ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA ELEKTROTECHNICKÁ

KATEDRA TECHNOLOGIÍ A MĚŘENÍ

DIPLOMOVÁ PRÁCE

Návaznost nástrojů pro analýzu rizik

Bc. Tomáš Horáček **2018**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš HORÁČEK**
Osobní číslo:	**E16N0020P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Komerční elektrotechnika**
Název tématu:	**Návaznost nástrojů pro analýzu rizik**
Zadávající katedra:	**Katedra technologií a měření**

Zásady pro vypracování:

1. Proveďte analýzu nástrojů řízení rizik se zaměřením na nástroje FMEA a FTA
2. Zhodnoťte možné a používané vazby mezi oběma nástroji
3. Zpracujte analýzu rizik s využitím metod FTA a FMEA
4. Proveďte zhodnocení navrženého přístupu a navrhněte způsob implementace do prostředí firmy

Rozsah grafických prací: **podle doporučení vedoucího**

Rozsah kvalifikační práce: **40 - 60 stran**

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

Seznam odborné literatury:

1. **ČSN EN 60812. Techniky analýzy bezporuchovosti systémů - Postup analýzy způsobů a důsledků poruch (FMEA). Praha: Český normalizační institut, 2007.**
2. **ČSN EN 61025. Analýza stromu poruchových stavů (FTA)Praha: Český normalizační institut, 2007.**
3. **PLURA, Jiří. Plánování a neustálé zlepšování jakosti. Vyd. 1. Praha: Computer Press, 2001. Business books (Computer Press). ISBN 80-7226-543-1.**
4. **příručky automobilového průmyslu**
5. **firemní materiály**

Vedoucí diplomové práce: **Ing. Petr Netolický, Ph.D.**
Regionální inovační centrum elektrotechniky

Datum zadání diplomové práce: **10. října 2017**

Termín odevzdání diplomové práce: **24. května 2018**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Ing. Aleš Hamáček, Ph.D.
vedoucí katedry

V Plzni dne 10. října 2017

Abstrakt

Předkládaná diplomová práce je zaměřena na návaznost analýz rizik, konkrétně na metody FMEA a FTA. Jsou zde uvedeny typy analýzy FMEA a také postup vypracování, který je popsán na typu design FMEA z důvodu návaznosti na praktickou část. Dále je popsána analýza FTA včetně kvalitativní a kvantitativní metody vyhodnocení. V teoretické části jsou také uvedeny softwarové nástroje, které jsou vhodné pro současné použití obou metod. Teoretické poznatky jsou poté aplikovány v praktické části na reálný produkt ve spolupráci se společností WITTE Nejdek.

Klíčová slova

FMEA, FMECA, DFMEA, PFMEA, boundary diagram, P-diagram, matice rozhraní, FTA analýza

Abstract

The master theses is focused on the follow-up of risk analysis, specifically FMEA and FTA methods. The types of FMEA analysis are defined and the elaboration procedure is described on the design FMEA type due the use in the application part. FTA analysis, including a quantitative and a qualitative evaluation method, is described. Software tools suitable for simultaneous use of both methods are also presented in the theoretical part. The theoretical knowledge are then applied in the application part on the real product in cooperation with WITTE Nejdek company.

Key words

FMEA, FMECA, DFMEA, PFMEA, boundary diagram, P-diagram, interface matrix, FTA analysis

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této diplomové práce, je legální.

.....

podpis

V Plzni dne 18.5.2018 Bc. Tomáš Horáček

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Petru Netolickému, Ph.D. za cenné profesionální rady, připomínky a metodické vedení práce. Také bych rád poděkoval panu Ing. Vladimíru Votápkovi za ochotu a cenné profesionální rady při zpracování analýz a poskytnutí potřebných podkladů.

Úvod

V současné době se ve všech odvětvích průmyslu neustále zdokonalují výrobní technologie, zákazníci přicházejí s novými požadavky a je proto kladem veliký důraz na kvalitu a bezpečnost produktů. Konkurence na trhu je obrovská, proto podniky, které dokáží analyzovat a řídit rizika spojená s návrhem a výrobou jejich produktů mají značnou výhodu. Analýza rizik je v této době nezbytná pro efektivní řízení výroby. V případě, že podnik analyzuje rizika již v rané fázi návrhu produktu a dokáže jim předejít ještě před spuštěním sériové výroby, znamená to obrovskou úsporu finančních prostředků.

Cílem této diplomové práce je provést analýzu používaných nástrojů pro analýzu rizik se zaměřením na nástroje FMEA (Failure mode and effects analysis), v českém překladu analýza způsobů a následků poruch, a FTA (Fault tree analysis), v českém překladu strom poruchových stavů. Dalším úkolem diplomové práce je poté zhodnotit používané vazby mezi těmito nástroji a s jejich využitím zpracovat analýzu rizik konkrétního produktu pro společnost WITTE Nejdek.

Metoda FMEA patří mezi vůbec nejpoužívanější nástroje pro analýzu rizik a je také součástí mnoha norem a referenčních příruček nejen pro automobilový průmysl, ale také pro letectví, farmacii, ropný průmysl atd. Jedná se týmovou analytickou metodu induktivního přístupu, tedy zdola nahoru. To znamená, že určí nejdříve příčiny poruch a následně analyzuje jejich následky. Naopak metoda FTA, která je též týmovou metodou, přistupuje k problému induktivně, tedy shoda dolů. V tomto případě se určí vrcholová událost (porucha) a následně se pomocí logických návazností určují její příčiny. Druhá z metod je často využívána pro grafickou dedukci poruchy a určení pravděpodobnosti jejího výskytu.

Použití návaznosti metod FMEA a FTA může přinést analytickému týmu hlubší a přesnější informace o potenciálním způsobu poruchy a jeho příčinách. Nevýhodou je však časová náročnost obou analýz a absence ukazatele finanční úspory.

Sezam zkratek

FTA	Strom poruchových stavů (*Fault Tree Analysis*)
FMEA	Analýza možných způsobů a následků poruch (*Failure Mode and Effects Analysis)*
FMECA	Analýza možných způsobů, následků a kritičnosti poruch (Failure Modes, Effects and Criticality Analysis)
DFMEA	Design FMEA, návrhová FMEA nebo konstrukční FMEA
PFMEA	Process FMEA nebo procesní FMEA
SFMEA / CFMEA	System FMEA nebo systémová FMEA
YC / YS	Speciální znaky pro klasifikaci v design FMEA
RPN	Číslo priority rizika
MKR	Minimální kritický řez
OR	Logický součet
AND	Logický součin
ETA	Analýza stromu událostí (Event Tree Analysis)
HAZOP	Analýza rizik a provozuschopnosti (Hazard and Operability Study)
QS 9000	Oborová norma amerického automobilového průmyslu
IATF 16949:2016	Oborová norma automobilového průmyslu
VDA	Svaz německého automobilového průmyslu (Verband der Automobilindustrie)
HACCP	Systém analýzy rizika a stanovení kritických kontrolních bodů
SPZ	Státní poznávací značka

Seznam obrázků

Seznam tabulek

1 FMEA

Zkratka metody FMEA vychází z anglického názvu *Failure Mode and Effects Analysis*, pro který se používá český překlad analýza způsobů a důsledků poruch nebo analýza způsobů a následků poruch. Jedná se o týmovou analytickou metodu, která se řadí k základním preventivním metodám managmentu jakosti a rizik. Používá se především analýza designu produktu (DFMEA) a procesu (PFMEA). Cílem metody je u návrhu produktu co nejdříve prozkoumat možnosti vzniku vad, určit jejich možné následky, ohodnotit rizika a navrhnout způsoby jak je redukovat. Analýza se provádí přednostně v rané etapě vývojového cyklu, aby se daný způsob poruchy odstranil ještě před její implementací do systému a tím se snížily náklady na její případné odstranění. Jedná se o časově náročný proces a je velmi důležité, aby byl zařazen do harmonogramu vývoje. [1, 2]

V týmu pro analýzu FMEA by mělo mít každé oddělení, které je součástí daného procesu nebo produktu, svého odborníka (z oddělení vývoje, technologie, konstrukce, výroby, kontroly, řízení jakosti, zásobování, ekonomické části a oddělení vztahu se zákazníky). Celý tým metodicky a organizačně řídí moderátor FMEA, který je za celou analýzu odpovědný. Výhodou práce v týmu je především podněcování procesu myšlení a zajištění nezbytné odborné kvalifikace. [1, 2]

Rozšířením analýzy FMEA je analýza způsobů, důsledků a kritičnosti poruch FMECA (Failure modes, effects and criticality Analysis), do které jsou navíc zahrnuty prostředky pro klasifikaci závažnosti způsobů poruch, aby bylo možné stanovit prioritu protiopatření. Používá se k mapování pravděpodobnosti poruchových stavů proti závažnosti jejich následků. Výsledek upozorňuje na režimy selhání s poměrně vysokou pravděpodobností a závažností důsledků. [3]

1.1 Historie FMEA

Tato metoda byla vyvinuta armádou USA na konci 40. let minulého století, aby odhalila všechny možné příčiny poruch. Návod jak se vyvarovat chybám u strojů a zařízení používaných armádou, byl poprvé popsán v roce 1949 v dokumentu MIL-P-1629. Ze začátku metodu využíval pouze jaderný a letecký průmysl jako spolehlivostní analýzu složitých systémů. Veliký úspěch zaznamenala NASA, která tuto metodu aplikovala na projekt Apollo a úspěšně přistála na měsíci. [3, 4]

Během 70. let se používání FMEA a souvisejících technik rozšířilo i do civilního sektoru, především do automobilového průmyslu. Průkopníkem byla společnost Ford Motor Company, která jí poprvé použila pro sériovou výrobu modelu Ford Pinto. Tomu přecházela aféra spojená se špatnou bezpečností vozu, u něhož se při nárazu do zadní části porušovaly palivové nádrže, a hrozilo nebezpečí vzplanutí. Ford použil stejný přístup i k výrobním procesům, aby zvážil možné selhání způsobené procesem před zahájením výroby (PFMEA). V roce 1993 začlenila akční skupina automobilového průmyslu (AIAG) metodu FMEA do standardu QS9000 pro automobilovou výrobu a její dodavatele. Od té doby byla metoda i nadále zlepšována a byla zahrnuta do celé řady dalších norem a standardů. V České Republice byla v roce 2007 zavedena norma ČSN EN 60812, která popisuje návod na použití analýz FMEA a FMECA. Jsou v ní také definovány vhodné termíny a předpoklady pro vypracování analýz. [3–5]

Ačkoliv byla metoda FMEA původně vyvinutá armádou, v současnosti se široce používá v řadě průmyslových odvětví, které požadují nejvyšší úroveň spolehlivosti. Mimo automobilový průmysl mezi ně patří například zpracování polovodičů, ropy, plynu, či softwaru nebo zdravotní péče. [3, 4]

1.2 Cíle a přínosy metody

Metoda se provádí od nižší úrovně k vyšší úrovni systému, jedná se tedy o metodu induktivní. Zkoumá se, jakým způsobem by mohly poruchy na nižní úrovni ovlivnit celkovou funkčnost zařízení. [5]

Do obecných cílů provádění analýzy FMEA je možné zahrnout:

- zjištění poruch, které by mohly narušit bezporuchovost systému nebo bezpečnost uživatele,
- splnění požadavků smlouvy se zákazníkem, pokud jsou v ní uvedeny,
- možnosti zlepšení bezporuchovosti nebo bezpečnosti systému,
- možnosti zlepšení udržovatelnosti systému. [1]

Hlavní přínosy vyplývající z řádně vypracované analýzy FMEA jsou:

- zdokumentovaná metoda pro výběr designu s vysokou pravděpodobností bezporuchového a bezpečného provozu,
- zdokumentovaná jednotná metoda posuzování potenciálních mechanismů

selhání, režimů selhání a jejich vlivu na provoz systému. Výsledkem je seznam režimů poruch seřazených podle závažnosti jejich dopadu na systém a pravděpodobnosti výskytu,

- včasná identifikace jednotlivých bodů selhání, které mohou být rozhodující pro úspěch mise nebo bezpečnost produktu,
- efektivní metoda pro hodnocení dopadu navrhovaných změn v návrhu nebo provozní postupy týkající se bezpečnosti a úspěchu mise,
- základ pro postupy při odstraňování závad během provozu a pro nalezení zařízení pro sledování výkonu a detekce poruch,
- kritéria pro včasné plánování zkoušek,
- náklady vynaložené na její provedení jsou jen zlomkem nákladů, které by mohly vzniknout při výskytu vad,
- použitím metody lze odhalit významnou část možných závad. [2]

Mezi nevýhody patří především časová náročnost, složitost a pracnost při použití na velmi rozsáhlé systémy. Je nutné zapojit mnoho odborníků a zpracovat veliké množství informací a při nesprávném použití může být metoda také neefektivní, zdlouhavá a nákladná. Dalším nedostatkem je neschopnost poskytnout ukazatel celkové bezporuchovosti systému a proto není způsobilá poskytnout konkrétní ukazatel vyjadřující zlepšení návrhu a vztah mezi přínosy a náklady této metody. [6]

1.3 Typy FMEA

Jak již bylo uvedeno, analýza FMEA má několik druhů. Každý z nich se zaměřuje na jinou část výroby nebo se může jednat o rozšíření původní analýzy, jako například analýza FMECA. Mezi používané typy analýzy FMEA patří:

- FMECA,
- systémová FMEA (SFMEA nebo CFMEA),
- procesní FMEA (PFMEA),
- design FMEA (DFMEA).

1.3.1 FMECA

Analýza FMECA (Failure modes, effects and criticality Analysis), v českém překladu analýza způsobů, důsledků a kritičnosti poruch, je rozšířením analýzy FMEA. Přidaná hodnota se vztahuje k analýze kritičnosti, kterou zastupuje písmeno C ve zkratce FMECA.

Zatímco analýza FMEA je považována za kvalitativní metodu, FMECA se používá ke kvantitativnímu mapování pravděpodobnosti výskytu poruchových stavů. Jednotlivým poruchovým stavům jsou přiřazeny indexy kritičnosti. Podle hodnoty indexu lze určit dopad a závažnost poruchy, na kterou je potřeba se zaměřit a zároveň i úroveň protiopatření ke zmírnění či odstranění poruchy. Pro hodnocení kritičnosti se používá metoda čísla priority rizika RPN (Risk Priority Number), v některých případech se také používá jednodušší forma nenumerické analýzy ukazatele potenciálního rizika R. [1, 7]

Ukazatel potenciálního rizika R

Tento způsob se používá v případech, kdy nejsou k dispozici ukazatele závažnosti důsledku, pravděpodobnosti výskytu příčiny a detekce. Pro stanovení ukazatele priority rizika R se v některých typech analýzy FMECA uvádí tento vztah:

$$R = S \times P, \tag{1}$$

kde

- S „je bezrozměrné číslo, které klasifikuje závažnost, tj. odhad, jak silně budou důsledky poruchy ovlivňovat systém nebo uživatele,
- P též bezrozměrné číslo, které vyznačuje pravděpodobnost výskytu. Když je menší než 0,2, může být nahrazeno číslem kritičnosti C, které používá v některých kvantitativních metodách analýzy FMEA, tj. odhadem pravděpodobnosti, že nastane daný důsledek poruchy.“[1]

Číslo priority rizika RPN

Metoda RPN (The risk priority number) určuje celkové číslo kritičnosti tří faktorů, mezi které patří bezrozměrná čísla reprezentující závažnost poruchy (S), pravděpodobnost výskytu poruchy (O) a možnost detekce poruchy (D). Výpočet se uvádí v následujícím tvaru:

$$RPN = (S) \times (O) \times (D). \tag{2}$$

Všechny tři faktory se hodnotí subjektivně podle tabulek v rozmezí 1 až 10, kde hodnoty 9 nebo 10 jsou posuzovány jako velmi závažné. Výsledné číslo se pohybuje mezi hodnotami 1 a 1000. Nedoporučuje se však určovat prahovou hodnotu RPN pro posouzení rizikovosti, ale je třeba brát v úvahu všechny tři faktory podle jejich závažnosti. [1, 2]

Při vyhodnocování výsledků by se mělo zaměřit nejprve na vysokou míru závažnosti a nikoliv pouze na velikost čísla RPN. Jako ukázku lze uvést dva případy způsobu poruch. První bude reprezentovat vysokou hodnotu závažnosti (10), nízkou pravděpodobnost výskytu (3) a též nízkou hodnotu detekce (2). Druhý bude mít všechny hodnoty průměrné (5). V prvním případě vyjde celkové číslo 60 a ve druhém 125. Nelze tedy posuzovat míru rizika pouze na základě celkového čísla RPN, které vyšlo mnohem nižní v prvním případě i přes to, že se zde vyskytla nejvyšší závažnost poruchy s číslem 10. Z tohoto důvodu se zavádějí dodatečné postupy, aby bylo vždy zajištěno odstranění způsobů poruchy s nejvyšší třídou závažnosti jako první. [1, 2]

1.3.2 Systémová FMEA

Systémová FMEA identifikuje možné způsoby selhání, účinky a příčiny, které mohou zabránit tomu, aby systém splnil všechny své systémové cíle. Systémová FMEA je proces, který analyzuje požadavky / charakteristiky zákazníka vzhledem k zamýšlené funkci, aby zajistil, zda výsledný produkt splňuje potřeby a očekávání zákazníků. Pokud jsou identifikovány potenciální poruchové režimy, musí být zahájena akce k vyloučení nebo snížení jejich výskytu. Posouzení rizik se provádí pomocí RPN, tímto způsobem jsou vyhodnoceny režimy selhání, které je nutné řešit prioritně.

