Posouzení bezpečnostních rizik fotovoltaické elektrárny

Martin Malý

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2012/2013

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

Jméno a příjmení:	**Martin MALÝ**
Osobní číslo:	**L10090**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Posouzení bezpečnostních rizik fotovoltaické elektrárny**

Zásady pro vypracování:

1. **Posouzení současného stavu zabezpečení fotovoltaické elektrárny**
2. **Posouzení bezpečnostních rizik fotovoltaické elektrárny**
3. **Minimalizace vybraných bezpečnostních rizik objektu fotovoltaické elektrárny**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] ČANDÍK, Marek. Objektová bezpečnost II. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. ISBN 80-7318-217-3.

[2] IVANKA, Ján. Mechanické zábranné systémy. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5 (brož.)

[3] UHLÁŘ, Jan. Technická ochrana objektů, II. díl – Elektrické zabezpečovací systémy II, Praha: PA ČR, 2005. 224 s. ISBN 80-7251-189-0.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **doc. Ing. Miroslav Tomek, Ph.D.**
Ústav krizového řízení

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **10. května 2013**

V Uherském Hradišti dne 25. února 2013

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

prof. PhDr. Ivo Barteček, CSc.
děkan

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

ABSTRAKT

MALÝ, Martin: *Posouzení bezpečnostních rizik fotovoltaické elektrárny.* [Bakalářská práce]. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení; Ústav krizového řízení. Vedoucí práce: doc. Ing. Miroslav Tomek, Ph.D. Stupeň odborné kvalifikace: Bakalář (Bc.) v programu: Procesní inženýrství, studijní obor: Ovládání rizik. Zlín: FLKŘ UTB, 2013. 46s.

Bakalářská práce pojednává o problematice posouzení bezpečnostních rizik objektu fotovoltaické elektrárny. Práce je rozdělena do dvou částí, teoretické a praktické. Teoretická část je zaměřena zejména na všeobecný popis dané problematiky a na současné možnosti mechanického a technického zabezpečení objektu. Praktická část se věnuje identifikaci bezpečnostních rizik, jejímu vyhodnocení pomocí různých metod a analýz. Závěr práce pojednává o redukci nejzávažnějších bezpečnostních rizik ohrožujících vybraný objekt.

Klíčová slova: bezpečnost, fotovoltaická elektrárna, ochrana, hodnocení rizik, zabezpečení

ABSTRACT

MALÝ, Martin: *The security risk assessments of photovoltaic power plant.* [Bachelor thesis]. Tomas Bata University in Zlin. Faculty of Logistics and Crisis management; Department of Crisis management. Thesis supervisor: doc. Ing. Miroslav Tomek, Ph.D. Level of professional qualifications: Bachelor (Bc) in the program: Process engineering. Field of study: Risk control. Zlin: FLCM TBU, 2013. 46 pages.

This bachelor thesis deals with problems of security risk assessments in the object of photovoltaic power plant. The thesis is divided into two parts, theoretical and practical. The theoretical part is focused on general description of the problems and possibilities of current mechanical and technical security. The practical part is devoted to identifying of security risks, it is evaluation using various methods and analyses. The conclusion deals with the reduction of the most serious security risks endangering the selected object.

Keywords: safety, photovoltaic power plant, protection, risk assessments, security

Poděkování

„Chtěl bych poděkovat především panu doc. Ing. Miroslavu Tomkovi, Ph.D., vedoucímu mé bakalářské práce, za důsledné vedení, cenné rady a připomínky.

Mé poděkování také patří majiteli fotovoltaické elektrárny, který mi poskytl důležité podklady a informace pro vypracování této práce.

V neposlední řadě bych rád poděkoval své rodině za trpělivou podporu, bez níž bych tuto práci nemohl dokončit.“

Prohlašuji, že

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

Prohlašuji,

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

V Uherském Hradišti dne 9. 5. 2013

.....

podpis studenta/ky

OBSAH

ÚVOD

Současná doba je charakteristická relativně vysokým nárůstem kriminality a násilí ve společnosti. Tento trend může být zapříčiněn upadající morálkou občanů, migrací osob, výchovou dětí a dalšími aspekty. Význam ochrany majetku a osob ve 21. století prudce vzrostl, stejně tak jako zájem o bezpečnost. K zájmu také přispívá větší dostupnost technických prostředků, jejichž cena v důsledku vývoje nových technologií klesla. [10]

Koncem posledního desetiletí vznikla spousta firem, která se zabývá dodávkou a montáží fotovoltaických elektráren. Nový průmyslový trend uvítalo bezesporu mnoho dalších subdodavatelských firem zabývajících se mimo jiné dodávkou zabezpečovací techniky, oplocení, kovových konstrukcí a elektroinstalací. Má osobní dlouholetá působnost v oboru obnovitelných zdrojů proto byla podnětem pro napsání této bakalářské práce.

Cílem předkládané bakalářské práce je posoudit současné možnosti zabezpečení objektu fotovoltaické elektrárny za pomoci mechanických zábran, technických prostředků, fyzické a režimové ochrany. Dílčím cílem je identifikovat bezpečnostní rizika, na základě studiem získaných teoretických poznatků, a pro nejzávažnější rizika navrhnout jejich redukci.

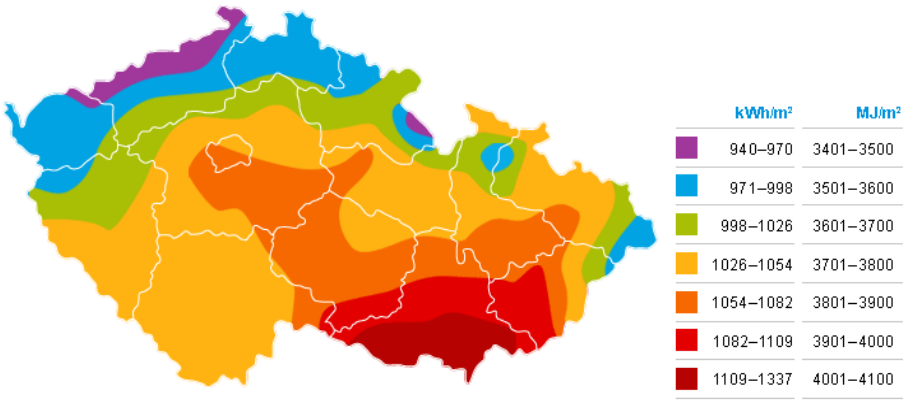
Bakalářská práce je členěna do dvou hlavních celků, a to teoretické a praktické části. V teoretické části se budu zabývat úvodem do problematiky bezpečnosti fotovoltaických elektráren, uvedu prvky mechanických zábranných systémů a prvky technického zabezpečení, jako jsou elektronické zabezpečovací systémy, v neposlední řadě také zmíním fyzickou a režimovou ochranou. V části praktické provedu popis vybraného objektu, za pomoci Ishikawova diagramu identifikuji bezpečnostní rizika z procesního a strukturálního hlediska. Analýzou Failure Mode and Effect Analysis vyhodnotím identifikovaná bezpečnostní rizika, jejichž výsledky verifikuji Paretovým pravidlem 80/20 a nakonec graficky zobrazím za pomoci Lorenzovy křivky. Závěrem bakalářské práce se budu věnovat návrhům na redukci nejzávažnějších bezpečnostních rizik, jež budou výsledkem předchozích analýz.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY ZABEZPEČENÍ FOTOVOLTAICKÉ ELEKTRÁRNY

Energie, zejména ta sluneční, je od pradávna základním a nenahraditelným prvkem podmiňujícím existenci naší civilizace. Sluncem vyzářená energie je prakticky využitelná v různých aplikacích, kterou již naši předkové využívali například k sušení nejrůznějších materiálů a potravin. Rozsah využití energie ze slunce je však podmíněn intenzitou slunečního záření v dané oblasti.

V poslední době se rozšiřuje využití slunečního záření také jako obnovitelný energetický zdroj. Nejčastějším využitím sluneční energie v současné době je ohřev užitkové vody nebo výroba elektrické energie přeměnou slunečního záření na elektrický proud. Česká republika (ČR) je z hlediska svého zeměpisného umístění relativně vhodná pro oba způsoby využití slunečního záření. Sluncem vyzářená energie, dopadající na území ČR, se totiž pohybuje v rozmezí 1000-1250 kWh*m^{-2} plochy (Obr. 1).



Obr. 1 Průměrný roční úhrn záření dopadající na území ČR [Zdroj: 13]

Zejména v posledních 5-10 letech vznikají na území ČR velká technologická zařízení na výrobu elektrické energie ze slunce, tzv. fotovoltaické elektrárny (FVE). Tato zařízení jsou situována na určitém ohraničeném území o určité rozloze, v němž je instalována samotná technologie zajišťující přeměnu sluneční energie na energii elektrickou.

Hodnota nainstalované technologie v objektu FVE je hlavním důvodem pro důkladné zabezpečení celého areálu. Většina realizovaných FVE je financována za pomoci bankovních úvěrů, které budou pro výrobce, v případě přerušení dodávky energie v důsledku poškození

nebo krádeže technologie, likvidační. Pořizovací náklady průměrné FVE se totiž pohybují, v závislosti na výkonu zařízení, v řádech desítek až stovek milionů korun.

Z hlediska možných nežádoucích trestných činností lze u objektů FVE počítat s vloupáním a krádežemi, vandalstvím nebo sabotážemi. Samotná technologie bude hlavním bodem zájmu případných pachatelů. Proto je vhodné předem identifikovat možná rizika, která v souvislosti s trestnou činností hrozí, a co nejefektivněji zabránit či ztížit vstup neoprávněných osob do objektu. Samostatnou kapitolou jsou vandalové, kteří často nerozlišují podstatu ničených věcí. Předmětem jejich útoků mohou být veřejná zařízení, soukromý majetek, automobily, skleníky nebo právě objekt FVE. Vandalům jde především o způsobení co největší škody.

Při návrhu zabezpečení objektu je vhodné vycházet z bezpečnostní analýzy, ve které je nezbytnou součástí identifikace a ocenění hlavních bezpečnostních rizik, nejlépe i včetně skrytých hrozeb. Z analýzy je poté možné určit návrh na redukci rizik, technické řešení, způsob provedení fyzické a režimové ochrany. Předpokladem úspěšné analýzy rizik je znalost možného typu útoku a následně fáze, ve které má být případný útok detekován.

Obecně lze zabezpečení objektů rozdělit na technické bezpečnostní prvky, fyzickou ochranu a režimová opatření. Vzhledem k požadavku na bezobslužnost bezpečnostního systému a častou situaci instalací do odlehlých míst se špatnou dostupností, stále zůstává hlavním bezpečnostním prvkem technická ochrana objektu. Tato ochrana obsahuje především mechanické zábranné a elektronické zabezpečovací systémy. Fyzickou ostrahu, kterou zabezpečují kvalifikované bezpečnostní agentury, využívají investoři hlavně v období výstavby FVE, kdy ještě nejsou technické bezpečnostní prvky k dispozici, případně nefungují zcela autonomně. Samozřejmostí každého bezpečnostního systému by měla být také určitá režimová opatření. Jedná se zejména o administrativní opatření k dosažení a kontrole dodržování řádné bezpečnosti v objektu i v jeho okolí.

