VŠB – Technická univerzita Ostrava
Fakulta strojní
Institut dopravy

Funkční bezpečnost vybraného systému silničního vozidla

Disertační práce

Studijní program: **P2301 Strojní inženýrství**
Studijní obor: **2301V003 Dopravní technika a technologie**
Školitel: **doc. Ing. Ivana Olivková, Ph.D.**
Doktorand: **Ing. et Ing. Michal Richtář**

Ostrava 2014

Anotace

RICHTÁŘ, Michal. *Funkční bezpečnost vybraného systému silničního vozidla*. Ostrava, 2013. 134s. Disertační práce. VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy. Školitel: OLIVKOVÁ, Ivana.

Obsahem této disertační práce je problematika funkční bezpečnosti v oblasti silničních vozidel, zvláště pak využití vhodných metod, postupů a modelů, v návaznosti na novou situaci spojenou se zaváděním nových norem.

Práce byla zaměřena na návrh vhodných postupů a využití kvalitativní a kvantitativní analýzy spolehlivosti vybraných systémů silničních vozidel, jež významně ovlivňují bezpečnost silničního provozu. Pro ověření skutečné úrovně vybraných parametrů spolehlivosti zařízení byl navržen program zkoušek spolehlivosti.

Pro hodnocení funkční bezpečnosti byly zvoleny postupy a nástroje, jež vycházejí z principů funkční bezpečnosti elektrických/elektronických systémů souvisejících s bezpečností, popsaných v normě ČSN EN 61508 a ISO 26262.

Disertační práce je tvořena částí teoretickou a experimentální a je rozčleněna do sedmi kapitol.

V teoretické části práce jsou přehledně zpracovány a rozvinuty základní principy používané v oblasti funkční bezpečnosti. Byl vytvořen nový postup pro klasifikaci rizik pro silniční vozidla, který zjednodušuje proces posuzování rizik a přiřazení úrovně integrity bezpečnosti. Dále byly vybrány a popsány a rozpracovány metody pro kvalitativní a kvantitativní hodnocení funkční bezpečnosti. Všechny tyto metody jsou v souladu s doporučeními normy ISO 26262.

Praktická část práce byla zaměřena na uplatnění postupů a metod navržených v teoretické části práce. Byly aplikovány na systém vstupních dveří autobusu a přední světlomet automobilu. V rámci kvalitativního hodnocení spolehlivosti byly s využitím postupu odpovídajících metod identifikovány jednotlivé funkce vstupních dveří autobusu a způsoby jejich selhání. Výsledkem je návrh různých opatření vedoucí ke snížení rizika.

V rámci kvantitativní analýzy LED světla byl s využitím vhodných postupů vytvořen teoretický model bezporuchovosti pro náhodné poruchy hardware, na jehož základě by bylo možné výpočtem určit konkrétní číselné hodnoty ukazatelů funkční bezpečnosti.

Annotation

RICHTÁŘ, Michal. *Functional safety of selected road vehicle system.* Ostrava, 2013. 134 p. Dissertation thesis. VŠB – Technical University of Ostrava, Faculty of Mechanical Engineering, Institute of Transport. Supervisor: OLIVKOVÁ, Ivana.

This thesis deals with the functional safety of road vehicles, especially the utilization of appropriate methods, procedures and models, in response to the new situation, coupled with the introduction of new standards.

The thesis was focused on the design of appropriate procedures and the utilization of qualitative and quantitative reliability analysis of motor vehicles selected systems, which significantly affect the road safety. To verify the actual levels of selected reliability parameters of equipment the reliability tests program has been created.

Selected procedures and tools for functional safety assessment, based on the principles of functional safety of electrical / electronic safety-related systems, as described in the standards EN 61508 and ISO 26262, have been chosen.

Dissertation thesis consists of theoretical and experimental part, and is divided into seven chapters. In the theoretical part are clearly organized and evolved the basic principles used in the field of functional safety. The new procedure for the risk classification for road vehicles, which simplifies the process of risk assessment and allocation of safety integrity levels, has been created. Furthermore, the methods for qualitative and quantitative evaluation of functional safety have been selected, described and elaborated. All these methods are in accordance with the recommendations of ISO 26262.

The practical part focuses on the application of the procedures and methods proposed in the theoretical part. These methods to the bus entrance door system and front headlight car have been applied. Each function of the bus entry doors and their failure modes using the appropriate methods and procedures have been identified in a qualitative assessment of reliability. The result is proposition of various measures to the risk reduction.

The theoretical model of reliability of random hardware failures using the appropriate procedures in a quantitative assessment of reliability has been performed. The specific numerical values for the functional safety parameters, on the basis of the performed model have been calculated.

Poděkování

Na tomto místě bych chtěl poděkovat své školitelce doc. Ing. Ivaně Olivkové, Ph.D. za vedení během mého doktorského studia. Zvláštní poděkování patří doc. Ing. Janu Famfulíkovi, Ph.D. a Ing. Janě Míkové, Ph.D. za cenné rady, připomínky, poskytnuté konzultace a jejich trpělivost při vypracování této disertační práce.

Obsah

Seznam použitých zkratek a symbolů

ALARP	co nejnižší rozumně dosažitelné riziko
ASIL	úroveň integrity bezpečnosti (Automotive Safety Integrity Layer)
ASAM	metoda stanovení integrity bezpečnosti (Automotive Safety Assesment Method)
CAN	datová sběrnice (Controller Area Network)
CPU	procesor (Central Processing Unit)
DC	diagnostické pokrytí (Diagnostic Coverage)
DC_{RF}	diagnostické pokrytí s ohledem na zbytkové poruchy
DC_{MPFL}	diagnostické pokrytí s ohledem na vícenásobné poruchy
E/E/PES	elektrický/elektronický/programovatelný elektronický systém
EUC	řízené zařízení (Equipment Under Control)
FMEA	analýza způsobů a důsledků poruch (Failure Mode and Effect Analysis)
FTA	analýza stromu poruch (Failure Tree Analysis)
RBD	blokový diagram bezporuchovosti (Reliability Block Diagram)
RPN	hodnota závažnosti rizika (Risk Priority Number)[-]
A	zvýšené zatížení
A_F	faktor zrychlení [-]
c	parametr polohy Weibullova rozdělení pravděpodobnosti [h]
C	konfidenční úroveň [-]
C	následek nebezpečné události
D	odhalitelnost poruchy
O	četnost vzniku poruchy
$E(T)$	střední hodnota náhodné veličiny [h]
E_A	aktivační energie [eV]
f	četnost výskytu nebezpečné události
$f(t)$	hustota pravděpodobnosti náhodné veličiny [-]
F_S	pravděpodobnost poruchy systému [-]
$F(t)$	distribuční funkce náhodné veličiny [-]
$G(T)$	rychlost reakce
K	Boltzmanova konstanta ($8{,}617385.10^{-5}$ $eV.K^{-1}$)
LFM	odolnost LFM (Latent Fault Metric)
$L(T)$	kvantitativní ukazatel spolehlivosti [h]
m	parametr tvaru Weibullova rozdělení pravděpodobnosti [-]
M	výrobky se během zkoušky opravují
n	počet výrobků zařazených do zkoušky spolehlivosti [-]
$P(A)$	pravděpodobnost náhodného jevu A [-]
PFD	pravděpodobnost nebezpečné poruchy [-]
PFH	cílová míra poruch
r	počet poruch během zkoušky spolehlivosti [-]
R	riziko systémů souvisejících s bezpečností [-]
R	výrobky se během zkoušky nahrazují
$R(t)$	doplněk k distribuční funkci náhodné veličiny [-]
R_S	pravděpodobnost bezporuchového stavu systému [-]
S	závažnost poruchy
SAE	Society of Automotive Engineers
SPM	odolnost SPM (Single Point Metric)
SIL	úroveň integrity bezpečnosti (Safety Integrity Level)
SIS	řízené technické zařízení (Safety Instrumented System)

SxO	rizikové číslo matice závažnosti [-]
t	hodnota náhodné veličiny T [h]
t_{AKU}	akumulovaná pracovní doba zkoušky [h]
T	absolutní teplota [K]
T_D	dolní mez konfidenčního intervalu [h]
T_H	horní mez konfidenčního intervalu [h]
U	výrobky se během zkoušky nenahrazují
α	hladina významnosti [-]
χ^2	statistika chí-kvadrát [-]
λ	parametr exponenciálního rozdělení pravděpodobnosti [h^{-1}]
$\lambda(t)$	intenzita náhodné veličiny [-]
λ_S	intenzita bezpečných poruch [h^{-1}]
ν	počet stupňů volnosti rozdělení chí-kvadrát [-]
θ	parametr náhodné veličiny
τ	doba trvání zkoušky [h]

1 Úvod

V souladu s názvem disertační práce je obsahem této disertační práce problematika funkční bezpečnosti v oblasti silničních vozidel, zvláště pak využití vhodných metod, postupů a modelů.

Funkční bezpečnost je termín, jenž se objevuje v oblasti technických systémů teprve v posledních letech a jeho význam pro procesy navrhovaní a dokumentování těchto technických systémů je nemalý. Uplatňování některých principů funkční bezpečnosti začíná stále více pronikat do technické praxe i v oblasti dopravních prostředků. V obecném pohledu jsou některé požadavky funkční bezpečnosti specifikovány mateřskou normou EN 61508 Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů související s bezpečností. V některých oblastech techniky jsou s respektováním výše uvedené mateřské normy EN 61508 již v platnosti také oborové normy, které vhodným způsobem doplňují a rozšiřují požadavky této mateřské normy.

Pro oblast silničních vozidel je krátce k dispozici znění vlastní oborové normy, známé jako ISO DIN 26262 - Road vehicles - Functional safety, jež má vhodným způsobem uplatňovat požadavky normy mateřské pro technické systémy automobilů. Protože oborové normy mají přednost před použitím základních norem (v tomto případě ČSN EN 61508, tzv. basic safety norm), a i když je existence této normy zatím krátká a její implementace do oblasti silničních vozidel ještě chvíli potrvá, rozhodl se autor práce s využitím praktických příkladů ukázat možné postupy pro uplatnění této oborové normy.

V souvislosti s ČSN EN 61 508 a zněním ISO 26262 je nutné ke každému technickému systému v oblasti konstrukce vozidel vypracovat bezpečnostní zprávu na základě požadavků odběratele nebo oborové autority, jejíž součástí je analýza a hodnocení rizik vyplývající z provozování hodnoceného systému, dále návrh opatření pro snížení rizik, kontrola účinnosti navržených opatření a prokazování dosažené úrovně funkční bezpečnosti.

Evropský a potažmo světový automobilový průmysl, byť respektující normativní záležitosti vztahující se ke konkrétním oblastem vozidlových systémů a požadavků na ně, nemá o funkční bezpečnosti v podstatě výrazné povědomí. Z tohoto důvodu jím nejsou principy funkční bezpečnosti komplexně používány a v praxi aplikovány a ani nejsou dořešeny některé konkrétní souvislosti zejména v návaznosti na konstrukci a požadavky řešení mechatronických systémů.

Z tohoto hlediska je možno považovat problematiku funkční bezpečnosti v oblasti silničních vozidel za vysoce aktuální a její řešení v disertační práci za přínosné z pohledu jak

pedagogického, ve vztahu aktuálnosti výukového procesu, tak také zejména vědeckého, ve vztahu k uplatnění moderních matematických teorií a dalších postupů.

Z těchto důvodů jsou v této práci uplatněny některé inovativní postupy na konkrétním systému silničního vozidla s cílem naplnit obecné požadavky na teoretický a experimentální obsah disertační práce.

1.1 Stav řešené problematiky

V současnosti jsou požadavky na spolehlivost a bezpečnost technických systémů upraveny existujícími národními a globálními standardy. Samozřejmě se tento stav dotýká také oblasti dopravních systémů, tedy i silničních vozidel.

Základním standardem specifikujícím požadavky na funkční bezpečnost silničních vozidel je oborová norma ISO 26262 Road vehicles - Functional safety v návaznosti na normu ČSN EN 61508 – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických systémů související s bezpečností. Dalším příspěvkem do uvedené oblasti je existence řady standardů SAE (Society of Automotive Engineers), například pro oblast RCM údržby standard SAE JA 1011. Jelikož technické systémy současnosti jsou velice úzce spojeny se systémy elektrickými či elektronickými, je možné je posuzovat jako elektronické systémy související s bezpečností. Z tohoto pohledu je k dispozici již zmíněná mateřská norma pro funkční bezpečnost ČSN EN 61508 Funkční bezpečnost elektrických /elektronických/programovatelných elektronických systémů souvisejících s bezpečností, která specifikuje požadavky pro všechny fáze životního cyklu hardware i software uvedených systémů. Pro jednotlivé úrovně integrity bezpečnosti (SIL) tato norma definuje konkrétní parametry bezporuchovosti hardware, které jsou požadovány pro dosažení požadované bezpečnosti systému.

Pro provádění analýzy spolehlivosti elektrotechnických systémů existuje řada kvalitativních a kvantitativních metod a nástrojů, jejichž postup je specifikován normami. Patří k nim:

- ČSN IEC 50(191) Mezinárodní elektrotechnický slovník – Kapitola 191: Spolehlivost a jakost služeb,
- ČSN IEC 812 Metody analýzy spolehlivosti systémů. Postup analýzy způsobů a důsledků poruch (FMEA),
- ČSN IEC 1025 Analýza stromů poruchových stavů (FTA),

- ČSN IEC 1078 Metody analýzy spolehlivosti. Metoda blokového diagramu bezporuchovosti,
- ČSN IEC 61703 Matematické výrazy pro termíny bezporuchovost, pohotovost, udržovatelnost a zajištěnost údržby,
- ČSN IEC 605 Zkoušky bezporuchovosti zařízení,
- MIL-HDBK-217F Reliability Prediction of Electronic Equipment (predikce bezporuchovosti elektronických zařízení); apod.

Pro prokázání dosažené úrovně spolehlivosti technických systémů je nezbytné předložení technické dokumentace dokládající postupy kvalitativního a kvantitativního hodnocení sledovaných ukazatelů a metody a výsledky jejich ověření. Tuto dokumentaci může pro výrobce technických systémů připravit řada specializovaných poradenských společností, nebo se na její realizaci může podílet některé z vysokoškolských pracovišť, zabývajících se problematikou spolehlivosti.

V České republice se problematice vzdělávání a vědeckovýzkumné činnosti v oblasti spolehlivosti věnují pracoviště následujících univerzit:

- Česká zemědělská univerzita v Praze, Technická fakulta – Katedra jakosti a spolehlivosti strojů,
- Univerzita obrany, Fakulta vojenských technologií – Katedra bojových a speciálních vozidel,
- Univerzita Pardubice, Dopravní fakulta Jana Pernera – Katedra dopravních prostředků a diagnostiky, Oddělení jakosti, spolehlivosti a diagnostiky;
- VŠB – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky – Katedra aplikované matematiky;
- VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy – Ústav dopravní techniky,
- Technická univerzita v Liberci, Fakulta mechatroniky a informatiky – Ústav řízení systémů a spolehlivosti.

V dalších zemích Evropské unie se problematikou spolehlivosti a bezpečnosti zabývají mimo jiné na pracovištích následujících univerzit:

- RWTH Aachen University - Institute of Automotive Engineering RWTH Aachen University,
- Technische Universität Darmstadt - Department of Mechanical Engineering,
- Technische Universität München, Německo – Institute for Safety and Reliability,

- University of Bradford, Velká Británie – Risk and Reliability Engineering,
- Loughborough University – Department of Aeronautical and Automotive Engineering,
- Faculté Polytechnique de Mons, Belgie – Risks Research Center,
- Bergische Universität Wuppertal, Německo – Section Safety Theory and Traffic Engineering,
- City University London, School of Engineering and Mathematical Sciences, Velká Británie – Centre for Risk Management, Reliability, and Maintenance.

V oblasti spolehlivosti, bezpečnosti a hodnocení rizika technických systémů existuje velké množství tuzemských a zahraničních publikací a také velký počet odborných časopisů a specializovaných serverů, které poskytují řadu informací o teoretických metodách a přístupech i praktických řešeních problematiky. Mimo jiné k nim patří:

- časopis Automotive Engineering International (problematika automobilového průmyslu),
- časopis Automobil Technische Zeitschrift (problematika automobilového průmyslu),
- časopis Device and Materials Reliability (problematika spolehlivosti materiálů v různých fyzikálních podmínkách apod.),
- časopis IEEE Transactions on Reliability (otázky bezporuchovosti, udržovatelnosti, pohotovosti, jakosti a bezpečnosti systémů kosmického průmyslu, komunikace, počítačů, průmyslové elektroniky, laserů, jaderné energetiky a dopravních systémů),
- časopis Microelectronics Reliability (časopis se věnuje oblasti bezporuchovosti mikroelektronických prvků, obvodů a systémů),
- časopis Reliability Engineering & System Safety (aplikace metod zlepšování bezpečnosti a spolehlivosti komplexních systémů, jako zařízení jaderné energetiky, kosmických systémů atd.),
- server RIAC – Reliability Information Analysis Center (účelové zařízení Ministerstva obrany USA poskytuje všestrannou podporu v oblasti zabezpečování spolehlivosti, tj. publikace, software, vzdělávací aktivity, databáze informací o bezporuchovosti mechanických a elektronických prvků apod.),
- server Weibull.com (web provozovaný společností ReliaSoft, která je výrobcem software pro kvalitativní a kvantitativní analýzu spolehlivosti, pro jednotlivé programy jsou k dispozici bezplatné demo verze, příručky použití a elektronické učební texty).

Pro hodnocení a ověření spolehlivosti elektrotechnických systémů tedy existuje celá řada zdrojů, informací a nástrojů. Ty mohou výrobcům těchto zařízení usnadnit prokazování skutečné úrovně posuzovaných parametrů bezporuchovosti, bezpečnosti apod.

1.2 Cíle disertační práce

V souvislosti s nově zaváděnou normou ISO 26262 „Road vehicles – Functional safety“ je cílem této disertační práce navrhnout a vyzkoušet metody a postupy vedoucí k praktickému uplatnění této normy v automobilovém průmyslu. Návrh bude zaměřen na uplatňování postupů této normy a na použití kvantitativních a kvalitativních metod k prokazování požadované úrovně funkční bezpečnosti. Na základě výše uvedených obecných souvislostí, lze shrnout primární cíle disertační práce do těchto následujících odstavců:

Teoretická část

- rozvinutí principů funkční bezpečnosti v souvislosti s novou normou ISO 26262 v segmentu silničních vozidel
- návrh postupu hodnocení rizik v oblasti silničních vozidel
- návrh postupů, kvantitativních a kvalitativních metod, nutných k prokazování požadované úrovně funkční bezpečnosti.

Experimentální část

- praktické uplatnění postupů navržených v teoretické části vybraného celku silničního vozidla s využitím kvalitativních metod
- praktické uplatnění postupů navržených v teoretické části vybraného celku silničního vozidla s využitím kvantitativních metod

2 Základní principy funkční bezpečnosti

Bezpečnost technických zařízení je ovlivňována velkým množstvím faktorů. Významný činitel představuje spolehlivost, kdy porucha zařízení, ať systematická nebo náhodná, může mít kritický vliv na bezpečný provoz systému. Pro jednotné hodnocení bezpečnosti systémů je žádoucí existence standardů, které by zaručily konzistentní přístup ke kvalitativním i kvantitativním faktorům ovlivňujícím bezpečnost.

Principy hodnocení a prokazování funkční bezpečnosti elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností, jsou stanoveny mezinárodní normou ČSN EN 61508. Tato mateřská norma funkční bezpečnosti stanovuje přístupy hodnocení bezpečnosti hardware a software ve všech fázích životního cyklu celkové bezpečnosti od stanovení koncepce a návrhu, přes vývoj a realizaci, provoz a údržbu, až po vyřazení z provozu. V oblasti automobilového průmyslu je do činností firem postupně implementována norma ISO 26262, která respektuje mateřskou normu ČSN EN 61508 a upravuje a vysvětluje postupy funkční bezpečnosti v oblasti silničních vozidel.

Norma ISO 26262 se skládá z následujících částí:

ISO 26262-1	Road vehicles - Functional safety - Part 1: Vocabulary
ISO 26262-2	Road vehicles - Functional safety - Part 2: Management of functional safety
ISO 26262-3	Road vehicles - Functional safety - Part 3: Concept phaseMore details
ISO 26262-4	Road vehicles - Functional safety - Part 4: Product development at the system level
ISO 26262-5	Road vehicles - Functional safety - Part 5: Product development at the hardware level
ISO 26262-6	Road vehicles - Functional safety - Part 6: Product development at the software level
ISO 26262-7	Road vehicles - Functional safety - Part 7: Production and operation
ISO 26262-8	Road vehicles -- Functional safety -- Part 8: Supporting processes

ISO 26262-9	Road vehicles - Functional safety - Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
ISO 26262-10	Road vehicles -- Functional safety -- Part 10: Guideline on ISO 26262

V jednotlivých částech této normy jsou popsány doporučené činnosti, vedoucí ke zvýšení bezpečnosti silničních vozidel zejména z pohledu bezpečnosti elektrických, elektronických nebo elektronických programovatelných systémů (E/E/PE).

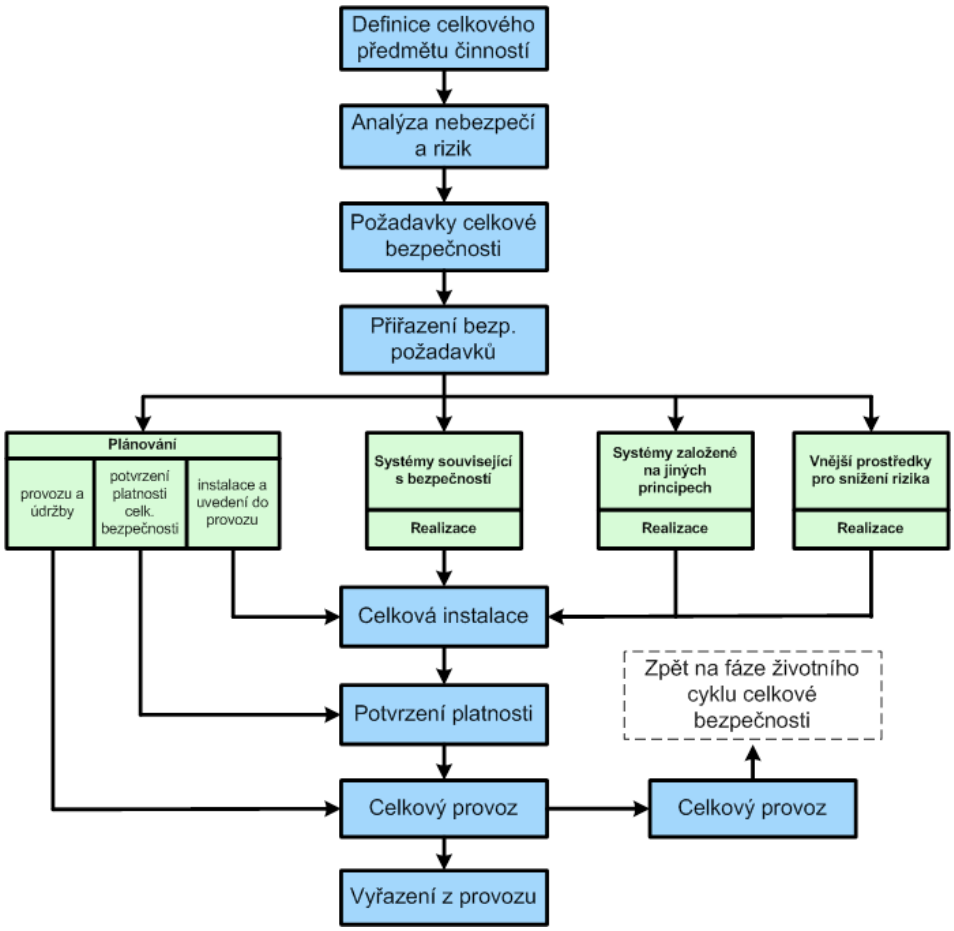
Hlavním cílem použití systémů souvisejících s bezpečností je snížení rizika vyplývajícího z činnosti zařízení prostřednictvím aplikace ochranných systémů, založených na různých technických principech.

Požadovaná úroveň funkční bezpečnosti u výše uvedených systémů je zajišťována realizací bezpečnostních funkcí. Specifikace bezpečnostních požadavků na tyto funkce je provedena na základě analýzy rizika systému, přiřazením cílové úrovně integrity bezpečnosti (ASIL). Pro jednotlivé úrovně integrity bezpečnosti jsou specifikovány konkrétní hodnoty cílové míry poruch, které jsou požadovány pro zajištění stanovené úrovně bezpečnosti systému.

Normy jsou zaměřeny cíleně pro systémy související s bezpečností, jestliže jsou založeny na principu elektrických, elektronických nebo elektronických programovatelných systémů (E/E/PE). Její použití je vhodné zejména v případě, kdy porucha těchto systémů by mohla mít dopad na bezpečnost osob nebo okolního prostředí, případně by porucha mohla způsobit vážné ekonomické následky [21].

2.1 Životní cyklus celkové bezpečnosti

Technický rámec pro aplikaci funkční bezpečnosti u systémů souvisejících s bezpečností je zajištěn prostřednictvím životního cyklu celkové bezpečnosti, který je zobrazen na obr. 2.1. Provádění činností v jednotlivých fázích tohoto cyklu je zajišťováno prostřednictvím managementu funkční bezpečnosti, který je zaměřen zejména na strategii dosažení funkční bezpečnosti, odpovědnost osob a organizací za provádění a kontrolu aktivit, vedení dokumentace, analýzu vzniklých nebezpečných událostí, sledování provozu a údržby zařízení, organizaci prověrek funkční bezpečnosti apod.



Zdroj: ISO 26262

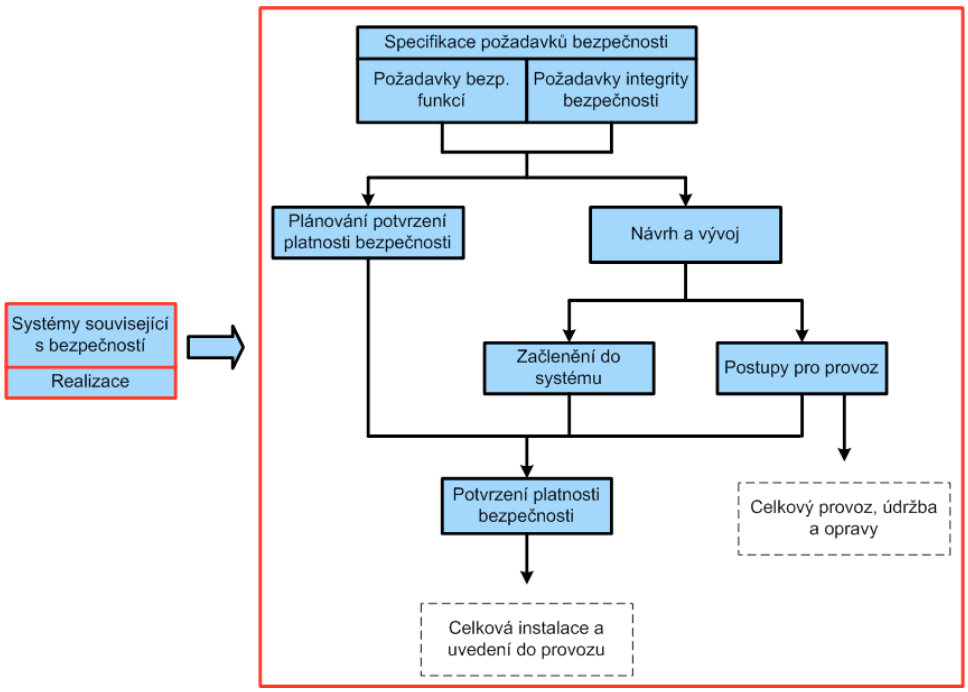
Obr. 2.1 Životní cyklus celkové bezpečnosti

Přestože se normy, jak bylo řečeno výše, zaměřují na systémy souvisejícími s bezpečností založenými na principu elektrických, elektronických nebo programovatelných elektronických systémů (E/E/PE systémy), jsou v životním cyklu celkové bezpečnosti zahrnuty také systémy související s bezpečností, založené na jiných technických principech a vnější prostředky pro snížení rizika, jejichž součinnost vede k efektivnímu snížení rizika systému na přijatelnou úroveň.

Požadavky funkční bezpečnosti, vyplývající z jednotlivých fází životního cyklu celkové bezpečnosti pro E/E/PE systémy, jsou stanoveny zvlášť jak pro hardware, tak i pro software systémů souvisejících s bezpečností. Životní cyklus hardware E/E/PE systémů je uveden na obr. 2.2 [13].

Systémy související s bezpečností založené na principu E/E/PE systémů jsou určeny ke snížení rizika tzv. řízených zařízení (EUC) s vlastním systémem řízení. Pokud není systém související s bezpečností oddělený a nezávislý na systému řízení EUC, pak i systém řízení

EUC musí být řešen jako systém související s bezpečností. Požadavky na funkční bezpečnost vycházejí z důkladného poznání a analyzování řízeného zařízení (EUC).



Zdroj: ISO 26262

Obr. 2.2 Životní cyklus hardware E/E/PE systémů

Jednotlivé fáze životního cyklu celkové bezpečnosti mají definované cíle a požadavky, které se aplikují pro E/E/PE systémy za účelem zajištění jejich funkční bezpečnosti. Pro každou fázi cyklu se musí stanovit ověřovací plán, pomocí kterého se prokáže (posouzením, analýzou, zkouškami), že výstupy fáze splňují všechny stanovené cíle a požadavky.

V úvodních fázích životního cyklu celkové bezpečnosti, tj. stanovení koncepce a definování zařízení, je vymezeno řízené zařízení (EUC), jeho prostředí (fyzické, legislativní apod.) a jsou stanoveny hranice EUC a systému řízení EUC.

Výše uvedené informace představují vstupní údaje pro analýzu nebezpečí a rizik EUC a systému řízení EUC, včetně zahrnutí chyb lidského činitele. Cílem této analýzy je definování nebezpečí a nebezpečné události ve všech režimech provozu pro všechny předvídatelné okolnosti (včetně poruchových podmínek a nesprávného použití). Mimo to by analýza měla zahrnovat kvalitativní nebo kvantitativní klasifikaci rizika na základě důsledků nebezpečných událostí a opatření ke snížení nebo odstranění nebezpečí a rizik, založené na vnějších prostředcích, případně běžné technické praxi.

Ve fázi stanovení požadavků celkové bezpečnosti je každému určenému nebezpečí přiřazena bezpečnostní funkce pro zajištění požadované funkční bezpečnosti. Bezpečnostní funkce jsou realizovány systémy souvisejícími s bezpečností, založenými na principu E/E/PE systémů nebo na jiných technických principech, čímž se dosáhne nutného snížení rizika řízeného zařízení (EUC).

Ve fázi přiřazení bezpečnostních požadavků jsou specifikované bezpečnostní funkce přiřazeny jednotlivým systémům souvisejícím s bezpečností a jsou pro ně stanoveny úrovně integrity bezpečnosti. Pokud aplikací systémů souvisejících s bezpečností na principu E/E/PE systémů, případně aplikací systémů založených na jiných principech nebo vnějších prostředků pro snížení rizika, nelze dosáhnout nutného snížení rizika EUC, musí se navržené bezpečnostní systémy modifikovat a proces daný touto fází se musí opakovat.

Na základě návrhu systémů souvisejících s bezpečností, vycházejícího z předešlých fází životního cyklu celkové bezpečnosti, je možné přistoupit k realizaci E/E/PE systémů. Současně s touto fází probíhá sestavení plánu pro instalaci systémů E/E/PE v rámci řízeného zařízení (EUC) a tvorba plánu provozu a údržby systémů E/E/PE, s cílem dosažení a udržení požadované funkční bezpečnosti. Ve fázi plánování je také vytvořen plán pro potvrzení platnosti celkové bezpečnosti z hlediska bezpečnostních požadavků a integrity bezpečnosti systémů E/E/PE [21].

Po instalaci zařízení a jeho uvedení do provozu je podle sestaveného plánu provedeno potvrzení platnosti celkové bezpečnosti. Cílem je prokázat, že E/E/PE systémy související s bezpečností splňují požadavky celkové bezpečnosti. Při prokazování musí být doložena dokumentace k předešlým fázím životního cyklu celkové bezpečnosti a informace o provedení zkoušky bezpečnostní funkce (podmínky a postupy zkoušení, použité nástroje a zařízení, výsledky zkušebních činností). Při neshodách mezi očekávanými a skutečnými výsledky je nutné provést analýzu, na jejímž základě se rozhodne o pokračování potvrzování platnosti, nebo se zažádá o změnu a navrátí se zpět k předchozímu kroku prokazování platnosti celkové bezpečnosti.

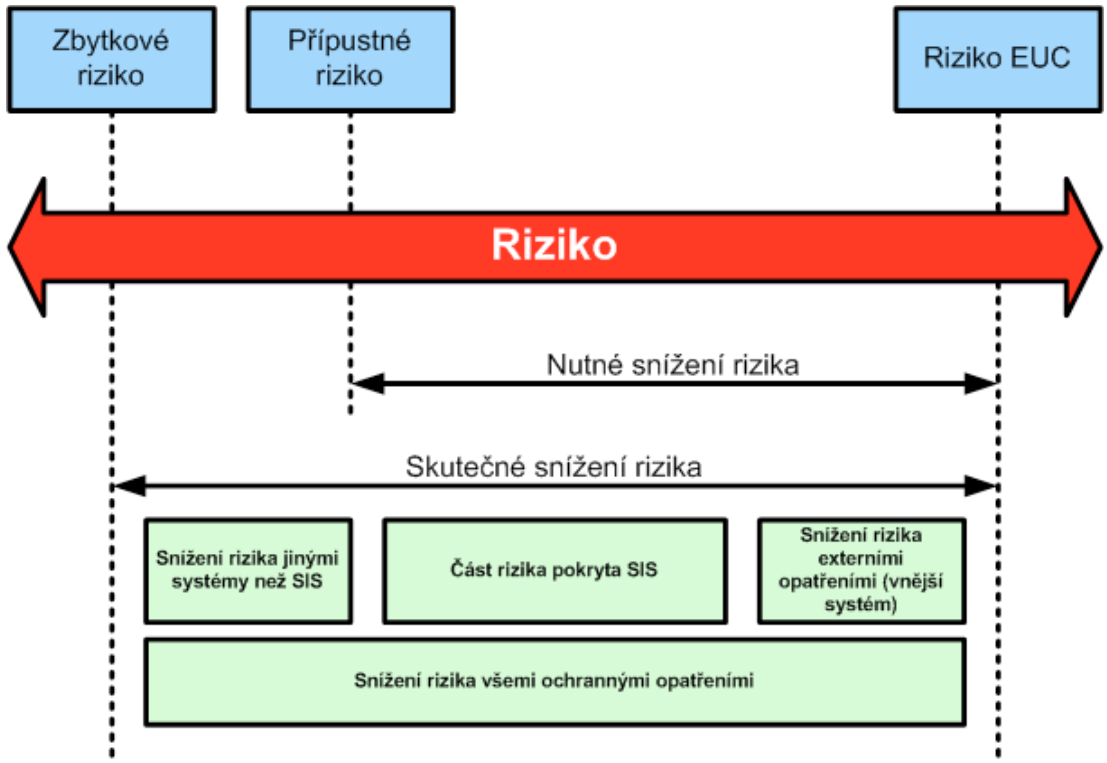
Po potvrzení platnosti celkové bezpečnosti je možné uvedení řízeného zařízení EUC s E/E/PE systémy související s bezpečností do běžného provozu, během kterého se provádí údržba a opravy zařízení v souladu s vytvořeným plánem tak, aby byla udržena požadovaná funkční bezpečnost. Pokud během provozu zařízení dojde ke snížení funkční bezpečnosti pod dovolenou úroveň, případně nastanou změny v bezpečnostní legislativě, nebo je provedena modifikace řízeného zařízení (EUC), je nutné přistoupit k modifikaci systémů souvisejících

s bezpečností. Tyto změny jsou spojeny s nutností provést znovu činnosti v předchozích fázích životního cyklu, které jsou modifikací dotčeny.

