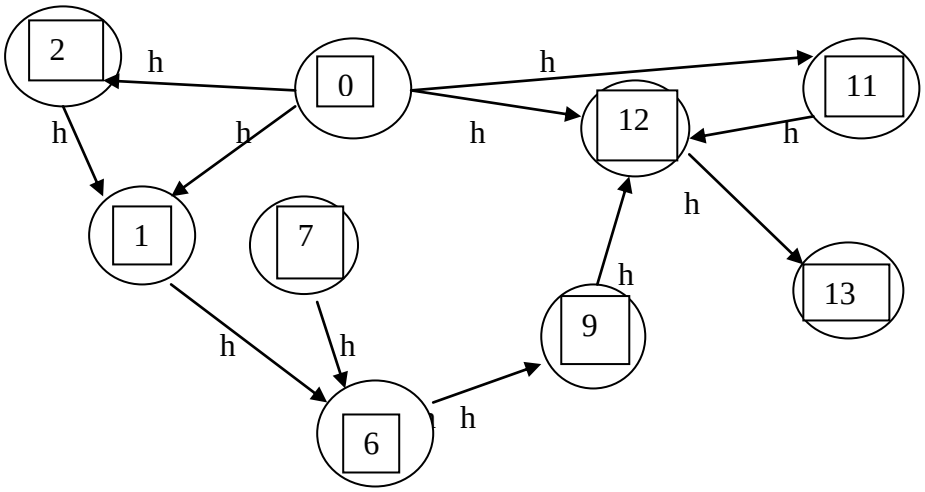
Tzás – čas zásahu proti narušitelovi 220[s]

Thl – interval mezi dvěma obhlídkami fyzické ostrahy 3600[s]

5.5 Model cesty nejmenšího odporu

Model minimální cesty se používá při určování účinnosti navrženého bezpečnostního poplachového systému formou scénáře, kdy narušitel má dostatečné informace o půdorisu objektu a rozmístění aktivních i pasivních detektorů ochrany. Scénář zhrnuje definované hodnoty jako konstantní (krajní hodnoty). Při ideálních podmínkách pro narušitele jsou časy napadení i úniku extremní (např. min. čas prolomení pasivních prvků ochrany, max.

čas zásahu zásahové jednotky. V pro tento model je vhodné použít model minimální cesty obrázek č.11. Modelově ukazuje možnosti postupu narušitele k ochrannému zájmu.



Obr.11. Sítový graf možných tras přesunu narušitele

Hrany mezi jednotlivými zonami představují časy přesunu narušitele od jedné zony k druhé. Tyto časy jsou průměry časů ověřovacích pokusů přesunu narušitele mezi jednotlivými zonami. Z těchto hran je možné jednoduše najít postup narušitele minimální cestou, součtem jednotlivých hran.

5.6 Možnosti postupu narušitele

1 / možnost je postup narušitele zónami 0-2-1-6-9-12-13, výsledek =2380[s]

Čas obsahuje prolomení okenní ochrany v přízemí budovy + tří dveří vnitřní ochrany a čas přesunu k ochrannému zájmu.

2 / možnost postupu zónami 0-12-13, výsledek =2620 [s]

Čas obsahuje vylezení po vnějším obvodu objektu do 3NP, prolomení okenní ochrany, jedenkrát vnitřní dveře a přesun na místo ochranného zájmu. Tento čas ale předpokládám jako nereálný, z důvodu potřeby zvláštní konstrukce k dosažení okenního otvoru ve 3NP.

3 / možnost postupu zónami 0-1-6-9-12-13, výsledek =2540 [s]

Čas obsahuje překonání vstupních dveří do objektu, dvou dveří vnitřní ochrany a přesunu k ochrannému zájmu.