Dohled nad ochranou objektu drží dohledové centrum, které přijímá a vyhodnocuje informace o dění v objektu. Tzv. pult centralizované ochrany (PCO) je zařízení, do kterého se sdružují výstupy z elektronického zabezpečovacího systému a kamerových jednotek. Obsluha PCO dokáže, na základě informací o poplachu vyhlášeném zabezpečovací ústřednou, včas rozpoznat napadení objektu a adekvátně na něj reagovat například vysláním rychlé zásahové jednotky. Pokud je v objektu stálá hlídací služba, PCO ji vyrozumí o napadení objektu. Tento model součinnosti PCO s fyzickou stálou ochranou objektu se v praxi aplikuje zejména u velmi rozlehlých nebo členěných objektů FVE.

2 VHODNÉ PRVKY ZABEZPEČUJÍCÍ OBJEKT FOTOVOLTAICKÉ ELEKTRÁRNY

Snahou všech bezpečnostních prvků, nejen v objektu FVE, je zabránit nebo ztížit pachateli vstup do chráněného prostoru, případně pokus o neoprávněný vstup odhalit ještě před jeho vykonáním. Současně je nutné monitorovat chráněný prostor dostatečně vyspělou technologií, která dokáže detekovat přítomnost neoprávněné osoby a vyhlásit poplach tak, aby na něj bylo možné včas a adekvátně reagovat.

V současnosti se dává přednost spíše elektronickým bezpečnostním prvkům, které jsou často velmi citlivé a v mnohých případech dokáží úspěšně a automaticky detekovat protiprávní čin ještě před tím, než je vykonán. Některé bezpečnostní prvky jsou již svou konstrukcí velmi nápadné, případně mohou vydávat doplňkové varovné světelné nebo zvukové signály. Takto nápadná zařízení mají svůj preventivně psychologický účinek.

2.1 Mechanické zábranné systémy

Mechanické zábranné systémy jsou považovány za základní prvek ochrany objektů a osob. Tyto systémy jsou nejstarším způsobem ochrany a vykazují se zejména svou mechanickou odolností. Pod mechanické zábranné systémy můžeme zařadit všechny mechanické prvky, které jakýmkoli způsobem ztěžují násilné vniknutí nepovolané osoby do chráněné zóny, případně zabraňují manipulaci s chráněnými předměty nepovolanou osobou. Násilné vniknutí je nejčastěji provedeno překonáním oplocení a cestou dveřních či okenních otvorů.

Mechanické zábranné systémy se využívají jako obvodová ochrana pro zabezpečení okolo chráněného objektu v podobě oplocení nebo zdí. Plášťová ochrana představuje zabezpečení pláště budovy prostřednictvím oken a dveří. Prostorová ochrana střeží určený prostor prostřednictvím pohybových čidel a předmětová ochrana se využívá k ochraně svěřených předmětů v různých úschovných schránkách. [11]

2.1.1 Plotové systémy

Plotové systémy jsou mechanické prvky obvodové ochrany, zabraňující narušení střeženého objektu (Obr. 2). Tyto systémy vytvářejí bariéru, prostorově oddělující chráněný prostor od jeho okolí, která představuje hranici střeženého objektu. Běžně se používá drátěné nebo svařované pletivo, pevně uchycené na plotové sloupky. Plotové systémy jsou často doplňovány o vrcholové zábrany a podhrabové desky, ztěžující vniknutí do objektu.

Vrcholové zábrany jsou využívány jako doplňkové řešení proti přelezení plotového systému. Instalují se nad plotový systém a vizuálně plot zvyšují. Můžou být tvořeny ostnatým nebo žiletkovým drátem, který poskytuje oproti ostnatému drátu lepší ochranu.

Podhrabové desky se využívají jako ochrana proti podlezení plotu a jsou tvořeny betonovými monolity, které se přichycují na sloupky plotu a jsou částečně zapuštěny do země. [6]

Obr. 2 Plotový systém s vrcholovou a podhrabovou zábranou [Zdroj: 6]

2.1.2 Vstupní brány a vjezdy

Vstupní brány a vjezdy jsou součástí plotového systému a umožňují povolaným osobám nebo vozidlům volný vstup do objektu. Brány (Obr. 3) mohou být jedno nebo dvoukřídlé konstrukce a jejich otevírání bývá na většině FVE řešeno manuálně. Nejčastěji se u objektů FVE používá otočný typ brány dovolující otevření křídla v rozmezí až 180 °.

Obr. 3 Vstupní brána do objektu FVE s žiletkovým drátem [Zdroj: 6]

Ochraně vstupů a vjezdů je třeba věnovat mimořádnou pozornost, jelikož tvoří hranici mezi volně přístupným a chráněným prostorem. Počet takovýchto vstupů do objektu by měl být minimalizován s ohledem na lepší kontrolu vstupu osob do objektu. [11]

2.1.3 Zámkové systémy

Zámkové systémy slouží k bezpečnému zajištění pohyblivých součástí vstupních dveří, bran a oken proti neoprávněnému či samovolnému otevření. U objektu FVE jsou to pak bezpečnostní cylindrické vložky nebo bezpečnostní visací zámky.

Bezpečnostní cylindrická vložka je přímou součástí otevíracího mechanismu vstupní brány a musí odolávat různým typům napadení- odvrtání, rozlomení nebo vytržení. Samotnou bezpečnost zámkového systému určuje velikost a tvar klíče, členitost a provedení uzamykacího ústrojí a také způsob upevnění cylindrické vložky.

Bezpečnostní visací zámek není na rozdíl od cylindrické vložky pevně uložen do otevíracího ústrojí vstupní brány a jeho konstrukce se většinou skládá z jednoho celku. Zámek musí být zhotoven z materiálů, které znemožňují přestřižení nebo přeřezání.

Zabezpečení zámkových systémů se dělí podle pyramidy bezpečnosti, jejichž údaj je obvykle vyžadován pojišťovnami. Systém pyramida bezpečnosti vychází z normy ČSN P ENV 1627, která definuje odolnost výrobků proti běžným typům napadení. Je zaměřena výhradně na certifikované výrobky a akceptována všemi pojišťovnami. [7]

2.2 Elektronické zabezpečovací systémy

Elektronické zabezpečovací systémy (EZS) jsou souborem technických prostředků, které jsou schopny detekovat pokus o vstup nebo již přítomnost nepovolané osoby ve střeženém prostoru, a tuto skutečnost opticky nebo akusticky na definovaném místě signalizovat. Hlavním posláním EZS je tedy informovat majitele objektu nebo dohledovou službu o narušení chráněného prostoru. Každý elektronický zabezpečovací systém se skládá z různých prvků, mezi které patří detektory, zabezpečovací ústředna, přenosové prostředky, signalizační a doplňková zařízení. [19]

Pro zabezpečení špatně dostupných a odlehlých míst, jako jsou například fotovoltaické elektrárny, se zpravidla využívá systémů s dálkovou signalizací a vyvedením na PCO. Dohledová služba je tak včas informována o vzniklém poplachu a může na něj adekvátně zareagovat vysláním zásahové jednotky. Při návrhu a uvedení bezpečnostního systému do provozu je vhodné co nejvíce eliminovat vznik falešných poplachů správnou konfigurací.

2.2.1 Perimetrická plotová ochrana

Perimetrický zabezpečovací systém je elektronické zařízení prioritně určené pro střežení obvodového oplocení a venkovních prostor. Na pletivo plotu se podélně připevní speciální senzorický detekční kabel (Obr. 4), který převádí mechanické namáhání a záchvěvy pletiva na elektrický signál, následně zpracovávaný vyhodnocovací jednotkou. Ta odfiltruje běžné rušení a vyhlásí poplach při pokusu o podlézání, přelézání nebo prostříhávání pletiva některé z plotových jednotek.

Podmínkou pro použití této technologie je dokonale vypnuté plotové pletivo. Plané poplachy může u tohoto způsobu zabezpečení způsobovat silný déšť, krupobití, silný vítr a přítomnost zvěře. [4]

Obr. 4 Perimetrický senzorický kabel na pletivu brány [Zdroj: 4]

2.2.2 Zemní detekční kabely

Zemní detekční kabely jsou patrně nejspolehlivějším ochranným perimetrickým systémem. V určité hloubce pod povrchem země je uložen speciální detekční kabel, který kolem sebe vytváří několik metrů široké detekční pole a vyhodnocuje jeho změny. Tyto kabely mají celou řadu výhod, mezi něž můžeme zařadit vysokou míru spolehlivosti, na rozdíl od ostatních ochranných systémů nejsou viditelné (neupozorňují na sebe), plynule kopírují všechny výškové nerovnosti a střežený koridor se nemusí skládat z přímek (jako například u optických či mikrovlnných bariér). Vzhledem k vyšší pořizovací ceně se tento typ technologie v zabezpečení fotovoltaických elektráren nepoužívá. [3]

2.2.3 Magnetické kontakty a mikrospínače

Magnetické kontakty a mikrospínače řadíme do skupiny kontaktních senzorů. Jejich nejčastější využití je pro střežení otevření vstupních cest, jako jsou dveře, okna a brány. Senzory rozpoznávají dva stavy: sepnuto a rozpojeno, neboli otevřeno a zavřeno. Jejich napojení na vstup centrální zabezpečovací ústředny tak efektivně detekuje například neoprávněné otevření dveří nebo brány, či jejich samovolného otevření.

2.2.4 Elektronické bariéry

Elektronické bariéry patří mezi často používané prvky pro zajištění obvodové ochrany. Obecně se jedná o aktivní elektronické zařízení skládající se z vysílače a přijímače, mezi nimiž vzniká aktivní zóna v podobě optického paprsku nebo mikrovlnného záření. V případě přerušení aktivní zóny je vyhlášený poplach přiveden na vstup centrální zabezpečovací ústředny a následně určitým způsobem vyhodnocen. Elektronické bariéry mohou být infračervené, mikrovlnné nebo kombinací obou předchozích technologií.

Infračervené bariéry (Obr. 5), nejčastěji používány právě v objektu FVE, mají zpravidla na jedné straně sloupek s určitým počtem vysílačů infračerveného záření a proti němu sloupek se stejným počtem přijímačů. Bezpečný a prakticky použitelný rozestup jednotlivých sloupků je 50 - 150 m. Při delších vzdálenostech však může docházet k rušení paprsků.

