VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2018 Bc. Vlastimil Müller

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

VÝUKOVÝ SOFTWARE PRO NÁVRH A ANALÝZU POPLACHOVÝCH ZABEZPEČOVACÍCH SYSTÉMŮ
EDUCATIONAL SOFTWARE FOR THE DESIGN AND ANALYSIS OF ALARM INTRUSION SYSTEMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Vlastimil Müller

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Karel Burda, CSc.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Vlastimil Müller ***ID:*** 198185
Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Výukový software pro návrh a analýzu poplachových zabezpečovacích systémů

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte a popište problematiku návrhu a analýzy poplachových zabezpečovacích systémů (PZS). Na tomto základě zvolte vhodnou metodu analýzy bezpečnosti PZS a tu detailně popište a vysvětlete. Následně vytvořte software pro návrh a analýzu PZS. Tento software by měl umožnit vytvářet a editovat jednoduché půdorysy staveb, umisťovat do půdorysu značky jednotlivých prvků PZS, zakreslovat propojení mezi těmito prvky a zakreslovat detekční diagramy detektorů. Vytvořený software by dále měl umožnit kvantitativní analýzu bezpečnosti navrženého PZS.

DOPORUČENÁ LITERATURA:

[1] Fikejs J.: Software pro podporu projektování elektrické zabezpečovací signalizace. (Diplomová práce). VUT v Brně, Brno 2010.

[2] Oyeyinka O. D. aj.: Determination of System Effectiveness for Physical Protection Systems of a Nuclear Energy Centre. Science and Technology 2014, č. 4, s. 9-16.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 21.5.2018

Vedoucí práce: doc. Ing. Karel Burda, CSc.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

UPOZORNĚNÍ:
Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Poplachové zabezpečovací systémy (PZS) jsou nedílnou součástí našeho pracovního i osobního života, kdy pomáhají jak s ochranou důležitých pracovních dat tak třeba vlastního majetku. Tato semestrální práce se zabývá teorií návrhu a analýzy PZS jakožto dvou důležitých faktorů ovliňujících efektivitu jejich finální realizace. V práci je rozebrán obecný postup návrhu, několik metod analýzy a samotné prvky používané pro PZS. Těchto teoretických znalostí je využito k návrhu a implementaci aplikace IASPlanner, která umožňuje zákres návrhu PZS a jeho následnou kvantitativní analýzu. Tato aplikace může být následně využita nejen k samotným návrhům, ale též při výuce předmětů zabývajících se zabezpečovacími systémy.

KLÍČOVÁ SLOVA

zabezpečení, systém, PZS, C#, software, návrh, analýza, WPF

ABSTRACT

Intrusion alarm systems (IAS) make inseparable part of our personal and work life which helps us with protection of important work data or personal property. This paper looks into the theory of IAS design and analysis which are two important factors influencing final system effectiveness. Furthermore, general procedure of IAS design, a number of analysis methods and IAS components are discussed. This theoretical knowledge is used to design and implement an aplication called IASPlanner, which allows users to draw a layout of IAS and subsequently analyse designed systems. The aplication can be used not only for the design itself, but also for educational purposes.

KEYWORDS

security, system, IAS, C#, software, design, analysis, WPF

MÜLLER, Vlastimil. *Výukový software pro návrh a analýzu poplachových zabezpečovacích systémů*. Brno, 2018, 70 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Karel Burda, CSc.

Vysázeno pomocí balíčku `thesis` verze 3.03; `http://latex.feec.vutbr.cz`

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Výukový software pro návrh a analýzu poplachových zabezpečovacích systémů“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Karlu Burdovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizovaný v laboratořích podpořených projektem Centrum senzorických, informačních a komunikačních systémů (SIX); registrační číslo CZ.1.05/2.1.00/03.0072, operačního programu Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

V dnešní době je instalace poplachových zabezpečovacích systémů (PZS) do firemních budov i domácností velmi rozšířená a lze se s těmito systémy setkat prakticky na každém kroku. Díky šíření PZS napříč firemním i soukromým sektorem dochází k vývoji nových a vylepšování starých metod detekce narušení a analýzy PZS. Návrh a následná realizace instalace PZS je komplexní proces jehož zvládnutí umožňuje kvalitní ochranu důležitých dat a majetku a zamezit tak například značným finančním ztrátám. Kvalitní návrh dokáže zjednodušit celou instalaci včetně kabelového vedení, počtu detektorů a následně i efektivitu a cenu celého provedení. V dalších kapitolách tohoto textu se proto budeme zabývat postupem návrhu PZS, jeho analýzou aplikací, která bude grafický návrh a následnou analýzu PZS umožňovat.

Nejprve tedy položíme teoretický základ některým termínům z teorie bezpečnosti a zmíníme některé normy a předpisy jimiž by se měl návrh a analýza PZS řídit. Tematiky návrhu a analýzy PZS jsou následně rozebrány podrobněji včetně všech jejich zohledňovaných hledisek. Z prezentovaných metod kvantitativní analýzy je vybrána jedna, která bude implmentována v rámci navržené aplikace. První teoretická část je zakončena výčtem nejběžnějších komponent PZS a jejich specifických vlastností.

Navazující kapitola se věnuje programu IASPLAnner, který uživateli umožňuje právě grafický návrh PZS a jeho kvantitativní analýzu. Nejprve jsou rozebrána technická hlediska návrhu takového programu jako je použitý programovací jazyk, vývojové prostředí a struktura programu a následně se text věnuje rozvržení grafického uživatelského rozhraní a popisu ovládání a funkcí spojených přímo s návrhem PZS. Veškeré funkce a možnosti programu jsou popsány tak, aby je byl každý uživatel schopen použít bez ohledu na jeho dovednosti práce s počítačem.

Závěr této práce je diskutuje schopnost aplikace zpracovat návrh PZS a provést nad ním kvantitativní analýzu a splnění zadání této práce.

1 Teoretický základ problematiky PZS

Problematika návrhu a analýzy PZS je poměrně rozsáhlá, a proto ji nelze opomíjet. Postupy návrhu PZS jsou obecně popsány v technických normách, které obsahují vodítka pro celý proces návrhu včetně některých hledisek výběru komponent PZS. V této kapitole nejprve zmíním vybrané základní pojmy, bude probrán postup návrhu PZS, tak jak je definován v normách, popíši metody kvantitativní analýzy systému a celou kapitolu zakončím výčtem charakteristikou nejběžnějších komponent PZS.

1.1 Základní pojmy

Pro snazší orientaci v textu této práce budou v následujícím části nejdříve uvedeny některé základní pojmy úzce souvisící s problematikou PZS. Jedná se o naprostý základ, který nepostihuje všechny možné termíny. Další pojmy budou doplněny v částech této práce, ve kterých to bude považováno za nutné.

Poplachové zabezpečovací systémy (PZS)

Poplachové zabezpečovací systémy (PZS), také označované jako Elektrické zabezpečovací systémy (EZS), slouží k zabezpečení aktiv ve vymezeném prostoru. K dosažení adekvátní míry bezpečnosti bývají PZS doplněny například systémy pro kamerový dohled, perimetrickými zabezpečovacími systémy či systémy pro řízení přístupu.

Aktiva

Aktivem rozumíme cokoliv, věc nebo data, co je považováno za cenné a jehož ztrátou by dané osobě nebo organizaci mohla vzniknout škoda.[1]

Hrozba

Hrozba popisuje, kdo nebo co (útočník nebo samovolná událost) a jakým způsobem může zapříčinit ztrátu určitých aktiv.[1]

Bezpečnost

Bezpečnost označuje stav, kdy možné ztráty aktiv nepřekračují určitou míru. Tato míra je ovlivněna hodnotou aktiv a případnými náklady na realizaci jejich ochrany.[1]

Ochrana

Ochranou rozumíme různá opatření (technická, personální...), která mají zabránit ztrátě aktiv. Různé typy ochran jsou seskupeny v komplexních systémech, kterým říkáme zabezpečení. Nedostačující nebo chybějící část zabezpečení potom označujeme jako slabinu.[1]

Autorita

Autorizací, tj. předáním přístupových práv, rozhoduje kdo a v jakém rozsahu smí přistupovat k určeným aktivům. [1]

Uživatel

Uživatel je autorizovaná osoba, která potřebuje přístup k daným aktivům z podstaty náplně své práce. Okruh aktiv, ke kterým má uživatel přístup se udržuje pokud možno co nejmenší.[1]

Útočník

Je osoba, která se snaží přistupovat k aktivům, ke kterým nemá oprávnění. Může se jednat jak o zaměstnance firmy spravující daná aktiva, tak o cizí osobu.[1]

Střežené prostory

Část budovy a/nebo místní oblasti, v níž může být PZS detekováno vloupání, pokus o vloupání nebo aktivace tísňového hlásiče.

Zóna

Stanovená oblast střeženého prostoru, v níž mohou být PZS detekovány stavy vloupání, pokusu o vloupání, nebo aktivace tísňového hlásiče.[2]

Komponenty PZS

Jednotlivá zařízení, která jsou spolu sestavena propojena a tvoří tak PZS.

Detektor

Typ komponenty PZS, který podle typu detekce určitým způsobem monitoruje přítomnost např. osob nebo jiných objektů uvnitř části střeženého prostoru. V případě, že je vyhodnoceno narušení, signalizuje poplach.

Poplach

Výstraha signalizovaná detektorem pro zbytek systému, upozorňující na přítomnost nebezpečí pro život, majetek nebo okolní prostředí.

Sabotáž
Úmyslná nedovolená manipulace s PZS nebo jeho částmi. [2]

1.2 Normy a předpisy

Problematiku návrhu, instalace, zkoušek a revizí PZS řeší v České republice rodina norem ČSN EN 50131 [2]. Pro návrh a realizaci zapojení PZS se dají jako nejdůležitější vybrat ČSN EN 50131-1 (Všeobecné požadavky) a ČSN CLC/TS 50131-7 (Pokyny pro aplikace). Celá rodina norem ČSN EN 50131 má tyto části:

- ČSN EN 50131-1 Všeobecné požadavky
- ČSN EN 50131-2-1 Společné požadavky na detektory
- ČSN EN 50131-2-2 Požadavky na pasivní infračervené detektory
- ČSN EN 50131-2-3 Požadavky na mikrovlnné detektory
- ČSN EN 50131-2-4 Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
- ČSN EN 50131-2-5 Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
- ČSN EN 50131-2-6 Požadavky na kontakty otevření
- ČSN EN 50131-2-7 Požadavky na detektory tříštění skla
- ČSN EN 50131-3 Ústředny
- ČSN EN 50131-4 Výstražná zařízení
- ČSN EN 50131-5-1 Společné požadavky na propojovací zařízení
- ČSN EN 50131-5-2 Propojovací zařízení využívající VF techniku
- ČSN EN 50131-5-3 Propojovací zařízení využívající ič. techniku
- ČSN EN 50131-6 Napájecí zdroje
- ČSN CLC/TS 50131-7 Pokyny pro aplikace

1.3 Postup návrhu PZS

Při návrhu PZS je zapotřebí shromáždit potřebné informace o zabezpečovaném objektu a aktivech, stanovit rozsah zabezpečení objektu a typy použitých detektorů a zařízení. Dle ČSN EN 50131-7 je postup realizace PZS strukturován takto:

- návrh systému,
- plánování montáže,
- montáž,
- prohlídka, funkční zkouška a přejímka,
- dokumentace a záznam o provozu systému,
- provoz a údržba systému.

Z hlediska tématu semestrální práce se dále budeme zabývat především částmi Návrh systému a Plánování montáže, z nichž budou vybrána hlediska důležitá pro návrh PZS.

1.3.1 Posouzení zabezpečovaných hodnot

Návrh PZS se odráží od míry rizika narušení střežených prostor. Míra rizika je závislá na charakteru a hodnotě střežených aktiv. Pro bezpečnostní posouzení zabezpečovaných hodnot můžeme uvažovat několik faktorů [2]:

- Druh majetku - snadnost jeho zpeněžení, atraktivita pro útočníka, nebezpečí vloupání,
- Hodnota majetku - maximální pravděpodobná hodnota jednotlivé ztráty, následné výdaje související se ztrátou, osobní vztah k věcem,
- Množství nebo velikost - možnost snadné demontáže, transportu, dalšího nakládání a přístupu do střežených prostor
- Historie krádeží - způsoby narušení střeženého prostoru a počet případných předchozích krádeží,
- Nebezpečí - pro okolní prostředí, zneužití střeženého majetku, pro okolní osoby,
- Poškození - riziko vandalismu, žhářství či jiného poškození střežených aktiv.

1.3.2 Bezpečnostní posouzení objektu

Při bezpečnostním posouzení objektu nebo prostor určených k zabezpečení je třeba prověřit množství hledisek, která se dají seskupit do následujících kategorií[2]:

- Posouzení zabezpečované budovy,
- Vlivy působící na PZS s původem uvnitř střežených prostor,
- Vlivy působící na PZS s původem mimo střežené prostory.

Všechny kategorie jsou dále uvedeny se seznamy nejběžnějších faktorů, které je potřeba při posuzování brát v úvahu. Tyto seznamy rozhodně nejsou konečné, protože

některé realizace PZS vyžadují zvážení vlastních specifických faktorů a nelze je tak obsáhnout všechny.

Posouzení zabezpečované budovy

K posouzení rizika jsou klíčovým faktorem zejména skutečnosti týkající se stavební dispozice zabezpečovaného objektu. Některé takové skutečnosti jsou [2]:

- Stavební dispozice objektu (stěny, střechy, podlahy a sklepení),
- Otevírané části budov (okna, dveře, střešní světlíky, ventilace apod.),
- Provoz střeženého objektu (ostraha, přístup veřejnosti, neobývané prostory),
- Dosažitelnost osob s klíči schopných reagovat na signalizaci PZS,
- Lokalita (riziko kriminality, přístup z jiných budov, doba odezvy na signalizaci PZS),
- Kvalita a rozsah stávajícího PZS a mechanických zabezpečovacích zařízení,
- Předcházející krádeže a hrozby, způsoby jejich provedení,
- Místní právní a správní předpisy, které mohou ovlivnit návrh PZS.

Vlivy působící na PZS s původem uvnitř střežených prostor

Vnitřní dispozice střeženého prostoru může mít negativní vliv na funkci některých komponent PZS, a proto je při návrhu potřeba tyto vlivy identifikovat a snažit se jejich působení na PZS pokud možno eliminovat. Tyto vlivy jsou často dobře ovlivnitelné uživatelem daného prostoru a patří k nim:

- Vytápění a vzduchotechnika může vlivem turbulence vzduchu nepříznivě působit na ultrazvukové detektory,
- Výtahy a další strojní zařízení mohou svými vibracemi ovlivňovat nebo spouštět například detektory otřesu,
- Fluorescenční světelné zdroje mohou rušit mikrovlnné detektory, kompaktní výbojky mohou způsobovat velké množství elektromagnetického rušení a bodové reflektory mohou osvětlovat a spouštět PIR detektory pohybu,
- Pohyb vody ve vodovodním potrubí může ovlivňovat blízko instalované mikrovlnné detektory,
- Neupevněné nebo pohyblivé předměty mohou spouštět detektory pohybu nebo zastínit jejich zorné pole,
- Elektromagnetické rušení (el. svařovací soupravy, el. generátory a motory, domácí spotřebiče),
- Vnější zvuky (zařízení nebo předměty generující zvuky s podobným frekvenčním spektrem jako ultrazvukové detektory),
- Domácí zvířata (vliv na detektory pohybu),
- Průvan (proudění vzduchu ovlivňuje ultrazvukové a PIR detektory),

- Stavební konstrukce (měkké materiály mohou způsobovat vibrace při montáži detektorů),
- Zvláštní vlivy (citlivosti detektorů otřesů a detektorů rozbití skla).