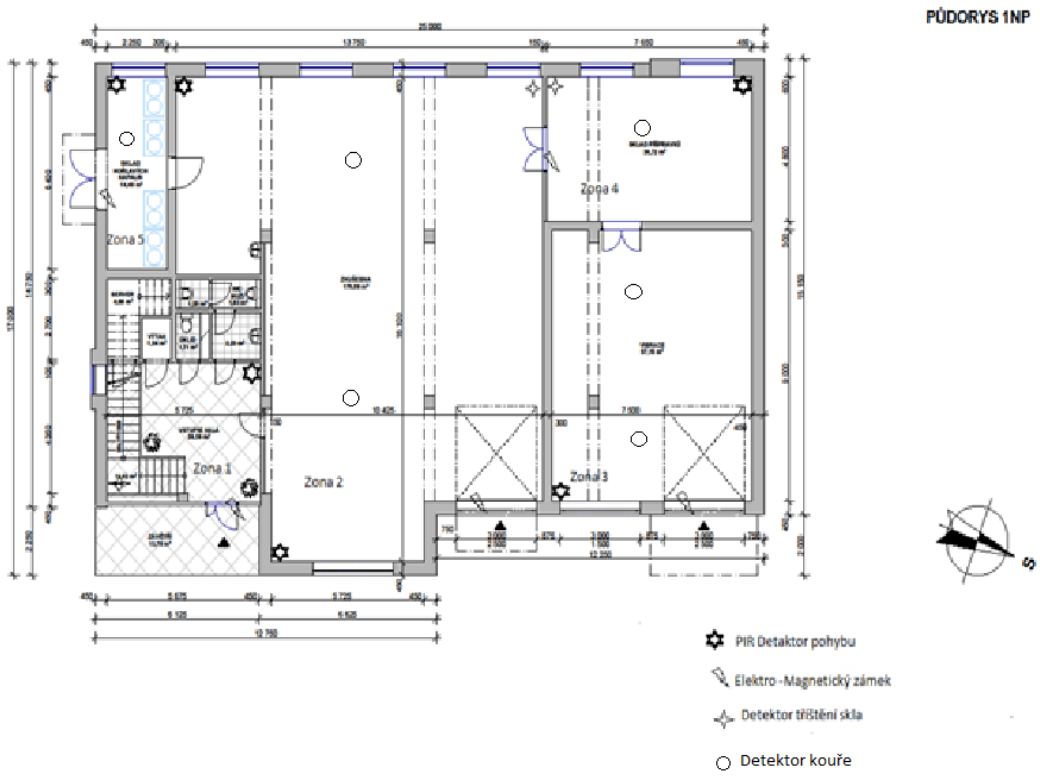
4 / možnost postupu zónami 0-11-12-13, výsledek =2740 [s]

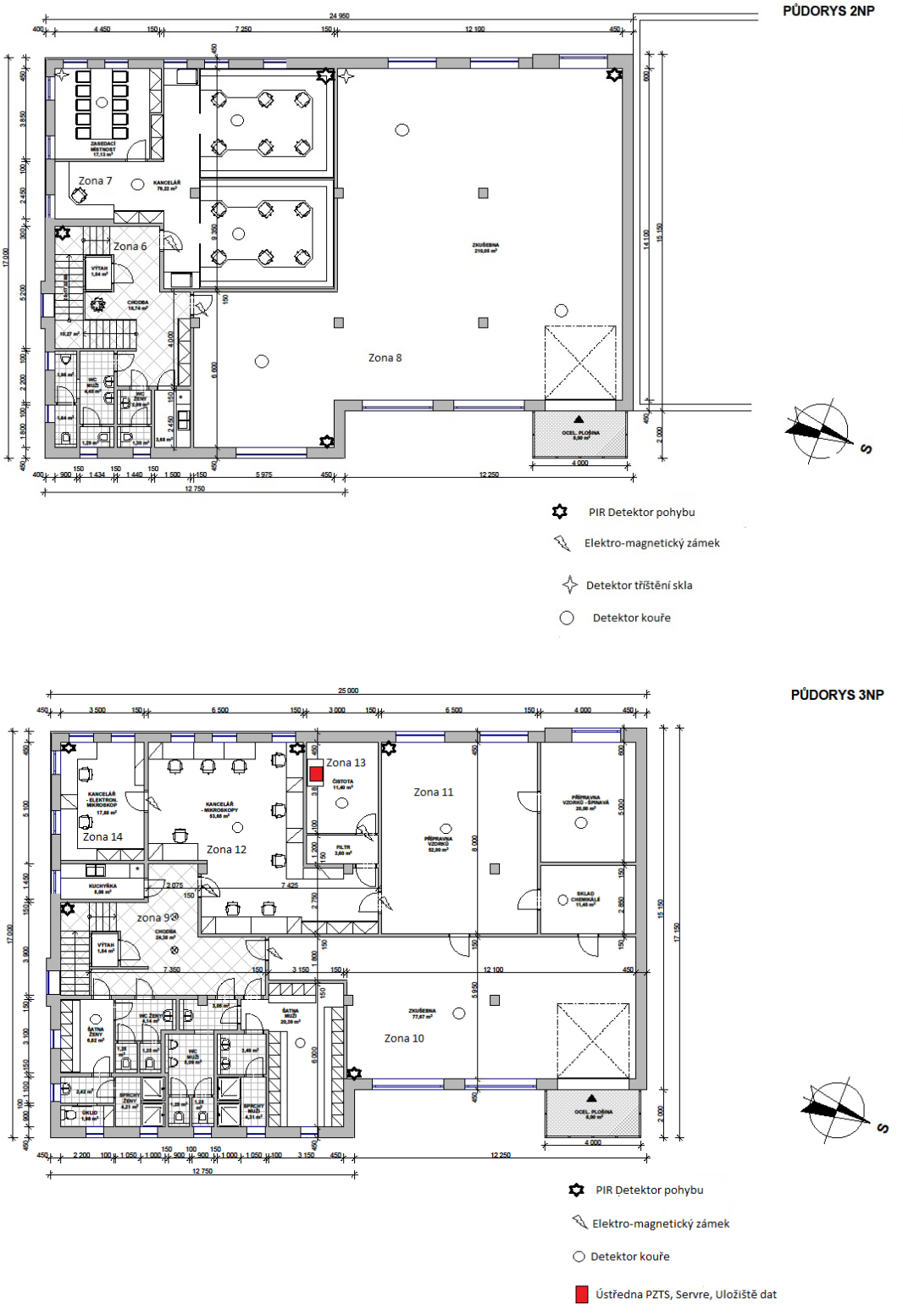
Čas obsahuje vylezení po vnějším obvodu objektu do 3NP, prolomení ochrany dvou vnitřních dveří a přesunu k ochrannému zájmu. Tento čas ale předpokládám jako nereálný, z důvodu potřeby zvláštní konstrukce k dosažení okenního otvoru ve 3NP.

