

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



ÚSTAV SOUDNÍHO INŽENÝRSTVÍ
INSTITUTE OF FORENSICS ENGINEERING

BEZPEČNOST PROVOZU MOBILNÍCH ROBOTŮ V INDOOR PROSTŘEDÍ

OPERATIONAL SAFETY OF MOBILE ROBOTS IN INDOOR ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

BC. JAKUB VOJTA

VEDOUCÍ PRÁCE
SUPERVISOR

ING. JIŘÍ KREJSA, PH.D.

BRNO 2012

ZADÁNÍ ZÁVĚREČNÉ PRÁCE

(na místo tohoto listu všíjte originál a nebo kopii zadání Vaší práce)

ABSTRAKT

Při spolupráci s firmou Bender Robotics. s. r. o. vznikl požadavek na posouzení provozní bezpečnosti autonomního mobilního robotu (AMR). Posouzení bezpečnosti je krokem na cestě k sériové výrobě robotu. Vstup výrobku na trh vyžaduje řetěz různých úkonů a posouzení bezpečnosti je jedním z nich.

K rozpoznání a ohodnocení závažnosti rizik bylo využito studia zákonných požadavků, osvědčených postupů daných normami, metody FMEA, experimentu a metody RIPRAN.

Analýza možných hrozeb, scénářů a rizik je probrána systematicky všemi oblastmi provozu robotu od vývoje, konstrukce, až po řídicí software. Kroky jsou popsány v logickém pořadí. Začíná se rešerší, pokračuje sérií analýz a končí se doporučeními ke snížení bezpečnostních rizik provozu autonomních mobilních robotů.

ABSTRACT

During cooperation with the Bender Robotics company a need for operational safety assessment of an autonomous mobile robot (AMR) emerged. Operational safety evaluation is a step towards mass production of the studied robot. Market entry of a product requires a string of various actions and safety assessment is one of them.

For risk identification and severity rating were used legal requirements, best practice given by standards, FMEA method, experiment and RIPRAN method.

Threats, possible scenarios and risks analysis is systematically discussed through all areas of operation of the robot, from design and construction to control software. All the steps are described in logical order. Starting with information research, going on with series of analysis and ending with suggestions for increased operational safety of autonomous mobile robots.

KLÍČOVÁ SLOVA

robot, robotika, provozní bezpečnost, FMEA, RIPRAN, DOE

KEYWORDS

robot, robotics, operational safety, FMEA, RIPRAN, DOE

PROHLÁŠENÍ O ORIGINALITĚ

Čestně prohlašuji, že diplomovou práci jsem vypracoval samostatně pod vedením svého vedoucího diplomové práce a s použitím odborné literatury, kterou jsem kompletně uvedl v seznamu literatury.

V Brně 23. 5. 2012

.....
Vojta Jakub

VZOR BIBLIOGRAFICKÉ CITACE

VOJTA, J. Bezpečnost provozu mobilních robotů v indoor prostředí. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2010. 65 s. Vedoucí diplomové práce Ing. Jiří Krejsa, Ph.D.

PODĚKOVÁNÍ

Děkuji zúčastněným z firmy Bender Robotics s. r. o., že jsem mohl být přítomen projektu, jehož smělým cílem je vytvoření funkčního a použitelného reálného výrobku. Dále děkuji vedoucímu své diplomové práce Ing. Jiřímu Krejsovi, Ph.D., za motivaci, rady a kolegiální přístup při tvorbě diplomové práce.

1 OBSAH

1	Obsah.....	11
2	Úvod.....	13
3	Formulace problému a cíle řešení.....	17
3.1	Úkol: Provedení rešerše platných norem.....	17
3.1.1	Plánované kroky při plnění úkolu.....	17
3.2	Úkol: Analyzovat bezpečnost provozu.....	17
3.2.1	Plánované kroky při plnění úkolu.....	18
3.3	Úkol: Navrhnout doporučení omezující rizika provozu aut. mob. robotů.....	18
4	Rešeršní studie.....	19
4.1	Současné přístupy k bezpečnosti.....	19
4.2	Management rizik.....	22
4.3	Opatření ke snižování rizik.....	22
4.4	Další vybrané přístupy řešení bezpečnosti.....	23
4.5	Metody posuzování bezpečnostních rizik.....	24
4.5.1	Kvantitativní metody analýz.....	24
4.5.2	Kvalitativní metody analýz.....	25
4.5.3	Komplexní postupy a modely.....	26
4.6	Technické normy.....	27
4.6.1	Normy mezinárodní.....	27
4.6.2	Evropské národní normy.....	28
4.6.3	Normy asociací, sdružení atp.....	28
4.6.4	Podnikové normy.....	29
4.6.5	Závaznost technických norem.....	29
4.6.6	Harmonizované normy a určené normy.....	29
4.6.7	Nalezené normy.....	30
4.7	Zákony.....	31
5	Rozbor problému.....	33
5.1	Zhodnocení rešeršní studie.....	33
5.2	Otázky v procesu analýzy systému.....	33
5.3	Autonomní mobilní robot Advee.....	35
5.3.1	Autonomní mobilní robot jako systém.....	36
5.4	Nalezené normy.....	37
5.5	Použité harmonizované normy.....	38
5.6	Dostupné prostředky a zdroje.....	38
5.7	Volba metod posuzování bezpečnosti.....	38
6	Provedení analýz.....	41
6.1	FMEA – analýza poruchových stavů.....	41
6.1.1	Tým FMEA.....	41
6.1.2	První sezení FMEA.....	41
6.1.3	Druhé sezení FMEA.....	44
6.2	Ověřovací experiment.....	44
6.2.1	Příprava experimentu.....	45
6.2.2	Popis experimentu.....	46
6.2.3	Výstup experimentu.....	47
6.3	Celková analýza bezpečnosti provozu AMR.....	47
6.3.1	Sepsání seznamu hrozba – scénář.....	47
6.3.2	Kvantifikace bezpečnostních rizik.....	48
6.3.3	Snižování rizika.....	48
7	Doporučení k provozu AMR.....	51
7.1	Role pracovníků.....	51

7.2	Obecná pravidla.....	51
7.3	Předpokládané použití robotu.....	52
7.4	Opatření ke snížení rizik plynoucích z elektrických zařízení.....	52
7.5	Opatření ke snížení rizik s lidským faktorem.....	54
7.6	Opatření ke snížení rizik plynoucích z mezních stavů a konstrukčních prvků.....	55
7.7	Opatření ke snížení rizik plynoucích z provozního prostředí.....	56
7.8	Opatření ke snížení rizik plynoucích z chyb softwaru.....	58
8	Závěr.....	59
9	Seznam použité literatury.....	61
10	Seznam obrázků, tabulek a příloh.....	63

2 ÚVOD

Hlavním smyslem této práce je prezentovat studii bezpečnosti konkrétního autonomního mobilního robotu a případně nalézt východiska společná pro provozování autonomních robotů obecně. Typickými hrozbami pro bezpečnost provozu tohoto robotu jsou různé projevy působení jeho kinetické a potenciální energie, ale i působení akumulované elektrické energie z jeho zdrojů napájení. Bohužel se negativně projevují i lidské chyby obsluhy a poruchy na jednotlivých funkčních částech. Myšlenky na bezpečnost robotu se prosazují již od počátku jeho vývoje, takže většina pohyblivých částí je skryta pod karosérií a řídicí elektronika má pojistné prvky. Robot disponuje sítí senzorů zabraňujících jeho vrážení do okolních předmětů a pádům.

Při uvádění nových výrobků na trh musí výrobce naplnit zákonné požadavky na bezpečnost a spolehlivost výrobku. Důvodem je snaha ochránit uživatele výrobku (spotřebitele), jeho zdraví, majetek a další. Ačkoliv základní motivací výrobce – podnikatele – je vytváření zisku, budování etického a důvěryhodného vztahu se spotřebitelem je předpokladem pro prosperitu podniku. Z toho důvodu by neměl vidět zákony a normy jako překážku, spíše jako jasně dohodnutá pravidla hry. Jsou pro něj vodítkem k dosažení oboustranné spokojenosti.

Česká republika vstupem do Evropské unie získala přístup na obrovský trh, platí zde sjednocená pravidla, tzv. směrnice ES (Evropského parlamentu a rady). Tyto směrnice jsou platné pro všechny členské země a je povinností každé z nich je zapracovat do svých národních zákonných aparátů. To přináší výhodu pro podnikatele, kteří mohou počítat s platností směrnic jak doma, tak v EU.

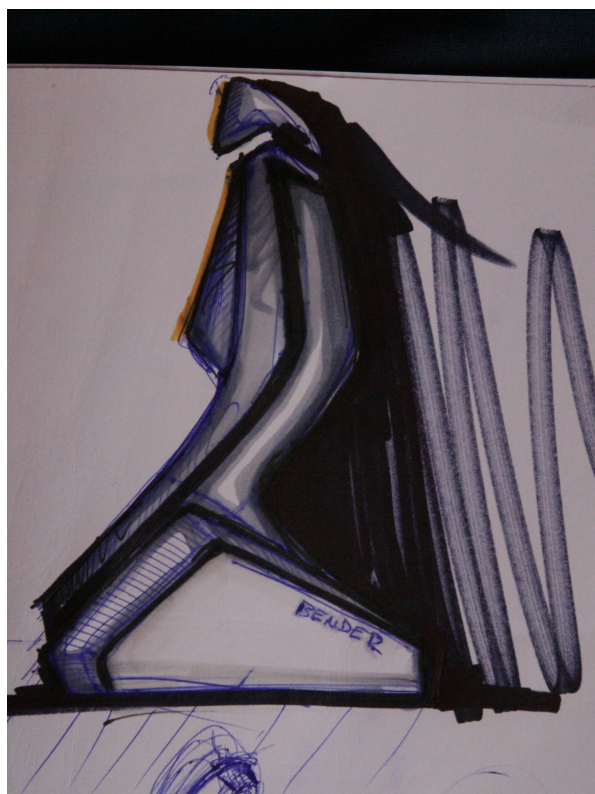
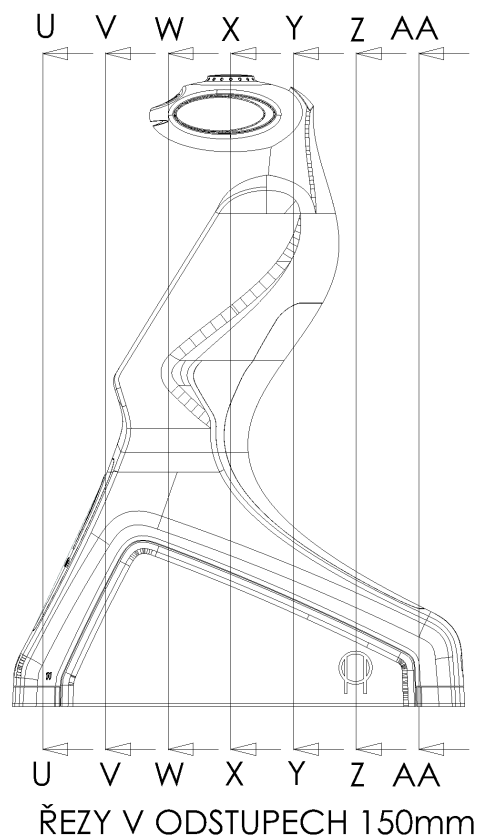
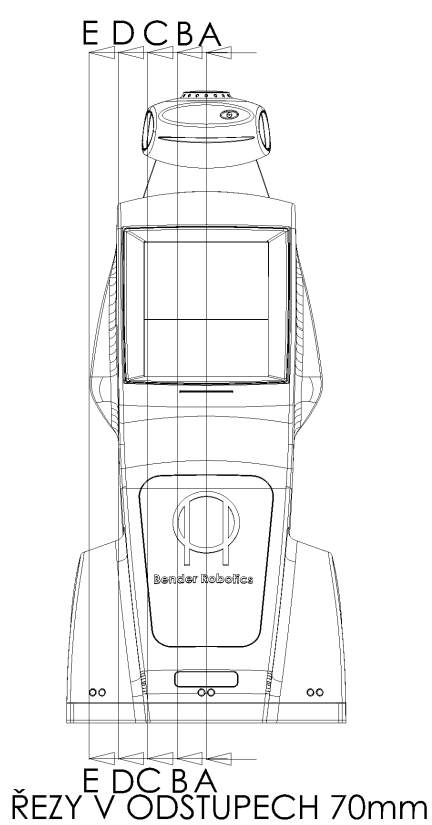
Právní předpisy EU se do zákonného aparátu ČR zavádějí jako zákony, nařízení a vyhlášky. Velká množina předpisů zaváděných v ČR upravuje požadavky na vlastnosti produktů, jež mají být uvedeny na trh anebo se mají využívat ke svému účelu. Bodem zájmu jsou tzv. směrnice nového přístupu, stanovující základní požadavky na bezpečnost výrobků a procedury, jimiž je podmíněno jejich uvedení na trh. Používání těchto směrnic je spojeno s používáním norem, s činnostmi notifikovaných míst, s vydáním prohlášení o shodě a označováním výrobků značkou CE. [1]

Kromě směrnic ES dále existují evropské normy (EN) a české technické normy (ČSN). Normy sice nejsou povinné, ale jejich neplnění může vést k porušování zákona, protože zákony se na tyto normy odkazují. Pokud se výrobci řídí normami, znamená to, že používají nejlepší praxe. Nakonec si mohou plnění požadavků norem nechat za určitých

podmínek certifikovat.

Kromě plnění zákonných požadavků je známa řada metod, jak bezpečnost prakticky ověřovat. Většinou se postupuje vytvořením týmu, který si postupně klade logické otázky o bezpečnostních hrozbách a hledá odpovědi. Ačkoliv jsou konstruktéři při stylu myšlení „Co se může pokazit?“ značně nervózní, přínos tohoto postupu je evidentní.

V této práci bude bezpečnost ověřována v logickém pořadí metodami FMEA, RIPRAN a experimentálně. V závěru budou formulována doporučení ke snižování bezpečnostních rizik.