Nutnou podmínkou pro bezproblémovou aplikaci technologie je rovný a upravený terén mezi vysílačem a přijímačem. Rizikovými faktory vzniku falešných poplachů jsou zejména mlha, silný déšť, padající sníh, vysoká tráva nebo přímý silný sluneční svit. [19]

Obr. 5 Infračervené bariéry [Zdroj: 3]

Mikrovlnné bariéry (Obr. 6) vytvářejí vysokofrekvenční elektromagnetické pole, typicky formou rotačního elipsoidu, vysílaného mezi vysílačem a přijímačem. Elektronický systém detekuje a vyhodnocuje změny vyslané energie zachycené přijímacím zařízením, která se mění v závislosti na rychlosti pohybu a velikosti předmětu pohybujícího se v aktivní zóně.

Výhodou mikrovlnných bariér je relativně široké rozpětí dosahu od 30 - 450 m, vysoká rezistence oproti povětrnostním vlivům a zaručená detekce i při částečném zastínění vyzařovaného svazku energie. Nevýhodou je však vyšší pořizovací cena oproti infračerveným bariérám, a proto se samostatně používají spíše méně často. Častější aplikací je použití menších mikrovlnných bariér v kombinace s infračervenou technologií. [19]

Obr. 6 Mikrovlnná bariéra [Zdroj: 1]

2.2.5 Pohybové senzory

Pohybové senzory obyčejně zabezpečují vnitřní prostory v určité místnosti daného objektu. V případě fotovoltaických elektráren se jedná spíše o doplňkové zařízené pro zabezpečení vnitřních prostor trafostanice a kiosku s technologiemi.

Pohybové senzory snímají a vyhodnocují pohyb ve střeženém prostoru, a proto je lze zařadit mezi prvky prostorové ochrany. Detektory využívají různé metody detekce pohybu. Nejčastěji se jedná o pasivní infračervené detektory, které snímají teplotu a můžou detekovat změnu vyzařované radiace ve střeženém prostoru. Dále lze použít aktivní mikrovlnné nebo ultrazvukové detektory, vysílající energetické vlny do prostor objektu a registrující změnu odrazu vyslané vlny od objektu. Pro minimalizaci falešných poplachů se v praxi uvádí duálních pohybových senzorů, jež svou kombinací předchozích technologií zvyšují svou spolehlivost detekce (například infračervený + mikrovlnný detektor). [3]

2.2.6 Systémy průmyslové televize

Systémy průmyslové televize (CCTV) jsou velmi významným pomocníkem v boji proti kriminalitě. V dnešní době tvoří nedílnou součást ochrany života, zdraví, majetku nevyjímaje významný preventivní účinek. Tyto systémy se využívají pro monitorování nejrůznějších objektů a pozemků, muzeí, benzinových pump, letišť a dalších objektů. CCTV je systém vhodný zejména jako podpora klasické EZS, v některých speciálních případech však může část úlohy EZS přímo převzít (např. detekce pohybu v určené zóně, případně automatická identifikace osob nebo vozidel).

Nejdůležitější součástí celého kamerového systému je samotná kamera, resp. kamerová jednotka, která může být vybavena černobílým nebo barevným snímacím čipem a fixní nebo otočné konstrukce. V oblasti zabezpečení FVE je velmi často kamerová jednotka doplněna o infračervený přísvitový modul, umožňující monitorovat střežený prostor i za snížených viditelných podmínek nebo v noci. [16]

Samotnou kapitolou jsou kamerové jednotky vybavené termocitlivým čipem. Tyto kamery umožňují monitorovat prostor termografickou metodou a vyznačují se vysokou přesností detekce s velmi malým procentem vyhlášených falešných poplachů. Fotografie skupiny pachatelů, zachycená na obrázku 7, je pořízena v zimním období za naprosté tmy. Pachatelé jsou přistiženi při pokusu o neoprávněný vstup do objektu prostřižením a přelezením oplocení. Tmavě zbarvené části fotografie naznačují místa s vyšší vyzařovanou teplotou než je jeho okolí. Technologie je však poměrně nákladná a nevyplatí se ke střežení menších objektů. Naopak je významná v případě pátrání po pohřešovaných osobách. [2]

Obr. 7 Termografický snímek protiprávního činu [Zdroj: 2]

Nespornou výhodou běžné CCTV je fakt, že hlídací služba (PCO, fyzická ostraha, dohledové centrum) nemusí ověřovat příčinu vyhlášeného poplachu přímo na místě, ale může pomocí kamery vzdáleně a dlouhodobě pozorovat konkrétní prostor bez rizika ohrožení pracovníků (případně k ověření falešného poplachu před výjezdem), což je u odlehlých instalací FVE velmi žádoucí vlastností. K pozdější analýze průběhu napadení lze záznam z kamerových jednotek archivovat na nejrůznějších typech rekordérů. Moderní systémy automaticky archivují záznam v digitální podobě na HDD a data je následně možné vypálit na CD/DVD, případně stáhnout do PC nebo na externí paměťové médium. [5]

2.2.7 Systémy předmětové ochrany

Systém předmětové ochrany se v objektu FVE používá k zabezpečení samotných fotovoltaických panelů a měničů napětí proti demontáži a zcizení. Jedná se o další elektronický podpůrný systém k zabezpečení chráněných předmětů, který doplňuje předchozí zmíněné bezpečnostní systémy perimetrické, prostorové ochrany a CCTV.

Tato technologie však detekuje poplach až v případě, že dochází k manipulaci s chráněným předmětem. Zabezpečení je realizováno provlečením ochranného elektrického signálního kabelu rámem panelu, měničem, případně celou nosnou konstrukcí. Při manipulaci či demontáži chráněné technologie je pachatel nucen signální drát přerušit, což vede k poplachovému hlášení s relativně přesnou lokalizací místa narušení.

Nespornou výhodou této technologie jsou nízké pořizovací náklady, jelikož se v praxi používá běžný jednožilový kabel, který nemá žádné speciální vlastnosti, a je určený pro použití ve vnějších podmínkách. Kabel lze také bez obtíží libovolně napojovat a tvořit tak dlouhé úseky, které mohou být rozděleny do různých podsekcí.

Systém předmětové ochrany pomocí kabelu se v případě FVE využívá především k doplnění bezpečnosti při stále hlídací službě, kde by se autonomní bezpečnostní systém EZS nevyplatilo instalovat a provozovat (např. areály firem s 24 hodinový provozem apod.).

2.3 Fyzická ochrana objektu

Fyzickou ostrahu obvykle zajišťuje fyzická osoba, která je fyzicky i psychicky zdatná a má určitý výcvik a školení. Fyzická ostraha může být jedno nebo vícečlenná s možným doplněním o vhodnou, pravidelně a odborně cvičenou, kynologickou složku.

Jedná se zpravidla o pracovníka soukromé bezpečnostní agentury, která pro majitele FVE vykonává potřebné služby na základě smlouvy. Hlavním úkolem fyzické ostrahy je zajistit

bezpečnost svěřeného objektu, majetku nebo technologie a zabránit trestné nebo jinak protiprávní činnosti. Ostraha může být realizována vzdáleně, výjezdy z dohledového centra, které má zároveň vzdálený dohled nad objektem prostřednictvím CCTV a EZS, nebo se může jednat o lokální fyzickou ostrahu s pravidelnou nebo nepravidelnou pochůzkovou činností.

Lokální ostraha má tu výhodu, že může velmi rychle reagovat na možné vniknutí do objektu a zabránit tak protiprávnímu jednání nebo případně odvrátit hrozící útok dříve než je vykonán. Preventivně také působní proti vandalství a s tím spojenými sabotážemi.

Tento způsob ochrany je velmi důležitý v počátku výstavby FVE, jelikož zpravidla ještě nejsou k dispozici autonomní bezpečnostní systémy EZS. V průběhu výstavby a instalace technologie je nutné zajistit ochranu objektu v režimu 24 hodin denně, aby nedošlo ke zcizení technologie ještě před samotnou instalací. Fyzická ostraha také často vykonává jak vstupní, tak i výstupní kontroly zaměstnanců či jiných externích pracovníků.

2.4 Režimová opatření

Režimová opatření spadají pod administrativně-organizační opatření a mohou být vydávány ve formě směrnic, nařízení nebo doporučení. Je to určitý souhrn pravidel, které stanovují zásady bezpečnosti uvnitř i vně objektu a určují pravidla při ochraně majetku a osob.

V případě FVE lze hovořit o legislativní úpravě, která stanoví způsob samotné kontroly při procesech vstupu a výstupu osob z nebo do objektu.

Velmi důležité je věnovat pozornost režimu manipulace s klíči a v případě, že je objekt FVE vybaven elektronickým přístupovým systémem, i identifikačním přístupovým prostředkům, jako jsou přístupové kódy a karty. Součástí tohoto režimu jsou směrnice pro přidělování, evidenci, manipulaci a uskladnění existujících přístupových prostředků. [12]

II. PRAKTICKÁ ČÁST

3 OBJEKT FOTOVOLTAICKÉ ELEKTRÁRNY

Fotovoltaická elektrárna (Obr. 8) je technologické výrobní zařízení instalované na konkrétním ohraničeném území, tvořící jeden celek neboli objekt. Toto technologické zařízení slouží k výrobě, respektive přeměně, sluneční energie na energii elektrickou. Za pomoci fotovoltaických panelů, které zachytávají dopadající sluneční záření, se vytvořený stejnosměrný elektrický proud transformuje na střídavý a dále se distribuuje do veřejné rozvodné sítě. Fotovoltaické elektrárny nevyžadují stálou obsluhu, jsou tedy téměř bezobslužné.

Obr. 8 Fotovoltaická elektrárna Vepřek, okres Mělník, výkon 35,1 MW [Zdroj: 15]

Princip fotovoltaického jevu byl poprvé popsán v roce 1839 francouzským fyzikem Antoinem Césarem Becquerelem, na jehož práci poté navázal jeho syn, Alexandre Edmond Becquerel. Původ slova fotovoltaika pochází z řeckých slov "foto" neboli světlo a "volt" neboli jednotka elektrického napětí. První funkční fotovoltaický článek byl sestrojen v roce 1884 americkým vynálezcem Charlese Frittsem, tedy celých 45 let po Becquerelově objevu fotovoltaického jevu. Článek byl vyroben ze seleniového polovodiče, potaženého velmi

tenkou vrstvou zlata, s nízkou účinností přibližně 1 %, což je prakticky nepoužitelná hodnota. Křemíkový fotovoltaický článek s konstrukcí, kterou známe a používáme dnes, byl vyroben v Bellových laboratořích až 100 let po objevu fotovoltaického jevu.