5 / možnost postupu zónami 0-7-6-9-12-13, výsledek =2420 [s]

Čas obsahuje vylezení po vnějším obvodu objektu do 2NP, prolomení ochrany tří vnitřních dveří a přesunu k místu ochranného zájmu.

5.7 Půdorysné schéma objektu zkušebny





Obr.12. Půdorisy objektu zkušebny

(Zdroj[Projekční kancelář UNIPROJEKT])

Po sečtení jednotlivých možných časů přesunu narušitele mezi zónami až k ochranému zájmu by byla možnost s výsledkem 2380s nejefektivnější.

Použitím binomické věty jsem spočítal pravděpodobnost přesunu narušitele k ochrannému zájmu pěti trasami (tabulka č.20). S ohledem, že narušitel je dobře obeznámen s jednotlivými trasami k dosažení tohoto cíle.

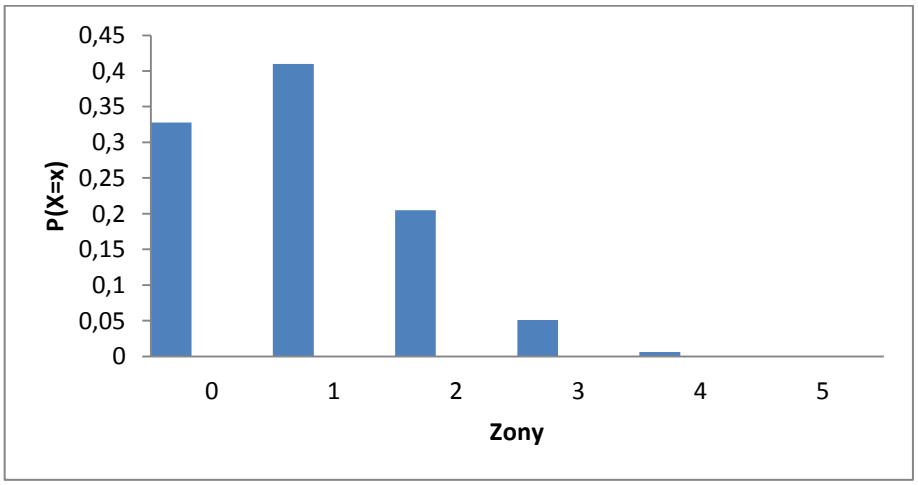
Použitý vztah:

$$\sum_{k}^{0} \mathrm{P}(\mathrm{X} = \mathrm{k}) = 1 \qquad (12)$$

Tab. 20. Binomické rozdělení pravděpodobnosti výběru zony.