Hlavní přínosy systémové FMEA jsou:

- pomáhá vybrat optimální koncepční alternativy nebo určit změny specifikací v návrhu systému,
- identifikuje potenciální poruchové režimy a příčiny v důsledku interakcí v rámci tohoto konceptu,
- zvyšuje pravděpodobnost, že budou brány v úvahu všechny potenciální účinky způsobů selhání navrhované koncepce,
- identifikuje požadavky na testování na úrovni systému a subsystému. [2, 8]

1.3.3 Design FMEA

Design FMEA (DFMEA), často uváděná jako návrhová či konstrukční FMEA, se používá při návrhu produktu. Metodickým přístupem identifikuje potenciální rizika zavedení nových nebo změněných návrhů produktu.

Tato metoda bude dále detailně popsána v následující kapitole z důvodu návaznosti na praktickou část diplomové práce.

1.3.4 Procesní FMEA

Procesní FMEA (PFMEA) je metodický přístup používaný k identifikaci rizik při změnách technologického postupu či zavádění nového procesu. Metoda zpočátku identifikuje procesní funkce, možné způsoby selhání a jejich účinky na proces. Pokud je použita design FMEA při návrhu produktu, je třeba ji zahrnout do vstupů procesní FMEA. Dále jsou identifikovány příčiny a jejich mechanismy selhání, které jsou hodnoceny pomocí čísla priority rizika RPN. V případě vysoké pravděpodobnosti výskytu příčiny poruchy se zavádí nápravná opatření a testování vybraných částí procesu. PFMEA se neustále obnovuje při provedených změnách v procesu nebo návrhu produktu, jedná se tedy o živý dokument, který musí být aktualizován.

Hlavními přínosy procesní FMEA jsou:

- identifikuje procesní funkce a požadavky,
- identifikuje potenciální poruchy související s procesem,
- posuzuje účinky potenciálních poruch na zákazníka,
- identifikuje nedostatky v procesu, které umožní odpovědným osobám soustředit se na kontroly pro snížení výskytu poruch nebo na zlepšení metod pro jejich odhalení. [2, 8, 9]

2 Design FMEA (DFMEA)

V této kapitole je podrobně popsána DFMEA, která byla základem pro vypracování praktické části. Procesní a design FMEA mají většinu kroků společných, proto bude při popisu postupu zmíněna také procesní FMEA. V případě společných bodů je zmíněna analýza FMEA obecně.

Analýza možných způsobů a důsledků poruch návrhu produktu (DFMEA) je analytická metoda posuzovaná odpovědným technikem / týmem, která má zajistit posuzování a řešení potenciálních způsobů selhání a jejich příčin nového nebo změněného návrhu výrobku / služby. Vychází ze stejných postupů jako analýza FMEA, je však v některých krocích jinak specifikována. Analýza návrhu produktu nejprve identifikuje konstrukční funkce, režimy selhání a jejich účinky na zákazníka s odpovídajícím stupněm závažnosti. Dále jsou identifikovány příčiny a jejich mechanismy selhání, schopnost odhalení poruch a rovněž se používá číslo priority rizika RPN. Je to živý dokument, který se musí při jakékoliv změně návrhu aktualizovat a především by měl být dokončen před uvedením návrhu produktu do výroby. [2]

2.1 Přínosy DFMEA

Design FMEA podporuje proces návrhu snižováním rizika selhání včetně neúmyslných funkcí. Hlavními přínosy této metody jsou:

- podpora objektivního hodnocení návrhu včetně funkčních požadavků a návrhových alternativ,
- vyhodnocení počátečního návrhu požadavků na výrobu, montáž, servis a recyklaci,
- zvyšování pravděpodobnosti, že potenciální poruchové režimy a jejich účinky na systém a provoz produktu byly zohledněny v procesu návrhu / vývoje,
- vypracování seznamu možných chybových režimů podle jejich vlivu na "zákazníka", čímž vznikne prioritní systém pro vylepšení návrhu, testování a analýzu vývoje a validace,
- poskytování dokumentu pro doporučení a sledování opatření ke snížení rizika,
- zaměření na potenciální způsoby selhání produktu způsobené nedostatky návrhu. [2]

Jak již bylo zmíněno, jedním z nejdůležitějších aspektů úspěšné realizace FMEA je včasnost. Analýza by tedy měla být provedena ještě před realizací produktu či procesu a nikoliv po dané události. Pro použití postupu FMEA existují 3 základní případy, přičemž má každý z nich odlišný předmět působnosti nebo zaměření:

1) Zavádění nového návrhu, nové technologie, nebo nový proces.
   V tomto případě je předmětem analýzy kompletní návrh produktu, technologického postupu nebo procesu.
2) Změna stávajícího návrhu, produktu nebo procesu.
   Předmětem analýzy je úprava stávajícího produktu, technologického postupu, nebo procesu, která vychází ze zkušenosti z fáze užití daného produktu a může být ovlivněna i změnami předpisů či norem.
3) Použití stávajícího návrhu nebo procesu v novém prostředí, umístění nebo aplikaci.
   Předmětem analýzy je dopad nového prostředí, nové aplikace či funkce na stávající návrh produktu nebo na stávající proces. [9]

Posloupnost úkonů

Na následujícím obrázku je zobrazena posloupnost úkonů, při vytváření analýzy FMEA. Jedná se o strukturované otázky, které by si měl tým odborníků pokládat k tomu, aby správně provedl analýzu.

Obrázek 1: Posloupnost úkonů při vytváření analýzy FMEA. [2]

2.2 Postup

Definování předmětu

Na začátku analýzy je potřeba vymezit rozsah, který jasně ohraničuje, co bude zahrnuto a co bude vynecháno. Zároveň také stanovuje, jaké bude mít zaměření a jakým směrem se bude analýza ubírat. Tento výběr by měl být velmi pečlivý. Předmět, který bude zahrnutý do analýzy, může být stejně důležitý jako ten, který bude z analýzy vynechán. [9]

Pro definování předmětu FMEA mohou týmu pomoci následující podpůrné metody, které slouží také jako vstupy do DFMEA nebo PFMEA:

- funkční model,
- blokové diagramy vztahů,
- diagramy parametrů,
- diagramy rozraní,
- vývojové diagramy procesu,
- matice rozhraní,
- základní schéma,
- rozpisky materiálů. [9]

Sestavení týmu

Po vymezení předmětu je možné sestavit víceoborový tým odborníků, za který je obvykle odpovědná jedna pověřená osoba. Může jím být technik ze zdroje návrhu produktu, výrobce, dodavatel, nebo subdodavatel. Je třeba, aby byl sestaven tým znalých osob (např. inženýři s potřebnými znalostmi v oblasti návrhu, analýzy / testování, výroby, montáže, servisu, recyklace, kvality a spolehlivosti). Členové týmu mohou podle potřeby zahrnovat též odborníky na nákup, dodavatele a další odborníky. Pro každou analýzu se mohou členové týmu měnit podle znalostí a zkušeností v potřebných oblastech. FMEA by měla podněcovat vzájemnou výměnu názorů a týmové myšlení. Je proto důležité, aby měla odpovědná osoba zkušenosti v týmovém jednání a pomáhala týmu v jeho aktivitách. [2, 9]

Definování zákazníka

Obecně při tvorbě FMEA je dalším krokem určení zákazníka, pro kterého bude analýza vypracovaná. V případě design FMEA se jedná převážně o interní dokument, který je důležitý pro předcházení nejrizikovějším faktorům při návrhu produktu. Obecně pro FMEA však existují čtyři typy zákazníků.

- **Konečný uživatel**
  Jedná se o osobu nebo organizaci, pro kterou bude produkt vyroben a bude jej také využívat. V tomto případě může analýza FMEA zahrnovat například životnost produktu pro koncového uživatele.

- **Montážní a výrobní centra výrobců a originálních zařízení (závody)**
  Jedná se o pracoviště, ve kterých se provádějí výrobní operace a montáže produktů. FMEA zahrnuje rozhraní mezi produktem a montážním prostředím.

- **Zpracování v rámci dodavatelského řetězce**
  Jedná se o jakékoliv výstupní procesy nebo nezávazný výrobní proces na pracovišti dodavatele (zpracování, zhotovování nebo kompletování výrobních materiálů nebo dílů).

- **Kompetentní orgány**
  Orgány státní správy, které mohou ovlivnit daný produkt nebo proces bezpečnostními a environmentálními předpisy nebo mohou definovat požadavky. [9]

2.2.1 Vstupy do design FMEA

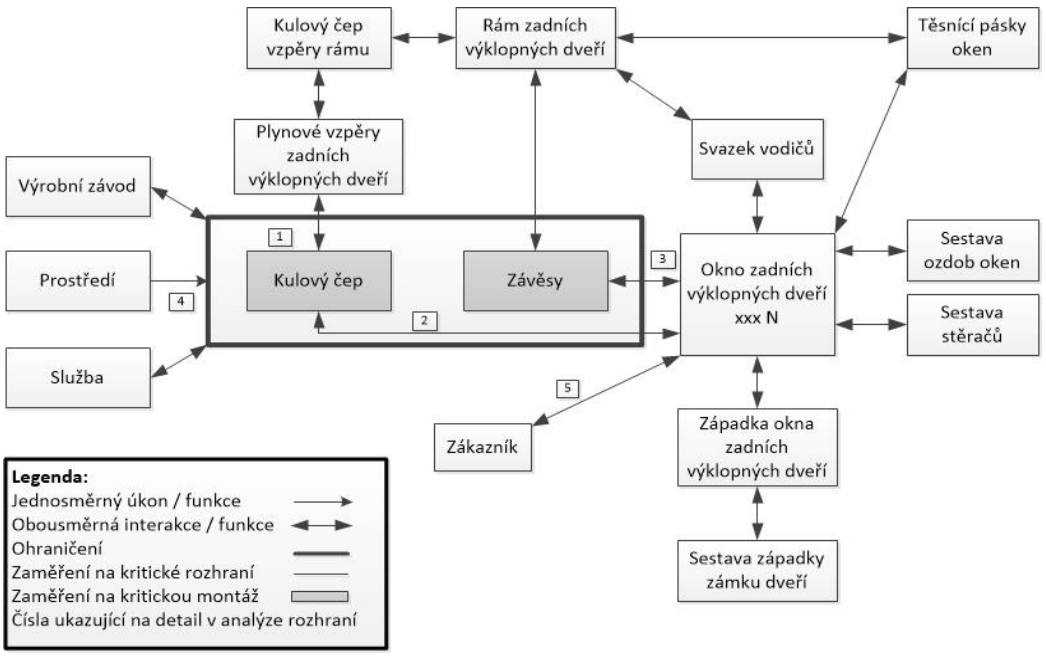
Jak již bylo řečeno, před vypracováním analýzy DFMEA je potřeba vymezit hranice, které definují, jaká část bude zahrnuta a jaká naopak vyloučena. Používá se k tomu tzv. *Boundary diagram.* Dalším užitečným nástrojem je P-diagram. Jedná se o diagram parametrů a funkcí, které ovlivňují produkt. Vztahy mezi podsystémy, sestavami, součástmi produktu a prostředími lze přehledně zaznamenat pomocí matice vzájemných vztahů. Dále se jedná o analýzu stromu poruchových stavů (FTA), která je podrobněji popsána v kapitole 3 FTA analýza.

Boundary diagram

Boundary diagram, neboli blokový diagram pro vymezení hranic, je grafickým znázorněním fyzikálních a logických vztahů mezi komponenty produktu. Patří sem subsystémy, sestavy, podsestavy, součásti produktu a rozhraní se sousedními systémy a prostředími. Hraniční diagramy jsou nutným prostředkem při design FMEA, jelikož rozděluje analýzu na části, které souvisí s daným produktem a které nikoliv. Pro nastavení rozsahu analýzy je třeba zjistit co je součástí a co je vyloučeno. Diagramy mohou být konstruovány na libovolnou úroveň detailů, je však důležité vždy identifikovat hlavní prvky, pochopit vzájemnou interakci a definovat jak se mohou prvky vzájemně ovlivňovat s vnějšími systémy. [2, 9]

V počáteční fázi návrhu může diagram obsahovat pouze několik bloků představujících hlavní funkce a jejich vzájemné vztahy na systémové úrovni. Poté, co je hotový design produktu, mohou být hraniční diagramy rozvíjeny na nižší úrovně detailů a to až na úrovně základních součástek. [2]

Na následujícím obrázku je jednoduchý boundary diagram znázorňující jednotlivé bloky reprezentující hlavní komponenty produktu nebo kroky procesu. Pro přehlednost provázanosti vzájemných vztahů mezi komponenty jsou bloky propojené čárami a šipky zde znázorňují vzájemné interakce.



Obrázek 2: Příklad blokového boundary diagramu. Převzato a upraveno z [9].

Matice rozhraní

Dalším užitečným nástrojem, který se používá jako vstup do analýzy DFMEA je matice rozhraní systému Znázorňuje vzájemné vztahy mezi podsystémy, sestavami, komponenty, a stejně tak i mezi rozhraními se sousedními systémy a prostředími. Matice ukazuje, která rozhraní musí být při analýze brána v úvahu. Rozhraní je bod nebo plocha, kde se setkávají dvě části nebo subsystémy a může mít i různé podoby. Existují čtyři základní typy rozhraní: fyzické propojení, výměna materiálu, přenos energie a výměna informace. Vzhledem k tomu, že na rozhraní se může vyskytovat až 50% nebo i více z celkových potenciálních poruch, je nezbytné, aby každá FMEA pečlivě zvážila rozhraní mezi subsystémy a komponenty.

Informace z matice systémového rozhraní poskytují cenné vstupy do design FMEA. Mezi tyto vstupy patří primární funkce či funkce rozhraní pro identifikaci funkce systému nebo účinky ze sousedních systémů, prostředí nebo člověka pro identifikaci selhání potenciálních příčin. Také poskytuje vstup do P-diagramu v sekci vstupních / výstupních a šumových faktorů. [2, 10]

Diagram parametrů (P-diagram)

P-diagram je strukturovaný grafický nástroj doporučený k identifikaci vstupů (signálů) a výstupů (funkcí) pro daný návrh produktu. Napomáhá týmu k pochopení fyzikální podstaty a správného fungování produktu. Nejdříve jsou vstupy a výstupy identifikovány pro určitou funkci, následně jsou určeny chybové stavy. Výkonost produktu ovlivňují také další faktory, které se dělí na řídící a šumové. Tento nástroj je nejužitečnější, pokud je analyzovaný produkt součástí komplexního systému s mnoha propojenými podsystémy, provozními podmínkami a konstrukčními parametry.

P-diagram tedy popisuje vlivy, které mohou způsobit poruchu či vadu (v českém překladu tzv. *šumové faktory*), dále řídící faktory, ideální funkci, chybové stavy a pomáhá při identifikaci:

- potenciální příčiny selhání,
- režimů selhání,
- potenciálních následků selhání,
- aktuálního řízení,

- doporučených akcí. [2, 9, 10]

2.2.2 Zápis do pracovního listu

Pro každý typ analýzy FMEA se používá odlišný pracovní list, avšak základní princip je stejný. Pro design FMEA je pracovní list zobrazen na obrázku č. 3. V první řadě je třeba vyplnit záhlaví, které jednoznačně identifikuje zaměření analýzy a obsahuje informace související s vypracováním a řízením dokumentu. Mezi tyto informace patří:

- číslo FMEA,
- název a číslo systému, podsystému nebo komponentu,
- tým odpovědný za návrh,
- rok výroby modelu / rok,
- rozhodné datum,
- data vypracování,
- osoba, která zpracovala analýzu. [2, 9]

ANALÝZA MOŽNÝCH ZÁVAD A JEJICH NÁSLEDKŮ

(FMEA NÁVRHU)

FMEA číslo _____

Str.:_____ z _____

____ systém

____ podsystém

____ součást _____ Odpovědnost za návrh _____ Zpracoval _____

model/rok_____ Rozhodné datum _____ Datum zprac. (orig) _____(rev.)_____

Řešitelský tým _____

Prvek / Funkce	Způsob možné závady	Možný důsledek závady	Závažnost	Klasifikce	Možná příčina(y)/ mechanismus(y) závady	Výskyt	Stávající opatření - prevence - odhalení	Odhalitelnost	UPR	Doporučená opatření	Odpovídá & termín splnění	Výsledky opatření: Opatření splněno	Závažnost	Výskyt	Odhalitel.	UPR

Obrázek 3: Pracovní list určený pro design FMEA. [9]

Po vyplnění identifikačních informací v záhlaví pracovního listu lze přistoupit k samotné analýze. Vypracování analýzy DFMEA lze rozdělit do pěti primárních částí. Každá část má odlišný účel a odlišné zaměření. Analýza je dokončena po částech v různých časových úsecích v rámci časového plánu projektu, nikoliv všechny najednou. [2, 9, 10]

První část (kvalita)

- **Objekt/funkce**

  Popisuje se funkce objektu v technické terminologii tak, aby bylo jasné, co má objekt dělat. Pro jeden objekt může být více funkcí.

- **Požadavek**

  Tento sloupec se může přidat dodatečně v případě dalších požadavků na funkci od zákazníka nebo po diskuzi v týmu. Požadavek musí být měřitelný a měl by mít definované zkušební metody. Z důvodu lepší orientace je doporučeno zapisovat požadavky a funkce samostatně, jelikož se může vyskytnout více požadavků na jednu funkci.

- **Možný způsob poruchy**

  Do tohoto sloupce se vypíší všechny možné způsoby, které mohou ohrozit plnění funkce komponentu, subsystému nebo systému. Existují 4 typy poruchových stavů. Mezi ně patří ztráta funkce, částečná / nadměrná / degradovaná funkce v čase, neočekávaná funkce a střídavá funkce.

- **Možný důsledek poruchy**

  V tomto sloupci se zaznamenávají možné důsledky poruchy funkcí produktu z pohledu vnímání zákazníka.

- **Závažnost**

  Závažnost každého důsledku poruchy je posuzována na základě dopadu nebo nebezpeční pro koncového uživatele / zákazníka. Pořadí závažnosti je v rozmezí 1 až 10, kde vyšší hodnota znamená větší závažnost. Všechna kritéria pro posouzení závažnosti jsou uvedena v následující tabulce.