Vlivy působící na PZS s původem mimo střežené prostory

Kromě klimatických podmínek prostředí, se vně střežených prostor mohou vyskytovat další faktory [2], které mohou ovlivňovat chod PZS a které je potřeba brát při v úvahu při volbě komponent PZS, zejména detektorů. Stejně jako u vnitřních vlivů, by zde měla platit maximální snaha o eliminaci vnějších vlivů vhodnou skladbou a rozmístěním komponent PZS.
Některé příklady vnějších vlivů:

- Dlouhodobé faktory (nemění se v řádu let, pozemní a podzemní komunikace, železnice, letecká doprava, parkoviště)
- Vlivy počasí (brát v potaz místa s nadměrným výskytem silných větrů, srážek, blesků, ale i otřesy a sesuvy půdy)
- Vysokofrekvenční rušení (přítomnost vojenských i civilních vysílačů nebo radarů může způsobovat silné el. mag. rušení, zvláště důležité u bezdrátových PZS)
- Sousedící prostory (například stroje pracující na sousedící stavbě, nebo provozovaná velká el. zařízení)
- Ostatní (části PZS, které mohou být volně přístupné zvenku například dětem)

1.3.3 Klasifikace prostředí

Komponenty používané v PZS jsou rozděleny to čtyř tříd [2]podle prostředí, ve kterém jsou schopny správně fungovat. Platí, že v případě potřeby je možné použít komponenty splňující podmínky vyšší třídy použity v prostředí s třídou nižší.

Třída	Název	Popis	Pracovní teploty
I	Vnitřní	Obytné nebo obchodní prostory se stálou teplotou.	+5°C až +40°C
II	Vnitřní všeobecné	Prostory bez trvalého vytápění, kde může docházet ke kondenzaci vody na oknech (chodby, haly, skladiště).	-10°C až +40°C
III	Venkovní chráněné	Obvykle vně budov, komponenty nejsou vystaveny povětrnostním podmínkám.	-25°C až +50°C
IV	Venkovní všeobecné	Vně budov, komponenty jsou plně vystaveny povětrnostním podmínkám.	-25°C až +60°C

Tab. 1.1: Klasifikace tříd prostředí.

1.3.4 Stupeň zabezpečení

Podle úrovně rizika útoku, znalostí a dovedností případného útočníka lze stanovit stupeň zabezpečení [2]. Vše přitom vychází z bezpečnostního posouzení prostoru objektu a zabezpečovaných hodnot. Pokud je PZS rozdělen do více subsystémů, mohou mít jednotlivé subsystémy rozdílné stupně zabezpečení. Stupeň zabezpečení subsystému odpovídá komponentě s nejnižším stupněm zabezpečení. Komponenty, které jsou sdílené více subsystémy, musí mít stupeň zabezpečení odpovídající nejvyššímu stupni zabezpečení ze všech takto připojených subsystémů. Tabulka 1.2 definuje stupně zabezpečení a jim odpovídající rizika.

Stupeň	Riziko	Útočník
1	Nízké	Útočníci mají malé znalosti PZS a disponují omezeným výběrem snadno dostupných nástrojů.
2	Nízké až střední	Útočníci mají určité znalosti PZS a disponují základním výběrem snadno dostupných nástrojů.
3	Střední až vysoké	Útočníci jsou obeznámeni s PZS a disponují úplným výběrem nástrojů a přenosných el. zařízení.
4	Vysoké	Zabezpečení má prioritu nad ostatními hledisky návrhu. Předpokládáme, že útočníci mají podrobné znalosti PZS a disponují kompletním výběrem zařízení včetně prostředků pro náhradu komponent.

Tab. 1.2: Určování stupně zabezpečení

1.3.5 Úrovně střežení a typy detekce

Norma [2] uvádí tabulku 1.3 jako pomůcku pro určování, které druhy narušení mohou nastat v různých částech střežených objektů. Na základě předem určeného stupně zabezpečení, lze pro určité části objektu vybrat co je potřeba detekovat. Tabulka není závazná a je vysoce pravděpodobné, že některé realizace PZS se stejným stupněm zabezpečení se budou lišit v některých typech detekcí.

Vstupní parametr	**Stupeň 1**	**Stupeň 2**	**Stupeň 3**	**Stupeň 4**
Obvodové dveře	O	O	O+P	O+P
Okna		O	O+P	O+P
Ostatní otvory		O	O+P	O+P
Stěny				P
Stropy nebo střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předmět (vysoké riziko)			S	S

Klíč:
O = otevření (nejčastěji detekce magnetickým nebo mechanickým kontaktem)
P = průnik (narušení stavebních součástí střeženého objektu, např. detekce tříštění skla nebo otřesů)
T = past (detekce útočníka v prostorech s vysokou pravděpodobností detekce, např. detektory pohybu)
S = detekce specifická pro daná aktiva (např. detekce sejmutí obrazu ze stěny)

Tab. 1.3: Určování typů detekcí

1.3.6 Návrh systému

Návrh systému by měl obsahovat všechny informace, které potřebuje zadavatel k tomu, aby se mohl přesvědčit, že navrhovaný PZS je pro danou realizaci vhodný. Takový návrh sice nemá pevnou strukturu, nicméně norma [2] uvádí následující povinné položky:

- Údaje o klientovi (jméno, adresa a obchodní jméno a další informace, nutné pro jasnou identifikaci klienta)
- Údaje o střežených prostorech (název, adresa, účel a popis střežených prostor)
- Stupeň zabezpečení PZS včetně rozpisu stupňů zabezpečení jednotlivých subsystémů
- Třída prostředí každého komponentu
- Seznam vybavení (typy a umístění veškerého zařízení a stanovení předpokládaného pokrytí detektory pohybu)
- Konfigurace systému (podrobné informace o hlavních funkcích systému, včetně postupu uvádění do stavu střežení/klidu a stavu střežení)
- Hlášení poplachu (informace o zařízeních, typ a umístění výstražných zařízení a komunikátorů a název poplachového přijímacího centra nebo jiného přijímacího centra, do nějž se poplachové signály budou přenášet)

- Právní předpisy (podrobné informace o shodě jednotlivých systémových komponentů nebo PZS s požadavky místních nebo národních právních předpisů, např. předpisy o ochraně proti hluku)
- Normy (informace, že PZS a jeho komponenty dodržují národní nebo evropské normy)
- Další předpisy (shoda systémových komponentů nebo celého PZS s jakýmikoli dalšími předpisy, např. směrnicemi pojišťoven)
- Certifikace (Podrobnosti prohlášení o certifikaci komponentů a PZS)
- Zásah (plánovaná odezva na aktivaci poplachu nebo poruchy, např. policie, držitelů klíčů od prostoru, zásahové služby apod.)
- Údržba (doporučení pro pravidelnou údržbu celého PZS a jeho komponentů, četnost servisních prohlídek a seznamu prací)
- Opravy (podrobné údaje o navrhované servisní firmě, včetně kontaktních údajů)

1.4 Kvantitativní analýza PZS

Účinnost PZS lze charakterizovat jako schopnost odolat možnému útoku a zabránit tak ztrátě zabezpečovaných aktiv a měla by být nedílnou součástí každého návrhu PZS [3]. Účinnost PZS nám tedy může sloužit jako ukazatel toho, jestli návrh nového systému dostačuje požadavkům zadavatele. Může nám také sloužit k vyhodnocení případných slabin stávající instalace, kterou můžeme poté doplnit nebo upravit podle potřeb. Ke zjištění účinnosti PZS užíváme metody kvantitativní analýzy, které se podobně jako komponenty PZS časem vyvíjejí a adaptují na nové potřeby. Kvantitativní analýza je používána především pro ochranu důležitých objektů s vysokým stupněm zabezpečením, jako jsou nukleární elektrárny, vojenská zařízení, letiště, banky, muzea, apod. Cílem vyhodnocování účinnosti PZS za pomocí kvantitativní analýzy je tedy především:

- Ověření, že PZS je navržen a implementován tak, aby splnil požadavky jeho uživatele.
- Identifikaci možných nedostatků, které musí být odstraněny, aby bylo splněno zadání.
- Analýzu a ověření výsledků případných změn a vylepšení PZS.
- Pravidelné ověřování účinnosti v návaznosti na změny v PZS nebo vývoji metod útoků.
- Vyhodnocení účinnosti výdajů na jednotlivé komponenty PZS.

Jednotlivé metody a modely kvantitativní analýzy se od sebe odlišují v používaných postupech. V další textu bude uvedená obecná metrika a stručný přehled metod s jejich rozdíly. V kapitole 2 bude potom vybrána jedna konkrétní metoda, která bude implementována v rámci aplikace určené pro návrh a analýzu PZS.

1.4.1 Metrika kvantitativní analýzy

V následující části jsou uvedeny základní parametry PZS, které jsou zjišťovány pro potřeby analýzy. Zdrojem pro tuto část mi byl převážně text [3]. Aby bylo PZS efektivní, musí být schopné detekovat a zpomalit případný útok a následně dosáhnout přerušení útoku a zadržení útočníka. Při kvantitativní analýze těchto schopností se vychází z rizika možného útoku na zabezpečovanou oblast. Toto riziko je definováno jako součin pravděpodobnosti nežádoucího vlivu (útoku) na PZS a rozsahu a vážnosti způsobených škod:

$$R = P \cdot C \tag{1.1}$$

kde:

P = pravděpodobnost útoku
C = rozsah způsobených škod

Podle konkrétního typu analytické metody může rozsah způsobených škod vyjadřovat přímo částku, kterou by musel uživatel zaplatit za náhradu nebo opravu střežených aktiv, případně se může jednat o nějaký interní koeficient předem určený uživatelem PZS.

Pravděpodobnost útoku P je dále chápána jako součin pravděpodobnosti uskutečnění tohoto útoku a pravděpodobnosti, že tento útok bude úspěšný. Rovnice 1.1 bude tedy vypadat následovně:

$$R = [P_A \cdot P_{S/A}] \cdot C \tag{1.2}$$

kde:

P_A = pravděpodobnost uskutečnění útoku
$P_{S/A}$ = pravděpodobnost úspěšnosti útoku

Pravděpodobnost, že útok bude úspěšný, se snižuje se schopností PZS útoku odolat a je vyjádřena pomocí:

$$P_{S/A} = 1 - P_E \tag{1.3}$$

kde:

P_E = pravděpodobnost, že PZS zabrání dokončení útoku

Rovnice 1.2 poté vypadá takto:

$$R = [P_A \cdot (1 - P_E)] \cdot C \tag{1.4}$$

Ve skutečnosti se však celkem obtížně určuje pravděpodobnost, že se útok stane P_A, a proto se u velmi důležitých a exponovaných objektů určují $P_A = 1$ (objekt časem určitě někdo napadne) a $C = 1$ (škody budou maximální) a tím se celá rovnice zjednoduší.

Čím je schopnost PZS zastavit probíhající útok vyšší, tím je nižší riziko a proto se právě tato schopnost někdy uvádí jako měřítko účinnosti PZS. Pravděpodobnost, že PZS zabrání dokončení útoku je tedy:

$$P_E = P_I \cdot P_N \tag{1.5}$$

kde:

P_I = pravděpodobnost, že se podaří přerušit útok
P_N = pravděpodobnost, že bezpečnostní služba bude schopna zastavit nebo odvrátit útok

Pravděpodobnost P_N je závislá na zkušenostech a vycvičenosti bezpečnostních složek, které mají na starosti ostrahu zabezpečovaných prostor. Určení této hodnoty vychází z praktických zkušeností osob provádějících analýzu daného PZS. V praxi bývá tato hodnota u některých metod vynechávána, respektive její hodnota bývá 1. Potom ze vztahu 1.5 dostaneme pravděpodobnost P_I jako hlavní kritérium účinnosti PZS. Pravděpodobnost P_I závisí na samotném návrhu PZS, rozmístění a využití jeho komponent a jejich parametrech. Konkrétní metody analýzy nakládají s výpočtem P_I navzájem odlišně, a proto budou způsoby určení P_I popsány v další části textu u jednotlivých vybraných metod analýzy.

Z výše uvedených definic vyplývá, že schopnost PZS účinně reagovat na útok se odvíjí zejména od včasné detekce útoku. Při návrhu a následné analýze PZS je tedy vhodné si stanovit tzv. **kritický detekční bod**. Jedná se o bod v čase, za kterým již nebude případná bezpečnostní služba schopna reagovat na útok včas a může dojít k úspěšné realizaci útoku.

Podobně se při kvantitativní analýze určuje **kritická cesta**, což je cesta útoku, která je nejzranitelnější, tedy nejméně zabezpečená.

Uvedené definice platí obecně a některé analytické modely mohou určité rovnice zpřesňovat nebo naopak zobecňovat či snad úplně vynechat. Případné rozdíly v metodách budou dále uvedeny.

1.4.2 Stručný přehled některých metod

EASI

Jde o metodu vyvinutou v Sandia National Laboratory (SNL) v USA pro analýzu účinnosti PZS u atomových elektráren a jiných důležitých zařízení. EASI je jednoduchá a snadno použitelná metoda pro vyhodnocení PZS na jedné určité cestě útoku s předem definovanou hrozbou. I přes své stáří je metoda stále hojně používána s dobrými výsledky v porovnání s novějšími metodami [3] [4] .

Vstup

EASI model využívá jako hlavní vstupní parametry schopnost daného prvku PZS detekovat útok, zpoždění útočníka a reakční dobu ostrahy. Pravděpodobnost správné komunikace s bezpečnostními složkami je taktéž využívána. Schopnost detekce je vyjádřena jako pravděpodobnost, že proběhne úspěšně, zatímco zpoždění a reakční doba jsou udávány jako střední hodnoty a jejich směrodatné odchylky. Příklad vstupních hodnot je vidět na obrázku 1.4.
Schopnost detekovat útok v určitém bodě cesty útoku je definována jako:

$$P(D) = P(S) \cdot P(T) \cdot P(A) \tag{1.6}$$

kde:

$P(S)$ = pravděpodobnost, že daný detektor zachytí neznámou nebo nepovolenou aktivitu
$P(T)$ = pravděpodobnost, že poplach bude vyslán do ústředny/centrály k vyhodnocení
$P(A)$ = pravděpodobnost, že vyslaný poplach bude správně vyhodnocen

Zpoždění útočníka na cestě je bráno jako čas, který útočníkovi zabere než se přemístí od jedné překážky k druhé i včetně doby potřebné k jejich překonání. Tyto časy jsou odhadovány na základě předpokládaných schopností útočníka a úrovně zabezpečení. Na vstup EASI se udává střední hodnota a zpoždění a jeho směrodatná odchylka.