2.2 Rizika a jejich snižování

Smyslem systémů souvisejících s bezpečností je snížení rizika řízených zařízení (EUC) na přijatelnou úroveň. Tato úroveň rizika je definována požadovanou úrovní integrity bezpečnosti, které má být pro daný bezpečnostní systém dosaženo. Snížení rizika je u těchto systémů realizováno snížením četnosti nebezpečných událostí a současně zmírněním jejich následků.

Snížení rizika na přípustnou úroveň u řízeného zařízení (EUC), systému řízení EUC a vlivu lidského činitele, založené na principu systémů souvisejících s bezpečností, spočívá ve snížení existujícího rizika (bez předpokladu jakýchkoliv bezpečnostních opatření) minimálně na společensky přijatelnou úroveň. Toho je dosahováno použitím kombinace ochranných prvků, založených na principu E/E/PE systémů souvisejících s bezpečností, systémů založených na jiných technických principech a vnějších prostředků pro snížení rizika, viz obr. 2.3.



Zdroj: EN 61508

Obr. 2.3 Princip nutného snížení rizika

U E/E/PE systémů souvisejících s bezpečností je snížení rizika na přijatelnou úroveň realizováno prostřednictvím následujících činností [24]:

- realizace požadované bezpečnostní funkce nutné pro dosažení nebo udržení bezpečného stavu u řízeného zařízení (EUC),
- dosažení nutné integrity bezpečnosti pro bezpečnostní funkci (samostatně nebo v součinnosti s ostatními bezpečnostními systémy), zajišťující dostatečně nízkou pravděpodobnost nebezpečných událostí a omezení jejich následků.

Pro přiřazení bezpečnostních požadavků systémů souvisejících s bezpečností, tj. bezpečnostních funkcí a úrovně integrity bezpečnosti (ASIL), se využívá řada metod, založených na různých principech (viz kap. 3).

2.3 Úroveň integrity bezpečnosti

Určující parametr funkční bezpečnosti E/E/PE systémů představuje úroveň integrity bezpečnosti ASIL – Automotive Safety Integrity Level. Integrita bezpečnosti má stanoveny čtyři hladiny od ASIL A až po ASIL D, přičemž vyšší hodnota představuje vyšší úroveň funkční bezpečnosti systému. Přiřazení úrovně integrity bezpečnosti u E/E/PE systémů, případně systémů založených na jiných technických principech, se provádí tak, aby se u daného systému souvisejícího s bezpečností dosáhlo snížení rizika na přijatelnou úroveň.

Ukazatel ASIL charakterizuje integritu bezpečnosti systémů E/E/PE, která vyjadřuje pravděpodobnost, že systém související s bezpečností plní požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu [23]. Integrita bezpečnosti zahrnuje jak integritu bezpečnosti hardware (týkající se náhodných nebezpečných poruch systému), tak i systematickou integritu bezpečnosti (související se systematickými poruchami systému).

Úroveň integrity bezpečnosti je prokazována parametrem zvaným cílová míra poruch, respektive cílová intenzita poruch. Hodnoty cílové míry poruch pro jednotlivé úrovně integrity bezpečnosti (ASIL) jsou uvedeny v tab. 2.1. dle *ISO 26262.*

Tab 2.1 Cílová míra poruch pro úrovně integrity bezpečnosti

Úroveň integrity bezpečnosti (ASIL)	**Cílová míra poruch [h^{-1}]**
ASIL D	$< 10^{-8}$
ASIL C	$< 10^{-7}$
ASIL B	$< 10^{-7}$
ASIL A	$< 10^{-6}$

Bezpečnostní funkce nemusí být realizována pouze jedním systémem, ale mnohdy je zajímavé a výhodné rozdělit její fungování mezi více E/E/PE systémů. Systém související s bezpečností je pak realizován dvěma nebo více subsystémy, jež mají svou logickou a funkční strukturu. Požadovaná úroveň integrity bezpečnosti (ASIL) je následně dosažena pomocí redukce architektury hardware [22]. Tento postup je v ISO 26262 nazván „dekompozice ASIL“. Redukce architektury je primárně závislá na typu soustavy, ze které je systém související s bezpečností tvořen.

Sériová architektura

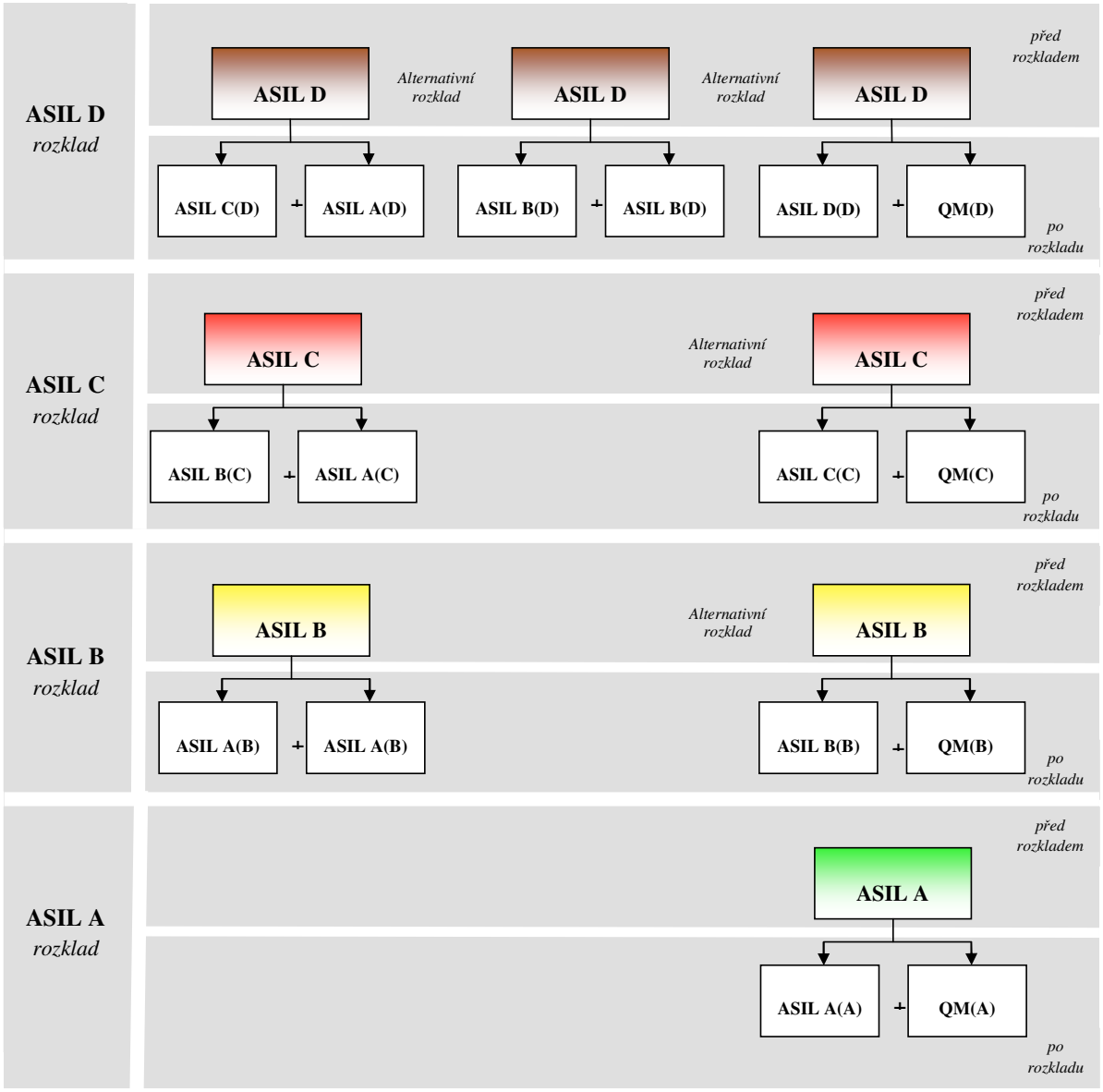
Bezpečnostní funkce je realizována u sériové architektury jediným kanálem a tedy k selhání bezpečnostní funkce při poruše jakéhokoliv tvořícího prvku (subsystému). Nejvyšší úroveň integrity bezpečnosti (ASIL), kterou je možno v tomto případě získat, je limitována nejnižší hodnotou úrovně integrity bezpečnosti ASIL tvořícího prvku (subsystému).

Paralelní architektura

Bezpečnostní funkce je realizována u paralelní architektury prostřednictvím dvou nebo více kanálů. Jestliže dojde k poruše tvořícího prvku (subsystému) v jednom kanálu, je možno zajistit zafungování bezpečnostní funkce dalšími tvořícími prvky (subsystémy) v dalších kanálech (typicky dvou). Zde se uplatní již zmiňovaná „dekompozice ASIL“, jejíž příklady je možno vidět na obr. 2.4.

Typické E/E/PE systémy související s bezpečností jsou obvykle tvořeny větším počtem subsystémů. Tyto mohou být reprezentovány subsystémy vstupů (senzorů), subsystémy logických bloků, subsystémy výstupů (akčních členů) apod. v jednokanálovém, případně vícekanálovém uspořádání.

Využitím obou výše uvedených přístupů omezení architektury hardware lze stanovit požadavek na úroveň integrity bezpečnosti systémů souvisejících s bezpečností tvořených libovolným počtem subsystémů v různém uspořádání kanálů zajišťujících bezpečnostní funkci. Postupnou redukcí architektury hardware lze stanovit maximální hodnotu ASIL, kterou daný systém související s bezpečností může dosáhnout.



Zdroj: ISO 26262

Obr. 2.4: Paralelní uspořádání subsystémů – dekompozice ASIL

2.4 Celkový postup procesu uplatnění principů funkční bezpečnosti

Na základě představených základních principů funkční bezpečnosti je tedy nutno navrhnout kroky, vedoucí k naplnění základního cíle. Tento základní cíl spočívá v uskutečnění jasně definovaných činností, takových, které umožní dosáhnout požadovanou bezpečnost systému.

Prvním předpokladem naplnění tohoto cíle je nutné vykonat činnosti ve fázi, jíž je možno vzhledem k jejímu charakteru nazvat částí analytickou.

Analytická fáze

Činnosti, prováděné během této fáze, by měly být uskutečňovány již v návrhové fázi života výrobku, z důvodu nutnosti minimalizovat úpravy jeho konstrukce a snížit tak počet nápravných opatření v průběhu výroby. Proto je nutno této fázi věnovat prioritní pozornost a péči. Je nutné poukázat na to, že se jedná o vysoce kvalifikovanou a týmovou činnost.
V rámci analytické fáze se provádějí následující kroky:

- identifikace nebezpečí, spojených s provozem zařízení, tato ohodnotit a určit úroveň integrity bezpečnosti ASIL pro zvažovaná nebezpečí
- analýza rizik pomocí vhodných metod a tato ohodnotit
- navrhnout potřebná bezpečnostní opatření, typicky technická (bezpečnostní funkce), údržbová, organizační a legislativní, případně vnější ochranný systém
- zhodnotit účinnost navržených opatření, tedy opakovat analýzu rizik
- stanovit dosažení úrově integrity bezpečnosti ASIL pro navržené bezpečnostní funkce

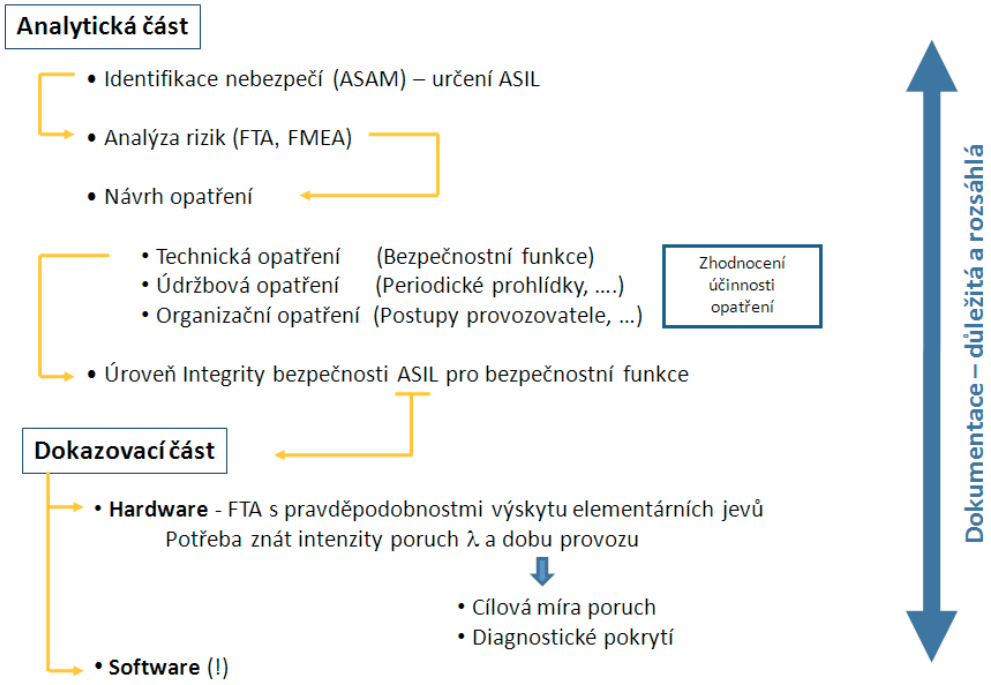
Návaznost činností v analytické části je možno v grafické formě spatřit v odpovídajícím segmentu na obr. 2.5.

Dokazovací fáze

Činnosti, prováděné během této fáze, vedou k prokázání parametrů spolehlivosti systému, takových, aby byly naplněny požadavky na snížení míry rizika a byla dosažena požadovaná bezpečnost systému. Tato fáze musí obsahovat potřebné výpočty pro prokázání požadované cílové míry poruch, včetně návrhu zkoušek.

Návaznost činností v dokazovací části je možno v grafické formě spatřit v odpovídajícím segmentu na obr. 2.5.

Na obr. 2.5 je v pravé části svislá modrá šipka s legendou. Popisuje nutnou, důležitou a rozsáhlou část práce, která se váže na potřebu vhodným způsobem dokumentovat všechny uskutečněné činnosti spojené s procesem funkční bezpečnosti. Této dokumentační a organizační části se věnuje oblast „Managementu funkční bezpečnosti“.



Zdroj: autor

Obr. 2.5 Celkový postup procesu funkční bezpečnosti

Management funkční bezpečnosti

Management funkční bezpečnosti lze chápat jako ucelený soubor přístupů, názorů, zkušeností a metod zajišťující účinnou realizaci technických požadavků, které jsou zaměřeny na dosažení a udržení funkční bezpečnosti systémů souvisejících s bezpečností.

Cíle managementu funkční bezpečnosti jsou následující:

- stanovení managementových a technických činností prováděných během fází životního cyklu celkové bezpečnosti, bezpečnosti E/E/PES a bezpečnosti softwaru, které jsou nutné pro dosažení požadované funkční bezpečnosti E/E/PE systémů souvisejících s bezpečností,
- stanovení odpovědnosti osob, oddělení a organizací zodpovědných za každou fázi životního cyklu celkové bezpečnosti, bezpečnosti E/E/PES a bezpečnosti softwaru nebo za činnosti v každé fázi prováděné,
- vytvoření postupů zajišťující, že nebezpečná událost bude analyzována a následně přijata opatření pro minimalizaci jejího opakovaného výskytu,
- vytvoření dokumentace funkční bezpečnosti – součást důkazů bezpečnosti.

Management funkční bezpečnosti musí zajistit:

- Začlenění managementu funkční bezpečnosti do organizační struktury společnosti,

- Identifikaci osob, oddělení a organizací (dodavatelé) odpovědných za provádění a kontrolování fází životního cyklu funkční bezpečnosti,
- Určení použitých fází životního cyklu funkční bezpečnosti (dle složitosti projektu).
- Způsob členění a rozsah dokumentovaných informací (součást ISO),
- Stanovit opatření a techniky použité pro splnění požadavků na posuzování funkční bezpečnosti.

Návrhy základních formulářů z oblasti managementu funkční bezpečnosti jsou uvedeny v příloze I. Jedná se o příklady formulářů, jelikož existuje jistá míra obecnosti při jejich sestavování, nicméně realizace vždy závisí na konkrétních podmínkách firmy.

3 Posuzování funkční bezpečnosti - kvalitativní metody

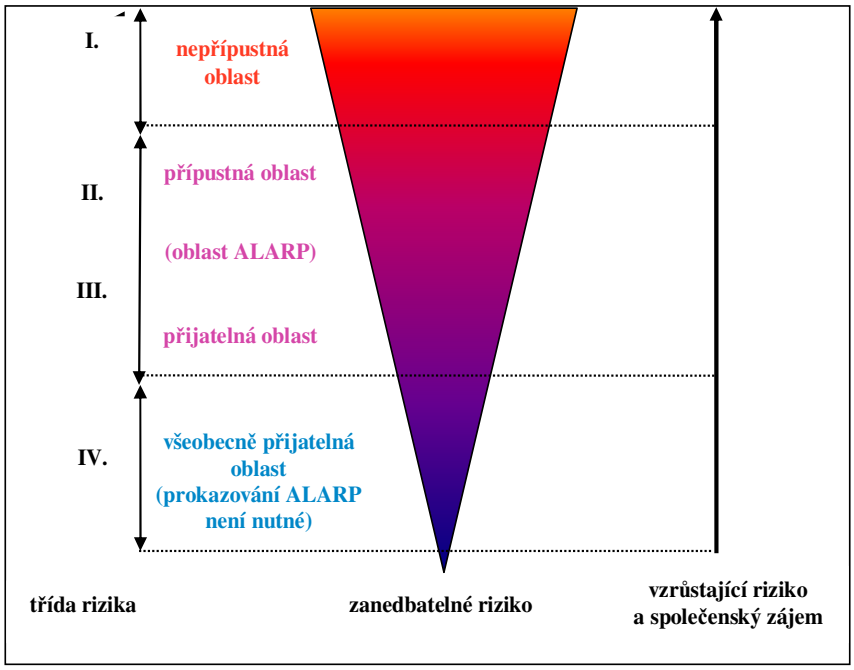
V této kapitole budou představeny metody, jež jsou využitelné převážně ve fázi analytické, tedy ve fázi kdy je nutno rizika identifikovat, posoudit a ohodnotit tak, aby mohla být navržena potřebná vhodná opatření pro jejich snížení a posouzen účinek takto navržených opatření (viz obr 2.5).

3.1 Metoda ALARP

Pomocí přístupu ALARP (As Low As Reasonably Practicable) je kategorizace rizika ohodnocena do třech různých stupňů následovně [21]:

- dané riziko je tak velké, že je nutné jej zcela odmítnout, (oblast I)
- dané riziko je tak malé (nebo bylo tak zmenšeno), že je bezvýznamné, (oblast IV)
- dané riziko je mezi dvěma předchozími stavy a už bylo sníženo na nejnižší možnou úroveň, s přihlédnutím na přínosy, které plynou z jeho přijetí a se zvážením nákladů na jakékoliv jeho další snížení. (oblast II, III)

Uvedený přístup je možné také uvést v příslušné grafické podobě, jak je možno vidět na obr. 3.1.



Zdroj: EN 61508

Obr. 3.1 Grafická podoba přístupu ALARP

V grafické interpretaci přístupu ALARP se dle definice objevují tři, respektive čtyři oblasti, do kterých posuzovaná rizika spadají. Na základě konkrétní pozice posuzovaného rizika jsou poté přijata opatření pro jeho žádoucí snížení. Bližší definice jednotlivých tříd rizika jsou uvedeny v tab. 3.1.

Tab. 3.1 Definice jednotlivých tříd rizika

Třída I.	Nepřípustné riziko
Třída II.	Nežádoucí riziko, přípustné pouze v případě, že snížení rizika je neproveditelné nebo v případě, že náklady jsou výrazně neúměrné dosaženým zlepšením
Třída III.	Přípustné riziko v případě, že náklady na jeho snížení by přesáhly dosažené zlepšení
Třída IV.	Zanedbatelné riziko

Přístup ALARP představuje základní filozofický náhled na práci s riziky a promítá se tak do všech činností a úvah při posuzování funkční bezpečnosti dopravních prostředků. Cílem je využít takové nástroje, postupy a opatření, aby pokud možno všechna rizika hodnoceného systému splňovala třídy IV. v tab. 3.1 a byla tedy zanedbatelná.

3.2 Diagram rizika

Diagram rizika představuje kvalitativní metodu umožňující určení úrovně integrity bezpečnosti systémů (SIL/ASIL) souvisejících s bezpečností na základě rizikových činitelů spojených se systémem. Je uveden jako doporučený postup normou ČSN EN 61508.

Princip metody diagramu rizika

Metoda zavádí několik parametrů, které dohromady charakterizují základní vlastnosti nebezpečné situace v případě selhání systému souvisejícího s bezpečností. Princip metody je založen na rovnici (3.1):

$$R = f \cdot C \tag{3.1}$$

kde:
R - riziko bez systémů souvisejících s bezpečností,
f - četnost výskytu nebezpečné události bez systémů souvisejících s bezpečností,
C - následek nebezpečné události.

Na základě uvedené rovnice (3.1) se vyhodnocují následující čtyři parametry rizika:

- následek nebezpečné události (C),

- režim vyžádání funkce způsobující nebezpečnou událost (F),
- možnost se vyhnout nebezpečné události (P),
- pravděpodobnost nežádoucího výskytu (W) – bez přidání jakýchkoliv systémů souvisejících s bezpečností, ale s použitím vnějších prostředků pro snížení rizika.

Pro hodnocení rizika s využitím metody diagramu rizika byly s ohledem na charakter systému definovány následující kategorie parametrů rizika (viz tab. 3.2, tab. 3.3, tab. 3.4 a tab. 3.5).

Tab. 3.2 Následek nebezpečné události

Parametr	Zkr.	Popis
Následek (C)	C1	menší zranění
	C2	zranění více osob s trvalými následky, smrt jedné osoby
	C3	smrt několika osob
	C4	smrt velkého počtu osob

Tab. 3.3 Režim vyžádání funkce

Parametr	Zkr.	Popis
Režim vyžádání funkce (F)	F1	vzácná a častější doba funkce
	F2	častá až trvalá doba funkce

Tab. 3.4 Možnost se vyhnout nebezpečné události

Parametr	Zkr.	Popis
Možnost se vyhnout nebezpečné události (P)	P1	možné za určitých podmínek
	P2	téměř nemožné

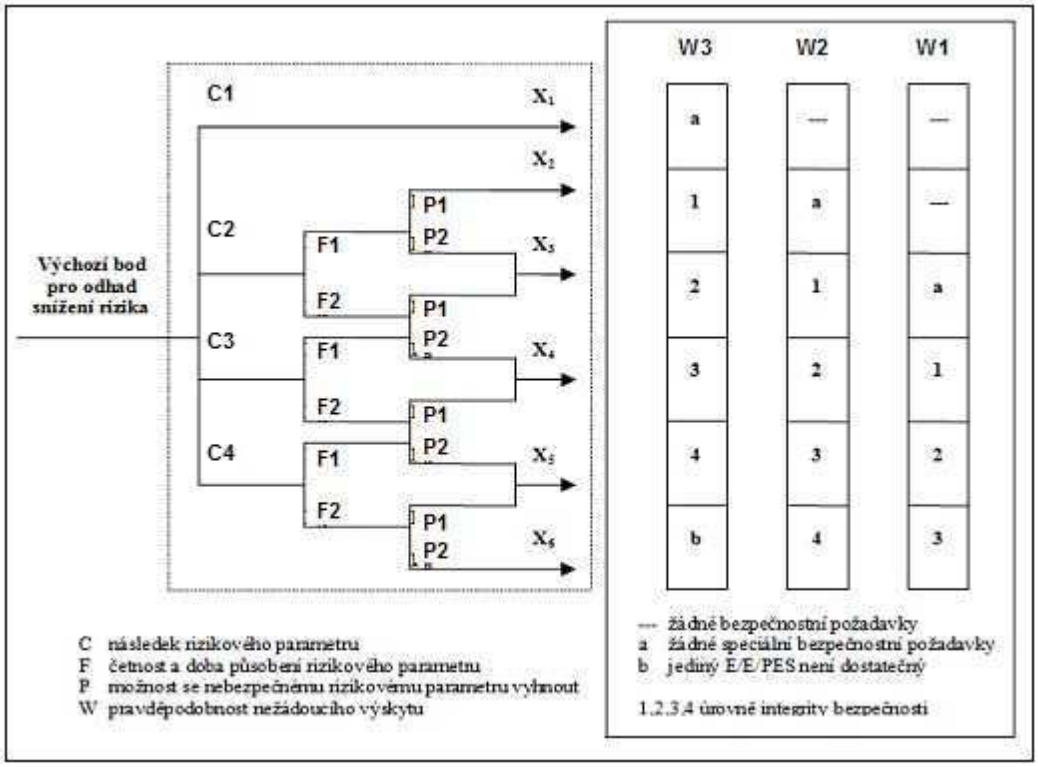
Pro možnost volby P1 (vyhnutí nebezpečné události za určitých podmínek) musí být splněny všechny následující předpoklady:

- upozornění obsluhy vnějšími prostředky, že systém selhal,
- možnost zabránění nebezpečné události,
- dostatečná doba k zabránění nebezpečné události.

Tab. 3.5 Pravděpodobnost nežádoucího výskytu

Parametr	Zkr.	Popis
Pravděpodobnost nežádoucího výskytu (W)	W1	velmi malá
	W2	malá
	W3	poměrně vysoká

S využitím výše uvedeného hodnocení se následně prochází vlastní diagram rizika (obr. 3.2), s cílem dospět k určení požadované hodnotě integrity bezpečnosti SIL/ASIL pro hodnocený objekt.



Zdroj: EN 61508

Obr. 3.2 Diagram rizika

Norma EN 61508 stanovuje 4 hladiny integrity bezpečnosti od nejslabší po nejsilnější úroveň SIL1, SIL2 , SIL3, SIL4. Norma ISO 26262 stanovuje podobně 4 hladiny integrity bezpečnosti od nejslabší po nejsilnější úroveň adekvátně k EN 61508, ale označování modifikuje vzhledem k automobilům na ASIL A, ASIL B, ASIL C, ASIL D.

3.3 Klasifikace nebezpečí (ISO 26262)

Podobnou funkci, jako zmíněná metoda Digramu rizika (viz kap. 3.2), plní identifikace nebezpečí a jejich klasifikace uvedena v normě ISO 26262–3. Umožňuje ohodnotit jednotlivá nebezpečí a určit pro ně úroveň integrity bezpečnosti ASIL. Je založena na hodnocení následujících parametrů:

- potenciální závažnost (S)
- pravděpodobnost vystavení se nebezpečné situaci (E)
- kontrolovatelnost situace (C)

Potenciální závažnost (S)

V této klasifikaci se hodnotí potenciální závažnost pro účastníka silničního provozu spojená s identifikovaným nebezpečím. Klasifikace je uvedena v tab. 3.6.

Tab. 3.6 Potenciální závažnost

Třída	**S0**	**S1**	**S2**	**S3**
Popis	Bez zranění	Lehké zranění	Těžké zranění (přežití pravděpodobné)	Těžké zranění, smrt

Pravděpodobnost vystavení se nebezpečné situaci (E)

V této klasifikaci se hodnotí pravděpodobnost vystavení se nebezpečné situaci pro účastníka silničního provozu spojená s identifikovaným nebezpečím. Klasifikace je uvedena v tab. 3.7.

Tab. 3.7 Pravděpodobnost vystavení se nebezpečné situaci

Třída	**E0**	**E1**	**E2**	**E3**	**E4**
Popis	Neuvěřitelně malá	Velmi malá	Malá	Střední	Vysoká

Kontrolovatelnost situace (C)

V této klasifikaci se hodnotí kontrolovatelnost situace řidičem nebo jinými účastníky silničního provozu spojená s identifikovaným nebezpečím. Klasifikace je uvedena v tab. 3.8.

Tab. 3.8 Kontrolovatelnost situace

Třída	**C0**	**C1**	**C2**	**C3**
Popis	Všeobecně kontrolovatelná	Jednoduše kontrolovatelná	Normálně kontrolovatelná	Těžce kontrolovatelná nebo nekontrolovatelná

Pro každé nebezpečí poté může být určena úroveň integrity bezpečnosti ASIL s využitím konkrétního hodnocení parametrů. K určení úrovně integrity bezpečnosti ASIL pak může být

využita tab. 3.9. Dle popsané metodiky jsou tedy definovány (dle tab. 3.8) čtyři úrovně integrity bezpečnosti, a to ASIL A, ASIL B, ASIL C a ASIL D. Úroveň ASIL D přitom stanoví nejpřísnější požadavky na zajištění bezpečnosti a úroveň ASIL A přitom stanoví nejjednodušší požadavky na zajištění bezpečnosti.

Tab. 3.9 Přiřazení úrovně integrity bezpečnosti ASIL

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	B	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

V tab. 3.9 identifikovatelná úroveň QM (Quality Management) nestanovuje žádné požadavky podle ISO 26262.

3.4 Identifikace a klasifikace nebezpečí ASAM

Identifikace a hodnocení nebezpečí je prvním a nejdůležitějším krokem spojeným s hodnocením rizik dopravního prostředku, jeho subsystému nebo jeho komponentu. V úvahu je třeba brát všechna nebezpečí, která se mohou v provozu vyskytnout. Na identifikaci nebezpečí by se tedy měli podílet jak konstruktéři, tak také pracovníci znalí provozního nasazení vozidla.

Nově předkládaný postup klasifikování funkcí byl vyvinut s podporou ČSN EN 61508 a ISO 26262 a slouží ke kvalitativnímu klasifikování identifikovaných nebezpečí s ohledem na jejich vztah k bezpečnosti, tzv. stupněm požadavku na integritu bezpečnosti (SIL/ASIL). Klasifikace nebezpečí využívá nově navržený postup, který umožňuje dle mého názoru vhodné kvalitativní hodnocení pro automobilový průmysl. Umožňuje zároveň přímé přiřazení

požadavků na integritu bezpečnosti ASIL, jelikož v sobě integruje také metodu Diagramu rizika (viz kap 3.2) a klasifikaci nebezpečí dle ISO 26262 (viz kap. 3.3).

Pro provedení identifikace a hodnocení nebezpečí byl autorem nově navržen integrovaný postup ASAM (Automotive Safety Assesment Method), jež umožňuje přehledné a lépe algoritmizovatelné činnosti. Pro identifikaci a hodnocení nebezpečí dle postupu ASAM jsou použity následující parametry:

- škody (S)
- pravděpodobnost výskytu (W)
- čas trvání (E)
- možnost zamezení (V)

Aby klasifikování bylo konzistentní a reprodukovatelné, jsou v dalším textu shora uvedené parametry definovány podrobněji:

Škody (S)

Škodami (S) se označují následky nebezpečí, které bylo identifikováno v souvislosti s provozem a údržbou vozidla. U každého nebezpečí je klasifikována největší možná reálná škoda, která na základě nebezpečí může vzniknout. Škoda je tvořena součinem počtu postižených osob (Sa) a zranění těchto osob (Sv) dle vztahu (3.2). Klasifikace škod je uvedena v tab. 3.10

$$S = S_a \cdot S_v \tag{3.2}$$

kde:
S_a - počet poškozených osob
S_v - stupeň zranění

Tab. 3.10 Klasifikace škod

Škody (S) = S_a x S_v	
Počet S_a	
jeden	1 osoba
více	$1 < x \leq 10$ osob
mnoho	> 10 osob
Stupeň zranění S_v	
lehké zranění	Nebezpečí vede k nehodě s lehkými poraněními (pohmožděniny, zlomeniny) pod 2 dny pobytu v nemocnici a bez nevratných následných škod
těžké zranění	Nebezpečí vede k nehodě s nejméně dvoudenním pobytem v nemocnici a/nebo nevratným následným poškozením (až do 50% omezení)
smrt	Nebezpečí vede k nehodě se smrtelnými poraněními (smrt nastane do 30 dnů po nehodě) či k okamžité smrti

Číselné hodnocení počtu poškozených osob a stupeň zranění je uveden v tab. 3.6. Volí se výhradně z konkrétních hodnot v tab. 3.6, nezadávají se libovolné hodnoty.

Pravděpodobnost vzniku poškození osob (W)

Zhodnocení pravděpodobnosti, zda nastane předpokládaný rozsah škod po selhání funkce, např. zda selhání světel povede k nehodě. Klasifikace pravděpodobnosti vzniku poškození osob je uvedena v tab. 3.11.

Tab. 3.11 Klasifikace pravděpodobnosti vzniku poškození osob

Pravděpodobnost vzniku poškození osob (W)	
nízká	Pravděpodobnost vzniku je nízká, když rozsah škod po selhání funkce je téměř vyloučen
střední	Pravděpodobnost vzniku je střední, když rozsah škod po selhání funkce není ani téměř vyloučen, ani že nutně nastane
vysoká	Pravděpodobnost vzniku je vysoká, když rozsah škod po selhání funkce se téměř nutně vyskytne

Číselné hodnocení pravděpodobnosti výskytu je uvedeno v tab. 3.14. Volí se výhradně z konkrétních hodnot v tab. 3.14, nezadávají se libovolné hodnoty.

Čas vystavení (E)

Vyhodnocení doby trvání nebezpečí (času vystavení) – jak dlouho jsou lidé vystavení nebezpečí. Například při nastupování/vystupování je doba vystavení nebezpečí krátká, při jízdě vozidla jsou lidé vystavení nebezpečí vzniku požáru trvale – doba dlouhá. Klasifikace času vystavení je uvedena v tab. 3.12.

Tab. 3.12 Klasifikace času vystavení

Čas vystavení (E)	
krátká	Čas vystavení je krátký, když tento je malý v porovnání k celkové době pobytu v prostoru vozidla
dlouhá	Čas vystavení je dlouhý, když po převážnou dobu pobytu v prostoru vozidla je vystaven potřebě ochrany před možným primárním nebezpečím

Číselné hodnocení času vystavení je uvedeno v tab. 3.14. Volí se výhradně z konkrétních hodnot v tab. 3.14, nezadávají se libovolné hodnoty.

Zamezení (V)

Vyhodnocení možnosti zamezení rozsahu škod postižených osob po vzniku nebezpečí (např. možnost útěku z hořícího vozidla). Klasifikace zamezení je uvedena v tab. 3.13.

Tab. 3.13 Klasifikace zamezení

Zamezení (V)	
není možné	Ohrožená osoba nemá žádnou možnost škodám zamezit
možné	Ohrožená osoba má vlastní ovladatelné možnosti škodám zabránit či je zmenšit, musí existovat možnost identifikace hrozícího nebezpečí

Číselné hodnocení zamezení je uvedeno v tab. 3.14. Volí se výhradně z konkrétních hodnot v tab. 14, nezadávají se libovolné hodnoty.

Na základě výše uvedeného slovního hodnocení jsou jednotlivým klasifikacím přiřazeny konkrétní hodnoty pro výpočet. Konkrétní hodnoty jsou uvedeny v tab. 3.14.

Tab. 3.14 Přiřazení konkrétních hodnot slovnímu hodnocení

Parametr škody (S)			
Počet S_a		**Stupeň zranění S_v**	
jeden	3	lehké zranění	2
více	5	těžké zranění	4
mnoho	8	smrt	9
Parametr pravděpodobnosti (W)			
nízká		1	
střední		1,7	
vysoká		3	
Parametr čas výskytu (E)			
krátká		1	
dlouhá		1,3	
Parametr zamezení (V)			
není možné		1	
možné		1,7	

Zjištění požadavku na úroveň integrity bezpečnosti (ASIL)

Z výše uvedených parametrů se spočítá takzvaný klasifikační indikátor podle následujícího vztahu (3.3).

$$I = (S_a \cdot S_v \cdot W \cdot E) / V \tag{3.3}$$

kde:
I - klasifikační indikátor
S_a - počet poškozených osob
S_v - stupeň zranění
W - pravděpodobnost vzniku poškození osob
E - čas vystavení
V - zamezení

Funkce je na základě spočítaného klasifikačního indikátoru I zařazena (klasifikována) do příslušného stupně požadavku na integritu bezpečnosti (ASIL). Konkrétní přiřazení je uvedeno v tab. 3.15.