Obr. 1: Nárys, bokorys, představa designera a realita, zdroj [2]

3 FORMULACE PROBLÉMU A CÍLE ŘEŠENÍ

Robot Advee vznikl jako společný produkt absolventů VUT v Brně. Je to komplexní stroj skládající se z cca. 700 jednotlivých dílů a součástí.[2] Už od chvíle, kdy konstrukce robotu nabrala směr k vytvoření komerčního produktu, mají tvůrci zájem o vytvoření kvalitního a bezpečného produktu. Z této snahy vznikla poptávka po analýze bezpečnosti autonomního mobilního robotu Advee.

3.1 Úkol: Provedení rešerše platných norem

Tento úkol má za cíl prohledat technické normy platné v rámci Evropské unie a identifikovat ty, jež se vztahují na zkoumaný produkt – autonomní mobilní robot v indoor prostředí. Úkol bude komplikován tím, že možná žádné normy konkrétně pro tento produkt nebyly navrženy a schváleny. Případně nalezené normy by měly být prostudovány. K tomu je potřeba ověřit jejich dostupnost, organizaci, která je vydala, cenu za výtisk nebo elektronickou kopii.

3.1.1 Plánované kroky při plnění úkolu

- Navštívit databáze standardizačních organizací a prohledat je v kontextu zkoumaného produktu. [3], [4]
- Prostudovat zákony České republiky regulující bezpečnost produktů.
- Prostudovat závěrečné práce zabývající se posouzením bezpečnosti nějakého produktu a identifikovat použitelné normy. [5],
- Kromě případných norem konkrétně určených pro zkoumaný produkt budou brány na zřetel i normy zaměřené buď na produkty obecně, nebo na nějaký technický detail použitý v produktu.
- V případě, že takové normy nebudou nalezeny, podobně jako v případě norem se vyhledá zákon obecný, který se na bezpečnost podobných výrobků vztahuje.
- Nezastupitelnou pomocí v tomto hledání budou existující publikace dotýkající se posuzování bezpečnosti (ideálně autonomních mobilních robotů) a vydávání tzv. prohlášení o shodě.
- Nalezení vhodných metod k posouzení rizik.

3.2 Úkol: Analyzovat bezpečnost provozu

- Technická praxe zná postupy posuzování bezpečnosti provozu strojních zařízení. Počítá se se spoluprací vývojářů z firmy Bender Robotics s. r. o.

3.2.1 Plánované kroky při plnění úkolu

- Na základě rešerše zákonů a norem zvolit oblasti posouzení bezpečnosti.
- Zvolit metody posuzování bezpečnosti.
- Připravit podmínky pro posouzení bezpečnosti.
- Vytvořit tým
- Dát základní školení osobám zodpovědným za vývoj částí robotu.
- Spolupracovat s osobami zodpovědnými za vývoj jednotlivých částí robotu.
- Provést připravené analýzy.

3.3 Úkol: Navrhnout doporučení omezující rizika provozu aut. mob. robotů

- Na základě provedených analýz navrhnout doporučení ke snížení rizik provozu AMR.
- Snažit se rozčlenit doporučení podle vhodného kritéria. Například podle zdroje rizika.

4 REŠERŠNÍ STUDIE

Tato kapitola je výčtem materiálů souvisejících s bezpečností AMR (autonomních mobilních robotů). Jsou zde nalezené normy, odkazy k zákonům, teze a teoretická východiska k bezpečnosti.

4.1 Současné přístupy k bezpečnosti

Co je středem zájmu?

Ekonomika se točí okolo produktů. Produkt je například výrobek továrny, ale i služba právního poradenství. Je tedy výstupem snažení firem. Například zákon 22/1997 Sb. „O technických požadavcích na výrobek“ používá pouze termín „výrobek“. Podle tohoto zákona je to jakákoliv věc, která byla vyrobena, vytěžena nebo jinak získána bez ohledu na stupeň zpracování a je určena k uvedení na trh. Technická praxe pojmy produkt a výrobek nerozlišuje, i když si například v současné terminologii norem ISO nejsou zcela rovné.[6]

Co je bezpečnost?

Bezpečnost je obecně vymezena jako stav objektu (výrobku, produktu), procesu nebo systému, u nichž při užívání k jejich stanovenému účelu je riziko ohrožení veřejných oprávněných zájmů omezeno na přijatelnou úroveň. Zajištění požadované úrovně bezpečnosti je tedy založeno na identifikaci, analýze, zhodnocení a ošetření rizik, přičemž rizikem se obecně rozumí kombinace četností nebo pravděpodobností výskytu specifikované nebezpečné události a jejich následků pocházejících z jejich činnosti.[6]

Odpovědnost za bezpečnost sdílejí výrobci se zákazníky. Zákazníci mají odpovědnost za správné užívání, tj. úplné dodržování instrukcí, provozních podmínek a omezení, provádění preventivní údržby atd. Zajištění stanovené nebo požadované úrovně bezpečnosti je v zájmu výrobců i zákazníků.

Zadefinujme spolehlivost:

Je termín vyjadřující (podle norem ISO) pohotovost výrobku. Spolehlivost je ovlivněna bezporuchovostí, udržitelností a zajištěnou údržbou. Bezporuchovost znamená, že se nevyskytují jevy, které vedou k ukončení schopnosti výrobku plnit určenou funkci.[6] Udržitelností se myslí možnost zasahovat do výrobku a například vyměňovat součásti, jejichž životnost se blíží svému konci. Pod zajištěním údržby si lze představit pravidelné technické prohlídky.

Bezpečnost v souvislosti se spolehlivostí

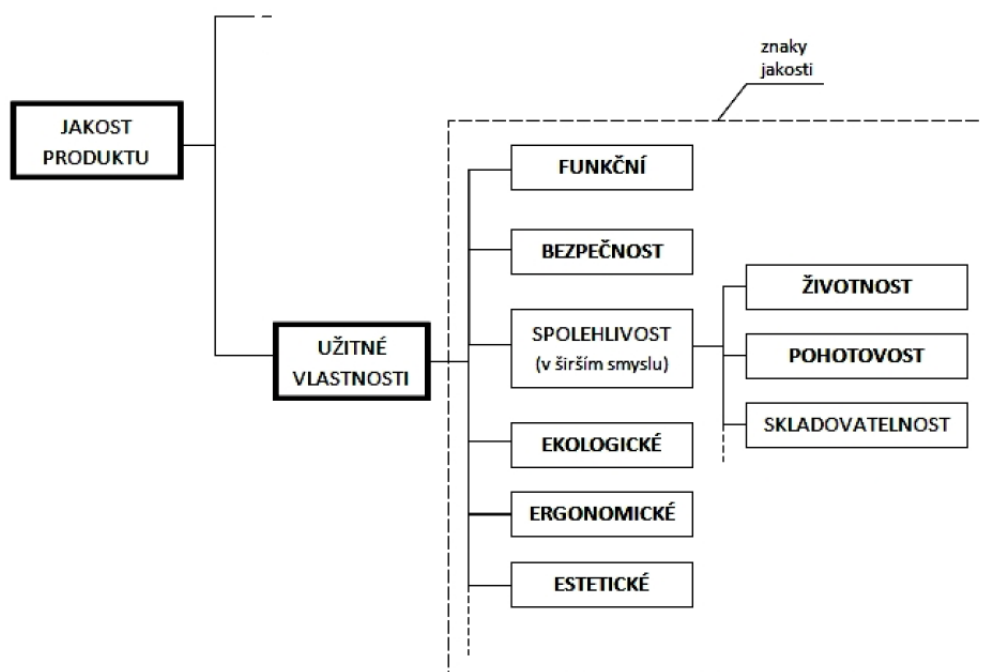
Bezpečnost nelze zaručit pouhým zajištěním spolehlivosti. Produkt, který je spolehlivý, a tedy pohotově plní svoji zamýšlenou funkci, zřejmě stále může představovat

bezpečnostní hrozby. Analyzovat spolehlivost je širší záměr než analyzovat bezpečnost. Zajišťování bezpečnosti předpokládá, že subsystémy jsou dostatečně spolehlivé.

Bezpečnosti nadřazený obor péče o jakost:

Nadřazený obor bezpečnosti je péče o jakost, česky je jakost „kvalita“, anglicky „quality“. Péče o jakost zahrnuje daleko více vlastností, než pouze bezpečnost, například:

- funkční vlastnosti – k jakému účelu se dá výrobek použít
- životnost – jak dlouho je možné produkt používat (než nastane mezní stav),
- skladovatelnost,
- ekologičnost,
- estetičnost.[6]



Obr. 2: Schéma vztahů jakost – bezpečnost, zdroj [6]

Intuitivní a individuální chápání jakosti – kvality:

Každý spotřebitel má intuitivně a individuálně zapsáno vnímání kvality. Zájemem výrobců je očekávání spotřebitelů naplňovat, aby se tento vracel s pocitem spravedlivého obchodu. Přestože spotřebitelé mohou definovat jakost různě podle svých preferencí, vznikají standardizované definice, kterými se může řídit výrobce. Tato standardní definování jakosti mohou být pro spotřebitele skrytá, nebo mimo jeho vnímání. Přesto slouží výrobcům

k naplňování očekávání spotřebitelů a ochráncům práv spotřebitelů k hodnocení produktů.

Definice podle autorit:

Jak již to bývá v oborech lidského bádání, neexistuje jednotná definice kvality. I když popisují stejnou věc, vlastní definice si vytváří například Americká společnost pro jakost, metodika Six sigma, norma ISO 9000, také jednotliví ekonomové, matematici i filozofové.

Jakost je v normě ISO 9000 (poněkud šifrovaně) definována jako „*stupeň splnění požadavků souborem inherentních charakteristik*“.[7] Do běžného jazyka by se asi dala definice přeložit jako „jak hodně produkt odpovídá předem daným požadavkům“.

Požadavek je například smluvní vztah mezi výrobcem a odběratelem o tom, jak má výrobek vypadat. Soubor charakteristik (požadavků) je množina vlastností produktu, které ho vymezují. Charakteristiku lze rozlišovat srovnáváním nebo měřením.

Jakost ať už měřitelná, nebo individuálně vnímaná spotřebitelem, se stává součástí výrobků. Uživatelé se ji naučili očekávat a vyžadovat. Výrobce, který správně zavede ve své výrobě mechanismus správy jakosti, má konkurenční výhodu, přispívá k budování důvěry a jeho jednotlivé výstupy se málo liší od svých předloh. Mimo těchto vlivů jsou samozřejmě důvody k péči o jakost povinné, dané zákony.

Zpět k riziku:

V souvislosti s bezpečností bylo zmíněno riziko jako kombinace pravděpodobnosti výskytu nebezpečné události a jejích následků. Pojem má zajímavou minulost, kdy pravděpodobně v mořeplavbě označoval útesy, kterým bylo nutné se vyhnout. Dnes souvisí s hrozbou obecně. Myslí se jím nebezpečí vzniku škody, poškození, ztráta a zničení, případně nezdar v podniku. [8]

Další definice rizika:[8]

- 1) Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.
- 2) Variabilita možných výsledků nebo nejistota jejich dosažení.
- 3) Odchýlení skutečných a očekávaných výsledků.
- 4) Pravděpodobnost jakéhokoliv výsledku, odlišného od očekávaného.
- 5) Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti.
- 6) Nebezpečí negativní odchylky od cíle (tzv. čisté riziko).
- 7) Nebezpečí chybného rozhodnutí.
- 8) Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko).
- 9) Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko).
- 10) Střední hodnota ztrátové funkce.

11) Možnost, že specifická hrozba využije specifickou zranitelnost systému.

Tyto vybrané definice popisují často společné dvě vlastnosti. Že výsledek bývá nejistý a že alespoň jeden z možných výsledků je nežádoucí. Existují alespoň dvě varianty, jak událost dopadne. Zajímavé je si uvědomit, že o riziku jde mluvit pouze tehdy, pokud se dá negativnímu účinkem něco udělat.

4.2 Management rizik

Z definic předchozí kapitoly mělo vyplynout, že zajišťování bezpečnosti technických systémů lze zajišťovat pomocí analýz rizik těchto systémů. Je proto nezbytné se u managementu a metod analýzy rizik zastavit a blíže si je popsat. Při identifikaci rizika se obecně zjišťuje jeho zdroj a cíl, závislosti a rozsah. Následně se riziko hodnotí, vypočítává se pravděpodobnost výskytu a s výskytem spojený dopad na cíle.

K analýze rizik technických systémů se přistupuje opakovaně, tzn., analýzy se opakují, dokud není hodnota rizika přijatelná. Rozlišujeme analýzy rizika kvalitativní a kvantitativní.

4.3 Opatření ke snižování rizik

Zde je několik obecně pojatých přístupů ke snižování rizika s popisem a příkladovou situací a jejím řešením. [9]

- **Alternativní řešení:** nalézt řešení, které obnáší nižší riziko. Například u výrobku použití dílu, který je sice dražší, ale mechanicky pevnější.
- **Likvidace zdroje hrozby:** likvidovat hrozbu dříve, než začne působit. Například školení pracovníků s novým výrobním strojem tak, aby se předešlo výrobě zmetků z neznalosti.
- **Ochrana před hrozbou:** ochráníme se před hrozbou, aby její působení mělo menší negativní následky. Například pronájem služeb odborníka na analýzu rizik, abychom se ochránili před nedostatečně provedenou analýzou prováděnou s malými vlastními zkušenostmi.
- **Modifikace scénáře:** pokud se hrozba realizovala, snažíme se ovlivnit scénář tak, aby měl příznivější průběh. Například ustanovíme krizového manažera, který lépe zvládne průběh krize.
- **Mobilizace rezerv:** vytváření rezerv na vyrovnání případných dopadů rizik. Například časové a finanční rezervy nebo záložní pracovní jednotka.
- **Snížení pravděpodobnosti výskytu scénáře:** snaha ovlivnit pravděpodobnost scénáře. Například zbudování soustavy včasného varování před tsunami sníží počet lidských obětí.

- **Snížení velikosti škody:** snaha snížit dopad scénáře. Například přesunutí činnosti, u které hrozí nedodržení termínu, mimo kritickou cestu projektu.
- **Přenesení rizika:** přenést riziko na jiný subjekt. Například pojištěním přeneseme riziko na pojišťovnu.
- **Rozdělení rizika:** snížit hodnotu rizika rozdělením dopadů na projekt. Například výrobce a zákazník si rozdělují odpovědnost za bezpečnost výrobku.