Reakční doba ostrahy RFT (reakční doba ostrahy - Response Force Time) je čas, který uběhne mezi vyvoláním poplachu a pokusem bezpečnostních složek zastavit útočníka. Reakční doba se skládá z po sobě jdoucích časových údajů, jako jsou například:

- doba nutná k vyrozumění o vyhlášení poplachu
- doba potřebná k vyhodnocení poplachu (obsluhou)
- doba nutná k vyrozumění ostrahy

- doba nutná k přípravě a dopravě ostrahy na místo poplachu
- doba nutná k provedení zásahu ostrahy

Na vstupu EASI modelu se ještě používá proměnná, která určí, kdy nastane detekce ve vztahu ke zpoždění útočníka. Jsou definovány tři vztahy:

- B - detekce před započetím daného časového úseku (např. videokamery)
- M - detekce během časového úseku (např. otřesy při prorážení zdi)
- E - detekce po skončení časového úseku

EASI		P_C		Reakční doba [s]	
				Střední hodnota	Směrodatná odchylka
		0.95		300	90
Krok	Popis	P_D	Zpoždění X detekce	Zpoždění [s]	
				Střední hodnota	Směrodatná odchylka
1	Přestřihnout plot	0	B	10	3
2	Doběhnout k budově	0	B	12	3,6
3	Otevřít dveře	0.9	B	90	27
4	Doběhnout do střežené oblasti	0	B	10	3
5	Otevřít dveře	0.9	B	90	27
6	Poškodit aktiva	0	B	120	36
Pravděpodobnost přerušení útoku:		0.4760			

Tab. 1.4: Příklad vstupních hodnot modelu EASI

Výstup

Výstupem EASI modelu je pravděpodobnost P_I, že bezpečnostní složky budou společně s PZS schopny přerušit útočníkův postup než se mu podaří ukrást nebo poškodit střežená aktiva. Pravděpodobnost P_I je vypočítávána podle obecného vzorce[5] pro i detekčních míst:

$$P_I = P(D_1) * P(C_1)P(R|A_1) + \sum_{i=2}^{n} P(D_i)P(C_i)P(R|A_i) \prod_{j=1}^{i-1}(1 - P(D_i))[] \qquad (1.7)$$

kde:

$P(D_i)$ = pravděpodobnost detekce útoku na prvku i

$P(C_i)$ = pravděpodobnost správné komunikace s bezp. složkami

$P(R|A_i)$ = pravděpodobnost, že bezpečnostní složky (R), přeruší útok před dokončením kroku, po detekci na prvku i

$\prod_{j=1}^{i-1}(1 - P(D_i))$ = pravděpodobnost, že detekce selže a útočník bude moci přejít k dalšímu kroku útoku

Pravděpodobnost správné komunikace s bezpečnostními složkami se značí P_C . Podle textu [4] je na základě výzkumu mnoha systémů vhodné volit za P_C implicitní hodnotu 0.95 a měnit ji pouze v případě vážných důvodů nebo pochybností o bezpečnostních složkách.

Pravděpodobnost $P(R|A_i)$ je vypočítána pro každý detektor na cestě útoku podle vzorce:

$$P(R|A) = P(x > 0) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx \tag{1.8}$$

kde:

x = TR - RFT je náhodná veličina
μ_x = E(TR) - E(RFT) je střední hodnota náhodné veličiny x s normální distribucí
σ_x^2 = Var(TR) + Var(RFT) je rozptyl náhodné veličiny x

TR (zbývající čas - Time Remaining) je čas, který zbývá útočníkovi k dosažení jeho cíle v momentě, kdy je útočník detekován PZS. K úspěšnému přerušení útoku musí být TR > RFT.

Pro výpočet $P(R|A)$ lze také využít statistickou funkci *NormSDist* v tabulkovém procesoru MS Excel. Tato funkce vrací normální rozdělení veličiny x se zadanou střední hodnotou a směrodatnou odchylkou. Příklad výpočtu $P(R|A)$ pomocí této funkce je znázorněn v [5] společně s kompletním výpočtem P_I pro vzorové zadání zabezpečovaných prostor.

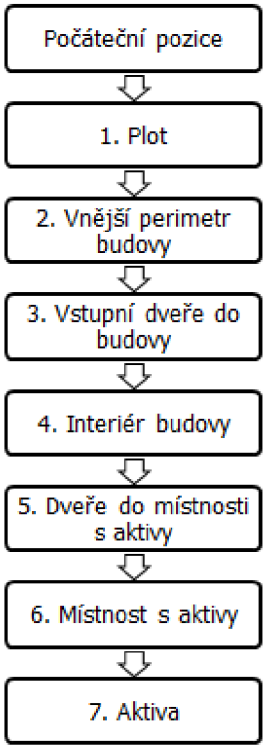
SAVI

Metoda SAVI provádí analýzu sekvenčních diagramů útoku na vstupu, aby mohla vyhodnotit zranitelnost analyzovaného PZS. Míra zranitelnosti je vyjádřena pomocí pravděpodobnosti přerušení útoku P_I. P_I udává, s jakou pravděpodobností se podaří bezpečnostním složkám střežícím zabezpečovanou oblast donutit útočníka k přerušení útoku, před dosažením aktiv. Výstupem metody SAVI je zpravidla deset nejzranitelnějších cest útoku seřazených podle jejich odpovídající P_I. K výstupům bývají přiřazeny i časové údaje o době, která zbývala útočníkovi do splnění jeho cíle a údaje o době, kterou potřebovala ostraha k zabránění útoku. Díky zahrnutí těchto časových hodnot je SAVI schopná určit i kritický detekční bod. [3] [6].

Postup

Postup analýzy se dá rozdělit do následujících kroků:

1. Identifikace aktiv a možných cest útoku
2. Vytvoření sekvenčního diagramu útoku
   Sekvenční diagram útoku popisuje posloupnost úkonů, které musí útočník vykonat k překonání jednotlivých prvků PZS na jeho cestě k dosažení zabezpečovaných aktiv. Ukázka sekvenčního diagramu je na obrázku 1.1.
3. Přiřazení číselných hodnot zpoždění a detekce u jednotlivých částí diagramu
   Zpoždění udává, kolik času zabere útočníkovi zdolání určité části diagramu a detekce je pravděpodobnost, že útočníka bude při dané aktivitě detekován. Příklady hodnot zpoždění a detekce jsou na obrázku 1.1.
4. Definovat typ útoku a schopnosti útočníka
   Výchozím kritériem pro úvahu je zde povaha chráněných aktiv, od které se budou odvíjet přepokládané schopnosti útočníka a jeho vybavení.
5. Definovat typ a schopnosti bezpečnostních složek
   Zde se vychází z praktických zkušeností a znalosti procedur při nasazování konkrétních druhů bezpečnostních složek.
6. Analýza a kontrola výsledků



	Úkon	Zpoždění (min)	Detekce
1.	Překonání plotu	1.00	0.0
2.	Doběhnutí k budově	0.20	0.0
3.	Překonání vstupních dveří	2.00	0.9
4.	Doběhnutí k místnosti s aktivy	0.50	0.0
5.	Překonání dveří k aktivům	5.00	0.9
6.	Dosažení aktiv	0.10	0.0
7.	Poškození / odcizení aktiv	1.00	0.0

Obr. 1.1: Příklad sekvenčního diagramu a jemu přiřazených hodnot zpoždění a detekce

SAPE

SAPE na rozdíl od jiných nástrojů nebere na vstup sekvenční diagram útoku nebo jinou podobu sledu akcí útočníka, ale pracuje s dvou rozměrnou mapou zabezpečované oblasti. Zabezpečovaná oblast je rozdělena na vrstvy, které jsou pokryty sítí rozdělující oblast na takové části, které již nejde dále dělit. K dosažení lepšího rozlišení se používá pro různé části jiné měřítko sítě. Následně je na tuto síť použit heuristický algoritmus, který určí nejzranitelnější cestu útoku. [7].

Účinnost PZS je zde vyjádřena jako pravděpodobnost přerušení útoku P_I na nejzranitelnější možné cestě. Nejzranitelnější cesta je v zabezpečené oblasti právě ta, která má nejmenší hodnotu P_I. Pravděpodobnost přerušení je funkce pravděpodobnosti detekce útoku, zpoždění útočníka a reakčního času bezpečnostních složek. Předpokládejme, že aktivum je zabezpečeno několika prvky PZS, pravděpodobnost přerušení útoku je tedy definována:

$$P_I = P(D_i)P(R|A_i) + \sum_{i=2}^{n} P(D_i)P(R|A_i) \prod_{j=1}^{i-1}(1 - P(D_j)) \tag{1.9}$$

kde:

$P(D_i)$	= pravděpodobnost detekce útoku na prvku i
$P(R\|A_i)$	= pravděpodobnost, že bezpečnostní složky (R), přeruší útok před dokončením kroku, po detekci na prvku i
$\prod_{j=1}^{i-1}(1 - P(D_j))$	= pravděpodobnost, že detekce selže a útočník přejde k dalšímu kroku

Hledání nejzranitelnější cesty je založeno na použití algoritmu A*, což je algoritmus používaný k vyhledávání cest v ohodnocených grafech. Tento algoritmus je aplikován na síť, kterou pokryjeme mapu zabezpečovaného prostoru. Algoritmus prochází celou síť z určeného počátečního bodu a hledá ve svém okolí kusy sítě, kde je nejnižší pravděpodobnost přerušení útoku P_I. Po průchodu celou sítí, tak zůstane na výstupu algoritmu celá cesta zabezpečenou oblastí až k aktivům.

Dai et al model

Jedná o relativně nový model, který slouží k analýze zabezpečení více aktiv. Tento model je založen na výpočtu rizika a využívá poměru výnosy-náklady. Výstupem analýzy je mimo určení celkového rizika systému i určení strategií pro jeho snížení včetně míry snížení rizika a tomu odpovídajícímu poměru výnosy-náklady [8].

Postup

Postup analýzy podle Dai et al modelu je rozdělen do následujících kroků:

1. Identifikace aktiv, zabezpečovacích prvků a cesty útoku přičemž předpokládáme, že:
   (a) Útočníci začínají mimo střeženou oblast a mají v úmyslu dosáhnout jednoho ze střežených aktiv.
   (b) Existuje alespoň jedna cesta, kterou se dá k aktivům dostat.
   (c) Všechny zabezpečovací prvky v cestě mají schopnost zpomalit útočníka a útočník musí vynaložit přiměřené úsilí k jejich překonání.
2. Určení efektivity každého zabezpečovacího prvku v cestě útoku Určitý prvek PZS potřebuje ke splnění úkolu střežení několik dílčích faktorů (např. detekce, zpoždění, reakce). Každý faktor má jinou pravděpodobnost splnění a může mít i jinou váhu pro hodnocení celkové efektivity daného prvku PZS. Efektivita jednoho zabezpečovacího prvku je potom dána:

$$U_j = \sum_{i=1}^{n} \omega_i \cdot log \frac{1}{1 - R_i} \tag{1.10}$$

   kde:

   j = 1,2,...,m
   i = 1,2,...,n
   R_i = pravděpodobnost úspěšného splnění daného faktoru zabezpečení
   ω_i = váha určitého faktoru, platí, že součet vah všech faktorů je roven 1

3. Určit celkovou efektivitu PZS pro každou cestu útoku
   Celková efektivita PZS na dané cestě je dána součtem efektivit jednotlivých prvků PZS

$$C(CestaU_1, U_2, ..., U_i) = \sum_{i=1}^{k} U_i \tag{1.11}$$

   kde:

   i = 1,2,...,k
   U_i = efektivita jednoho prvku PZS. Též značena $C(U_i)$ jako náklady útočníka na jeho překonání.

4. Zhodnotit riziko pro každé aktivum
   Předpokládáme, že útočník si zvolí cestu s nejslabším zabezpečením a určíme efektivitu zabezpečení jednotlivých aktiv:

$$E(aktivum) = Min(C(Cesta_1), C(Cesta_1), ..., C(Cesta_n)) \tag{1.12}$$

   Riziko útoku vychází z rovnice 1.2 přičemž uvažujeme, že s vyšší efektivitou zabezpečení se snižuje pravděpodobnost úspěšného útoku $P_{S/A}$. Tento vztah je pro jedno aktivum vyjádřen rovnicí:

$$E(aktivum) = log\frac{1}{P_{S/A}} \tag{1.13}$$

   V případě více střežených aktiv můžeme rovnici 1.2 po dosazení rovnice 1.13 za $P_{S/A}$ vyjádřit ve tvaru:

$$Risk = \sum_{i=1}^{n}(P_A\frac{1}{e^{E(aktivum_i)}}C_i) \tag{1.14}$$

   kde:

   P_A = pravděpodobnost uskutečnění útoku
   C_i = cena aktiva i

5. Určit poměr výnosy-náklady pro každé aktivum a případně navrhnout změny v systému ke snížení rizika
   Poměr výnosů a nákladů umožňuje zvážit náklady na navrhované zabezpečení, případně ukazuje na míru změny rizika při úpravách již existujícího systému. Poměr výnosy-náklady pro určitou navrženou změnu v systému lze vypočítat:

$$\frac{Výnosy}{Náklady} = \frac{Riziko\,po\,navržených\,změnách - Riziko\,před\,změnami}{Cena\,návrhu} \tag{1.15}$$

1.4.3 Volba metody

Z dostupných zdrojů týkajících se kvantitativních analytických metod vyplývá, že mezi nejstarší a zároveň nejrozšířenější patří metody EASI a SAVI. Novější metody včetně metod Dai et al a SAPE mají s metodami EASI a SAVI společný teoretický základ a liší spíše v přístupu k výpočtu některých hodnot, než že by přicházely s úplně novou technikou hodnocení účinnosti PZS. Metoda SAPE zatím nezaznamenala velké využití a její implementaci jsem v rámci této práce vyhodnotil jako časově příliš náročnou. Postup metody SAVI je sice popisován v mnoha odborných textech, ale konkrétní způsoby výpočtů pravděpodobnosti P_I v nich chybí. Texty od původních autorů metody jsou k dostání na vyžádání na vědeckých serverech avšak během zpracování této práce jsem od nich neobdržel žádnou odpověď. Metoda Dai et al je ve svém původním textu dobře popsaná, avšak pro potřeby této práce jsem vyhodnotil, že její algoritmus počítající všechny možné cesty útoku, by byl pro rozsah této práce příliš výpočetně náročný, zvláště u větších systémů. Metoda Dai et al také, podobně jako metoda SAPE, zatím nebyla často aplikována v praxi, takže lze jen těžko hodnotit její přesnost. Nakonec jsem si jako metodu kvantitativní analýzy PZS pro navrhovanou aplikaci zvolil metodu EASI. K tomuto rozhodnutí přispěla dobrá dostupnost odborné dokumentace, vzorových příkladů, které můžu použít pro porovnání výsledků při implementaci a také fakt, že se jedná o jednu ze základních používaných analytických metod, ze které vychází novější metody.

1.5 Komponenty používané při realizaci PZS

1.5.1 Ústředny

Úkolem ústředny, která tvoří jádro celého PZS je přijímat a vyhodnocovat signály z připojených detektorů, ovládat nastavení systému a signalizačních prvků a zajišťovat diagnostiku systému. V následující části, která se věnuje ústřednám jsem vycházel pedevším z textů [1] [9]. Ústředny mají vlastní napájecí zdroje, které slouží jako zdroje napětí pro samotnou ústřednu a kabelem připojené detektory a signalizační zařízení. Ostatní zařízení PZS bývají napájena vlastním přívodem. Napájení ústředny je zálohováno pro případ výpadku dodávky elektrické energie záložní baterií, většinou 12V. Vzhledem k důležité roli ústředny v rámci PZS je doporučeno ji umisťovat uvnitř střeženého prostoru v části nejvyšším stupněm zabezpečení. Kvůli zvýšení odolnosti proti sabotáži PZS jsou ústředny stejně jako senzory vybavovány sabotážními kontakty, což jsou většinou mechanické kontakty sepnuté zavřeným krytem daného zařízení.