Klasifikace se zapisuje do formuláře Záznam o nebezpečí. Záznam o nebezpečí používá nejen stupeň integrity bezpečnosti, ale také slovní hodnocení kritičnosti jednotlivých nebezpečí viz tab. 3.15.

Tab. 3.15 Nutný stupeň integrity bezpečnosti (ASIL) dle indikátoru

Klasifikační indikátor I	Stupeň požadavku na úroveň bezpečnosti (ASIL)	Slovní hodnocení	Třídy dle přístupu ALARP
0 – 21	QM	Nezávažný, bez opatření	IV.
22 – 35	ASIL A	Závažný, opatření doporučeno	III.
36 – 72	ASIL B	Závažný opatření velmi doporučeno	III.
73 – 122	ASIL C	Kritický, opatření jsou povinná	II.
123 - 281	ASIL D	Katastrofický, opatření povinné	I.

Klasifikace se zapisuje do formuláře Záznam o nebezpečí. Záznam o nebezpečí používá nejen stupeň integrity bezpečnosti, ale také slovní hodnocení kritičnosti jednotlivých nebezpečí viz tab. 3.14.

Navržená opatření

V rámci hodnocení nebezpečí by měla být také navržena opatření pro snížení nebezpečí (rizika). Opatření jsou navržena samostatně nebo na základě dalších užitých metod (např. analýzy FTA a analýzy FMEA – viz kap. 3.5 a 3.6).

Opatření jsou rozdělena do skupin podle jejich charakteru:

- **Opatření technická**, zpravidla bezpečnostní nebo provozní funkce realizované technickým systémem (elektrický, mechanický, apod.).
- **Opatření vnějším systémem**, opatření zajišťuje vnější ochranný systém umístěný na vozidle nebo mimo něj, je nutno uvést o jaký systém se jedná.
- **Opatření údržbové**, opatření je realizováno údržbou (nutné uvést co udržovat, jak udržovat a kdy udržovat).
- **Opatření organizační a legislativní**, opatření je realizováno organizačním opatřením provozovatele či výkonné moci (např. odvoláním na předpisy provozovatele apod.).

3.5 Analýza stromů poruch (FTA)

Cílem metody FTA je analýza pravděpodobnosti selhání celého systému a s tím související preventivní opatření, která by měla spolehlivost systému zvýšit. Jde o grafické vyjádření systému, které poskytuje popis kombinací možných výskytů problémů v systému, který může vyústit v problém, který nechceme, aby vůbec vznikl. Analýzu FTA lze též provádět k tomu účelu, aby poskytovala model předpovědi bezporuchovosti systému a aby umožnila provádění studií optimalizace nákladu a přínosu v etapě návrhu produktu. Analýza FTA použitá jako nástroj pro zjišťování a kvalitativní či kvantitativní vyhodnocování příčin poruchových stavu představuje účinnou metodu pro identifikaci a vyhodnocování druhu poruch a příčin známých či podezřelých následku. [29]

Konstrukce stromu poruch

Při analýze FTA je touto událostí obvykle porucha, poruchový stav nebo zhoršené fungování systému, snížení bezpečnosti nebo zhoršení jiných důležitých provozních atributů. Strom poruch lze definovat jako „uspořádaný systém logicky svázaných vstupních událostí vedoucích k předem determinované nežádoucí události“. [29]

Vlastní sestavení stromu poruch vychází z vrcholové události (TOP jev) a strom je postupně rozvíjen hledáním příčin vzniku této nežádoucí události (tj. „Kdy může tato událost nastat?“). Při rozvíjení TOP jevu využíváme logických operátorů (AND, OR a další). Speciálním případem operátoru je m dobrých z celkového počtu n součástí (2 ze 3 a podobně).

Postupným rozvíjením nově vzniklých událostí rozvíjíme strom poruch až k primárním událostem (porucha komponenty, resp. dílčí porucha komponenty či podsystému, lidská chyba, příp. jiné související události), které jsme schopni kvantifikovat. Tyto události se stávají prvky stromu poruch a musí být nezávislé (to znamená, že nesmí mít společnou příčinu). Druhou důležitou zásadou je, že stejná primární událost se ve stromu poruch nesmí objevit vícekrát, např. porucha zdroje vyřadí z činnosti čidla i řídící logiku, přesto se ve stromu poruch může objevit pouze jednou.

Je třeba si uvědomit, že strom poruch není modelem všech možných systémových poruch, ale pouze těch příčin, které způsobují poruchu systému (resp. vrcholovou událost – TOP jev).

Pravidla pro konstrukci a popis stromu poruch

Postup při konstrukci stromu poruch lze shrnout do několika základních pravidel.

- „Popiš děje, které vstupují do bloku událostí jako poruchy (resp. chyby); urči přesně, co jsou poruchy a kdy k nim dojde“. Při popisu dějů se nevyhýbáme ani rozsáhlejšímu popisu, který však je třeba formulovat přesně a výstižně tak, abychom ho mohli v dalším postupu jednoznačně rozvíjet (např. „nenastartování motoru při el. napájení“ atd.).
- Další pravidlo je pravidlo „žádného zázraku“. Obecně lze připustit, že posloupnost poruchy může být blokována „zázračnou“ a neočekávanou poruchou nějakého komponentu. Předpokládáme však normální funkce ostatních komponent, tj. volné šíření poruchového následku stromem poruch.
- Systematický postup lze definovat jako pravidlo „kompletního hradla“ definující tvorbu stromu poruch po úrovních, tzn., že pokud nejsou definovány všechny vstupy do určitého hradla, nelze pokračovat na nižší úroveň.
- Důslednou analýzu podmiňuje pravidlo, které můžeme definovat jako „zákaz z hradla do hradla“. Jinými slovy, každý další krok konstrukce stromu by měl být popsán komentářem, přímý přechod z hradla do hradla se prezentuje jako nepořádně provedená analýza.

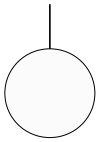
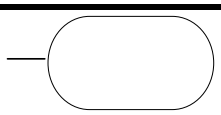
Terminologie a symbolika

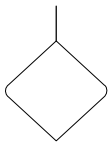
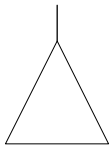
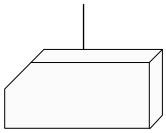
Strom poruch zpracováváme graficky, k vyjádření logiky „nebo“ (příp. OR) a „a“ (příp. AND) využíváme symbolů nazývaných hradla. Pro vyjádření stromu jsou dále užívány symboly pro primární události (resp. „meziudálosti“) a symboly přenosu.

Značení primárních událostí

U primárních událostí uvažujeme pět možných typů (viz tab. 3.16):

Tab. 3.16 Primární události

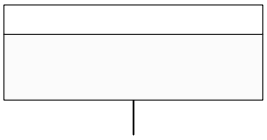
	***Základní událost*** porucha, kterou dále nerozvíjíme, např. porucha procesoru, tranzistoru apod.
	***Podmíněná událost*** specifické podmínky nebo omezení týkající se některých logických hradel.

	***Nerozvinutá událost*** událost, která není dále rozvíjena buď z důvodu jejího malého významu, nebo proto, že o ní nemáme informace.
	***Nerozvedená událost*** událost, pro kterou již existuje jiný strom poruch (podstrom), který byl vyhodnocen separátně. Používá se typicky pro rozsáhlé stromy poruch.
	***Vnější událost*** událost, o které předpokládáme, že se vyskytne, ale nejedná se o poruchu zkoumaného systému.

Značení meziudálostí

U meziudálostí používáme následující značení (viz tab. 3.17):

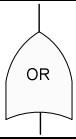
Tab. 3.17 Meziudálost

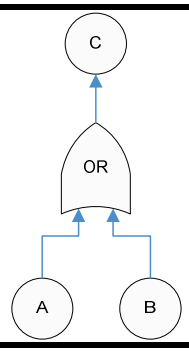
	***Meziudálost (zprostředkovaná událost)*** událost, ke které dojde z jedné nebo několika příčin spojených logickými hradly (používá se pro přehledné „čtení stromů poruch“ a má v podstatě funkci komentáře).

Příklady a funkce hradel

U následujících příkladů je respektována teze o tom, že logická 0 reprezentuje bezporuchový stav a logická 1 reprezentuje poruchu. Příklad pro hradlo OR je uveden v tab. 3.18 a příklad pro hradlo AND je uveden v tab. 3.19.

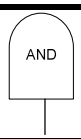
Tab. 3.18 Hradlo OR a příklad využití s pravdivostní tabulkou

	***Hradlo „OR“ (disjunkce)*** k výstupní události dojde tehdy, dojde-li alespoň k jedné (nebo více) ze vstupních událostí. Vstupní události musí být vzájemně nezávislé, tj. vznik jedné vstupní události nesmí nijak ovlivnit vznik druhé vstupní události.

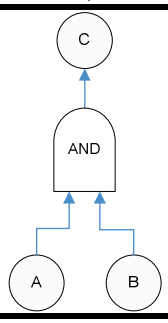


Pravdivostní tabulka hradlo "OR"		
A	B	C
0	0	0
1	0	1
0	1	1
1	1	1

Tab. 3.18 Hradlo AND a příklad využití s pravdivostní tabulkou



Hradlo„AND“ (konjunkce)
k výstupní události dojde pouze tehdy, jestliže dojde ke všem vstupním událostem.



Pravdivostní tabulka hradlo "AND"		
A	B	C
0	0	0
1	0	0
0	1	0
1	1	1

Číslování stromů poruch

Stromy poruch se sestavují pro bezpečnostní funkce, provozní funkce a nebezpečí (hazardy). Použije se následující označení:

BF – strom poruch pro znázornění bezpečnostní funkce,

PF – strom poruch pro znázornění provozní funkce,

H – strom poruch pro znázornění nebezpečí (hazard).

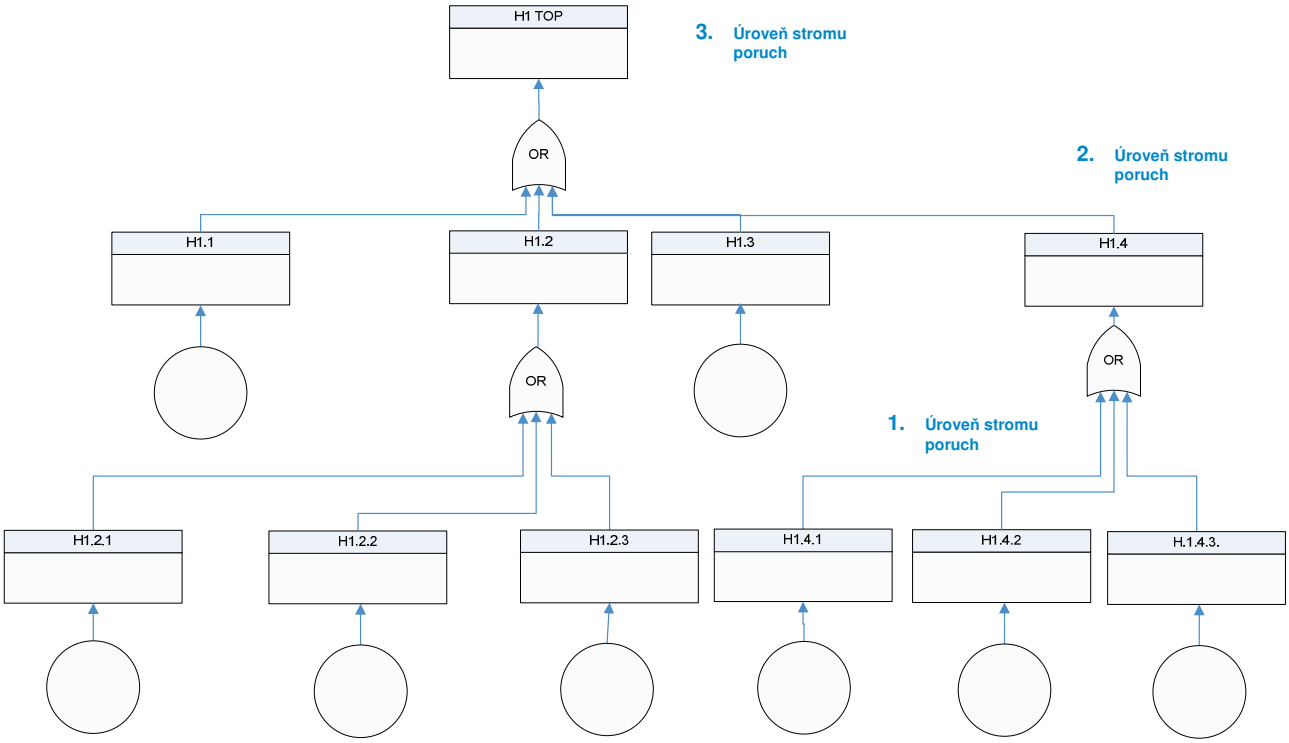
Každý strom poruch musí mít jedinečné číselné označení TOP jevu odpovídající konkrétnímu označení bezpečnostní funkce, provozní funkce nebo nebezpečí.

BF1 – označení TOP jevu stromu poruch pro bezpečnostní funkci č. 1

PF1 – označení TOP jevu stromu poruch pro provozní funkci č. 1

H1 – označení TOP jevu stromu poruch pro nebezpečí č. 1

Příklad elementárního stromu poruch spolu s číslováním jednotlivých úrovní je uveden na obr. 3.3.



Zdroj: autor

Obr. 3.3 Příklad elementárního stromu FTA

3.6 Analýza způsobů a důsledků poruch (FMEA)

Metoda FMEA (Failure Mode and Effect Analysis), tedy analýza způsobů a důsledků poruch, je strukturovaná, kvalitativní analýza sloužící k identifikaci způsobů poruch systémů, jejich příčin a důsledků. V současnosti patří metoda k nejpoužívanějším metodám prediktivní analýzy spolehlivosti a je využívána v řadě oborů, nejen pro analýzu technických systémů, ale také pro analýzu procesů a software.[30]

Princip metody FMEA

- Metoda FMEA je metoda induktivní, která provádí kvalitativní analýzu bezporuchovosti a bezpečnosti systému a zkoumá, jakým způsobem mohou objekty na nižší úrovni selhat a jaký důsledek mohou mít tato selhání pro vyšší úrovně systému. K hlavním cílům metody patří:
- posouzení důsledků a posloupnosti jevů pro každý zjištěný způsob poruchy prvku, s jakoukoliv její příčinou, na různých funkčních úrovních systému,

- určení významnosti každého způsobu poruchy vzhledem k požadované funkci nebo provozuschopnosti systému s uvážením důsledků na bezporuchovost nebo bezpečnost daného procesu,
- klasifikace zjištěných způsobů poruch podle možnosti, jak lze zjistit, diagnostikovat, testovat, nahradit danou součást nebo provádět kompenzační a provozní opatření (oprava, údržba, logistický systém atd.), nebo podle jiných odpovídajících charakteristik,
- odhady ukazatelů významnosti poruchy, jsou-li k dispozici potřebná data.

Využití metody je především v etapě návrhu a vývoje systému, kde slouží jako součást přezkoumání návrhu jako tzv. metoda předběžného varování, která má zabránit pozdějším problémům vyplývajícím z nespolehlivosti systému. Dále se uplatňuje i v etapě tvorby koncepce a specifikace požadavků, jako nástroj předběžné analýzy rizik, a při modifikacích a modernizacích systému nebo při změnách provozních podmínek jako prostředek identifikace a posouzení důsledků konstrukčních změn a provozních podmínek na bezporuchovost a bezpečnost systému. Metoda je také používána při prokazování, že navrhovaný systém splňuje v oblasti bezporuchovosti a bezpečnosti požadavky norem, předpisů nebo uživatele.

Pro možnost vyhodnocení analýzy FMEA je určována relativní významnost poruchy, která je označována jako hodnota „Risk Priority Number“ (RPN) a určí se podle vztahu (3.3):

$$RPN = S \cdot O \cdot D \tag{3.3}$$

kde:
S - závažnost důsledku poruchy (Severity),
O- četnost vzniku poruchy (Occurence),
D - odhalitelnost poruchy (Detection).

Jelikož se FMEA analýza a určování RPN provádí při vstupním hodnocení bez jakýchkoli opatření a následně opakovaně po navržení opatření ke snížení rizika, je také potřebný vztah (3.3) pro výpočet RPN v tabulkách modifikován.

Pro vstupní hodnocení bez opatření jsou hodnoty označeny následujícím způsobem s využitím indexace:

$$RPN_i = S_i \cdot O_i \cdot D_i \tag{3.4}$$

kde:
S_i - závažnost důsledku poruchy - počáteční (Severity initial),
O_i - četnost vzniku poruchy - počáteční (Occurrence initial),
D_i - odhalitelnost poruchy- počáteční (Detection initial).

Pro hodnocení následné po navržení opatření ke snížení rizika jsou hodnoty označeny následujícím způsobem opět s využitím indexace:

$$RPN_r = S_r \cdot O_r \cdot D_r \tag{3.5}$$

kde:
S_r - závažnost důsledku poruchy - následná (Severity revised),
O_r - četnost vzniku poruchy - následná (Occurrence revised),
D_r - odhalitelnost poruchy - následná (Detection revised).

Klasifikace jevů souvisejících s poruchami (závažnost poruchy, výskytu poruchy, možnosti detekce poruchy atd.) je uvedena v tab. 3.20, 3.21 a 3.22.

Klasifikace závažnosti poruchy

Klasifikace závažnosti důsledků poruchy je modifikována pro provoz silničních vozidel (tab. 3.19). Poruchy mají následující závažnost:

- nezávažná porucha – porucha, jejímž důsledkem je vznik zpoždění vozidla,
- závažná porucha – porucha, v jejímž důsledku vzniká úplná ztráta provozuschopnosti, nebo lehké zranění,
- kritická porucha – porucha, která může způsobit ohrožení bezpečnosti silničního provozu, v jejímž důsledku může dojít ke zranění osob nebo smrti jedné osoby,
- katastrofická porucha – porucha, která způsobí ohrožení bezpečnosti silničního provozu, v jejímž důsledku může dojít ke zranění nebo usmrcení několika osob, ohrožení životního prostředí apod., např. vlivem srážky silničních vozidel apod.

V analýze závažnosti poruch je zvažován vždy jen nejzávažnější důsledek dané poruchy, i když se může jevit jako krajně nepravděpodobný.

Tab. 3.20Klasifikace závažnosti poruchy S

S	Typ poruchy
1	nezávažná
2	závažná
3	kritická
4	katastrofická

Klasifikace četnosti vzniku poruchy

Četnost vzniku poruchy (tab. 3.21) je posuzována na základě odhadu. Při hodnocení četnosti poruch bývá zohledněno:

- umístění prvku modulu ve vozidle – vyšší četnost poruch je u prvků, které se nacházejí v podvozku vozidla (vliv vlhkosti, teploty, vibrací apod.), nižší četnost u prvků modulu, které se nacházejí uvnitř vozidla,
- počet subsystémů – četnost poruch vzrůstá s množstvím prvků (procesorové desky, sběrnice, dvoubránové paměti apod.) a subsystémů,
- četnost vyžádání funkce – vyšší četnost při nepřetržitém vyžádání funkce, nižší četnost, pokud je funkce s nízkým vyžádáním,
- vliv lidského činitele – poruchy způsobené chybou obsluhy vozidla mají vyšší četnost než poruchy např. elektronických systémů.

Tab. 3.21 Klasifikace četnosti poruchy O

O	Četnost poruchy
1	téměř nikdy
2	velice mírná
3	nízká
4	střední
5	vysoká
6	téměř jistá

Klasifikace odhalitelnosti poruchy

Klasifikace odhalitelnosti poruchy je také modifikována pro provoz silničních vozidel (tab. 3.22). Poruchy mají následující závažnost:

Tab. 3.22 Klasifikace četnosti poruchy D

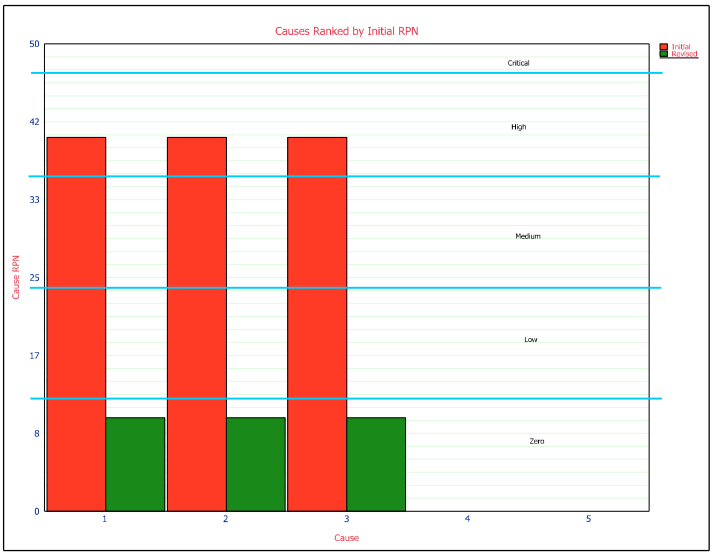
D	Odhalitelnost poruchy
1	téměř jistá
2	vysoká
3	střední
4	nízká
5	téměř nemožná

Maximální hodnota rizikového čísla RPN (RPN = S x O x D) s využitím výše uvedené klasifikace tedy může dosáhnout hodnoty RPN = 120 (RPN = 4 x 6 x 5). Za hranici přijatelného rizika (mezní hodnotu) se u této konkrétní klasifikace považuje hodnota RPN =

12 (zhruba 10x méně než je maximální hodnota). Snahou je tedy dostat se pod uvedenou mezní hodnotu rizikového čísla RPN. Je však možné setkat se situací, kdy mezní hodnota RPN bude jiná než uvedených 12. Zpravidla si může určit svou vlastní mezní hodnotu zákazník, tedy odběratel či provozovatel vozidla a ta může být přísnější než představená hodnota.

Takto klasifikované hodnocení poruch se vyplňuje nejčastěji do speciální tabulky, kde je nejprve provedeno již zmíněné hodnocení objektu bez opatření pomocí rizikového čísla RPNi, poté jsou navržena konkrétní opatření pro snížení rizika tam, kde rizikové číslo RPNi překročilo mezní hodnoty a poté je provedeno nové hodnocení objektu, kdy se znovu posuzuje závažnost, četnost výskytu a odhalitelnost po již přijatých opatřeních ke snížení rizika (opatření technická, organizační, údržbová nebo vnější systém) pomocí rizikového čísla RPNr.

Pokud se opatření přijatá ke snížení rizika ukázala jako účinná, rizikové číslo RPNr kleslo pod mezní hodnoty. Tam, kde rizikové číslo nekleslo pod mezní hodnoty, nebyla přijatá opatření ke snížení rizika dostatečná a je tedy nutno znovu tato opatření iteračně revidovat. Účinnost přijatých opatření je možno zobrazit také graficky (viz obr. 3.4).



Zdroj: autor

Obr. 3.4 Počáteční a koncové hodnoty RPN

3.7 Matice závažnosti (matice rizika)

Pro možnost vyhodnocení analýzy FMEA je často užito zobrazení výsledků analýzy pomocí matice závažnosti (matice rizika), která zohledňuje pouze hodnoty hodnocení –

závažnost a četnost výskytu. Charakteristické rizikové číslo matice se označuje symbolem (SxO) a je vyjádřitelné dle vztahu (3.6).

$$(SxO) = S \cdot O \tag{3.6}$$

kde:
S - závažnost důsledku poruchy (Severity),
O - četnost vzniku poruchy (Occurence),

Jelikož se také matice závažnosti sestavuje při vstupním hodnocení bez jakýchkoli opatření a následně opakovaně po navržení opatření ke snížení rizika, je také potřebný vztah (3.6) pro (SxO) modifikován.

Pro vstupní sestavení bez opatření jsou hodnoty označeny následujícím způsobem s využitím indexace:

$$(SxO)_i = S_i \cdot O_i \tag{3.7}$$

kde:
S - závažnost důsledku poruchy – počáteční (Severity initial),
O - četnost vzniku poruchy – počáteční (Occurence initial),

Pro hodnocení následné po navržení opatření ke snížení rizika jsou hodnoty označeny následujícím způsobem opět s využitím indexace:

$$(SxO)_r = S_r \cdot O_r \tag{3.8}$$

kde:
S - závažnost důsledku poruchy – následná (Severity revised),
O - četnost vzniku poruchy – následná (Occurence revised),

S použitím této klasifikace se dále sestavují třípásmové (nebo v duchu přístupu ALARP čtyřpásmové) matice závažnosti zařízení.

V tab. 3.23 je možno vidět čtyřpásmovou matici závažnosti. Osa x matice je tvořena klasifikací závažnosti a osa y matice je tvořena klasifikací četnosti výskytu. Klasifikaci úrovně rizika je možno vidět v tab. 3.24.

Tab. 3.23 Matice závažnosti

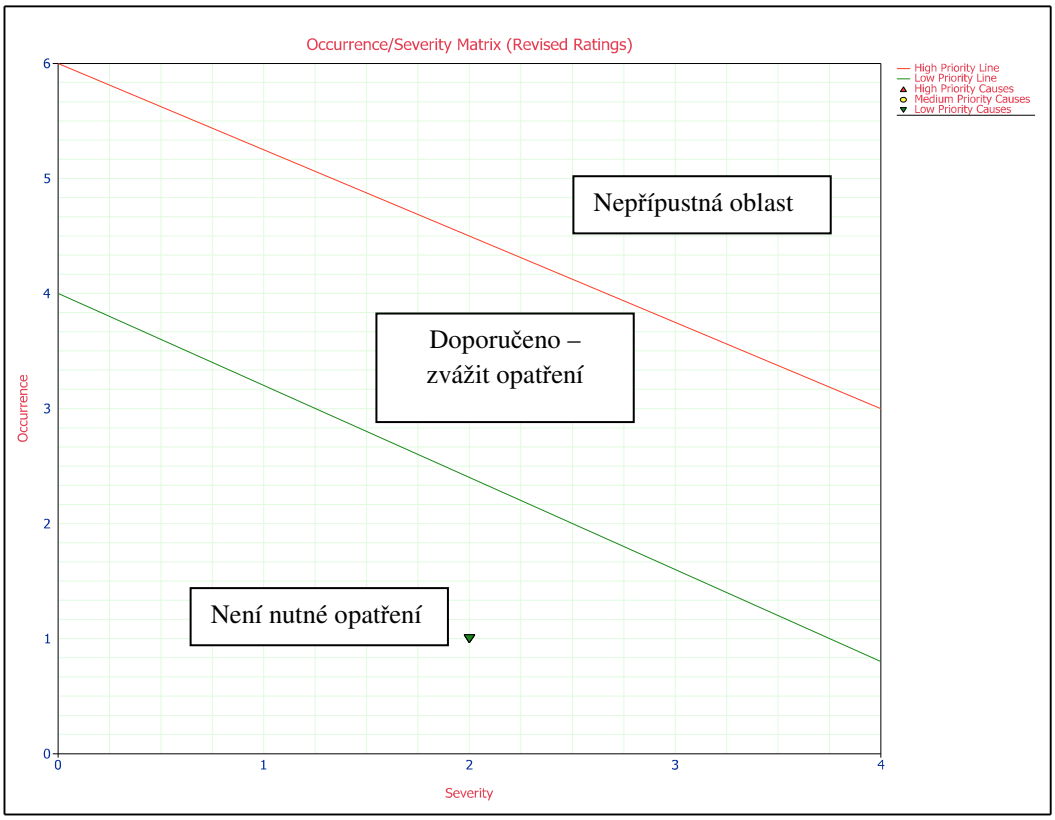
Četnost výskytu nebezpečné události	Kategorie rizika			
Častá (téměř jistá)	Nežádoucí	Nepřístupné	Nepřístupné	Nepřístupné
Pravděpodobná (vysoká)	Přípustné	Nežádoucí	Nepřístupné	Nepřístupné
Občasná (střední)	Přípustné	Nežádoucí	Nežádoucí	Nepřístupné
Malá (nízká)	Zanedbatelné	Přípustné	Nežádoucí	Nežádoucí
Nepravděpodobná (velice mírná)	Zanedbatelné	Zanedbatelné	Přípustné	Přípustné
Vysoce nepravděpodobná (téměř nikdy)	Zanedbatelné	Zanedbatelné	Zanedbatelné	Zanedbatelné
	Nezávažné	Závažné	Kritické	Katastrofické
	Úrovně závažnosti			

Výsledek v matici rizika představují barevná pole, jež reprezentují úroveň rizika posuzovaného objektu. Pokud hodnocení posuzovaného objektu spadá do zelené oblasti (zanedbatelné), lze riziko přijmout. Pokud spadá do oblasti hnědé (nežádoucí) nebo žluté (přípustné) je nutno riziko opatřeními eliminovat. Jeho přijetí je možné, jen pokud by byly náklady na jeho odstranění příliš vysoké nebo je-li dosaženo souhlasu zákazníka, provozovatele nebo schvalovací autority. Pokud hodnocení spadá do červené oblasti (nepřípustné), poté je nutno vhodnými opatřeními riziko vždy snížit.

Tab. 3.24 Úroveň rizika v matici závažnosti

Kategorie rizika	**Opatření použitá v každé kategorii**
Nepřípustné	Musí být odstraněno.
Nežádoucí	Smí být přijato pouze tehdy, jestliže snížení rizika je prakticky nedosažitelné, a se souhlasem provozovatele nebo řídícího orgánu pro otázky bezpečnosti (podle okolností).
Přípustné	Lze ho přijmout při přiměřené kontrole a se souhlasem provozovatele.
Zanedbatelné	Lze ho přijmout se souhlasem/ bez souhlasu provozovatele.

Matice závažnosti může být znázorněna také grafickým způsobem. Příklad takové matice závažnosti je uveden na obr. 3.5. Kategorie rizika, vyplývající z tab. 3.23 tab. 3.24 jsou v souladu s přístupem ALARP (viz kap. 3.1).



Zdroj: autor

Obr. 3.5 Grafické vyjádření matice závažnosti

V tomto případě se hodnocení objektu nachází v některém ze tří pásem grafu. Pokud hodnocení posuzovaného objektu spadá do oblasti pod zelenou čarou, lze riziko přijmout. Pokud spadá do oblasti nad zelenou čarou a současně pod červenou čarou je nutno riziko opatřeními eliminovat. Jeho přijetí je možné, jen pokud by byly náklady na jeho odstranění příliš vysoké nebo je-li dosaženo souhlasu zákazníka, provozovatele nebo schvalovací autority. Pokud hodnocení spadá do oblasti nad červenou čarou, poté je nutno vhodnými opatřeními riziko vždy snížit.

4 Posuzování funkční bezpečnosti - kvantitativní metody

Kvantitativní metody se uplatňují především ve fázi prokazování úrovně funkční bezpečnosti. Mezi kvantitativní metody řadíme výpočet diagnostického pokrytí, cílové míry poruch a zkoušky spolehlivosti.

4.1 Blokové diagramy bezporuchovosti (RBD)

Metoda blokového diagramu bezporuchovosti (RBD) se velmi často používá ke stanovení hodnot ukazatelů bezporuchovosti a pohotovosti zejména neopravovaných systémů nebo systémů, kde nezáleží na pořadí poruch.[31]

Je to model bezporuchovosti, který poskytuje grafickou reprezentaci bezporuchovosti systému a vyjadřuje logickou vazbu (fungování) komponent, potřebných pro fungování systému.

Výhodou metody RBD je, že diagramy lze obvykle vypracovat přímo z funkčního diagramu systému, v tomto případě ze stromů poruch FTA. To má za následek další výhodu - snížení chyb při vypracování diagramu.

Při této technice lze zacházet s většinou typu konfigurace systému, včetně paralelních, redundantních, pohotovostních a alternativních funkčních cest. Metoda RBD je způsobilá provádět analýzu citlivosti pro zjištění objektu, které převážně přispívají k celkové bezporuchovosti systému.

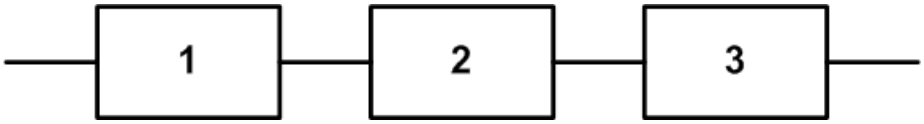
Metoda umožňuje vypracovat modely pro vyhodnocení celkové bezporuchovosti a pohotovosti systému. Další výhodou je, že poskytuje přesné a lehce interpretovatelné diagramy pro celý systém. Metoda má však i jistá omezení.

Hlavní předpoklad je, že komponenty (podsystémy) mohou existovat pouze ve dvou stavech - použitelný (funkční) a nepoužitelný (nefunkční).

Dalším předpokladem je, že porucha (nebo obnova) libovolného bloku nesmí ovlivnit pravděpodobnost poruchy (nebo obnovy) jakéhokoliv jiného bloku v systému, který se modeluje. Z toho vyplývá, že poruchy a obnovy jednotlivých bloku se považují za statisticky nezávislé události [3].

Sériová soustava

Sériová soustava je tvořena za sebou řazenými tvořícími prvky (obr. 4.1). Jedná se o systém bez zálohy a tedy o nejporuchovější zapojení. Systém bude bez poruchy, jen pokud budou bez poruchy všechny tvořící komponenty.



Zdroj: autor

Obr. 4.1 Příklad sériového systému tvořeného třemi prvky

Pro sériový systém v bezporuchovém stavu by potom platil následující vztah (4.1):

$$R_S = P(X_1 \cap X_2 \cap ... \cap X_i) \tag{4.1}$$

kde:
R_S - pravděpodobnost bezporuchového stavu systému [-]
X_i - pravděpodobnost bezporuchového stavu i-tého prvku systému, i=1, 2 …n [-]

Za existence předpokladu, že poruchy tvořících prvků vznikají nezávisle, je možno vztah (4.1) převést na součin pravděpodobností a bezporuchovost systému dle obr. 4.1 se vypočte dle vztahu (4.2):

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \tag{4.2}$$

kde:
$R_S(t)$ - bezporuchovost systému [-]
$R_1(t)$ - bezporuchovost prvku 1 [-]
$R_2(t)$ - bezporuchovost prvku 2 [-]
$R_3(t)$ - bezporuchovost prvku 3 [-]

Jestliže doby do poruchy tvořících prvků mají exponenciální rozdělení pravděpodobnosti s konstantní intenzitou poruch λ_i [h^{-1}], platí pro sériovou soustavu vztah (4.3):

$$R_S(t) = \prod_{i=1}^{n} e^{-\lambda_i \cdot t} \tag{4.3}$$

Celková intenzita poruch sériového systému dle obr. 4.1 je dána součtem jednotlivých intenzit, jak je uvedeno ve vztahu (4.4):

$$\lambda_S = \lambda_1 + \lambda_2 + \lambda_3 \tag{4.4}$$

kde:

λ_S - intenzita poruch systému [h^{-1}]

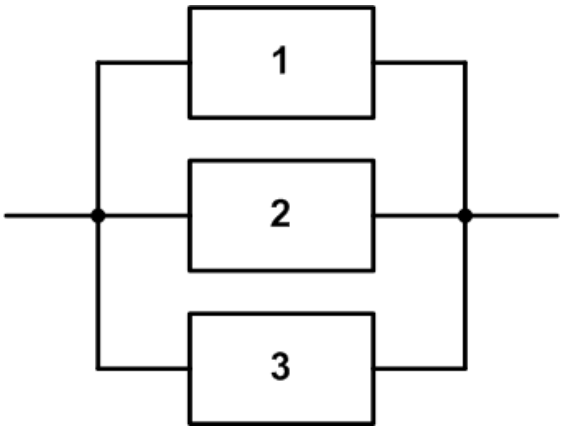
λ_1 - intenzita poruch prvku 1 [h^{-1}]

λ_2 - intenzita poruch prvku 2 [h^{-1}]

λ_3 - intenzita poruch prvku 3 [h^{-1}]

Paralelní soustava

Paralelní soustava je tvořena vedle sebe řazenými tvořícími prvky (obr. 4.2). Jedná se o systém zálohovaný a tedy o nejméně poruchové zapojení. Systém bude v poruše, jen pokud budou v poruše všechny tvořící komponenty.