4.4 Další vybrané přístupy řešení bezpečnosti

Poka-yoke:

Pochází z japonštiny a dá se přeložit jako „snadno pochopitelný“ nebo též „blbu-vzdorný“ (což je bližší původnímu názvu baka-yoke, který z důvodu hanlivosti výrazu musel být zmírněn). Myšlenkou přístupu je konstruovat takové výrobky, které už ve svém návrhu snižují rizika neúmyslné lidské chyby. Tato myšlenka není úplně nová, koncept byl formálně zaveden panem Shigeo Shingo jako součást produkčního systému Toyoty. Jako příklad lze uvést sklíčidlo, do kterého lze upínat pouze patřičný nástroj, nebo elektronické počítadlo svářených spojů, které hlídá, že dělník jich udělal dostatek.[10]

Ve výrobě jsou podle Shigeo Shinga rozlišovány tři přístupy poka-yoke: [11]

- Kontaktní metoda rozpoznávající zmetky podle velikosti, tvaru a dalších fyzických vlastností.
- Metoda konstantního čísla varující obsluhu, že daný počet kroků nebyl udělán.
- Sekvenční metoda zajišťující předepsanou posloupnost kroků procesu.

Six Sigma:

Je strategií, jak zvyšovat jakost pomocí hledání a odstraňování příčin chyb. Poskytuje nástroje ke zlepšování procesů ve firmách a odstraňování zmetkovosti u produktů. Předpokládá, že snížení odchylek od sledovaných vlastností produktů vede ke snižování poruch, zvyšování zisků, morálky zaměstnanců a kvality produktů. Jde o systematickou metodologii, která využívá informace a statistickou analýzu k měření a zlepšování výkonnosti organizace.[12]

Redundance

Přístup spočívá v přidávání nadbytečných subsystémů tak, aby mohly nahradit selhávající subsystém. Tento způsob se vyskytuje hojně v přírodě, většina živých tvorů má některé orgány párové.

Zajištění proti selhání, pasivní bezpečnost

Pasivní bezpečnost znamená, že již v konstrukci jsou navrženy subsystémy, které zafungují v případě nastalé hrozby vyřazením systému z chodu. V literatuře často uváděný

subsystém pasivní bezpečnosti jsou pružinové brzdy na lanech výtahů. Brzdy jsou udržovány v otevřeném (nezabrzdném) stavu napnutým lanem. Pokud lano povolí, brzdy se aktivují a zastaví kabinu před pádem.

Tolerance k selhání

Znamená, že systém snese určité množství selhání subsystémů, než dojde ke kritickému selhání celého systému.

Izolování selhání

Typicky používané v systémech vodovodních potrubí jako soustava ventilů, kde je potřeba izolovat případný únik nebo obejít modernizovanou část.

4.5 Metody posuzování bezpečnostních rizik

Smyslem je podrobit návrhy systémů analýze tak, aby se identifikovaly hrozby, a možné scénáře projevů hrozeb. V dalších krocích se zavádějí požadavky na výrobek snižující rizika na únosnou mez.

Používané metody je zvykem dělit podle jejich popisných aparátů na kvantitativní a kvalitativní. Kvalitativní přístupy se řídí otázkou „Jaká hrozba musí nastat, aby se odehrál určitý scénář?“. Kvantitativní přístupy používají odhady pravděpodobností a dopadů hrozeb.

Analýza je závislá na zkušenostech řešitele analýzy a znalosti analyzovaného systému.

4.5.1 Kvantitativní metody analýz

Ke slovu u těchto metod přichází matematická statistika. Hlavně teorie pravděpodobnosti a popisné statistiky. Kvantitativní analýzy předpokládají, že výsledky pozorování a měření mají určité předpokládatelné zákonitosti. Mimo to vykazují i určité náhodné odchylky. Data pro statistickou analýzu se sbírají měřením (napětí, průměr, rychlost otáčení atd.) a počítáním (počet vyrobených kusů, počet nýtů ve spoji dvou plechů, atd.).[6]

Za kvantitativní metody analýz se považují:

- histogramy a výpočet základních ukazatelů souborů dat: forma grafu s množstvím sloupců představujících kvantifikovaná data. Je-li to vhodné, data se seřadí podle velikosti. Mají výhodu vizualizace informace, jsou přehlednější, než tabulky.
- grafy různých typů: také grafická forma, koláčové grafy, trojrozměrné plochy. Dobré pro přehlednost, ale omezení počtu sledovaných kvantifikovaných vlastností.
- Paretova analýza: využívá předpokladu, že poměrně malé množství příčin má rozhodující podíl na negativních jevech. Je to stará metoda, využívaná při složitých procesech, kdy nelze všechny problémy řešit naráz. Paretova analýza pomáhá vybrat ty s největším efektem. Využíván je přitom histogram nazývaný jako Paretův diagram.

Tento zobrazuje kumulativní anebo relativní a kumulativní četnosti jednotlivých příčin. Tyto četnosti jsou sestupně seřazené a dávají tak poznat nejpodstatnější vlivy.

- Korelační a regresní analýza: využívá se ke zjišťování stochastických závislostí mezi dvěma a více veličinami, reprezentovanými dvěma a více soubory dat. Ke grafickému zobrazení závislostí se používá bodových diagramů. Soubory dat se v tomto případě zobrazují ve dvojicích (a více-ticích) bodů, vždy po jednom ze souboru. Podle tvaru grafu se dá usuzovat, jaké jsou mezi soubory vztahy, případně se dají vztahy vyloučit. Vztah souborů dat může být lineárně těsný, lineárně volný, nebo nelineární.
- SPC, statistické řízení procesů, statistická regulace procesů: pracuje s tzv. statistickou stabilitou. Předpokládá výskyt odchylek ovlivnitelných a neovlivnitelných.

4.5.2 Kvalitativní metody analýz

Hodí se pro zpracování údajů, které se těžko zaznamenávají číselně, ale jsou užitečné pro rozhodování. Aby byly kvalitativní metody efektivní, vyžaduje se týmová práce. Tým by měl reprezentovat jak znalosti o problematice, tak nestranné názory mimo prostředí firmy.[6]

- Kontrolní záznamy, záznamníky, formuláře: používají se ke sběru údajů o produktech, aby bylo možné získat jasnou představu o sledovaných vlastnostech. Jsou součástí mnoha používaných metod a slouží hlavně ke zpřehlednění informací.
- Metoda příčina – následek: analyzuje daný problém z pohledu jeho příčin. Často se rozlišuje několik úrovní příčin a jejich následků tam, kde projevená hrozba spouští lavinu dalších hrozeb.
- Ishikawův diagram: grafické znázornění metody příčina – následek, které je názornější než například tabulka. Při jeho tvorbě vzniká charakteristický tvar rybí kostry.
- Diagram afinit: jde o třídění informací do skupin podle společných vlastností.
- Benchmarking: metoda spočívá v porovnávání produktu s jinými stejného druhu, u kterých je jakost známa.
- Brainstorming: týmová metoda sloužící ke shromáždění co nejvíce podnětů a nápadů. Má dvě fáze. V první se vyzve skupina lidí, aby vyslovila co nejvíce nápadů, jakkoliv nesmyslné se mohou na první pohled zdát. Důležité v této první fázi je zdržet se komentářů hodnotících jednotlivé nápady. Hodnocení probíhá až ve druhé fázi, kde se teprve probírají hlubší souvislosti shromážděných nápadů.
- Vývojový digram: zachycuje posloupnost kroků nějakého postupu. Umožňuje zachytit větve jednotlivých rozhodnutí. Zkoumání vzájemných vztahů jednotlivých kroků má vést k nalezení možných problémů.
- Stromový diagram: používá se ke grafickému znázornění analýzy požadavků na daný

kvalitativní znak. Nejdříve se stanoví hlavní kategorie. Pro každou kategorii se potom hledají její prvky a kreslí se jako větve okolo této kategorie. Takto je možno iterovat do více úrovní. Pochopitelně je potřeba dohlédnout, aby míra podrobnosti rozkladu byla smysluplná.

- Diagram vzájemných vztahů: využívá se pro rozpoznání logických souvislostí mezi kategoriemi. Tyto kategorie je potřeba stanovit předem.
- Maticový diagram: určený k posouzení vzájemných souvislostí mezi dvěma, nebo více kategoriemi daného problému. Mívá formu tabulky, kde v prvním řádku a sloupci jsou sledované kategorie a na spojnice se zaznamenává jejich vztah.
- Síťový graf: nejznámější je metoda kritické cesty. Metoda kritické cesty slouží k plánování tzv. kritických činností projektů. Kritické činnosti jsou takové, jejichž časová rezerva je nulová a jejich zpoždění má vliv na celý projekt. Využívá uzlů pro záznam časových údajů po realizaci činností a orientované úsečky pro znázornění návazností činností. Zajímavé je, že v Evropě je rozšířená upravená metoda kritické cesty. Ta interpretuje uzly jako činnosti a úsečky jako návaznosti činností. Odpadá tím několik problémů spojených se znázorňováním návazností činností.

4.5.3 Komplexní postupy a modely

Protože předmětem analýz bývají komplexní systémy a soustavy, používá se množství metod, které kombinují kvalitativní a kvantitativní přístupy. Zde jsou vybrané z nich.[6]

- Analýza bezporuchové činnosti člověka (HRA)
- Analýza blokového diagramu bezporuchovosti (RBD)
- Analýza možných druhů poruch a jejich následků (Fault Modes and Effect Analysis): prověřuje možné poruchové stavy materiálu, součástek, zařízení, postupů, atp. navrhovaných produktů. Následně poruchové stavy uspořádá podle stupně závažnosti. Nakonec se hledají možná nápravná opatření k odstranění nejzávažnějších poruchových stavů, prioritně u těch nejzávažnějších.
- Analýza stromu poruch (FTA): analýza využívá stromové diagramy. Na vrcholu diagramu je „vrcholová událost“ (například vážný úraz). Od této události se postupuje deduktivně k zaznamenání jejích možných příčin. Postupuje se na nižší a nižší úroveň příčin, v případě výrobku se končí na jednotlivých součástkách.
- Analýza stromu událostí (ETA)
- CRAMM: metoda využívá stejnojmenný software a původně byla určena k vyhodnocování rizik telekomunikačních projektů. Software obsahuje předpřipravené dotazníky a knihovnu opatření pro snížení rizik. Proces řízení rizik je tak do značné

míry usnadněn a automatizován. Cena produktu je vyšší, než je zvykem u uživatelských programů.[13], [8]

- Markovova analýza
- Metoda pro analýzu projektových rizik RIPRAN (RIsk PROject ANalysis) je určena zejména pro analýzu projektových rizik. Autorem metody je B. Lacko. Metoda vznikla původně pro analýzu rizik automatizačních projektů v rámci výzkumného záměru na VUT v Brně. Praxe ukázala, že po určitých úpravách je metodu možno aplikovat pro analýzu rizik širokého spektra různých projektů a v určitých případech i pro analýzu jiných druhů rizik než jsou projektová rizika. RIPRAN™ je ochranná známka, registrovaná autorem v Úřadu průmyslového vlastnictví Praha pod reg. 283536.[9]
- Navrhování experimentů (Design Of Experiments): metoda se používá ve vývojových stádiích výrobku. Prakticky jde o řízený pokus, často v upravených (laboratorních) podmínkách.
- Studie provozuschopnosti (HAZOP)
- Předběžná analýza nebezpečí
- Předpověď intenzity poruch

4.6 Technické normy

Technická norma je dokument, který stanoví technické požadavky, řešení nebo postupy. Zabývá se kvalitou výrobků, zkušebními postupy, názvoslovím, značením, ale i ochranou zdraví, bezpečností práce, požární ochranou a ekologií. Zpravidla lze najít normu všude, kde je zavedena sériová výroba.

Normy z hlediska jejich platnosti můžeme rozčlenit do následující soustavy:

- Normy mezinárodní
- Normy národní
- Normy asociací, sdružení
- Normy podnikové.[14]

4.6.1 Normy mezinárodní

Nejvíce rozšířené normy jsou označené ISO. Vydává je mezinárodní organizace pro standardizaci (International Organization for Standardization). V Evropě máme normy označované EN, vydávány Evropským výborem pro normalizaci (Comité Européen de Normalisation). ČR je členem CEN, a proto přijímá do své soustavy normy evropské. Takovým se potom říká harmonizované a mají zkratku ČSN EN.

Normy určené pro strojní zařízení se dělí do tří typů:

- Normy typu A (základní bezpečnostní normy), definují pojmy, popisují zásady pro projektování a všeobecně aplikovatelná pravidla použitelná na všechny stroje.
- Normy typu B (skupinové bezpečnostní normy), zaměřené na jeden bezpečnostní aspekt nebo jeden typ bezpečnostního zařízení, použitelné pro široký rozsah strojů:
 - normy typu B1 se týkají jednotlivých bezpečnostních aspektů (vzdálenost, vlhkost, prašnost, hlučnost)
 - normy typu B2 se týkají příslušných bezpečnostních zařízení (kryty, pojistky, zámky).

Normy typu C (bezpečnostní normy pro stroje) popisují konkrétní bezpečnostní požadavky konkrétní skupinu strojů, která je uvedena v předmětu normy.[15]

4.6.2 Evropské národní normy

Jedná se o normy jednotlivých států, například: ČSN česká technická norma (ČR), BS (Anglie), SN (Švédsko), STN (Slovensko), ÖN (Rakousko), DIN (Německo), GOST (Ruská federace). Národní normy vznikají na půdě standardizačních orgánů svých zemí. Podstatné je zmínit existenci Evropského centra pro normalizaci – CEN. Státy, které jsou členy CEN, mají povinnost do soustavy národních norem přebírat normy evropské. Tím dochází k sjednocování evropské soustavy, alespoň tedy v členských zemích. Tyto přebrané normy jsou pak doplňovány značkou EN, hned za značkou národní. Např.: ČSN EN, STN EN atp. [14]

Členy CEN jsou: Belgie, Česká republika, Dánsko, Estonsko, Finsko, Francie, Irsko, Island, Itálie, Kypr, Litva, Lotyšsko, Lucembursko, Maďarsko, Malta, Německo, Nizozemsko, Norsko, Polsko, Portugalsko, Rakousko, Rumunsko, Řecko, Slovensko, Slovinsko, Spojené Království, Španělsko, Švédsko, Švýcarsko.[16]

Dále je tendence společně řešit evropské normy EN přebíráním norem ISO. Tím, protože ISO jsou světově uznávané, dochází k širokému sjednocování technických norem. Značení takto řešených norem je pak například ČSN EN ISO, DIN EN ISO atp.