Dnešní moderní fotovoltaické články dosahují účinnosti kolem 17 % a existují ve třech nejpoužívanějších variantách. Jedná se o amorfní, polykrystalické a monokrystalické. Amorfní panely jsou tvořeny napařovanou křemíkovou vrstvou, mají účinnost okolo 4-8 % a jedná se o nejlevnější variantu. Používají se především v místech, kde není omezen prostor pro výstavbu a jejich výhodou je cena a vyšší výkon při snížených světelných podmínkách. Nevýhodou pak relativně malá účinnost. Polykrystalické panely jsou tvořeny křemíkovou podložkou s účinností kolem 10-14 %. Výhodou polykrystalických panelů je zejména levnější a také jednodušší výroba. Monokrystalické panely jsou tvořeny podobně jako panely polykrystalické z křemíkové podložky, avšak účinnost je u tohoto typu panelů nejvyšší a pohybuje se kolem 13-17 %. Rozdílem oproti polykrystalickým panelům je velikost krystalu, který v řezu dosahuje velikosti více než 10 cm.

Všechny typy panelů jsou složeny z matice křemíkových článků vzájemně propojených letovanými spoji. Ze spodní strany jsou panely chráněny pevnou deskou a z horní strany pak tvrzeným leštěným sklem, díky kterému jsou schopny odolat nepříznivým vlivům počasí. Na trhu jsou k dostání panely různých výrobců a také s různým výkonem. [14]

Dalším nezanedbatelným prvkem fotovoltaické elektrárny jsou měniče napětí. Hlavním úkolem měniče napětí je přeměna stejnosměrného napětí, generovaného fotovoltaickými panely, na napětí střídavé a tedy použitelné pro většinu běžných spotřebičů v elektrické síti. Podobně jako v případě panelů, figuruje i v případě střídačů mnoho výrobců nabízejících střídače různých výkonů a různých provedení, přičemž účinnost těchto zařízení se průměrně pohybuje okolo 98 % přeměněné energie.

Celý komplex výrobního zařízení je poté doplněn o rozvaděče napětí, ve kterých se sdružují kabely od jednotlivých panelů a následně o trafostanice a kiosky, ve kterých se sdružují kabely od jednotlivých střídačů.

Všechny ostatní instalované technologie, centrální ústředna zabezpečovacích systémů, CCTV rekordéry, monitoring výroby, datové komunikátory atd. jsou soustředěny do centrálního kiosku, který je zpravidla součástí hlavní trafostanice.

3.1 Popis vybraného objektu fotovoltaické elektrárny

Konkrétní objekt fotovoltaické elektrárny, ve kterém budu vyhledávat a hodnotit rizika, se nachází území ČR v Jihomoravském kraji. Vzhledem ke komerční povaze soukromého objektu a vzhledem k rozboru bezpečnostních opatření nemohu objekt konkrétněji lokalizovat. Údaje o fotovoltaické elektrárně mi byly poskytnuty na základě souhlasu majitele pod podmínkou utajení přesné lokality samotného objektu.

Objekt fotovoltaické elektrárny se nachází na soukromém pozemku vlastněném investorem o rozloze 84 272 m^2. Celý areál je oplocen svařovaným pletivem o výšce 180 cm, které je nadstaveno ostnatým drátem ve dvou řadách nad sebou. V areálu jsou vybudovány dvě vstupní trasy tvořené dvěma dvoukřídlými bránami o šířce 6 m. Podhrabové desky nejsou součástí oplocení tohoto objektu, ačkoli by bezpochyby zvýšily odolnost oplocení.

V objektu je nainstalováno celkem 21 376 ks fotovoltaických panelů různých výkonů, což odpovídá celkovému instalovanému výkonu 4,595 MWp. Panely jsou uchyceny v řadách nad sebou na speciálních kovových konstrukcích se klonem 34°, které jsou pevně spojeny se zemními vruty. Všechny řady jsou situovány na jih, aby se co nejlépe využilo světelné energie dopadající na plochu panelů (Obr. 9).

Obr. 9 Rozložení fotovoltaických panelů [Zdroj: vlastní]

Stejnosměrnou elektrickou energii z panelů přeměňuje celkem 334 ks střídačů, které jsou upevněny přímo na konstrukci pod jednotlivými řadami panelů. Elektrická kabeláž ze střídačů je následně svedena do 5 ks trafostanic, kde se napětí dále transformuje a distribuuje do veřejné rozvodné sítě. V tomto místě jsou také uloženy měřicí a regulační prvky fotovoltaické elektrárny, včetně dalšího podpůrného technologického zázemí.

Každá trafostanice má betonový skelet (Obr. 10) o rozměrech 3x5 m, rovnou střechu opatřenou pasivním hromosvodem. Vnitřní prostory trafostanice jsou rozděleny na dvě až tři samostatné místnosti se samostatným vchodem, vždy opatřeným zámkem. V jedné místnosti je umístěn vysokonapěťový transformátor a ve druhé části jsou umístěny rozvody nízkého napětí, měřicí a regulační technika, ústředna EZS a ostatní komunikační zařízení.

Bezprostředně okolo trafostanice je vybudován zpevněný podklad a drenážní odtokový kanál, aby se zabránilo případnému vniknutí vody do prostor trafostanice.

Obr. 10 Trafostanice s betonovým skeletem [Zdroj: vlastní]

3.2 Zabezpečení vybraného objektu v současnosti

Perimetrická ochrana objektu FVE je řešena pomocí plotového systému ze svařovaného pletiva s výškou 180 cm a dvěma řadami ostnatých drátů. Na oplocení je přichycen perimetrický senzorický drát v jedné vrstvě s typickým "Z" zakřivením (Obr. 11) po 2-3 plotových blocích. Jednotlivé plotové bloky jsou systematicky rozděleny do sekcí, aby bylo možné případný poplach částečně nebo přesně lokalizovat.

Perimetrický drát vyhodnocuje mechanické namáhání pletiva a je částečně odolný proti běžnému rušení, které vzniká v důsledku lehkých povětrnostních vlivů. Dále je vybaven automatickým hysterezním systémem s čidly, který automaticky vyhodnocují okolní povětrnostní podmínky a upravují nastavení perimetrického kabelu. Technologie automatické hystereze dokáže poměrně spolehlivě snížit počet falešných poplachů (dokáže rozeznat např. přistání ptactva na plot, případně jiné nárazy do oplocení způsobené drobnou zvěří).

Obr. 11 Zakřivení perimetrického kabelu typu "Z" [Zdroj: vlastní]

Vnitřní perimetrickou ochranu objektu zabezpečují duální elektronické bariéry. Tyto bariéry jsou tvořeny duální technologií mikrovlnného a infračerveného typu. V objektu se nachází celkem 10 ks těchto bariér, jejichž paprsky se vzájemně překrývají tak, aby nikde nebylo možné vstoupit bez přerušení detekční zóny. Každá bariéra je vybavena sabotážním spínačem a vyhříváním, aby se zabránilo zamlžení nebo zapadání detekční části bariéry sněhem. V případě detekce špatných povětrnostních vlivů (například silného sněžení nebo mlhy), kdy infračervená technologie selhává, bariéra automaticky zesílí signál mikrovlnné části a zamezí tak vyhodnocování falešných poplachů. Výška každé perimetrické jednotky je 3 m a všechny jsou umístěny na betonovém podkladu se základy.

Prostor objektu je monitorován pomocí 27 fixních a 2 otočných kamerových jednotek, upevněných na ocelových sloupech o výšce 4 m (Obr. 12). Fixní kamerové jednotky jsou rozmístěny po vnitřním obvodu tak, aby každá kamerová jednotka viděla na jednotku následující a aby byl monitorován prostor před a za oplocením, včetně vstupních tras. Tato technologie usnadňuje lokalizaci a orientaci v prostoru, kde hrozí riziko vniknutí do objektu. Otočné kamery jsou rozmístěny tak, aby měly celkový přehled nad chráněným prostorem FVE a zároveň kontrolu nad vstupními trasami (lze s nimi vzdáleným ovládáním sledovat pohyb osob po objektu v reálném čase). Všechny kamery jsou doplněny o infračervený (IR) přísvitový modul, který umožňuje monitorování za snížených nebo žádných světelných podmínek, především pak v noci. Dosvit IR modulu je maximálně 50 m. Každá jednotka je vybavena sabotážním kontaktem, který vyvolá poplach v případě snahy o zcizení kamery nebo její části. Záznam z kamer je uchováván na záznamovém zařízení, které dokáže archivovat nahrávky ve 24 hodinovém záznamovém režimu až 3 týdny nazpět.

Obr. 12 CCTV + IR modul, duální elektronické bariéry [Zdroj: vlastní]

Trafostanice a její vnitřní prostory jsou střeženy infračerveným pohybovým čidlem, které detekuje pohyb uvnitř technologického kiosku. Dveře trafostanice jsou chráněny proti vysazení a dále zabezpečeny zámkovým systémem včetně použití magnetických kontaktů detekujících otevření dveří. Každá trafostanice je vybavena detektorem kouře, který v případě požáru vyhlásí poplašný signál na vstup zabezpečovací ústředny, která o incidentu vyrozumí PCO, dohledové centrum a majitele FVE.

Předmětová ochrana panelů je řešena pomocí jednožilového kabelu, který je propleten otvory v rámu panelu a tvoří nepřerušenou smyčku. Každá řada panelů má vlastní detekční zónu, proto je možné poměrně přesně určit, kde v objektu dochází k manipulaci s chráněnými předměty. Dráty jsou připojeny do sdružovacích jednotek, které komunikují se zabezpečovací ústřednou. Pomocí smyčkového drátu byly dodatečně zabezpečeny i střídače napětí.

Zabezpečovací ústředna EZS je umístěna v prostorách jedné z trafostanic. Do této ústředny jsou svedeny výstupy všech bezpečnostních čidel a bariér, použitých v objektu. Samotná ústředna je napájena záložní baterií a její výstup je vyveden na duální GSM komunikátor, zabezpečující datovou komunikaci s PCO a dohledovým centrem, které spravuje FVE na základě smluvního vztahu. Funkčnost celého systému je zpravidla každý měsíc fyzicky ověřována vyškoleným technikem.

4 ANALÝZA BEZPEČNOSTNÍCH RIZIK

V následující části práce se budu věnovat vyčíslení investovaných částek do chráněných aktiv, analýze a vyhodnocení identifikovaných rizik. Pomocí graficky znázorněného Ishikawova diagramu provedu strukturální a procesní identifikaci rizika a vybranou metodou identifikovaná rizika zhodnotím. Výsledky analýzy poté verifikuji na základě Paretova principu 80/20 a graficky znázorním pomocí Lorenzovy křivky.