Zdroj: autor

Obr. 4.2 Příklad paralelního systému tvořeného třemi prvky

Pro paralelní systém by potom platilo následující:

$$F_S = P(\overline{X}_1 \cap \overline{X}_2 \cap ... \cap \overline{X}_i) \tag{4.5}$$

kde:

F_S - pravděpodobnost poruchy systému [-]

X_i - pravděpodobnost poruchy i-tého prvku systému, i=1, 2 …n [-]

Za existence předpokladu, že poruchy tvořících prvků vznikají nezávisle, je možno vztah (4.5) převést na součin pravděpodobností a bezporuchovost systému dle obr. 4.2 se vypočte dle vztahu (4.6):

$$F_S(t) = F_1(t) \cdot F_2(t) \cdot F_3(t) \tag{4.6}$$

kde:
$F_S(t)$ - pravděpodobnost poruchy systému [-]
$F_1(t)$ - pravděpodobnost poruchy prvku 1 [-]
$F_2(t)$ - pravděpodobnost poruchy prvku 2 [-]
$F_3(t)$ - pravděpodobnost poruchy prvku 3 [-]

Jestliže pravděpodobnost poruchy F(t) a bezporuchovost R(t) mají k sobě disjunktní vztah, je možno pravděpodobnost bezporuchového vztahu pro paralelní soustavu vyjádřit s využitím vztahu (4.7):

$$R_S(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right] \tag{4.7}$$

kde:
$R_S(t)$ - bezporuchovost systému, [-]
$R_i(t)$ - bezporuchovost i-tého prvku systému, i=1, 2 …n [-]

Jestliže doby do poruchy tvořících prvků mají exponenciální rozdělení pravděpodobnosti s konstantní intenzitou poruch λ_i [h^{-1}], platí pro paralelní soustavu a její bezporuchovost následující vztah (4.8):

$$R_S(t) = 1 - \prod_{i=1}^{n} \left[1 - e^{-\lambda_i \cdot t}\right] \tag{4.8}$$

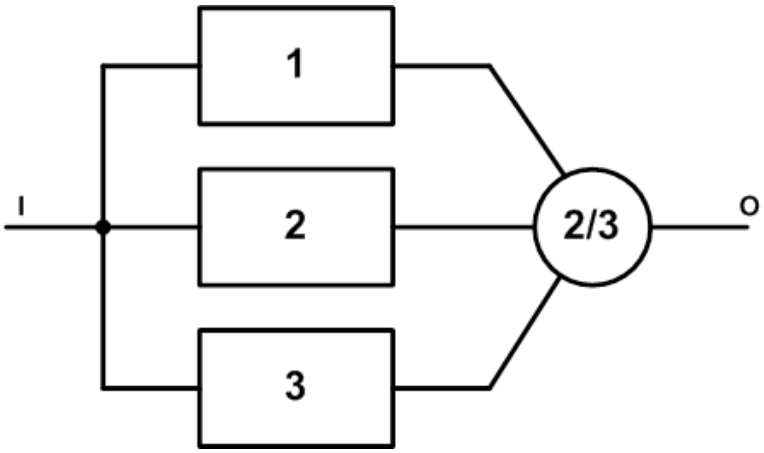
kde:
$R_S(t)$ - bezporuchovost systému, [-]
$\lambda_i(t)$ - intenzita poruch i-tého prvku systému, i=1, 2 …n [h^{-1}]

Z uvedeného vztahu vyplývá, že intenzita poruch paralelní soustavy není snadno vyjádřitelná jako u soustavy sériové.

V praxi se samozřejmě vyskytují systémy složitější než samostatně stojící sériový nebo paralelní systém. V případě existence takového sério-paralelního sytému se k řešení takové soustavy využívá zjednodušení pomocí metody dekompozice systému.

Soustava 2 ze 3 (obecně m z n)

V oblasti funkční bezpečnosti je možné se setkat i s takovouto architekturou. Taková soustava je tvořena vedle sebe řazenými tvořícími prvky (obr. 4.3) s majoritním zálohováním. Systém bude v bezporuchovém stavu, jen pokud budou 2 ze 3 tvořících komponent pracovat bez poruchy (obecně m z n).



Zdroj: autor

Obr. 4.3 Příklad systému 2 ze 3 tvořeného třemi prvky

Jestliže je takovýto systém tvořen stejnými tvořícími prvky z pohledu bezporuchovosti, je možno bezporuchovost vyjádřit pomocí následujícího vztahu (4.9):

$$R_S = \sum_{k=m}^{n} \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} \tag{4.9}$$

kde:

m - minimální počet prvků v bezporuchovém vztahu,

n - celkový počet prvků systému,

p - pravděpodobnost bezporuchového stavu prvku v systému, [-]

Jestliže doby do poruchy tvořících prvků mají exponenciální rozdělení pravděpodobnosti s konstantní intenzitou poruch λ [h^{-1}], platí pro soustavu *m* z *n* a její bezporuchovost následující vztah (4.10):

$$R_S(t) = \sum_{k=m}^{n} \binom{n}{k} \cdot e^{-\lambda \cdot t \cdot k} \cdot \left(1 - e^{-\lambda \cdot t}\right)^{n-k} \tag{4.10}$$

kde:

m - minimální počet prvků v bezporuchovém vztahu,

n - celkový počet prvků systému,

λ - intenzita poruch prvku systému [h^{-1}]

Intenzita poruch pro tento systém je mimo hodnoty parametru λ jednotlivých tvořících prvků závislá také na konfiguraci systému (hodnotách *m* a *n*) [3].

4.2 Diagnostické pokrytí a odolnost systému

U systémů E/E/PE souvisejících s bezpečností jsou podle vlivu poruchy na bezpečnostní funkci rozlišovány poruchy nebezpečné, které uvádějí systém související s bezpečností do stavu, kdy nemůže vykonávat svou funkci, a poruchy bezpečné, kdy funkce systému souvisejícího s bezpečností není omezena.

Každá porucha, která se vyskytne na hardwarové části vztahující se k bezpečnosti, může být klasifikována následovně [13]:

- Samostatná porucha – porucha součásti, která není pokryta bezpečnostním mechanismem a vede přímo k narušení bezpečnostních cílů,
- Zbytková porucha – část poruch, které by samy vedly k narušení bezpečnostních cílů, vyskytující se na hardwaru, která není pokryta existujícím bezpečnostním mechanismem z důvodu jeho selhání,
- Vícenásobná porucha – jedna porucha z několika nezávislých poruch, které v kombinaci vedou k vícenásobné poruše (buď vnímané, detekované nebo skryté),
- Bezpečná porucha – porucha, jejíž výskyt signifikantně nezvýší pravděpodobnost narušení bezpečnostních cílů,

Intenzita poruch λ každé hardwarové části vztahující se k bezpečnosti může být rozdělena následujícím způsobem:

- Intenzita poruch přiřazená samostatným poruchám hardwarové části λ_{SPF}
- Intenzita poruch přiřazená zbytkovým poruchám hardwarové části λ_{RF}
- Intenzita poruch přiřazená vícenásobným poruchám hardwarové části λ_{MPF}
- Intenzita poruch přiřazená pozorovaným nebo detekovaným vícenásobným poruchám hardwarové části $\lambda_{MPF\,DP}$
- Intenzita poruch přiřazená skrytým vícenásobným poruchám hardwarové části $\lambda_{MPF\,L}$
- Intenzita poruch přiřazená bezpečným poruchám hardwarové části λ_S

Pro celkovou intenzitu poruch pak platí následující vztah (4.11):

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S \tag{4.11}$$

kde:

λ - celková intenzita poruch hardwarové části $[h^{-1}]$

λ_{SPF} - intenzita poruch přiřazená samostatným poruchám hardwarové části $[h^{-1}]$

λ_{RF} - intenzita poruch přiřazená zbytkovým poruchám hardwarové části $[h^{-1}]$

λ_{MPF} - intenzita poruch přiřazená vícenásobným poruchám hardwarové části [h^{-1}]
λ_S - intenzita poruch přiřazená bezpečným poruchám hardwarové části [h^{-1}]

Pro intenzitu poruch přiřazenou vícenásobným poruchám hardwarové části λ_{MPF} pak platí následující vztah (4.12):

$$\lambda_{MPF} = \lambda_{MPFDP} + \lambda_{MPFL} \tag{4.12}$$

kde:
λ_{MPF} - intenzita poruch přiřazená vícenásobným poruchám hardwarové části [h^{-1}]
$\lambda_{MPF\,DP}$ - intenzita poruch přiřazená pozorovaným nebo detekovaným poruchám hardwarové části [h^{-1}]
$\lambda_{MPF\,L}$ - intenzita poruch přiřazená skrytým vícenásobným poruchám hardwarové části[h^{-1}]

Riziko u systémů souvisejících s bezpečností je tedy vyvoláno vznikem nebezpečných poruch. Nutné snížení rizika těchto systémů pro zachování integrity bezpečnosti je v tomto případě prováděno včasnou detekcí nebezpečných poruch. Za tímto účelem musí být u systémů E/E/PE zajištěno provádění automatických diagnostických testů, které jsou založeny na principu porovnávacích kontrol, standardních zkušebních programů, trvalého monitorování signálů, zkoušek vnějšími podněty apod.

Diagnostické pokrytí (DC) vyjadřuje podíl na snížení pravděpodobnosti nebezpečných poruch hardware v důsledku provádění automatických diagnostických testů [17].

Skutečně nebezpečné poruchy systémů E/E/PE souvisejících s bezpečností představují poruchy, které vedou ke ztrátě bezpečnostní funkce a současně nejsou detekovány prováděním automatických diagnostických testů.

Na základě definice jednotlivých intenzit poruch je tedy možno definovat diagnostické pokrytí. Požadavky na prokázání požadované úrovně integrity bezpečnosti dle ISO 26262 definují dvě diagnostická pokrytí a odolnost SPM a odolnost LFM.

Diagnostické pokrytí

Na obr. 2.5 je v rámci procesu dokazování nutné stanovit diagnostické pokrytí. Diagnostické pokrytí se rozděluje na diagnostické pokrytí s ohledem na zbytkové poruchy (DC_{RF}) a diagnostické pokrytí s ohledem na skryté vícenásobné poruchy ($DC_{MPF\,L}$) [13].

Diagnostické pokrytí s ohledem na zbytkové poruchy (DC_{RF}) vyjadřuje účinnost diagnostického systému. Intenzita poruch přiřazená zbytkovým poruchám může být stanovena použitím diagnostického pokrytí bezpečnostních mechanismů, které zabraňují samostatným

poruchám hardwarové části. Odhad intenzity poruch přiřazené zbytkovým poruchám vyjadřuje vztah (4.13):

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \cdot 100 \tag{4.13}$$

kde:

DC_{RF} - diagnostické pokrytí s ohledem na zbytkové poruchy [%]

λ_{RF} - intenzita poruch přiřazená zbytkovým poruchám hardwarové části $[h^{-1}]$

λ - celková intenzita poruch hardwarové části $[h^{-1}]$

Diagnostické pokrytí s ohledem na skryté vícenásobné poruchy (DC_{MPFL}) vyjadřuje opět účinnost diagnostického systému. Intenzita poruch přiřazená skrytým vícenásobným poruchám může být stanovena použitím diagnostického pokrytí bezpečnostních mechanismů, které zabraňují skrytým vícenásobným poruchám hardwarové části. Odhad intenzity poruch přiřazené skrytým vícenásobným poruchám vyjadřuje vztah (4.14):

$$DC_{MPFL} = \left(1 - \frac{\lambda_{MPFL}}{\lambda}\right) \cdot 100 \tag{4.14}$$

kde:

$DC_{MPF\,L}$ - diagnostické pokrytí s ohledem na vícenásobné poruchy [%]

$\lambda_{MPF\,L}$ - intenzita poruch přiřazená vícenásobným poruchám hardwarové části $[h^{-1}]$

λ - celková intenzita poruch hardwarové části $[h^{-1}]$

Odolnost SPM (Single Point Metric)

Tato odolnost pokrytí odráží odolnost objektu na samostatné poruchy, a to buď pokrytím bezpečnostními mechanismy, nebo konstrukcí. Vysoká odolnost SPM znamená, že podíl samostatných poruch a zbytkových poruch hardwaru je nízký [13]. Definice je dána následujícím vztahem (4.15):

$$SPM = 1 - \frac{\sum(\lambda_{SPF} + \lambda_{RF})}{\sum \lambda} \cdot 100 = \frac{\sum(\lambda_{MPF} + \lambda_{S})}{\sum \lambda} \cdot 100 \tag{4.15}$$

kde:

λ - celková intenzita poruch $[h^{-1}]$

λ_{SPF} - intenzita poruch přiřazená samostatným poruchám hardwarové části $[h^{-1}]$

λ_{RF} - intenzita poruch přiřazená zbytkovým poruchám hardwarové části $[h^{-1}]$

λ_{MPF} - intenzita poruch přiřazená vícenásobným poruchám hardwarové části $[h^{-1}]$

λ_{S} - intenzita poruch přiřazená bezpečným poruchám hardwarové části $[h^{-1}]$

Odolnost LFM (Latent Fault Metric)

Tato odolnost odráží odolnost objektu na skryté poruchy, které jsou pokryty buď bezpečnostními mechanismy, nebo řidičem, nebo konstrukcí. Vysoká odolnost LFM znamená, že podíl skrytých poruch hardwaru je nízký [13]. Definice je dána následujícím vztahem (4.16):

$$LFM = 1 - \frac{\sum \lambda_{MPFL}}{\sum (\lambda - \lambda_{SPF} - \lambda_{RF})} \cdot 100 = \frac{\sum (\lambda_{MPFDP} + \lambda_S)}{\sum (\lambda - \lambda_{SPF} - \lambda_{RF})} \cdot 100 \qquad (4.16)$$

kde:

λ - celková intenzita poruch [h^{-1}]

λ_{SPF} - intenzita poruch přiřazená jednoduchým poruchám hardwarové části [h^{-1}]

λ_{RF} - intenzita poruch přiřazená zbytkovým poruchám hardwarové části [h^{-1}]

λ_{MPFDP} - intenzita poruch přiřazená pozorovaným nebo detekovaným poruchám HW [h^{-1}]

λ_{MPFL} - intenzita poruch přiřazená skrytým vícenásobným poruchám HW [h^{-1}]

λ_S - intenzita poruch přiřazená bezpečným poruchám hardwarové části[h^{-1}]

Požadavky na odolnost SPM a LFM pro různou úroveň integrity bezpečnosti (ASIL) jsou uvedeny v tab. 4.1.

Tab. 4.1 Odolnost SPM a LFM pro stupeň integrity bezpečnosti (ASIL)

Úroveň integrity bezpečnosti	ASIL B	ASIL C	ASIL D
Odolnost SPM	> 90 %	> 97 %	> 99 %
Odolnost LFM	> 60 %	> 80 %	> 90 %

Pro splnění požadavků požadované úrovně integrity bezpečnosti je tedy nutno splnit potřebnou odolnost.

4.3 Cílová míra poruch

Na obr. 2.5 je v rámci procesu dokazování nutné stanovit cílovou míru poruch. Cílová míra poruch (PFH) představuje základní kvantitativní ukazatel hodnocení funkční bezpečnosti hardware systémů E/E/PE souvisejících s bezpečností v souvislosti se vznikem náhodných poruch. Postup výpočtu této hodnoty je závislý na režimu provozu a na architektuře hardware uvedených systémů.

V tab. 4.2 jsou uvedeny hodnoty cílové míry poruch pro splnění bezpečnostních požadavků náhodných chyb hardwaru. Hodnoty vycházejí z doporučení normy pro funkční bezpečnost automobilů ISO 26262.

Tab. 4.2 Cílové hodnoty náhodných chyb hardware

Hladina ASIL	Cílové hodnoty náhodných chyb hardware [h^{-1}]
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

Pro splnění požadavků na úroveň integrity bezpečnosti ASIL jsou určeny následující třídy intenzit poruch. Kalkulace vychází z tab. 4.2 platí pro ni následující:

- Intenzita poruch odpovídající třídě 1 musí být menší než cílová hodnota pro ASIL D dělená 100.
- Intenzita poruch odpovídající třídě 2 musí být menší než desetinásobek intenzity poruch třídy 1.
- Intenzita poruch odpovídající třídě 3 musí být menší než stonásobek intenzity poruch třídy 1.

Hodnoty intenzit poruch pro jednotlivé definované třídy 1, 2 a 3 jsou přehledně zobrazeny v tab. 4.3.

Tab. 4.3 Intenzity poruch pro jednotlivé třídy intenzit

Třída intenzity poruch	Intenzita poruch [h^{-1}]
Třída 1	$< 10^{-10}$
Třída 2	$< 10^{-9}$
Třída 3	$< 10^{-8}$

Na základě takto sestavených tříd intenzit poruch je možno definovat požadavky na splnění úrovně integrity bezpečnosti ASIL integrací cílové míry poruch (intenzity poruch zařízení) a diagnostického pokrytí s ohledem na zbytkové a vícenásobné poruchy [13]. Tabulky přiřazení cílových hodnot tříd intenzit poruch jsou uvedeny v následujících tabulkách tab. 4.4 a tab. 4.5.

Tab. 4.4 Cílové třídy intenzity poruch HW s ohledem na zbytkové poruchy

		Diagnostické pokrytí ve vztahu ke zbytkovým poruchám		
		> = 99 %	> = 90 %	< 90 %
ASIL	D	Třída 3	Třída 2	Třída1
	C	-	Třída 3	Třída 2
	B	-	Třída 3	Třída 2

Tab. 4.5 Cílové třídy intenzity poruch HW s ohledem na vícenásobné poruchy

		Diagnostické pokrytí ve vztahu k vícenásobným poruchám		
		> = 99 %	> = 90 %	< 90 %
ASIL	D	-	Třída 3	Třída2
	C	-	-	Třída 3

4.4 Zkoušky spolehlivosti

Kvalita každého výrobku se plně projeví až v průběhu jeho dlouhodobého provozu. Dostačující nejsou pouze jeho technické parametry, ale také odpovídající úroveň jeho provozní spolehlivosti.

Aby bylo možné objektivně posoudit skutečnou spolehlivost těchto výrobků, je u nich nutné provést zkoušku spolehlivosti. Tímto postupem lze ověřit informace o spolehlivosti výrobků, které byly určeny analytickými metodami, tedy vyplývající z teoretického modelu spolehlivosti, a tím provést jejich potvrzení nebo zamítnutí. V případě, kdy nejsou použity prediktivní metody pro zjištění parametrů spolehlivosti, se zkoušky spolehlivosti využívají k přímému experimentálnímu stanovení parametrů spolehlivosti zkoušených výrobků.

Tyto zkoušky jsou obvykle prováděny na omezeném množství výrobků a často ve zvláštních podmínkách. Informace získané těmito zkouškami jsou pak exaktními postupy zpracovány, zhodnoceny a zobecněny pro celou populaci vyrobených výrobků. Cílem výrobců, pro zachování konkurenceschopnosti výrobků na trhu, je provedení těchto zkoušek v nejkratším možném čase a při nejnižších možných nákladech, současně při zachování vysoké věrohodnosti dosažených výsledků. V praxi se tak používá řada metod, vedoucích ke snížení počtu zkoušených výrobků, zkrácení průběhu zkoušek nebo zrychlení mechanismu vzniku poruch.

Zkouškou spolehlivosti se rozumí experimentální určení nebo ověření ukazatelů spolehlivosti, uvedených pro objekt v technické dokumentaci. Nejčastěji jsou předmětem zkoušek životnost, bezporuchovost, udržovatelnost, pohotovost, případně bezpečnost.

4.4.1 Typy zkoušek spolehlivosti

Podle účelu, kterému slouží a výrobků, jichž se týkají, lze zkoušky spolehlivosti rozdělit na [4]:

- **Typové zkoušky** – předmětem zkoušek jsou funkční vzorky, prototypy a výrobky nulté série. Stanovují se při nich ukazatele bez možnosti rozšířit výsledky na pozdější výrobky sériové.
- **Periodické zkoušky** – předmětem zkoušek jsou sériové výrobky. Provádí se na vzorku výrobků a z výsledků odhadujeme vlastnosti všech sériových výrobků.
- **Výrobní zkoušky** – jsou určeny pro sériové výrobky. Jde při nich o kontrolu stability výrobního provedení. Jejich cílem není kontrola ukazatelů spolehlivosti v pravém smyslu.

Podle cílů zkoušky lze zkoušky rozdělit následujícím způsobem:

- **Zkoušky určující** – jejich cílem je experimentální určení ukazatelů spolehlivosti. Před zkouškou o jejich hodnotách není nic známo a nic se nepředpokládá.
- **Zkoušky ověřovací** – jejich cílem je experimentální ověření, zda hodnota ukazatelů spolehlivosti souhlasí se stanovenými požadavky.

Podle namáhání a časového průběhu je možné určit:

- **Zkoušky normální** – zkoušky, zaměřené na experimentální určení nebo ověření ukazatelů spolehlivosti v normálních podmínkách.
- **Zkoušky zkrácené** – zkoušky spolehlivosti, které končí dříve, než dojde k poruše všech zkoušených objektů. Obecně se mohou provádět v normálních i zvláštních podmínkách.
- **Zkoušky zrychlené** – zkoušky, prováděné ve zvláštních podmínkách s cílem získat informace v kratších lhůtách, než při zkoušení v podmínkách, stanovených technickou dokumentací.

U zrychlených zkoušek má význam tzv. faktor zrychlení zkoušky. Je to poměr téhož ukazatele spolehlivosti při zvýšeném a při jmenovitém (normálním) zatížení. Zrychlená zkouška je jenom ta, u které je faktor zrychlení znám nebo může být zjištěn.

Zvláštní podmínky spočívají obvykle ve zvětšení zátěže nebo zrychlení časového průběhu zkoušky (zrychlení frekvence namáhání). Přitom je nutné zajistit, aby nedošlo ke kvalitativní změně mechanismu degradace vlastností (mechanismu poruchy).

Podle podmínek, ve kterých zkouška probíhá, rozlišujeme zkoušky:

- laboratorní (simulační),
- provozní.

4.4.2 Zkušební plány

V technické praxi není většinou možné realizovat zkoušky spolehlivosti u všech vyrobených objektů, a to z důvodů ekonomických, časových, ale i z toho důvodu, že řada zkoušek je destrukčních. Z praktických důvodů je tedy nutné se omezit na zkoušení vhodně vybrané skupiny objektů (zkušební vzorek) a z výsledků jeho zkoušek usuzovat na vlastnosti všech vyráběných objektů (známo jako základní soubor). Při shromažďování údajů pro odhady ukazatelů je nutno postupovat podle jasných pravidel, jejichž souhrn je možno nazývat zkušební plán.[4]

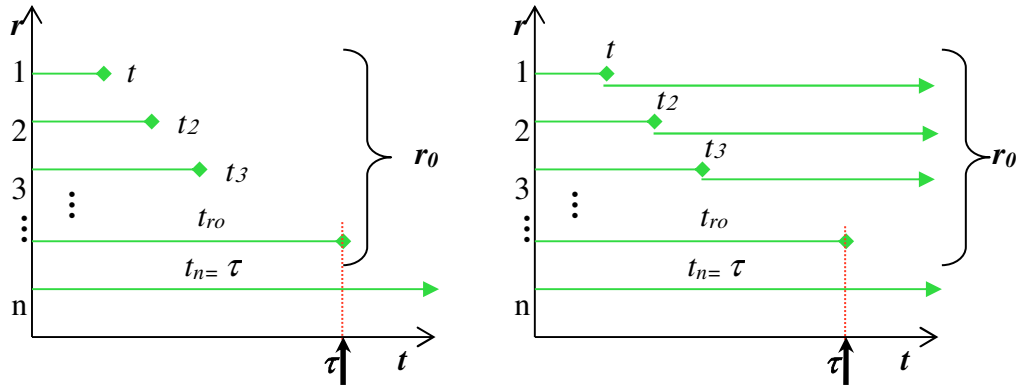
Pro zkušební plány se používá označení sestávající z kombinace tří symbolů, uzavřených do hranatých závorek. Na prvním místě je uveden počet zkoušených objektů n. Na druhém místě jsou symboly U, R nebo M podle způsobu nahrazování objektu po jeho poruše v průběhu zkoušky. Na třetím místě je symbol r (zkouška se ukončí při výskytu r-té poruchy, přitom r = 0, 1, 2, 3, ..., n) nebo t (zkouška se ukončí po uplynutí předepsané doby τ).

Každá zkouška spolehlivosti se realizuje s ni výrobky (i = 1, 2, … , n). Zkouška končí buď po určité době trvání $t = \tau_0$, nebo po vzniku určitého počtu poruch $r = r_0$. Lze tedy rozlišit dvě základní skupiny zkušebních plánů [4]:

- *r* – plány – do zkoušky je zařazeno n_i stejných výrobků. Zkouška končí po nastoupení předem daného počtu poruch $r = r_0$. Porušené prvky se v průběhu zkoušky buď nahrazují novými [*n, R,* r_0], nebo nenahrazují [*n, U,* r_0], nebo se opravují [*n, M,* r_0]. Náhodnou veličinou je doba trvání zkoušky $t = \tau$. Soubor údajů, získaných pomocí tohoto typu zkušebních plánů, se označuje jako jednoduše cenzurovaný soubor I. typu

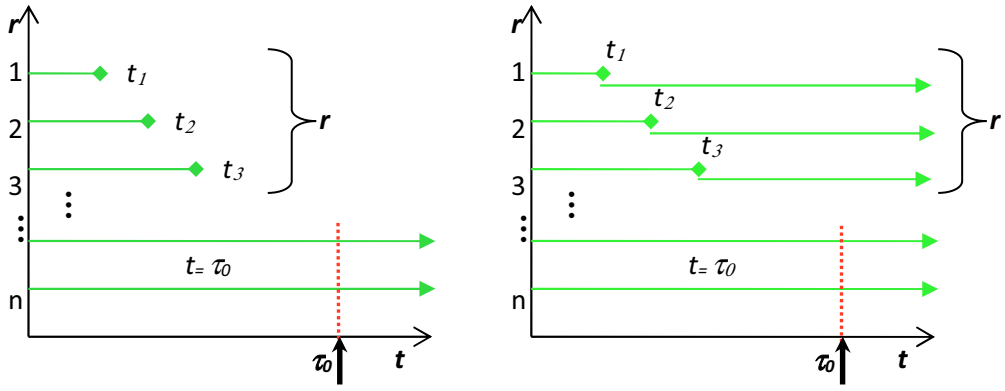
(cenzurovaný počtem poruch). Grafické znázornění tohoto zkušebního plánu je na obr. 4.4.

- t – plány – do zkoušky je zařazeno n_i stejných výrobků. Zkouška končí po uplynutí předem dané doby zkoušení $t = \tau_0$. Porušené prvky se v průběhu zkoušky buď nahrazují novými $[n, R, \tau_0]$, nebo se nenahrazují novými $[n, U, \tau_0]$ nebo se po poruše opravují $[n, M, \tau_0]$. Náhodnou veličinou je počet poruch r, který nastane po dobu trvání zkoušky. Soubor údajů, získaný pomocí tohoto typu zkušebních plánů, se označuje jako jednoduše cenzurovaný soubor II. typu (cenzurovaný dobou trvání zkoušky). Grafické znázornění tohoto zkušebního plánu je uvedeno na obr. 4.5.



Zdroj: autor

Obr. 4.4 Schéma zkušebních plánů: r – plány



Zdroj: autor

Obr. 4.5 Schéma zkušebních plánů: t – plány

Cílem zkoušek spolehlivosti je odhad parametrů spolehlivosti, které reprezentují nejen vybraný zkušební soubor, ale všechny vyrobené výrobky, tedy celou populaci. Pro tyto účely se parametr spolehlivosti určuje jako intervalový odhad na zvolené konfidenční úrovni C, ve kterém se nachází skutečný parametr populace s vysokou, předem stanovenou pravděpodobností.

Vzhledem ke skutečnosti, že u zkoušek spolehlivosti podle zkušebních plánů, se vyskytují cenzurované soubory dat, nelze pro ně jednoznačně určit typ rozdělení pravděpodobnosti náhodné veličiny. Z tohoto důvodu nelze pro odhad parametrů spolehlivosti použít metody intervalového odhadu. Lze však dokázat [4], že pro vztah parametru spolehlivosti získaného výběru (zkušebního souboru) a parametru spolehlivosti základního souboru (populace) existuje statistika, pro kterou platí, že má chí-kvadrát rozdělení pro zadanou konfidenční úroveň C a počet stupňů volnosti 2ν. Pro pravděpodobnost platí vztah (4.17):

$$P\left(\chi^2_{2\nu;\alpha/2} \le 2\nu \cdot \frac{\hat{\theta}}{\theta} \le \chi^2_{2\nu;1-\alpha/2} \right) = C = 1 - \alpha \tag{4.17}$$

kde:

$\hat{\theta}$ - parametr spolehlivosti zkušebního souboru [h]

θ - parametr spolehlivosti populace [h]

C - konfidenční úroveň [-]

α - hladina významnosti [-],

χ^2 - hodnota chí-kvadrát rozdělení [-].

V - počet stupňů volnosti [-].

Z uvedeného vztahu lze odvodit rovnice jak pro určení oboustranného konfidenčního intervalu (ohraničeného dolní a horní mezí), tak i jednostranného odhadu parametru spolehlivosti.

Při odhadu parametrů spolehlivosti s využitím zkušebních plánů se hledaný parametr spolehlivosti obvykle určuje jako levostranný konfidenční interval, kdy je pro daný parametr spolehlivosti vypočtena pouze dolní mez. Pak s pravděpodobností C je hodnota parametru spolehlivosti základního souboru (populace) rovna nebo větší než dolní mez intervalu.

Pro exponenciální rozdělení pravděpodobnosti dob do poruchy se dolní mez TD konfidenčního intervalu, představujícího intervalový odhad střední doby do poruchy, určí podle vztahu (4.18):

$$T_D \ge \frac{2 \cdot t_{AKU}}{\chi^2_{2\nu;C}} \tag{4.18}$$

kde:
T_D - dolní mez konfidenčního intervalu [h],
t_{AKU} - akumulovaná pracovní doba výrobků ve zkoušce [h],
χ^2 - hodnota chí-kvadrát rozdělení [-].

V uvedeném vztahu (4.18) představuje člen t_{AKU} [h] akumulovanou pracovní dobu výrobků zařazených do zkoušky. Jeho hodnota se určí jako součet doby činnosti všech výrobků po dobu zkoušky (do vzniku poruchy nebo do ukončení zkoušky, pokud porucha nevznikne), neboli platí vztah (4.19):

$$t_{AKU} = \sum_{i=1}^{r} t_i + (n - r) \cdot \tau \tag{4.19}$$

kde:
t_{AKU} - akumulovaná pracovní doba výrobků ve zkoušce [h],
t_i - doba do poruchy i-tého výrobku [h],
n - počet výrobků zařazených do zkoušky [-],
r - počet poruch výrobků při zkoušce [-],
τ - doba trvání zkoušky [h].

Hodnota chí-kvadrát rozdělení ve vztahu (4.18) se určí pro konfidenční úroveň C a počet stupňů volnosti 2ν, který je funkcí počtu poruch zkoušených výrobků r:

$$2\nu = 2 \cdot (r + 1) \tag{4.20}$$

kde:
2ν - počet stupňů volnosti [-],
R - počet výrobků zařazených do zkoušky [-],

V zájmu zachování konkurenceschopnosti výrobků na trhu je zájmem výrobce provedení zkoušek spolehlivosti během co nejkratší doby. Z přístupu využívající zkušební plány vyplývá, že zkrácení zkoušky se dosáhne zvýšením počtu výrobků zařazených do zkoušky.

Zkoušky spolehlivosti s využitím t – plánů a r – plánů, jsou tedy vhodnou a velice intenzivně využívanou technikou pro zjišťování parametrů spolehlivosti výrobků v oblasti funkční bezpečnosti dopravních prostředků.

Z tohoto důvodu byl zpracován v prostředí MS Excel elementární autorský software RTE, který umožňuje, v podstatě rychle a přehledně, tyto zkoušky na bázi t – plánů a r – plánů vyhodnotit včetně grafického výstupu.

Vzhled tohoto autorského softwaru pro vyhodnocení výše zmíněných zkušebních plánů je uveden na obr. 4.6.

Vyhodnocení zkoušek spolehlivosti					
Projekt:	Tlačítko				
T plán		ano	R plán		
Počet výrobků	[ks]	797	Počet výrobků	[ks]	15
Počet poruch	[-]	0	Počet poruch	[-]	10
Doba výměny (opr)	[h]	6			
Doba zkoušky	[dnů]	365			
Taku	[h]	6981720	Taku	[h]	1078
Počet st. volnosti	[-]	2	Počet st. volnosti	[-]	22
Konfidenční úroveň	[-]	0,5	Konfidenční úroveň	[-]	0,5
Chí-kvadrát (0,5)	[-]	1,386294	Chí-kvadrát (0,5)	[-]	21,33704
Konfidenční úroveň	[-]	0,7	Konfidenční úroveň	[-]	0,7
Chí-kvadrát (0,7)	[-]	2,407946	Chí-kvadrát (0,7)	[-]	24,93902
Konfidenční úroveň	[-]	0,9	Konfidenční úroveň	[-]	0,9
Chí-kvadrát (0,9)	[-]	4,60517	Chí-kvadrát (0,9)	[-]	30,81328
MTBF (0,5)	[h]	10072493	MTBF (0,5)	[h]	101,0449
MTBF (0,7)	[h]	5798902	MTBF (0,7)	[h]	86,45089
MTBF (0,9)	[h]	3032122	MTBF (0,9)	[h]	69,96983
Konf. úroveň vlastní	[-]	0,99	Konf. úroveň vlastní	[-]	0,99
Chí-kvadrát	[-]	9,21034	Chí-kvadrát	[-]	40,28936
MTBF (vlastní)	[h]	1516061	MTBF (vlastní)	[h]	53,51289

Zdroj: autor

Obr. 4.6 Software RTE pro vyhodnocení zkoušek spolehlivosti (příklad)

Další možnosti zrychlení zkoušek spolehlivosti jsou uvedeny v následující kapitole.

4.4.3 Zrychlené zkoušky spolehlivosti

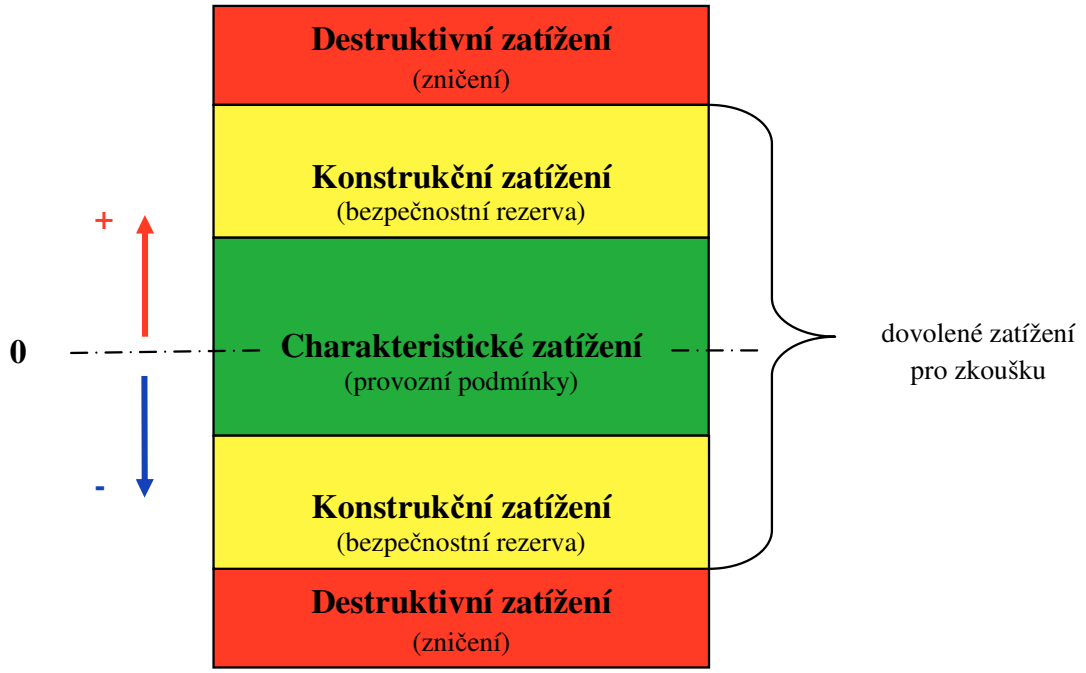
U mnoha systémů, výrobků nebo součástí se předpokládá jejich bezporuchová činnost po dlouhou dobu v řádu let. Aby bylo možné získat informace o skutečné úrovni spolehlivosti těchto systémů, je nutné provést zkoušku jejich spolehlivosti. Z důvodu nutnosti získání dat o dobách do poruchy výrobků a z důvodu zachování konkurenceschopnosti na trhu, musí být doba provádění zkoušky značně kratší než očekávaná doba života výrobku.