Ústředny bývají děleny podle způsobu komunikace s ostatními prvky na:

- kabelové - senzory a další zařízení jsou připojeny pomocí kabelu
- radiové - senzory a další zařízení jsou připojeny bezdrátově

Některé dostupné ústředny podporují oba způsoby komunikace nebo mohou být jejich původní komunikační schopnosti rozšířeny doplněním o příslušné komunikační moduly.

Kabelové ústředny

I přes možné komplikace při složitějších instalacích zůstávají kabelové ústředny hodně rozšířené, hlavně díky větší odolnosti proti rušení a tím pádem i větší spolehlivosti. Kabelové ústředny se dále dělí na několik podkategorií, které budou dále rozebrány.

Smyčkové ústředny

Do smyčkové ústředny se detektory připojují pomocí smyček. Smyčky jsou jednoduché obvody, na které se připojují kontakty jednotlivých detektorů. Smyčkové ústředny podporují více připojení více smyček a identifikaci původu poplachu. Zpravidla je také možné ústředny doplnit o rozšiřující karty pro podporu dalších smyček [1].

Smyčky mohou mít nastaveno různé chování a sice:

- okamžité - poplach je vyvolán okamžitě po narušení zastřeženého prostoru
- zpožděné - po aktivaci je nejprve vyslán signál, po dobu jehož trvání může uživatel systém odstřežit (při vstupu) nebo opustit oblast, která bude následně zastřežena (často využívané v domácnostech)
- 24-hodinové - systém je sledován i v případě odstřežení, např. proti případné sabotáži.

Typy chování a uspořádání smyček se liší podle typu a výrobce a výše uvedené chování tedy není úplné. Ústředny, které mají více jak jednu smyčku je většinou možné zastřežit nebo odstřežit i částečně.

Sběrnicové ústředny

Sběrnicové ústředny jsou s ostatními zařízeními v PZS propojeny pomocí datové sběrnice. Zařízení se k této sběrnici připojují zpravidla paralelně. Standardy využívané pro komunikaci sběrnicové ústředny se liší podle výrobce a typu ústředny, ale obvyklé je využití standardu RS-485. Ústředna v pravidelných intervalech posílá připojeným zařízením dotazy na jejich stav, pokud nepřijde odpověď detektoru je signalizována porucha nebo sabotáž daného zařízení. Protože má každé připojené zařízení svůj vlastní identifikátor je snadné zjistit, kde přesně došlo k poruše nebo vyvolání poplachu. Výhodou sběrnicových ústředen je přehlednější kabeláž a přesná identifikace zařízení a poplachů. Právě přesná identifikace může být, ale zdrojem vyšších nákladů, protože ke sběrnici nelze připojovat běžná zařízení, která bychom mohli připojit například ke smyčkové ústředně [1].

Hybridní ústředny

Hybridní ústředny jsou kompromisem mezi smyčkovými a sběrnicovými ústřednami. Na sběrnici se k ústředně připojují takzvané koncentrátory, do kterých se připojují smyčky s připojenými detektory. Pokud na každou smyčku připojíme jeden detektor, získáme schopnost přesné identifikace zařízení stejně jako čisté sběrnicové ústředny [1].

Radiové ústředny

Rádiové ústředny užívají bezdrátový přenos dat ke komunikaci s připojenými senzory a dalšími zařízeními PZS. Přenos dat je často veden v bezlicenčních pásmech na kmitočtech 433 MHz, 868 Mhz a 2,4 GHz. Ke komunikaci je využíván simplexní (starší detektory) a duplexní (novější detektory) provoz. Ústředna pak komunikuje s připojenými zařízeními v někdy až několika minutových intervalech. Z uvedených charakteristik vyplývají výhody a nevýhody bezdrátových ústředen:

- není nutné zasahovat do konstrukce střežené budovy nebo prostoru kvůli absenci kabeláže
- jistá větší volnost při návrhu systému
- zařízení v PZS jsou napájena bateriemi, které je nutné kontrolovat a měnit
- při návrhu a kontrole systému je potřeba brát v potaz možné rušení použitého přenosového pásma
- dosah některých zařízení může být díky stavební konstrukci omezen
- delší prodleva mezi hlášeními detektorů může usnadnit případný útok

1.5.2 Ovládací, signalizační a akční prvky

Ovládací prvky

K ovládání, zastřežení a odstřežení, a nastavování systémů využíváme několik druhů ovládacích prvků. Bezdrátové ovladače slouží k odstřežení nebo zastřežení daného systému pomocí zpráv s plovoucím kódem (například dálkové ovládání vjezdové brány). Ovládací klávesnice, které umožňují zastřežit nebo odstřežit určité části systému a jejich jednoduchou diagnostiku (indikaci zastřežení, poruchy, poplachu). K ovládacím klávesnicím je často potřeba se přihlásit pomocí vlastního číselného hesla PIN, pomocí RFID čipu nebo jejich kombinací. Programové vybavení může zobrazovat stavy detektorů a jiných zařízení na půdorysu střeženého prostoru. Zároveň je možné upravovat oprávnění přístupu jednotlivých uživatelů a diagnostikovat celý systém [1].

Signalizační prvky

Ze signalizačních prvků jsou významné zejména sirény [1] [9]. Exteriérová siréna slouží k akustické i optické signalizaci poplachu v okolí střeženého prostoru. Zvuková signalizace exteriérové sirény trvá pouze určitou dobu a následně už je poplach indikován pouze optickou signalizací. Exteriérová siréna se umisťuje vně střežených budov, mimo dosah případného útočníka, ale zároveň tak, aby byla dobře vidět a slyšet její signalizace. Sirény i jejich kabelové přívody by měly být zabezpečeny proti narušení nebo zničení například použitím sabotážních kontaktů nebo skrytím kabelového vedení. Externí siréna může být vybavena záložním napájením, které v případě jejího odpojení od stálého přívodu zajistí spuštění poplachu. Vnitřní sirény často neobsahují optickou signalizaci nebo nemusí mít záložní napájení. Vnitřní sirény však– signalizují poplach akusticky po celou dobu jeho trvání a mimo upozornění autorizovaných osob tak mohou útočníkovi značně znepříjemnit pobyt ve střeženém prostoru .

Akční prvky

Jde o zařízení, která podle potřeb PZS, případně jeho uživatelů, provádí určitou činnost. Například se může jednat o automatické rozsvěcení světel nebo zamlžovací systém jehož cílem je zpomalit postup útočníka tím, že narušenou oblast vyplní hustou mlhou.

1.5.3 Senzory

Vnitřní detektory

Jsou určeny k detekci případného útočníka uvnitř střeženého prostoru. Oproti venkovním perimetrickým detektorům, které v mnoha případech využívají stejných principů detekce nejsou nijak zodolněné, což se ale na druhou stranu může projevit nižšími pořizovacími náklady.

Pasivní infračervené detektory (PIR)

Jde o nejčastěji používaný detektor pohybu uvnitř i vně střeženého prostoru. PIR (pasivní infračervený detektor – Passive Infra-Red) detektor pracuje na principu snímání změn teploty oproti okolí, tedy přítomnost nějakého zdroje infračerveného záření (útočníka) v zastřežené oblasti. PIR detektor k tomu využívá pyroelektrický jev, tedy elektrické nabíjení povrchu těles vlivem působení tepla. Jádrem PIR detektoru je elektronická součástka skládající se z destiček z pyroelektrického materiálu, která nám umožňuje snímat rozdíl infračerveného záření [1] [9].

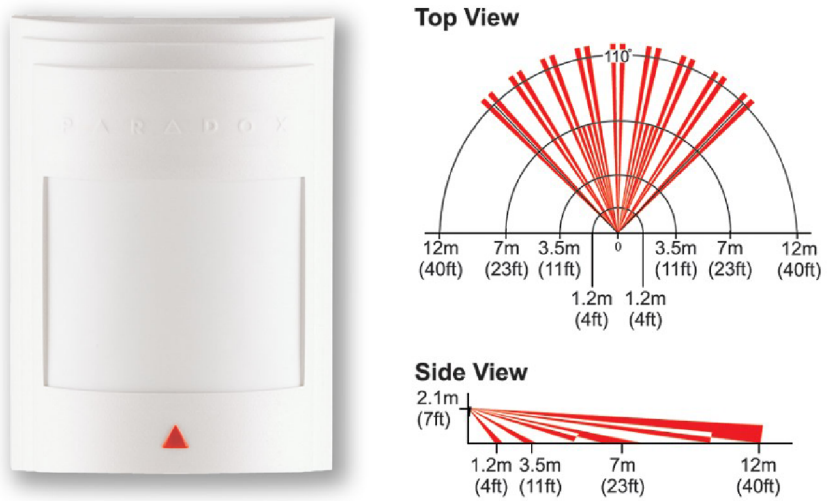
Základní vlastnosti PIR detektoru:

- nevyzařuje žádnou energii, navzájem se neovlivňují, mohou se překrývat
- falešné poplachy od zvířat, při rychlých teplotních změnách prostředí
- slabá rozlišovací schopnost při velkých teplotách okolního prostředí
- kvůli principu snímání záření nemohou detekovat statické zdroje záření

Citlivost detekce dosáhneme u PIR detektoru umístěním pole štěrbin před samotný PIR senzor a tím tak uměle napomáhat vytváření rozdílu potenciálu záření, které je snímáno.

Dosah PIR detektoru je možné zvýšit použitím čoček. Kromě obyčejných čoček se nejčastěji používají Fresnelovy čočky, které vykazují menší optické ztráty a navíc díky přechodům tvořeným jejich tvarem vznikají optické vady, které mají stejnou funkci jako pole štěrbin. Různým uspořádáním Fresnelových čoček nebo například použitím soustavy lomených zrcadel lze různě tvarovat snímací charakteristiku celého PIR detektoru. Pokrytí PIR detektoru lze také značně vylepšit použitím více

samostatných PIR senzorů. Dosah, citlivost, a snímací charakteristika jsou důležité vlastnosti PIR detektoru, které je potřeba zvážit před jeho použitím.



Obr. 1.2: PIR detektor DM60 pro instalaci na sběrnici s jeho snímací charakteristikou. [10]

Aktivní infračervené detektory (AIR)

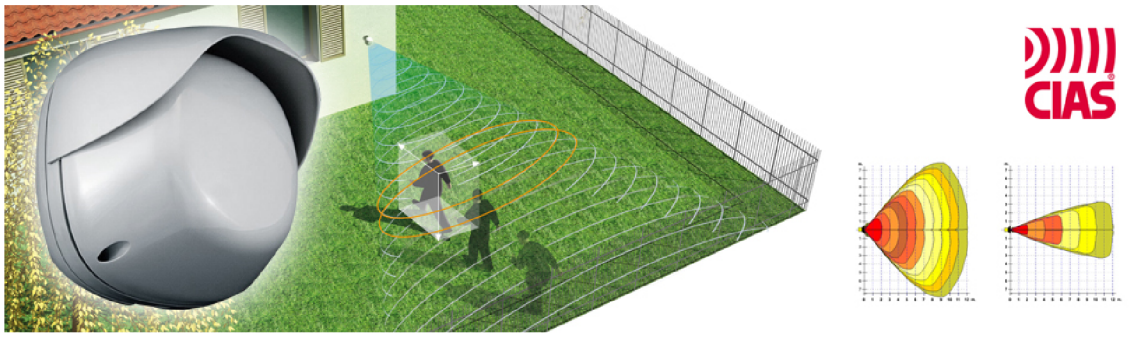
Aktivní infračervené detektory jsou odpovědí na nižší rozlišovací schopnosti a nemožnost detekce statických zdrojů infračerveného záření PIR detektorů. AIR detektory vysílají pulsy infračerveného světla a vyhodnocují úrovně přijatých odražených signálů. Pokud se ve střeženém prostoru pohybuje útočník, změní se hodnota pulzů a dojde k vyhlášení poplachu. AIR detektory tak zvládnou detekovat i pohyb objektů s malým nebo žádným vyzařování tepla. Tyto detektory mají však díky své aktivní povaze větší spotřebu el. energie a vzhledem k tomu, že jsou samy zdrojem infračerveného záření, je relativně snadné zjistit, kde jsou instalovány [1] [9].

Aktivní ultrazvukové detektory (US)

Vyzařují energii ve formě signálu v ultrazvukovém pásmu se stálou frekvencí a amplitudou, který je po odrazu od objektů ve střeženém prostoru opět přijímán a vytváří tak přehled o celé oblasti. Pokud do střeženého prostoru vstoupí útočník, změní se tím podle Dopplerova jevu část frekvence přijímaného signálu a detektor vyvolá poplach. Některé předměty mohou pohlcovat ultrazvukové vlnění (pěnové materiály, látky) a snižovat tak citlivost detektorů. Umisťování více US detektorů v jedné místnost je podmíněno tím, že se detektory navzájem nebudou ovlivňovat (například stejnou frekvencí signálu)[1].

Aktivní mikrovlnné detektory (MW)

Stejně jako US detektory využívají Dopplerova jevu [1]. K detekci používají elektromagnetické vlnění v pásmech 2,5 GHz, 10 GHz a 24 GHz. Mikrovlnné detektory jsou schopny detekovat pohyb i přes stěny, a proto je při jejich umisťování prát ohled na jejich dosah a citlivost. Citlivost MW detektoru klesá se vzrůstající vzdáleností od detektoru. Další hledisko, se kterým je potřeba počítat při instalaci je elektromagnetické rušení (zařivky, blízká el. zařízení), které silně ruší MW detektory.



Obr. 1.3: Aktivní MW detektor ve venkovním provedení. [11]

Kombinované detektory

Za účelem eliminace některých výše uvedených nevýhod existují kombinované detektory, které pod jedním krytem skrývají více detektorů snímajících různé jevy. K vyhlášení poplachu je zpravidla potřeba, aby byly všechny jednotlivé části aktivovány současně. Toto nám umožňuje kombinovat nastavení citlivostí jednotlivých detektorů, které by v samostatném provedení spouštěly falešné poplachy.

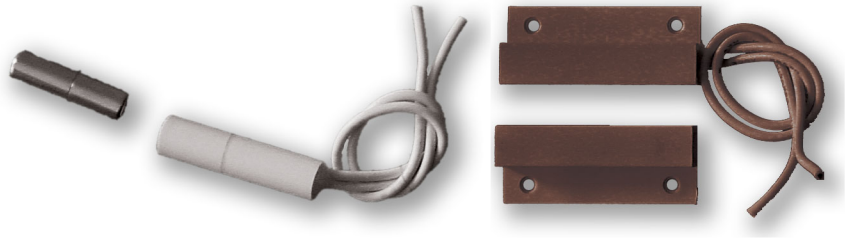
Plášťové detektory

Slouží k detekci útočníka při pokusu o proniknutí do budovy, ve které se nachází střežená aktiva. Kromě venkovních detektorů a zábran mohou být první překážkou na cestě případného útočníka. Mohou jej tak odradit ještě než se mu podaří ukrást nebo poškodit střežená aktiva. V následujícím textu si uvedeme ty nejčastěji používané[1].