4.1 Analýza chráněných aktiv

Aby bylo možné efektivně investovat do zabezpečení objektu, je vhodné provést analýzu aktiv, na jejímž základě lze určit maximální možnou přípustnou částku, kterou lze do zabezpečení investovat. V tabulce 1 je uvedena hodnota chráněné technologie. Dle principu As Low as Reasonably Achiavable (ALARA) je přípustné investovat do zabezpečení kolem 10 % (ve zvláštních případech až 15 %) z celkové částky chráněných aktiv. Riziko je následně nutné snižovat tak dlouho, dokud náklady na zabezpečení objektu nepřesahují hodnotu chráněného zájmu. [17]

Tabulka 1 Chráněná aktiva objektu fotovoltaické elektrárny

pol.	Aktiva objektu fotovoltaické elektrárny	
1	Oplocení objektu	1 500 000,- Kč
2	Konstrukce pro montáž panelů	33 100 000,- Kč
3	Fotovoltaické panely (21 376 ks)	181 500 000,- Kč
4	Střídače (334 ks)	27 600 000,- Kč
5	Trafostanice a kiosky (včetně kabeláže)	3 450 000,- Kč
6	Ostatní (projekt, audit, revize)	180 000,- Kč
Celkem		**247 330 000,- Kč**

[Zdroj: vlastní]

Dle tabulky 1 byla hodnota chráněných aktiv vyčíslena na 247 330 000,- Kč. Z toho vyplývá, že do zabezpečení objektu je přípustné investovat maximálně 24 733 000,- Kč. Reálná hodnota investovaná do bezpečnostní technologie byla 3 650 000,- Kč, což je přibližně 15 % z přípustné investiční částky.

Pro případné rozšiřování bezpečnostní technologie je zde, z hlediska investic, poměrně velký prostor. Mnoho majitelů FVE však na elektronickém zabezpečení neuváženě a přílišně šetří. Kalkulace byla poskytnuta majitelem objektu a je uváděna bez DPH.

4.2 Procesní a strukturální identifikace bezpečnostních rizik

Analýza a hodnocení bezpečnostních rizik v objektu je základním předpokladem pro úspěšné řídící a rozhodovací procesy. V praxi se využívá velkého množství různých metod, které se nadále rozrůstají a zpřesňují. Mezi často používané metody můžeme zařadit metodu Fault Tree Analysis (FTA), neboli analýzu stromem poruch a dále analýzu Event Tree Analysis (ETA), tedy analýzu stromem událostí. Tyto dvě předchozí metody bývají často doplňovány o analýzu Failure Mode and Effect Analysis (FMEA), jež analyzuje možné poruchy systému a jejich následky.

Pro potřeby této práce jsem zvolil metodu Ishikawova diagramu, dle kterého provedu analýzu procesních a strukturálních bezpečnostních rizik. Výsledkem je identifikace nejzávažnějších rizik, které graficky znázorním do přehledného modelu, často také nazývaného modelem rybí kosti.

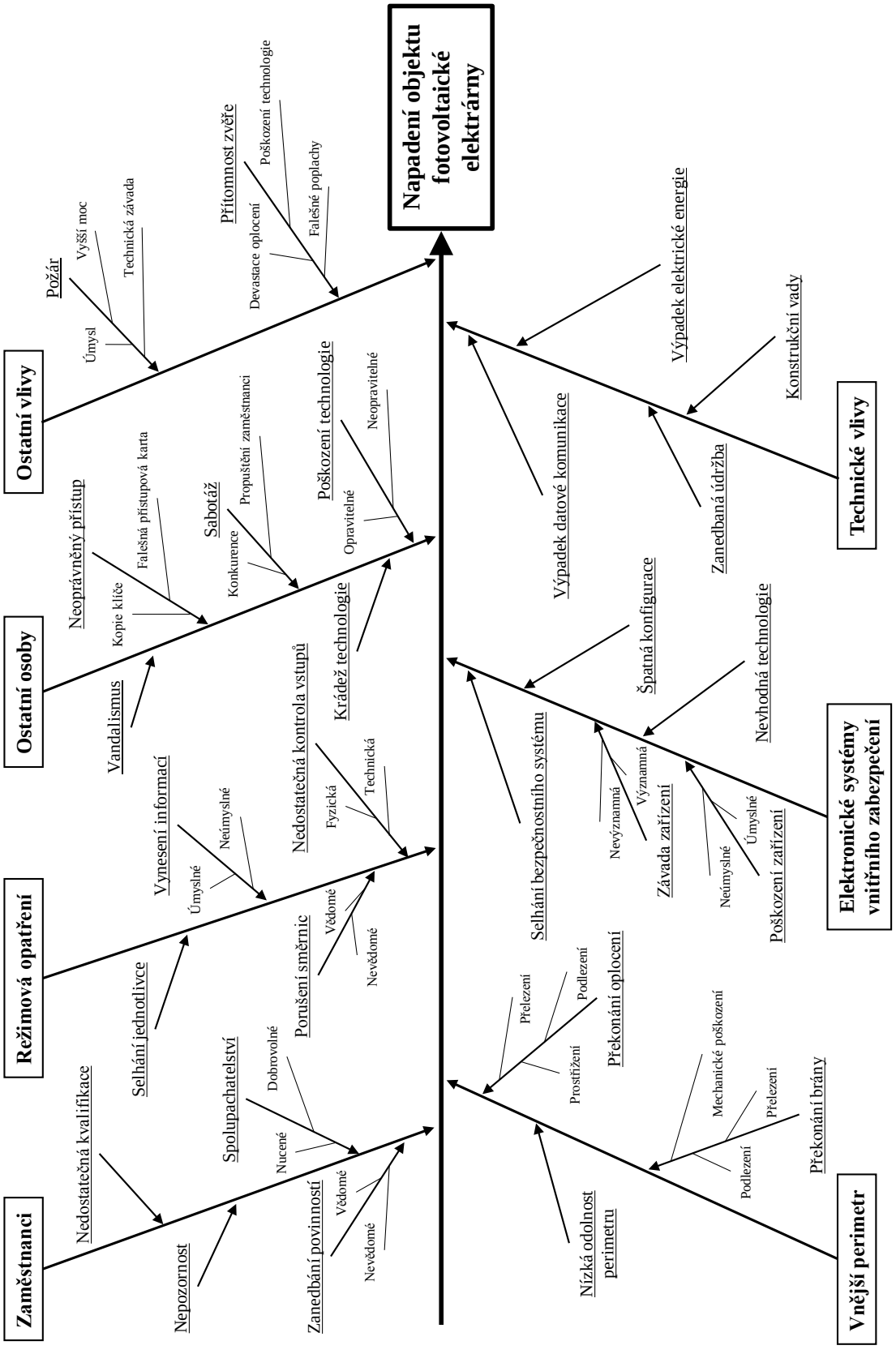
Analýzou procesní identifikace rizika lze vymezit pravděpodobné příčiny ohrožení bezpečnosti objektu včetně kroků, které mohou těmto hrozbám předcházet. Pravděpodobně nejslabším místem celého bezpečnostního systému je selhání lidského faktoru, který může následnou bezpečnost objektu přímo nebo nepřímo ovlivnit. Lidský faktor byl do modelu zapracován v podobě procesních rizik. Při projektování fotovoltaické elektrárny by měl být brán zřetel zejména na profesní odbornost pracovníků a co možná nejvíce omezit styk osob s citlivými daty o zabezpečovacím zařízení, aby nemohlo dojít ke zneužití informací.

Strukturální identifikace rizik představuje analýzu technických nebo konstrukčních závad, které mohou bezprostředně ohrozit bezpečnost chráněného objektu nebo mít zásadní vliv na selhání bezpečnostního systému jako celku. Jedná se zejména o závady na elektrickém zařízení či jeho špatném nastavení.

Analýzou bezpečnostních rizik stanovím slabá místa celého bezpečnostního systému, se kterými je třeba dále pracovat (například zajistit náhradní bezpečnostní zařízení v případě poruchy, zdvojit GSM komunikátor, použít záložní baterie atd.).

4.3 Modelování vybraných bezpečnostních rizik

Modelováním vybraných bezpečnostních rizik jsem identifikoval procesní a strukturální rizika za pomoci grafické metody přehledného Ishikawova diagramu na obrázku 13. Identifikovaná rizika z Ishikawova diagramu vyhodnotím metodou Failure Mode and Effects Analysis a uspořádám do tabulky podle nejvyšší rizikovosti.



Obr. 13 Identifikace bezpečnostních rizik v Ishikawově diagramu [Zdroj: vlastní]

4.4 Hodnocení vybraných bezpečnostních rizik

Hodnocení rizik jsou předem dané postupy, které přispívají k rozvoji poznání rizika a slouží pro potřeby rozhodovacího procesu. Cílem hodnocení rizik je zajistit rozhodování ve prospěch chráněného zájmu, a proto musí být používán otestovaný model, který zaručuje objektivitu a nezávislost. V řadě případů jsou posuzované problémy komplexní nebo mají mnoho nejistot, což vyžaduje použití složitějších vyhodnocovacích metod (často za pomoci náročných softwarových programů).

V následující kapitole provedu hodnocení jednotlivých rizik pomocí metody Failure Mode and Effects Analysis (FMEA), která vychází z předchozí identifikace rizik na základě Ishikawova diagramu. Rizika budu vyhodnocovat zvlášť pro hledisko procesní a zvlášť pro hledisko strukturální, i když mohou dohromady tvořit určité celky, které se navzájem prolínají a ovlivňují.

Metoda FMEA je metodou analýzy příčin a následků poruch systému, kterou lze sledovat jednotlivé poruchy, či skupiny poruch bezpečnostního systému. Pomocí této metody se identifikují zdánlivě jednoduché poruchy, které však mohou významně přispívat k havárii nebo ohrožení objektu. Může být provedena jedním analytikem, nicméně by výsledky měly být zkontrolovány analytikem druhým. Metoda FMEA se ale nehodí pro obsáhlý výčet seznamů poruch, pro který je vhodnější používat jinou robustnější vyhodnocovací metodu, nejlépe pak za současného použití odborné softwarové podpory.

Cílem analýzy dle FMEA je zjištění nejpravděpodobnějších příčin a událostí vedoucích ke snížení bezpečnosti nebo spolehlivosti celého bezpečnostního systému. Obvykle se provádí formou přehledné tabulky s uvedením jednotlivých rizik a výchozí hodnotou metody je výpočet rizikového čísla R. Výstupem metody je pak ucelený přehled možných rizik, na jehož základě lze navrhnout určitá opatření k redukci nejzávažnějších z nich. [8]; [9]

Výpočet rizikového čísla R (1):

$$R = P * N * H \tag{1}$$

Kde: R- míra rizika,
P- pravděpodobnost vzniku rizika,
N- závažnost následků,
H- odhalení rizika.

K výpočtu rizikového čísla R jsem vybral procesní a strukturální rizika dříve identifikovaná v Ishikawově diagramu. Výpočtem ověřím, zdali se jedná o závažné nebo bezvýznamné riziko.

Míra rizikovosti a pravděpodobnost vzniku rizika je uvedena v tabulce 2, kde byl stanoven předpoklad pro vznik rizika od nahodilého až po trvalý stav. Posouzení závažnosti následků, které mohou způsobit malý úraz nebo až dokonce smrt, jsem seřadil do tabulky 3, stejně tak jako možnou odhalitelnost rizika.

Pro potřeby této analýzy jsem vybral pouze 5 parametrů z celkového počtu 10, které udává norma ČSN EN 60812 Techniky analýzy bezporuchovosti systému – postup analýzy způsobů a důsledků poruch (FMEA).