Zony (k)	0	1	2	3	4	5	∑
P(X=k)	0,328	0,410	0,205	0,0512	0,0064	0,00032	1

Pro lepší názornost uvádím graf scénáře postupu narušitele k ochrnnému zájmu nejmenší cestou odporu.



Obr. 13. Graf pravděpodobnosti přesunu zonami narušitelem

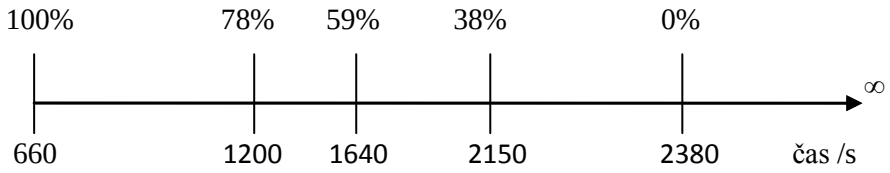
5.8 Pravděpodobnost zásahu zásahové jednotky

Hustotou pravděpodobnosti funkce (x) jsem vypočítal časy, které nabývají jednotlivých hodnot, kde výpočty znamenají pravděpodobnost v jakém časovém horizontu zasáhne zásahová jednotka.

Použitá základní distribuční funkce byla ve tvaru:

$$F(x)=\begin{cases}0 & \text{pro } x\in(-\infty,a)\\ \dfrac{x-a}{b-a} & \text{pro } x\in\langle a,b\rangle\\ 1 & \text{pro } x\in(b,\infty)\end{cases} \tag{12}$$

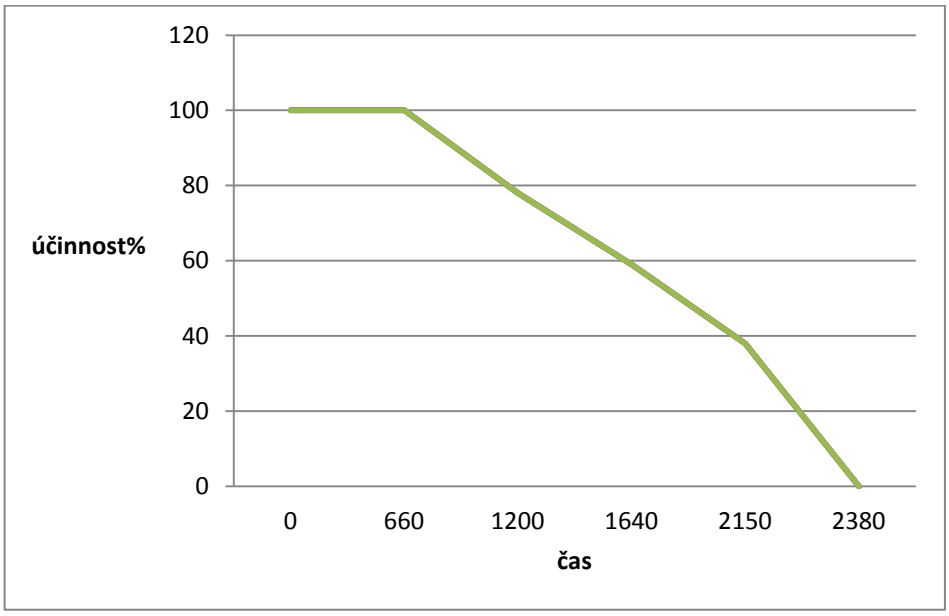
Hledaná pravděpodobnost:



Obr. 14. Časová osa

Na časové ose jsem vyznačil časy od 660[s](celkový čas zásahu zásahové jednotky) po čas 2380[s], který představuje celkový čas útoku narušitele až po jeho únik z chráněnného prostoru. Časy 1200[s], 1640[s] a 2150[s] jsou náhodně vzbráné z intervalu < 660, 2380 > . Jednotlivé časy představují účinnost zásahu zásahové jednotky (pravděpodobnost účinného zásahu). Pro čas 1200[s] vychází koeficient pravděpodobnosti 0,22 . Po převodu na procenta je koeficient 22%. Rozdíl koeficientu 22% a 100% vychází 78%, který udává