Magnetické kontakty

Magnetické kontakty slouží k detekci otevření dveří, oknech, nebo jiných podobných stavebních otvorů. Magnetický kontakt se skládá z permanentního magnetu a jazýčkového relé. Permanentní magnet se instaluje do pohyblivé části (okna, dveře) a relé do rámu. Pokud jsou například dveře zavřené a relé je v blízkosti magnetického pole magnetu, dojde k sepnutí kontaktů relé a smyčkou protéká proud. Pokud dveře

někdo otevře, dojde k přerušení smyčky a signalizaci poplachu. Magnetické kontakty je podobně jako ostatní zařízení možné jistit proti sabotáži připojením na sabotážní smyčku ústředny PZS[1].



Obr. 1.4: Vlevo: zavrtávací magnetický kontakt. Vpravo: povrchový magnetický kontakt. [10]

Otřesové detektory

Otřesové detektory se používají na části stavební konstrukce, které by mohl případný útočník chtít překonat bouráním, vrtáním, řezáním nebo jinou podobnou aktivitou. Otřesové detektory mohou být vybaveny buďto piezoelektrickým nebo kuličkovým snímačem. U piezoelektrického snímače je piezoelektrický krystal přitlačen na střežený objekt. Při vibracích se na krystalu díky piezoelektrickému jevu objeví proměnlivé elektrické napětí. Pokud je toto napětí vyhodnoceno útok, dojde ke spuštění poplachu. U kuličkového snímače je uvnitř snímače malá ulička, která elektricky spojuje vnitřní kontakty. Pokud dojde k vibracím, kulička se začne pohybovat a náhodně propojovat kontakty. Vzniklý elektrický proud se opět vyhodnocuje a při rozpoznání příznaků útoku dojde k vyhlášení poplachu. Otřesové detektory je kvůli správné funkci nutné pevně připevnit ke střeženému tělesu.

Obr. 1.5: Bezdrátový detektor otřesu nebo náklonu JA-82SH. [12]

Detektory rozbití skla

Tyto detektory slouží k detekci rozbití oken, výloh a jiných podobných částí střežených budov. U detektorů rozbití skla se využívá typů snímání, a sice piezoelektrického a akustického. Piezoelektrické snímání pracuje podobně jako otřesové detektory s vibracemi okenní tabule a akustické snímání vyhodnocuje zvuky tříštění skla. Ke spuštění poplachu je nutné vyhodnotit signál malé frekvence následovaný signálem vysoké frekvence, což odpovídá tlaku na tabuli skla následovanému jejím roztříštěním. Při instalaci detektorů rozbití skla je nutné dbát pokynů od výrobce a respektovat citlivost a snímací charakteristiky daných detektorů. Předejde se tak například falešným poplachům způsobeným vibracemi a okolními zvuky v blízkosti střežených oken.

Obr. 1.6: Detektor rozbití skla GBS-210. [12]

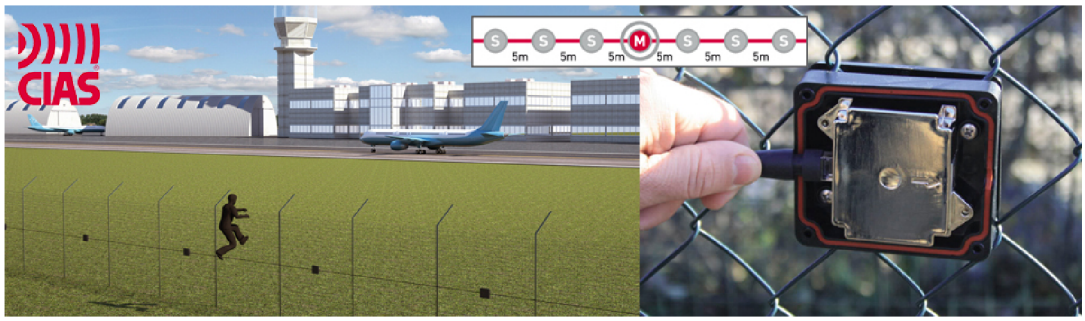
Venkovní detektory

Venkovní detektory [1] [9] jsou první instancí PZS, která nám umožňuje detekovat narušení zastřeženého prostoru a to ještě vně budov, kdy útočník ještě neměl šanci napáchat větší škody. Podle způsobu instalace dělíme venkovní detektory na:

- plotové
- zemní
- přehradné

Plotové detektory mají velké množství provedení. Základním principem je měření mechanických otřesů plotu. Starší metody využívají detektory tahu ve vybraných drátech plotu, u kterých jsou dráty na jednom konci pevně spojeny se sloupkem a poté volně vedeny až na druhý konec k detektorům s piezoelektrickými snímači. Novější plotové detektory pracují s takzvanými otřesovými kabely, které jsou volně zavěšené na plot, aby mohly detekovat otřesy v plotu 1.7. Tyto kabely jsou založeny na různých typech indukce (magnetická, elektromagnetická, elektrostatická). Mezi

nejnovější metody patří měření otřesů pomocí bezdrátových akcelerometrů připevněných na plot.



Obr. 1.7: Plotový detektor otřesů. [11]

Zemní detektory jsou umisťovány do země podél hranice střeženého perimetru. Základními příznaky útoku jsou zde mechanické otřesy nebo změny elektromagnetického pole. Na principu detekce tlaku funguje optovláknový zemní detektor. V případě tlaku nebo otřesů dochází k vychylování a deformaci světelného paprsku procházejícího optickým kabelem. Tyto změny můžeme měřit a vyhodnotit tak případně jako útok. Optovláknové detektory mohou střežit velmi dlouhé zóny v řádech kilometrů. Zemní snímače otřesů se skládají z permanentního magnetu, kolem kterého je volně navinutá cívka. Při otřesech se magnet a cívka navzájem pohybují a tím se i průběžně mění indukované elektrické napětí na cívce. Jestliže napětí překročí stanovené hodnoty, je vyhlášen poplach. Snímače otřesů se umisťují v řadě na hranici střeženého pozemku. Snímače změny elektromagnetického pole sestávají ze dvou šterbinkových koaxiálních kabelů, jedním pro vysílání a druhým pro příjem. Štěrbinky umožňují vysílacímu kabelu vyzařovat část energie, kterou zachycuje přijímací kabel. Pokud přes kabely projde útočník, změní tím intenzitu el. mag. pole a dojde k signalizaci poplachu.

Přehradné detektory jsou instalovány nad zemí podél střeženého pozemku. Základním principem je vysílání a následné vyhodnocení přijímaného elektromagnetického záření. Přehradné detektory dělíme na dvoustranné a jednostranné. Dvoustranné detektory mají vysílač i přijímač jako samostatná zařízení umístěná naproti sobě zatímco jednostranné detektory mají vysílač i přijímač v jednom zařízení. Pokud útočník naruší paprsek vysílaného záření, dojde k přerušení vysílaného nebo změně času odraženého paprsku a je signalizován poplach. Současně jsou oblíbené jednostranné laserové detektory. Ty umožňují vysílaný paprsek rozptylovat pomocí zrcadel do kruhové výseče, jejíž rozměry a tvar je možné upravovat dle potřeb uživatele.

Obr. 1.8: Vlevo: infra závora. Vpravo: mikrovlnná závora. [11]

2 Software pro návrh a analýzu PZS

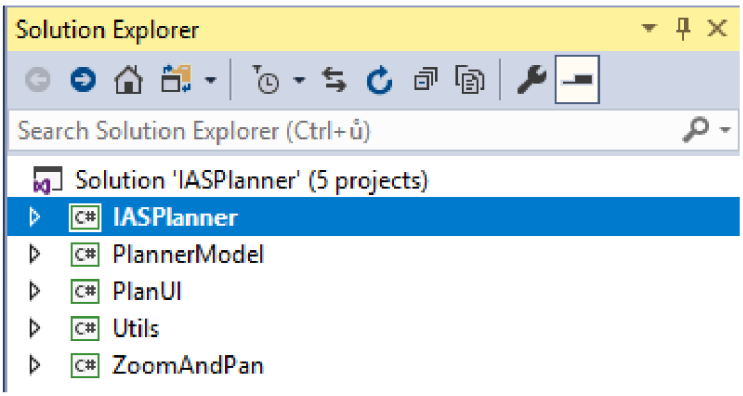
V této kapitole je popsána aplikace *IASPlanner*, kterou jsem vytvořil v rámci praktické části zadání diplomové práce. Je rozebrán výběr programovacího jazyka, model návrhu aplikace, provedení a funkce GUI (grafické uživatelské rozhraní – Graphical User Interface) a implementace metody kvantitativní analýzy EASI.

2.1 Struktura aplikace a použité programovací techniky

Aplikace IASPlanner je napsána v objektově orientovaném programovacím jazyce C#. Jedná se o hojně rozšířený programovací jazyk se snadnou implementací desktopových aplikací. Jako vývojové prostředí jsem použil MS Visual Studio 2017. GUI využívá technologie WPF (Windows Presentation Foundation) [15], která dovoluje poměrně snadně vytvářet graficky bohatá prostředí s velkou variabilitou a funkčností.Struktura aplikace je rozvržena podle návrhového modelu MVVM (Model-View-ViewModel) jehož podrobnosti řeší [13].

Při implementaci aplikace jsem vycházel ze zkušeností nabraných při zpracování předchozí práce [14], která se zabývala návrhem a tvorbou softwarové aplikace pro modelování topologií počítačových sítí. Jádro a základní funkce předchozí práce splňovali požadavky pro praktickou část diplomové práce a tak jsem jich využil, kde to bylo možné.

Na základě použití návrhového modelu MVVM je řešení programu aplikace rozděleno do celkem pěti samostatných projektů. Každý projekt řeší specifické funkce aplikace bude řešení aplikace ve vývojovém prostředí sestávat minimálně ze třech samostatných projektů, tak jak ukazuje obrázek 2.1, případně dalších pomocných projektů podle potřeby. Každý projekt je zodpovědný za určitou část celé aplikace a s tím spojenou funkcionalitu.



Obr. 2.1: Ukázka rozvržení programu podle MVVM

IASPlanner je projekt aplikace. Obsahuje definici prvků GUI metodu EASI reprezentaci pracovní plochy.

PlannerModel obsahuje třídy reprezentující objekty v zákresu. Zpracovává pouze údaje o těchto objektech.

PlanUI obsahuje třídy a funkce pracující s grafickými reprezentacemi objektů zákresu. Nezasahuje do dat objektů.

Utils obsahuje pomocné metody pro konverze datových typů a jiné výpočty.

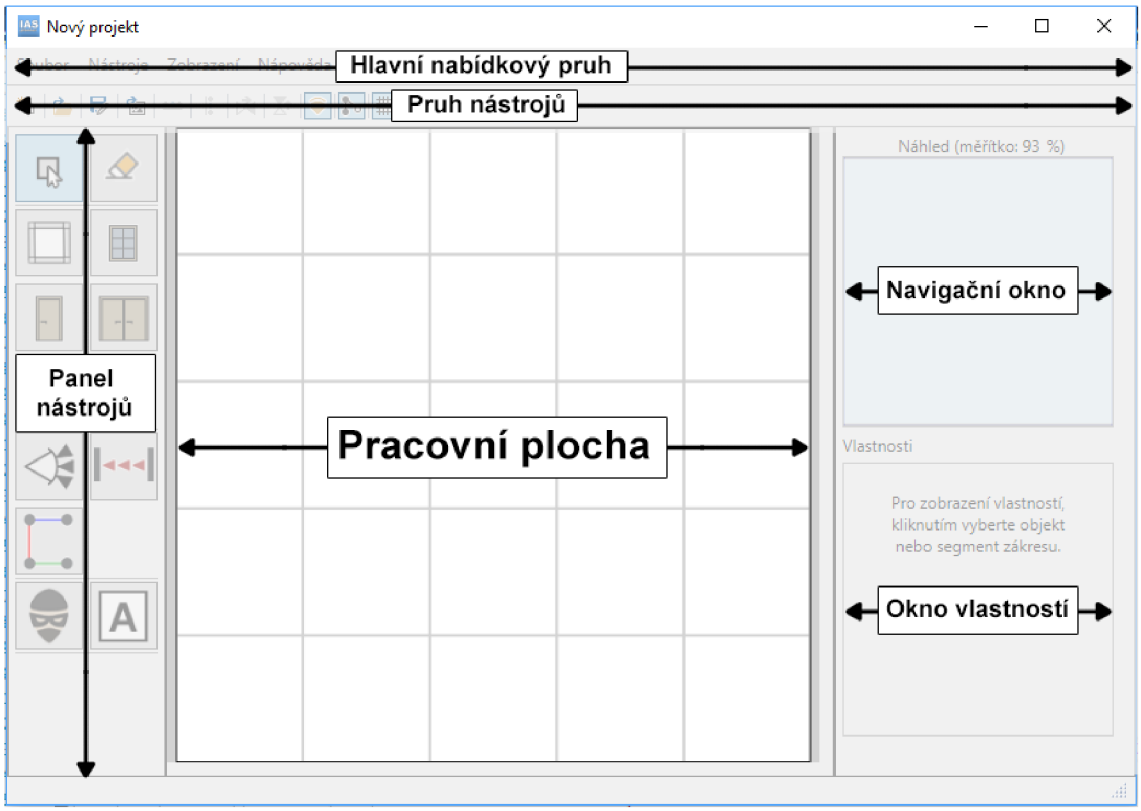
ZoomAndPan jsou pomocné metody pro pohyb, přiblížení a ovládání pracovní plochy.

2.2 Uživatelské rozhraní a jeho možnosti

Technologie WPF dovoluje vytvořit funkční a graficky bohatá uživatelská rozhraní. K tomu využívá vlastní programovací jazyk XAML, který není nepodobný jazyku HTML. XAML představuje poměrně jednoduchou metodu jak vytvořit kód pro uživatelské rozhraní, který je přehledně oddělen od zbytku kódu aplikace [13][15]. To samozřejmě velmi usnadňuje testování a případné úpravy GUI.

2.2.1 Rozvržení uživatelského rozhraní

Uživatelské rozhraní je navrženo tak, aby měl uživatel všechny důležité ovládací prvky ihned po ruce. Na obrázku 2.2 je zobrazeno primární okno aplikace s vyznačeným rozvržením hlavních ovládacích prvků.



Obr. 2.2: Hlavní prvky grafického uživatelského rozhraní

Pracovní plocha

Pracovní plocha představuje jakési plátno, na které uživatel vkládá objekty a prvky PZS a vytvořil tak kompletní zákres. Pracovní plocha je pokryta metrovou sítí, která zlepšuje orientaci a usnadňuje kreslení půdorysů. Zobrazení metrové sítě lze vypnout v hlavním nabídkovém pruhu z položky Zobrazit nebo z pruhu nástrojů v hlavním okně.

Hlavní nabídkový pruh

Hlavní nabídkový pruh obsahuje funkce ovládající aplikaci jako celek stejně jako některé dodatečné funkce. Z hlavního nabídkového pruhu se například spouští funkce kvantitativní analýzy. Hlavní nabídkový pruh obsahuje čtyři položky:

Soubor - odsud lze vytvořit nový projekt, načíst nebo uložit projekt, exportovat projekt do obrazového souboru a ukončit běh aplikace.