Metody zrychlení zkoušek spolehlivosti, jejichž cílem je získání konkrétních dat o spolehlivosti výrobku, jsou:

- zrychlení větším využitím,
- zrychlení přetížením.

Pro výrobky s velmi vysokou nebo nepřetržitou dobou provozu se musí v průběhu zkoušky spolehlivosti stimulovat vznik poruchy. Provádí se přivedením vyššího zatížení než je zatížení výrobku při normálních provozních podmínkách. Data o dobách do poruchy, získaná za těchto podmínek, jsou pak extrapolována pro provozní podmínky. Tyto zkoušky spolehlivosti mohou být prováděny při vysoké nebo nízké teplotě, vlhkosti, napětí, tlaku, vibracích atd., nebo při kombinaci těchto zatížení.

Při zrychlených zkouškách spolehlivosti musí být zvoleny druh a úroveň zatížení tak, aby se zrychlil proces těch poruch, které se vyskytují při provozním zatížení. Zrychlující zvýšené zatížení by nemělo vyvolat poruchy, které se v běžných provozních podmínkách nikdy nevyskytují (viz úrovně zatížení na obr. 4.7) [10].



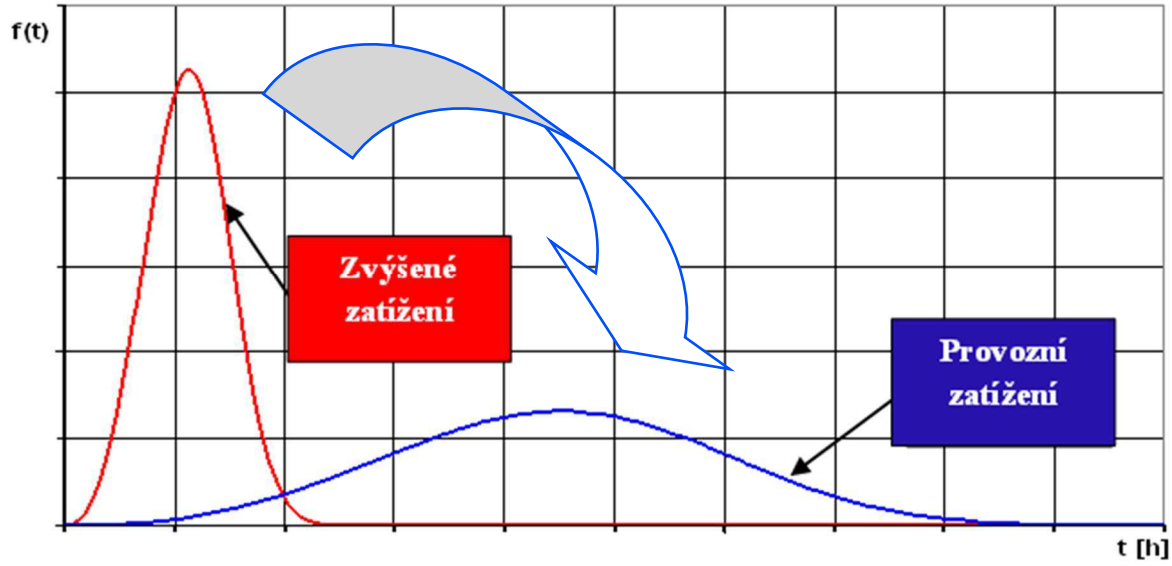
Zdroj: autor

Obr. 4.7 Úrovně zatížení výrobku

Volba druhu a úrovně zatížení má nejvyšší význam při plánování zrychlené zkoušky. Návrh zrychlené zkoušky musí být posuzován s ohledem na konstrukci výrobku a použité materiály tak, aby bylo možné určit stimulující zatížení a meze zvýšené úrovně zatížení.

Cílem prováděných zkoušek spolehlivosti je na základě získaných dat zjistit konkrétní charakteristiky spolehlivosti výrobku, jako střední hodnota, intenzita poruch, funkce bezporuchovosti apod., tedy zjistit průběh a konkrétní parametry rozdělení pravděpodobnosti

dob do poruchy. Průběh tohoto rozdělení popsaný např. funkcí hustoty pravděpodobnosti se při provozním zatížení a zvýšeném zatížení liší (viz obr. 4.8). Musí tak být známa metoda převodu výsledků ze zkoušky při zvýšeném zatížení na běžné provozní podmínky [10].



Zdroj: [7]

Obr. 4.8 Průběh hustoty pravděpodobnosti pro provozní a zvýšené zatížení

Modely zrychlených zkoušek

Pro běžně prováděné zrychlené zkoušky spolehlivosti se využívají následující modely závislosti doby života na zatížení, pro převod výsledků na normální provozní zatížení [6]:

- Arrheniův model,
- Eyringův model,
- model inverzní mocninné křivky,
- teplotně-netepelný model,
- teplotně-vlhkostní model,
- model více proměnných,
- model časově proměnného zatížení.

Arrheniův model

Arrheniův model závislosti doby života výrobku na zatížení je nejčastěji používaný vztah při provádění zrychlených zkoušek spolehlivosti v případech, kde zrychlující zatížení ke

stimulaci poruchy má tepelný charakter, např. teplota. Je odvozen z Arrheniovy rovnice rychlosti reakce [6]:

$$G(T) = A \cdot e^{-\frac{E_A}{K \cdot T}} \tag{4.21}$$

kde:
G(T) - rychlost reakce ,
A - netepelná konstanta [-],
E_A - aktivační energie [eV],
K - Bolzmanova konstanta [$eV.K^{-1}$],
T - absolutní teplota [K].

Aktivační energie je energie, kterou musí molekula mít, aby se mohla účastnit reakce, tedy míra vlivu teploty na reakci.

Arrheniův model závislosti doby života na zatížení je formulován za předpokladu, že doba života je úměrná obrácené hodnotě rychlosti reakce v procesu, tedy:

$$L(T) = C \cdot e^{\frac{B}{T}} \tag{4.22}$$

kde:
L(T) – kvantitativní ukazatel spolehlivosti (např. střední hodnota, medián),
T - úroveň zatížení[K],
C - parametr modelu (musí být určen),
B - parametr modelu (musí být určen).

V případech, kdy zvýšené zatížení je výlučně tepelné, lze parametr modelu B určit pomocí následujícího vztahu (4.21):

$$B = \frac{E_A}{K} \tag{4.23}$$

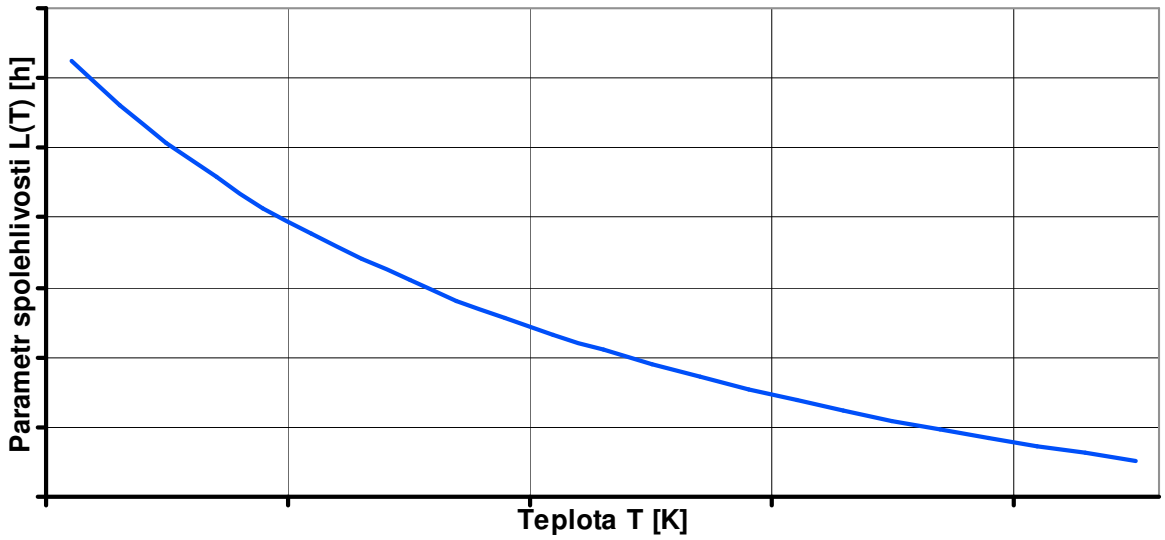
kde:
E_A - aktivační energie [eV],
K - Bolzmanova konstanta [$eV.K^{-1}$],

Faktor zrychlení, udávající poměr hodnot ukazatele spolehlivosti při provozním zatížení a vyšším zatížení při zrychlené zkoušce, je pro Arrheniův model určen vztahem (4.24):

$$A_F = \frac{L_U}{L_A} = \frac{C \cdot e^{\frac{B}{T_U}}}{C \cdot e^{\frac{B}{T_A}}} = e^{B \cdot \left(\frac{1}{T_U} - \frac{1}{T_A} \right)} \tag{4.24}$$

kde:

A_F - faktor zrychlení [-],
L_U - hodnota ukazatele spolehlivosti při provozním zatížení [h],
L_A - hodnota ukazatele spolehlivosti při zvýšeném zatížení [h],
T_U - úroveň zatížení při provozních podmínkách (absolutní teplota) [K],
T_A - zvýšená úroveň zatížení při zkoušce (absolutní teplota) [K],
K - Bolzmanova konstanta [$eV.K^{-1}$],
C - parametr modelu,
B - parametr modelu.



Zdroj: [7]

Obr. 4.9: Arrheniův model – závislost parametru spolehlivosti na teplotě

Pro možnost určení faktoru zrychlení zkoušky je nutné znát předem parametr modelu B, resp. aktivační energii. V praxi se aktivační energie E_A určuje vyhodnocením dob do poruchy skupin identických součástí zkoušených při různých teplotách, nebo je pro jednotlivé typy součástí uváděna v katalozích výrobků.

4.4.4 Predikce bezporuchovosti – elektronická část

V oblasti predikce bezporuchovosti elektronických systémů se nabízí využít predikčních metod integrovaných do postupů zmiňovaných například v MIL – HDBK – 217F, Bellcore i6, Telcordia i2 apod.

Na základě stanoveného pracovního prostředí jsou dále predikovány hodnoty intenzit poruch λ nebo střední doby do poruchy MTBF pro jednotlivé tvořící součástky systému.

4.4.5 Predikce bezporuchovosti – mechanická část - SBRA

V oblasti predikce bezporuchovosti mechanických systémů by bylo možno využít přístupu SBRA (Simulation-based Reliability Assessment). Pomocí metody SBRA by tedy bylo možné vypočítat pravděpodobnosti poruchy jednotlivých komponentů mechanické soustavy.

Metoda SBRA počítá pravděpodobnostními postupy přímo pravděpodobnost poruchy konstrukce. Všechny vstupní veličiny ovlivňující bezpečnost uvažuje jako náhodně proměnné vyjádřené ve formě histogramů rozdělení jejich hodnot. Jako matematický aparát využívá SBRA metodu Monte Carlo.

Za jednotlivé náhodně proměnné pak slouží například mez kluzu materiálu, plocha profilu, velikost a směr zatížení nebo imperfekcí a mnohé další. Pro jednotlivou simulaci podmínky bezpečnosti se náhodně vybere jedna konkrétní hodnota každé vstupní veličiny. Po dostatečně velkém množství simulací (v řádech miliónů) je možné stanovit pravděpodobnost poruchy jako podíl počtu vyhodnocených nevyhovujících výběrů k počtu všech provedených výběrů. Metoda je popsána například v literatuře [32].

5 Experimentální část – elektricky ovládané vstupní dveře

Postup využití kvantitativních metod v problematice funkční bezpečnosti je možno ukázat na příkladu elektricky ovládaných dveří pro autobus.

5.1 Popis systému

V této kapitole je představen postup užití některých kvantitativních metod funkční bezpečnosti. Cílem je ukázat postupy, nezbytné pro správné vyhotovení analytické části, ve které se posuzuje míra rizika objektu. Tyto postupy odpovídají schématu činností, uvedených v kap. 2.

Na základě identifikovaných nebezpečí, spojených s prací posuzovaného objekty (elektricky ovládané dveře autobusu), jsou sestaveny stromy poruch FTA a pro elementární události stromů poruch je provedena FMEA analýza včetně vyhodnocení včetně vyhodnocení a návrhu opatření.

5.2 Koncepční uspořádání a základní funkce dveří

Vstupní dveře se skládají ze dvou křídel a pohonu, který mechanickým spojením synchronně ovládá obě křídla.

Vnější ovládací tlačítko vstupních dveří je umístěno na vnější straně levého křídla poblíž čelní hrany dveří (při pohledu z vnější strany vozidla), vnitřní ovládací tlačítko je umístěno uvnitř vozidla na krytech vstupních dveří nebo madlech. Vstupní dveře je možné navíc vybavit orientačním zvukovým modulem pro nevidomé osoby, který je doplněn o přijímací jednotku povelů umožňující nevidomým osobám otevřít odblokované vstupní dveře.

Dále jsou vstupní dveře vybaveny světelnou LED lištou pro optickou signalizaci, mechanickým zámkem obou křídel vstupních dveří, ochrannou lištou proti nechtěnému přivření cestujícího, či zařízením nouzového ovládání.

Všechny elektrické komponenty použité pro ovládání vstupních dveří odpovídají platným normám pro provoz na silničním vozidle.

V duchu uvedeného je zařízení možno dekomponovat na následující prvky (subsystémy):

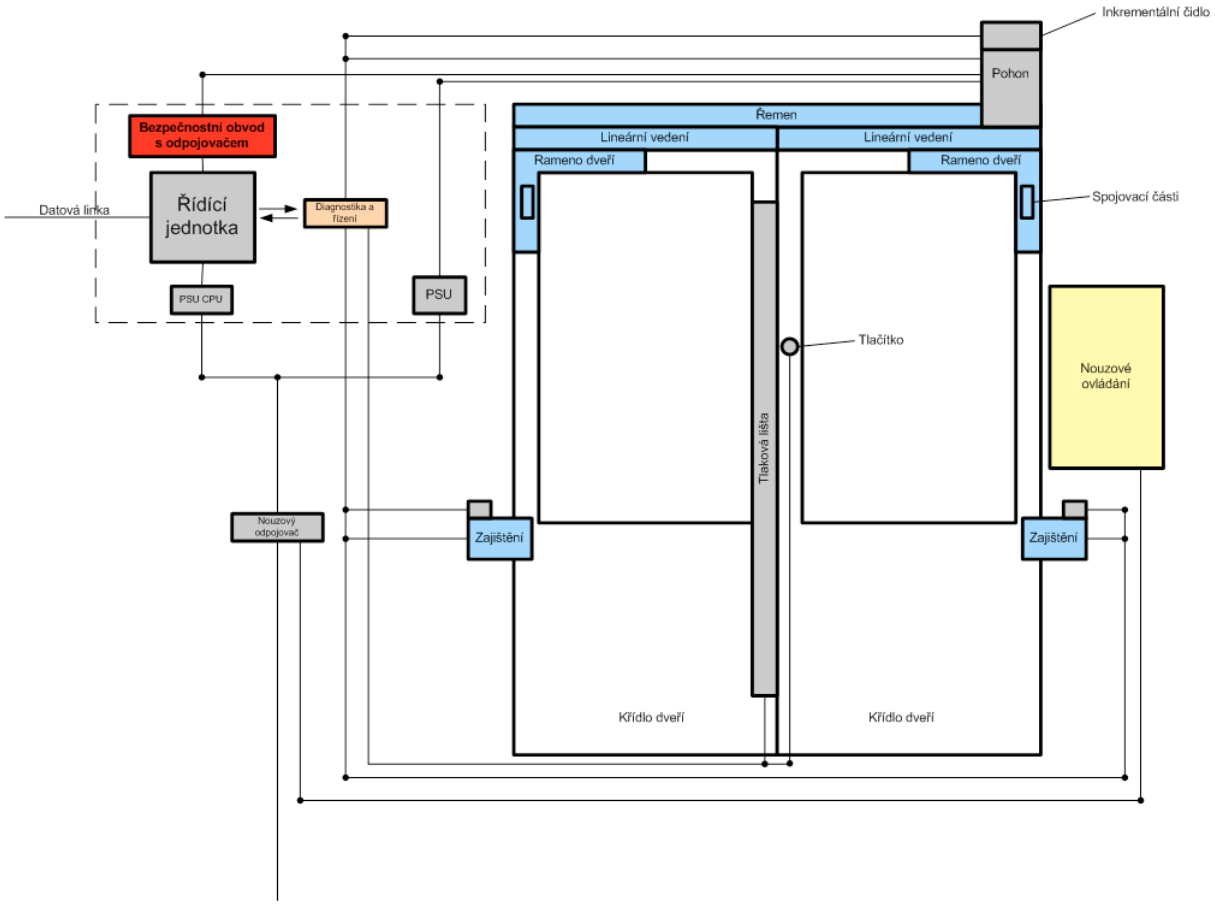
- **Řídící jednotka (CPU)**
    - Samostatná jednotka CPU
    - Blok diagnostiky a řízení
    - Zdroj PSU CPU
    - Zdroj PSU motoru
    - Obvod bezpečnostního odpojovače
    - Datová linka – ovládaní řídící jednotky dveří a kontrolky

- **Hlavní mechanické části dveří**
    - Křídlo dveří
    - Rameno dveří
    - Spojovací části dveří
    - Lineární vedení
    - Mechanické zajištění dveří

- **Pohon dveří a čidla**
    - Pohon – elektromotor
    - Řemen pohonu
    - Inkrementální čidlo
    - Tlačítko
    - Čidlo mechanického zajištění dveří
    - Tlaková lišta

- **Nouzové ovládání**
    - Táhla
    - Nouzový odpojovač
    - Páky
    - Čepy

Tyto prvky mají mezi sebou logické a funkční vazby takové, aby zařízení plnilo všechny požadované funkce správně a bezpečně tak, aby splňovalo požadavky funkční bezpečnosti. Blokové schéma, jež respektuje výše uvedené vazby je uvedeno na obr. 5.1.



Zdroj: autor

Obr. 5.1 Blokové schéma elektricky ovládaných dveří

Řídící jednotka (blok CPU) zajišťuje ovládání dveří, diagnostiku a komunikaci s nadřazeným systémem řízení (elektronikou vozidla). Od nadřazeného systému řízení dostává signál k otevření dveří. Svými výstupy ovládá pohon dveří a odjišťuje mechanické zajištění dveří. Dále snímá signály z příslušných čidel dveří (inkrementální čidlo, čidlo zajištění dveří, tlaková lišta).

5.3 Záznam o nebezpečí ASAM

Identifikace a hodnocení nebezpečí je prvním a nejdůležitějším krokem spojeným s hodnocením rizik dopravního prostředku, jeho subsystému nebo jeho komponentu.

Pro provedení identifikace a hodnocení nebezpečí byl navržen integrovaný postup ASAM (Automotive Safety Assesment Method), jež umožňuje přehledné a částečně automatizované

činnosti. O hodnocení pomocí metody ASAM pojednává kapitola 3.2. Jedná se o přístup kvalitativní, což možná na první pohled nezapadá do experimentální části s využitím kvantitativních metod funkční bezpečnosti, ale tento krok je nezbytný pro identifikaci nebezpečí a přiřazení úrovní integrity bezpečnosti ASIL těmto nebezpečím. Na základě konkrétní úrovně integrity bezpečnosti ASIL pro jednotlivá identifikovaná nebezpečí jsou pak přijata konkrétní opatření pro snížení úrovně rizika dle přístupu ALARP (viz kap. 3.1).

Každé identifikované nebezpečí je samostatně hodnoceno s využitím postupů ASAM (viz kap. 3.2) a výsledkem je konkrétní hodnota Klasifikačního indikátoru, který určuje požadovanou úroveň integrity bezpečnosti ASIL. Konkrétní úrovně integrity bezpečnosti ASIL pro jednotlivá identifikovaná nebezpečí s využitím formuláře „Záznam o nebezpečí" jsou uvedeny v tab. 5.1.

Výsledkem analýzy nebezpečí je identifikace pěti poruchových stavů dveří, kdy u tří poruchových stavů musí návrh dveří respektovat požadavek ASIL B, dva poruchové stavy ASIL C. Ostatní poruchové stavy jsou pro cestující možná nepříjemné, ale z hlediska bezpečnostní analýzy nepředstavují riziko, které je nutné snížit.

Další analýzy budou metodicky zaměřeny na poruchové stavy vedoucí k vzniku nebezpečí, v tabulce jsou označeny jako H1, H2, H3, H4, H5, H6 a H7.

Po primární analýze hrozících nebezpečí tedy následuje analýza stromů poruch FTA. Ta je pro uvažovaná nebezpečí zpracována v následující kapitole.

Tab. 5.1 Záznam o nebezpečí pro dveře

INSTITUT DOPRAVY VŠB-TU OSTRAVA ©MR	INSTITUT DOPRAVY, Fakulta strojní, VŠB TU - Ostrava Hodnocení nebezpečí	Dokument č.	
		Změna č.	
Výrobek:	Vstupní dveře s elektrickým pohonem	Požadavek č.	
Číslo výkresu:		Název projektu :	
Předkladatel:	Ing. et Ing. Michal Richtář	Datum:	
Zaznamenal:	Ing. et Ing. Michal Richtář	Datum:	
Pracovník odpovědný za navržená opatření:		Datum:	
Schválil:		Datum:	

No.	Nebezpečí	Popis nebezpečí - následky nebezpečí	Příčiny nebezpečí, uzly, zařízení	Hodnocení nebezpečí podle ASAM						
				Škody počet (SA)	Škody zranění (SV)	Pravděp odobnost výskytu (W)	Doba vystavení (E)	Zamezení (V)	Klasifikační indikátor (I)	ASIL
H1	Náhlé uvolnění (otevření, odpadnutí) vstupních dveří	1 a více osob (u dveří může stát pouze jedna osoba, popřípadě se na dveře může tlačit více osob) - lehké zranění (vypadnutí při nízké rychlosti na vozovku nebo na ostrůvek), těžká zranění (vypadnutí při vysoké rychlosti na vozovku, nebo na ostrůvek) smrt (vypadnutí při vysoké rychlosti na vozovku a střet s vozidlem), kritické nebezpečí	1) násilím došlo k zničení zámku dveří, 3) dveře odpanou poškozením závěsu, 4) selže elektronika, 5) funkční nouzové ovládání (dveře se jim daly otevřít), 6) dveře odpadnou poškozením závěsu - vysoké zatížení šroubů, držící dveře v závěsu	5,00	9,00	1,70	1,30	1,00	99	C
H2	Vozidlo nejde opustit dveřmi - standardní situace, dveře se neotevřely: výstup, nástup cestujících na zastávce	1 a více osob, vznikne panika - lehká zranění (v důsledku tlačenice k jiným dveřím), nezávažné nebezpečí	1) selhání elektroniky, 2) nedošlo k mechnickému oblokování dveří, 3) zamrznutí dveří, 4) dveře byly z důvodu poruchy odstaveny (nebyly označeny)	5,00	2,00	1,70	1,00	1,00	17	0
H3	Vozidlo nejde opustit dveřmi - nouzová situace, dveře se neotevřely, nejdou otevřít po nehodě : výstup	1 a více osob, vznikne panika - těžká zranění (např. oheň v blízkosti cestujících, avšak možnost úniku z vozidla), smrt (oheň v bezprostřední blízkosti dveří, kde cestující stojí a kde dveře nejdou otevřít), závažné nebezpečí	1) selhání nouzového ovládání dveří, 2) násilné poškození dveří - zničení zámku, 3) pohon způsobil neotevření dveří	5,00	9,00	1,70	1,30	1,70	59	B
H4	Osoba (cestující) je dveřmi přivřena : nástup, výstup	1, popř. 2 osoby (do dveří může vcházet pouze jedna osoba, ale i matka s dítětem nebo se mohou předhánět školáci)- těžká zranění (amputace některé části těla), smrt (nevšimnutí si přivřené osoby a následně dojde k rozjetí vozidla), nezávažné nebezpečí	1) selhání elektroniky, 2) neopartnost cestujícího, 3) řidič si nevšiml nastupujícícho cestujícího	3,00	9,00	1,70	1,00	1,00	46	B
H5	Nezavření (nedovření) dveří, vozidlo se rozjede	1 a více osob (při jízdě dojde k nečekanému otevření dveří) - lehká zranění (dojde k otevření dveří při nižší rychlosti - přiskřípnutí cestujících poblíž dveří), těžké zranění (otevření dveří při vysoké rychlosti - zlomeniny, rozdrcení kostí) : pokračuje viz. bod H1, kritické nebezpečí	1) zaklíněný předmět ve dveřích (schválně) - nemístný žert, 2) náhodně zaklíněný předmět, 3) nefunkční jedna část mechanického zavírání, 4) elektronika	5,00	9,00	1,70	1,30	1,00	99	C
H6	Vznícení (požár) dveří	1 a více osob - těžké zranění (cestující má možnost se vzdálit od ohniska požáru a zachránit se), nezávažné nebezpečí	1) zkrat nebo jiné poškození el. Instalace, 2) vysoká venkovní teplota, 3) intenzivní sluneční záření	5,00	2,00	1,00	1,30	1,00	13	0
H7	Zabití, zranění elektrickým proudem	1 osoba - zranění (jedná se o 24V) smrt 1 i více osob (na dveře spadne trolej), závažné nebezpečí	1) špatné ukostření 2) špatné izolační kabely	5,00	9,00	1,00	1,30	1,00	59	B

5.4 Analýza stromů poruch FTA pro dveře

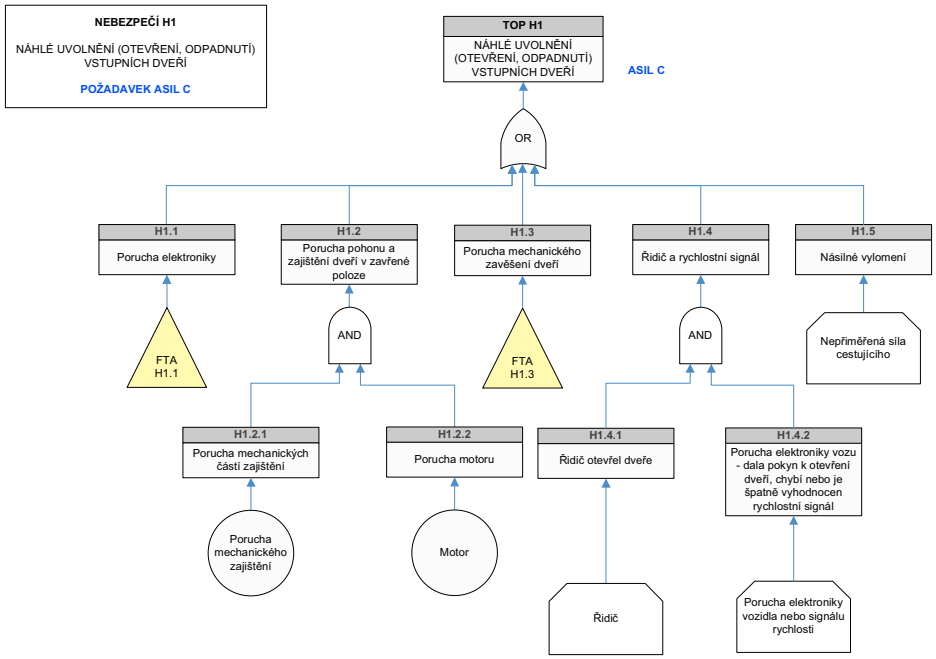
Analýza stromů poruch je kvalitativní a současně i kvantitativní metodou, doporučenou jak mateřskou normou ČSN EN 61508 tak i automobilní ISO 26262 pro činnosti ve fázi posuzování funkční bezpečnosti.

Na základě provedené identifikace nebezpečí (viz tab. 5.1) jsou v této kapitole rozkresleny stromy poruch FTA pro jednotlivá identifikovaná nebezpečí (hazardy). Každé identifikované nebezpečí pak představuje nejvyšší hladinu (top jev) v konkrétním stromu poruch. Cílem je postupnou dekompozicí nalézt dle míry této dekompozice konkrétní součást nebo uzel, jehož selhání způsobí vrcholovou událost (nebezpečí).

Jelikož jsou jednotlivým nebezpečím, jak bylo uvedeno výše (viz tab. 5.1), přiřazeny konkrétní hodnoty úrovně integrity bezpečnosti ASIL, jsou stromy poruch také doplněny o hodnoty úrovně integrity bezpečnosti ASIL pro všechny prvky v jednotlivých hladinách.

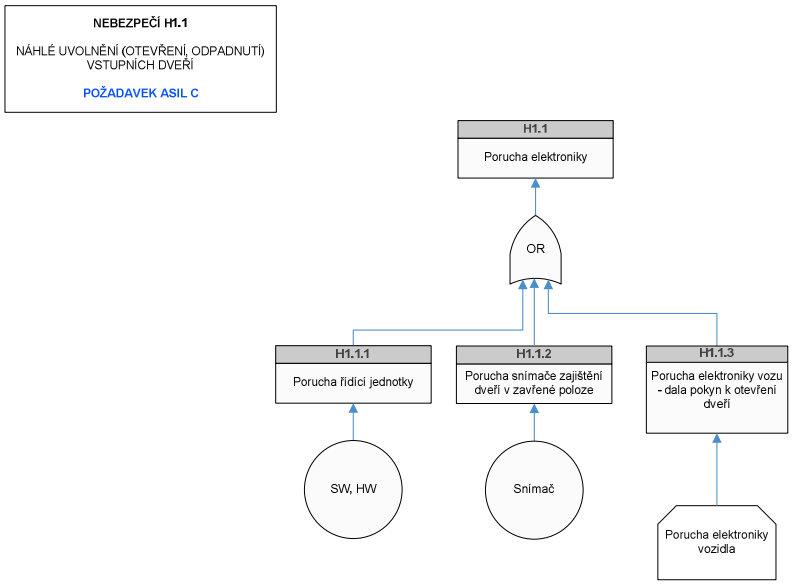
Pro všechny stromy poruchových stavů FTA byly vypracovány příslušné formuláře, které respektují základní definovaná pravidla označování (viz kap. 3.5) a které jsou součástí vyžadované dokumentace pro funkční bezpečnost.

Konkrétní stromy poruch FTA pro identifikovaná nebezpečí jsou uvedeny na následujících obrázcích:



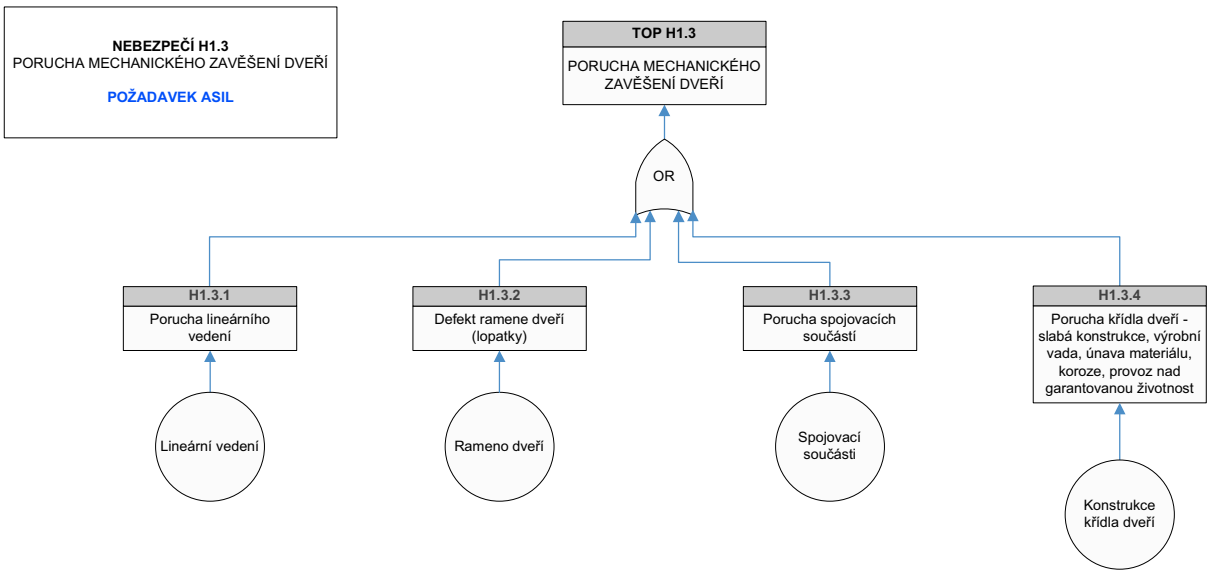
Zdroj: autor

Obr. 5.2 FTA analýza pro nebezpečí H1



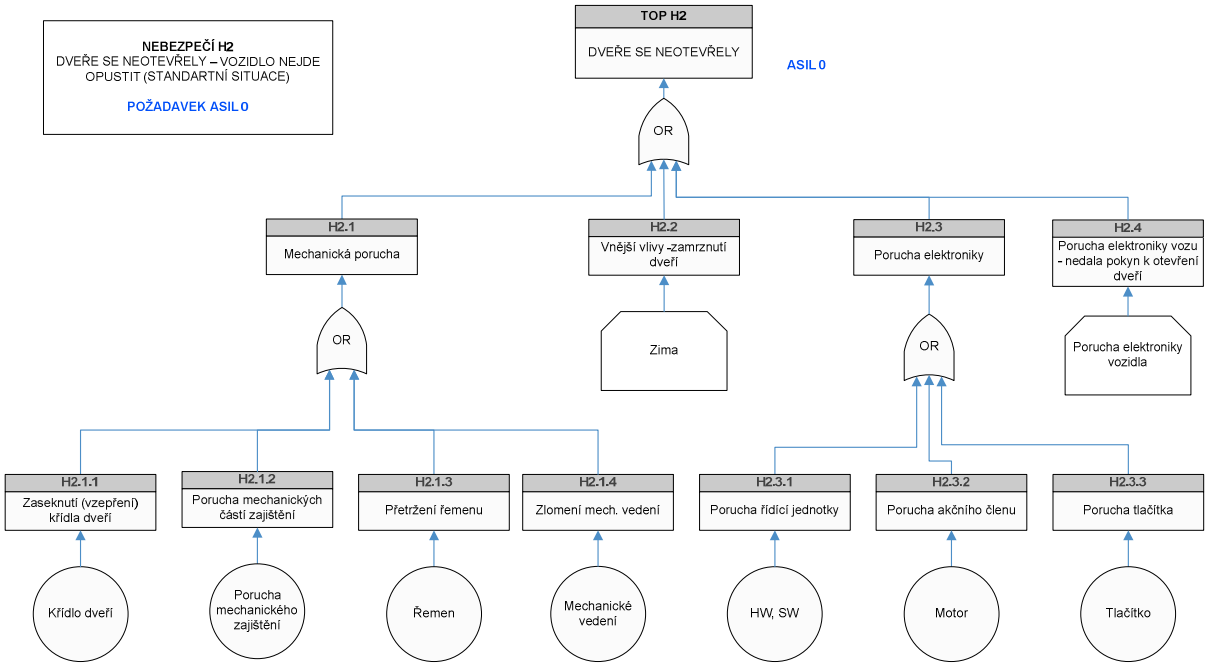
Zdroj: autor

Obr. 5.3 FTA analýza pro nebezpečí H1, část H1.1



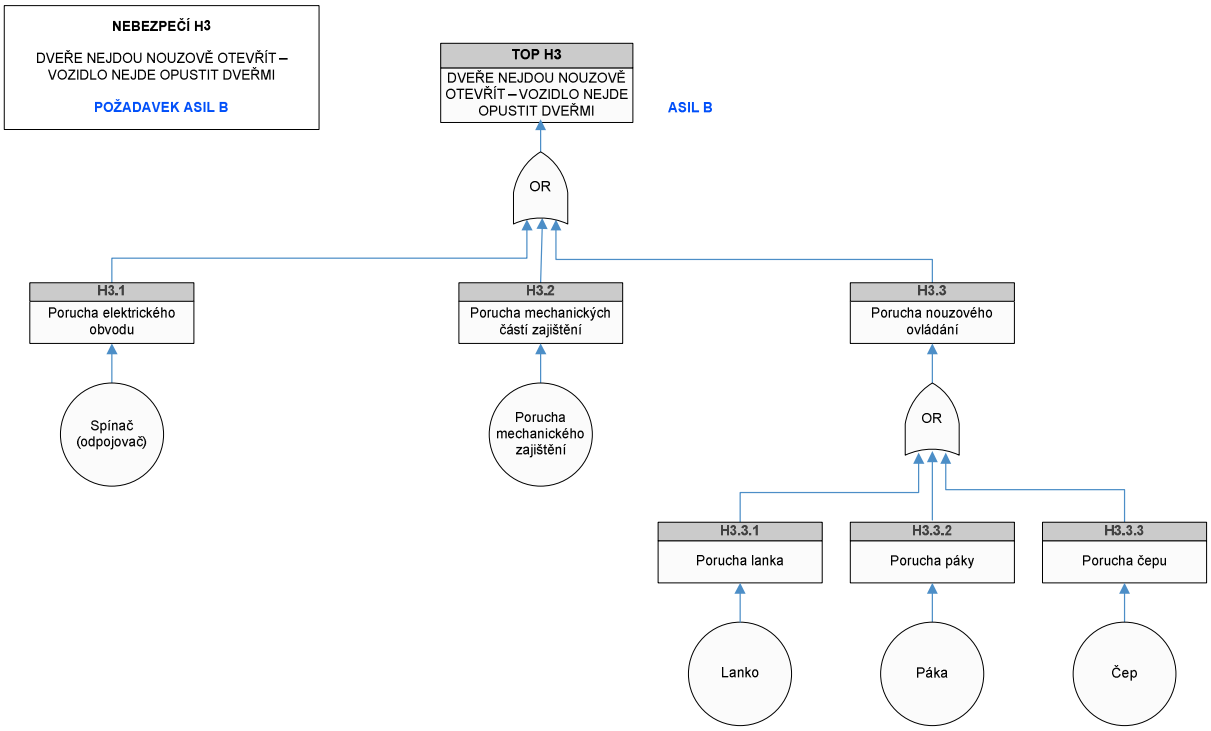
Zdroj: autor

Obr. 5.4 FTA analýza pro nebezpečí H1, část H1.3



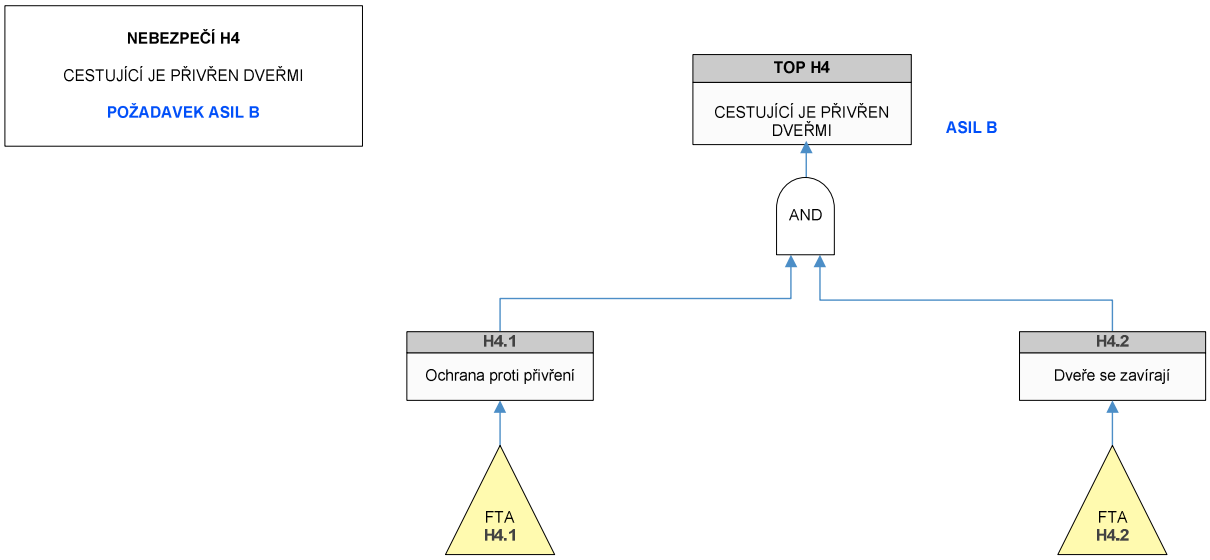
Zdroj: autor

Obr. 5.5 FTA analýza pro nebezpečí H2



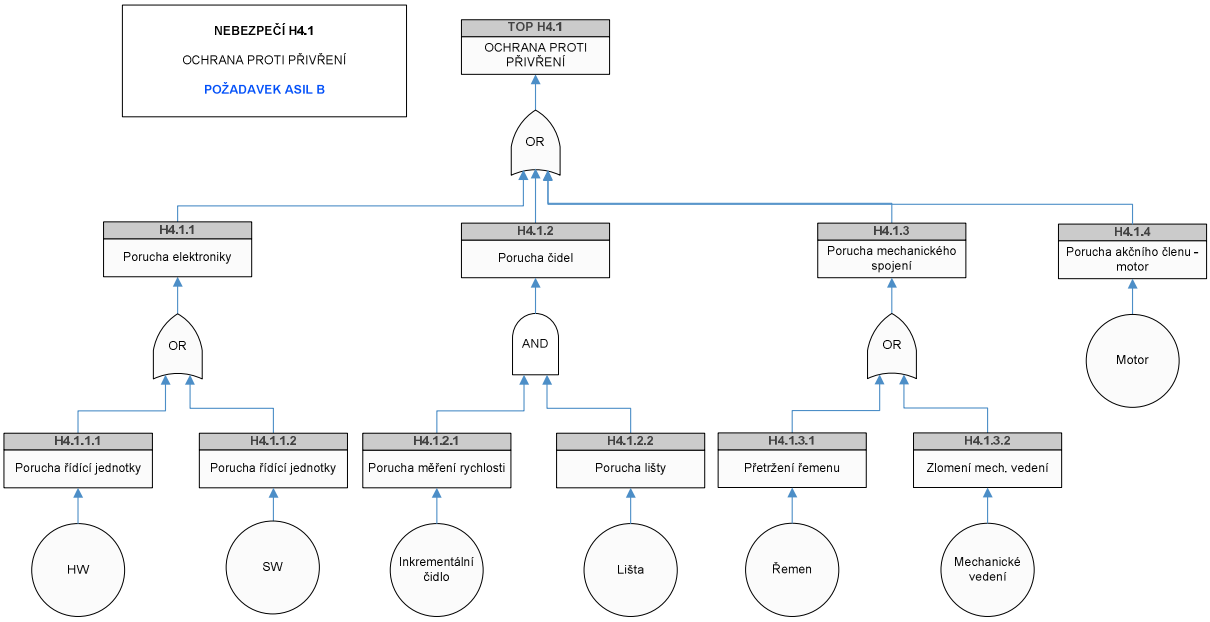
Zdroj: autor

Obr. 5.6 FTA analýza pro nebezpečí H3



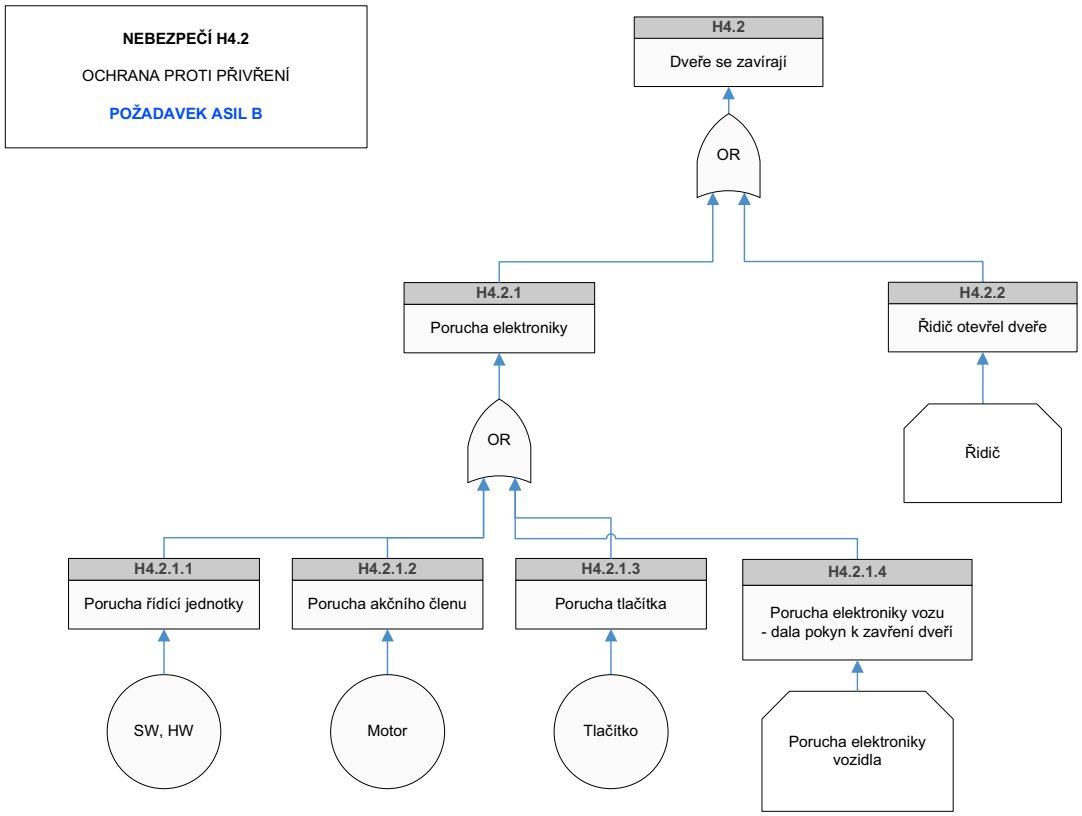
Zdroj: autor

Obr. 5.7 FTA analýza pro nebezpečí H4



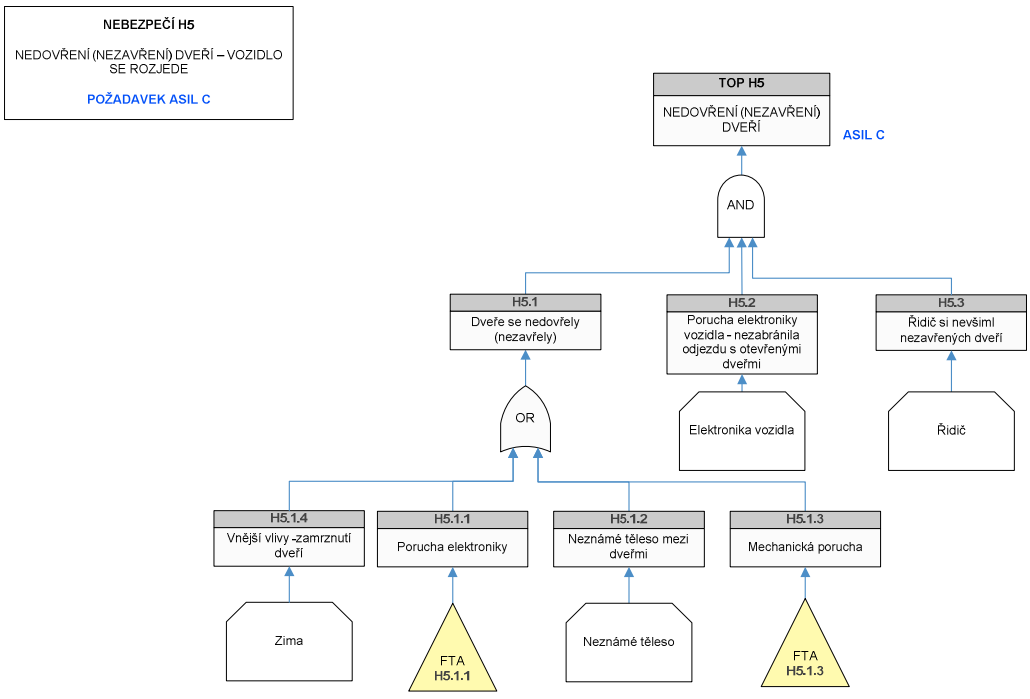
Zdroj: autor

Obr. 5.8 FTA analýza pro nebezpečí H4, část H4.1



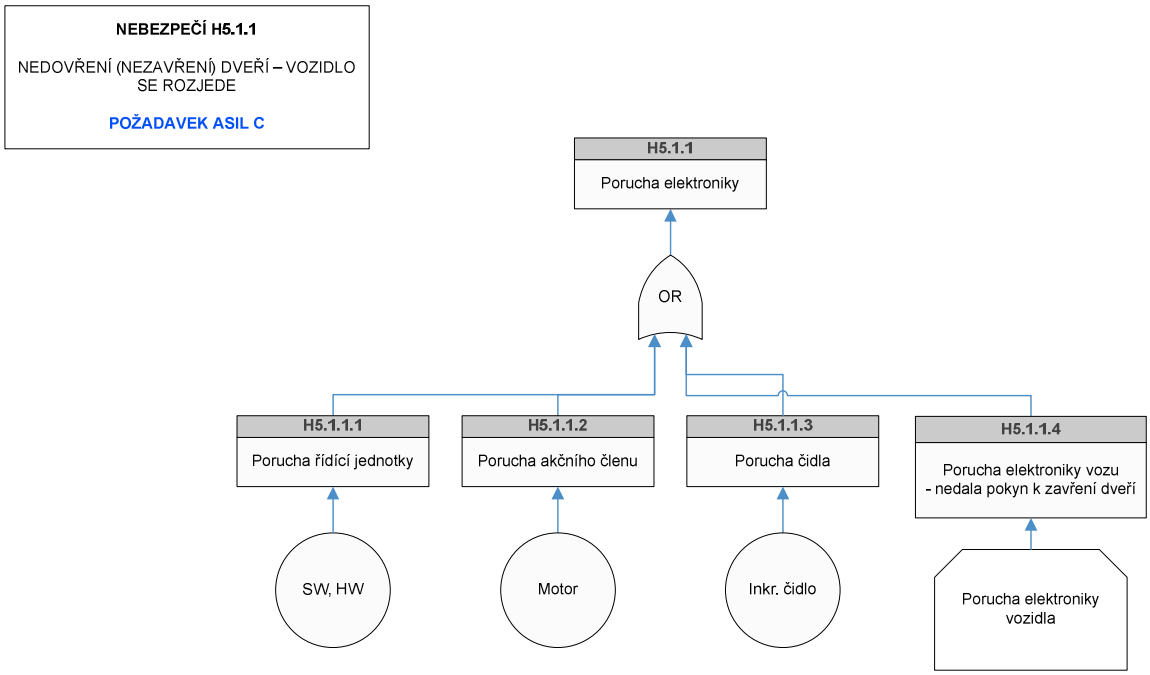
Zdroj: autor

Obr. 5.9 FTA analýza pro nebezpečí H4, část H4.2



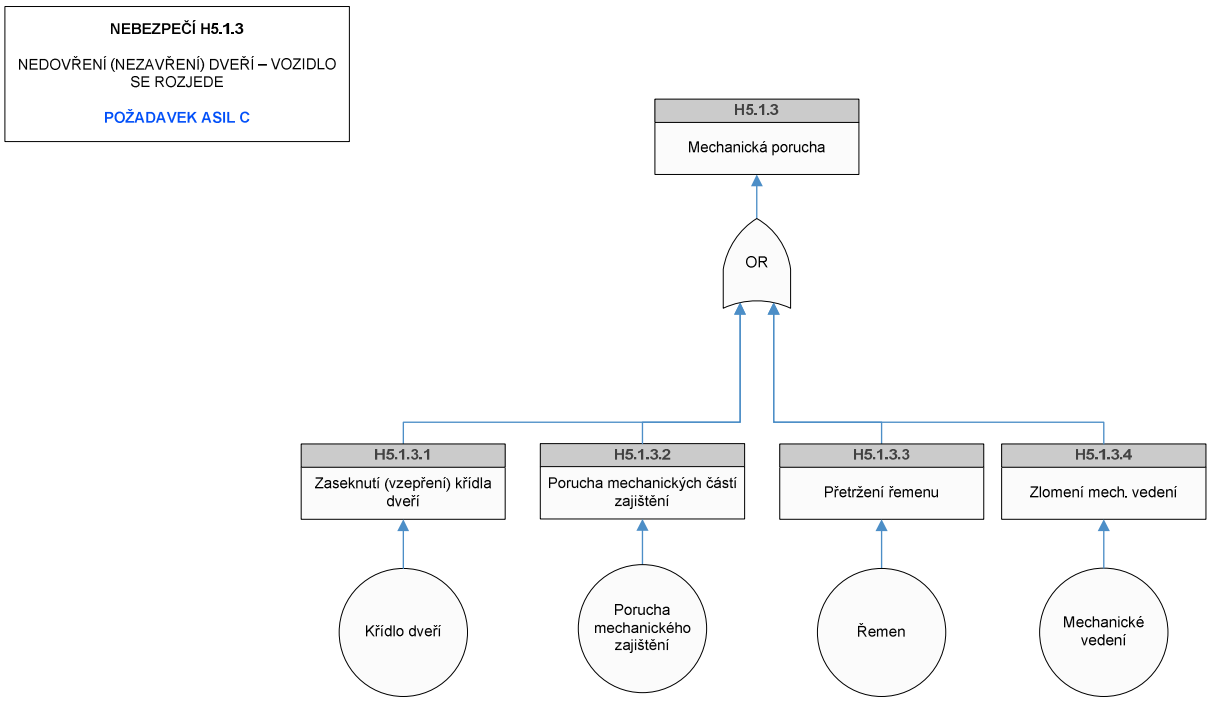
Zdroj: autor

Obr. 5.10 FTA analýza pro nebezpečí H5



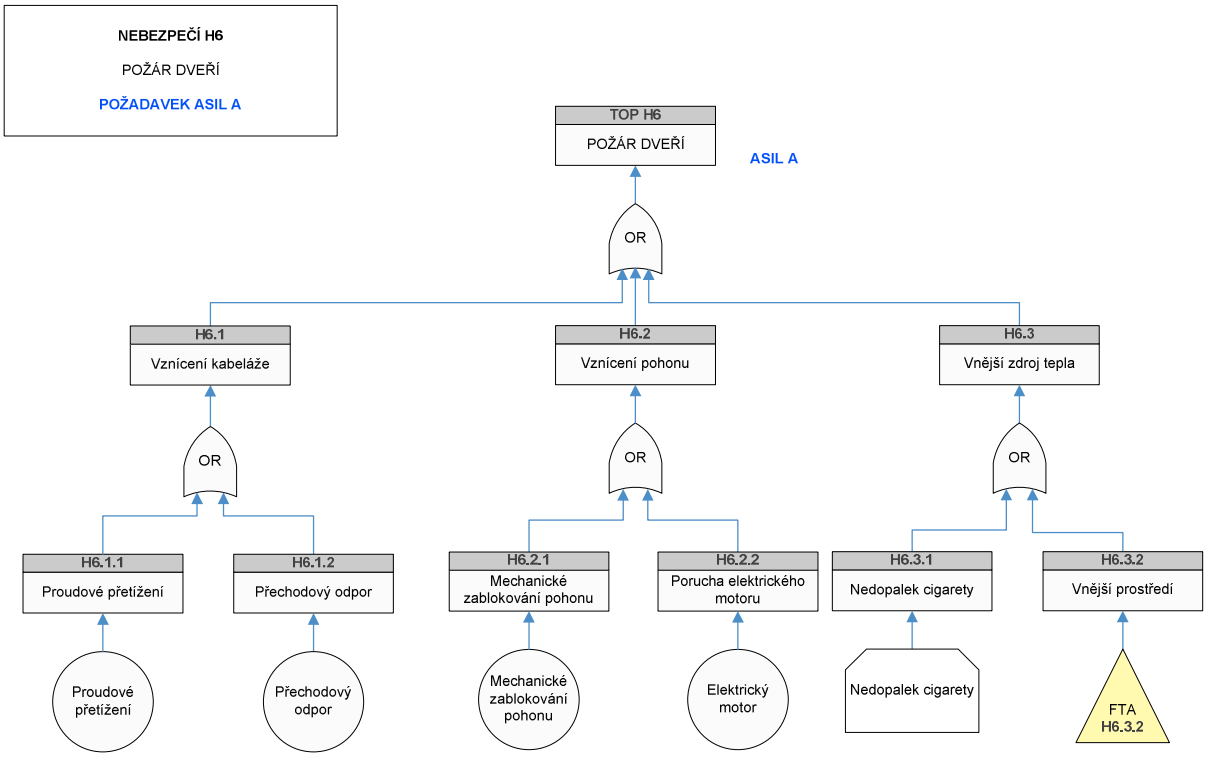
Zdroj: autor

Obr. 5.11 FTA analýza pro nebezpečí H5, část H5.1.1



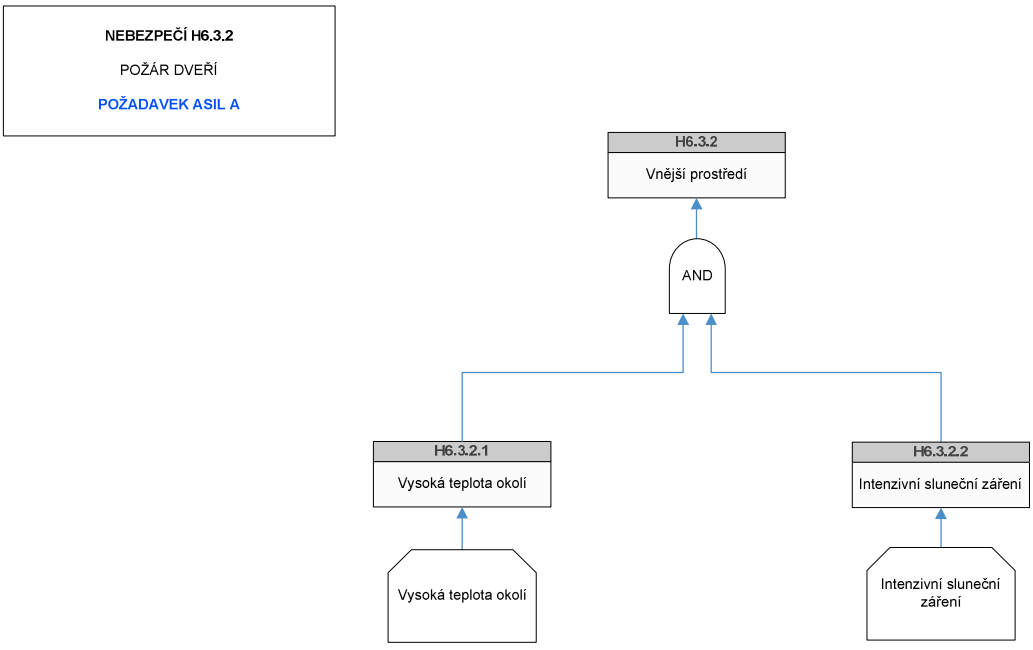
Zdroj: autor

Obr. 5.12 FTA analýza pro nebezpečí H5, část H5.1.3



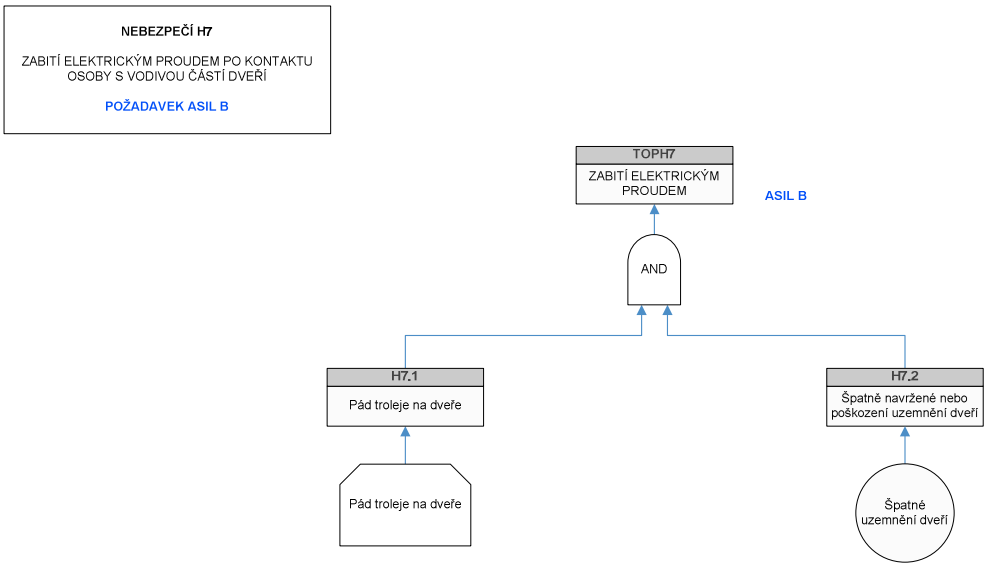
Zdroj: autor

Obr. 5.13 FTA analýza pro nebezpečí H6



Zdroj: autor

Obr. 5.14 Strom poruch FTA pro nebezpečí H6, část H6.3.2



Zdroj: autor

Obr. 5.15 FTA analýza pro nebezpečí H7

Dílčí závěr:

Z uvedené analýzy vyplývá, že na celkové bezpečnosti se podílí nejen elektrická část objektu, ale také část mechanická. Elementární příčiny poruch budou dále analyzovány pomocí metody FMEA.

5.5 Analýza FMEA

Analýza FMEA je kvalitativní metodou, doporučenou jak mateřskou normou ČSN EN 61508 tak i automobilní ISO 26262 pro činnosti ve fázi posuzování funkční bezpečnosti.

Pro možnost vyhodnocení analýzy FMEA je určována relativní významnost poruchy (viz kap. 3.6), která je označována jako hodnota „Risk Priority Number“ (RPN). V rámci výpočtu rizikového čísla RPN se hodnotí parametry závažnosti, četnosti výskytu a odhalitelnosti poruchy. Klasifikace závažnosti, četnosti výskytu a odhalitelnosti odpovídá klasifikaci dle tab. 3.19, tab. 3.20 a tab. 3.21.

Maximální hodnota rizikového čísla RPN (RPN = S x O x D) s využitím výše uvedené klasifikace tedy může dosáhnout hodnoty RPN = 120 (RPN = 4 x 6 x 5). Za hranici přijatelného rizika (mezní hodnotu) se u této konkrétní klasifikace považuje hodnota RPN = 12 (zhruba 10x méně než je maximální hodnota). Snahou je tedy dostat se pod uvedenou mezní hodnotu rizikového čísla RPN s využitím přijetí nutných opatření.

Vyhodnocení analýzy FMEA bude provedeno také pomocí zobrazení výsledků v matici závažnosti (matice rizika), která zohledňuje pouze hodnoty hodnocení – závažnost a četnost výskytu. Charakteristické rizikové číslo matice se označuje symbolem (SxO), jak bylo popsáno v kap. 3.7.

FMEA analýza zde bude metodicky provedena pouze vybraný strom poruch s cílem poukázat na z ní vyplývající opatření pro snížení rizika. Ostatní stromy poruch je samozřejmě ve firemní praxi nutno řešit obdobným způsobem.

Pro využití postupu FMEA analýzy je vybrán strom poruch odpovídající identifikovanému nebezpečí H1. Provedená FMEA analýza pro nebezpečí H1 je uvedena v tab. 5.2.

Tab. 5.2 FMEA analýza pro vybraný systém dveří – část 1

Funkce	Porucha	Dusledek	Příčina	Si	Oi	Di	RPNi	(SxO)i	Opatření technické (BF)	Typ BF	Opatření organizační a legislativní	Opatření údržbové	Opatření vnějším systémem	Sr	Or	Dr	RPNr	(SxO)r
H1 - Náhlé uvolnění (otevření, odpadnutí) vstupních dveří																		
Náhlé uvolnění (otevření, odpadnutí) vstupních dveří	Porucha HW řídící jednotky.	Řídící jednotka dá pokyn k otevření dveří když nemá, možnost zranění osob.	ChF - Chyba funkce	2	3	4	24	6	Uvedení řídící jednotky do bezpečného stavu. Signalizace poruchy řidiči.	BF1 BF2	Typová zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola bezpečnostní funkce po 30000km.	Není.	2	3	2	12	6
		Řídící jednotka nefunguje.	ZF - Ztráta funkce	1	3	4	12	3	Signalizace poruchy řidiči.	BF2	Typová zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola bezpečnostní funkce po 30000 km.	Není.	1	3	2	6	3
	Porucha SW řídící jednotky.	Nedojde k zastavení a otevření dveří, možnost zranění osob.	ChF - Chyba funkce	2	3	4	24	6	Testování SW řídící jednotky dle ISO 26262-6.		Není.	Není.	Není.	2	1	4	8	2
	Porucha mechanickéh o zajištění.	Dveře nejsou mechanicky jištěny, lze je lehce otevřít, možnost zranění osob.	ZF - Ztráta funkce	2	3	4	24	6	Vhodné dimenzování mechanismu jištění, kontrola pomocí MKP.		Životnostní zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Není.	2	1	4	8	2
	Porucha motoru.	Dveře nejsou zajišťovány motorem v zavřené poloze (nadproud), možnost zranění osob.	ChF - Chyba funkce	2	3	4	24	6	Motor s požadovanými technickými a spolehlivostními parametry.		Není.	Není.	Není.	2	1	4	8	2

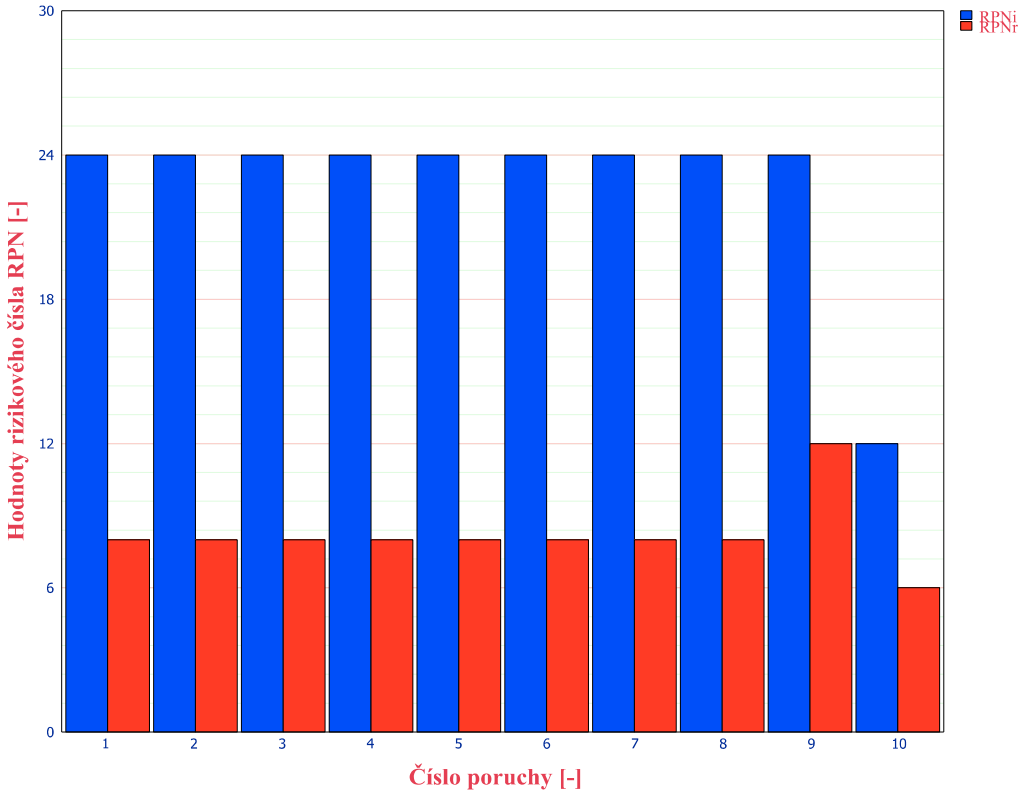
Tab. 5.2 FMEA analýza pro vybraný systém dveří – část 2

Funkce	Porucha	Dusledek	Příčina	Si	Oi	Di	RPNi	(SxO)i	Opatření technické (BF)	Typ BF	Opatření organizační a legislativní	Opatření údržbové	Opatření vnějším systémem	Sr	Or	Dr	RPNr	(SxO)r
H1 - Náhlé uvolnění (otevření, odpadnutí) vstupních dveří																		
Náhlé uvolnění (otevření, odpadnutí) vstupních dveří	Porucha snímače zajištění dveří v zavřené poloze.	Není informace o stavu zajištění dveří.	ZF - Ztráta funkce	2	3	4	24	6	Signalizace poruchy řidiči. Snímač s požadovanými technickými a spolehlivostními parametry.	BF2	Řidič postupuje dle předpisů provozovatele.	Kontrola bezpečnostní funkce po 30000 km.	Není.	2	2	2	8	4
	Porucha lineárního vedení.	Možnost nekontrolovaného pohybu křídla dveří. Zranění osob.	ZF - Ztráta funkce	2	3	4	24	6	Vhodné dimenzování mechanismu lineárního vedení, kontrola pomocí MKP.		Životnostní zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Není.	2	1	4	8	2
	Defekt ramene dveří.	Možnost nekontrolovaného pohybu křídla dveří. Zranění osob.	ZF - Ztráta funkce	2	3	4	24	6	Vhodné dimenzování ramene dveří, kontrola pomocí MKP.		Životnostní zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu po ujení 30000 km.	Není.	2	1	4	8	2
	Porucha spojovacích součástí.	Možnost nekontrolovaného pohybu křídla dveří. Zranění osob.	ZF - Ztráta funkce	2	3	4	24	6	Vhodné dimenzování spojovacích součástí, utažení správným dotahovacím momentem.		Životnostní zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola a dotažení spojovacích částí správným dot. momentem po ujetí 30000km.	Není.	2	1	4	8	2

Tab. 5.2 FMEA analýza pro vybraný systém dveří – část 3

Funkce	Porucha	Dusledek	Příčina	Si	Oi	Di	RPNi	(SxO)i	Opatření technické (BF)	Typ BF	Opatření organizační a legislativní	Opatření údržbové	Opatření vnějším systémem	Sr	Or	Dr	RPNr	(SxO)r
H1 - Náhlé uvolnění (otevření, odpadnutí) vstupních dveří																		
Náhlé uvolnění (otevření, odpadnutí) vstupních dveří	Porucha křídla dveří.	Možnost nekontrolovaného pohybu křídla dveří. Zranění osob.	ZF - Ztráta funkce	2	3	4	24	6	Vhodné dimenzování křídla dveří, kontrola pomocí MKP.		Životnostní zkouška. Řidič postupuje dle předpisů provozovatele.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Není.	2	1	4	8	2

Grafické zobrazení výsledků FMEA analýzy, tedy účinnost přijatých opatření ke snížení rizika pomocí hodnocení rizikového čísla RPN je uvedeno na obr. 5. 16.