Tvorba samostatných národních norem bez součinnosti s ISO nebo CEN ztrácí význam.

4.6.3 Normy asociací, sdružení atp.

Do této skupiny se počítají normativní dokumenty obchodních řetězců, nějaké oblasti výrobků a technické normy vojenských sdružení (aliancí, paktů, jednotlivých armád). Například NATO má normy AQAP, které jsou v České republice převedeny do ČOS (České

obránné standardy).[14]

4.6.4 Podnikové normy

Jedná se o normy vypracované jednotlivými organizacemi. Podnikové normy můžeme dělit do dvou skupin:

- Normy vnitropodnikové: jsou dané nejlepší praxí uvnitř podniků. Jejich platnost je omezena rámcem jedné organizace. Řeší například průběh výstupních kontrol. Mohou být interní a utajené.
- Podnikové normy využívané pro styk mezi výrobcí a odběrateli.

Podnikové normy bývají zpravidla zaměřeny na technické vlastnosti výrobků. Vzácněji na zkušební metody. Takové bývají hodně specifického zaměření nebo omezeného okruhu použití. Také je možné se setkat s podnikovými normami, jimiž jsou v podstatě modifikované verze norem státních i mezinárodních. Motivací bývá dosáhnout na plné požadavky státních a mezinárodních norem postupně, nebo některé prvky vynechat.[14]

4.6.5 Závaznost technických norem

Technické normy nejsou závazné obecně. Mohou se stát závaznými v určitých případech:

- Uvedením objednavce potvrzené smlouvou. Nezáleží na druhu normy, ani zda je v době uzavření smlouvy platná. Není-li ve smluvním vztahu stanovena žádná norma, může se případný spor řídit použitelnou technickou normou. Jakost stanovená normou může být soudem považována za obvyklou pro daný případ.[14]
- Odkazem v právním předpisu. Závazná je samozřejmě pro případy uvedené v daném právním předpisu. Je snaha závaznost tímto způsobem neřešit.[14]

4.6.6 Harmonizované normy a určené normy

Členství v CEN určuje povinnost zavádět evropské normy do národní soustavy. Takové normy se nazývají harmonizované a mají v souvislosti se závazností zvláštní pozici. Navazují na právní předpisy a jsou jako harmonizované oznámeny ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ).[17]

Harmonizované a určené technické normy obsahují podrobnější popis požadavků, než právní předpisy. Právní předpisy k technickým požadavkům jsou zpravidla o nařízení vlády ke stanoveným výrobkům. Pokud je splněn požadavek normy, plní se tím i požadavek právního předpisu. Je ale možné splnit požadavek právního předpisu i když nejsou splněny

všechny požadavky normy. Smyslem je, aby normy nebránily technickému rozvoji.[14]

4.6.7 Nalezené normy

ISO/DIS 13482: Roboti a robotická zařízení – bezpečnostní požadavky pro neprůmyslové roboty – nemedicínské roboty pro osobní péči.

Tato norma specifikuje požadavky na bezpečný design, ochranná opatření a informace pro používání robotů pro osobní péči. Zaměřená je na tři typy robotů osobní péče, jmenovitě „mobilní služební robot“, „tělesný asistenční robot“ a „osobní přepravní robot“. Popisovány jsou hrozby spojené s používáním těchto robotů. Dále jsou doporučována opatření k eliminaci, nebo omezení rizik spojených s těmito hrozbami.

Roboty pro osobní péči by měly dodržovat standardy a nařízení s nimi související. Například robot pro osobní přepravu by měl splňovat požadavky pro provoz na veřejných komunikacích. Výjimečný je tento standard tím, že pokrývá oblasti, kde dochází k fyzickému kontaktu mezi člověkem a strojem. To je něco téměř vyloučeného u průmyslových robotů. Pro úplnost se hodí dodat, že se nevztahuje na vodní, létající, ani průmyslové roboty.

ČSN EN 292: Základní pojmy, všeobecné zásady pro projektování. Je norma typu A. Velmi obecně popisuje zásady výroby bezpečných strojů. Ve spojení s ČSN EN 414 „Pravidla pro navrhování a předkládání bezpečnostních norem“, poskytuje strategii tvůrcům norem typu C. Důležitá je tato norma pro návrháře a konstruktéry výrobků, pro které nejsou vytvořeny normy typu C (speciálně pro daný výrobek). Autonomní mobilní roboty jsou pravděpodobně případem neexistující normy typu C. Je podporou ve využívání norem typu B a je výhodné používat její názvosloví v dokumentaci. Norma byla nahrazena ČSN EN ISO 12100.[15]

ČSN EN 414: Pravidla pro navrhování a předkládání bezpečnostních norem. Tato norma se používá především při navrhování norem typu C. Specifikuje požadavky pro navrhování a předkládání evropských bezpečnostních norem pro strojní zařízení a norem pro bezpečnostní součásti. Smyslem normy je, aby byl dosažen soulad a přijatelná kvalita při přípravě nových norem. Norma také uvádí požadavky týkající se kritérií pro výběr nových pracovních témat a kritérií pro postupy, umožňující, aby normy byly připravovány a zpracovávány účinným a efektivním způsobem.[18]

ČSN EN ISO 12100: Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika. Norma specifikuje základní terminologii, zásady a metodologii pro dosažení bezpečnosti při konstrukci strojního zařízení. Norma specifikuje zásady posouzení a snižování rizika jako pomoc konstruktérům k dosažení tohoto cíle. Tyto zásady jsou založeny na znalosti a zkušenosti z konstrukce, používání, nehod, úrazů a rizik u strojních zařízení. Jsou popsány postupy pro identifikaci nebezpečí a pro odhad

a hodnocení rizik v relevantních fázích životního cyklu stroje, a pro vyloučení nebezpečí nebo pro opatření dostatečně snižující riziko. Je uveden návod na dokumentaci a ověřování procesu posouzení rizika a snížení rizika.[19]

ISO 13849: Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů. Navrhuje strategie celkového snížení rizika u stroje. Zaměření je na části ovládacích systémů, které jsou určeny k plnění bezpečnostních funkcí.

ČSN EN 60335: Bezpečnost elektrických spotřebičů pro domácnost a podobné účely. Tato norma se vztahuje na bezpečnost strojů, jejichž jmenovité napětí nepřesahuje 250V. V možné míře pojednává tato norma o běžných nebezpečích představovaných spotřebiči, se kterými se setkávají všechny osoby v domácnosti a v blízkém okolí. Tato norma nebere všeobecně v úvahu: používání spotřebičů malými dětmi nebo nesvéprávnými osobami bez dozoru, ani hru malých dětí se spotřebičem.

ČSN EN 60335-1: respektuje mezinárodně přijímanou úroveň ochrany před úrazem elektrickým proudem, mechanickým a tepelným nebezpečím, nebezpečím požáru a záření u elektrických spotřebičů pro domácnost a podobné účely, pokud pracují jako při normálním používání, a bere přitom v úvahu pokyny výrobce.

ČSN EN 60065: Požadavky na bezpečnost elektronických přístrojů, napájených ze sítě, pro domácí a podobné použití.

ČSN EN 60664-1: Koordinace izolace zařízení nízkého napětí - Část 1: Zásady, požadavky a zkoušky.

ČSN EN 60529: Stupně ochrany krytem.

ČSN EN 61010-1: Bezpečnostní požadavky na elektrická měřicí, řídicí a laboratorní zařízení - Část 1: Všeobecné požadavky.

ČSN EN 50081-1: Elektromagnetická kompatibilita. Všeobecná norma týkající se vyzařování.

ČSN EN 50082-2: Elektromagnetická kompatibilita - Všeobecná norma týkající se odolnosti.

ČSN EN 61310: Bezpečnost strojních zařízení – Indikace, značení a uvedení do činnosti.

ČSN EN 61496: Bezpečnostní strojních zařízení - Elektrická snímací ochranná zařízení.

4.7 Zákony

Základním právním předpisem je zákon o technických požadavcích na výrobky číslo 22/1997 Sb. Definiuje českou technickou normu, říká, že ČSN není obecně závazná,

vysvětluje pojmy harmonizovaná a určená norma. Dále popisuje postup tvorby ČSN a stanovuje podmínky tvorby a vydávání ČSN. Vysvětluje, jakou úlohu v uvedených činnostech má Úřad pro technickou normalizaci, metrologii a státní zkušebnictví i Ministerstvo průmyslu a obchodu.[14], [20]

Bezpečnost výrobku je zájmem, který by měl být naplňován v etapách před výrobou. Prvním krokem při sledování bezpečnostních zájmů je obstarání a prostudování úplného a aktuálního znění zákona č. 22/1997 Sb. například zde [20].

Po identifikaci těch nařízení vlády (NV), která se výrobku týkají, lze naplánovat pracovní postup. Dobré vodítko je například v [1]. Vyhneme se tak vymýšlení vlastních nevyzkoušených postupů a začátečnických chyb.

Právní prostředí v ČR je podřízené jejím vstupem do EU. ČR je součástí jednotného trhu EU, kde se výrobky pohybují volně, jako by se jednalo o jeden stát. Řada pravidel je platných i pro import na tento rozšířený trh z venkovních trhů.

Bezpečnostní problém

Podle zprávy japonské komise pro přístup k otázce robotického průmyslu (Robot Industry Policy Committee) zatím neexistují žádné metody ani nařízení k vyhodnocení bezpečnosti autonomních robotů. Dokud nebudou tyto ustanoveny, musí se výrobci a uživatelé odkazovat na standardy určené pro průmyslové výrobky obecně.[21]

5 ROZBOR PROBLÉMU

Chceme poznat vlastnosti autonomních mobilních robotů (AMR) ovlivňující bezpečnost. Bylo by přínosné shromáždit množství pohledů na výrobek z různých možných úhlů, například z úhlu vývojářů, uživatelů, zákazníků, právních autorit, atp. Zároveň by měla být věnována pozornost pouze podstatným detailům.

Proces analýzy se bude přidržovat rámce některé ze zavedených metod analýz. V případě potřeby bude použita metoda rozšířena, pokud nebude v originále stačit na zachycení všech problémů. Požadavek je, aby zachycovala bezpečnostní rizika z vnějšku i vnitřku systému AMR.

5.1 Zhodnocení řešeršní studie

Zkoumání praxe v přístupu k bezpečnosti objasnilo pojmový aparát. Bylo odhaleno, jak řešení bezpečnosti produktu souvisí s vyhodnocováním rizik. Byl získán přehled o množství metod používaných k analýze rizik. Jsou-li rizika rozpoznána a vyhodnocena jejich závažnost, nastupují postupy syntézy návrhů ke snižování rizik. V technické praxi se bezpečností průmyslových produktů zabývají týmy odborníků, nikoliv jednotlivci.

Posouzení bezpečnosti bude provedeno jako analýza možných rizik. Počítá se se zapojením vývojářů z firmy Bender Robotics, kteří mají unikátní zkušenosti s vývojem a provozem AMR pojmenovaného Advée. Bude vybrána některá z komplexních metod analýz.

5.2 Otázky v procesu analýzy systému

Kde jsou hranice bezpečnostních zájmů?

Bezpečnost AMR zkoumáme hlavně kvůli možným škodám na zdraví a majetku způsobených výrobkem. Pokud takové škody nastávají, zpravidla se hledá konkrétní viník a tyto případy zaměstnávají soudy. Případné pokuty potom mohou být pro výrobce likvidační.

Jak systém funguje?

Bude potřeba pochopit v širších souvislostech funkce AMR. Výhodou jsou zkušenosti ze samotného vývoje robotu, který probíhá již několik let. Mohlo by napomoci vytvoření systémového modelu AMR a zachycení jeho funkcí a subsystémů.

Co se může stát?

Budou zkoumány poruchové stavy, hrozby plynoucí z provozu AMR. Opět se uplatní zkušenosti z vývoje a provozu robotu, „pouze“ budou zasazeny do rámce metod pro analýzu rizik.

Jak se to může stát?**Proč se to může stát?**

Vytvoří se model vztahů typu příčina – následek ke zmapování a vyšší názornosti stavů snižujících bezpečnost. Někdy známe příčinu a doplňujeme možné následky, jindy máme záznamy o následcích (haváriích) a pátráme, co je způsobilo.

Jak pravděpodobně se to může stát?

Protože se nejedná o sériový výrobek, ani neexistují statistická data, bude pravděpodobnost projevů hrozeb odhadována na subjektivních stupnicích s pomocí znalostí expertů.

Jaké následky jsou, když se to stane?

Možné následky je potřeba znát pro vyhodnocení rizik jako součinu pravděpodobnosti a dopadů projevené hrozby.

Co se dá udělat, kolik to bude stát?

Nakonec se navrhnou možná opatření ke snížení bezpečnostních rizik. To se dá udělat buď snížením pravděpodobnosti jejich výskytu, nebo snížením jejich dopadů. Vytvořené analýzy z předchozích kroků budou sloužit k ospravedlnění jejich zavedení.

5.3 Autonomní mobilní robot Advee



Rozměry (d×š×v): 100 × 66 × 160 cm

Obr. 3: Robot Advee ve foyer hotelu Clarion v Praze, zdroj [22]

Určení robotu s marketingovým jménem Advee je interaktivní forma propagace. Robot se má autonomně pohybovat mezi lidmi v komerčně zajímavém místě, například v obchodním domě. Svou kamerou zabudovanou v hlavě umí rozpoznávat lidské tváře a detekovat tak potenciální uživatele. Těm pomocí přednastavených hlášek nabízí interakci přes dotykový displej. Pokud se najde takový uživatel, jenž interakci zahájí dotykem na displej, robot přeruší autonomní pohyb a spustí se menu s několika možnými aktivitami. Asi nejzajímavější je možnost vyhrát v zábavné hře a odnést si zosobněný kupón na slevu. Vše lze upravit pro propagaci komerční značky.