Tabulka 2 Míra rizika a pravděpodobnost jeho vzniku

R	Míra rizika	P	Pravděpodobnost vzniku rizika
0-3	Bezvýznamné riziko	1	Nahodilá
4-10	Akceptovatelné riziko	2	Spíše nepravděpodobná
11-50	Mírné riziko	3	Pravděpodobná
51-100	Nežádoucí riziko	4	Velmi pravděpodobná
101-125	Nepřijatelné riziko	5	Trvalá

[Zdroj: 18]

Tabulka 3 Závažnost následků a odhalitelnost rizika

N	Závažnost následků	H	Odhalitelnost rizika
1	Malý delikt, malá škoda, malý úraz	1	Riziko odhalitelné v době jeho spáchání
2	Větší delikt, úraz s pracovní neschopností, velká škoda	2	Snadno odhalitelné riziko
3	Střední delikt, úraz s převozem do nemocnice, vyšší škoda	3	Odhalitelné riziko
4	Těžký delikt, těžký úraz s trvalými následky, vysoká škoda	4	Nesnadno odhalitelné riziko
5	Smrt osob, velmi vysoká škoda na majetku	5	Neodhalitelné riziko

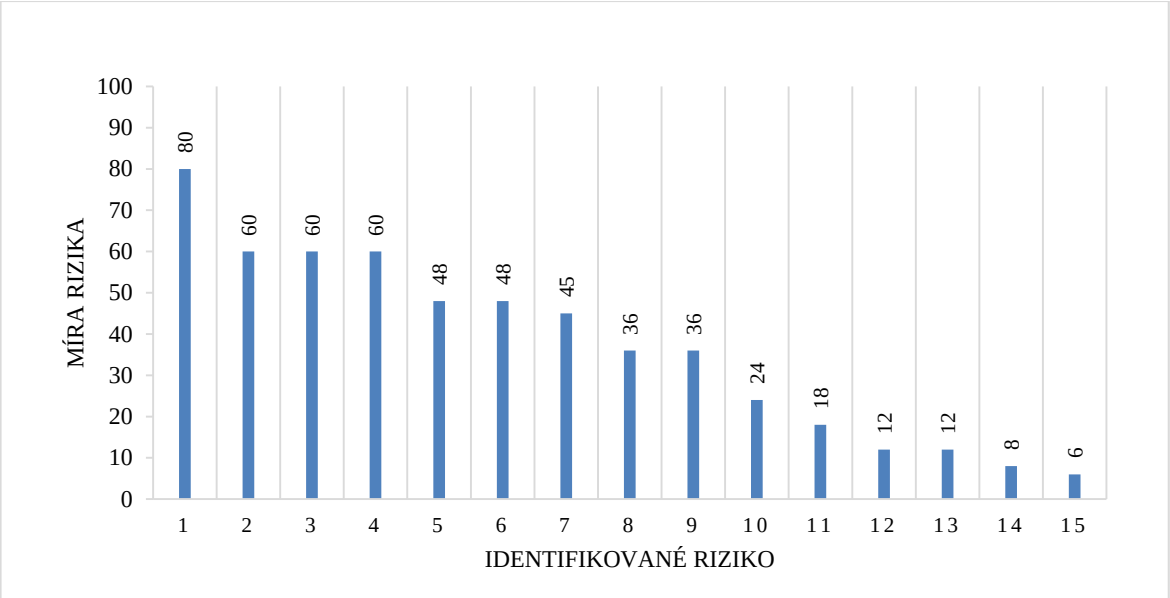
[Zdroj: 18]

Identifikovaná bezpečnostní rizika z procesního hlediska jsem sestupně uspořádal do tabulky 4 podle vypočtené míry rizika R. Pro snazší verifikaci vybrané FMEA analýzy jsem tabulku doplnil o četnost výskytů R a celkovou kumulativní četnost výskytů. Míru závažnosti výsledků analýzy v tabulce 4 jsem následně přehledně graficky zpracoval do grafu 1.

Tabulka 4 Analýza procesního rizika

p.č.	Identifikace procesního rizika	R	P	N	H	Četnost	Kumulativní četnost
1	Vandalismus	**80**	5	4	4	3,70 %	3,70 %
2	Neoprávněný přístup	**60**	5	4	3	11,11 %	14,81 %
3	Krádež technologie	**60**	5	4	3	11,11 %	25,93 %
4	Poškození technologie	**60**	5	3	4	11,11 %	37,04 %
5	Sabotáž	48	4	3	4	7,41 %	44,44 %
6	Spolupachatelství	48	3	4	4	7,41 %	51,85 %
7	Nedostatečná kontrola vstupů	45	5	3	3	3,70 %	55,56 %
8	Vynesení informací	36	3	4	3	7,41 %	62,96 %
9	Porušení směrnic	36	3	4	3	7,41 %	70,37 %
10	Požár	24	3	4	2	3,70 %	74,07 %
11	Selhání jednotlivce	18	2	3	3	3,70 %	77,78 %
12	Přítomnost zvěře	12	4	1	3	7,41 %	85,19 %
13	Zanedbání povinností	12	2	3	2	7,41 %	92,59 %
14	Nepozornost	8	1	4	2	3,70 %	96,30 %
15	Nedostatečná kvalifikace	6	1	3	2	3,70 %	100,00 %

[Zdroj: vlastní]



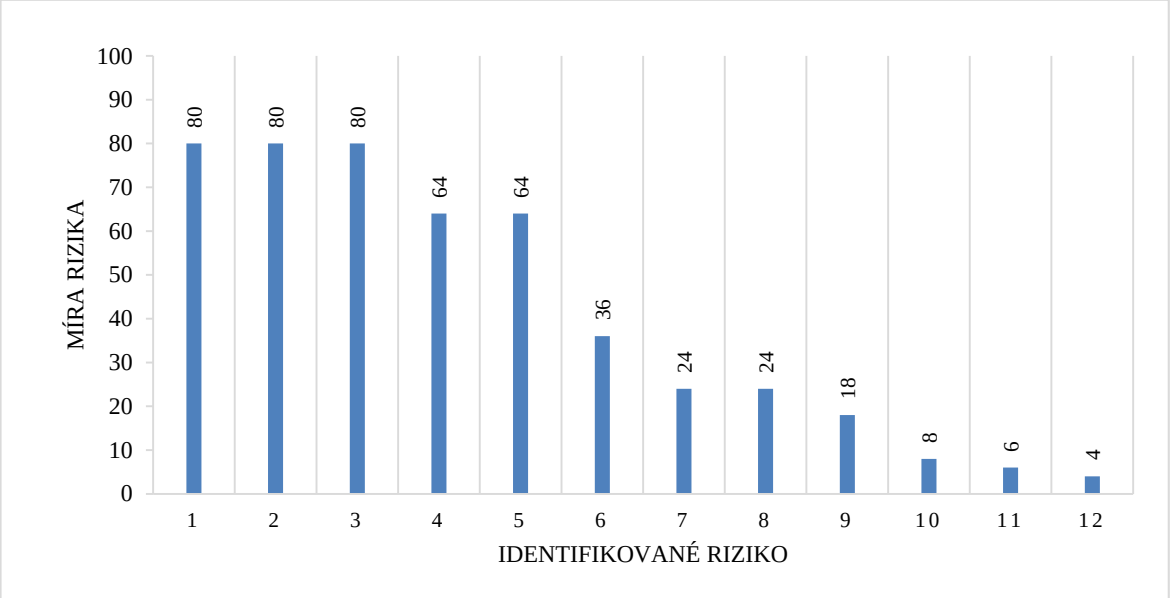
Graf 1 Míra závažnosti procesního rizika [Zdroj: vlastní]

Stejně jako v případě procesních rizik, jsem identifikovaná strukturální rizika zapracoval do tabulky 5 a vyhodnocenou míru závažnosti graficky znázornil do grafu 2. I v případě strukturálních rizik je tabulka 5 doplněna o četnost výskytů R a celkovou kumulativní četnost všech výskytů.

Tabulka 5 Analýza strukturálního rizika

p.č.	Identifikace procesního rizika	R	P	N	H	Četnost	Kumulativní četnost
1	Překonání oplocení	**80**	5	4	4	13,64 %	13,64 %
2	Překonání brány	**80**	5	4	4	13,64 %	27,27 %
3	Poškození zařízení EZS	**80**	5	4	4	13,64 %	40,91 %
4	Selhání bezpečnostního systému	**64**	4	4	4	9,09 %	50,00 %
5	Závada zařízení	**64**	4	4	4	9,09 %	59,09 %
6	Špatná konfigurace	36	3	4	3	4,55 %	63,64 %
7	Výpadek elektrické energie	24	3	4	2	9,09 %	72,73 %
8	Výpadek datové komunikace	24	3	4	2	9,09 %	81,82 %
9	Zanedbaná údržba	18	2	3	3	4,55 %	86,36 %
10	Konstrukční vady	8	2	2	2	4,55 %	90,91 %
11	Nízká odolnost perimetru	6	1	3	2	4,55 %	95,45 %
12	Nevhodná technologie	4	1	2	2	4,55 %	100,00 %

[Zdroj: vlastní]

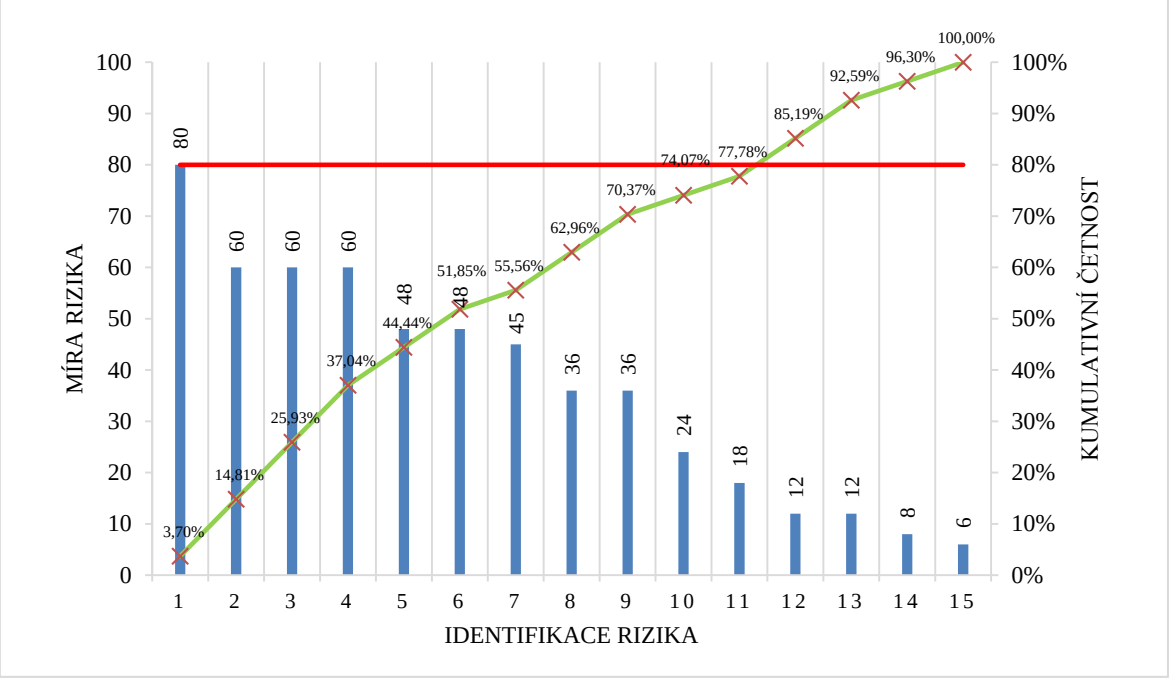


Graf 2 Míra závažnosti strukturálního rizika [Zdroj: vlastní]