Tabulka 1: Kritéria hodnocení závažnosti analýzy DFMEA. [9]

Důsledek	**Kritéria:** **Závažnost důsledku ve vztahu k produktu** **(Důsledek ve vztahu k zákazníkovi)**	**Známka hodnocení**
Nesplnění bezpečnostních požadavků a/nebo požadavků předpisů	Možný způsob poruchy, který bez varování ovlivňuje bezpečný provoz vozidla a/nebo znamená nesoulad s právními předpisy.	10
	Možný způsob poruchy, který i s varováním ovlivňuje bezpečný provoz vozidla a/nebo znamená nesoulad s právními předpisy.	9
Ztráta nebo zhoršení primární funkce	Ztráta primární funkce (vozidlo je nepojízdné, neovlivňuje bezpečný provoz vozidla).	8
	Zhoršení primární funkce (vozidlo je pojízdné, avšak při sníženém výkonu).	7
Ztráta nebo zhoršení sekundární funkce	Ztráta sekundární funkce (vozidlo je pojízdné, ale funkce zajišťující pohodlí nejsou funkční).	6
	Zhoršení sekundární funkce (vozidlo je pojízdné, ale funkce zajišťující pohodlí jsou na nižší úrovni výkonu).	5
Nepříjemnost	Vzhled nebo hluk, vozidlo je pojízdné, objekt není ve shodě a všimla si toho většina zákazníků (>75%).	4
	Vzhled nebo hluk, vozidlo je pojízdné, objekt není ve shodě a všimlo si toho hodně zákazníků (50%).	3
	Vzhled nebo hluk, vozidlo je pojízdné, objekt není ve shodě a všimli si toho velmi nároční zákazníci (<25%).	2
Žádný důsledek	Žádný znatelný důsledek	1

- **Klasifikace**

  Tento sloupec může být použit pro klasifikace jakýchkoliv speciálních charakteristik produktu pro komponenty, subsystémy nebo systémy, které mohou vyžadovat dodatečné konstrukčních nebo procesní kontroly. Může se také použít pro označení možných poruch s vysokou prioritou pro lepší orientaci. Často se používají znaky *YC* pro závažnost poruchy 9 - 10 a znaky *YS* pro závažnost poruchy 5 - 8.

Druhá část (kvalita)

- **Možná příčina poruchy / mechanizmy selhání**

  Možné příčiny poruchy my měly být určeny na úrovni fyzikálních vlastností. Příčiny na úrovni komponentů mohou souviset s vlastnostmi materiálu, geometrií, rozměry, rozhraními s dalšími součástmi a dalšími energiemi, které by mohly zabránit správné funkci. Tyto příčiny mohou být odvozeny ze vstupních nástrojů (boundary diagram, p-diagram, matice rozhraní).

- **Nástroje řízení prevence**

  Prevence používaná týmem FMEA při plánování / dokončení návrhu pomáhá ke snížení pravděpodobnosti výskytu poruchy. Jako typické prevenční kontroly se používají ověřené konstrukční standardy, osvědčená technologie (s podobným zatížením) a podpůrné počítačové techniky zvané CAE (computer-aided engineering).

- **Výskyt**

  Výskyt je pravděpodobnost, že konkrétní příčina / způsob závady nastane v průběhu trvání projektu. Proti příčinám s vysokým výskytem mohou být určeny akce pro jejich nápravu, zejména u hodnocení s čísly 9 nebo 10.

Tabulka 2: Kritéria hodnocení výskytu poruchy v rámci FMEA.[9]

Pravděpodobnost poruchy	**Kritéria: výskyt příčiny – DFMEA (projektovaná doba života/ bezporuchovost objektu/vozidla)**	**Kritéria: výskyt příčiny – DFMEA (Počet případů na počet objektů/vozidel)**	**Klasifikace**
Velmi velká	Nová technologie/nový návrh produktu bez historie.	≥ 100 na tisíc ≥ 1 z 100	10
Velká	Porucha je v případě nového návrhu produktu, nového použití nebo změny při pracovním cyklu/ provozních podmínkách nevyhnutelná.	50 na tisíc 1 z 20	9
	Porucha je v případě nového návrhu produktu, nového použití nebo změny při pracovním cyklu/ provozních podmínkách pravděpodobná.	20 na tisíc 1 z 50	8
	Porucha je v případě nového návrhu produktu, nového použití nebo změny při pracovním cyklu/ provozních podmínkách nejistá.	10 na tisíc 1 ze 100	7
Střední	Časté poruchy spojované s podobnými návrhy nebo při simulaci a zkoušení návrhu produktu.	2 na tisíc 1 z 500	6
	Náhodné poruchy spojované s podobnými návrhy nebo při simulaci a zkoušení návrhu produktu.	0,5 na tisíc 1 z 2 000	5
	Ojedinělé poruchy spojované s podobnými návrhy nebo při simulaci a zkoušení návrhu produktu.	0,1 na tisíc 1 z 10 000	4
Malá	Pouze ojedinělé poruchy spojované s téměř identickým návrhem nebo při simulaci a zkoušení návrhu produktu.	0,01 na tisíc 1 z 100 000	3
	Žádné zjištěné poruchy spojované s téměř identickým návrhem nebo při simulaci a zkoušení návrhu produktu.	≤ 0,001 na tisíc 1 z 1 000 000	2
Velmi malá	Porucha je eliminována nástroji řízení prevence	Porucha je eliminována nástroji řízení prevence	1

Třetí část (kvalita)

- **Nástroje řízení pro stávající návrh produktu**

  Činnosti prováděné za účelem ověření bezpečnosti a účinnosti návrhu jsou umístěny ve sloupci nástroje řízení detekce. Zkoušky a hodnocení určené k prokázání způsobilosti jsou přizpůsobeny příčinám a poruchám označeným nejvyššími riziky. Existují dva typy ovládacích prvků / funkcí, které je třeba zvážit:

  a) Prevence: zabránění vzniku příčin / mechanizmů nebo způsobům / důsledkům poruchy nebo snížení jejich výskytu.

  b) Detekce: odhalení způsobu či mechanizmu nebo režimu selhání pomocí analytických nebo fyzikálních metod předtím, než je položka uvolněna do výroby.

- **Odhalení**

  Hodnocení detekce je přiřazeno ke každé zkoušce na základě typu zkušební / vyhodnocovací techniky s ohledem na dobu jejího provádění. Ideální je provádět testy (na velice rizikových objektech) co nejdříve v návrhu. Kritéria pro určení hodnoty detekce jsou uvedena v následující tabulce 7.

Tabulka 3: Kritéria pro hodnocení detekce v rámci design FMEA. [9]

Možnost detekce	**Kritéria: Pravděpodobnost odhalení nástrojem řízení návrhu produktu**	**Klasifikace**	**Pravděpodobnost odhalení**
Žádná možnost detekce	Žádná nástroj řízení stávajícího návrhu produktu; nelze odhalit nebo není analyzováno.	10	Téměř nemožná
V žádné etapě není pravděpodobná možnost detekce	Analýza návrhu produktu/nástroje řízení detekce mají slabou detekční způsobilost; virtuální analýza **není v korelaci** s očekávanými skutečnými provozními podmínkami	9	Velmi mizivá
Po zmrazení návrhu produktu a před zahájením (zkoušek)	Ověřování/validace produktu po zmrazení návrhu produktu a před zahájením zkoušení **vyhověl/ nevyhověl** (zkoušení subsystému nebo systému s přejímacími kritérii, např. jízda a jízdní vlastnosti, hodnocení expedice atd.).	8	Mizivá
	Ověřování/validace produktu po zmrazení návrhu produktu a před zahájením **zkoušek do poruchy** (zkoušení subsystému nebo systému až do výskytu poruchy, zkoušení iterací systému atd.).	7	Velmi malá
	Ověřování/validace produktu po zmrazení návrhu produktu a před zahájením zkoušek na **zhoršování vlastností** (zkoušení subsystému nebo systému až do výskytu poruchy, zkoušení iterací systému atd.).	6	Malá
Před zmrazením návrhu produktu	Validace produktu (zkoušení bezporuchovosti, vývojové nebo validační testy) před zmrazením návrhu produktu s využitím zkoušením **vyhověl/ nevyhověl** (např. přejímací kritéria pro výkonnost, funkční zkoušky atd.).	5	Střední
	Validace produktu (zkoušení bezporuchovosti, vývojové nebo validační testy) před zmrazením návrhu produktu s využitím **zkoušky do poruchy** (např. pokud nedojde k netěsnosti, deformaci, trhlinám atd.).	4	Středně velká
	Validace produktu (zkoušení bezporuchovosti, vývojové nebo validační testy) před zmrazením návrhu produktu s využitím zkoušek na **zhoršování vlastností** (např. datové trendy, hodnoty před/po atd.).	3	Velká
Virtuální analýza	Analýza návrhu produktu/nástroje řízení detekce mají silnou detekční způsobilost. Virtuální analýza je před zmrazením návrhu **produktu v pevném vztahu** se skutečnými nebo očekávanými podmínkami.	2	Velmi veliká
Detekci nelze použít; prevence poruchy	Příčina poruchy nebo způsob poruchy nemohou nastat, protože se jim ve velké míře předchází formou řešení návrhu produktu (např. osvědčené návrhové standardní podmínky atd.).	1	Téměř jistá

Čtvrtá část

- **Ukazatel priority rizika RPN (The Risk Priority Number)**
  Tento ukazatel byl zmíněn již dříve v kapitole FMECA. Jedná se o součin určených klasifikací závažnosti, výskytu a detekce. V analýze DFMEA se stejně jako u ostatních modifikací nedoporučuje provádět nápravná opatření pouze podle prahových hodnot RPN.
- **Doporučená opatření**
  Do tohoto sloupce se zapisují veškerá doporučená opatření pro redukci potenciálních způsobů poruch. Měla by být natolik podrobná, aby byla pochopitelná i pro ostatní techniky. Opatření souvisejí s nejvyššími hodnotami (9 nebo 10) u závažnosti, výskytu a detekce.
- **Odpovědná osoba a termín dokončení**
  Zadává se jméno osoby, odpovědné za realizaci doporučeného opatření, a datum naplánovaného dokončení. Datum se může nahradit milníkem, pokud na časové ose existuje vazba mezi datem a milníkem dokončení.

Pátá část (výsledky opatření)

- **Přijaté opatření a termín dokončení**
  Uvádí se přijaté opatření nebo odkaz na zkušební protokol, ve kterém se nacházejí výsledky nápravy. Analýza DFMEA by měla vézt k opatřením, která sníží hodnoty rizik na přijatelnou úroveň.
- **Přepočtená klasifikace RPN**
  Po provedení nápravných opatření se znovu klasifikuje závažnost, výskyt a detekce a spočítá hodnota priority rizika, které by mělo být nižní než původní. Přepočtené RPN může být stále příliš vysoké, v tomto případě je nutné zavést další nápravná opatření. Tato akce se poté opakuje, dokud není dosaženo přijatelného čísla priority rizika. [1, 2, 9, 10]

2.2.3 Výstupy DFMEA

Mnohé výstupy z design FMEA slouží jako vstupy do procesní FMEA, jedná se především o výsledky doporučených opatření proti vzniku či eliminaci poruch. Mezi výstupy DFMEA tedy patří:

- Seznam možných způsobů a příčin poruchy.
- Seznam potenciálních kritických charakteristik a / nebo významných charakteristik.
- Seznam doporučených akcí pro snížení závažnosti, odstranění příčin selhání produktu, snížení výskytu a zlepšení detekce.
- Zpětná vazba návrhových změn do konstrukční komise. [2]

3 FTA analýza

Analýza stromu poruchových stavů, anglicky Fault tree analysis (FTA), je deduktivní analytická metoda, která zkoumá příčiny vzniku nežádoucí vrcholové události. Strom poruchových stavů má logickou strukturu, která určuje vztahy mezi vrcholovou událostí a příčinami jeho vzniku. Cílem metody je určit všechny možné primární příčiny poruchy (vrcholové události) a to kvalitativní nebo kvantitativní metodou. Často se používá při analýze bezpečnosti, spolehlivosti, pohotovosti či udržitelnosti systémů. Metoda se využívá v mnoha oborech, mezi nejvýznamnější patří letecký a automobilový průmysl, jaderná energetika nebo chemický a farmaceutický průmysl. [5, 11]

3.1 Historie FTA analýzy

Tato metoda byla vytvořena v letech 1961-1962 H.A. Watsnem ze společnosti Bell Telephone Laboratories v souvislosti s vývojem bezpečnosti startovacího systému rakety Minuteman. Po prvním zveřejnění této metody v bezpečnostní studii rakety Minuteman I společnosti Boeing a AVCO rozšířili použití FTA analýzy na celý navazující projekt Minuteman II. Metoda se poměrně rychle rozšířila z kosmonautiky a letectví do dalších odvětví například do jaderné energetiky, zbrojního průmyslu a byly vyvinuty první výpočtové programy pro kvantitativní i kvalitativní vyhodnocení analýzy. Dále byla a stále je metoda využívána nejčastěji v technických oborech, kde také došlo k zavedení celé řady standardů, norem a referenčních příruček. První normou zabývající se FTA analýzou byla v roce 1990 IEC 1025 – Analýza stromu poruchových stavů, kterou vydala Mezinárodní elektrotechnická komise IEC. Obsahuje zkušenosti z praktického využití a principy tvorby analýzy včetně nástrojů pro vyhodnocení výsledků. V České Republice byla tato norma vydána v roce 1993. Nejnovější mezinárodní norma v českém překladu zabývající se pouze FTA analýzou, s označením ČSN EN 610125, byla vydána v roce 2007. Tato norma popisuje druhy FTA analýzy, postup jejich použití a kombinace s dalšími metodami, pro které je vhodným rozšířením, nebo metody sloužící k vyhodnocení FTA analýzy. [5, 11–13]

V současné době je FTA analýza využívaná v celé řadě odvětví, převládá však v technických oborech. Pro tvorbu této analýzy vzniklo a stále vzniká mnoho softwarových nástrojů, které značně zjednodušují praktické použití analýzy. [5, 11]

3.2 Cíle metody

FTA analýza může být aplikována samostatně nebo společně s dalšími metodami bezporuchovosti. Mezi hlavní cíle analýzy patří:

- identifikace příčin nebo jejich kombinací vedoucích k vrcholové události,
- posouzení konkrétního ukazatele spolehlivosti, zda splňuje stanovený požadavek,
- stanovení příčiny / příčiny poruchy, které nejvíce přispívají k pravděpodobnosti výskytu vrcholové události (poruchy),
- zlepšení bezporuchovosti systému pomocí analýzy a porovnání různých alternativ návrhu,
- ověření správnosti předpokladů jiných analýz bezporuchovosti či rizik (např. Markovova analýza, FMEA, atd..),
- identifikace možné příčiny / způsoby poruchy, jejich pravděpodobnost výskytu a zmírnit jejich následky,
- výpočet pravděpodobnosti výskytu primárních, mezilehlých a vrcholové události. [11]

3.3 Postup a struktura stromu poruchových stavů

Pro popis struktury stromu poruchových stavů je nejprve nutné uvést definice základních pojmů, které se v literatuře často liší. Definice použitá v této diplomové práci pochází přímo z normy ČSN EN 61025 - Analýza stromu poruchových stavů (FTA). [11]

Výstup (*outcome*) - výsledek děje nebo jiného vstupu či následek příčiny. Může jím být událost nebo stav.

Vrcholová událost (*top event*) - výstup kombinací všech vstupních událostí. Vrcholová událost je předmětem zájmu analýzy stromu poruchových stavů.

Konečná událost, finální událost (*final event*) - konečný výsledek kombinací všech vstupních, mezilehlých a základních událostí.

Vrcholový výstup (*top outcome*) - výstup zkoumaný sestavením stromu poruchových stavů.

Hradlo (*gate*) - značka, která se používá ke stanovení symbolické logické vazby mezi výstupní událostí a odpovídajícími vstupy.

Kritický řez, množina řezů (cut set) - skupina událostí, které by při současném výskytu způsobily výskyt vrcholové události.

Minimální kritický řez, minimální množina řezů (minimal set cut) - nejmenší množina událostí, které se musí vyskytnout, aby způsobily vrcholovou událost.

Událost (event) - výskyt určité podmínky, nebo určitého děje.

Základní událost (basic event) - událost nebo stav, kterou (který) nelze dále rozvíjet.

Primární událost (primary event) - událost, která se nachází na základní úrovni stromu poruchových stavů. Primární událost může znamenat základní událost.

Mezilehlá událost (intermediate event) - událost, která není ani vrcholovou událostí, ani primární událostí.

Nerozvíjená událost (undeveloped event) - událost, která nemá žádné vstupní události. Tato událost není v analýze rozvíjená, může být rozvíjená v jiné analýze, nebo chybějí podrobnější informace k jejímu dalšímu rozvinutí.

Jednobodová porucha (událost) (single point failure (event)) - poruchová událost, která, jestliže nastane, způsobí celkovou poruchu systému nebo sama sobě, bez ohledu na jiné události nebo jejich kombinace, způsobí vrcholovou nežádoucí událost (výstup).

Události se společnou příčinou (common cause events) - odlišné události v systému nebo ve stromu poruchových stavů, které mají stejnou příčinu svého výskytu.
Společná příčina (common cause) - příčina výskytu několika událostí.