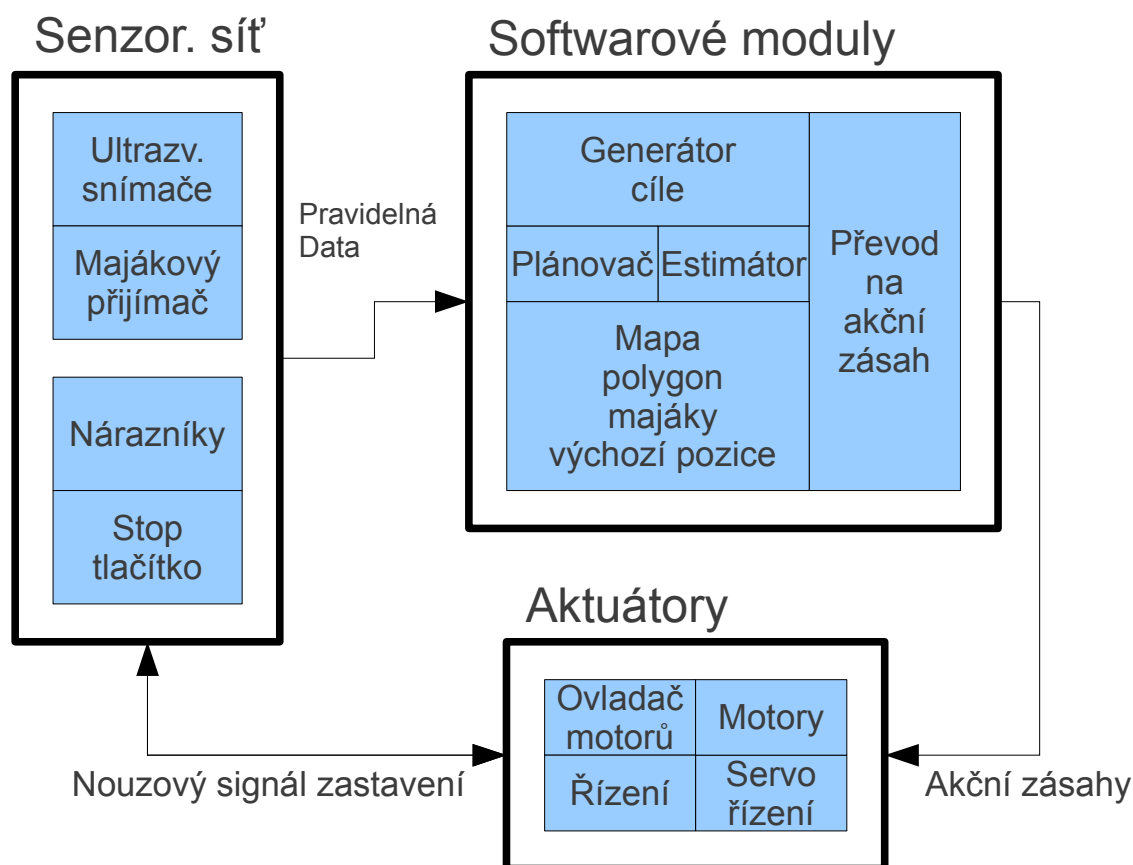
Robot Advee využívá koncepcí čtyřkolového podvozku s Ackermannovým řízením. Výhodami koncepce jsou dobrá stabilita a energetická úspornost. Odpružení kol je pasivní, podvozek je částečně odpružen pomocí kyvné nápravy. Ta zajišťuje lepší přilnavost kol k vozovce. Rám je vyroben z hliníkových svařovaných profilů. K přenášení slouží madla v přední a zadní části rámu. Celková hmotnost robotu včetně baterií se pohybuje okolo 90 kg. Podvozek je vybaven mechanicky spínanými nárazníky v přední a zadní části. Nárazníky slouží jako bezpečnostní pojistka v případě selhání senzorů a kolize s překážkou. Robot je

poháněn stejnosměrným motorem Maxon RE50 200W s dvoustupňovou planetovou převodovkou. Zadní poloosy jsou s motorem spojeny přes otevřený diferenciál. Ackermannovské řízení je poháněno stejnosměrným servomotorem značky Berger Lahr s planetovou převodovkou. Do výbavy patří tiskárna, průmyslovým kapacitní dotykový displej, zásobník papíru, zvukový zesilovač, reproduktory, senzory různého charakteru a řídicí elektronikou nezbytnou pro jeho funkci. Zdrojem energie je 8 článků lithiových baterií s palubním napětím 28V a celkovou kapacitou 2,5 kWh. Vnější skořepina respektuje tvar konstrukce a byla navržena renomovaným designérem.[23]

Problematika detailních technických parametrů robotu Advee je mimo zaměření této práce, doporučena je velmi dobrá publikace vývojářů: [23]

5.3.1 Autonomní mobilní robot jako systém

Sledovaný systém lze modelovat jako soubor subsystémů, jejichž funkce dohromady tvoří funkce systému jako celku. Subsystémy rozumíme hardware, software a člověkem ovládané prvky. Podrobnost rozlišování subsystémů bude dána rozlišitelností poruchových stavů. Vytvořený model systému podpoří analýzu rizik.



Obr. 4: Zjednodušený model AMR, zdroj [2]

5.4 Nalezené normy

Bylo vyhledáváno na webech standardizačních organizací s účinností v Evropě, na webech zaměřených na robotiku a v článkách zveřejněných k tématům bezpečnosti AMR. Velmi pomohla možnost přistupovat k databázi norem ČSN v knihovně VUT.

Nalezené normy jsou vypsány v rešeršní kapitole. Všechny jsou obecně zaměřené na výrobky a na elektrické spotřebiče. Jejich prostudování upozornilo na oblasti a hrozby, jimž je potřebné věnovat pozornost.

Během studia norem bylo nalezeno množství norem zaměřených na průmyslové roboty, kde se většinou pracuje s principem oddělení prostoru průmyslového robotu od lidské obsluhy. Byla nalezena pouze jedna norma určená pro „domácí nemedicínské roboty“. Tato norma je sestavována organizací ISO a nese označení ISO/DIS 13482, v době psaní této práce je ve stádiu schvalování a její kopie stojí 66 švýcarských Franků (cca 1370,- Kč). [24] Pro tuto práci norma ISO/DIS 13482 prostudována, protože není k dispozici ve zdrojích dostupných pro tuto práci.

Při hledání v zahraničních textech byla velmi zajímavá série zpráv pana Yueh-Hsuan

Weng.[25] Pan Weng je z Pekingské univerzity a zabývá se právními otázkami střetu umělé inteligence a oprávněných zájmů lidí. Neomezuje se nutně jenom na roboty, ale často o nich píše. Jeho anglicky psané texty umožňují přístup k informacím o stavu věcí v Číně a Japonsku, jsou čtivé a obsahují i odkazy na vědeckotechnickou literaturu. Podstatné je, že poukazuje na nepřípravenost právních soustav na výskyt inteligentních robotů v lidské společnosti. Jeho zprávy podporují domněnku, že zákony a normy pro AMR nejsou připraveny ani v technologicky vyspělých společnostech východní Asie.[21]

5.5 Použité harmonizované normy

Pro výrobek AMR byly zohledněny tyto harmonizované normy:

ČSN EN 60335: Bezpečnost el. spotřebičů pro domácnost a podobné účely.

ČSN EN 60065: Požadavky na bezpečnost elektronických přístrojů, napájených ze sítě, pro domácí a podobné použití

ČSN EN 60664-1: Koordinace izolace zařízení nízkého napětí - Část 1: Zásady, požadavky a zkoušky

ČSN EN 60529: Stupně ochrany krytem (krytí - IP kód) ČSN EN 61010-1: Bezpečnostní požadavky na elektrická měřicí, řídicí a laboratorní zařízení - Část 1: Všeobecné požadavky

ČSN EN 50081-1: Elektromagnetická kompatibilita. Všeobecná norma týkající se vyzařování

ČSN EN 50082-2: Elektromagnetická kompatibilita - Všeobecná norma týkající se odolnosti

ČSN EN 61310-1,2,3: Bezpečnost strojních zařízení - Indikace, značení a uvedení do činnosti - Část 1, Část 2, Část 3

ČSN EN ISO 12100-1,2: Bezpečnost strojních zařízení. Základní pojmy, všeobecné zásady pro konstrukci. Část 1, Část 2

5.6 Dostupné prostředky a zdroje

Kromě veřejně dostupných zdrojů budou pro analýzu k dispozici tyto zdroje:

autonomní mobilní robot Advee,

jeho technická dokumentace,

záznamy z proběhlých akcí,

zkušenosti vývojového týmu,

databáze norem ČSN v knihovně FSI VUT.

5.7 Volba metod posuzování bezpečnosti

Bylo rozhodnuto, že pro prvotní analýzu bezpečnosti bude použita konstrukční FMEA. Budou prozkoumány objevující se poruchy a jejich důsledky. Zejména poruchy jsou zdrojem

stavů, kdy robot není schopen plnit své zamýšlené funkce nebo vznikají situace ohrožující osoby a majetek v okolí robotu. FMEA bude zkoumat tyto oblasti: konstrukci, software, elektroniku, a provozní postupy.

FMEA by měla odhalit možné projevy poruch. Dalším krokem bude stanovení otázek, které budou experimentálně ověřeny. Použitou metodou bude navrhování experimentu (DOE). Spočívá v definování jevů, které budou pečlivě sledovány při běžném provozu robotu.

Pro celkovou analýzu bezpečnosti a při hledání doporučení bude použito některé metody s hledáním příčiny – následky. Nabízí se vyzkoušení metody RIPRAN, která vznikla v českém prostředí.

6 PROVEDENÍ ANALÝZ

6.1 FMEA – analýza poruchových stavů

V říjnu 2011 proběhla analýza FMEA těchto oblastí: konstrukce, elektronika, a software. Byl sestaven tým odborníků přímo ze skupiny vývojářů, doplněný o uživatele a realizátory (technický dozor na provoz robotu). Tento tým byl přítomen na dvou sezeních. První bylo školicí, kdy se vysvětlovaly činnosti nutné k provedení FMEA. Druhé pokračovalo v rozpracovaných analýzách a hledala se možná opatření.

6.1.1 Tým FMEA

Byl zvolen šestičlenný tým, což se osvědčilo. Každý byl schopen se zapojit, byli zastoupeni odborníci z technických oblastí i uživatelé a realizátoři (specialisté na provozování robotu v určeném místě). Při větším počtu osob by mohly vznikat neshody. Je žádoucí, aby členové nebyli jen znalí odborníci, protože ti jsou často zafixováni v rámci svého oboru. Běžní uživatelé, pokud zapojí fantazii a vyjádří své názory, přichází s mnohdy neviděnými úhly pohledu. Týmová práce přinesla řadu výhod, byly to právě přidané úhly pohledu na řešený problém, rozproštění nároků na zpracování a vzájemná motivace ke společnému smysluplnému úkolu.

Podařilo se probudit u členů týmu komunikativnost. Byli ochotni spolupracovat, sdělovat své myšlenky, uměli se dohodnout, naslouchat cizím názorům. K podnícení nových nápadů bylo využito metod brainstormingu a brainwritingu.

Při brainstormingu každý vyjadřuje své nápady k danému tématu a inspiruje tak ostatní, kteří náměty doplňují. Po první fázi, kde se nápady pouze sbíraly, bylo diskutováno, které jsou kvalitní. Ty byly následně rozvíjeny. Tím se shromažďovaly návrhy a dále rozpracovávaly. Podstatné je žádný vyslovený nápad hned neodsuzovat, aby někteří členové nezačali své názory cenzurovat. Jednotlivé fáze byly časově ohraničeny.

Při brainwritingu se pomáhá vyjádřit se přemýšlivějším účastníkům, kteří by se při rychlé diskuzi neprosadili. Princip využívá zapisování nápadů na kartičky, které se nakonec předloží a objasní ostatním.

6.1.2 První sezení FMEA

Bylo vysvětleno, že cílem analýzy je odhalit možný výskyt poruch v konstrukci, elektronice a softwaru. Analýza bude využita nejen při zlepšování kvality v těchto oblastech, ale i bezpečnostních vlastností produktu. Každému členovi byl předán formulář a zkrácené vysvětlivky všech polí. Vysvětlení bylo podáno i přímo, a to následovně.

Prvek/Funkce	Způsob možné závady	Možný důsledek závady	Závažnost Klasifikace	Možná příčina(y) mechanismus(y) závady	Výskyt	Stávající opatření pro prevenci
--------------	---------------------	-----------------------	--------------------------	---	--------	------------------------------------

Obr. 5: Ukázka záhlaví formuláře FMEA

- **Prvek/Funkce:** značí, jakého konstrukčního prvku se závada týká.
- **Způsob možné závady:** uvádí závady, které se mohou na daném prvku vyskytnout. Vychází se ze zkušeností z vývoje a provozu, ale může jít i o poruchy, které jsou pouze teoretické a zatím nikdy nenastaly.
- **Možný důsledek závady:** projevy poruchy, které nastanou v souvislosti s vadou tak, jak je zaznamená zákazník.
- **Možná příčina, mechanismus závady:** náchylné místo v systému, jejímž důsledkem je způsob možné závady. Nejpravděpodobnější příčina každé potenciální poruchy.
- **Výskyt:** pravděpodobnost, výskytu příčiny závady. Bodovalo se čísly 1 až 10 podle tabulky. Odhad četností je chápán jako počet výskytů za časový úsek v hodinách.
- **Klasifikace:** hodnotí závažnost poruchy v případě, že se tato realizuje. Bodoje se čísly 1 až 10 podle tabulky klasifikace významu.
- **Odhalitelnost:** pravděpodobnost odhalení poruchy před tím, než se produkt dostane k zákazníkovi. Uvažujeme přitom současná opatření pro kontrolu kvality. Hodnotí se opět od 1 do 10 podle tabulky klasifikace odhalitelnosti.
- **Opatření pro prevenci:** jak by se dalo předejít výskytu vady.