Ke konečné verifikaci výsledků předchozích analýz dle FMEA jsem využil Paretovo pravidlo 80/20 a grafické znázornění Lorenzovou křivkou. Podle ekonoma Vilfreda Pareta, autora principu 80/20, platí, že 80 % všech důsledků pramení z 20 % všech příčin. Nepřijatelná rizika se pak vyznačují do 80 % součtu kumulativní četnosti a zbylých 20 % je považováno za rizika přijatelná. [18]

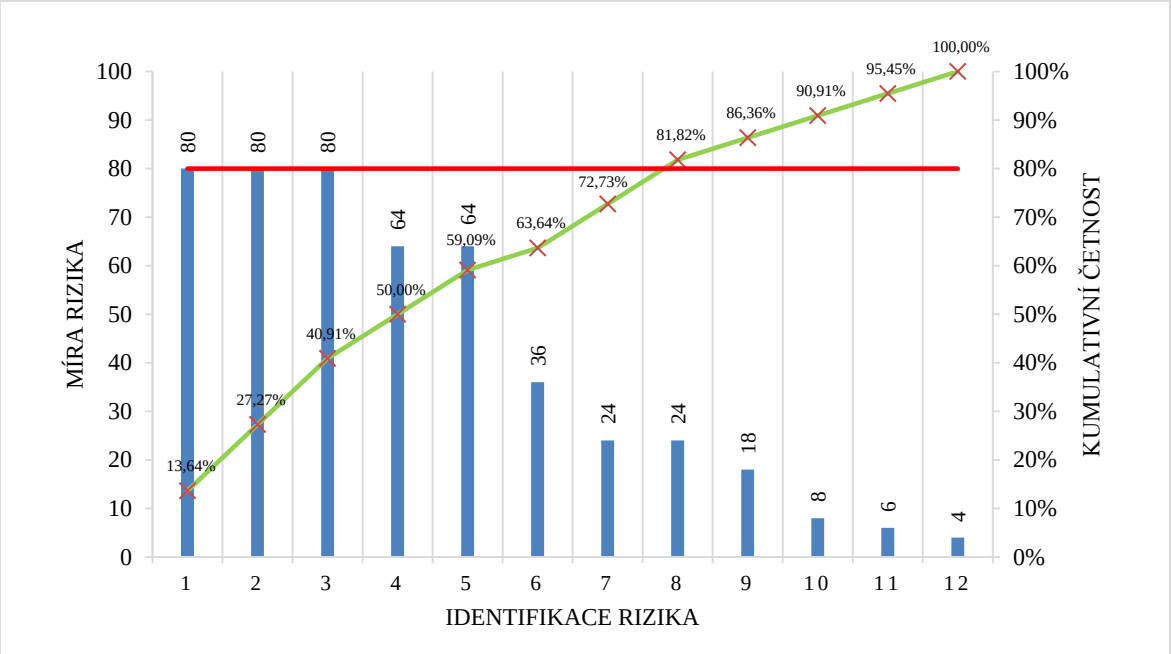
Kumulativní četnosti R, uvedené v tabulkách 4 a 5, jsem znázornil pomocí Lorenzovy křivky do grafů 3 a 4, opět zvlášť pro procesní a strukturální hledisko. Za nepřijatelná rizika jsem dle grafů označil všechna rizika, jejichž rizikové číslo R je vyšší než 50 a zároveň, jejichž kumulativní četnost výskytů je nižší než 80 %.

Závažná bezpečnostní rizika v objektu z procesního hlediska jsem na základě Paretova pravidla 80/20 z grafu 3 identifikoval v podobě vandalismu, neoprávněného vstupu, krádeže a poškození technologie, sabotáže, spolupráce s pachatelem, nedostatečné kontroly vstupů, vynesení citlivých informací, porušení směrnic, požáru a selhání jednotlivce.



Graf 3 Paretova analýza 80/20 – procesní hledisko rizika [Zdroj: vlastní]

Z hlediska strukturálního jsem za pomoci Paretova pravidla 80/20 z grafu 4 identifikoval bezpečnostní rizika v podobě překonání vnějšího perimetru, poškození zařízení EZS, selhání bezpečnostního systému, závady nebo špatné konfigurace zařízení a výpadku elektrické energie nebo datové komunikace.



Graf 4 Paretova analýza 80/20 – strukturální hledisko rizika [Zdroj: vlastní]

4.5 Výsledek analýzy bezpečnostních rizik

Na základě identifikace bezpečnostních rizik jsem určil 15 rizik z procesního hlediska a 12 rizik z hlediska strukturálního. Procesně nepřijatelných rizik jsem identifikoval 12, strukturálně pak 8. Takto určená rizika lze považovat za závažná, jelikož jsou v 80 % případů příčinou ohrožení chráněného zájmu. Zbylá rizika 20 % případů mohu, na základě analýz, považovat za zanedbatelná.

Dle Paretova pravidla 80/20 a výše rizikového čísla R jsem z celkového počtu rizik všech hledisek vybral 9 nejzávažnějších bezpečnostních rizik, které dle mého názoru a aplikovaného výpočtu, nejvíce ohrožují bezpečnost chráněného objektu. Tato rizika mají rizikové číslo R vyšší jak 50 a zároveň se jejich kumulativní součet četnosti vyznačuje do 80 % celkového součtu.

Nejzávažnější bezpečnostní rizika jsem přehledně setřídil do tabulky 6, zvlášť pro procesní a zvlášť pro strukturální hledisko. V praxi se však tato hlediska částečně nebo zcela překrývají a doplňují. Proto se musí částečně nebo zcela překrývat i návrhy na jejich redukci. Návrh na redukci jednoho určitého rizika však může významně ovlivnit míru závažnosti rizika druhého, případně druhé riziko zcela eliminovat. Příkladem může být překonání vnějšího perimetru. Pokud dokážeme snížit riziko překonání vnějšího perimetru, současně se sníží míra rizik krádeže nebo poškození technologie.

Tabulka 6 Nejzávažnější bezpečnostní rizika

Nejzávažnější bezpečnostní rizika			
č.	**Procesní hledisko rizika**	**č.**	**Strukturální hledisko rizika**
1	Vandalismus	1	Překonání oplocení
2	Neoprávněný přístup	2	Překonání brány
3	Krádež technologie	3	Poškození zařízení EZS
4	Poškození technologie	4	Selhání bezpečnostního systému
		5	Závada zařízení

[Zdroj: vlastní]

Z mého pohledu se nicméně nejzávažněji jeví rizika v podobě vandalismu, krádeže nebo poškození technologie. Selhání bezpečnostního systému je bezesporu také velmi významným problémem. Většina rizik je však přímo ovlivněna možností neoprávněného vstupu pachatele do objektu překonáním oplocení nebo vstupní brány. Proto by tyto rizika měla být co možná nejvíce redukována v první řadě.

Všem vybraným rizikům v tabulce 6 je třeba věnovat mimořádnou pozornost, protože se jedná o nejpravděpodobnější příčiny napadení objektu a tudíž i ohrožení chráněné technologie.

Samostatnou kapitolou je selhání bezpečnostního systému nebo jeho části, které se nikdy nedá spolehlivě simulovat a otestovat. Kvalitnější zařízení by proto měly být v oblasti zabezpečení preferovány a vybírány na základě dlouhodobých zkušeností.

5 NÁVRH NA REDUKCI VYBRANÝCH BEZPEČNOSTNÍCH RIZIK

Na základě analýz v předchozí kapitole jsem určil nejzávažnější rizika, se kterými je nutné dále pracovat. V této kapitole se pokusím navrhnout řešení k redukci rizika pro 6 vybraných bezpečnostních rizik. Největší prostor pro redukci rizika spatřuji v aktivním monitorování okolí objektu v periodickém časovém úseku. Výsledkem by měl být přehled, co se v okolí objektu fotovoltaické elektrárny odehrává, jaké je sociální složení a úroveň místního obyvatelstva. Případné napadení objektu pachatelem je nejčastěji iniciováno právě od nejbližších osob, které mají nad děním v objektu určitý přehled (např. kdy, kdo a jak se v objektu pohybuje). Nedílným požadavkem je také rychlá reakce zásahové bezpečnostní agentury, která by měla mít v rizikovějších oblastech kratší dojezdovou dobu.

Současně je nutné podotknout, že objekt vybrané fotovoltaické elektrárny je poměrně dobře technicky zabezpečen. V objektu nechybí žádný základní prvek pasivní ochrany, technická ochrana elektronickými zabezpečovacími prvky je vzájemně provázána a tvoří tak komplexní celek bezpečnostního systému. Všeobecným problémem, které jsem do analýzy nezahrnul, jsou nepředvídatelné vlivy počasí. Většina fotovoltaických elektráren je však proti zásahu vyšší moci (úder blesku, kroupy, vniknutí vody do zařízení atd.) kryta pojistkou. Při projektování je pak nutné s těmito riziky počítat a do projektu zakomponovat kupříkladu odtokové kanály kolem trafostanic, vodotěsné kabelové průchodky, aktivní nebo pasivní hromosvodové systémy a použití přepěťových ochran. Fotovoltaické panely a střídače napětí splňují normu krytí proti vniknutí vody, a proto je lze bez starostí používat ve venkovním prostředí. Trafostanice a ostatní elektrická zařízení jsou ukryta v kiosku, chráněném betonovým skeletem se střechou.

Vandalismus je rozšířený problém napříč společností. Většinou je páchán bez zjevného úmyslu a pachateli slouží spíše pro odreagování. Pachatelům jde o jistý druh adrenalinového zážitku a těší je, pokud napáchají co nejvíce škody. Napadení objektu fotovoltaické elektrárny vandaly bývá nejčastěji realizováno velmi rychlým útokem zpoza vnějšího perimetru. Vandalové přehazují oplocení, a kameny nebo cihlami rozbíjejí fotovoltaické panely, případně přestřihují detekční perimetrické kabely nebo ničí oplocení. Známy jsou také případy vhození nádoby s barvou do objektu elektrárny, kdy barva pokryla větší plochu panelů a znehodnotila je, nebo také sestřelování kamerových jednotek plynovými pistolemi. Proti vandalismu je však tato elektrárna kryta určitým pojištěním. Pro snazší identifikaci a dopadení případného pachatele, je prostor před a za oplocením monitorován kamerami s dlouhodobým záznamem. Rozpoznání vandala a běžného vycházkového občana je

nicméně skoro nemožné a prakticky neexistuje žádné efektivní, automatizované a finančně únosné řešení pro předcházení případnému útoku.