Několikanásobná nebo opakovaná událost (replocated or repleated event) - událost, která je vstupem pro více než jednu událost na vyšší úrovni stromu poruchových stavů. [11]

3.3.1 Postup

Postup analýzy stromu poruchových stavů se dá rozdělit do čtyř základních částí:

- přípravná část (vymezení rozsahu analýzy, seznámení se s funkcemi zařízení a určení vrcholové události),
- tvorba stromu poruchových stavů,
- analýza logiky stromu poruchových stavů (kvalitativní, kvantitativní metoda),
- vyhodnocení analýzy. [5]

Přípravná část

Analýza stromu poruchových stavů začíná přípravnou částí. Analytik, nebo analytický tým nejprve shromáždí informace o fungování systému a jeho použití, aby jim dokonale porozuměl. Mezi nezbytné informace pro analýzu patří znalost konstrukčního uspořádání a popis systému, dále režimy provozu systému a údržba systému. Důležité je také vymezení hranic systému, aby bylo zřejmé, které části jsou zahrnuty a které jsou mimo rozsah. Tato analýza je často využívaná s dalšími metodami, proto mohou být použity také informace jimi získané. Například pro vymezení hranic je možné použít boundary diagram, pro pochopení funkce P-diagram. Všechny tyto informace poslouží týmu k jasnému vymezení vrcholové události a k nalezení všech možných příčin jejího výskytu. Vrcholová událost může být také bezporuchový stav, kde se stanovují podmínky pro realizaci požadované funkce. [5, 11]

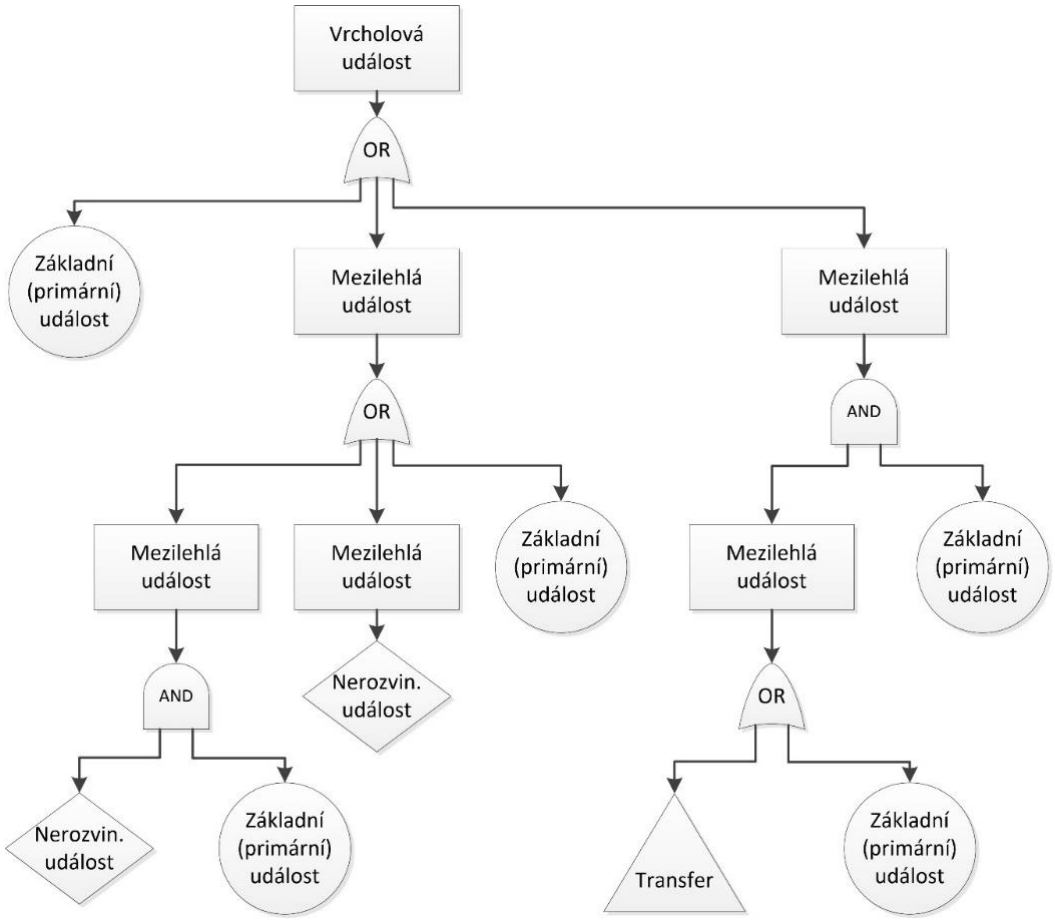
Tvorba stromu poruchových stavů

Dalším krokem je tvorba stromu poruchových stavů, používají se definované značky pro dané typy událostí a logických členů (hradel). Nejčastěji používané značky jsou uvedeny v tabulce 4. Analýza stromu poruchových stavů je deduktivní metoda, zkoumající příčiny výskytu vrcholové události shora dolů. Tvorba stromu poruchových stavů tedy začíná od vrcholové události a postupnou analýzou kauzálního vztahu se rozvíjí přes mezilehlé až k primárním událostem. Mezilehlé, primární či jiné události jsou identifikovány jako vstupy do vrcholové události a jejich kombinace je reprezentována vhodným hradlem. Všechny vstupy se dále systematicky rozvíjejí směrem dolů až k primárním událostem nebo k událostem, které jsou rozvinuty v jiné části analýzy či k nerozvinutým událostem. Příklad rozvinutého stromu poruchových stavů je zobrazen na obrázku 4. [5, 11]

Tabulka 4: Nejčastěji používané značky pro strom poruchových stavů.[11]

Symbol	Název	Popis
	Základní (primární) událost BASIC EVENT	Událost na nejnižší úrovni, po kterou jsou k dispozici pravděpodobnosti výskytu nebo informace o bezporuchovosti.
	Podmínková událost CONDITIONAL EVENT	Událost, která je podmínkou výskytu další události, když obě musejí nastat, aby nastal výstup

	Nerozvíjená událost UNDEVELOPED EVENT	Primární událost, která reprezentuje část systému, která doposud nebyla rozvíjena.
	Transfer TRANSFER	Hradlo naznačující, že je tato část systému rozvíjena v jiné části nebo na jiné straně diagramu.
	House event Přepínací událost	Událost, která je TRUE (pravdivá, zapnuto), nebo FALSE (nepravdivá, vypnuto). Může být částí stromu poruchových stavů, která je začleněna (ON) do analýzy, nebo je z ní vyloučena (OFF).
	Hradlo OR Logický součet OR	Výstupní událost nastane, jestliže nastane jakákoliv ze vstupních událostí.
	Hradlo MAJORITY VOTE Majoritní hradlo	Výstupní událost nastane, jestliže nastane m nebo více vstupních událostí z celkového počtu n vstupních událostí.
	Hradlo EXCLUSIVE OR Nonekvivalence, vzájemná výlučnost	Výstupní událost nastane, jestliže nastane jedna, ale ne jiná vstupní událost.
	Hradlo AND Logický součin	Výstupní událost nastane pouze tehdy, pokud nastanou všechny vstupní události.
	Hradlo priority AND (PAND) Prioritní logický součin	Výstupní událost (porucha) nastane pouze tehdy, jestliže nastanou vstupní události v pořadí zleva doprava.
	Hradlo INHIBIT Blokování	Výstupní události nastanou pouze tehdy, jestliže nastanou obě události, z nichž jedna je podmínková.
	Hradlo NOT Negace	Výstupní událost nastane pouze tehdy, jestliže nenastane vstupní událost.



Obrázek 4: Příklad rozvinutého stromu poruchových stavů.

Analýza logiky stromu poruchových stavů

Analýzu logiky stromu poruchových stavů lze realizovat dvěma metodami a to kvalitativní a kvantitativní.

Kvalitativní metoda

Tato metoda se nejčastěji používá v případech, kdy není možné přesně určit pravděpodobnost výskytu primárních událostí. Události se hodnotí subjektivně pomocí popisné pravděpodobnosti jako „vysoce pravděpodobná“, „velmi pravděpodobná“, „středně pravděpodobná“, velmi málo pravděpodobná“ a tak podobně. [11]

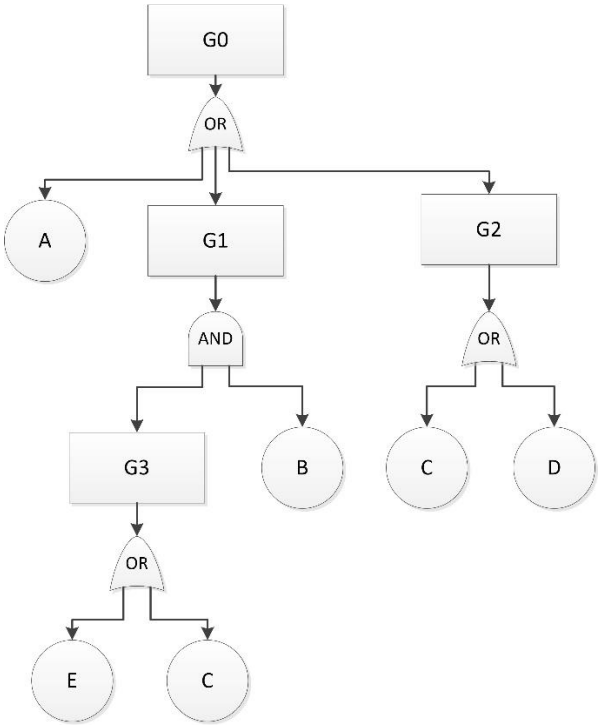
Cílem metody je nalézt všechny možné způsoby poruch, které by mohly vést k výskytu vrcholové události. K tomu metoda využívá tzv. ***kritické řezy***, pomocí nichž lze sestavit konečnou množinu primárních, dále nerozvíjejících a jinde analyzovaných událostí.

Současný výskyt těchto událostí vede ke vzniku vrcholové události. Pokud se jedná o konečnou množinu primárních událostí, která je sama kritickým řezem, ale současně žádná její vlastní podmnožina není kritickým řezem, jedná se o ***minimální kritický řez*** (MKR). [5, 14]

Metodu minimálního kritického řezu lze použít v případech, kde se stejná primární událost vyskytuje ve více větvích stromu poruchových stavů. Není možné ji však použít v případě závislosti vrcholové události na časování či posloupnosti jevů. [5, 14]

Princip metody spočívá v použití Booleovské redukce na rozvinutý strom poruchových stavů a jeho logických vazeb mezi jednotlivými událostmi. Nejdříve se vyjádří logická kombinace stavů, které bezprostředně způsobují vrcholovou událost. Dále postupujeme stejným způsobem na nižší úrovně, dokud není vrcholová událost vyjádřená pouze logickou kombinací primárních událostí. [5, 14]

Na následujícím příkladu je vysvětlen detailní postup. Obrázek 5 znázorňuje jednoduchý rozvinutý strom poruchových stavů, kde písmenem G_x je znázorněna vrcholová nebo mezilehlá událost a písmeny *A, B, C, D, E* jsou znázorněny primární události. Mezi nimi jsou uvedeny logické vazby *OR* (+) nebo *AND* (·).



Obrázek 5: Příklad stromu poruchových stavů pro kvalitativní metodu.

Metodu minimálního kritického řezu zahájíme vyjádřením logických stavů, které způsobují vrcholovou událost:

$$G_0 = A + G_1 + G_2 \tag{3}$$

Dále dosadíme za událost *G1* a *G2* logický výraz, který vyjadřuje logickou kombinaci jeho bezprostředních příčin:

$$G_0 = A + [G_3 \cdot B] + C + D \tag{4}$$

$$G_0 = A + [(E + C) \cdot B] + C + D \tag{5}$$

Tento vztah následně upravíme do podoby prostého sjednocení průniku jevů:

$$G_0 = A + B \cdot E + B \cdot C + C + D \tag{6}$$

Uvážíme-li podstatu sjednocení jevů, můžeme výraz zjednodušit následujícím způsobem:

$$B \cdot C + C = C \tag{7}$$

Výsledný výraz popisující rovnici minimálních řezů je:

$$G_0 = A + B \cdot E + C + D \tag{8}$$

Rovnici lze interpretovat jako soustavu čtyř minimálních kritických řezů:

$$\sum MKR = \{A\}, \{B \cdot E\}, \{C\}, \{D\} \tag{9}$$

Tento příklad postupu je velmi jednoduchý, lze jej aplikovat na jednoduché struktury stromu poruchových stavů, pro složitější a rozsáhlejší stromy se však stává velmi zdlouhavou a náročnou metodou. V těchto případech lze využít některý z výpočetních softwarů vyvinutých přímo pro potřeby výpočtů stromu poruchových stavů. [5, 14]

Kvantitativní metoda

Kvalitativní metodu výpočtu stromu poruchových stavů používáme v případech, kdy jsou známé pravděpodobnosti výskytu primárních událostí. Mezi hlavní cíle metody patří především pravděpodobnost, že nastane nežádoucí vrcholová událost v zadaném provozu systému. Velmi často se tato metoda kombinuje s dalšími statistickými metodami výpočtů, kterých je celá řada. Mezi nejpoužívanější však patří tyto dvě metody:

- metoda přímého výpočtu,
- metoda minimálních kritických řezů. [5, 11, 14]

Metoda minimálních kritických řezů pro výpočet kvantitativní metody je analogií MKR pro kvalitativní metodu výpočtu FTA analýzy, proto zde nebude dále uvedena.

Metoda přímého výpočtu se používá pouze v případech, kdy se primární událost vyskytuje pouze jednou. Postup výpočtu se zahájí od nejnižší úrovně stromu poruchových stavů, tedy od primárních událostí, a s pomocí vztahů pro hradlo OR a pro hradlo AND, se určují postupně pravděpodobnosti výskytu všech mezilehlých událostí až k vrcholové události. Tento výpočet lze použít pouze pro jednoduché stromy poruchových stavů, pro složitější a obsáhlejší stromy poruchových stavů je nutné použít některý z výpočetních softwarových nástrojů. [5, 11]

Vztah pro výpočet pravděpodobnosti výskytu nežádoucí události reprezentované hradlem OR lze vyjádřit dvěma způsoby:

$$F(t) = 1 - \prod_{i=1}^{n} [1 - F_i(t)] \tag{10}$$

nebo

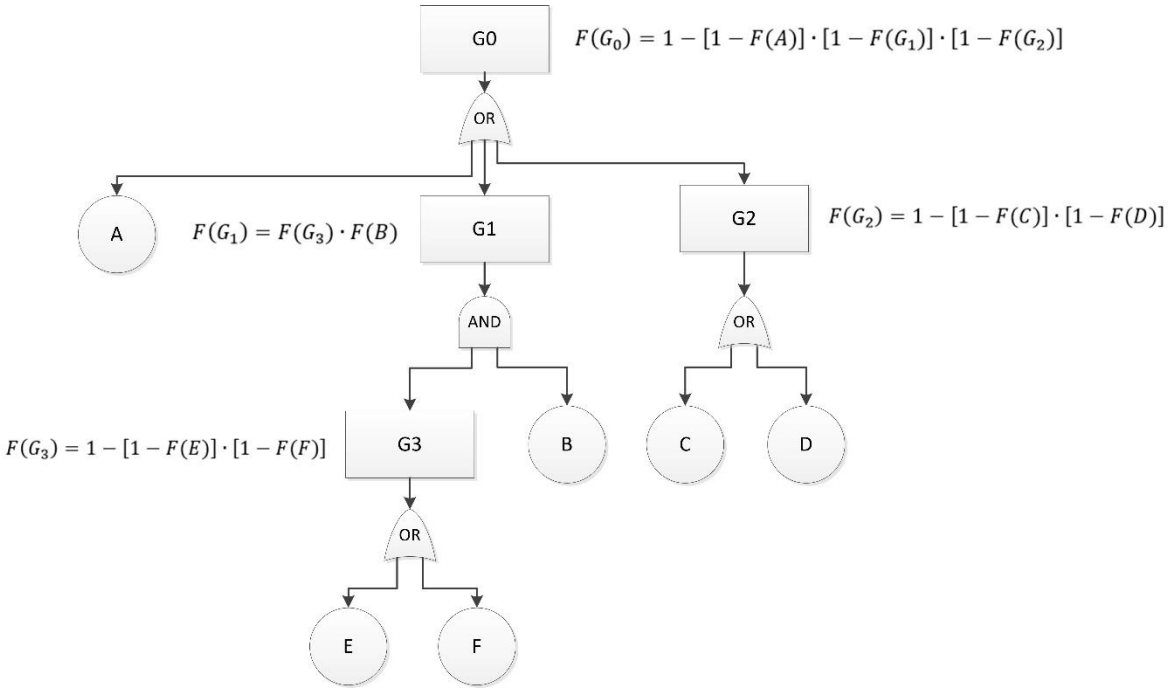
$$F_s(t) = 1 - [1 - F_1(t)] \cdot [1 - F_2(t)] \cdot [1 - F_3(t)] \cdot \ldots [1 - F_n(t)] \tag{11}$$

Vztah pro výpočet pravděpodobnosti výskytu nežádoucí události reprezentované hradlem AND lze vyjádřit jako:

$$F(t) = \prod_{i=1}^{n} F(t) \tag{12}$$

Použité vzorce (10) a (12) byly převzaty z [5] a vzorec (11) byl převzat z normy [11].

Ukázka řešení stromu poruchových stavů pomocí metody přímého výpočtu je zobrazena na obrázku 6.



Obrázek 6. Příklad výpočtu stromu poruchových stavů metodou přímého výpočtu.