Tabulka 1: Pravděpodobnost výskytu vady, zdroj: upravena verze [6]

Kritérium klasifikace výskytu poruchy	Odhad četnosti	Bodování
Nepravděpodobný výskyt	0	1
Velmi malý, ojedinělý výskyt	1/5000	2
	1/2000	3
	1/1000	4
	1/500	5
Střední	1/200	6
Vysoká, poruchy jsou časté	1/100	7
	1/50	8
Velmi vysoká, z pohledu uživatele téměř jistota	1/20	9
	1/10	10

Tabulka 2: Hodnocení závažnosti poruchy, zdroj: upravené z [6]

Kritérium klasifikace významu poruchy	Bodování
Zanedbatelná, neovlivní plnění účelu výrobku	1
Nízká, porucha způsobí uživateli potíže, funkce výrobku nejsou omezeny	2 3
Střední, uživatelské pohodlí je ovlivněno, snížené funkčnosti si uživatel všimne	4 5 6
Vysoká, porucha působí značné potíže, až poškození výrobku, bezpečnost není ovlivněna	7 8
Velmi vysoká, porucha ovlivňuje bezpečnost provozu výrobku, nezpůsobilost k provozu	9 10

Tabulka 3: Odhalitelnost poruchy, zdroj: upravené z [6]

Kritéria klasifikace odhalitelnosti poruchy	Odhad pravděpodobnosti odhalení [%]	Bodování
Velmi vysoká pravděpodobnost, porucha neprojde kontrolou kvality	100 – 95	1
Vysoká pravděpodobnost	94 – 85 84 – 75	2 3
Střední	74 – 65 64 – 55 54 – 45	4 5 6
Nízká	44 – 35 34 – 25	7 8
Velmi nízká, porucha projde kontrolami kvality a projeví se u uživatele	24 – 15 14 – 0	9 10

K vyhodnocení rizika je potřeba všech tří hledisek. Pro každou možnou vadu se určí vzájemným součinem tzv. rizikové prioritní číslo:

$$RPČ = \text{závažnost} * \text{výskyt} * \text{odhalitelnost}$$

Hodnota rizikového čísla slouží k sestavení seznamu vad, vyvolaných určitou příčinou, podle jejich důležitosti. Vyšší číslo představuje naléhavější nepřijatelný stav. Veškeré chyby, které se mohou objevit, by se měly kontrolovat. Ovšem některé chyby se vyskytují v tak malé četnosti (nebo se ještě nestaly), že se nekontrolují. Proto se především kontrolují takové chyby, které by způsobily závažné důsledky, vyskytují se často a jsou hůře odhalitelné.

Členové týmu odcházeli s rozpracovanými formuláři a úkolem doplnit možné vady, jejich závažnost, výskyt a odhalitelnost.

6.1.3 Druhé sezení FMEA

Druhé sezení probíhalo týden po prvním. Začalo vysvětlováním rozpracovaných analýz v následujících krocích:

- Popsání dílu, kterého se možná porucha týká, hlavně jeho funkce.
- Uvedení potenciálních možných poruch, k nimž může teoreticky dojít.
- Doplnění dalších poruch s využitím brainstormingu a týmu.
- Vyjmenování možných příčin, jak může k poruchám dojít.
- Odhadnutím následků, které lze při dané poruše očekávat.

Dále bylo s pomocí týmových metod navrhováno, jaká opatření jsou k dispozici. Cyklicky byla postupně zkoumána opatření snižující pravděpodobnost výskytu, snižující intenzitu dopadů a zvyšující pravděpodobnost odhalení.

U míry odhalení bylo nutné členům týmu znovu zopakovat, že je to odhalitelnost předtím, než se výrobek dostane k uživatelům produktu. Odhalitelnost byla několika členy týmu pochopena, jako míra rozpoznatelnosti poruchy ve chvíli, kdy nastane. Jeden člen si dokonce představil odhalitelnost za použití metod zkušebnictví, což jsou drahé a sofistikované metody zkušebních laboratoří. Je nutné připustit možnost, že odhalitelnost nebyla dobře vysvětlena.

Bylo odhaleno několik konstrukčních chybových stavů, které mohou robot zcela vyřadit z provozu, ale neovlivňují jeho bezpečnostní vlastnosti. Naproti tomu existuje několik málo poruch s nízkou pravděpodobností výskytu, které mohou vést až k usmrcení osob. Tyto poruchy musejí být uvedeny v návodu, technologicky ošetřeny a sděleny obslužnému personálu.

Pracovníci mají dobrý přehled o možných poruchových stavech ve svých oblastech zájmu. Nebyla odhalena žádná porucha, která by byla vyloženě překvapením. Metoda přinesla systematický přístup k dokumentaci poruch. Dosud nebyla tato metoda iteračně opakována, některá opatření jsou v řešení.

Zajímavé bylo zjištění, že nejsnáze se ošetřují chybové stavy v softwaru. Vysvětlit to lze tak, že tvorba software je nejméně náročná na použité technologie. Jediným omezením jsou tak schopnosti pracovníka. Tyto schopnosti byly s pomocí FMEA posíleny natolik, že v době mezi oběma sezeními byla více, jak polovina možných poruch softwaru ošetřena.

6.2 Ověřovací experiment

Na základě FMEA byla identifikována chování robotu, která jsou projevem možných vad. Při experimentu byla sledována jejich četnost.

- Vyjetí robotu z naprogramovaného polygonu: robot je určen pro pohyb ve známém prostředí vytyčeném virtuální hraniční čarou polygonu. Pokud z něj vyjede, značí poruchu. Prostředí mimo polygon není na provoz robotu upraveno a možné následky jsou na nejvyšším stupni.
- Robot ignoruje uživatele: v provozním prostoru robotu se budou pohybovat lidé. Ty musí robot detekovat jako dynamické překážky. Detekuje je kamerou, ultrazvukovými senzory a v poslední řadě nárazníky.
- Robot ztratí informaci o poloze: znamená, že robot neopustil polygon, ale hlásí evidentně chybnou polohu. Tento stav se kontroluje odečítáním dat přes vzdálené připojení a pozorováním reality.
- Nerovnoměrné pokrytí polygonu: sleduje se, zda robot nezůstává pouze v jedné oblasti polygonu.
- Výpadek WiFi: na externím zařízení je kontrolován počet výpadků spojení s robotem. Výpadky bezdrátové technologie jsou hrozbou při dálkovém řízení operátorem. Vážným příkladem je výpadek těsně před odesláním příkazu o zastavení pohybu.
- Sepnutí nárazníku: protože nárazník je poslední v sérii senzorů detekujících překážky, signalizuje kdy byl robot zastaven nejzazším způsobem.
- Ostatní postřehy: pracovník pověřený záznamem výskytů dostal instrukce zapsat jakékoliv další odchylky od normální funkce robotu.

Experiment probíhal 6 dní v říjnu 2012, ve vstupní hale budovy A1 FSI VUT v Brně.. Bylo využito několik prvků statistického navrhování experimentů (DOE – Design Of Experiments).

Byly stanoveny cíle provozovat robot Advee za běžných podmínek a odhalit tak četnost poruch, případně identifikovat další. Byla diskutována varianta vystavit robot zatěžkávacímu testu a zjistit krajní mezní stavy. Varianta byla zamítnuta z důvodu dojednaných akcí, kterých se měl robot účastnit. Robot by byl po takovém testu pravděpodobně vyřazen z provozu a několik dní až týdnů servisován.

6.2.1 Příprava experimentu

Příprava na experiment probíhala podobně jako na většinu proběhlých propagačních akcí a zahrnovala tyto kroky:

- Nabití baterií robotu a soustavy majáků
- Připravení multimediálního materiálu pro prezentační funkce robotu
- Rozpis služeb pozorovatelů

- Zaměření a vytyčení provozního prostoru
- Rozmístění majáků

6.2.2 Popis experimentu

- Robot byl provozován na určeném polygonu
- Byl dozorován vždy alespoň jednou osobou
- Byl udržován písemný protokol o nežádoucích projevech
- Byl automaticky pořizován záznam údajů zpracovávaných robotem
- Po polygonu se pohybovali lidé, kteří nebyli nijak instruováni, představovali dynamické překážky
- Byla umožněna interakce s osobami procházejícími polygonem

DOE Observation Sheet					Doba experimentu				Pozorování	
DOE Název		temp		Produkt / #		Advee 2			Datum experimentu	
#	Očekávaný znak/chování	Neočekávaný znak/chování	Počet pozorování znaku/chování							
			1	2	3	4	5	6	7	8
1		Robot vyjede z polygonu								
2		Robot nepokrývá rovnoměrně polygon (pohyb se soustředí jen na omezenou oblast)								
3		Robot ignoruje uživatele								
4		Při dotyku na obrazovku je nutné potvrdit přítomnost uživatele								
5		Robot se nepohybuje elegantně								
6		Robot ztratí informaci o poloze								
7		Uživatel odejde od robotu uprostřed interakce, robot v ní pokračuje								
8		Problémy s tiskárnou								
9		Kopnutí do nárazníku								
10		Výpadek WIFI								
11		Výpadek diagnostického centra								

Obr. 6: Vzor protokolu o pozorování znaků/chování, zdroj [6]

6.2.3 Výstup experimentu

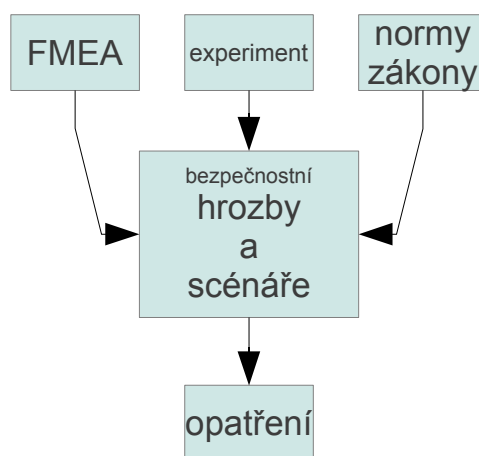
Během čtvrtého dne nastalo 5 případů vyjetí z polygonu. Po zkoumání událostí se zjistilo, že nebyla ověřena funkčnost navigačních majáků. Jeden z majáků při instalaci na zeď spadl a poškodil se, následně docházelo k chybám v lokalizaci. Majáky musí být před ostrým provozem kontrolovány.

Za celou dobu experimentu byl 13 krát sepnut nárazník. Většina byla způsobených uživateli, 1 případ byl v důsledku chyby operátora při ručním ovládání.

Postřehy z pozorování byly zpracovány v další analýze.

6.3 Celková analýza bezpečnosti provozu AMR

K provedení analýzy bezpečnosti provozu byla zvolena komplexní metoda RIPRAN. Vstupem metody jsou výsledky analýzy FMEA, závěry experimentu, postřehy z pozorování a vybrané normy. Zadání se lišilo od FMEA. Nebyly hledány poruchy, které se projeví na funkčnosti robotu. Samotná nefunkčnost nemusí snižovat bezpečnost provozu AMR. Například porucha motoru se projeví tak, že robot zůstane stát na místě, ovšem musí se zrovna nacházet v předepsaném provozním prostoru a ne uprostřed prudce nakloněné roviny.



Obr. 7: Schéma hledání opatření

6.3.1 Sepsání seznamu hrozba – scénář

V tomto kroku byla použita tabulka se sloupci nadepsanými

- **Hrozba:** je to projev konkrétního nebezpečí, příčina nežádoucího stavu (například schodiště v provozním prostoru robotu)
- **Scénář:** je následkem hrozby, nežádoucí stav (například pád robotu ze schodiště)
Mezi hrozbou a scénářem je vztah příčina – důsledek.
- **Poznámka**

Řádky tabulky byly postupně vyplňovány dvěma způsoby. Buď tak, že se hledala odpověď na otázku „**Co se může přihodit nepříznivého pro bezpečnost osob a majetku, když se realizuje daná známá hrozba?**“ Tedy postup HROZBA $\Rightarrow$ SCÉNÁŘ, kdy k hrozbě hledáme možné následky.

Druhý způsob spočívá v hledání odpovědi na otázku „**Co může být příčinou, že nastane známý scénář nepříznivý pro bezpečnost osob a majetku?**“ Tedy postup SCÉNÁŘ $\Rightarrow$ HROZBA, kdy ke scénáři hledáme jeho příčinu.

V několika případech bylo složité určit možné scénáře a řádek zůstal definován pouze hrozbou, která ohrožuje bezpečnost. U případů selhání softwaru nelze přesně určit hrozbu, takže zůstalo pouze u scénářů.

Po skončení vyplňování polí hrozeb a scénářů byl seznam předán odborníkům, aby ho doplnili nebo opravili. Po ověření byl seznam potvrzen jako platný výsledek identifikace hrozeb a scénářů v otázkách bezpečnosti provozu AMR.

6.3.2 Kvantifikace bezpečnostních rizik

Pro kvantifikaci rizik byla použita vytvořená tabulka hrozba – scénář. Bylo rozhodnuto, že se použije stejných klasifikačních stupnic jako u určování pravděpodobnosti a významu u FMEA. Toto rozhodnutí umožnilo využít zažitých dovedností z předchozích analýz. S pomocí klasifikačních tabulek byly doplňovány jednotlivé dvojice hrozba – scénář o hodnotu pravděpodobnosti a velikosti dopadu. Bodování bylo určeno na základě shody účastníků analýzy. Hodnota rizika potom byla stanovena jako součin bodů za výskyt a bodů za možné dopady.

Získané hodnocení rizik bylo dále protříděno takto:

- Dvojice hrozba – scénář s malou pravděpodobností a nízkým významem byly pouze zdokumentovány pro pozdější přehodnocení. Hodnota jejich rizika byla do 15 včetně.
- Dvojice hrozba – scénář s vysokou pravděpodobností a vysokým významem byly ihned zařazeny do pracovních úkolů zodpovědných osob.
- Ostatní dvojice byly zařazeny pro zpracování doporučení opatření ke snížení rizika.

Po roztřídění byly formuláře založeny pro další zpracování do dokumentace k AMR Advee.

6.3.3 Snižování rizika

Pro každou dvojici hrozba – scénář bylo hledáno opatření, které by mohlo snížit hodnotu rizika. Návrhy byly zapisovány do stejné tabulky, s jakou se pracovalo doposud

v této metodě. Zdrojem pro návrhy opatření byly znalosti odborníků z jednotlivých oblastí, doporučení v ČSN. Našlo se i několik netradičních opatření, která by měla být podrobena zkoumání.