účinnost zásahu. Tedy, při detekci narušitele a času 1200[s] je 78% účínnost zásahu zásahové jednotky



Obr. 15. Grafické znázornění úspěšnosti zásahu

5.9 Hodnocení účinnosti pasivních prvků

Z uvedené distribuční funkce jsem dále počítal pravděpodobnost odolnosti jednotlivých pasivních prvků ochrany použitých pro zabezpečení ochrany v časových intervalech. Okenní stavební otvory mají při čase napadení v 1110s jen 38% účinou odolnost vůči napadení narušitele. Vnitřní prostorové dveře mají při čase napadení v 320s účinou odolnost 94%. Další výsledky odolnosti použitých pasivních ochranných prvků se lze dočíst v tabulce.

Tab. 21. Odolnosti použitých pasivních prvků ochrany

	Pravděpodobnost odolnosti pasivních prvků (pp)				
okenní stavební otvor 200[s]	0,38	0,29	0,22	0,12	0,05
odolnosti (%)	62	71	78	88	95
vstupní vchodové dveře 240[s]	0,36	0,28	0,21	0,11	0,03
odolnosti (%)	64	72	79	89	97
vnitřní prostorové dveře 180[s]	0,39	0,3	0,23	0,13	0,06
odolnosti (%)	61	70	77	87	94
stavební konstrukce 880[s]	0,1	0,008	-	-	-
odolnosti (%)	90	99	100	100	100
Cas prolomení pasivních prvků ochrany	1110	900	730	500	320
Popis: V tabulce jsou uvedeny výpočty (pp) pasivních prvků ochrany a procentuální účinnost ochrany jednotlivých pasivních prvků					

5.10 Technické parametry PZTS

Technické parametry PZTS musí splnovat požadavky která patří mezi elektrická – elektronická zařízení. Tato technika se řídit požadavky:

- nařízení vlády č. 616/2006 Sb., technické požadavky na výrobky z hlediska jejich elektromagnetické kopatibility,
- nařízení vlády č. 17/2003 Sb., technické požadavky na elektrická zařízení nízkého napětí,
- nařízení vlády č. 426/200 Sb., technické požadavky na radiová a na telekomunikační koncová zařízení [1]

5.10.1 Výběr ústředny

Pro objekt ústředny byla vybrána ústředna do vnitřních prostor, napájením 12V-24V, radiové spojení GSM, připojení detektorů sítí nebo bezdrátové, kontrola 4 subsystémů.
Objekt zkušebny potřebuje obsáhnout ochranu proti neoprávněnému vstupu subsystémem (ACS), ochranu perimetru objektu (CCTV), požární ochranu (EPS) a ochranu bezpečnosti práce (SAS).

5.10.2 Počet detektorů

Rozloha objektu zkušebny je 3*425m². Na objekt je naplánováno 16 detektorů pohybu a tříštění skla. Pokud jsou všechny detektory funkčí a spuštěn stav zastřežení je tento počet dostačující. Komponenty však musí splnovat 3 a 4 stupeň bezpečnosti, které splnují časy pro ověřování a maximální nedostupnost propojení.

5.10.3 Přístup osob

Přístupový subsystém objektu musí splnovat úroven bezpečnosti 2 a výše. Přístup k ovládacím prvkům má osoba která ovlivnuje provozní stav a má přístup vymezen klíčem nebo jiným ekvivalentem bezpečnosti (kod, zámek).

Dílčí závěr

Hodnocení účinnosti bezpečnostního poplachového systému je součástí projektu bezpečnostní opatření. Tato opatření jsou dostatečná či nikoli. Ke kontrole bezpečnostních opatření objektu je nutné hodnotit jeho účinnost. V této kapitole jsem se zabýval hodnocením účinnosti bezpečnostních opatření u nového objektu zkušeby umístěného do areálu výrobní organizace. Použitím několika metod (pravděpodobnost detekce narušitele, účinnosti detekce pasivních prvků systému, pravděpodobnost zásahu zásahové jednotky,.) jsem posuzoval účinnost bezpečnostního systému vzhledem požadavků bezpečnosti (počet detektorů/ rozloha objektu, rozmístění detektorů, požadavek přístupové úrovně.