Vyhodnocení FTA analýzy

Vyhodnocení může být logické (kvalitativní), číselné (kvantitativní), nebo obojí. Vhodným prostředkem vyhodnocení je zpráva o analýze FTA, která by měla obsahovat následující body:

- předmět a cíl analýzy,
- technickou dokumentaci, která byla při analýze použita,
- popis funkcí a konstrukce komponentů systému včetně vymezení hranic,
- provozní režimy systému,
- jednoznačnou definici vrcholové události či událostí,
- kompletní strom poruchových stavů,
- výsledky kvalitativní a kvantitativní analýzy (v závislosti na zvolené metodě),
- vyhodnocení analýzy včetně návrhů na změnu konstrukce a podmínek provozu či prostředí. [5, 11]

4 Návaznost analýz FMEA a FTA

Kombinace analýzy FMEA a FTA se velmi často doporučuje především kvůli odlišnému přístupu obou metod. FMEA je metoda „zdola nahoru“, která zkoumá režimy selhání komponentů v rámci systému a sleduje potenciální účinky každého selhání jednotlivých komponentů na systém, jedná se o model *příčina - následek*. FTA je metoda „shora dolů“, která identifikuje podmínky (včetně selhání součástí) vedoucí k definované vrcholové události (následek). V tomto případě se tedy jedná o model *následek – příčina*. FTA analýza umožňuje grafické znázornění logické návaznosti jednotlivých událostí, zatímco analýza FMEA zaznamenává systémové účinky každé příčiny v tabulkové podobě. Kombinace těchto dvou metod zvyšuje robustnost systému a odhalení všech příčin, které by mohly narušit jeho funkčnost, nebo v případě návrhu produktu by ohrozili funkčnost produktu. [11, 15, 16]

4.1 Postup

Postup při použití obou analýz se v literatuře často liší a existuje tak více způsobů, jak analýzy kombinovat:

- provádět samostatně FMEA i FTA analýzu,
- použít smíšený přístup,
    - nejdříve vypracovat analýzu FMEA a poté ji rozšířit o analýzu FTA,
    - nejdříve použít analýzu FTA a poté rozšířit o analýzu FMEA. [11, 16]

V diplomové práci se zaměřuji na poslední uváděný způsob kombinace analýz vzhledem k návaznosti na praktickou část.

Prvním krokem v tomto modelu je vymezení hranic analýzy, funkcí a vrcholové události. Poté vytvoření stromu poruchových stavů viz kapitola 3 FTA analýza. Vzhledem k rozsáhlosti stromu poruchových stavů se doporučuje použití některého ze softwarových nástrojů, jelikož tato analýza by poté byla časově velmi náročná. Po vytvoření stromu poruchových stavů je možné zapsat stavy / události do pracovního listu FMEA, kde jsou dále analyzovány. Pro analýzu se použijí historická data o výskytu a detekci příčin. Po provedení předběžné FMEA by měl být strom poruchových stavů revidován prostřednictvím výsledků z analýzy FMEA. Do stromu poruchových stavů lze také přidat nové primární události, které pravděpodobně nastanou. Poté se stanoví minimální kritické řezy MKR

a číselná analýza pravděpodobnosti výskytu jednotlivých událostí. Po výpočtu pravděpodobnosti výskytu se provádí analýza důležitosti výskytu událostí. Konečným krokem analýzy je dokončení zbytku FMEA pro nejkritičtější příčiny. [17]

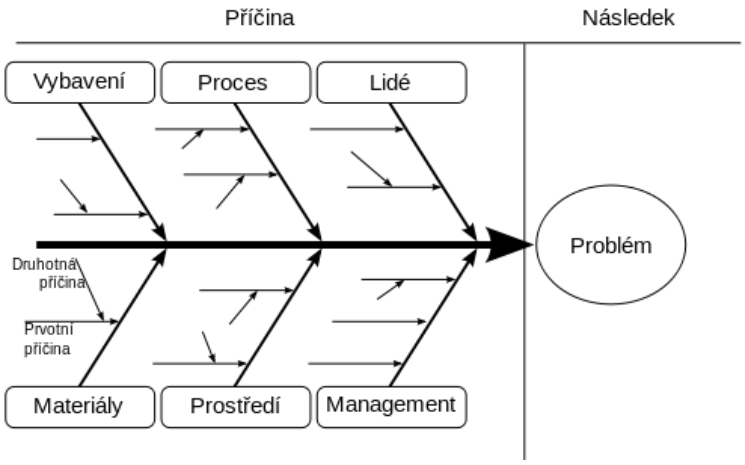
Jak již bylo řečeno ke zdokonalení metod samotných a zejména jejich kombinací přispívají především softwarové nástroje, které celý proces zaznamenávají, automaticky analyzují a umožňují rychlou kontrolu a úpravu dat. [17]

5 Další metody pro analýzu rizik

Metod, které analyzují a řídí rizika je celá řada. Kromě nejpoužívanějších metod FMEA a FTA, se používají další metody orientovaných stromů událostí, metody grafů a blokových diagramů bezporuchovosti či doplňující statistické metody. [18]

5.1 Ishikawův diagram

Nejjednodušším nástrojem pro analýzu rizik je *Ishikawův diagram,* pro jeho vzhled zvaný také *rybí kost*. Patří k týmovým technikám, proto je vhodné při tvorbě diagramu použít brainstorming. Každý následek má svojí příčinu, nebo kombinaci příčin, z této kauzality vychází základní princip. Cílem metody je nalezení nejpravděpodobnější příčiny řešeného problému. Při tvorbě diagramu se začíná definováním problému, který představuje hlavu. Dále se vytvoří páteř s kostmi, které tvoří hledané příčiny rozdělené do kategorií (materiál, procesy, metody, technologie, stroje, lidé, prostředí). Po nalezení všech možných příčin se ohodnotí ty nejvýznamnější a navrhnou se nápravná opatření. [18]



Obrázek 7: Ishikawa diagram. [19]

5.2 ETA (Event Tree Analysis)

ETA, v českém překladu analýza stromu událostí, patří mezi orientované stromy událostí. Princip je podobný jako u FTA analýzy, rozdíl je však v tom, že se sledují události vedoucí k poruše, ne pouze selhání, jako v případě FTA analýzy. Pomocí grafického logického modelu se zobrazují sekvence činností a událostí v procesu vedoucí k nehodě. Používá se pro identifikaci a analýzu systémových, projektových a procesních slabých míst. Uplatnění nachází v různých odvětvích průmyslu, od letectví, chemického zpracování, automobilového průmyslu až po obranný průmysl a dopravní systémy. Na rozdíl od jiných technik spolehlivosti je ETA založená na relativně elementárních matematických principech. Velmi často je analýza ETA kombinována s FTA analýzou, tato kombinace se někdy nazývá analýza příčin a následků (CCA – Cause-Consequence Analysis). [11, 20]

5.3 HAZOP (Hazard and Operability Study)

Analýza rizik a provozuschopnosti (HAZOP) je týmová, strukturovaná a systematická technika pro systémovou kontrolu a řízení rizik. Metoda je založena na teorii, která předpokládá, že rizikové události jsou způsobeny odchylkami od designu nebo provozních záměrů. Identifikace je usnadněna použitím „vodících slov“ jako systematického seznamu odchylek. Tento přístup je unikátní vlastností metody HAZOP, která pomáhá stimulovat představivost členů týmu při zkoumání možných odchylek. Umožňuje identifikovat nebezpečné stavy, které se mohou na zkoumaném zařízení vyskytnout, hledá kritická místa a následně vyhodnocují potenciální rizika. Pro nejrizikovější stavy se následně navrhují opatření na jejich eliminaci. Používaná je zejména jako technika pro identifikaci problémů s provozem, které mohou vést k nekonformním výrobkům. [21]

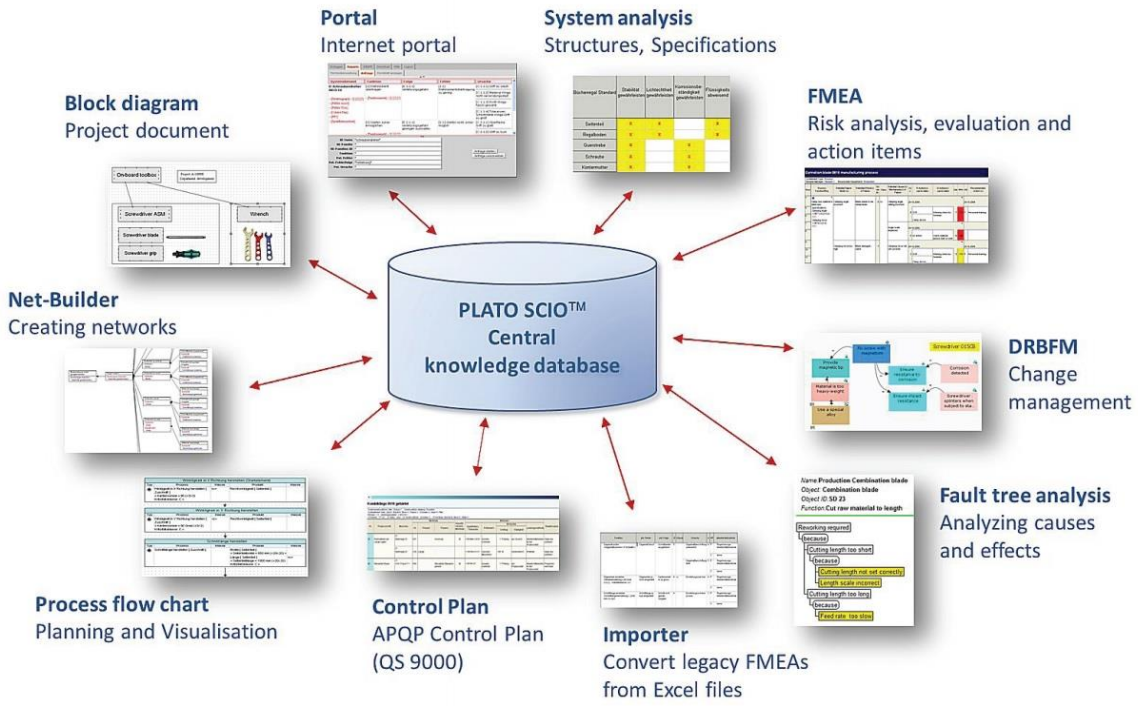
6 Software pro analýzu rizik

Softwarových nástrojů pro různé typy anýzy rizik je na trhu celá řada, většina z nich se však zaměřuje čistě na FTA analýzu, nebo na analýzu FMEA a celý managment rizik. Jedním takovým komplexním softwarem, který se zaměřuje na systém řízení kvality a rizik s ním spojený je například *PlastatCAQ*. Tento software však neobsahuje modul pro FTA analýzu, proto se jím zde dále nebudeme zabývat. Zajímavé softwarové nástroje, které dokáží propojit data z FTA a FMEA analýz jsou například *PLATO AG* nebo *RISK SPECTRUM*.

6.1 PLATO AG

Společnost PLATO AG poskytuje firmám podporu pro vývoj produktů a procesů od roku 1992. Software nabízí řešení pro inženýrství a dodržování stanovených předpisů pomocí datové koncepce zahrnující všechny fáze od analýzy požadavků až po výrobu. *PLATO SCIO*^{TM} je produktová řada s praktickými moduly, které splňují širokou škálu požadavků a provádějí řadu technických úkolů. V oblasti inženýrství poskytuje software podporu pro celý vývojový proces, počínaje požadavkem zákazníka a specifikací pro analýzu rizik a opatřeními vyplývajícími z analýzy. [22]

Hlavní předností tohoto softwarového nástroje je centrální databáze, která je sdílená se všemi moduly a umožňuje tak efektivní řízení znalostí a schopnost jejich opětovného využití. Například při vytváření analýzy rizik pomocí FTA a FMEA je databáze neustále aktualizována a vytvořená událost v jedné analýze je automaticky přenesena do té druhé. Podporuje celou řadu standardů (QS 9000, IATF 16949:2016, VDA, HACCP a další), díky tomu jej lze použít přesně podle specifikací zákazníka a snadno také sdílet potřebná data. [22]

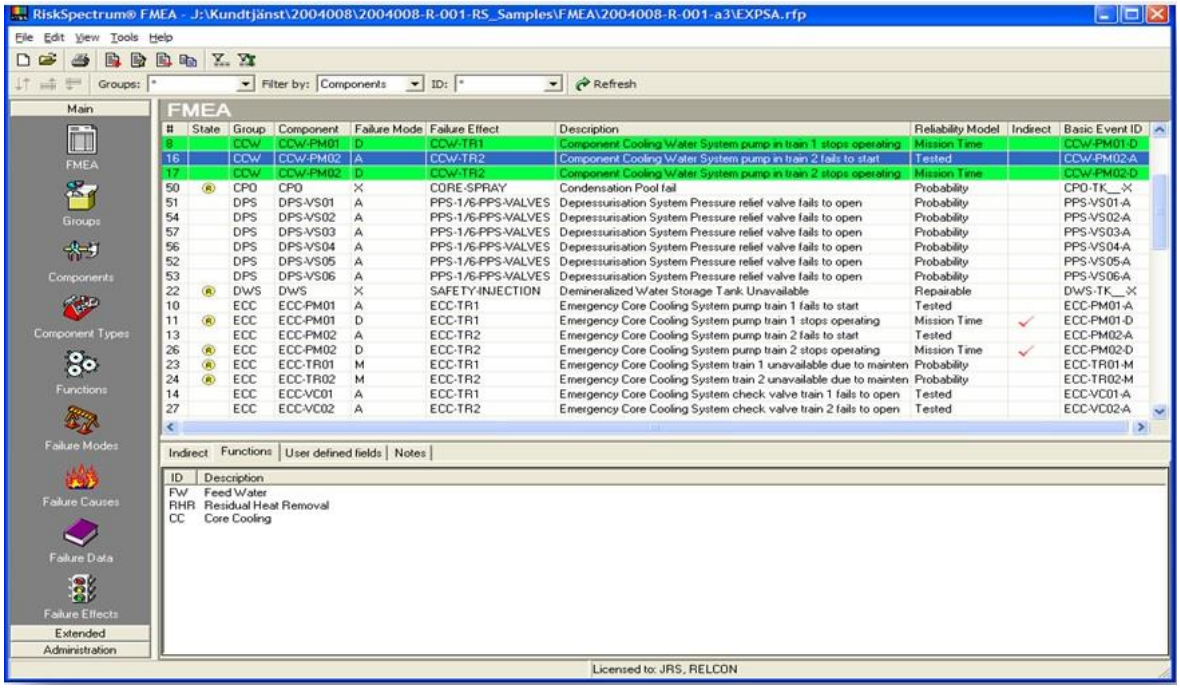


Obrázek 8: Ukázka rozčlenění systémových modulů a uchování informací v softwaru PLATO SCIO^{TM}*. Převzato z [22].*

6.2 RiskSpectrum

Software RiskSpectrum byl vytvořen, nadále udržován a podporován společností Lloyd's Register Consulting. Je to komplexní software pro analýzu rizik a spolehlivosti využívaný především v jaderném, obraném a dopravním průmyslu. Obsahuje nástroje pro modelování a analýzu stromů chyb, dokumentaci, sledování rizik, hodnocení spolehlivosti a selhání. [23]

Pokud se zaměříme pouze na analýzy FMEA a FTA, nabízí software přímé propojení mezi těmito metodami. Vychází z podrobné a přesné identifikace událostí v analýze FMEA, ty poté automaticky generuje společně s jejich parametry do analýzy FTA. Generace událostí je možná taktéž v opačném směru, tedy z FTA do FMEA. Informace o jednotlivých primárních událostech, se kterými software pracuje, jsou na sobě nezávislé, to umožňuje uživateli s těmito daty pracovat i v dalších modulech pro analýzu rizik a spolehlivosti. [23]



Obrázek 9: Ukázka zápisu dat do modulu FMEA softwarového nástroje RiskSpectrum. Převzato z [24].

7 Praktická část

Praktická část diplomové práce byla vytvořena ve spolupráci s konzultantem společnosti WITTE Nejdek, spol. s.r.o. (dále jen WITTE Nejdek) panem Ing. Vladimírem Votápkem. V této části bude popsána analýza design FMEA s podporou analýzy stromu poruchových stavů (FTA) pro konkrétní produkt společnosti WITTE Nejdek. Dále zde budou použity pomocné metody boundary diagram, P-diagram a matice rozhraní, které byly popsány v teoretické části.

7.1 Profil společnosti WITTE Automotive

Společnost WITTE Automotive vznikla před více než sto lety a zabývá se zamykacími a ovládacími systémy v automobilovém průmyslu. WITTE Nejdek spadá pod WITTE Automotive Česká Republika. Název WITTE Automotive je společným označením závodů v Bulharsku, České Republice, Francii a Německu, avšak v celosvětovém měřítku působí v rámci aliance VAST v Asii, Jižní a Severní Americe. Produkty této společnosti se nacházejí téměř ve všech značkách automobilů. [25]

Obrázek 10: Areál společnosti WITTE Nejdek, spol. s.r.o. [25]

7.2 Současný stav

Automobilový průmysl podléhá vysokým nárokům na kvalitu a bezpečnost všech použitých komponentů. Z tohoto důvodu bylo zavedeno mnoho norem, standardů a referenčních příruček, které stanovují či doporučují správný postup při navrhování nových produktů, řízení výrobních procesů a managmentu kvality. Mezi ně patří například mezinárodní standard systému managmentu kvality pro automobilový průmysl IATF 16949. Mnoho ze standardů, norem a referenčních příruček obsahuje jako nedílnou součást analýzu FMEA, ostatní metody (jako FTA analýza) se doporučují, nebo jsou spíše doplňující pro větší robustnost celého systému.

Společnost WITTE Nejdek používá pro každý návrh produktu analýzu FMEA v softwaru PLATO-SCIO. Pro zcela nové produkty se začíná používat i FTA analýza, boundary diagram, P-diagram a matice rozhraní pro správné pochopení funkce. Není to však vždy podmínkou a tento proces je možné zjednodušit v rámci časového plánu. FTA analýza navíc není tvořená podle normy a jde spíše o částečnou vizualizaci způsobů poruch v programu Microsoft Visio. Společnost vyrábí často velmi podobné díly nebo se jedná o stejný díl s jinými specifikacemi (např. automobil určený pro trh v Rusku, nebo naopak pro Střední Afriku bude odolávat jiným teplotním či okolním vlivům). V takovýchto případech se nevytváří zcela nová analýza, ale využijí se zkušenosti z předešlé analýzy a modifikuje se pro nové specifikace.