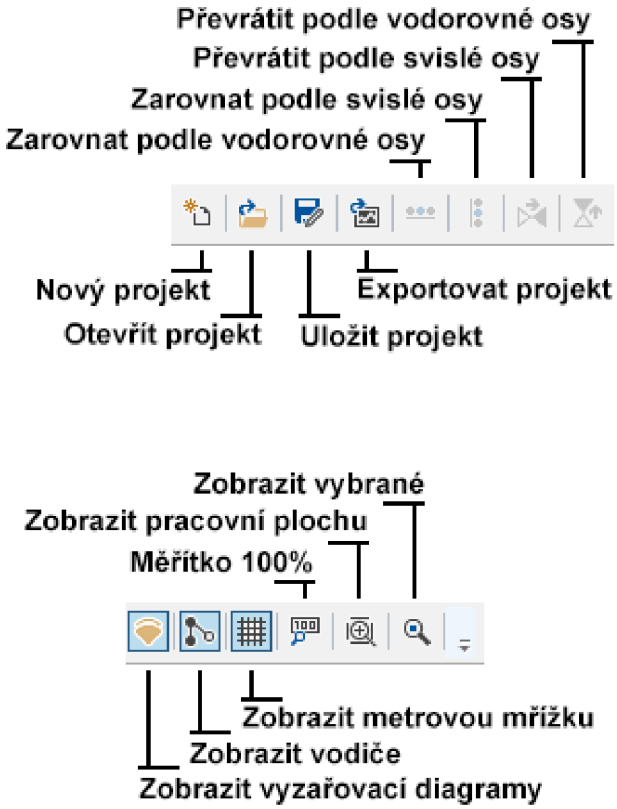
Nástroje - zde jsou funkce umožňující práci s objekty v zákresu. Odsud se také spouští kvantitativní analýza.

Zobrazit - umožňuje zapínat, vypínat a upravovat zobrazení některých objektů zákresu.

Nápověda - odsud lze zobrazit dialogové okno obsahující nápovědu pro práci s aplikací IASPlanner.

Pruh nástrojů

Pod hlavním nabídkovým pruhem je umístěn pruh nástrojů, který uživateli zpřístupňuje doplňkové funkce aplikace aniž by musel prohledávat hlavní nabídkový pruh aplikace. Rozložení pruhu a význam ikon je znázorněno na obrázku 2.3.



Obr. 2.3: Popis pruhu nástrojů

Některé nástroje dostupné z pruhu nástrojů ovlivňují nebo pracují s určitou skupinou objektů. Vysvětlení některých nástrojů:

Měřítko 100% - nastaví měřítko na 100%.

Zobrazit vybrané - přiblíží vybrané prvky nebo celou oblast zákresu.

Zobrazit pracovní plochu - zobrazí celou pracovní plochu.

Zarovnat dle vod. osy - zarovná vybrané objekty podle vodorovné osy. Zarovnávat lze více objektů různých typů dohromady.

Zarovnat dle svis. osy - zarovná vybrané objekty podle svislé osy. Zarovnávat lze více objektů různých typů dohromady.

Převrátit podle vod. osy - převrátí vybrané dveře podle vodorovné osy.

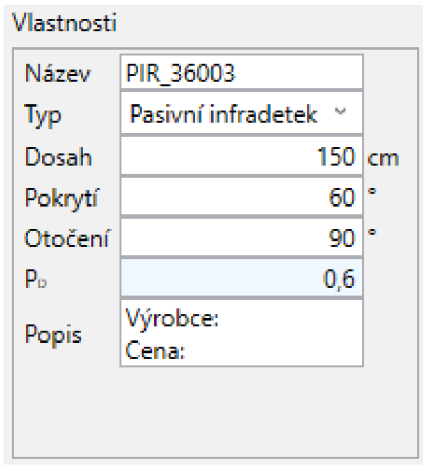
Převrátit podle svis. osy - převrátí vybrané dveře podle svislé osy.

Panel nástrojů

Panel nástrojů je umístěn na levém okraji primárního okna aplikace a obsahuje ve dvou sloupcích vedle sebe umístěny ovládací prvky určené ke vkládání, mazání a manipulaci s objekty zákresu. Všechny nástroje jsou opatřeny interaktivním popiskem funkce a jsou dále popsány v nápovědě aplikace.

Okno vlastností

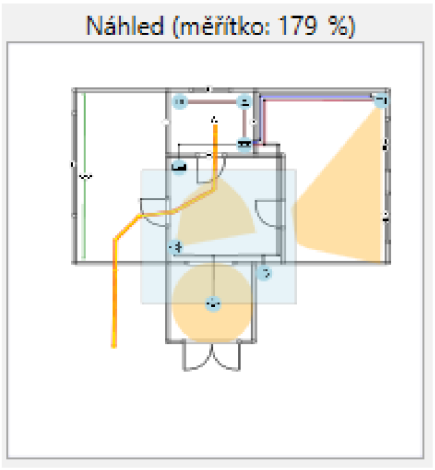
Okno vlastností je ve výchozím stavu, kdy není vybrán žádný objekt zákresu, prázdné. Po vybrání nějakého objektu se na základě jeho typu zobrazí příslušné okno vlastností. Okna vlastností obsahují například položky jako název, popis, provedení konstrukce, materiál nebo instalované detektory. Všechny možnosti budou rozebrány dále a jsou uvedeny také v nápovědě aplikace.



Obr. 2.4: Příklad okna vlastností objektu.

Navigační okno

Navigační okno slouží uživateli ke zlepšení přehledu nad většími zákresy. Nad horním okrajem okna se nachází aktuální měřítko zobrazení pracovní plochy.



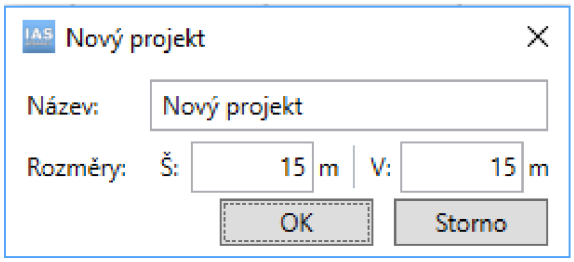
Obr. 2.5: Navigační okno aplikace

2.3 Ovládání aplikace IASPlanner

V této části jsou popsány některé zvláštní funkce aplikace IASPlanner a postupy ovládání. Popsané funkce jsou dostupné buďto z hlavního nabídkového pruhu, pruhu nástrojů anebo pomocí klávesových zkratek a tlačítek myši.

2.3.1 Vytvoření nového projektu

Nový projekt lze vytvořit pomocí tlačítka Nový projekt, které je dostupné buďto z položky Soubor hlavního nabídkového pruhu nebo z pruhu nástrojů, viz obrázek 2.3. Po kliknutí na tlačítko se zobrazí dialogové okno, ve kterém může uživatel nastavit rozměry zákresu a název projektu, viz obrázek 2.6. Po stisknutí tlačítka OK dojde k vytvoření nového projektu.



Obr. 2.6: Dialogové okno vytvoření nového projektu

2.3.2 Přejmenování projektu

Stávající projekt je možné přejmenovat pomocí volby Přejmenovat projekt z hlavního nabídkového pruhu nebo kliknutím na stejnojmenné tlačítko v pruhu nástrojů. Do

zobrazeného dialogového okna lze zadat nové jméno projektu a potvrdit tlačítkem OK.

2.3.3 Vkládání, odstranění a manipulace s objekty

Aplikace IASPlanner obsahuje několik základních typů objektů. Od těchto typů se odvíjí možnosti manipulace s nimi.

Vkládání objektů

a) Objekty typu Překážka

Mezi tyto objekty se řadí překážka, okno, otvor a infra závora. Postupným klikáním LTM (levé tlačítko myši) na pracovní plochu lze do zákresu umístit několik na sebe navazujících segmentů tohoto objektu. Po vytvoření dostatečného počtu na sebe navazujících segmentů lze cyklus přerušit kliknutím PTM (pravé tlačítko myši). Následně lze opět začít vkládat nové segmenty klikáním LTM. Je též možné začít umisťovat novou překážku napojením na hraniční bod jiné překážky nebo připojit překážku doprostřed již vytvořeného segmentu jiné překážky.

b) Samostatné objekty

Mezi samostatné objekty patří dveře, detektory, ústředna a další prvky PZS. Tyto objekty se do zákresu umisťují kliknutímLTM na pracovní plochu. Zvláštním případem jsou dveře, které lze navíc umístit do již umístěné zdi.

c) Instalované detektory

Jedná se o tři typy detektorů, a to magnetický detektor otevření, detektor rozbití skla a detektor otřesů a náklonu. Tyto detektory se do zákresu nevkládají samostatně, nýbrž se definují jako vlastnost určitého objektu. Je tedy možné kliknout řekněme na dveře a v okně vlastností jim zaškrtnou instalaci detektoru otevření. Při zaškrtnutí instalace některého z těchto detektorů se u příslušného objektu objeví ikonka instalovaného detektoru.

Obr. 2.7: Ukázka detektorů instalovaných do okna

Manipulace s objektem

Objekty lze označit pomocí kliknutí LTM. Pomocí PTM lze výběr zrušit. Pozici samostatných objektů a hraničních bodů překážek a dveří lze měnit přidržením LTM a tažením kurzoru myši. V případě dveří dochází k jejich otáčení okolo jejich druhého hraničního bodu, protože dveře mají pevnou délku.

a) Výběr více prvků najednou

Pro snazší manipulaci objekty existují dva způsoby jak jich vybrat více najednou, přičemž oba používají nástroj Výběr. V prvním případě drží uživatel stisklou klávesu `Ctrl` a klikáním LTM označuje další objekty. V druhém případě opět drží uživatel stisklou klávesu `Ctrl`, stiskne LTM a táhne kurzorem, aby se zobrazil výběrový obdélník. Označeny jsou všechny prvky, které se po skončení výběru nacházejí uvnitř obdélníku.

Odstranění objektu

Objekty ze zákresu lze odstranit dvěma způsoby. V prvním případě lze při zvoleném nástroji Odstranění z panelu nástrojů kliknout LTM na zvolený objekt a ten bude odstraněn. V druhém případě stačí objekt vybrat pomocí nástroje Výběr a stisknout klávesu `Delete`. Po odstraněných objektech typu překážka a dveře zůstávají na pracovní ploše jejich hraniční body, aby nedošlo k případnému narušení zbytku zákresu.

2.3.4 Vodorovné a svislé zarovnání

Vodorovné a svislé zarovnání je dostupné z pruhu nástrojů při výběru více hraničních bodů nebo segmentů překážek, oken, otvorů atd. Po stisku tlačítka příslušného typu zarovnání dojde k zarovnání vybraných prvků podle vybrané osy.

2.3.5 Převrácení dveří podle os

Otočení podle vodorovné a svislé osy je dostupné z pruhu nástrojů při výběru objektu dveří. Lze s ním měnit směr otevírání již vložených dveří tak, abychom nemuseli předělávat napojení dveří.

2.3.6 Načtení a uložení grafu ze souboru

Aplikace IASPlanner umožňuje ukládat a následně načítat zpracované projekty ze souboru ve formátu .xml. Projekty uložené v souboru .xml jsou přehledné a některé základní údaje o grafu může uživatel vyčíst přímo z nich. Soubory je také možné

ručně upravovat, avšak nedoporučuji to dělat ve větší míře, protože by soubor při načítání nemusel projít kontrolou správnosti.

2.3.7 Export projektu do obrazového souboru

Tato funkce exportuje zpracovaný projekt do obrazového souboru ve formátu .png. Rozlišení souboru .png je dáno velikostí grafu a určuje jej aplikace sama.

2.4 Návrh PZS

Jak již bylo naznačeno v předchozích oddílech, návrh PZS v aplikaci IASPlanner sestává z umisťování několika typů objektů na pracovní plochu, jejich vzájemného propojování a upravovaná patřičných vlastností. Při upravování vlastností by měl uživatel dbát pozornost zejména při určování hodnoty P_D, která ovlivňuje schopnost detekce útoku na daném prvku a ve výsledku i účinnost celého PZS. Určování hodnot P_D není jednoduchá záležitost a je vhodné se při něm řídit buďto vlastními zkušenostmi nebo odbornými texty a postupy. [5]
Příloha **??** obsahuje příklad zákresu s veškerými jeho možnostmi. Z důvodu názornosti přílohy jsem se oprostil od pravidel návrhu PZS z reálného světa. Dále popíši typy objektů, jejich vlastnosti a základní práci s nimi.

2.4.1 Objekty v zákresu

a) Překážka

Jedná se o reprezentaci například zdi nebo plotu. Překážka je tvořena dvěma hraničními body a jejich spojnicí, viz obrázek 2.8.

Překážka má definovány tyto vlastnosti:

Název - název daného prvku.

Materiál - materiál překážky.

Tloušťka - tloušťka překážky v cm.

Instalované detektory - lze přidat detektor otřesů a náklonu.

P_D - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel na základě předpokládané efektivity daného prvku vzhledem k uvažovanému útoku.

Popis - místo pro volný popis prvku, např. uvedení konkrétního typu a výrobce.

Obr. 2.8: Grafická reprezentace překážky.

b) Okno

Okno je podobně jako překážka reprezentováno spojením dvou hraničních bodů. S oknem je možné manipulovat stejně jako s překážkou.

Okno má definovány tyto vlastnosti:

Název - název daného prvku.

Typ skla - popis použitého skla (obyčejné, tvrzené, atd.).

Provedení - provedení rámu okna (otevíratelné, pevné, atd.)

Tloušťka - tloušťka skla v mm.

Instalované detektory - lze přidat detektor otřesů a náklonu, magnetický detektor otevření a detektor rozbití skla.

$\mathbf{P_D}$ - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel na základě předpokládané efektivity daného prvku vzhledem k uvažovanému útoku.

Popis - volný popis prvku.

Obr. 2.9: Grafická reprezentace okna.

c) Dveře

Dveře jsou speciálním případem překážky. Jsou tvořeny dvěma hraničními body a spojnicí, ale umisťují se jako samostatné objekty. Dveře mají pevnou délku 90 cm.

Dveře mají definovány tyto vlastnosti:

Název - název daného prvku.

Typ dveří - typ podle použitých bezpečnostních prvků (obyčejné, bezpečnostní apod.).

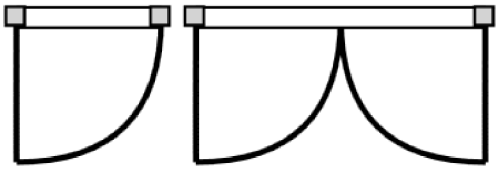
Materiál - materiál, ze kterého jsou dveře vyrobeny.

Tloušťka - tloušťka dveří v cm.

Instalované detektory - lze přidat detektor otřesů a náklonu, magnetický detektor otevření.

P_D - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel na základě předpokládané efektivity daného prvku vzhledem k uvažovanému útoku.

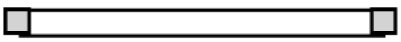
Popis - volný popis prvku.



Obr. 2.10: Grafická reprezentace dveří.

d) Otvor

Otvor se chová podobně jako okno. Jde pouze o logickou reprezentaci otvoru nebo průchodu, která může pomoci s ohraničování navrhovaných půdorysů. Otvor nemá definovány žádné vlastnosti a nelze na něj instalovat žádné detektory.