Překonání oplocení nebo brány by mělo být především ztíženo mechanickou odolností použitých komponent, včetně instalované vrcholové zábrany. Mechanické namáhání, které vzniká při pokusu o překonání oplocení nebo brány, je detekováno perimetrickým kabelem. Pokud by pachatel překonal oplocení nebo bránu bez vyhlášení poplachu, jeho pohyb spolehlivě zachytí vnitřní elektronické bariéry. Bezpečnostní systém je na vybrané fotovoltaické elektrárně dobře zvolen. Případnou redukci rizika vidím především v pravidelné profylaxi celého systému a jeho samotném nastavení.

Krádež nebo poškození chráněné technologie by mělo být minimalizováno již v rámci předchozího odstavce. Mnoho pachatelů se však zachová vandalsky, pokud zjistí, že nejsou schopni panely odmontovat a zcizit. Vyhlášený poplach, patřičně akusticky signalizován, pachatele vyleká, a ti se snaží co nejrychleji prchnout nebo poplach „utišit“. Při takovém jednání pachatelé poškozují technologii za účelem utišení vyhlášeného poplachu, případně poničí ostatní vybavení při pokusu o útěk. Pro minimalizaci škod navrhuji zajištění včasného dojezdu zásahové bezpečnostní agentury na místo poplachu, eventuelně poplach akusticky signalizovat již při pokusu o překonání vnějšího perimetru. Samotné fotovoltaické panely a měniče vybraného objektu jsou dostatečně chráněny předmětovou ochranou za pomoci provlečeného signálního drátu. Takové zabezpečení je nad rámec základních možností, nicméně někteří investoři jej považují za zbytečné. Této rozlehlejší elektrárně však pomůže případnou krádež přesně lokalizovat tak, aby výjezdová služba přesně věděla, kde má zásah proti pachateli provést. Ušetřený čas pak zvyšuje efektivnost zásahu.

Selhání bezpečnostního systému je problém, který nemusí být nikterak detekován. Selhání může nastat bezprostředně při útoku, před nebo také po něm. Většinou se jedná o závady na elektronickém zařízení, respektive selhání vznikne v souvislosti se špatným nastavením systému a čidel nebo jejich nedostatečné údržby. Riziko selhání systému nelze nikdy zcela vyloučit. Jako redukci rizika spojeného se selháním bezpečnostního systému navrhuji periodickou kontrolu zařízení včetně periodické údržby jeho okolí (zkrácení vysokého porostu trávy, větví stromů zasahujících do oplocení atd.). Pro kontrolu stavu kamerového systému, včetně kontroly kapacity záznamového zařízení, navrhuji vzdálenou kontrolu 3x týdně. Pro fyzickou kontrolu všech elektronických prvků technikem, včetně odzkoušení funkčnosti elektronického zabezpečovacího systému s PCO, navrhuji periodickou kontrolu v 1 měsíčním intervalu. Takto lze včas eliminovat případné špatné nastavení detektorů.

ZÁVĚR

V současnosti je bezpečnost chráněných zájmů a objektů stále důležitější téma. Tak, jak rychle se vyvíjejí a zdokonalují současné systémy ochrany a zabezpečení, stejným tempem nebo možná rychleji se vyvíjejí zařízení a technologie pro jejich překonání. Vždy existovala, a existovat bude, snaha o snadné nelegální nabytí hodnot. Standardní klasická ochrana se svým preventivním psychologickým účinkem, při současném splnění požadované úrovně zabezpečení a průlomové odolnosti, neztratila nic ze svého významu. Doplněna vhodnými prvky detekce narušení má stále svůj nepostradatelný význam. Její nepřekonatelnost je však bohužel pouze zdánlivá, protože není možné vytvořit naprosto dokonalé obvodové zabezpečení. Použitím EZS však lze případné napadení objektu včas odhalit a adekvátně na něj reagovat. Každé zabezpečení lze překonat, je otázkou za jak dlouho a jakým způsobem. Proto se k němu při návrhu a výběru technologie také tak musí přistupovat.

Cílem práce bylo posoudit současné možnosti technického zabezpečení vybraného objektu fotovoltaické elektrárny a také posoudit možná bezpečnostní rizika, která bezprostředně ohrožují vybraný objekt, respektive jeho chráněnou technologii. Na základě tohoto posouzení bylo dílčím cílem vypracovat návrh na redukci nejzávažnějších bezpečnostních rizik.

V první části práce jsem se zabýval důvody, kvůli kterým je nutné objekt fotovoltaické elektrárny patřičně zabezpečit. Následně jsem se zaměřil na teoretickou stránku související s mechanickým a technickým zabezpečením, fyzickou a režimovou ochranou. Zde jsem uvedl vhodné prvky a technologie používané pro zabezpečení různých objektů v praxi.

Druhá část práce byla zaměřena na seznámení se s vybraným objektem fotovoltaické elektrárny. V této části jsem popsal současnou úroveň a prvky zabezpečení vybraného objektu. Pomocí Ishikawova diagramu jsem identifikoval procesní a strukturální bezpečnostní rizika analýzou FMEA, která jsem poté verifikoval pomocí Paretova pravidla 80/20 a graficky znázornil použitím Lorenzovy křivky. Nakonec jsem vybral nejzávažnější rizika, pro něž jsem navrhl způsob jejich redukce. Jelikož je ale vybraný objekt velmi dobře technicky zabezpečen, návrhy na redukci rizika mají spíše režimový, respektive profylaxní charakter. Současné zabezpečení vybraného objektu fotovoltaické elektrárny považuji spíše za nadstandardní.

Závěrem bych chtěl říct, že žádný bezpečnostní systém nezajistí dokonalou ochranu chráněného zájmu. Proto je nutné bezpečnostní technologie naučit spolupracovat tak, aby se staly jedním komplexním autonomním celkem, který se vzájemně umí doplňovat.

SEZNAM POUŽITÉ LITERATURY

[1] ABBAS. *Perimetrie* [online]. 2012 [cit. 2013-02-14]. Dostupné z: http://www.abbas.cz/produkty-a-sluzby/technologie/perimetrie.

[2] ABBAS. *Termokamery FLIR* [online]. 2012 [cit. 2013-02-15]. Dostupné z: http://www.abbas.cz/clanky/pripadove-studie/ochrana-fve-termokamery-flir.

[3] ADI GLOBAL DISTRIBUTION. *Elektronické perimetrické systémy* [online]. 2012 [cit. 2013-03-04]. Dostupné z: http://www.adiglobal.cz.

[4] ALCAM PROFI. *Perimetrická ochrana objektů.* [online]. 2012 [cit. 2012-12-04]. Dostupné z: http://www.alcamprofi.cz/perimetricka-ochrana-objektu.html.

[5] AL-TEZA GROUP. *Záznamová zařízení - CCTV* [online]. 2012 [cit. 2013-01-04]. Dostupné z: http://www.altezagroup.cz/ochrana-majetku/42-kamerove-zabezpecovaci-systemy/76-zaznamova-zarizeni.

[6] APLEG SYSTEMS. *Plotové systémy* [online]. 2012 [cit. 2013-03-03]. Dostupné z: http://www.apleg-ploty.cz.

[7] ASSA ABLOY Czech & Slovakia. *Pyramida bezpečnosti* [online]. 2012 [cit. 2013-01-04]. Dostupné z: http://www.fab.cz/stranky/pyramida-bezpecnosti.

[8] BERNATÍK, Aleš. *Prevence závažných havárií I*. 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2006. 86 s. ISBN 80-866-3489-2.

[9] ČSN EN 60812. *Techniky analýzy bezporuchovosti systému – postup analýzy způsobů a důsledků poruch (FMEA)*. Praha: Český normalizační institut, 2007.

[10] HOLUBOVÁ, Věra; ŠČUREK, Radomír. *Ochrana objektu - transport peněz, cenin a eskorta osob*. Ostrava, 2008. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/ochrana_objektu.pdf. VŠB TU Ostrava.

[11] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.

[12] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

[13] MIVVY. *Sluneční mapa* [online]. 2012 [cit. 2013-02-08]. Dostupné z: http://solar.mivvy.eu/slunecni-mapa.

[14] OBNOVITELNÉ ZDROJE PARDUBICE. *Něco o fotovoltaice* [online]. 2012 [cit. 2013-01-24]. Dostupné z: http://www.solarni-vetrne-elektrarny.cz/info-fotovoltaice.

[15] SILEKTRO. *Instalace na volných plochách* [online]. 2012 [cit. 2013-01-24]. Dostupné z: http://www.silektro.cz/reference/instalace-na-volnych-plochach-2.

[16] S-TECH SYSTÉMY. *Kamerové systémy - CCTV* [online]. 2012 [cit. 2013-01-29]. Dostupné z: http://www.systemy-stech.cz/cctv.

[17] ŠČUREK, Radomír. THE SCIENCE FOR POPULATION PROTECTION. *Analýza rizik objektu kritické infrastruktury*. 2011. Dostupné z: http://www.population-protection.eu/attachments/038_vol3n1_scurek.pdf.

[18] ŠČUREK, Radomír. *Studie analýzy rizika protiprávních činů na letišti.* Ostrava, 2009. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/analyzy_rizika_letisti.pdf. VŠB TU Ostrava.

[19] UHLÁŘ, Jan. *Technická ochrana objektů.* Vyd. 1. Praha: Policejní akademie české republiky, 2005. 229 s. ISBN 80-725-1189-0.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ALARA	metoda As Low As Reasonably Achiavable - neboli „tak nízké, jak je rozumně dosažitelné“
CCTV	Closed Circuit Television - systém průmyslové televize
ČSN EN	převzatá (harmonizovaná) evropská norma
ČSN P ENV	evropská předběžná norma
ETA	metoda Event Tree Analysis - analýza stromu událostí
EZS	elektronická zabezpečovací signalizace
FMEA	metoda Failure Mode and Effects Analysis - analýza možného výskytu a vlivu vad
FTA	metoda Fault Tree Analysis - analýza stromu poruchových stavů
FVE	fotovoltaická elektrárna
GSM	komunikační standard pro mobilní komunikaci
H	index odhalení rizika
HDD	Hard Disk Drive - zařízení k uchovávání dat
IR	infračervené záření
N	index závažnosti následků
P	index pravděpodobnosti vzniku rizika
PCO	pult centrální ochrany
R	index míry rizika
Wh	watthodina, jednotka elektrické energie
Wp	nominální výkon fotovoltaických panelů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