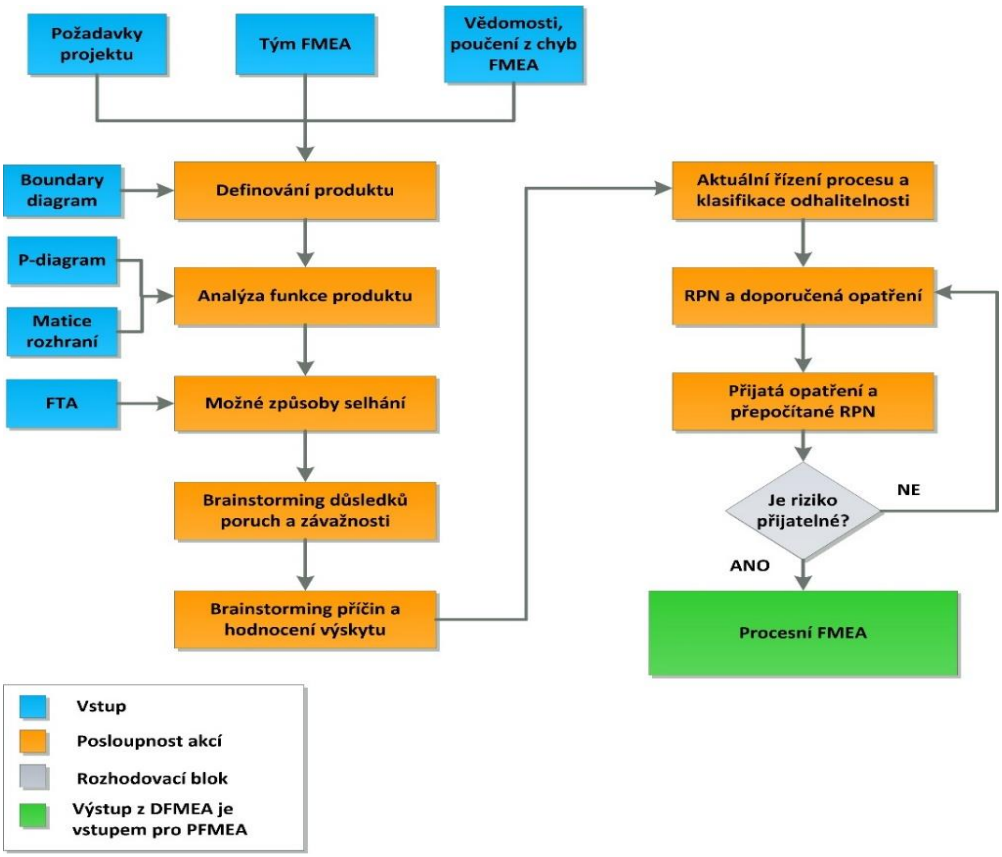
7.3 Postup při vypracování analýz DFMEA a FTA

Diplomová práce je orientovaná na návaznost nástrojů pro analýzu rizik se zaměřením na nástroje FMEA a FTA. Ve společnosti WITTE Nejdek se tyto analýzy standardně nepoužívají dohromady pro každý produkt, proto je praktická část věnovaná propojení všech těchto nástrojů a může dále sloužit jako šablona pro typově stejné, nebo podobné produkty.

Každá analýza začíná u zákazníka, který si určí požadované funkce a specifikace pro daný produkt. Na základě těchto informací od zákazníka se sestaví tým, který zahrnuje zástupce všech zainteresovaných oborů. Tyto informace se uvádějí do pracovního sešitu DFMEA. Následně je vytvořen boundary diagram (diagram rozhraní) pro stanovení rozsahu analýzy. Dalšími použitými nástroji jsou také P-diagram a matice rozhraní. Vypracování těchto pomocných metod umožňuje týmu DFMEA si udělat ucelený přehled o veškerých možných okolních vlivech, fyzikálních funkcích i vzájemných interakcích jednotlivých dílů.

Nyní má tým DFMEA dostatek informací pro sestavení stromu poruchových stavů (FTA), kde se uvedou všechny možné poruchy a hledají se jejich příčiny, tzv. primární události, pro které se určí pravděpodobnosti výskytu, následně i pravděpodobnost výskytu mezilehlých událostí a vrcholové události. Tyto poruchové stavy a jejich příčiny jsou vstupními informacemi do DFMEA. Přiřazují se jim podle tabulek klasifikace závažnosti, výskytu a možnosti detekce. Následně se tyto hodnoty násobí a výsledkem je číslo priority rizika (RPN). Pro každý poruchový stav se stanoví doporučená opatření, zvolí se ta nejvhodnější a poté se přepočítá nový výsledek RPN. Pokud tato hodnota stále není přípustná, musí se stanovit další opatření a opět se přepočítá nové RPN. Tento proces se opakuje, dokud riziko neklesne na přijatelnou úroveň.

Následující obrázek graficky znázorňuje postup při sestavování analýzy DFMEA, který byl aplikován. Jsou zde uvedeny vstupy do jednotlivých částí projektu a posloupnost akcí. Výsledek analýzy je dále vstupním faktorem pro procesní FMEA, ta však není předmětem praktické části této diplomové práce, proto není dále rozvedena.

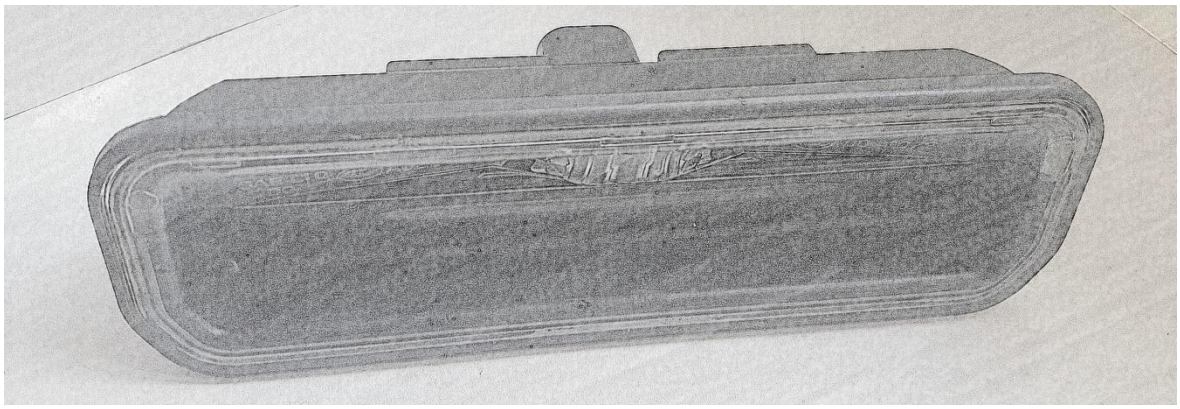


Obrázek 11: Postup při sestavování analýzy Design FMEA. [2, 10]

7.4 Aplikace analýzy na konkrétní produkt WITTE Nejdek

Pro vypracování diplomové práce byla zvolena klika zadních dveří s osvětlením plochy státní poznávací značky (dále jen SPZ). Klika je určena pro typ automobilu „hatchback“ jistého modelu vozu jisté výrobní značky. Hlavní funkcí tohoto produktu je vyslat signál pro otevření dveří zavazadlového prostoru a zároveň osvítit plochu SPZ. Na následujícím obrázku je znázorněn daný produkt, který se skládá z několika součástí:

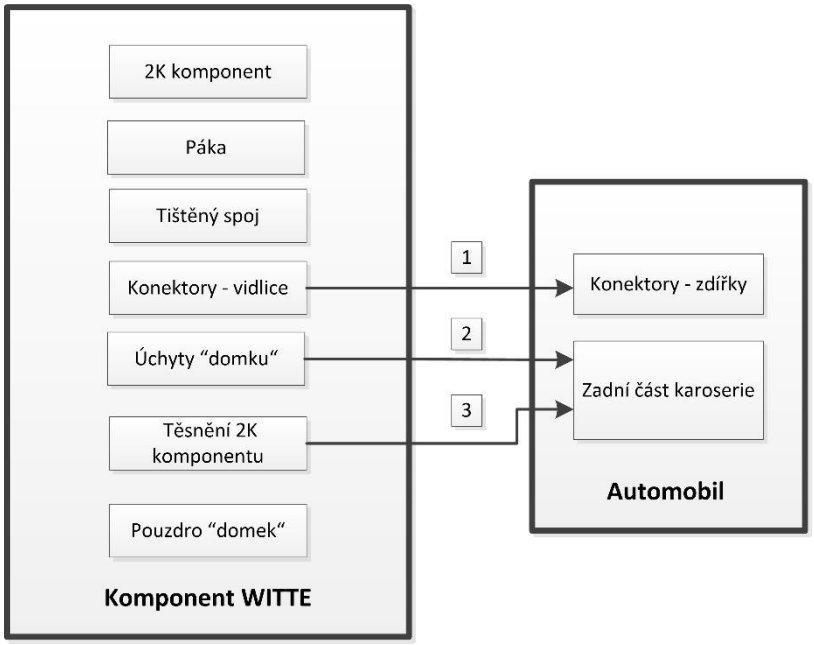
- 2K komponent (horní dvousložkový díl – měkká část určená k přenosu mechanické síly od iniciace rukou na páku a Fresnelova čočka),
- páka,
- tištěný spoj,
- konektory,
- pouzdro (dále jen “domek“).



Obrázek 12: Klika zadních dveří s osvětlením plochy SPZ.

7.4.1 Boundary diagram

Na následujícím obrázku je zpracován blokový diagram, pro znázornění interakce komponentů s okolním prostředím. Pomůže týmu přehledně zobrazit součásti produktu a hranice pro vypracování DFMEA. Je zde uveden na levé straně komponent WITTE, který obsahuje níže popsané součásti, a na pravé straně jsou uvedeny součásti automobilu, které jsou s tímto komponentem spojeny. Zde je důležité si povšimnout, že interakce mezi díly na rozhraní je pouze ve třech případech, ostatní díly jsou uvnitř komponentu. Čísla 1, 2 a 3 odkazují na přiloženou tabulku, ve které se uvádí charakter příslušné akce mezi předměty a požadavky na rozhraní předmětů.



Obrázek 13: Boundary diagram pro kliku zadních dveří WITTE.

Tabulka 5:Popis akcí a požadavků na rozhraní pro kliku zadních dveří WITTE.

Označení	Název / předmět akce	Požadavek na rozhraní
1	Zasunutí konektoru - zdířky (automobil) do konektoru - vidlice (komponent WITTE)	rozměry
		čistota
		přítlačná síla F (kontakty)
2	Nacvaknutí úchytů "domku" (komponent WITTE) do zadní části karoserie (automobil)	rozměry
		síla F (uchycení)
		umístění
3	Přilnutí těsnění 2K komponentu (komponent WITTE) na zádní část karoserie (automobil)	umístění
		nezdeformování těsnění
		těsnící funkce

7.4.2 P-diagram

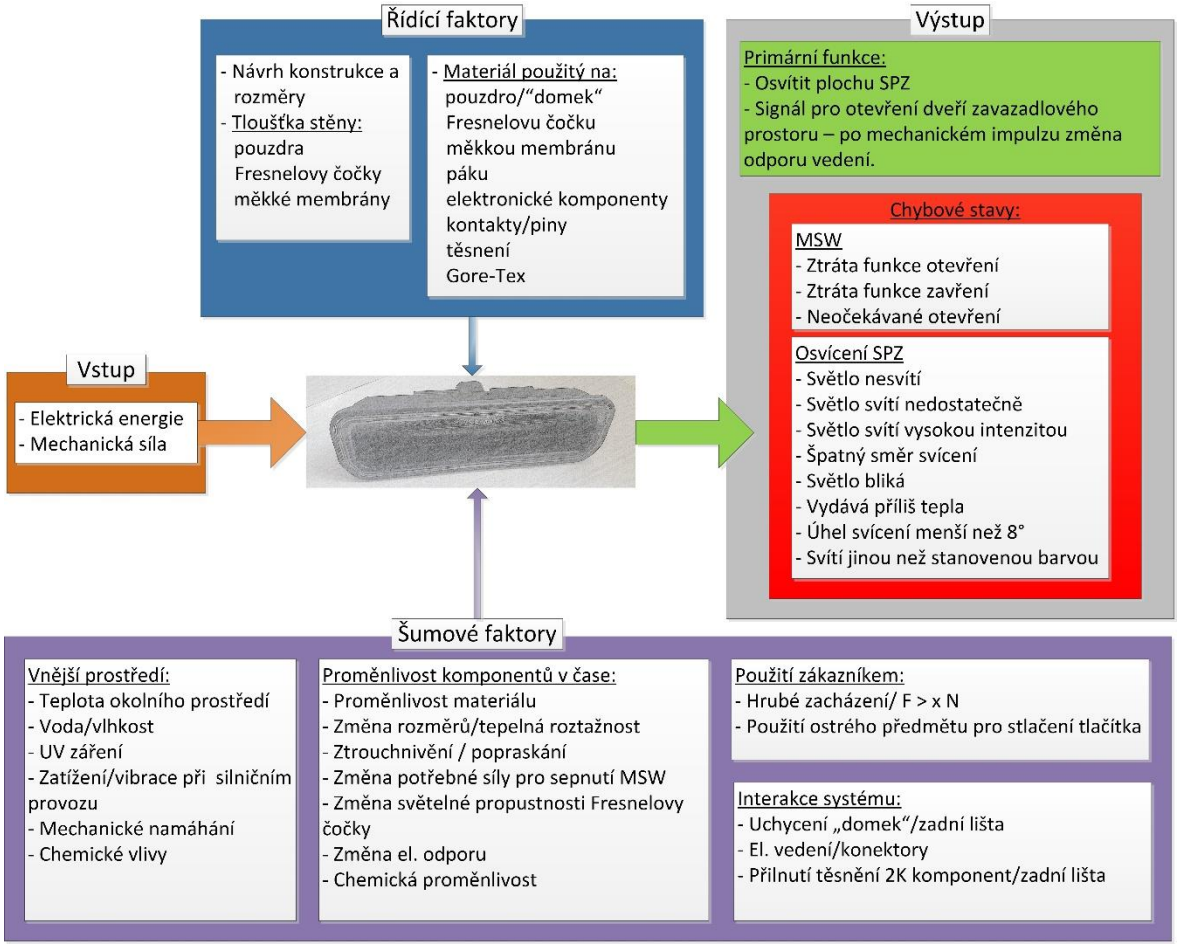
Diagram parametrů je pro tým důležitý především pro přehledné znázornění faktorů, které ovlivňují produkt mezi vstupními a výstupními parametry či funkcemi.

V první řadě se určí vstupní a výstupní parametry či funkce. Vstupujícími parametry pro tuto kliku je elektrický signál z řídící jednotky (napětí 12V pro diodu) a mechanická síla potřebná pro stlačení tlačítka od uživatele. Hlavním vystupujícím faktorem jsou stanovené funkce tlačítka zákazníkem. V tomto případě se jedná o funkci osvítit plochu SPZ v rámci normy ECE-R4 a otevřít dveře zavazadlového prostoru, tedy vyslat signál po stlačení tlačítka pomocí změny odporu vedení. Výstupní funkce může být také nežádoucí chybový stav, který je nutné eliminovat. Zde je tabulka rozdělena na dvě části. První se vztahuje k MSW (microswitch), pro který jsou nežádoucími chybovými stavy ztráta funkce otevření, ztráta funkce zavření a neočekávané otevření. Druhá tabulka se vztahuje k funkci osvítit plochu SPZ, která musí být v souladu s normou ECE-R4, pokud nejsou specifikace dodrženy, jedná se o chybový stav. Výčet specifikací je uveden na obrázku 14. [26]

Faktory, které ovlivňujeme, neboli řídíme, rozhodují o správné funkci zařízení. Pro kliku zadních dveří se jedná o správný návrh konstrukce a rozměry všech komponentů, dále tloušťky stěn pro odolání vnějšímu prostředí či dostatečnou pružnost membrány a také použití správných materiálů pro všechny komponenty.

Vlivy, které mohou způsobit poruchu či vadu, tzv. šumové faktory, působí na produkt a ovlivňují jej, proto je nutné o rizicích všech těchto faktorů vědět a uzpůsobit produkt tak, aby jim byl schopen odolat. Jsou rozděleny do čtyř skupin. První skupinou je ovlivnění produktu působením vnějšího prostředí, druhou je proměnlivost použitých komponentů v čase, dále neobvyklé použití zákazníkem a poslední skupinou je interakce systému, která navazuje na boundary diagram.

Kompletní P-diagram je zobrazen na následujícím obrázku. Společně s maticí rozhraní a boundary diagramem vytváří robustní systém pro analýzu funkcí, která je potřebná pro určení chybových stavů v FTA analýze.



Obrázek 14: P-diagram pro kliku zadních dveří WITTE

7.4.3 Matice rozhraní

Matice rozhraní byla v diplomové práci pojata poněkud netradičně pro vzájemnou interakci jednotlivých součástek uvnitř komponentu, nikoliv jako vzájemnou interakci celého komponentu s okolím. Tento postup však tým umožňuje detailní náhled do vzájemného ovlivnění jednotlivých součástí jak v pozitivním, tak i v negativním smyslu.

Do tabulky se napisují všechny použité součásti tak, aby je bylo možné mezi sebou porovnat. Následně se určují čtyři možné vzájemné interakce, kterými jsou fyzický kontakt, přenos energie, přenos informace a materiálová výměna. Každá z nich se hodnotí v rozmezí od -2 do 2, kde -2 znamená interakci, které je pro správnou funkci potřeba zabránit a 2 je interakce nezbytná pro správnou funkci. Logika vyplňování tabulky je uvedena na následujícím příkladu interakce diody s plošným spojem.

2	2

- I. kvadrant se vztahuje k výměně energie - *E*. Je nutné, aby došlo k výměně elektrické energie mezi diodou a plošným spojem, proto je hodnota 2.

- II. kvadrant označuje fyzický kontakt - *P*. Pro správnou funkci je nutné, aby byla dioda pevně připájena k plošnému spoji, dochází zde tedy k fyzickému kontaktu, proto je hodnota 2.

- III. kvadrant se vztahuje k výměně informace - *I*. Plošný spoj nepřenáší diodě žádnou informaci, pouze přenáší elektrickou energii, proto je políčko prázdné, může se použít i 0.