Po doplnění možných opatření byly návrhy prověřovány z hledisek časové a materiální náročnosti, proveditelnosti, smysluplnosti a účinnosti.

Analýza byla ukončena v lednu 2012 a v současné době jsou schválená a prováděná opatření předmětem vyhodnocování. Zejména jejich vlivu na hodnoty rizika. Jestliže možné dopady budou vyhodnoceny jako stále velmi vysoké, i když jejich pravděpodobnost je malá, měla by být připuštěna možnost zastavit provozování robotu. Zároveň s takovýmto časovým prostorem by měla být informace o riziku předána na nejvyšší místa řízení ve firmě Bender Robotics s. r. o.

7 DOPORUČENÍ K PROVOZU AMR

Smyslem této kapitoly je prezentovat a komentovat navržená opatření ke snížení rizik bezpečnosti provozu AMR.

7.1 Role pracovníků

Aby práce na dozorování a udržování robotu byla koordinovaná, měly by být rozděleny pracovní role. Rozdělení je možné například podle tohoto schématu. Pravomoci každého by mely být specifikovány tak, aby bylo jasné, kdo má rozhodující slovo.

Tabulka 4: Role pracovníků

role	kvalifikace	zodpovědnosti	pravomoc
manažer realizátorů	školení realizátorů organizační schopnosti	- stejné jako realizátor, navíc: - kontrolovat dodržování pravidel a pokynů dle návodů - dohlížet hladký průběh akce - dodržovat bezpečnostní pravidla - vyplňování formulářů o průběhu akce - kontaktování servisního technika v případě závady - kontrolovat, že je robot po ukončení činnosti plně vypnutý	- stejné jako realizátor, navíc: - vypínat a zapínat zdroj napájení soustavy robotu - řídit ostatní realizátory - určovat dočasně svého zástupce z řad realizátorů
realizátor	školení realizátorů	- co nejpřesněji vykonávat úkoly zadané manažerem realizátorů - odstavit okamžitě robot v případě závady - volat tísňové linky v případě kritické havárie - kontaktovat co nejrychleji manažera realizátorů v případě nastalé rizikové situace	- zastavit robot nouzovým tlačítkem - upozornit osoby jejichž činnost v okolí robotu vede ke zvýšenému riziku ohrožení bezpečnosti osob - vyměňovat náplně a doplňovat zdroje energie
servisní inženýr	školení servisního technika paragraf 6/1978 Sb.	- dodržovat zásady BOZP - kontrolovat robot preventivně každých 500 hodin provozu	- vypínat a zapínat zdroje napájení soustavy robotu - otevírat kryt elektroniky robotu - provádět servisní zásahy
uživatel	nemá kvalifikaci	- používat zdravý rozum - neotvírat, ani nerozebírat robot - nevstupovat robotu prudce do cesty - používat pouze dotykový displej - nesnažit se robot převrhnout	

7.2 Obecná pravidla

Robot byl konstruován s ohledem na maximální bezpečnost uživatele při běžném

provozu. Když je plně sestaven, uživatel nepřichází do styku s nebezpečným elektrickým napětím ani pohyblivými částmi. Realizátor, který dozoruje robot v provozu, by měl být proškolen v bezpečné instalaci robotu a v základních pravidlech servisního zásahu.

7.3 Předpokládané použití robotu

Neměly by být odstraňovány kryty ani části karoserie robotu, který je v provozu, anebo v jehož okolí se nachází neproškolené osoby (uživatelé).

Měl by být vyčerpávajícím způsobem zpracován návod a být vyžadováno jeho dodržování. Nemělo by docházet k žádným uživatelským a neodborným úpravám robotu, k jeho provozování v nesestaveném stavu. Neměl by být provozován způsoby ignorujícími pokyny návodu, protože zvyšují rizika úrazu nebo škod na majetku.

Robot by měl být provozován v prostředí s daným rozmezím teploty a vlhkosti. Pokud je skladovací prostor chladnější než provozní, je nutno před provozem robotu počkat, než se přístroj teplotně srovná. Předpokládají se tyto vlastnosti provozního prostředí:

- Skladovací prostory
Teplota: -20 – 50 °C
Relativní vlhkost: 10 – 80 % (nesmí kondenzovat)
- Provozní prostory
Teplota: 4 – 40 °C
Relativní vlhkost: 10 – 80 % (nesmí kondenzovat)

7.4 Opatření ke snížení rizik plynoucích z elektrických zařízení

Měla by být zavedena následující opatření:

- Odvádění statické elektřiny pomocí částečně vodivého spojení s podlahou, např. vlečným pruhem.
- Zabránění vystavování atmosférickým výbojům, např. za bouřek.
- Zkonstruování krabice baterií tak, aby v případě tepelných úniků výšlehy směřovaly k podlaze.
- Předcházení chybnému zapojení baterií klíčovými konektory
- Předcházení zkratům, otřesům, prorážení baterií.
- Odstavovat robot při proražení krabice baterií.
- Odstavovat robot v případě akustických projevů selhání baterií, zařídít vyklizení provozních prostor, volat nouzové telefonní číslo 150, hlásit operátorovi přítomnost

akumulátorů.

- Zamezit provádění servisních zásahů při zvýšené vlhkosti, poškozených kabelech, porušení ochranné krabice baterií.
- Odstranit namáhání kabelů robotu, zabránit působení nepříznivým vlivům sil a momentů na kabely.
- Věnovat pozornost předmětům spadlým do robotu např. při servisním zásahu.
- Používat pojistek ve zdroji robotu vhodných parametrů.
- Plánovat preventivní prohlídky elektroniky robotu, včasné odstraňovat závady a poruchy.
- Povolit zásahy pouze odborným pracovníkům.
- Používat pouze předepsané nářadí.
- Včasné odborně opravovat poškozená el. zařízení v provozním prostoru.
- Vést vodiče elektrické sítě mimo provozní prostory.
- Šetrné zacházení s vodiči a přívody.
- Zamezit zásahům do robotu mokrýma rukama.
- Seznámit uživatele během interakce možnými hrozbami.
- Neponechávat robot zapnutý po skončení jeho provozu nebo během skladování.
- Zapracovat bezpečnost práce s el. spotřebiči do návodu.
- Před použitím robotu vizuálně kontrolovat stav robotu.
- Nepoužívat poškozené přívodní kabely.
- Připojovat k napájení pouze určeným konektorem a z napájecího zdroje k tomu určenému.
- Vybavit robot štítkem s informacemi o napájecím napětí a proudu.
- Vybavit nadproudovou ochranou, nouzovým tlačítkem, zařízením zajišťujícím ochranu před nebezpečným dotykem neživých částí a zásuvky.
- Před připojením na síť mít spínače v poloze „vypnuto“.
- Neprovozovat robot s chybějícími částmi karoserie.
- Pravidelné kontroly a revize.
- Před prováděním údržby, oprav a čištění odpojit robot od sítě.
- Šetrně zacházet s kabelem (nepoužívat k vlečení robotu).
- Nepoužívat poškozené kabely.
- Nemanipulovat (nepřenášet) zapnutý nebo k el. síti připojený robot.
- Dodržovat zákaz odstraňovat kryty mimo servisní zásahy, kdy by se pracovník mohl dostat do styku s napětím na vodivé kostře nebo se přímo dotýkal obnažených vodičů.

- Odborné opravy přívodních kabelů provádí pouze elektrikář.
- Spoje odlehčovat od tahu, prodlužovací šňůry připojovat s ochranným vodičem a nepřerušenou ochranou, zajistit ochranný vodič o něco delší, aby se při vytržení přerušil jako poslední.
- Zakázat vedení přívodních kabelů přes frekventovaný prostor.
- Před manipulací odpojit napájecí kabel.
- Přívodní kabel k robotu klást mimo ostré hrany.
- Po ukončení nabíjení odpojit ze zásuvky.
- Zkonstruovat brzdy aktivované při výpadku napájení.

7.5 Opatření ke snížení rizik s lidským faktorem

Měla by být zavedena následující opatření:

- Odstranění vlhkosti z ploch v provozním prostoru, nebezpečí uklouznutí.
- Odstranění objektů, o které je možno zakopnout.
- Udržovat schůdnost provozního prostoru.
- Zabránit vylézání na židle s kolečky.
- Neodstranitelné překážky označit černožlutým nebo červenobílým šrafováním.
- Udržovat volné komunikační průchody.
- Nemanipulovat v prostoru s varnými konvicemi a otevřenými nádobami s nápoji.
- V případě rozlitych kapalin v provozním prostoru odstavit robot do jejich odstranění.
- Utěsnění spár v konstrukci karoserie robotu.
- Konstrukce odvodních kanálků v karoserii robotu.
- Přestávky v práci s robotem.
- Kompenzační cvičení při dlouhotrvající práci s robotem.
- Odstranit přebytečné světelné zdroje za monitorem.
- Detekovat výkyvy v zatížení motorů robotu, zastavení v případě náhlé změny.
- Odstavit robot při poškození karoserie.
- Do provozu uvádět pouze robot v dobrém technickém stavu.
- Signalizovat softwarově zjistitelné závady.
- Zastavit v případě zjištění závady během provozu, závadu odstranit, případně povolat technika pro odborný zásah.
- Zajišťovat kvalifikaci operátorů.
- Senzory důležité pro zastavení nevypínat v režimu manuálního řízení.
- Dálkově řídit robot pouze s podmínkou dobrého zdravotního stavu operátora.
- Neřídit robot mimo dohled operátora.

- Nepožívat návykové látky před a během řízení robotu.
- Stanovit a dodržovat pracovní režim operátora.
- Stanovit a dodržovat přestávky v řízení.
- Dodržovat správné způsoby ruční manipulace.
- Nepřetěžovat pracovníky, při přenosu dodržování limitu zátěže 50 kg na osobu.
- Určit pracovníka, který bude manipulaci koordinovat.
- Výcvik a školení pracovníků o správných způsobech a postupech manipulace.
- Dodržovat zásady bezpečnosti práce a zdraví nezávadného způsobu manipulace, zejména bez ohnutých zad.
- Správný pohyb při manipulaci (rovná záda, plynulý pohyb, břemeno blízko těžiště těla...).
- Zajistit dostatek prostoru ve směru zdvihu.
- Ujistit se, že podlaha je stabilní.
- Udržovat rovné, suché a nekluzké podlahy.
- Používat vhodnou obuv.
- Zajistit, aby pracovník mohl zaujmout bezpečný postoj pro přenos.
- Zajistit odpočinek, je-li námaha častá nebo dlouhá.
- Přizpůsobit tempo nejpomalejšímu pracovníkovi.
- Zajištění koordinace osob přenášejících robot.
- Používání vhodných pomůcek (madla, popruhy, palety).
- Používání pouze určených úchopových částí kostry robotu.
- Kontrolování stavu robotu, zabezpečení před manipulací.
- Zákaz používání opotřeбенých pomůcek.
- Využívat manipulačních podložek, které mají mezeru od podlahy.
- Připravit trasu manipulace s robotem předem.
- Upravit okolí úchopových otvorů, odstranit ostré hrany.
- Vyloučení manipulace s poškozenými částmi robotu, naštípnutým laminátem, prasklou koustou, rozbitými skleněnými částmi.

7.6 Opatření ke snížení rizik plynoucích z mezních stavů a konstrukčních prvků

Měla by být zavedena následující opatření:

- Konstruovat karoserii tak, aby se znesnadnilo sahání do disků kol.
- Opatřit robot výstražnými samolepkami ve spodku karoserie (typ sekačka).
- Volit disky kol bez otvorů.

- Opatrnost při servisním zásahu.
- Výměnu součástí provádět pouze proškoleným personálem.
- Konstrukci kostry nahradit opracovanějšími díly.
- Upevnit vodiče v robotu zamykacími pásky, nejlépe ke kostře robotu a mimo její ostré hrany.
- Výstražné značení proti vsunování končetin pod robot.
- Pravidelné kontroly technického stavu po 500 h provozu.
- Testování nárazníku před ostrým provozem.
- Odstranit překážky uložené ve výšce hlavy robotu (např. schodiště, poličky, zavěšená osvětlení).
- Pokud překážka nejde odstranit, vyjmutí prostoru kolem ní z provozního prostoru.
- Upozornit na slepá místa senzorické sítě.
- Detekce osob kamerou, ultrazvukovými senzory, kontaktním nárazníkem.
- Zavedení zřetelného nouzového stop tlačítka do konstrukce.
- Signalizace směru pohybu světly (automobil).
- Pravidelné kontroly:
 - Stavů pneumatik,
 - Přílnavosti plných obručí k ráfkům,
 - Zachycení cizích předmětů v discích kol,
 - Stavů řídicí soustavy,
 - Částí kyvné nápravy,
 - Neporušenosti vany robotu.

7.7 Opatření ke snížení rizik plynoucích z provozního prostředí

Měla by být zavedena následující opatření:

- Před uvedením robotu do provozu upravit prostor, upozornit na vyžadované vlastnosti prostoru v návodu.
- Odstranit objekty se špatnou statikou z prostoru.
- Objekty v prostoru musí být stavěny stabilně.
- Odstranit předměty z okrajů nábytku.
- Udržovat pořádek na nábytku.
- Nepřetěžovat nábytek, police.
- Dodržovat zmapované rozmístění nábytku.
- Udržovat pořádek zavedený v provozním prostoru.
- Důsledně zavírat zásuvky a dveře skříní.