Výsledek hodnocení účinnosti bezpečnostního poplachového systému objektu je:

1. Objekt má dostatečnou bezpečnostní ochranu spolu s použitím aktivních prvků detekce narušitele. Detektory splnují požadavky i funkce kladené na ochraná opatření. Dostatečně rychle informují fizickou ochranu i zásahovou jednotku o narušení perimetru ochrany objetu.
2. Detekce narušitele fyzickou ochranou objekt je nevyhovující. Pravděpodobnost zásahu proti narušiteli je nízká (pohybuje se po 1) a zásah by byl neúčinný. Pro zlepšení účinnosti ochrany bych navrhoval kratší interval obchůzek nebo zvýšit investice do lepší bezpečnostní úrovně ochrany objektu.
3. Detekce psivními prvky ochrany je závislá od počtu jejich instalace v objektu. V 1NP jsou všechna okna zajištěna zámky a detekcí uzamčrní společně s bezpečnostní folií. Hlavní vchod je zabezpečen zámkem s chráněn přístupovým systémem. Ostatní vchody a vrata jsou chráněna zámky s detekcí narušení (magnetické kontakty). Hystorie bezpečnostních událostí ukazuje, že objek je dostatečně zajištěn proti napadení zvenčí. Pokud by byl útok veden osobou, která má přístup do objektu bude těžké zábránit jí v uskutečnění. Jedinou ochranou by měla být instalace CCTV přímo v prostorách ochranného zájmu. Systém by zaručoval detekci narušitele záznamu jeho útoku.
4. K určení hodnocení účinnosti bezpečnostních opatření objektu jsem použil scénář postupu narušitele cestou nejmenšího odporu. Touto metodou hodnocení jsem zjistil nejefektivnější postup detekčními zonami k ochrannému zájmu.

S výsledným časem je možné dál pracovat (vyhodnocovat), zvyššováním ochraných opatření. Účinnost instalovaného systému PZTS je akceptovatelná v poměru s cestou nejmenšiho odporu.

ZÁVĚR

Téma mé diplomové práce „ Hodnocení účinnosti bezpečnostního poplachového systému“, které jsem si zvoli pro mne znamená zabývat se objektovou bezpečností. Rozsah tohoto tématu má široky záběr, může se týkat objektů v občanské zástavbě, průmyslových objektů i objektů veřejných. Studiem v oboru bespečnostní technologie systémy a management jsem získal dostatečné znalosti a informace, které jsem použil v této práci. Pro modelový objekt jsem si vybral průmyslový objekt. Hodnocení účinnosti ochrannách opatření bezpečnosti je důležitým článkem jak organizace chrání svá aktiva i zaměstnance. Dává pravdivý pohled na systém jako celek a ukazuje i práci subsystémů. Pokud je hodnocení účinnosti zprávně zpracované a má vypovídající výstup, ukazuje bezpečnostnímu managementu, kde je bezpečnost ochraných opatření neúčinná a je potřeba investic nebo jiných opatření a kde je naopak dostačující a není potřeba nových nákladů do stávajícího systému bezpečnosti.

Investice, které vtšina firem dává do svých systémů bezpečnosti jsou spíše nedostatečné a plně nechrání jejich zájmy. V současné době je ale mnoho firem, které nabizí ucelené porfoio svých služeb v oblasti komerční bezpečnosti. Služby které nabízí jsou i posouzení bezpečnosti a hodnocení účinnosti stávajícího bezpečnostního systému organizace. Není proto složité zadat takovouto zakázku. Vidím jen jediný problém, vybrat tu správnou firmu.

SEZNAM POUŽITÉ LITERATURY

[1] VALOUCH, Jan. *Projektování bezpečnostních systémů*. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5 152s.

[2] VALOUCH, Jan. *Projektování integrovaných systémů*. [skriptum]. Zlín: UTB, 2013. ISBN 978-80-7454-296-1 152s.

[3] ČSN EN 50131-1 ed. 2. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy.* Část 1: Systémové požadavky. Praha: Český normalizační institut, 2007.

[4] ČSN CLC/TS 50131-7. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy.* Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, meteorologii a státní zkušebnictví, 2011.