Zdroj: autor, [26]

Obr. 5.16 Počáteční a koncové hodnoty RPN

Počáteční a koncové hodnoty RPN dle poruch z obr. 5.16 jsou následující:

1 RPNi = 24, RPNr = 8 - Porucha křídla dveří. (ZF)

2 RPNi = 24, RPNr = 8 - Porucha spojovacích součástí. (ZF)

3 RPNi = 24, RPNr = 8 - Defekt ramene dveří. (ZF)

4 RPNi = 24, RPNr = 8 - Porucha lineárního vedení. (ZF)

5 RPNi = 24, RPNr = 8 - Porucha snímače zajištění dveří v zavřené poloze. (ZF)

6 RPNi = 24, RPNr = 8 - Porucha motoru. (ZF)

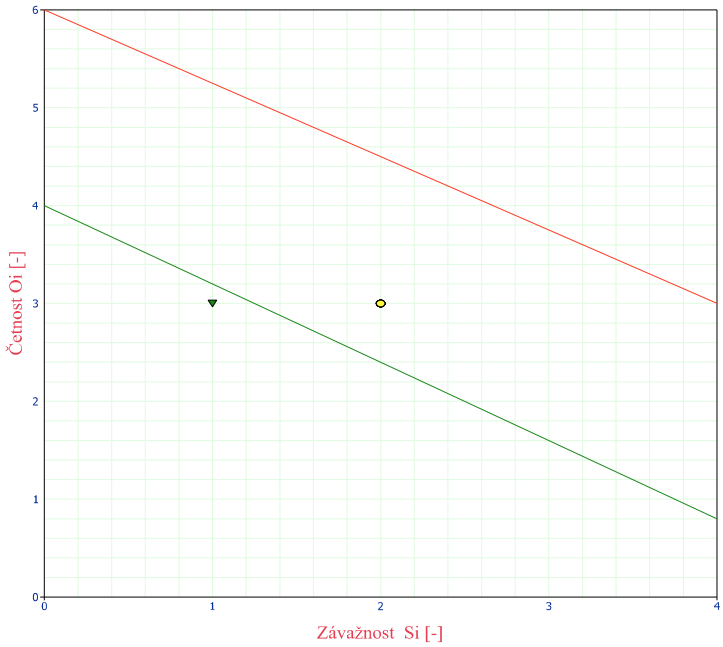
7 RPNi = 24, RPNr = 8 - Porucha mechanického zajištění. (ZF)

8 RPNi = 24, RPNr = 8 - Porucha SW řídící jednotky. (ChF)

9 RPNi = 24, RPNr = 12 - Porucha HW řídící jednotky. (ChF)

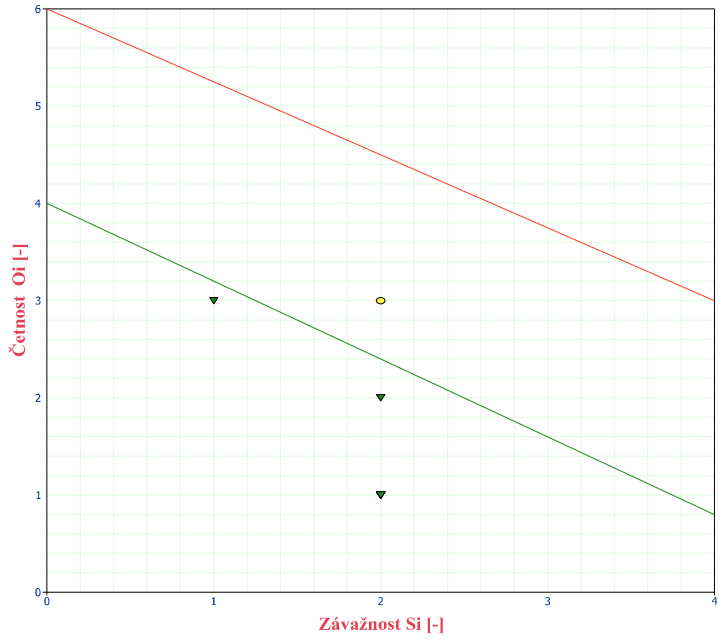
10 RPNi = 12, RPNr = 6 - Porucha HW řídící jednotky. (ZF)

Grafické zobrazení výsledků FMEA analýzy, pomocí hodnocení rizikového čísla matice závažnosti SxO bez opatření je uvedeno na obr. 5. 17. Hodnocení rizikového čísla matice závažnosti SxO po opatřeních je uvedeno na obr. 5. 18.



Zdroj: autor, [26]

Obr. 5.17 Grafické vyjádření matice závažnosti SxO bez opatření



Zdroj: autor, [26]

Obr. 5.18 Grafické vyjádření matice závažnosti SxO po opatřeních

Hodnocení rizikového čísla matice závažnosti SxO bez opatření ukazuje, že jediná z vyšetřovaných poruch se umístila v oblasti „Poruchy s nízkou prioritou“ (pod zelenou čarou v obr 5.17), kde není nutno přijímat žádná bezpečnostní opatření. Ostatní poruchy se umístily v oblasti „Poruchy se střední prioritou“ (mezi červenou a zelenou čarou v obr 5.17), kde je nutno zvážit přijetí bezpečnostní opatření. Žádná z vyšetřovaných poruch se neumístila v oblasti „Poruchy s vysokou prioritou“ (nad červenou čarou v obr 5.17). Konkrétní hodnocení bez opatření je následující:

Poruchy se střední prioritou

- Porucha křídla dveří. (ZF) Si = 2, Oi = 3
- Porucha spojovacích součástí. (ZF) Si = 2, Oi = 3
- Defekt ramene dveří. (ZF) Si = 2, Oi = 3
- Porucha lineárního vedení. (ZF) Si = 2, Oi = 3
- Porucha snímače zajištění dveří v zavřené poloze. (ZF) Si = 2, Oi = 3
- Porucha motoru. (ZF) Si = 2, Oi = 3
- Porucha mechanického zajištění. (ZF) Si = 2, Oi = 3
- Porucha SW řídící jednotky. (ChF) Si = 2, Oi = 3
- Porucha HW řídící jednotky. (ChF) Si = 2, Oi = 3

Poruchy s nízkou prioritou

- Porucha HW řídící jednotky. (ZF) Si = 1, Oi = 3

Hodnocení rizikového čísla matice závažnosti SxO po přijatých opatřeních ukazuje, že jediná z vyšetřovaných poruch se umístila v oblasti v oblasti „Poruchy se střední prioritou“ (mezi červenou a zelenou čarou v obr 5.18). Ostatní poruchy se umístily v oblasti „Poruchy s nízkou prioritou“ (pod zelenou čarou v obr 5.18. Žádná z vyšetřovaných poruch se neumístila v oblasti „Poruchy s vysokou prioritou“ (nad červenou čarou v obr 5.18). Konkrétní hodnocení po přijetí opatření je následující:

Poruchy se střední prioritou

- Porucha HW řídící jednotky. (ChF) Sr = 2, Or = 3

Poruchy s nízkou prioritou

- Porucha křídla dveří. (ZF) Sr = 2, Or = 1
- Porucha spojovacích součástí. (ZF) Sr = 2, Or = 1

- Defekt ramene dveří. (ZF) Sr = 2, Or = 1
- Porucha lineárního vedení. (ZF) Sr = 2, Or = 1
- Porucha snímače zajištění dveří v zavřené poloze. (ZF) Sr = 2, Or = 2
- Porucha motoru. (ZF) Sr = 2, Or = 1
- Porucha mechanického zajištění. (ZF) Sr = 2, Or = 1
- Porucha SW řídící jednotky. (ChF) Sr = 2, Or = 1
- Porucha HW řídící jednotky. (ZF) Sr = 1, Or = 3

Dílčí závěr:

Z uvedených analýz vyplývá, že identifikované poruchy vykazují jistou míru bezpečnostního rizika. Proto byla navržena konkrétní opatření (technická, organizační a legislativní, údržbová a vnějším systémem) pro jeho snížení na přijatelnou mez. Analýza pomocí matice závažnosti prokázala, že opatření jsou účinná. Jedinou poruchou, u které se nepodařilo snížit rizikové číslo matice závažnosti SxO, je porucha HW řídící jednotky dveří (chyba její funkce). Avšak FMEA analýza prokázala, že přijetím opatření ke snížení rizika se jej podařilo snížit na přijatelnou mez nejen u ostatních poruch, ale i u z matice závažnosti vyplývající poruchy HW řídící jednotky dveří (chyba její funkce). Zde konkrétně díky tomu, že zavedení bezpečnostních funkcí BF1 a BF2 výrazně zlepší odhalitelnost poruchy.

Ve formuláři v příloze III. jsou přehledně zpracována všechna opatření (technická, organizační a legislativní, údržbová a vnějším systémem), jež byla navržena pro vybrané nebezpečí H1 ke snížení úrovně rizika. Současně je i definována odpovědnost výrobce, dodavatele nebo provozovatele za dohled a realizaci těchto navržených bezpečnostních opatření ke snížení identifikovaného rizika.

Diskuze k obdrženým výsledkům:

Z představených analýz jasně vyplývá, že bezpečnost dveřního systému je rozdělena mezi elektronickou část a mechanickou část dveří.

Zajímavým, a to nejen v oblasti dopravních prostředků, je tedy pohled na systémovou architekturu posuzovaného objektu. Je evidentní, že v současné době jsou tyto systémy založeny na interakci mechanické části systému a elektronické části systému. Lze tedy hovořit v podstatě o systému mechatronickém.

Část cílové míry poruch takovéhoto systému připadá na systém elektronický a pochopitelně část cílové míry poruch připadá na systém mechanický. Související požadavky ISO 26262 a EN 61508 v podstatě deklarují požadavky na elektrické, elektronické a elektronické programovatelné systémy. Ale pokud bychom v podstatě nic nevěděli o pravděpodobnosti poruchy mechanického systému, jen velmi těžko můžeme systém považovat za bezpečný.

V této uvažované situaci by bylo možné realizovat v podstatě dvě možnosti řešení uvedeného požadavku:

Zkoušky spolehlivosti

Zařízení navrhnout, vyrobit a podrobit jej zkouškám spolehlivosti. Avšak v případě, že zařízení bude vykazovat nízké hodnoty intenzity poruch λ budou zkoušky náročné po časové a finanční stránce. Nebo využít zrychlené zkoušky výrobku [9].

Predikovat požadované parametry

Vytvořit a zpracovat stromy poruchových stavů (FTA) a blokové diagramy bezporuchovosti (RBD) pro mechanickou část systému do úrovně dílů, pro které by bylo možné využít metodu SBRA (Simulation-Based Reliability Assessment). Pomocí metody SBRA by tedy bylo možné vypočítat pravděpodobnosti poruchy jednotlivých komponentů mechanické soustavy a tyto pravděpodobnosti dále využít pro řešení soustavy pomocí RBD. Tímto postupem lze získat pravděpodobnost poruchy mechanické soustavy za navrženou životnost zařízení. Na základě tohoto lze dovodit cílovou míru poruch v duchu požadavků funkční bezpečnosti.

Navazující záležitostí je také problematika diagnostického pokrytí. U elektronických systémů můžeme úspěšně navrhnout a realizovat toto diagnostické pokrytí (DC). Otázkou však zůstává, jakým způsobem zajistit diagnostické pokrytí o mechanické části systému. Zde je možno uvážit následují postupy:

- **Periodická kontrola funkce**

  Předepsat opakované zkoušení funkce ve stanových intervalech. Tento přístup však nelze použít za všech situací a u všech prvků.

- **Nedestruktivní kontrola prvků**

  Kontrolovat prvky s využitím nedestruktivních metod (např. defektoskopie)

- **Využít dobrou identifikovatelnost závady**

Identifikace, ale bez nebezpečí, např. viditelného lomu – v podstatě 100% diagnostické pokrytí.

- **Elektronický systém**

  Některé prvky mechanického systému by mohly být hlídány vhodnou elektronikou. Elektronický systém, který se stará o bezpečnostní funkce elektronické části nemůže a nesmí řešit diagnostické pokrytí mechanické části systému. Mechanický systém musí být diagnostikován jinou částí elektroniky.

S tím ale souvisí otázka toho, jakou úroveň integrity bezpečnosti (SIL, ASIL) musí takový elektronický systém splňovat:

- Buď musí být úroveň integrity bezpečnosti (SIL, ASIL) této části elektronického systému na úrovni integrity bezpečnosti (SIL, ASIL) mechanické části systému
- Nebo musí dát dohromady s mechanickým systémem požadovanou úroveň integrity bezpečnosti (SIL, ASIL) na mechanický systém

V souvislosti s uvedenými skutečnostmi vyvstává otázka toho, jakým způsobem a na jaké úrovni vlastně hodnotit schopnost mechanické soustavy splňovat požadavky integrity bezpečnosti.

Jednou z možností je inovativně, vzhledem k požadavkům ISO 26262 a EN 61508, nastavit úroveň integrity bezpečnosti pro mechanickou soustavu: **MSIL – Mechanical Safety Integrity Level**

V rámci tohoto hodnocení by byla prokazována cílová míra poruch na základě uvedených možností zjišťování nebo predikce pravděpodobnosti poruchy mechanického systému (zkoušky spolehlivosti, SBRA), diagnostického pokrytí (periodická kontrola, defektoskopie) a definovaných zásad konstruování mechanické části.

Pokud bude mechanický systém navržen na okamžitou identifikaci poruchy, tak by měl být navržen jedině v režimu stálé práce (horká záloha).

Pokud bude pracovat v režimu vyžádání (studená, spící záloha), pak je navržen s požadavky na periodickou kontrolu, kontrolu nedestruktivními metodami či požadavky na pravidelnou údržbu a kontrolu funkce.

Samostatně vedle mechanické soustavy stojí elektronika pro diagnostikování poruch, což by mělo platit jak pro systém pracující jako horká záloha, tak i pro systém pracující jako

studená záloha. Požadavek na úroveň integrity bezpečnosti (SIL, ASIL) musí být stejný, jako požadavek na úroveň integrity bezpečnosti pro mechanickou část (MSIL).

Pravděpodobnost poruchy elektronického systému a mechanického systému se vypočítává jiným způsobem, ale jelikož je pravděpodobnost bezrozměrná veličina, může se s ní pracovat dle zásad matematické teorie pravděpodobnosti s respektováním pravidel pro řešení soustav a lze tedy rozdělit požadavky na mechanický a elektronický subsystém. Principiálně je jedno, který systém zajistí snížení úrovně rizika. Výhodou je možnost využití např. paralelního řazení mechanického a elektronického systému, přičemž podíl snížení úrovně rizika jednotlivými systémy je v podstatě nevýznamný, důležitá je celková míra snížení úrovně rizika.

6 Experimentální část – návrh LED světlometu

Postup využití kvantitativních metod v problematice funkční bezpečnosti je možno ukázat na příkladu využití LED pro přední světlomety automobilu.

6.1 Popis systému

V této kapitole je představen postup užití některých kvantitativních metod funkční bezpečnosti. Cílem je ukázat postupy, nezbytné pro prokázání úrovně skutečné bezpečnosti posuzovaného objektu. Tyto postupy odpovídají schématu činností, uvedených v kap. 2.

Na základě identifikovaných nebezpečí, spojených s prací posuzovaného objekty (LED světlometu), jsou sestaveny stromy poruch (FTA) s využitím blokových a obvodových schémat a spočítána predikovaná spolehlivost a bezpečnost. Následně jsou navrženy vhodné zrychlené zkoušky pro ověření predikované bezpečnosti.

Požadavky na světla a světlomety jsou pro silniční vozidla dána zejména pro území Evropské unie (ale i další země) příslušnými předpisy EHK (ECE). Předpisů, upravující uvedenou oblast, je řada a vztahují se ke všem osvětlovacím systémům vozidla.

Pro LED světlomety pak existuje předpisy EHK (ECE) 128 „Jednotná ustanovení pro homologaci zdrojů světla se světlo vyzařujícími diodami (LED) pro použití v homologovaných jednotkách svítilen/světlometů motorových vozidel a jejich přípojných vozidel“. V souladu s uvažovanými předpisy a normami existují požadované svítivosti a světelné mapy, toto je však problematika určené pracovníkům optického řešení světlometů, práce na ní není zaměřena a v práci není dále rozvíjena.

Žárovková světla vozidel jsou v současné době nahrazována světly tvořenými svítivými diodami (LED). Použití LED diod jak pro přední světlomety, tak pro zadní světla automobilů se v současné době stává standardem pro vozidla vyšších cenových kategorií a postupně proniká také do segmentu střední a nižší třídy.

Kromě estetických aspektů má použití LED světel také další výhody. Jedním z důvodů jejich využívání je zlepšení parametrů spolehlivosti světel, LED diody mají řádově vyšší spolehlivost než dnes používané žárovky. Řádové zvýšení střední doby mezi poruchami (MTBF) světla na bázi LED a tedy i menší počet poruch sníží náklady na údržbu vozidla, zvýší bezpečnost silničního provozu a to vše při podstatném snížení spotřeby elektrické

energie. Použití technologie LED diod však přináší nové bezpečnostní problémy, proto je nutné při jeho návrhu použít postupy používané v oblasti funkční bezpečnosti.

6.2 Koncepční uspořádání a základní funkce LED světla

Světlomet se skládá z následujících prvků:

- Samostatný dálkový světlomet
- Integrovaný obrysový světlomet, potkávací světlomet a světlo pro denní svícení

Základní koncepce je dána technickým řešením světlometu. Světlomet je možno rozdělit na konkrétní prvky (subsystémy), jež na dané elementární úrovni reprezentují nutné funkční celky. Světlo se bazálně skládá z většího počtu vysocesvítivých LED diod, napájecích zdrojů, řídicí a diagnostické jednotky, bezpečnostního obvodu s odpojovačem. V duch uvedeného je zařízení možno dekomponovat na následující prvky (subsystémy):

- **Řídící jednotka (CPU)**
  - Samostatná jednotka CPU
  - Bloky diagnostiky a řízení
  - Zdroj CPU

- **Blok PSU – zdroje**
  - Samostatný zdroj pro Blok dálková světla
  - Samostatný zdroj pro Blok obrysová světla, potkávací světla a LED pro denní svícení

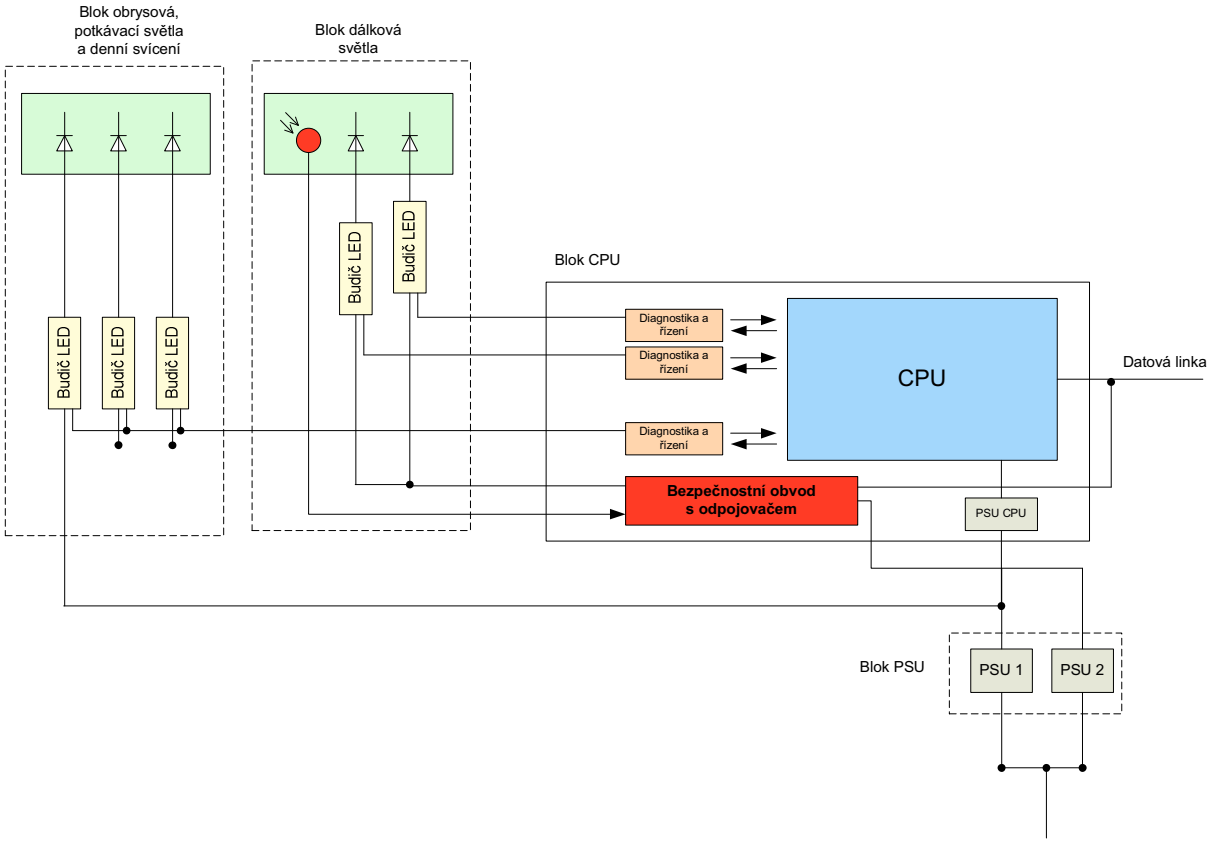
- **Blok LED pro dálkový světlomet**
  - Vlastní LED diody
  - Budiče LED

- **Blok LED pro Integrovaný obrysový světlomet, potkávací světlomet a světlo pro denní svícení**
  - Vlastní LED diody
  - Budiče LED

- **Obvod bezpečnostního odpojovače**

- **Datová linka – ovládaní světla a kontrolky**

Tyto prvky mají mezi sebou logické a funkční vazby takové, aby zařízení plnilo všechny požadované funkce správně a bezpečně tak, aby splňovalo požadavky funkční bezpečnosti. Blokové schéma, jež respektuje výše uvedené vazby je uvedeno na obr. 6.1.



Zdroj: Autor

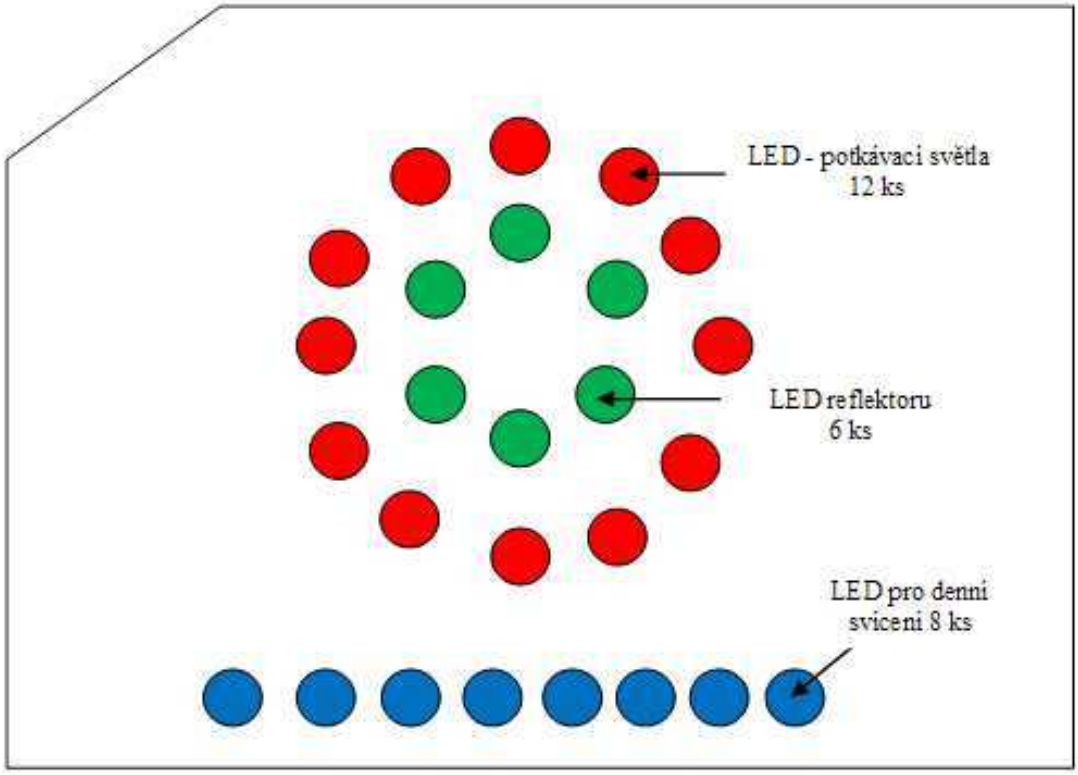
Obr. 6.1 Blokové schéma LED světlometu

Blok CPU, zajišťuje ovládání světla, diagnostiku a komunikaci s nadřazeným systémem řízení. Svými výstupy ovládá budiče LED diod, tyto řídí velikost proudu protékající LED diodou a tím její svítivost a dále zajišťují diagnostiku LED diod. Koncepční uspořádání LED diod ve světlometu je patrné z obr. 6.2.

Počet LED pro denní svícení a potkávací světla je vyšší, než by vyžadovalo základní dimenzování z hlediska svítivosti. Tento konstrukční záměr příznivě ovlivní bezporuchovost, protože uvažovanými LED diodami bude protékat menší proud, než je proud jmenovitý a sníží se tak ve výsledku jejich tepelné zatížení.

Při poruše jedné nebo více LED diod je stav registrován řídící jednotkou prostřednictvím diagnostiky, jež je vestavěna v budiči LED. Řídící jednotka na základě této informace zvýší

svítivost zbylých LED diod, které jsou v bezporuchovém stavu a nahradí tak úbytek svítivosti LED světlometu. Z hlediska spolehlivosti se v tomto případě jedná o systém s majoritním zálohováním typu n dobrých z m. Je samozřejmě zjevné, že optická část světlometu musí být navržena tak, aby porucha LED diody co nejméně změnila světelnou mapu světlometu.



Zdroj: Autor

Obr. 6.2 Koncepční uspořádání LED diod

Napájecí zdroje jsou koncipovány jako DC/DC měniče. V případě proražení zdroje PSU2, nebo při chybné funkci dalších obvodů, nastává bezpečnostní problém a světlomet je doplněn bezpečnostním obvodem s odpojovačem. Bezpečnostní obvod prostřednictvím čidla kontroluje stav (svítí/nesvítí) LED diod dálkového světla, a to nezávisle na činnosti CPU a diagnostiky vestavěné v LED budičích.

Jak bude ukázáno dále, nevyžádané rozsvícení LED diod dálkových světel představuje značné bezpečnostní riziko, které je nutné snížit. Z tohoto důvodu bezpečnostní obvod obsahuje odpojovač, který při nevyžádaném rozsvícení dálkového světla přeruší napájení budičů LED a tímto vynutí zavedení bezpečného stavu.

6.3 Záznam o nebezpečí ASAM

Identifikace a hodnocení nebezpečí je prvním a nejdůležitějším krokem spojeným s hodnocením rizik dopravního prostředku, jeho subsystému nebo jeho komponentu.

Pro provedení identifikace a hodnocení nebezpečí byl navržen integrovaný postup ASAM (Automotive Safety Assesment Method), jež umožňuje přehledné a částečně automatizované činnosti. O hodnocení pomocí metody ASAM pojednává kapitola 3.2. Jedná se o přístup kvalitativní, což možná na první pohled nezapadá do experimentální části s využitím kvantitativních metod funkční bezpečnosti, ale tento krok je nezbytný pro identifikaci nebezpečí a přiřazení úrovní integrity bezpečnosti ASIL těmto nebezpečím. Na základě konkrétní úrovně integrity bezpečnosti ASIL pro jednotlivá identifikovaná nebezpečí jsou pak přijata konkrétní opatření pro snížení úrovně rizika dle přístupu ALARP (viz kap. 3.1).

Každé identifikované nebezpečí je samostatně hodnoceno s využitím postupů ASAM (viz kap. 3.2) a výsledkem je konkrétní hodnota Klasifikačního indikátoru, který určuje požadovanou úroveň integrity bezpečnosti ASIL. Konkrétní úrovně integrity bezpečnosti ASIL pro jednotlivá identifikovaná nebezpečí s využitím formuláře „Záznam o nebezpečí“ jsou uvedeny v tab. 6.1.

Výsledkem analýzy nebezpečí je identifikace třech poruchových stavů světla, kdy u dvou poruchových stavů musí návrh světla respektovat požadavek ASIL A, jeden poruchový stav ASIL B. Ostatní poruchové stavy jsou pro řidiče samozřejmě nepříjemné, ale z hlediska bezpečnostní analýzy nepředstavují riziko, které je nutné snížit. Další analýzy budou proto zaměřeny na poruchové stavy vedoucí k vzniku nebezpečí, v tabulce jsou označeny jako H1, H3 a H8. K diskuzi nebezpečí H9, tedy požár světla. Je známo, že požár vozidla v dlouhém tunelu byl příčinou katastrof značného rozsahu s velkým počtem usmrcených osob. Z hlediska návrhu se však jedná o problém použití vhodných materiálů (plastů), odolných proti působení vysokých teplot a potlačující vývin nebezpečných plynů při hoření. Proto nebude nebezpečí H9 dále posuzováno, protože práce je primárně orientovaná na hodnocení náhodných poruch hardware.

Tab. 6.1 Záznam o nebezpečí pro LED světlomet

INSTITUT DOPRAVY VŠB-TU OSTRAVA ©MR	INSTITUT DOPRAVY, Fakulta strojní, VŠB TU - Ostrava Hodnocení nebezpečí	Dokument č.	
		Změna č.	
Výrobek:	**LED světlo automobilu**	**Požadavek č.**	
Číslo výkresu:		**Název projektu :**	
Předkladatel:	**Ing. et Ing. Michal Richtář**	**Datum:**	
Zaznamenal:	**Ing. et Ing. Michal Richtář**	**Datum:**	
Pracovník odpovědný za navržená opatření:		**Datum:**	
Schválil:		**Datum:**	

No.	Nebezpečí	Popis nebezpečí - následky nebezpečí	Příčiny nebezpečí, uzly, zařízení	Hodnocení nebezpečí podle ASAM						
				Škody počet (SA)	Škody zranění (SV)	Pravděp odobnost výskytu (W)	Doba vystavení (E)	Zamezení (V)	Klasifikační indikátor (I)	ASIL
H1	Světlo pro denní svícení nesvítí, nebo svítí málo.	Zhoršerná identifikace vozidla, svítí druhé světlo. Možnost vzniku nehody, smrt více osob. Řidič může použít potkávací světlo.	1) Porucha CPU, 2) porucha budičů	5,00	9,00	1,00	1,30	1,70	34	A
H2	Světlo pro denní svícení svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H3	Potkávací světlo nesvítí, nebo svítí málo.	Zhoršená identifikace překážek, zhorčená identifikace vozidla, svítí druhé světlo. Možnost vzniku nehody, nebo sražení chodců, cyklisty. Řidič nemůže světlo opravit.	1) Porucha CPU, 2) porucha budičů	5,00	9,00	1,00	1,30	1,70	34	A
H4	Potkávací světlo svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H5	Obrysové světlo nesvítí, nebo svítí málo.	Zhoršerná identifikace vozidla, svítí druhé světlo, nebo řidič může použít denní světlo. Bez následků, dále nehodnoceno.								0
H6	Obrysové světlo svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H7	Dálkové světlo sesvítí nebo svítí málo.	Zhoršená identifikace překážek, ridič použije potkávací světla. Bez následků, dále nehodnoceno.								0
H8	Dálkové světlo svítí nevyžádaně.	Řidič vozidla nemůže reflektor vypnout. oslnění řidičů protijedoucích vozidel, Zranění nebo smrt více osob v důsledku nehody.	1) Porucha CPU, 2) porucha zdroje PSU 2, 3) porucha bezpečnostního obvodu.	5,00	9,00	1,00	1,30	1,00	59	B
H9	Vznícení (požár) světla	1 a více osob - lehké zranění, cestující má možnost se vzdálit od ohniska požáru a zachránit se.	1) zkrat nebo jiné poškození el. Instalace, 2) vysoká venkovní teplota.	5,00	2,00	1,00	1,30	1,70	8	0

6.4 Analýza stromů poruch FTA

Analýza stromů poruch je kvalitativní a současně i kvantitativní metodou, doporučenou jak mateřskou normou ČSN EN 61508 tak i automobilní ISO 26262 pro činnosti ve fázi posuzování funkční bezpečnosti.

V kap. 3.5 je podrobně popsán postup a zásady používané při FTA analýze. Popsaný postup bude použit pro kvalitativní i kvantitativní analýzu světla, kdy top jev je poruchový stav vedoucí na nebezpečí hodnocené v tab. 6.1.

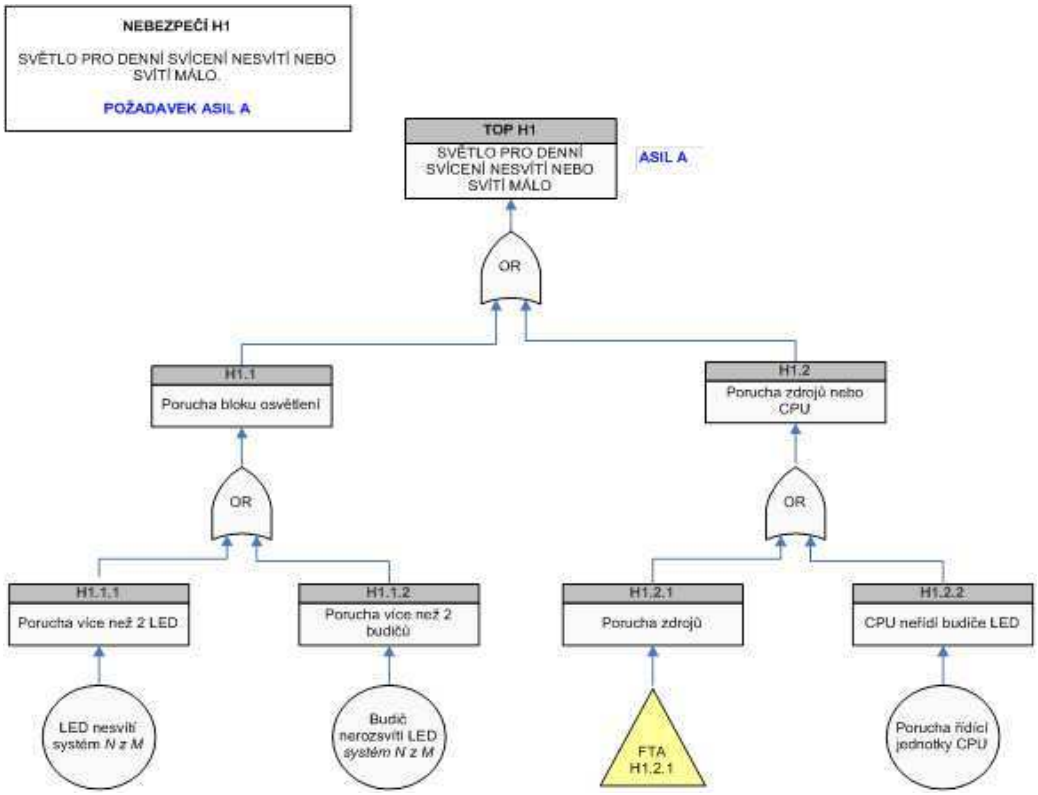
Teoreticky je samozřejmě možné rozšířit FTA analýzu i na další poruchové stavy, uvedené v záznamu o nebezpečí. Takto by bylo vhodné postupovat při predikci spolehlivosti celého světla, ale z hlediska použití principů funkční bezpečnosti je nutné analýzu provést pouze pro stavy, kde je požadavek vyšší než ASIL 0.

V tomto případě to znamená analyzovat tři poruchové stavy, vedoucí na nebezpečí H1, H3, H8.

6.4.1 Kvalitativní analýza světla

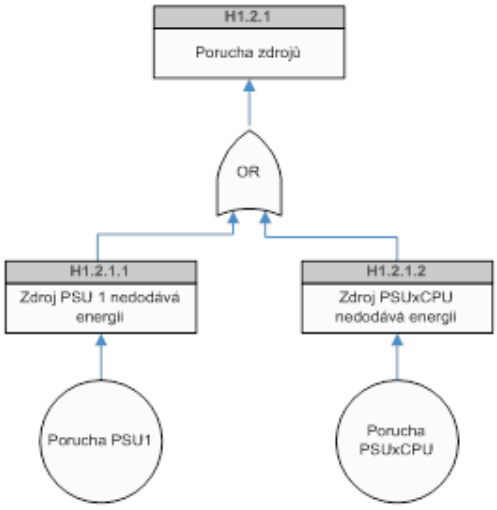
Pro všechny stromy poruchových stavů FTA byly vypracovány příslušné formuláře, které respektují základní definovaná pravidla označování (viz kap. 3.5) a které jsou součástí vyžadované dokumentace pro funkční bezpečnost.

Strom poruch FTA na obr. 6.3 představuje poruchový stav, kdy světlo pro denní svícení nesvítí vůbec nebo málo, tedy nebezpečí H1.