- IV. kvadrant se vztahuje k materiálové výměně - *M*. Zde materiálová výměna nehraje roli, proto je políčko opět prázdné.

Tabulka 6: Matice rozhraní pro kliku zadních dveří společnosti WITTE.

Matice rozhraní	Domek (spodní část)		Fresnelova čočka		Plošný spoj		Dioda		MSW (microswitch)		Konektory		Páka		Těsnění (domek-horní část)		Softtouch	
Domek (spodní část)			2	1	2						2	-1	2	2	2		2	
																2		2
Fresnelova čočka	2	1				2		2				2			2		2	
																2		2
Plošný spoj	2			2			2	2	2	2	2	2	-1	-1				
									2		2							
Dioda				2	2	2						2						
									-1		2		-2					
MSW (microswitch)				2	2	2						2	2	2				2
			2		2		-1				2		2				2	
Konektory	2	-1		2	2	2		2		2								
					2		2		2								2	
Páka	2	2			-1	-1	-2		2	2							2	2
									2								2	-1
Těsnění (domek-softtouch)	2		2														2	
		2		2														
Softtouch	2		2							2			2	2	2			
		2		2					2		2		2	-1				

P	E
I	M

2	Interakce je nezbytná pro správnou funkci
1	Interakce je výhodou, není však nutná pro správnou funkci
0	Interakce neovlivní funkčnost
-1	Interakce způsobuje negativní účinky, ale nezabrání funkčnosti
-2	Pro správnou funkčnost musí být zabráněno interakci

7.4.4 FTA analýza

Po důkladné analýze pochopení správné funkce pomocí boundary diagramu, P-diagramu a matice rozhraní je možné přistoupit k dalšímu kroku a tím je analýza možných způsobů selhání pomocí FTA analýzy. Hlavní výhodou této metody je, že se jedná o deduktivní metodu, která zkoumá poruchy shora dolů od vrcholové k primární události. Při návrhu produktu je vhodné uvážit jakoukoliv poruchu, která by mohla vést k selhání funkce, bez ohledu na pravděpodobnost jejího výskytu. Důležité je znát riziko, že by taková porucha mohla vzniknout.

Analýzu zahájíme zvolením vrcholové události. V našem případě se bude jednat o více vrcholových událostí, jelikož klika zadních dveří WITTE má více funkcí. Budeme analyzovat vrcholové události „do poruchy“, proto budeme hledat možné způsoby poruch od vrcholové, přes mezilehlé až po primární události, které způsobují prvotní příčinu poruchy. Pro určení vztahu mezi událostmi se budou používat logické členy. Pro každou událost a logický člen budou použity definované značky převzaté z normy ČSN EN 61025 [11]. Po zjištění všech událostí se primárním událostem přiřadí pravděpodobnost výskytu poruchy podle tabulky 2 v kapitole DFMEA. Pro určení pravděpodobnosti, že nastane vrcholová událost, bude použita kvantitativní analýza. Budeme postupovat od primárních událostí směrem k vrcholové události přes logické členy OR (logický součet). Pro výpočet použijeme následující vzorec přímého výpočtu pravděpodobnosti poruchy systému skládajícího se z n nezávislých vstupních logických členů OR nebo událostí:

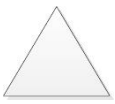
$$F_s(t) = 1 - [1 - F_1(t)] \cdot [1 - F_2(t)] \cdot [1 - F_3(t)] \cdot \dots [1 - F_n(t)] \tag{11}$$

Kde

$F_s(t)$ reprezentuje pravděpodobnost poruchy systému, v našem případě se bude jednat o pravděpodobnost výskytu nežádoucí vrcholové události.

$F_n(t)$ reprezentuje nezávislá vstupní hradla, primární události nebo nerozvinuté události v současné analýze FTA.

Tabulka 7: Použité symboly v FTA analýze.

Symbol	Název	Popis
	Základní (primární) událost	Událost na nejnižší úrovni, po kterou jsou k dispozici pravděpodobnosti výskytu nebo informace o bezporuchovosti.
	Nerozvíjená událost	Primární událost, která reprezentuje část systému, která doposud nebyla rozvíjena.
	Transfer	Hradlo naznačující, že je tato část systému rozvíjena v jiné části nebo na jiné straně diagramu.
	Logický součet OR	Výstupní událost nastane, jestliže nastane jakákoliv ze vstupních událostí.

Všechny možné chybové stavy jsou uvedeny v P-diagramu. Vzhledem k rozsáhlosti FTA analýzy bude pro vysvětlení postupu zvolena jen porucha osvícení SPZ, konkrétně „LED nesvítí / svítí nedostatečně“. Jedná se o stav, kdy LED dioda, připájená na plošném spoji, nesvítí nebo svítí nedostatečně pro homogenní osvícení plochy SPZ.

Na následujícím obrázku 15 je znázorněna část stromu poruchových stavů. Je zde zvolená vrcholová událost (LED nesvítí / svítí nedostatečně), která může být způsobena událostmi na nižších úrovních, kterými jsou:

- nevhodně zvolená dioda s nižší intenzitou svícení (primární událost),
- nedostatečné napětí nebo žádné napětí (mezilehlá událost),
- proud vyšší než stanovený (mezilehlá událost).

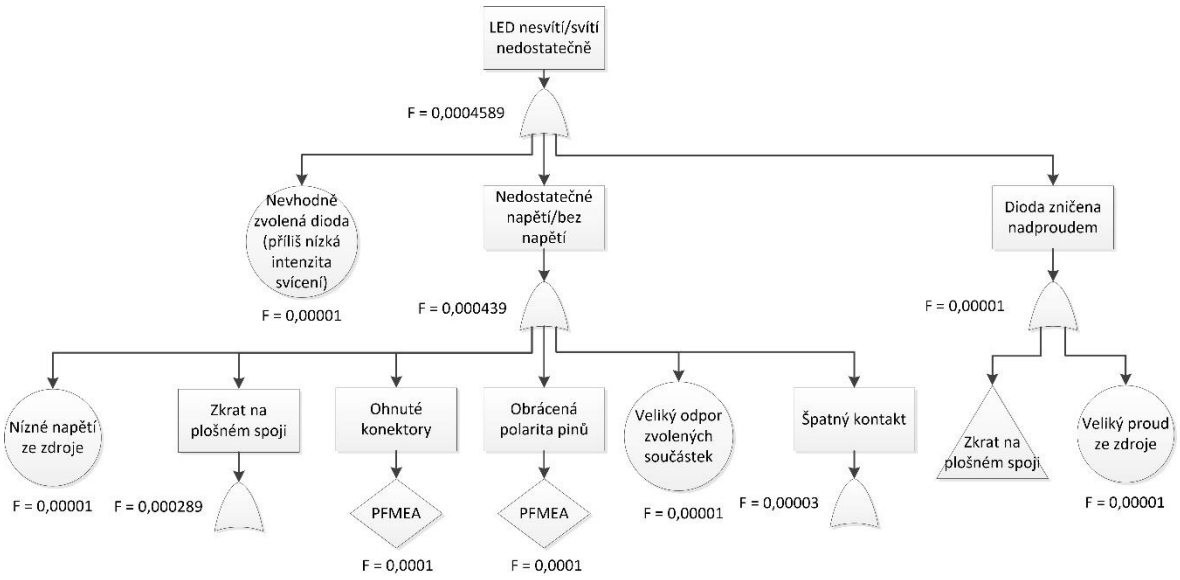
Primární události můžeme přiřadit pravděpodobnost výskytu. Podle tabulky 2 DFMEA bude malá pravděpodobnost výskytu s číselnou hodnotou F = 0,00001 (0,01 výskytů na tisíc objektů).

Mezilehlé události se dále rozvíjí do nižší úrovně. Mohou nastat v případě, že nastane jakákoliv primární či mezilehlá událost na nižší úrovni. Mezilehlé události „ohnuté konektory“ a „obrácená polarita pinů“ v této části nejsou dále rozvinuty, neboť souvisejí s chybu v procesu a jsou součástí stromu poruchových stavů v procesní FMEA. Je však

potřeba brát pravděpodobnost těchto událostí v úvahu při výpočtu poruchovosti systému. Tato pravděpodobnost výskytu událostí byla vypočítána v samostatné FTA analýze pro proces FMEA.

Dalším použitým symbolem je transfer u události „zkrat na plošném spoji“. Tato událost již byla rozvinuta v jiné části pro stejnou vrcholovou událost, není ji proto nutné rozvíjet znovu.

Strom poruchových stavů končí primárními událostmi, nebo částmi analýzy, které jsou rozvinuty na jiném místě či v jiné analýze.



Obrázek 15: Část analýzy stromu poruchových stavů (FTA).

Po dokončení stromu poruchových stavů určíme pravděpodobnosti všech primárních událostí a událostí, které jsou rozvinuty v jiné analýze. Pravděpodobnost vrcholové události určíme podle vzorce (11).

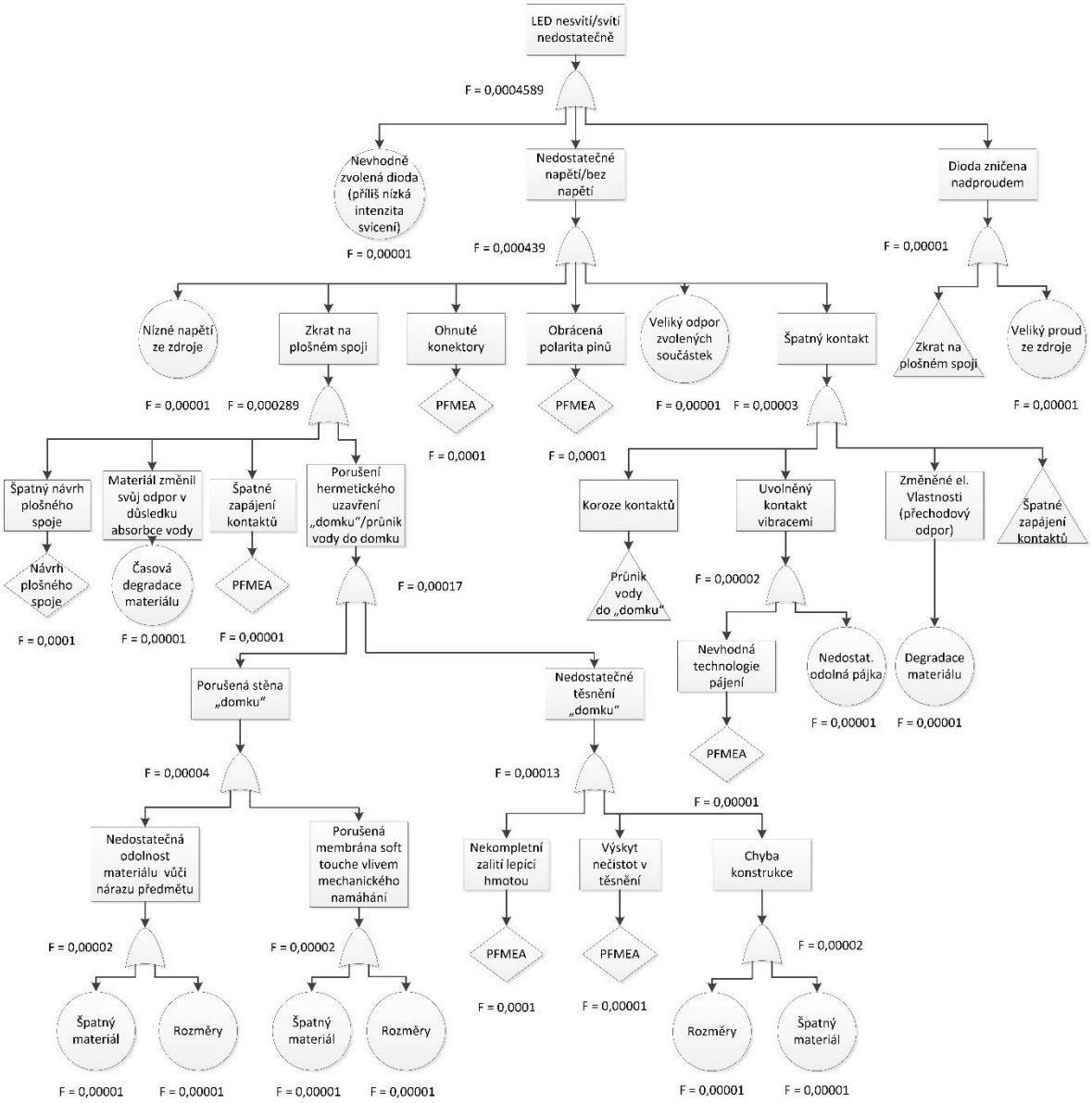
Výpočet bude uveden na příkladu mezilehlé události „porušená stěna domku“ viz obrázek 16:

$$F = 1 - [1 - 0{,}00001] \cdot [1 - 0{,}00001]] \cdot [1 - 0{,}00001]] \cdot [1 - 0{,}00001] = 0{,}00004 \quad (13)$$

Tímto způsobem můžeme určit pravděpodobnosti výskytu vrcholové události a všech mezilehlých událostí způsobených primárními událostmi, které budou obsaženy v DFMEA.

Po aplikaci tohoto výpočtu na strom poruchových stavů bude pravděpodobnost výskytu vrcholové události F = 0,0004589.

Pomocí již dříve zmiňované tabulky výskytu pro DFMEA zpětně určíme úroveň výskytu. Známka hodnocení bude 5, tedy střední pravděpodobnost poruchy výskytu vrcholové události.



Obrázek 16: Strom poruchových stavů FTA pro vrcholovou událost „LED nesvítí/svítí nedostatečně" včetně pravděpodobností výskytu.

Zhodnocení FTA analýzy

V této FTA analýze byly použity pouze logické členy OR (událost může nastat, pokud nastane jakákoliv z jeho příčin), tedy vrcholová událost může nastat, pokud nastane jakákoliv s primárních událostí. Pro významnou redukci výskytu vrcholové události „LED nesvítí/svítí nedostatečně“ je tedy nutné se zaměřit na primární příčiny vrcholové události, jimiž jsou:

- nevhodně zvolená dioda (příliš nízká intenzita svícení),
- nízké napětí ze zdroje,
- veliký odpor zvolených součástek,
- veliký proud ze zdroje,
- časová degradace materiálu,
- nedostatečně odolná pájka,
- nevhodně zvolený materiál pro kontakty (veliký přechodový odpor),
- nevhodně zvolený materiál a rozměry pro pouzdro „domek“,
- nevhodně zvolený materiál a rozměry pro softtouch,
- nevhodně zvolený materiál a rozměry těsnící složky.

V kombinaci s DFMEA by se v ní však měly objevit všechny jednobodové poruchy (porucha, která je obsažená v minimálním kritickém řezu) obsažené v FTA analýze, proto je užitečné znát jejich pravděpodobnosti výskytu pro úplnost informací vstupujících do DFMEA. Grafické zobrazení také pomáhá k dobré orientaci v návaznosti poruch, které by v DFMEA nebyly možné.

7.4.5 Design FMEA

Jak již bylo uvedeno v úvodu praktické části, do pracovního listu DFMEA se nejdříve uvedou informace o projektu, jeho týmu atd. v záhlaví pracovního listu.

POTENTIAL FAILURE MODES & EFFECTS ANALYSIS							
Název systému					Projekt		
Diplomová práce Horácek					Diplomová práce		
Předmět	ID předmětu	Vytvořil	Datum vytvoření	Poslední úpravy	Datum změny	Typ	Status
Softouch	ZCU	VotapekV	30.10.2017	Horáček	02.04.2018	Design	Uvolněno
Odpovědný člen týmu		Odpovědné oddělení		Atribut			
-		-		Vývojový díl			
Členové týmu							
Weber; Kocourek; Kuehn; OEM; Horáček; Designer; Novák							
Komentáře							
30.10.2017 FMEA založena pro účely vypracování diplomové práce. Jednotlivé parametry jsou pozměněny, i když se pohybují v rámci běžné praxe.							

Obrázek 17: Záhlaví DFMEA.

Dalším krokem je stanovení požadovaných specifikací a funkcí od zákazníka. V tomto případě jsou funkce rozděleny do dvou hlavních části, na primární a sekundární funkce. Primární funkce:

- vyslat signál pro otevření dveří zavazadlového prostoru za stanovených podmínek (síla stlačení, teplotní rozsah),
- bez stisku tlačítka nebude vyslán signál pro otevření zavazadlového prostoru,
- osvítit plochu SPZ v souladu s požadavky normy ECE-R4.

Sekundární funkce:

- bezpečnost,
- vzhled,
- ergonomie,
- zneužití,
- životnost,
- mechanická odolnost,
- hluk,
- životní prostředí a recyklace,
- chemická odolnost a koroze,
- elektrické vlastnosti,
- doprava k zákazníkovi.

Tyto funkce již byly uvedeny v P-diagramu, kde pomohly týmu ke správnému pochopení žádané funkce. Následně je uveden příklad návaznosti výsledků z FTA analýzy do DFMEA.

Nr.	Funkce	Možný způsob poruchy	Možný důsledek poruchy	Závažnost	Klasifikace	Možná příčina poruchy	Výskyt	Aktuální řízení procesu	Odhalení	RPN	Doporučené opatření	Odpovídá a termín dokončení	Výsledky opatření					
													Přijaté opatření	Závažnost	Výskyt	Odhalení	RPN	Stav [%]
1.3	Osvítit plochu SPZ (evropský trh) v rámci normy ECE-R4	LED nesvítí/svítí nedostatečně	Není splněná norma ECE-R4	10	YC	Nevhodně zvolená dioda (příliš nízká intenzita svícení)	3	P: Výběr diody podle katalogu	2	60								
								D: Funkční test										
						Dioda zničena nadproudem	2	P: Výběr diody podle katalogu	3	60								
								D: Test životnosti										
						Nedostatečné napětí/bez napětí	5	P: výběr součástek podle katalogu	6	300	12.12.2017							uzavřeno
								P: Simulace LED obvodu			P: Simulace obvodu LED	20.02.2018: Weber, Designer	P: Simulace obvodu LED	10	3	3	90	uzavřeno
								P: Použití odolného materiálu podle katalogu			P:Změna materiálu pouzdra		P:Změna materiálu pouzdra					
								P: Gore-Tex pro odvod vlhkosti			P: Změna rozměrů pouzdra		P: Změna rozměrů					
								P: Tloušťka stěny min 3mm			P: Fotometrická kontrola těsnící plochy		P: Fotometrická kontrola těsnící					
								P:Těsnicí plocha bez otřepů a dělené linie.			P:Navýšení tloušťky stěny na 3 mm		P:Navýšení tloušťky stěny na 3 mm					
								D: Test životnosti			D: Test životnosti		D: Test životnosti					
								D: Klimatický test			D: Klimatický test		D: Klimatický test					
								D: Funkční test			D: Funkční test		D: Funkční test					

Obrázek 18: Část design FMEA pro způsob poruchy „LED nesvítí / svítí nedostatečně“.