[5] LOVEČEK, Tomáš. Reišpís, Josef. *Projektovanie a hodnotenie systémov ochrany objektov*. Zilina : EDIS – vydavateltvo ZU, 2011. 281 s. ISBN 978-80-554-0457-8

[6] LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management.1.vyd. Zlín: VeRBuM, 2011. 316s. ISBN 978-80-87500-19-4

[7] LOVEČEK, Tomáš. *Zranitel´nost informačných systémov*, In: Securitológia Zeszyty Naukowe European Associtation for Security 2007 č. 6, ISBN 978-83-925072-0-8.

[8] ROPER, C. *Risk Management for security Professionals*. Oxford, Butterworth Heinemann 1999. ISBN 0-7506-7113-0.

[9] LOVEČEK, Tomáš. *Faktory hodnotiace kvalitu bezpečnostného system.* Krízový manažment č. 1/2005. Žilina: EDIS 2005. ISSN 1336-0019-02.

[10] SEDLÁČEK, J. *Bezpečnostní ochrana jaderných zařízení a jaderních material – analýza a hodnocení účinnosti system fyzické ochrany.* Praha: Československá komise pro atomovou energii v Ustavu jaderných informací 1991.

[11] **Š**EFČÍK, Vladimír. *Analýza rizik*. Zlín. Univerzita Tomáše Bati ve Zlíně. Academia centrum. 2009. ISBN 978-80-7318-696-8.

[12] PIATKA, L´. Matematika IV, *Numerické metody, pravděpodobnost a matematická statistika*. Žilina. 1987. ISBN 80-05-00006-5

[13] http://www.alarmy.lesovna.eu/gsm-alarmy/379-esim364-wireless.html [online] 2014 [cit. 2011-05-25]. Detektory pohybu. Dastupné z WWW<http://www.alarmy.lesovna.eu/gsm-alarmy/379-esim364-wireless.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS – Poplachový zabezpečovací a tísňový systém

I&HAS - Poplachový zabezpečovací a tísňový systém (Evropské označení)

EPS – Elektronická požární signalizace

DPPC – Dohledové přijímací poplachové centrum

CCTV – Uzavřený televizní okruh

SAS - Systém přivolání pomoci

ACS – Přístupový poplachový systém (doplnkové ovládací zařízení)

APS - záložní napájecí zdroj

CSN - Česká technická norma

EMS - Elektromagnetická odolnost

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: MODEL OBJEKTU ZKUŠEBNY

PŘÍLOHA P 2: KOMBINOVANÝ DETEKTOR POHYBU A ROZBITÍ SKLA

Kombinovaný detektor pohybu a rozbití skla

Technická specifikace:

Typ detektoru	PIR detektor a detektor tříštění skla
Barva	bílý
Napájení	8,2 - 16VDC
Proudový odběr (klid / max)	16/22mA
Typ snímače	Čtyřnásobný PIR senzor / Glassbreak
Dosah	PIR 15m, Glassbreak 10m
Tamper kontakt	ano
Duální detektor	ano
PET imunita	ano
Digitální zpracování signálu	ano
Nastavitelná citlivost	ano
Čítač pulsů	ano
Montážní výška	2,4m
Rozměry (š×v×h)	62,5 x 118 x 41 mm [13]

PŘÍLOHA P 3: GSM ZABEZPECOVACÍ ÚSTREDNA

GSM zabezpečovací ústředna ESIM364 ELDES- 4 podsystémy, nadstavba 868 MHz

Technická specifikace:

- Napájení: 12 - 24 V AC nebo DC
- Použití: vnitřní prostory
- Pracovní frekvence: 868 MHz
- Přenos poplachu: GSM síť
- Připojení detektorů: drátové i bezdrátové
- Značka: ELDES [13]

PŘÍLOHA P 4: ELRKTRICKÝ ZÁMEK, ZÁPADKA EB2109

Elektrický zámek, západka EB2109

Pro posílení zabezpečení vstupních dveří. Lze jej ovládat kódovými klávesnicemi, čtečkami otisku prstů či jinými zařízeními.

- Napájení: 9 - 12V DC
- Použití: vnitřní prostory
- Připojení: drátové
- Značka: AMPERTECH [13]

PŘÍLOHA P 5: OKENNÍ ZÁMEK S AUTOMATICKÝM UZAMYKÁNÍM

5.11 FTS 99

Okenní zámek s automatickým uzamykáním

- pro všechny typy oken
- uzamčení automaticky při uzavírání okna
- odemykání zámku klíčem
- ocelová závora o odolnosti 1 tuna