Obr. 2.11: Grafická reprezentace otvoru.

e) Prvek PZS

Jedná se o jednoduchý objekt reprezentovaný grafickou značkou daného prvku. V případě, že se jedná o vyzařující detektor, je znázorněn i diagram vyzařování. Prvky PZS se dají mezi sebou propojovat vodiči. Na základě konzultace s vedoucím diplomové práce je počet typů prvků PZS pevně stanoven. Přehled implementovaných prvků je uveden v příloze C.

Některé definované vlastnosti prvků jsou:

Název - název daného prvku.

Typ - typ prvku, podle kterého se mění grafická značka prvku.

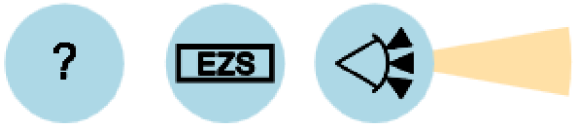
Dosah - dosah vyzařovacího diagramu v cm.

Pokrytí - úhel, který pokrývá vyzařovací diagram v jeho nejširším místě.

Otočení - úhel natočení vyzařovacího diagramu.

P_D - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel na základě předpokládané efektivity daného prvku vzhledem k uvažovanému útoku.

Popis - volný popis prvku.



Obr. 2.12: Grafická reprezentace prvků PZS.

f) Infra závora

Infra závora je opět tvořena spojnicí dvou bodů, které reprezentují vysílač a přijímač infračerveného záření. Infra závoru nelze umisťovat do překážek ani na jiné prvky. Z pohledu PZS a kvanitativní analýzy se jedná o samostatný detektor.

Infra závora má definovány tyto vlastnosti:

Název - název daného prvku.

P_D - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel na základě předpokládané efektivity daného prvku vzhledem k uvažovanému útoku.

Popis - volný popis prvku.

Obr. 2.13: Grafická reprezentace infra závory.

h) Vodiče

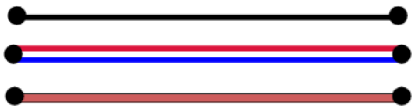
Slouží jako grafická reprezentace vodičového spojení mezi jednotlivými prvky PZS. Na výběr je i propojení pomocí datové sběrnice. Propojení prvků PZS vodičem a rozmístění vodičů nemají žádný vliv na výsledek kvantitativní analýzy.

Název - název daného prvku.

Typ - na výběr je jeden nebo dva vodiče a datová sběrnice.

Barva - umožňuje měnit barvu jednotlivých vodičů. Grafický styl datové sběrnice se nedá měnit.

Popis - volný popis prvku.



Obr. 2.14: Shora: grafická reprezentace jednoduchého, dvojitého vodiče a datové sběrnice.

i) Cesta útoku

Jedná se o spojitý sled segmentů, který vyznačuje cestu útočníka až k zamýšleným aktivům uvnitř střeženého prostoru nebo objektu. Cesta útoku musí být vyznačena, pokud chce uživatel použít metodu kvantitativní analýzy. Její použití bude vysvětleno v části týkající se metody EASI.

Obr. 2.15: Grafická reprezentace cesty útoku.

j) Aktiva

Aktiva představují jednoduchý objekt, který je cílem uvažovaného útoku na zabezpečenou oblast. Z hlediska návrhu se může jednat o fyzický objekt nebo o znázornění nějaké aktivity nebo činnosti. Aktiva mají definovánu pravděpodobnost P_D
. Ta představuje pro potřeby analýza jakýkoliv možný způsob zajištění aktiv, který si uživatel vymyslí.
Infra závora má definovány tyto vlastnosti:

Název - název daného prvku.

P_D - pravděpodobnost detekce útoku tímto prvkem. Hodnotu vyplňuje uživatel pokud jsou aktiva jakýmkoliv způsobem zajištěna.

Popis - volný popis prvku.

Obr. 2.16: Grafická reprezentace cesty aktiv.

2.5 Kvantitativní analýza metodou EASI

Pro analýzu uživatelem navrženého PZS je využita metoda EASI [5]. Analýza je možné spustit z hlavního nabídkového pruhu, viz 2.2, přes položky Nástroje, Analýza, EASI. Pokud jsou splněny vstupní podmínky pro spuštění funkce, dojde k otevření sekundárního dialogového okna obsahujícího formulář, ve kterém uživatel nastaví vstupní parametry potřebné ke spuštění analýzy. V opačném případě bude uživatel aplikací upozorněn na nedostatky v zákresu.

2.5.1 Postup analýzy

V této části textu popíši počáteční podmínky pro spuštění analýzy a postup jakým funkce pro kvantitativní analýzu vyhodnocuje pravděpodobnost přerušení útoku P_I.

Počáteční podmínky

Aby bylo možné spustit analýzu navrženého PZS, musí uživatel do zákresu umístit cestu útoku pomocí nástroje z panelu nástrojů. Další podmínkou je, aby byla umístěná cesta útoku spojitá. Podle definice v [5] je také vhodné, aby cesta útoku byla navržena tak, že každý její segment bude odpovídat překonání jednoho detektoru nebo jednoho samostatnému kroku útoku. Aplikace sice sama dokáže rozdělit segment na více kroků, ale při složitějších kombinacích detektorů a překážek, nemusí být kroky v jednom segmentu správně uspořádány.

Postup

Určení pravděpodobnosti přerušení útoku, tedy určení výsledku funkce pro metodu EASI, sestává ze dvou částí. V první části aplikace sama projde uživatelem naznačenou cestu útoku a zpracuje ji do podoby formuláře, viz tabulka 1.4.

Postup funkce pro první část:

1. Kontrola počátečních podmínek pro zpracování cesty útoku.
2. Průchod cestou útoku a detekce kolizí každého jejího segmentu s detektory a překážkami v zákresu.
3. Při detekci kolize vytvoří aplikace krok sekvenčního diagramu útoku a naplní jej potřebnými daty.
4. Všechny kroky sekvenčního diagramu jsou předány do formuláře metody EASI.
5. Zobrazení formuláře metody EASI.

Ve zobrazeném formuláři může nyní uživatel zkontrolovat vyplněná pole a případně doplnit další hodnoty. V hlavičce dokumentu se jedná o následující tři hodnoty:

$\mathbf{P_C}$ - pravděpodobnost správné komunikace. Volí se v rozmezí 0.95 až 1. [5]

Střední hodnota reakční doby - doba, za kterou jsou bezpečnostní složky schopny dostat se ke střežené oblasti.

Směrodatná odchylka reakční doby - podle [5] lze určit jako 30% střední hodnoty.

Každý řádek formuláře obsahuje následující položky, které je potřeba zkontrolovat nebo upravit dle potřeby:

Krok - automaticky vyplněný textový popis. Uživatel si jej může libovolně změnit.

$\mathbf{P_D}$ - pravděpodobnost detekce útoku na daném kroku. Hodnoty v rozmezí 0 až 1.

Zpoždění x Detekce - indikace, kdy může být útok detekován. Hodnoty jsou B - před překonáním, M - během překonávání, E - po překonání. Hodnoty představují koeficienty pro výpočet dílčích proměnných v rovnici výpočet 1.8 pro $P(R|A_i)$.

Střední hodnota zpoždění - zpoždění útočníka na daném kroku, tedy doba jakou útočníkovi trvá jeho překonání.

Směrodatná odchylka zpoždění - podle [5] lze určit jako 30% střední hodnoty.

Údaje reakční doby a zpoždění útočníka mohou být udávány v sekundách nebo minutách, důležité pouze je, aby byly oba údaje ve stejných jednotkách.

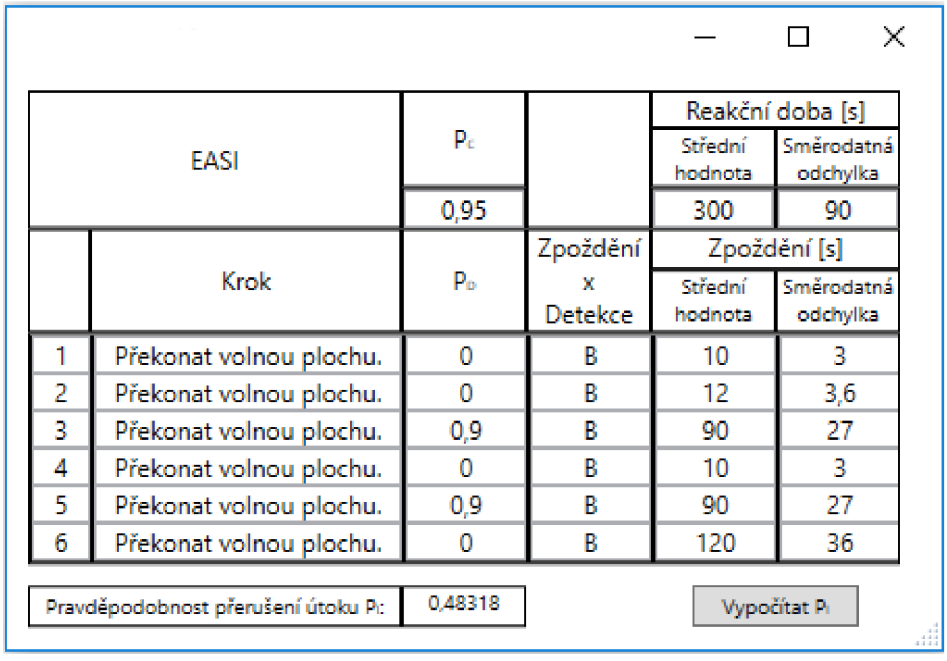
Po doplnění hodnot může uživatel spustit funkci pro výpočet pravděpodobnosti přerušení útoku P_I kliknutím na tlačítko Výpočet. P_I je vypočítána podle rovnice 1.7. K dílčím výpočtům $P(R|A_i)$ podle rovnice 1.8 slouží implementace funkce `NormSDist` známé z tabulkového procesoru MS Excel. Okomentovaný zdrojový kód metod, které počítají pravděpodobnosti $P(R|A_i)$ a P_I je přiložen v příloze D.
Při úpravách hodnot ve formuláři je potřeba, aby si uživatel uvědomil, že hodnoty P_D, P_C, reakčních časů a zpoždění je potřeba stanovit individuálně pro každý jednotlivý krok. Tyto hodnoty nemohou být stanoveny automaticky aplikací, vzhledem k velkému počtu kombinací různých vstupních faktorů, které je potřeba brát v úvahu. Například překonání dřevěných dveří s bezpečnostním zámkem může nezkušenému útočníkovi trvat stejně dlouho jako zkušenému překonání bezpečnostních kovových dveří. Schopnost detekce narušení může být různá i u detektorů stejných parametrů v závislosti na jejich umístění apod. Další položky. Proto je vhodné při stanovování těchto hodnot využít například naměřených hodnot z reálného prostředí nebo odborné literatury, například [5].

Práce s výsledky

Výsledná pravděpodobnost P_I odráží úspěšnost zabezpečované oblasti a nastavení prvků PZS v zamezení případného útoku na střežená aktiva. V případě, že by se nám výsledná hodnota zdála nízká nebo jsme chtěli pouze vyzkoušet jiné nastavení parametrů se stejnou cestou útoku, je možné prostě změnit hodnoty P_I a časy zpoždění a nechat funkci vypočítat P_I znovu. Parametry prvků PZS můžeme případně změnit následně, jakmile dosáhneme uspokojující metody P_I.

2.5.2 Ověření správnosti implementace

K ověření správnosti implementace funkce pro výpočet pravděpodobnosti P_I jsem využil příklad uvedený v [5], ve kterém je uveden postup k sestavení sešitu MS Excel, který je výpočet schopen provést. Do vlastní aplikace i do sestaveného sešitu jsem dosadil stejné vstupní hodnoty a porovnal výsledek. Na obrázcích 2.17 a 2.18 je vidět nepatrný rozdíl ve vypočítané P_I, a to přibližně 0,7%. Odchylka je způsobena rozdílným zpracováním desetinných čísel v programu MS Excel a jazykem C#. MS Excel i C# se navíc nepatrně liší přesností desetinných čísel a při dílčích výpočtech může tedy docházet k většímu přenosu z nižších řádů do vypočítaných hodnot.



Obr. 2.17: Hodnota P_I vypočítaná IASPlanner

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0,95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3,6
3	Open Door	0,9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0,9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption:	0,47604073

Obr. 2.18: Hodnota P_I vypočítaná MS Excel

3 Závěr

Problematika návrhu poplachových zabezpečovacích systémů je poměrně rozsáhlá avšak v dnešní době již velmi dobře popsaná. Důležité aspekty návrhu PZS nám určují technické normy [2] a pro kvantitativní analýzu navržených systémů již bylo navrženo mnoho metod, viz [3]. Důležité normy a základní přehled kvantitativních analytických metod jsou rozebrány v textu této práce společně s nejběžnějšími komponenty, které se používají k realizaci PZS. Metodu EASI jsem vybral jako metodu, kterou jsem dle její definice [5] implementoval do aplikace IASPlanner. Aplikace IASPlanner umožňuje zakreslení půdorysu střežené budovy a umístění vybraných typů detektorů a dalších prvků PZS. Prvky PZS je možné mezi sebou propojovat a přiřazovat jim různé vlastnosti nebo popisky. Na základě sestaveného půdorysu a navržené cestě útoku je aplikace schopna provést kvantitativní analýzu návrhu a určit jestli je daný PZS schopen s pravděpodobností P_I zastavit postup útočníka. Takto navržená a realizovaná aplikace splňuje podmínky zadání diplomové práce. Doufám však, že na základě této práce by mohly vzniknout další, které budou toto téma dále rozvíjet a že by aplikace mohla najít využití jako pomůcka při výuce.

Literatura

[1] BURDA, K., STRAŠIL, I. *Zabezpečovací systémy* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011

[2] ČSN CLC/TS 50131-7 *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace.* 46 stran. Praha: Úřad pro technickou normalizaci a státní zkušebnictví, 2011.

[3] VINTR, Z., VINTR, M., MALACH, J. *Evaluation of physical protection system effectiveness* [.pdf] Conference paper, 2012, DOI: 10.1109/CCST.2012.6393532, Dostupné z: `https://www.researchgate.net/publication/261391922`

[4] OYEYINKA, O. D., DIM, L. A., ECHETA, M. C., KUYE, A. O. *Determination of system effectiveness for physical protection systems of a nuclear energy centre* [.pdf] Science and Technology, 2014, DOI: 10.5923/j.scit.20140402.01

[5] GARCIA, M. L. *The Design and Evaluation of Physical Protection Systems* [.pdf] Sandia National Laboratories, 2001, ISBN: 0-7506-7367-2, Dostupné z: `https://archive.org/details/Design_Evaluation_of_Personal_Protection_Systems_The`

[6] SNELL, M. *Outsider assessment* [.pdf] Sandia National Laboratories: International nuclear engineering and technology, 2015, SAND2015-7719C

[7] JANG, S. S., KWAK, S. W., YOO, H., KIM, J. S., YOON, W. K. *Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection (SAPE)* [.pdf] Nuclear engineering and technology, vol. 41, 2009, DOI: 10.5516/NET.2009.41.5747

[8] DAI J., HU, R., CHEN, J., CAI, Q. *Benefit-cost analysis of security system for mutple protected assets on information entropy* [.pdf] Entropy, 2012, DOI: 10.3390/e14030571, Dostupné z: `www.mdpi.com/1099-4300/14/3/571/pdf`

[9] FIKEJS, J. *Software pro podporu projektování elektrické zabezpečovací signalizace.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. Vedoucí diplomové práce doc. Ing. Karel Burda, CSc.