V FTA analýze byla zvolena vrcholová událost „LED nesvítí / svítí nedostatečně“, která je zde uvedena jako možná příčina poruchy, jejímž možným důsledkem je nesplnění normy ECE-R4. Nesplnění normy, či právních předpisů je klasifikováno podle tabulky 1 hodnotou 10, tedy nejzávažnější. Závažnost poruchy je dána charakterem poruchy, proto jí není možné nijak ovlivnit, pouze v případě změny legislativy. Pokud má porucha stupeň závažnosti 9 nebo 10, existuje potenciální kritická charakteristika. Když je identifikována potenciální kritická charakteristika, zadávají se písmena *YC* do sloupce *klasifikace* a spustí se proces FMEA podle interní metodiky WITTE.

Do sloupce *možná příčina poruchy* se vypíší všechny příčiny poruchy z FTA analýzy. Pro lepší orientaci se poruchy vypisují od vrcholové události k primárním událostem. Možným příčinám poruchy se přidělí hodnota výskytu podle pravděpodobnosti výskytu v FTA analýze a tabulky výskytu. Do sloupce aktuální řízení procesu se uvedou způsoby prevence *P* a detekce *D*. Například v FTA analýze se vyskytla mezilehlá událost „nedostatečná odolnost proti nárazu předmětu“, kterou mohou způsobit nesprávné rozměry

nebo volba špatného materiálu. Obě tyto události se zahrnou do prevence a doporučených opatření, jak je uvedeno na obrázku 19. Poté se možným příčinám poruch přidělí hodnocení detekce podle tabulky 3 a spočítá se číslo priority rizika RPN.

$$RPN = závažnost \cdot výskyt \cdot detekce$$

Jak je vidět na obrázku 18, první dvě příčiny poruch mají přijatelnou úroveň výskytu i detekce, proto nebyla přijata žádná další opatření. Naopak v případě možné příčiny poruchy „nedostatečné napětí / bez napětí“ je nutné tato navržená opatření zavést. Vysoké hodnocení je způsobeno množstvím primárních událostí, které tuto poruchu způsobují. Na obrázku 19 jsou jednotlivé poruchy rozepsány a hodnoceny samostatně. Pro určení výskytu a detekce poruchy „nedostatečné napětí / bez napětí“ jsou vybrány pouze nejvyšší hodnocení. Navržená a přijatá opatření jsou též v souladu se samostatně rozepsanými poruchami včetně přepočítaných hodnot RPN. Můžeme zde vidět, že jsme eliminovali výskyt a detekci poruch na přijatelnou úroveň pomocí přijatých opatření.

Nr.	Funkce	Možný způsob poruchy	Možný důsledek poruchy	Závažnost	Klasifikace	Možná příčina poruchy	Výskyt	Aktuální řízení procesu	Odhalení	RPN	Doporučené opatření	Odpovídá a termín dokončení	Výsledky opatření					
													Přijaté opatření	Závažnost	Výskyt	Odhalení	RPN	State [%]
1.3	Osvítit plochu SPZ (evropský trh) v rámci normy ECE-R4	Zkrat na plošném spoji	Není splněná norma ECE-R4	10	YC	Špatný návrh tištěného spoje	4	P: Simulace LED obvodu	3	120	12.12.2017							uzavřeno
			LED nesvítí					D: Funkční test			P: Simulace obvodu LED diody	10.02.2018: Weber	P: Simulace obvodu LED diody	10	3	2	60	uzavřeno
						Materiál změnil svůj odpor v důsledku absobce vody (zkrat)	3	P: Použití odolného materiálu podle katalogu	6	180	12.12.2017							uzavřeno
								P: Gore-Tex pro odvod vlhkosti			D:Klimatický test	20.02.2018: Designer	P: Změna materiálu	10	2	3	60	uzavřeno
								D: Klimatický test					D: Klimatický test OK					
						Porušení hermetického uzavření domku (průnik vody)	4	P: Použití odolného materiálu domku	4	160	10.12.2017							uzavřeno
								P: Kontrola rozměrů v návrhu			P: Změna rozměrů	10.02.2018: Designer	P: změna rozměrů pouzdra	10	3	3	90	uzavřeno
								D: Test životnosti			P: Použití odolného materiálu		D: Test životnosti OK					
						Nedostatečná odolnost materiálu proti nárazu předmětu (průnik vody)	3	P: Tloušťka stěny min 3mm	5	150	10.12.2017							uzavřeno
								P: Kontrola rozměrů v návrhu			P:Navýšení tloušťky stěny na 3 mm	20.02.2018: Designer	P: Navýšení tloušťky stěny na 3 mm	10	2	3	60	uzavřeno
								P: Použití odolného materiálu podle katalogu			P: Změna materiálu							
								D: Test životnosti					D: Test životnosti OK					
								D: Test pomocí OEM										

Obrázek 19: Část design FMEA pro možný způsob poruchy „zkrat na plošném spoji“.

7.5 Zhodnocení použitých metod

V rámci praktické části diplomové práce byly zpracovány obsáhlé analýzy FTA a DFMEA s podporou pomocných metod k pochopení funkcí a chybových stavů. Část z těchto analýz zde byla použita pro vysvětlení principu jejich tvoření a návaznosti.

Pomocí FTA analýzy byly identifikovány všechny primární příčiny vrcholových událostí a jejich logické návaznosti při výskytu poruchy pro primární funkce produktu. Doplněním pravděpodobností výskytů a následným výpočtem pravděpodobnosti mezilehlých a vrcholových událostí získal tým velmi cenné informace, které dále posloužily jako vstup do analýzy DFMEA. Díky deduktivnímu přístupu v FTA analýze byly identifikovány všechny příčiny důsledků, které byly použity v DFMEA. Pokud by byla použita pouze DFMEA, tým by neměl takto ucelený přehled o logickém propojení příčin a jejich následků, jelikož se do pracovního listu zapisují příčiny poruch jako jednotlivé body. Následné určení výskytu příčin v DFMEA je poté vyhodnoceno na základě výpočtů jejich předcházejících primárních příčin z FTA analýzy. Například porucha „zkrat na plošném spoji“ má hned několik příčin s různými mezilehlými a primárními událostmi a je zároveň příčinou vrcholové události „LED nesvítí / svítí nedostatečně“. Při určení výskytu v DFMEA tedy tým pracuje s množinou pravděpodobností a návazností událostí z FTA. Výslednou pravděpodobnost události „zkrat na plošném spoji“ lze poté určit s větší přesností. Je tedy zřejmé, že analýzy na sebe navazují a doplňují se. Použití analýz FTA a FMEA s doplňujícími metodami boundary diagram, P-diagram a matice rozhraní činí analýzu rizik komplexnější a robustnější.

7.6 Implementace do podniku

Společnost WITTE Nejdek používá při tvorbě analýzy rizik analýzu FMEA v softwarovém nástroji PLATO – SCIO a pro tvorbu FTA analýzy využívá software Microsoft Visio. Standardně však analýzy nejsou využívány zároveň a tím není možné plně využít potenciál jejich návaznosti.

Navrhuji tedy implementaci FTA analýzy do podniku pro každý produkt a rozšíření softwarového nástroje PLATO – SCIO o modul FTA analýzy. Díky centrální databázi událostí, příčin a následků poruch lze automaticky implementovat poznatky z FTA analýzy do FMEA a naopak. Lze tvořit stromy poruchových stavů včetně kvalitativní a kvantitativní analýzy a všechny informace poté využít pro vývoj dalších produktů. Počáteční

implementace systému bude časově velmi náročná, avšak při vytvoření dostatečně detailního stromu poruchových stavů lze analýzu pro další produkty pouze modifikovat. Kvalitnější analýza rizik znamená nižší poruchovost produktu a tím i větší spokojenost zákazníků.

Závěr

Cílem diplomové práce bylo provést analýzu používaných nástrojů pro analýzu rizik, především se zaměřením na metody FMEA a FTA a jejich návaznost. Poznatky z této analýzy byly dále použity v praxi ve spolupráci se společností WITTE Nejdek.

V teoretické části byla nejprve popsána metoda FMEA. Základem metody je zaznamenání všech možných příčin a způsobů poruchy, navržení opatření a sledování daného rizika. Existuje více typů metody FMEA, kde nejpoužívanější jsou procesní FMEA a design FMEA. Postup vypracování analýzy byl detailně vysvětlen na design FMEA, která byla poté použita v praktické části. Dále byla popsána metoda FTA, postup tvoření a vyhodnocení pomocí kvalitativní a kvantitativní metody. Důležité bylo také zmínit pomocné metody boundary diagram, P-diagram a matice rozhraní, které též navazovaly na praktickou část. Byla popsána také návaznost obou metod, další používané metody a příklady vhodných softwarových nástrojů.

Návaznost obou analýz se obecně často doporučuje vzhledem k deduktivnímu přístupu FTA analýzy a induktivnímu přístupu analýzy FMEA. Existují různé způsoby jejich vzájemných kombinací. V praktické části byla využita varianta, kde FTA analýza předcházela analýze design FMEA. Tato varianta umožňuje týmu nejprve do detailu prozkoumat provázanosti primárních příčin poruchy a jejich vzájemné vazby s mezilehlými událostmi a vrcholovou událostí (nežádoucí stav / porucha), určit pravděpodobnost výskytu pomocí kvantitativní metody vyhodnocení a poté tyto poznatky použít v design FMEA. Pokud bychom použili pouze metodu design FMEA, nebylo by možné všechny tyto provázanosti identifikovat, jelikož se příčiny poruch zapisují do pracovního listu jako jednotlivé body.

V praktické části byla zpracována rozsáhlá analýza rizik na produktu společnosti WITTE Nejdek, konkrétně na klice zadních dveří, za pomoci interních dokumentů a poznatků z dřívějších analýz. Analýza byla zaměřena na návrh produktu pomocí metod design FMEA a FTA analýza. FTA analýza byla zpracována pro každou hlavní funkci produktu a poznatky z této analýzy byly použity pro zpracování design FMEA, kde byly analyzovány rizika poruchy hlavních funkcí (např. vyslání signálu pro otevření zadních dveří a osvětlení plochy SPZ) i sekundárních funkcí (např. bezpečnost, vzhled, hluk, atd.).

Pro robustnost celé analýzy byly použity metody boundary diagram, P-diagram a matice rozhraní, které pomohly pochopit správnou funkci produktu a jasné vymezení faktorů, které na něj působí a ovlivňují jej.

Ve společnosti WITTE Nejdek se FTA analýza provádí v programu Microsoft Visio, který je vhodný pro grafické znázornění. FTA analýza se však stává více užitečná při použití kvantitativní či kvalitativní analýzy. V tomto případě již tento softwarový nástroj není vhodný. Existuje mnoho softwarových nástrojů, které slouží přímo k vytváření stromu poruchových stavů, některé dokáží propojit výsledky z FTA analýzy s analýzou FMEA automaticky. Mezi ně patří i software PLATO-SCIO, který je ve společnosti využíván při tvorbě analýzy FMEA.

Navrhuji proto implementovat rozšiřující modul softwaru PLATO – SCIO pro FTA analýzu. Návaznosti příčin poruch a jejich výskyt lze poté lépe identifikovat a celý systém se stává přehlednější a komplexnější. Provázanosti příčin a následků poruch se dále mohou promítnout i do procesní FMEA. Výhodou jsou také aktualizace stavu, pokud je například odstraněna jedna příčina poruchy, sníží se pravděpodobnost výskytu vrcholové události v FTA analýze a zároveň i v dokumentu design FMEA, to činí celou analýzu efektivnější a celý systém robustnější. Implementace tohoto rozšíření bude zpočátku velmi časově náročná, pokud však bude FTA analýza provedena dostatečně detailně s logickými návaznostmi na jeden typ produktu, pro další typy může být dále pouze modifikována podle zadaných specifikací. Vzhledem k centralizaci dat o poruchách, příčinách a jejich provázanosti z FMEA a FTA analýz získá společnost mnohem komplexnější informace o rizicích spojených s návrhem i výrobním procesem. Využitím těchto komplexních informací o možném výskytu poruch jim dokáže lépe předcházet, snížit poruchovost produktů a tím také zvýšit spokojenost zákazníků.

Seznam literatury a informačních zdrojů

[1] ČSN EN 60812. *Techniky analýzy bezporuchovosti systémů - Postup analýzy způsobů a důsledků poruch (FMEA)*. Praha: Český normalizační institut. 2007

[2] LEHMAN, Catherine. *Failure Mode and effects analysis: FMEA handbook*. 4.2. Dearborn, Mi: Ford motor company, 2011.

[3] Failure mode and effects analysis. *Wikipedia: the free encyclopedia* [online]. [cit. 14.1.2018]. Dostupné z: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

[4] *What is FMEA* [online]. [cit. 16.1.2018]. Dostupné z: https://www.datalyzer.com/knowledge/fmea/

[5] HOLUB, Rudolf, VINTR, Zdeněk. *Spolehlivost letadlové techniky*. B.m., 2001. Vysoké učení technické v Brně.

[6] VESELÝ, Milan. *POUŽITÍ METODY FMEA PRO PREVENCI CHYB*. B.m., 2012. b.n.

[7] LOCK, Dennis. *The essentials of project management*. 3rd ed. Burlington, VT: Gower, 2007. ISBN 9780566088056.

[8] LITTLE, David M. Failure Modes and Effects Analysis General Description of FMEA. 2015.

[9] PETRAŠOVÁ, Ivana. *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka.* 4th vyd. Praha: Česká společnost pro jakost, 2008. ISBN 9788002021018.

[10] CARLSON, Carl. *Effective FMEAs*. 1st vyd. Hoboken, N.J.: Wiley, 2012. ISBN 9781118007433.

[11] ČSN EN 61025. *Analýza stromu poruchových stavů (FTA)*. Praha: Český normalizační institut. 2007

[12] MARTENSEN, Anna, BUTLER, Ricky. *NASA Technical Memorandum 89098 The Fault-Tree Compiler* [online]. 1987. [cit. 24.4.2018]. ISBN 1987001133. Dostupné z: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19870011332.pdf

[13] ERICSON, Clifton. Fault Tree Analysis – A History. *The 17th International System Safety Conference* [online]. 1999, [cit. 24.4.2018]. 1–9. Dostupné z: http://www.fault-tree.net

[14] VINTR, Zdeněk, VALIŠ, David, VINTR, Michal. *Prediktivní analýzy spolehlivosti a možnosti jejich využití*. B.m.: Česká společnost pro jakost. 2016. ISBN 9788072319657

[15] *Choosing between Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA)* [online]. [cit. 2.5.2018]. B.m.: Egerton Consulting. Dostupné z: https://egertonconsulting.com/fmea-v-fta/?doing_wp_cron=1525175842.3094201087951660156250

[16] CRISTEA, G., CONSTANTINESCU, D. M.. A comparative critical study between FMEA and FTA risk analysis methods. *IOP Conference Series: Materials Science and Engineering* [online]. 2017. [cit. 2.5.2018.] Dostupné z: http://iopscience.iop.org/article/10.1088/1757-899X/252/1/012046/pdf

[17] LIU, Chi Tang, HWANG, Sheue Ling, LIN, I. K.. *Safety analysis of combined FMEA and FTA with computer software assistance* [online]. [cit. 2.5.2018]. B.m.: IFAC, 2013. ISBN 9783902823359. Dostupné z: doi:10.3182/20130619-3-RU-3018.00370

[18] TICHÝ, Milík. *Ovládání rizika*. Vyd. 1. V Praze: C.H. Beck, 2006. ISBN 8071794155.

[19] Diagram příčin a následků. *Wikipedia: Diagram příčin a následků* [online]. 2016 [cit 2.5.2018]. Dostupné z: https://cs.wikipedia.org/wiki/Diagram_příčin_a_následků

[20] IEC 62502:2010. *Analysis techniques for dependability - Event tree analysis (ETA)*. 1.0. B.m.: International electrotechnical commission. 2010

[21] PRODUCT QUALITY RESEARCH INSTITUTE. Hazard & Operability Analysis (HAZOP). *Risk management training guides* [online]. 2014, [cit. 2.5.2018] 1–9. Dostupné z: http://pqri.org/wp-content/uploads/2015/08/pdf/HAZOP_Training_Guide.pdf

[22] *PLATO-SCIO* [online]. 2014. [cit. 3.5.2018]. Dostupné z: https://w3.plato.de/scio-470.html

[23] *RiskSpectrum* [online]. 2014. [cit. 3.5.2018]. Dostupné z: http://www.riskspectrum.com/en/risk/

[24] *RiskSpectrum FMEA* [online]. 2014. [cit. 3.5.2018]. Dostupné z: http://www.riskspectrum.com/en/risk/Meny_2/RiskSpectrum_FMEA/

[25] *WITTE Automotive* [online]. [cit. 14.4.2018]. Dostupné z: https://www.witte-automotive.cz/

[26] UNITED NATIONS. *Addendum 3: Regulation No. 4* [online]. 2013. [cit. 20.4.2018] Dostupné z: http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2018/R004r3am3e.pdf