- Zajištění dveří v otevřené poloze, zanesení prostoru dveří jako zakázané zóny v mapě robotu.
- Příčný sklon odstavných ploch max. 5 %.
- Podélný sklon odstavných ploch max. 3 %.
- Označit vstupy do pracovního prostoru přenosnou značkou „provozní prostor robotu“.
- Zajištění odstaveného robotu zádržkami kol.
- Rovnoměrné osvětlení provozního prostoru.
- Zajištění poklopů proti posunutí.
- Uzavírání poklopů.
- Vyměňování poškozených částí podlah v provozním prostoru.
- Přidání detekce otvorů (schodiště) do senzorické sítě robotu.
- Vyjmutí neúnosných povrchů z provozního prostoru.
- Odstranění překážek nižších, než je úroveň senzorů.
- Zmapování nebezpečných výstupků v podlaze.
- Pokud překážky nelze odstranit, je potřeba je zanést do mapy robotu jako zakázanou oblast.
- Zajistit rovný, nevytlučený a nekluzký povrch podlah.
- Použití senzorické sítě.
- Použití nárazníků.
- Zavést do konstrukce nouzové tlačítko.
- Vyjmout prostory kolem únikových východů z provozního prostoru robotu.
- Vyloučení provozu robotu přes můstky a nájezdové rampy s nízkou nosností.
- Neprovozovat robot v prostorech s hořlavými kapalinami, plyny a výpary.
- Před uvedením robotu do provozu odstranit překážky v bezprostřední blízkosti jeho dálkoměrů.
- Zajistit pokrytí provozního prostoru majáky.
- Udržovat vzdálenost robotu od jeho majáků do 6 m.
- Před uvedením robotu do provozu zkontrolovat lokalizaci zkušební jízdy.
- Definování překážek, které je robot schopen detekovat do návodu.
- Odstranění nedetekovatelných překážek z provozních prostor.
- Zajistit dostatek prostoru, odklizení překážek, udržování pořádku ve skladovacích prostorech.
- Zabezpečit přepravní vozík proti samovolnému pohybu.
- Držet vozík tak, aby prsty nepřesahovaly šíři vozíku.

- U vozíku s rudlem využívat boční chrániče madel.
- Při vjíždění do omezených prostor přepravní vozík zatlačovat a přibrzďovat zezadu.
- Zjistit, zda poklopy a části podlahy jsou dostatečně únosné.
- Ujistění se, že přejížděné podlahy jsou dostatečně široké.
- Zajištění pojezdových kol přepravního vozíku.
- Rovnoměrné a symetrické rozložení hmotnosti robotu.
- Rovná, pevná a suchá přejezdová plocha.
- Odstraňovat překážky před samotnou manipulací.
- Výměna lokalizačních dat mezi roboty v případě souběžného provozu několika robotů.
- Ověřit, že nedochází k interferencím ultrazvukových senzorů.
- Provozní plochy musí být do 5% sklonu.

7.8 Opatření ke snížení rizik plynoucích z chyb softwaru

Měla by být zavedena následující opatření:

- Psaní robustního softwaru.
- Implementace programů s hlídáním funkcí.

8 ZÁVĚR

Cílem práce bylo posouzení bezpečnosti AMR v indoor prostředí. Cesta k cíli začala hledáním existujících norem, které by obsahovaly rady a doporučení k dosažení bezpečnosti autonomních mobilních robotů. Tématicky nejbližší zjištěná norma, připravovaná Mezinárodní organizací pro standardizaci, řešící fyzický kontakt člověka a robotu je ISO/DIS 13482: Bezpečnostní požadavky na neprůmyslové roboty – nemedicínské roboty osobní péče. Jediným vodítkem pro výrobce tedy zůstává obecná norma ISO 12100 pro bezpečná strojní zařízení a řada norem pro bezpečnost elektrických zařízení.

Podstatná část práce se věnovala řetězu analýz rizik možných poruch a experimentálnímu ověření výskytu a vážnosti bezpečnostních rizik. Analýzy byly prováděny týmově s využitím zkušeností z provozu konkrétního autonomního mobilního robotu. Vrcholem praktické části byla analýza v metodice RIPRAN, která kombinuje informace z předchozích analýz, z experimentu, požadavky z vybraných technických norem a názor zúčastněných odborníků a uživatelů. Výstupem poslední analýzy je soubor doporučení ke snížení rizik provozu.

Identifikaci a hodnocení bezpečnostních rizik nelze prohlásit za ukončené. Vyhodnocování rizik, stejně jako proces zvyšování kvality, je rekursivní proces využívající při každém kroku ohlédnutí do minulosti. Hlavním přínosem práce je nastartování procesu zlepšování ve firmě Bender Robotics, během kterého byly utříděny existující (nejenom) bezpečnostní problémy produktu. Byly tak uvedeny v život principy pro vytváření bezpečných výrobků ve fázích vývoje, těsně před výrobou a dalších. Byla sestavena množina doporučení ke snížení rizik provozu AMR. Některá doporučení jsou nyní aplikována a vyhodnocována, jiná budou zanesena do příruček k provozování robotu Advee. Pozornost byla soustředěna na management technických rizik u produktu, jeho poruch, poruchových stavů a jejich předcházení. Byly vzaty v potaz základní normy a zákony související s jakostí a bezpečností.

Při tvorbě práce vyvstávala otázka, zda by bylo možné předložený návrh doporučení použít obecně pro větší množinu AMR, než je jeden konkrétní zkoumaný. Pátrání po dokumentačních materiálech jiných autonomních robotů [26] ukazuje, že buď jsou zveřejněná technická data velmi kusá, nebo je použitá technologie dosti odlišná. Otázku zobecnění doporučení tedy nelze spolehlivě zodpovědět a zůstává otevřená pro další zkoumání.

Z výše uvedených odstavců je zřejmé, že všechny úkoly stanovené v zadání byly dobře definované, proveditelné a jejich zpracování umožnilo odpovědět na řadu otázek

vývojářů konkrétního produktu. Otázka zobecnění bezpečnostních doporučení zůstává sice otevřená, nicméně cílů stanovených v zadání této diplomové práce bylo bezezbytku dosaženo.

9 SEZNAM POUŽITÉ LITERATURY

- [1] ŠENK, Josef et al. *Rukověť pracovníka pro posuzování shody výrobku*. Praha: Národní informační středisko pro podporu jakosti, 2004. ISBN 80-02-01668-8.
- [2] *Interní dokumentace firmy Bender Robotics s.r.o.*
- [3] ISO - International Organization for Standardization [online]. Dostupné z: <http://www.iso.org/iso/home.html> [cit. 2012-04-20].
- [4] *Databáze ČSN dostupná z knihovny FSI VUT.*
- [5] MOŽNÝ, Radek, Bc. *Analýza rizik v procesu posuzování shody: Diplomová práce*. Brno, 2010. Diplomová práce Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství.
- [6] MYKISKA, Antonín - ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE. STROJNÍ FAKULTA. *Bezpečnost a spolehlivost technických systémů*. V Praze: Vydavatelství ČVUT, 2004. ISBN 80-01-02868-2.
- [7] *Normy jakosti ISO 9000, ISO 9001, ISO 9004* [online]. Dostupné z: <http://normy.jakosti.cz/> [cit. 2012-04-20].
- [8] SMEJKAL, Vladimír - RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada, 2006. 269 s. ISBN 8024716674.
- [9] *RIPRAN - Metoda pro analýzu projektových rizik* [online]. Dostupné z: <http://ripran.cz/popis.html> [cit. 2012-04-10].
- [10] *Poka-Yoke* [online]. Dostupné z: <http://www.poka-yoke.org.uk/> [cit. 2012-03-3].
- [11] SHINGO, Shigeo et al. *A study of the Toyota production system from an industrial engineering viewpoint*. Productivity Press, 1989. 306 s. ISBN 9780915299171.
- [12] *Six Sigma* [online]. Dostupné z: <http://www.isixsigma.com/dictionary/six-sigma/> [cit. 2012-03-3].
- [13] *How CRAMM works* [online]. Dostupné z: <http://www.cramm.com/overview/howitworks.htm> [cit. 2012-05-12].
- [14] *Soustava technických norem* [online]. Dostupné z: <http://www.skolalextilu.cz/normy/index.php?page=1> [cit. 2012-05-1].
- [15] *Náhled obsahu normy ČSN EN 292-2 (833001) - Bezpečnost strojních zařízení. Základní pojmy, všeobecné zásady pro projektování. Část 2: Technické zásady a specifikace - listopad 1994* [online]. Dostupné z: <http://shop.normy.biz/d.php?k=16411> [cit. 2012-02-22].
- [16] *:: CEN - European Committee for Standardization :: Members* [online]. Dostupné z: <http://www.cen.eu/cen/Members/Pages/default.aspx> [cit. 2012-05-1].
- [17] *Úvod - ÚNMZ* [online]. Dostupné z: <http://www.unmz.cz/urad/uvod> [cit. 2012-05-18].
- [18] *ČSN EN 414 - Náhled* [online]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/83/60918/60918_nahled.htm [cit. 2012-02-23].

- [19] ČSN EN ISO 12100 - *náhled normy* [online]. Dostupné z: http://www.technicke-normy-csn.cz/inc/nahled_normy.php?norma=833001-csn-en-iso-12100&kat=88295 [cit. 2012-02-25].
- [20] Zákon č. 22/1997 Sb. - *o technických požadavcích na výrobky a související předpisy - TzB-info* [online]. Dostupné z: <http://www.tzb-info.cz/pravni-predpisy/zakon-c-22-1997-sb-a-souvisejici-predpisy> [cit. 2012-02-19].
- [21] WENG YUEH-HSUAN et al. *The Legal Crisis of Next Generation Robots - On Safety Intelligence*. 1001 Ta Hsueh Rd. Hsinchu 300, Taiwan: National Chiao Tung University College of Computer Science, 2007. 5 s.
- [22] *Bender Robotics s.r.o.* [online]. Dostupné z: <http://www.advee.eu/> [cit. 2012-05-4].
- [23] RIPEL, T. *Návrh a realizace konstrukce kolového mobilního robotu*. Brno, 2010. Diplomová práce Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství.
- [24] ISO/DIS 13482 - *Robots and robotic devices -- Safety requirements for non-industrial robots -- Non-medical personal care robot* [online]. Dostupné z: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53820 [cit. 2012-05-3].
- [25] Yueh-Hsuan Weng | *European University Institute | Legal Informatics, AI & Law | Visiting Researcher* [online]. Dostupné z: http://works.bepress.com/weng_yueh_hsuan/ [cit. 2012-05-5].
- [26] *Humanoid robot projects* [online]. Dostupné z: <http://mindtrans.narod.ru/robots/robots.htm> [cit. 2012-05-17].

10 SEZNAM OBRÁZKŮ, TABULEK A PŘÍLOH

Obr. 1: Nárys, bokorys, představa designera a realita, zdroj [2].....	15
Obr. 2: Schéma vztahů jakost – bezpečnost, zdroj [6].....	20
Obr. 3: Robot Advée ve foyer hotelu Clarion v Praze, zdroj [22].....	35
Obr. 4: Zjednodušený model AMR, zdroj [2].....	37
Obr. 5: Ukázka záhlaví formuláře FMEA.....	42
Obr. 6: Vzor protokolu o pozorování znaků/chování, zdroj [6].....	46
Obr. 7: Schéma hledání opatření.....	47
Tabulka 1: Pravděpodobnost výskytu vady, zdroj: upravena verze [6].....	42
Tabulka 2: Hodnocení závažnosti poruchy, zdroj: upravené z [6].....	43
Tabulka 3: Odhalitelnost poruchy, zdroj: upravené z [6].....	43
Tabulka 4: Role pracovníků.....	51
Příloha 1: Ukázka formuláře DOE.....	64
Příloha 2: Ukázka formuláře FMEA.....	65

Příloha 1: Ukázka formuláře DOE

Zjednotlivě uložte každý

DOE Observation Sheet

DOE Název		temp	Produkt / #	Doba experimentu	Pozorování experimentu	Datum experimentu	Vedoucí									
#	Očekávaný znak/chování	Neočekávaný znak/chování	Počet pozorování znaku/chování													
			1	2	3	4	5	6	7	8	9	10				
1		Robot vyjede z polygonu	8:30*	8:47*	9:58*	11:01	11:49									
2		Robot nepokryje rovnoměrně polygon (pohyb se soustředí jen na omezenou oblast)	14:23													
3		Robot ignoruje uživatele	10:17													
4		Při dotyku na obrazovku je nutné potvrdit přítomnost uživatele	14:23													
5		Robot se nepohybuje elegantně	14:23													
6		Robot ztratí informaci o poloze														
7		Uživatel odejde od robota uprostřed interakce, robot v ní pokračuje	8:33	9:52	11:41	11:49										
8		Problémy s tiskárnou														
9		Kopnutí do nárazníku														
10		Vypadek WIFI														
11		Vypadek diagnostického centra														

* 8:30 - Získal seřít ve velké místnosti polygon

Příloha 2: Ukázka formuláře FMEA

	Prvek/Funkce	Způsob možné závady	Možný důsledek závady	Závažnost	Klasifikace	Možná příčina(y) mechanismus(y) závady
1	Zadní poloosy	Ukroucení vlivem přetížení	Upadnutí zadního kola, ztráta pohybových schopností celého zařízení, možnost poškození celého zařízení	10		Cyklická únava zadní poloosy, mechanické přetěžování hřídele, nedostatečně dimenzovaná hřídel
2	Diferenciál	Uvolnění šroubů na kolech diferenciálu, uvolnění šroubů na věnci diferenciálu	Nefunkčnost diferenciálu, ztráta pohybových schopností celého zařízení	10		Uvolnění závitů šroubů
3	Mechanismus nárazníků	Uvolnění matic nárazníků, vyhlodání materiálu závitem na šroubech nárazníku	Omezení funkce nárazníků, přerušování kontinuální jízdy zařízení	9		Uvolnění matic na nárazníku
4	Přední poloosy	Únava materiálu na přední poloose	Upadnutí předního kola, ztráta pohybových schopností celého zařízení, možnost poškození celého zařízení	9		Cyklická únava vlivem rázů
5	Oje řízení	Otlačení v místě spojení přes těsné pero	Negativní ovlivnění řiditelnosti	6		Nedostatečná styková plocha mezi perem a nábojem
6	Řídicí tyče	Ohnutí řídicích tyčí	Negativní ovlivnění řiditelnosti	5		Ohnutí vlivem rázů
7	Čepy řízení	Zatvrdnutí těles řízení na čepech řízení	Totální ztráta řiditelnosti, ztráta pohybových schopností celého zařízení	9		Špatná volba materiálu těles a čepů (obojí nerez ocel)
8	Kyvná tyč	Ohnutí kyvné tyče	Snížení světlé výšky zařízení až po kontakt s podlahou, ztráta pohybových schopností celého zařízení	8		Nedostatečně nadimenzovaná hřídel
9	Zadní pohon	Pískání pohonu	Potenciálně obtěžující	2		Konstrukční chyba