[10] Variant plus, spol. s.r.o. *E-shop firmy Variant plus* [online]. Brno, 2008-2015. Dostupné z: `https://www.variant.cz/`

[11] ShopSys Enterprise, *E-shop firmy ABBAS* [online]. Ostrava, 2017. Dostupné z: `http://katalog.abbas.cz/`

[12] TELMO, a.s., *E-shop firmy Jablotron* [online]. Praha, 2017. Dostupné z: https://www.jabloshop.cz/

[13] DAJBYCH, V. *MVVM: Model-View-ViewModel* [web]. dotnetportal.cz, 2009. Dostupné z: http://www.dotnetportal.cz/clanek/4994/MVVM-Model-View-ViewModel

[14] MÜLLER, V. *Modely topologií počítačových sítí I.* Olomouc, UNIVERZITA PALACKÉHO V OLOMOUCI. Přírodovědecká fakulta, 2015. Vedoucí bakalářské práce doc. Ing. Lence Carr-Motyčková, CSc.

[15] VÁVRA, J. *WPF pro začátečníky* [web]. programujte.com, 2014. Dostupné z: http://programujte.com/clanky/27-wpf-silverlight/

Seznam symbolů, veličin a zkratek

GUI	grafické uživatelské rozhraní – Graphical User Interface
NVR	síťový video server – Network Video Recorder
US	ultrazvuk – Ultra Sonic
PIR	pasivní infračervený detektor – Passive Infra-Red
MW	mikrovlny – Micro Waves
WPF	Windows Presentation Foundation
MVVM	Model-View-ViewModel
TR	zbývající čas - Time Remaining
RFT	reakční doba ostrahy - Response Force Time
LTM	levé tlačítko myši
PTM	pravé tlačítko myši

A Obsah přiloženého DVD

Následuje stručný popis obsahu přiloženého DVD.

`bin/`

Obsahuje adresáře `Setup` a `Portable`. Adresář `Setup` obsahuje instalátor aplikace `IASPlanner`. V Adresáři `Portable` se nachází aplikace IASPlanner ve spustitelné verzi přímo z DVD. Verze `Portable` může také vyžadovat dodatečou instalaci dalšího softwaru viz readme.txt.

`doc/`

Diplomová práce ve formátu PDF, vytvořená dle závazného stylu FEKT VUT pro diplomové práce, včetně všech příloh, a všechny soubory nutné pro bezproblémové vygenerování PDF souboru dokumentace (v ZIP archivu).

`src/`

Kompletní zdrojové soubory aplikace `IASPlanner` se všemi potřebnými zdrojovými texty, knihovnami a dalšími soubory pro bezproblémové vytvoření spustitelných verzí programu (v ZIP archivu).

`readme.txt`

Soubor readme.txt obsahuje návod k instalaci a užívání aplikace `IASPlanner`. Stejně tak popisuje software a hardware potřebný k jejímu bezproblémovému chodu.

Navíc DVD obsahuje:

`data/`

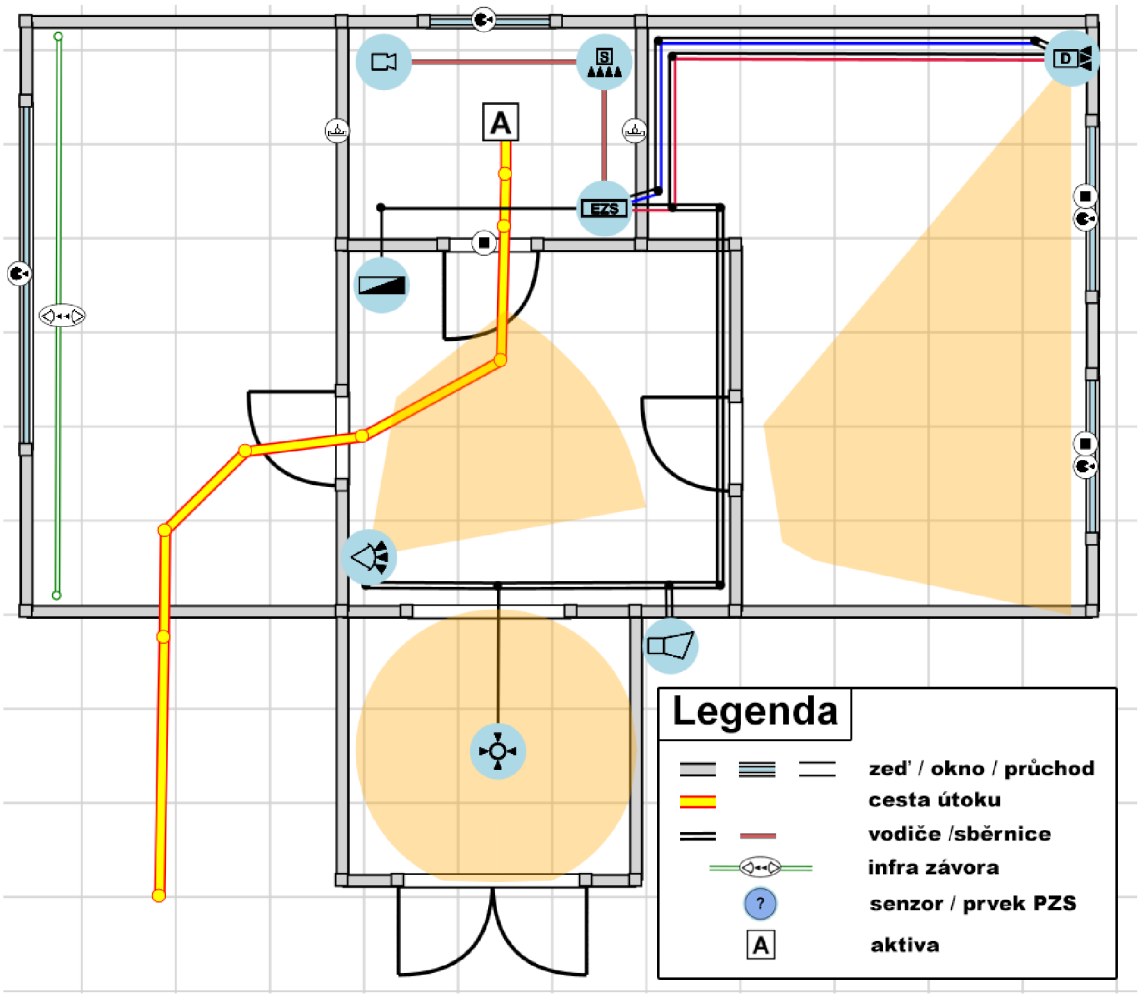
Soubory s ukázkovým zákresem vytvořeným v aplikací `IASPlanner` a sešit MS Excel pro výpočet metody EASI.

`literature/`

Literatura využitá při vypracování bakalářské práce. Především [1] [2] [3] [4] a [5].

U veškerých odjinud převzatých materiálů obsažených na DVD povolují jejich zahrnutí podmínky pro šíření. U všech těchto materiálů je uveden jejich zdroj (webová adresa) v textu práce nebo v souboru `readme.txt`.

B Příklad vypracovaného zákresu



C Přehled použitých značek prvků PZS

	Detektor rozbití skla.
	Magnetický detektor otevření.
	Pasivní infra detektor.
	Pasivní infra detektor stropní (charakteristika 360°)
	Duální detektor.
	IR infra závora.
	Otřesový detektor.
	Hlásič úniku plynu.
	Hlásič požáru.
	Siréna vnitřní.
	Siréna vnější s blikačem.
	Siréna vnější bez blikače.
	Signalizace optická.
	Signalizace akustická.
	Ústředna EZS.
	Ovladač EZS.

D Zdrojový kód vyhodnocení pravděpodobnosti přerušení útoku

D.1 Vstupní parametry metody EASI

```
1  //Vstupní hodnoty předávané metodě 'Evaluate' pomocí polí. V každém poli jsou
       hodnoty dané  proměnné pro všechny řádky tabulky EASI.
2  //Pravděpodobnost P_D
3  double[] detectionProb
4  //Střední hodnota zpoždění útočníka
5  int[] meanDelays
6  //Směrodatná odchylka zpoždění útočníka
7  double[] standardDevs
8  //Koeficienty B,M,E
9  string[] locationDetections
10 //Pravděpodobnost správné komunikace s bezp. složkami
11 double p_c
12 //Střední hodnota doby příjezdu bezp. složek
13 int rft
14 //Směrodatná odchylka  doby příjezdu bezp. složek
15 double rftDev
16
17 //Následují vnitřní proměnné metody 'Evaluate':
18
19 //Počet kroku v útoku, udává počet iteraci výpočtů
20 int stepCount = detectionProb.Length;
21   //Pravděpodobnost správného vyhodnoceni alarmu P_A
22 double[] assesmentProb = new double[stepCount];
23 //Pravděpodobnost selhání detekce na daném kroku a přechod k dalšímu kroku
24 double[] detectionFailProb = new double[stepCount];
25 //Pravděpodobnost, ze zde dojde k první detekci
26 double[] firstDetectionProb = new double[stepCount];
27 //Střední hodnota náhodné veličiny (TR -RFT) na daném kroku
28 double[] cumulativeDelays = new double[stepCount];
29 //Sm. odchylka náhodné veličiny (TR -RFT) na daném kroku
30 double[] cumulativeVariance = new double[stepCount];
31 //Střední hodnota náhodné veličiny (TR -RFT) ovlivněna B,M nebo E
32 double[] trueMean = new double[stepCount];
33 //Sm. odchylka náhodné veličiny (TR -RFT) ovlivněna B,M nebo E
34 double[] trueVariance = new double[stepCount];
35 //Vstupní hodnota pro výpočet P(R|A)
36  double[] zValues = new double[stepCount];
37 //Pravděpodobnost, že bezp. složky, přeruší útok před dokončením kroku
38 double[] stepInterruptionProb = new double[stepCount];
39 //Pravděpodobnost přerušení útoku pro daný krok
40 double[] partialInterruptionProb = new double[stepCount];
```

Výpis D.1: Vstupní parametry metody EASI

D.2 Výpočet P_I metodou EASI

```
1  public class EASI
2  {
3      public static double Evaluate( //Vstupní proměnné byly popsány v předchozí č
           ásti.)
4      {
5          //Výpočet proměnných pro rozptyl náhodné veličiny, do vzorce pro PR|A
6          //Počítá se samostatně, protože je potřeba smyčku procházet odzadu
7          for (int j = stepCount - 1; j >= 0 ; j--)
8          {
9              if (j == stepCount - 1)
10             {
11                 cumulativeVariance[j] = standardDevs[j] * standardDevs[j];
12                 cumulativeDelays[j] = meanDelays[j];
13             }
14             else
15             {
16                 cumulativeVariance[j] = standardDevs[j] * standardDevs[j] +
                       cumulativeVariance[j + 1];
17                 cumulativeDelays[j] = meanDelays[j] + cumulativeDelays[j + 1];
18             }
19         }
20
21         //Výpočet dílčích hodnot pro všechny řádky
22         for (int i = 0; i < stepCount ;i++)
23         {
24             //Výpočet pravděpodobnosti správného vyhodnoceni alarmu
25             assesmentProb[i] = detectionProb[i] * p_c;
26
27             //Výpočet pravděpodobnosti selhání detekce na daném prvku
28             if (i != 0) detectionFailProb[i] = (1 - assesmentProb[i]) *
                   detectionFailProb[i - 1];
29             else detectionFailProb[i] = (1 - assesmentProb[i]);
30
31             if (i != 0) firstDetectionProb[i] = assesmentProb[i] *
                   detectionFailProb[i - 1];
32             else firstDetectionProb[i] = assesmentProb[i];
33
34             //Podle nastavení proměnné zpoždění x detekce jsou střední hodnoty
                   a směrodatné odchylky násobeny koeficienty
35             switch (locationDetections[i])
36             {
37                 case "B":
38                     if (i == stepCount - 1) trueMean[i] = meanDelays[i];
39                     else trueMean[i] = cumulativeDelays[i + 1] + meanDelays[i];
40                     if (i == stepCount - 1) trueVariance[i] = standardDevs[i] *
                           standardDevs[i];
41                     else trueVariance[i] = cumulativeVariance[i + 1] +
                           standardDevs[i] * standardDevs[i];
42                     break;
43                 case "M":
44                     if (i == stepCount - 1) trueMean[i] = meanDelays[i] * 0.5;
45                     else trueMean[i] = cumulativeDelays[i + 1] + meanDelays[i]
                           * 0.5;
46                     if (i == stepCount - 1) trueVariance[i] = standardDevs[i] *
                           standardDevs[i] * 0.25;
```

```
47                      else trueVariance[i] = cumulativeVariance[i + 1] +
                            standardDevs[i] * standardDevs[i] * 0.25;
48                      break;
49                  case "E":
50                      if (i == stepCount - 1) trueMean[i] = 0;
51                      else trueMean[i] = cumulativeDelays[i + 1];
52                      if (i == stepCount - 1) trueVariance[i] = 0;
53                      else trueVariance[i] = cumulativeVariance[i + 1];
54                      break;
55              }
56              //Výpočet vstupní hodnoty pro funkci SNormDist
57              zValues[i] = (trueMean[i] - rft) / Math.Sqrt(rftDev * rftDev +
                    trueVariance[i]);
58
59              //Výpočet hodnoty PR|A podle funkce pro normální distribuci náhodné
                    veličiny, SNormDist
60              stepInterruptionProb[i] = SNormDist(zValues[i]);
61
62              //Do pole ukládáme pravděpodobnost přerušení útoku každého řádku
63              partialInterruptionProb[i] = stepInterruptionProb[i] *
                    firstDetectionProb[i];
64          }
65          //Jako výsledek vracíme sumu všech dílčích pravděpodobností přerušení
66          return partialInterruptionProb.Sum();
67      }
```

Výpis D.2: Výpočet P_I

D.3 Výpočet P(R|A_i) pomoci funkce pro rozdeleni nahodne veliciny

```
1  // Implementace funkce SNormDist, která slouží k výpočtu P(R|A)
2  // Pomocná metoda pro metodu EASI, která vychází z definice rozdělení náhodné
       veličiny
3  public static double SNormDist(double x)
4  {
5      const double b1 = 0.319381530;
6      const double b2 = -0.356563782;
7      const double b3 = 1.781477937;
8      const double b4 = -1.821255978;
9      const double b5 = 1.330274429;
10     const double p = 0.2316419;
11     const double c = 0.39894228;
12
13     if (x >= 0.0)
14     {
15         double t = 1.0 / (1.0 + p * x);
16         return (1.0 - c * Math.Exp(-x * x / 2.0) * t * (t * (t * (t * (t * b5 +
               b4) + b3) + b2) + b1));
17     }
18     else
19     {
20         double t = 1.0 / (1.0 - p * x);
21         return (c * Math.Exp(-x * x / 2.0) * t * (t * (t * (t * (t * b5 + b4) +
               b3) + b2) + b1));
22     }
23 }
```

Výpis D.3: Výpočet P(R|A_i)