Zdroj: autor

Obr. 6.3 FTA analýza pro nebezpečí H1

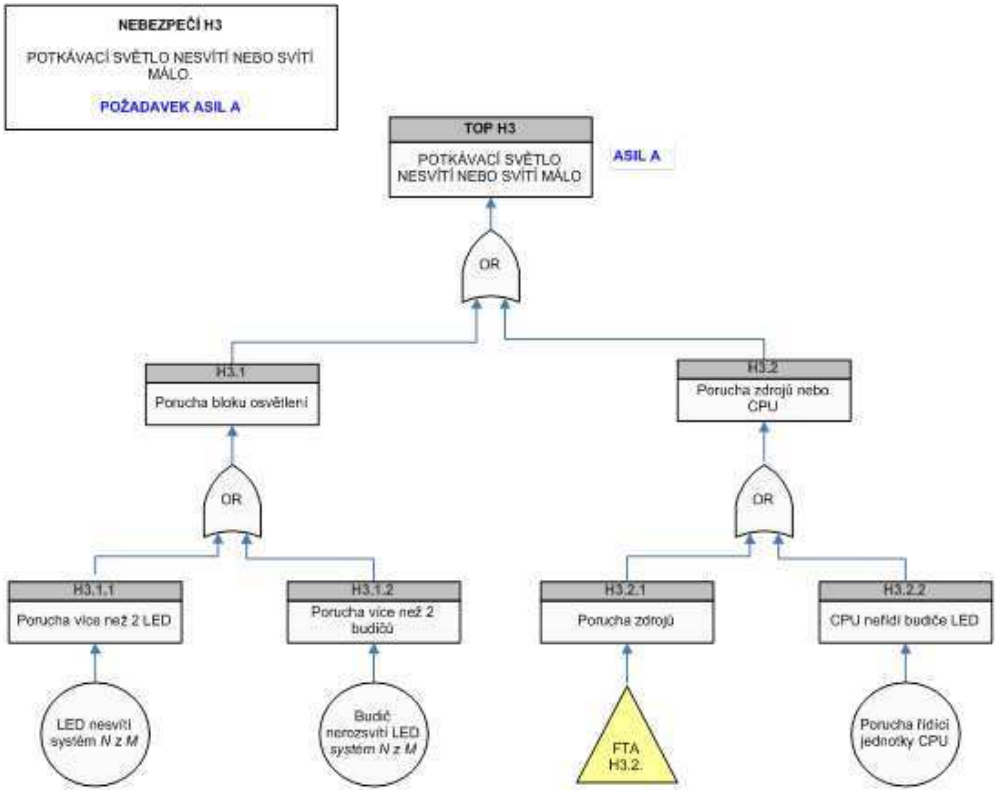


Zdroj: autor

Obr. 6.4 FTA analýza pro nebezpečí H1, část H1.2.1

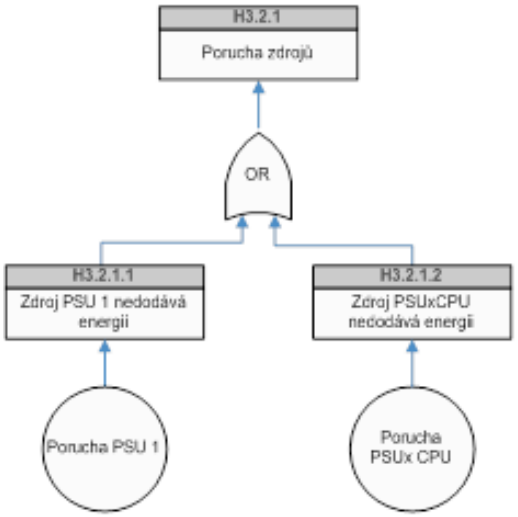
Z hlediska spolehlivosti představuje vzájemné propojení tvořících bloků soustavu se sériovým uspořádáním. Avšak skupina LED diod a jejich budičů (část H1.1.1 a H1.1.2) je soustava s majoritním zálohováním, zde konkrétně 6 dobrých z 8.

Strom poruch na obr. 6.5 představuje poruchový stav, kdy potkávací světlo nesvítí vůbec nebo málo, tedy nebezpečí H3.



Zdroj: autor

Obr. 6.5 FTA analýza pro nebezpečí H3

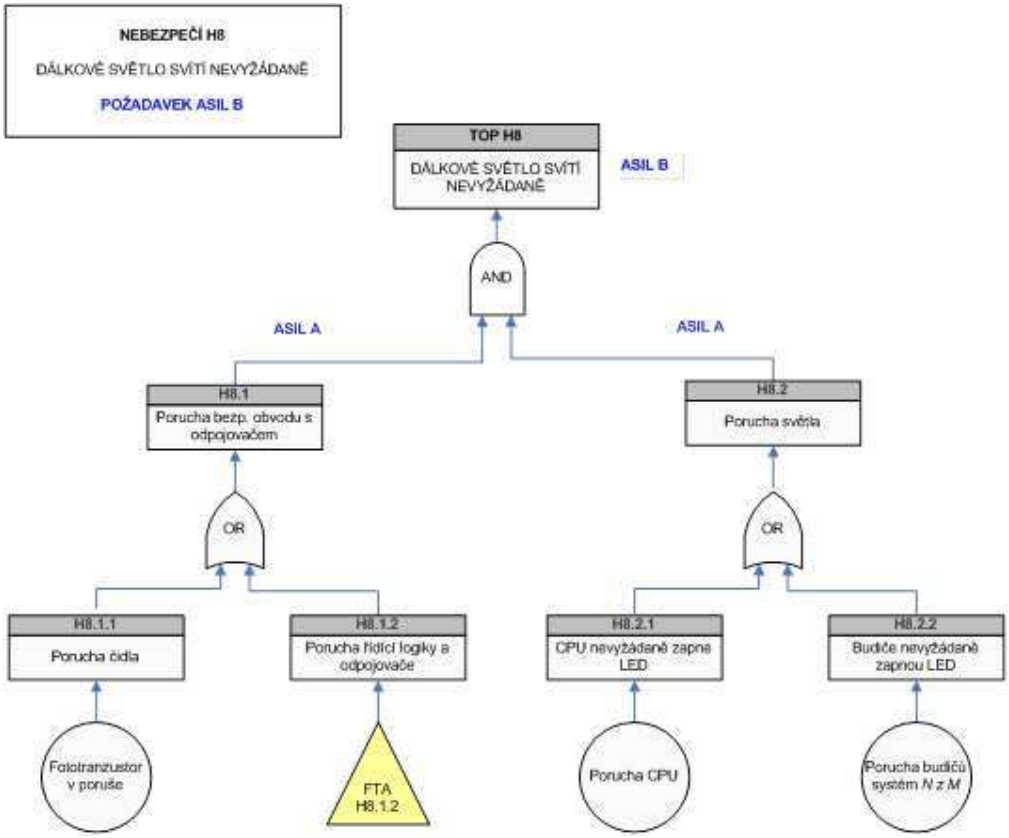


Zdroj: autor

Obr. 6.6 FTA analýza pro nebezpečí H3, část H3.2.1

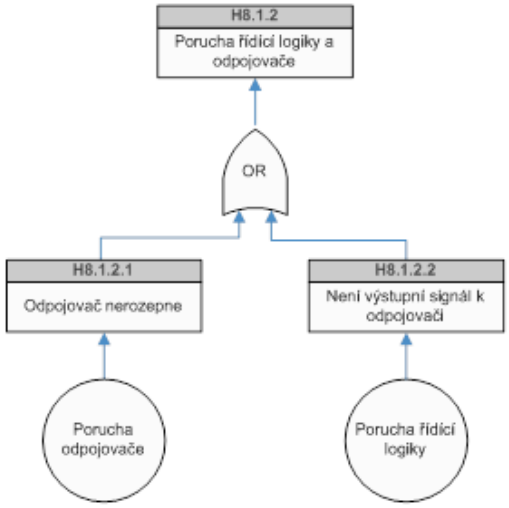
Z hlediska spolehlivosti představuje vzájemné propojení tvořících bloků soustavu se sériovým uspořádáním. Avšak skupina LED diod a jejich budičů (část H3.1.1 a H3.1.2) je soustava s majoritním zálohováním, zde konkrétně 10 dobrých z 12.

Strom poruch na obr. 6.7 představuje poruchový stav, kdy dálkové světlo nevyžádaně svítí, tedy nebezpečí H8.



Zdroj: autor

Obr. 6.7 FTA analýza pro nebezpečí H8 (autor)



Zdroj: autor

Obr. 6.8 FTA analýza pro nebezpečí H8, část H8.1.2

Z hlediska spolehlivosti představuje vzájemné propojení tvořících bloků kombinovanou soustavu. Větve H8.1 a H8.2 jsou řazeny paralelně, představují zálohovaný systém, vnitřní uspořádání obou větví je sériové. Avšak skupina LED budičů (část H8.2.2) je soustava s majoritním zálohováním, zde konkrétně 5 dobrých z 6.

6.4.2 Kvantitativní analýza světla

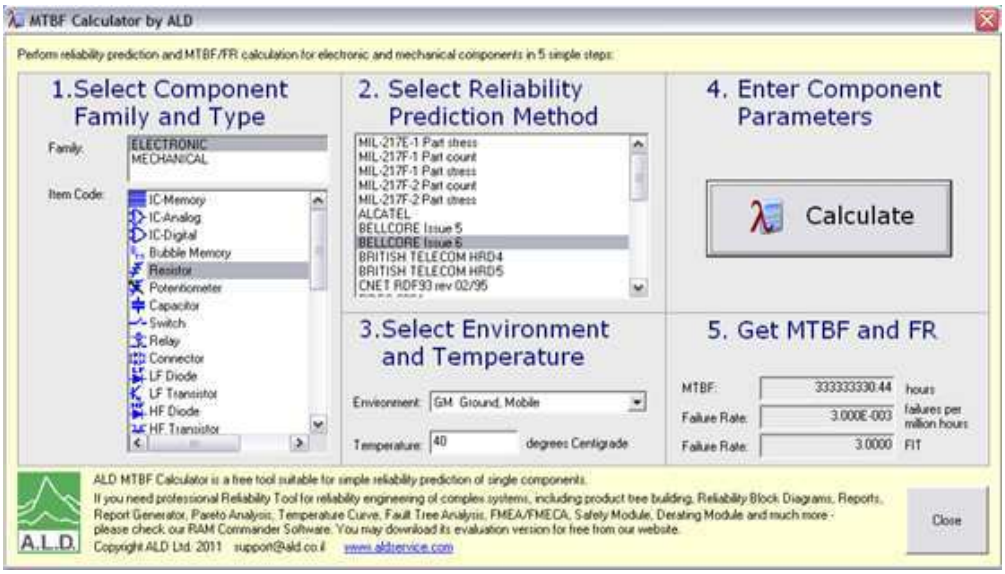
Cílem této části práce je ověřit parametry LED světla z hlediska požadavků funkční bezpečnosti. Je tedy nutné, již ve stádiu návrhu, provést výpočet spolehlivostních charakteristik a diagnostického pokrytí LED světla a tyto porovnat s požadavky normy ISO 26262. Výpočet vychází ze struktur popsaných pomocí stromů poruch FTA v předcházející kap. 6.5. Všechny výpočty jsou založeny na obecně známém předpokladu, že elektronické součástky mají exponenciální rozdělení doby do poruchy. Toto je popsáno distribuční funkcí ve vztahu (6.1):

$$F(t) = 1 - e^{-\lambda \cdot t} \tag{6.1}$$

kde:
F(t) - distribuční funkce pravděpodobnosti poruchy, [-]
t - doba provozu, [h]
λ - intenzita poruch [h^{-1}]

Intenzitu poruch tvořících součástek je možné zjistit třemi způsoby, s využitím údajů od výrobce, výpočtem vycházejícím z různých norem nebo zkouškami spolehlivosti.

Údaje od výrobce jsou vždy preferovány, problémem je situace, kdy výrobce tyto informace neuvádí.



Zdroj: autor, A.D.L

Obr. 6.9 Výstupní formulář MTBF Calculator

Potom je nutné použít nástroj, obvykle software, pro predikce intenzit poruch. V této práci byla autorem použita bezplatná verze programu MTBF Calculator od společnosti A.D.L.

V programu byl výpočet nastaven dle standardu Bellcore Issue 6, a ukázka výstupního formuláře je na obr. 6.9.

Výpočet pro nebezpečí H1

Nebezpečí H1 představuje poruchový stav, kdy světlo pro denní svícení nesvítí vůbec nebo málo, strom poruch je na obr. 6.3. Cílem výpočtu je stanovit cílovou míru poruch, tj. intenzitu poruch systému. Výpočet bude proveden tak, že ze známých intenzit poruch tvořících bloků budou stanoveny pravděpodobnosti jejich poruch a následně pravděpodobnost TOP jevu. Výslednou intenzitu poruch TOP jevu stanovíme s využitím vztahu (6.1), kdy po úpravách získáme výsledný vztah (6.2):

$$\lambda = \frac{-\ln(1-F(t))}{t} \tag{6.2}$$

kde:
F(t) - distribuční funkce pravděpodobnosti poruchy, [-]
t - doba provozu, [h]
λ - intenzita poruch [h^{-1}]

Intenzita poruch každého tvořícího bloku je vypočítána s využitím obvodového schématu a z typů jednotlivých součástí. Výrobce LED světlometu schéma ani typy součástek neuvolnil k zveřejnění, budou proto použity hodnoty za celý blok. Jako ukázka postupu výpočtu jednoho bloku bude použit blok LED diod.

Příklad výpočtu bloku LED diod

Blok LED diod pro denní svícení tvoří 8 LED diod, soustava je v bezporuchovém stavu při poruše maximálně 2 ks LED diod. Výpočet bude proveden s využitím binomického rozdělení dle vztahu (4.10), kdy pravděpodobnost vzniku elementárního jevu je dána exponenciálním rozdělením. Výsledky výpočtu pro blok LED diod je uveden v tab. 6.2.

Tab. 6.2 Výpočet bloku LED diod – denní svícení

Vstupní parametry		**Výpočet**	
Počet LED	12	Bezporuchovost $R_s(t)$	$9{,}99 \cdot 10^{-1}$
Doba provozu LED (h)	8000	Pravděpodobnost poruchy F(t)	$9{,}24 \cdot 10^{-4}$
Intenzita poruch 1 ks LED (h^{-1})	$3{,}33 \cdot 10^{-6}$	**Intenzita poruch soustavy λ (h^{-1})**	**$1{,}16 \cdot 10^{-7}$**
Architektura *m* z *n*	6 z 8		

Postup výpočtu stromu poruch vychází z pravdivostních tabulek přiřazených ke každému hradlu. Výpočet probíhá směrem zdola nahoru, vstupní hodnota základní události je pravděpodobnost poruchy každého bloku. Výsledky výpočtu jsou uvedeny v tab. 6.3.

Tab. 6.3 Výpočet FTA pro nebezpečí H1

Vstupní hodnoty		**Výpočet**	
Blok	**F(t)**	**Hradlo**	**F(t)**
LED diody	$9{,}24 \cdot 10^{-4}$	H1.2.1	$5{,}43 \cdot 10^{-4}$
Budiče	$2{,}38 \cdot 10^{-5}$	H1.2	$9{,}27 \cdot 10^{-4}$
CPU	$3{,}84 \cdot 10^{-4}$	H1.1	$9{,}48 \cdot 10^{-4}$
PSU1	$3{,}60 \cdot 10^{-4}$	TOP	$1{,}87 \cdot 10^{-3}$
PSUxCPU	$1{,}84 \cdot 10^{-4}$	**λ (h^{-1})**	**$2{,}34 \cdot 10^{-7}$**

Dílčí závěr:

Obvodové řešení pro nebezpečí H1 cílovou míru poruch splňuje na úrovni ASIL A.

Výpočet pro nebezpečí H3

Nebezpečí H1 představuje poruchový stav, kdy potkávací světlo nesvítí vůbec nebo málo, strom poruch je na obr. 6.4. Cílem výpočtu je stanovit cílovou míru poruch, tj. intenzitu poruch systému. Výpočet provedeme obdobně jako u nebezpečí H1, pravděpodobnosti poruch tvořících bloků budou stejné v tab. 6.3, výjimkou je blok LED diod a blok budičů. U obou bloků je použita architektura 10 z 12 a doba provozu bude kratší. Výpočet bloku LED diod je uveden v tab. 6.4, výpočet hodnot FTA je v tab. 6.5.

Tab. 6.4 Výpočet bloku LED diod – potkávací světlo

Vstupní parametry		**Výpočet**	
Počet LED	12	Bezporuchovost $R_s(t)$	$9{,}99 \cdot 10^{-1}$
Doba provozu LED (h)	4000	Pravděpodobnost poruchy F(t)	$4{,}67 \cdot 10^{-4}$
Intenzita poruch LED (h^{-1})	$3{,}33 \cdot 10^{-6}$	**Intenzita poruch λ (h^{-1})**	**$1{,}17 \cdot 10^{-7}$**
Architektura *m* z *n*	10 z 12		

Tab. 6.5 Výpočet FTA pro nebezpečí H3

Vstupní hodnoty		**Výpočet**	
Blok	**F(t)**	**Hradlo**	**F(t)**
LED diody	$4{,}67 \cdot 10^{-4}$	H3.2.1	$5{,}43 \cdot 10^{-4}$
Budiče	$1{,}43 \cdot 10^{-5}$	H3.2	$9{,}27 \cdot 10^{-4}$
CPU	$3{,}84 \cdot 10^{-4}$	H3.1	$4{,}82 \cdot 10^{-4}$
PSU1	$3{,}60 \cdot 10^{-4}$	TOP	$1{,}41 \cdot 10^{-3}$
PSUxCPU	$1{,}84 \cdot 10^{-4}$	**λ (h^{-1})**	**$1{,}76 \cdot 10^{-7}$**

Dílčí závěr:

Obvodové řešení pro nebezpečí H3 cílovou míru poruch splňuje na úrovni ASIL A.

Výpočet pro nebezpečí H8

Nebezpečí H8 představuje poruchový stav, kdy dálkové světlo nevyžádaně svítí, strom poruch je na obr. 6.5. Cílem výpočtu je stanovit cílovou míru poruch, tj. intenzitu poruch systému. Výpočet provedeme obdobně jako u nebezpečí H3, je však nutné respektovat jinou architekturu systému. Budiče tvoří soustavu s majoritním zálohováním, nebezpečí nastane při průrazu dvou budičů ze šesti. Bezpečnostní obvod je paralelně řazen vedle řídícího obvodu. Výpočet bloku budičů v tab. 6.6 a výpočet hodnot FTA je v tab. 6.7.

Tab. 6.6 Výpočet bloku budičů – dálkové světlo

Vstupní parametry		**Výpočet**	
Počet budičů	6	Bezporuchovost $R_s(t)$	$9{,}99 \cdot 10^{-1}$
Doba provozu budiče (h)	1000	Pravděpodobnost poruchy F(t)	$1{,}92 \cdot 10^{-5}$
Intenzita poruch budiče (h^{-1})	$3{,}33 \cdot 10^{-6}$	**Intenzita poruch λ (h^{-1})**	**$1{,}93 \cdot 10^{-8}$**
Architektura *m* z *n*	4 ze 6		

Tab. 6.7 Výpočet FTA pro nebezpečí H8

Vstupní hodnoty		**Výpočet**	
Blok	**F(t)**	**Hradlo**	**F(t)**
Fototranzistor	$4{,}67 \cdot 10^{-4}$	H8.1.2	$3{,}05 \cdot 10^{-4}$
Budiče	$1{,}43 \cdot 10^{-5}$	H8.1	$3{,}79 \cdot 10^{-4}$
CPU	$3{,}84 \cdot 10^{-4}$	H8.2	$4{,}03 \cdot 10^{-4}$
Odpojovač	$3{,}60 \cdot 10^{-4}$	TOP	$1{,}53 \cdot 10^{-7}$
Řídící logika	$1{,}84 \cdot 10^{-4}$	**λ□ (h^{-1})**	**$1{,}53 \cdot 10^{-7}$**

Dílčí závěr:

Obvodové řešení pro nebezpečí H8 cílovou míru poruch splňuje na úrovni ASIL B.

6.4.3 Posouzení diagnostické pokrytí a odolnosti

Posouzení diagnostického pokrytí principiálně využívá fenomenologické schéma diagnostického sytému [8]. Hodnocení kvality obvodového návrhu LED světla se provádí pomocí tří parametrů. Parametr odolnosti SPM popsaný vztahem (4.15) ukazuje, jaké procento poruch povede na vznik nebezpečného stavu, protože poruchy nejsou pokryty diagnostickým systémem, nebo diagnostický systém poruchy nerozpozná, přesto že by měl.

Další parametr odolnosti LFM popsaný vztahem (4.16) ukazuje, jaké procento skrytých (tj. vícenásobných) poruch povede na nebezpečný stav. Příkladem může být porucha zdroje, kdy na výstupu zdroje vznikne přepětí. Toto následně způsobí poruchu diagnostického systému, který nedokáže lokalizovat poruchu a vznikne nebezpečný stav.

Třetí parametr DC_{RF} popsaný vztahem (4.13) hodnotí kvalitu obvodového návrhu diagnostického systému. V jistém smyslu chápání (rozšířeném) parametr hodnotí „účinnost“ diagnostického systému.

Posouzení SPM odolnosti

Posouzení SPM odolnosti se provádí na základě obvodové analýzy každého bloku. Zkoumáme, zda porucha nějaké součásti vede na vznik nebezpečného stavu, zda je detekovatelná diagnostickým systémem a s jakou účinností. Protože obvodové schéma výrobce neuvolnil k zveřejnění, bude uvedený postup ukázán na demonstrativním příkladu (tab. 6.8). Výpočet SPM provedeme dle vztahu (4.15).

Tab. 6.8 Příklad analýzy SPM odolnosti

Součástka	λ součástky (h^{-1})	Typ poruchy	Rozdělení poruchy (%)	Způsobí porucha nebezpečí	Pokrytí diagnostikou (%)	λ_{RF} (h^{-1})	λ_{SPF} (h^{-1})	Poznámka
Odpor	6,00E-08	Přerušení	45	x	100	0,00E+00	0,00E+00	
		Zkrat	45	x	100	0,00E+00	0,00E+00	
		Změna hodnoty	10	x	0	0,00E+00	6,00E-09	
Dioda	4,00E-08	Přerušení	50					Nezpůsobí nebezpečí
		Zkrat	50	x	100	0,00E+00	0,00E+00	
LED dioda	3,33E-06	Přerušení	50	x	90	1,67E-07	0,00E+00	
		Zkrat	49	x	90	1,63E-07	0,00E+00	
		Ztráta funkce	1	x	0	0,00E+00	3,33E-08	Proud teče, ale LED nesvítí
Budič LED	3,30E-06	Zkrat (proražení)	50	x	100	0,00E+00	0,00E+00	Nevyžádané rozsvícení dálkového světla
		Přerušení	45					
		Ztráta funkce	5	x	0	0,00E+00	1,65E-07	Nefunkční diagnostický výstup z budiče
Suma	**6,73E-06**					**3,30E-07**	**2,04E-07**	
SPM (%)	**92,07**							
DC_{rf}	**95,10**							

Legenda k tab. 6.8:

- 2. sloupec obsahuje intenzitu poruch součástky
- 3. sloupec obsahuje možné poruchové stavy součástky
- 4. sloupec obsahuje procentuální rozdělení poruchových stavů
- 5. sloupec obsahuje informaci, zda porucha součásti může způsobit nebezpečí
- 6. sloupec obsahuje procentuální pokrytí poruchy diagnostikou
- 7. sloupec obsahuje zbytkovou intenzitu poruch součásti, kterou nedokáže pokrýt diagnostický systém
- 8. sloupec obsahuje intenzitu poruch součásti, která není vůbec pokryta diagnostickým systém

Dílčí závěr:

Dosažená hodnota SPM = 92,7 % vyhovuje na úrovni ASIL B.

Posouzení DC_{RF}

Posouzení kvality návrhu diagnostiky je možné provést přímo s využitím výsledků v tab. 6.8. Výpočet provedeme s využitím vztahu (4.13):

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \cdot 100 = \left(1 - \frac{3{,}30E^{-7}}{6{,}73E^{-6}}\right) \cdot 100 = 95{,}1\ (\%)$$

Dílčí závěr:

Dosažená hodnota DC_{RF} = 95,1 % vyhovuje na úrovni ASIL B.

Posouzení LFM odolnosti

Posouzení LFM odolnosti se provádí na základě obvodové analýzy každého bloku. Zkoumáme, zda porucha nějaké součásti při souběhu s poruchou jiné součásti vede ke vzniku nebezpečného stavu, zda je detekovatelná diagnostickým systémem a s jakou účinností. Protože obvodové schéma výrobce neuvolnil ke zveřejnění, bude uvedený postup ukázán na demonstrativním příkladu (tab. 6.9). Výpočet LFM provedeme dle vztahu (4.16). Výpočet LFM provedeme dosazením do vztahu (4.16).

$$LFM = 1 - \frac{\sum \lambda_{MPFL}}{\sum \left(\lambda - \lambda_{SPF} - \lambda_{RF}\right)} \cdot 100 = \frac{2{,}03 \cdot 10^{-6}}{6{,}73 \cdot 10^{-6} - 3{,}3 \cdot 10^{-7} - 2{,}04 \cdot 10^{-7}} \cdot 100 \qquad (4.16)$$

Dílčí závěr:

Dosažená hodnota odolnosti LFM = 67,25 % vyhovuje na úrovni ASIL B.

6.5 Návrh zrychlené zkoušky LED světla

Cílem této části práce je navrhnout zrychlenou zkoušku LED světla a ověřit, zda je splněna hodnota cílové míry poruch a zda světlo odpovídá požadavkům na bezporuchovost z hlediska profilu životního cyklu. Zrychlená zkouška vychází ze zkušebních plánů, pro stanovení faktoru zrychlení bude použit Arrheniova modelu popsaného v kap. 4.

Tab. 6.9 Příklad analýzy LFM odolnosti

Součástka	**λ součástky (h^{-1})**	**Typ poruchy**	**Rozdělení poruchy (%)**	**Způsobí skrytá (vícenásobná) porucha nebezpečí**	**Pokrytí diagnostikou (%)**	**λ_{MPFL} (h^{-1})**	**Poznámka**
Odpor	6,00E-08	Přerušení	45	x	0	2,70E-08	Vznikne přepětí na zdroji
		Zkrat	45				Nezpůsobí nebezpečí
		Změna hodnoty	10	x	0	6,00E-09	Vznikne přepětí na zdroji
Dioda	4,00E-08	Přerušení	50				Nezpůsobí nebezpečí
		Zkrat	50	x	100	0,00E+00	
LED dioda	3,33E-06	Přerušení	50	x	90	1,67E-07	
		Zkrat	49	x	0	1,63E-06	
		Ztráta funkce	1	x	0	3,33E-08	Proud teče, ale LED nesvítí
Budič LED	3,30E-06	Zkrat (proražení)	50	x	100	0,00E+00	Nevyžádané rozsvícení dálkového světla, pokryté bezpečnostním obvodem
		Přerušení	45				
		Ztráta funkce	5	x	0	1,65E-07	Nefunkční diagnostický výstup z budiče
Suma	**6,73E-06**					**2,03E-06**	
LFM (%)	**67,25**						

Legenda k Tab. 6.9:

- 2. sloupec obsahuje intenzitu poruch součástky
- 3. sloupec obsahuje možné poruchové stavy součástky
- 4. sloupec obsahuje procentuální rozdělení poruchových stavů
- 5. sloupec obsahuje informaci, zda porucha součásti v kombinaci s poruchou jiné součásti může způsobit nebezpečí
- 6. sloupec obsahuje procentuální pokrytí poruchy diagnostikou
- 7. sloupec obsahuje intenzitu vícenásobné (skryté) poruchy součásti, kterou nedokáže pokrýt diagnostický systém

6.5.1 Výchozí podmínky pro návrh

Vzhledem k očekávanému profilu životního cyklu vozidla je výpočtová doba životnosti LED světla stanovena na 8 let (cca 70 000 hodin) a celková doba svícení 8000 hodin. Protože však zkouška musí modelovat stav, kdy světlo svítí a kdy je bez napětí (vozidlo není v provozu), bude zkouška rozdělena na dva úseky. V prvním úseku bude světlo zkoušeno pod napětím, v druhém bez napětí. Takto simulovaný životní cyklus však znamená, že v každém úseku bude dosaženo jiného faktoru zrychlení. Je to dáno tím, že faktor zrychlení je závislý na teplotě a bude se proto měnit s rozdílem zkušební a provozní teploty. Situaci ukazuje tab. 6.10.

Tab. 6.10 Provozní a zkušební teploty

Režim práce	**Zkušební teplota (°C)**	**Teplota v provozu (°C)**	**Rozdíl (°C)**
pod napětím	90	50	40
bez napětí	90	20	70

Stanovení akumulovaného času zkoušky (t_{AKU})

Stanovení akumulovaného času zkoušky t_{AKU} provedeme úpravou vztahu (4.18). Cílová míra poruch je dána požadavkem normy, tím je i stanoven požadavek na T_D. Zkoušku vyhodnotíme na konfidenční úrovni C = 0,7, což je minimální hodnota stanovena normou, dále předpokládáme, že při zkoušce nevznikne žádná porucha. Výsledná hodnota t_{AKU} tak odpovídá nejmenší možné hodnotě t_{AKU} nutné k prokázání požadované cílové míry poruch T_D.

S využitím vztahu (4.18):

$$T_D \geq \frac{2 \cdot t_{AKU}}{\chi^2_{2\nu;C}} \tag{4.18}$$

kde:
T_D - dolní mez konfidenčního intervalu [h],
t_{AKU} - akumulovaná pracovní doba výrobků ve zkoušce [h],
χ^2 - hodnota chí-kvadrát rozdělení [-].

Dostáváme následují hodnotu t_{AKU} ve vztahu (6.3)

$$t_{AKU} \geq \frac{T_D \cdot \chi^2_{2\nu;C}}{2} = \frac{1 \cdot 10^6 \cdot 2{,}40}{2} = 1{,}2 \cdot 10^6 [h] \tag{6.3}$$

Dílčí závěr:

K prokázání cílové míry poruch je požadovaná hodnota akumulovaného času zkoušky t_{AKU} stanovena na 1,2 . 10^6 hodin.

Stanovení faktoru zrychlení

Faktor zrychlení, udávající poměr hodnot ukazatele spolehlivosti při provozním zatížení a vyšším zatížení při zrychlené zkoušce, je pro Arrheniův model po úpravách určen vztahem (4.24) a vztahem (4.23).

Pří znalosti aktivační energie E_A a dále zkušební a provozní teploty je možné stanovit faktor zrychlení. Při zkoušce bloku LED diod je aktivační energie u všech zkoušených součástek shodná a lze ji zjistit u výrobce nebo v [7]. Dosazením do vztahů (4.24) a (4.23) a s použitím údajů o teplotách z tab. 6.10 získáme dvě hodnoty faktoru zrychlení odpovídající různým režimům práce světla. Výsledky jsou uvedeny v tab. 6.11.

Tab. 6.11 Faktor zrychlení při režimech světla

Vstupní parametry		**Režim práce**	**Zkušební teplota T_A**	**Teplota v provozu T_U**	**Faktor zrychlení A_F**
			(K)	**(K)**	**(-)**
E_A (eV)	0,876	pod napětím	363	323	32
K (eV·K^{-1})	8,62E-05	bez napětí	363	293	805

Návrh profilu zkoušky

Zkouška bude rozdělena na dva úseky. V prvním úseku bude blok LED diod pracovat v režimu pod napětím, tj. při teplotě součástí 90 °C (odpovídá 363 K). Tomu musí být přizpůsobena vnitřní teplota ve zkušební komoře, která musí být nižší (např. 75 °C), protože LED diodami protéká proud a dochází tak k dalšímu vývinu tepla ohřívající součástky. Po úspěšném ukončení první části zkoušky, tj. alespoň m z n LED diod u každého bloku svítí, byla prokázána cílová míra poruch. Ke stanovení doby zkoušky při zvýšené teplotě použijeme následující vztah (6.4):

$$T_l \geq \frac{t_{AKU}}{n \cdot A_{FS}} \tag{6.4}$$

kde:
T_l - doba trvání zkoušky [h],
t_{AKU} - akumulovaná doba zkoušky [h],
n - počet zkoušených výrobků [-],
A_{FS} - faktor zrychlení práce pod napětím [-],

Pokud bude zařazeno do zkoušky 10 ks bloků LED diod, dosazením do vztahu (6.4) vypočítáme následující výsledek (6.5):

$$T_l = \frac{t_{AKU}}{n \cdot A_{FS}} = \frac{1{,}2 \cdot 10^6}{10 \cdot 32} = 3450[h] \tag{6.5}$$

Dílčí závěr:

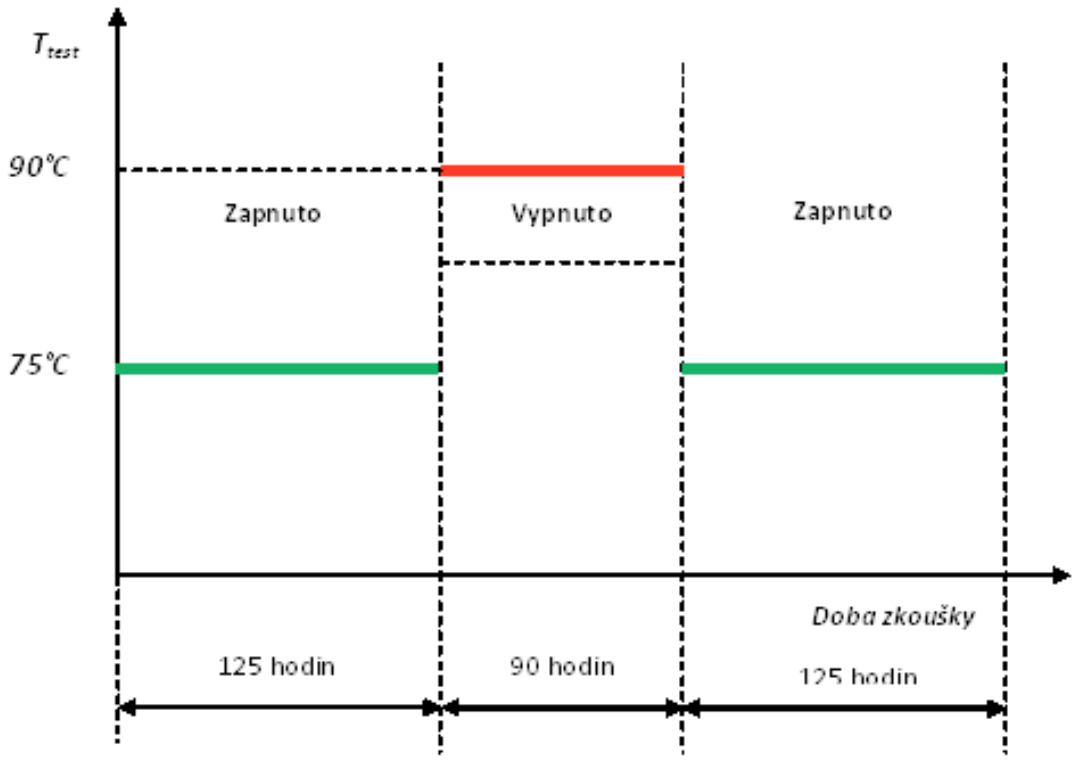
Doba trvání první část zkoušky ukončené bez poruchy musí být realizována v délce nejméně 3450 hodin.

Druhá část zkoušky má za cíl ověřit bezporuchovost světla z hlediska životního cyklu. Cílem zkoušky je prokázat, že blok LED diod odpovídá požadavkům na životnost, který výrobce definoval tak, že po uplynutí životnosti je alespoň 5 z 10 výrobků v bezporuchovém stavu. Zkouška bude simulovat stav, kdy světlo svítí (8000 hodin) a kdy je bez napětí (72000 hod). Doba zkoušky je stanovena dle vztahu (6.6) a (6.7).

$$T_{2S} = \frac{t_{sviti}}{A_{FS}} = \frac{8 \cdot 10^3}{32} = 250[h] \tag{6.6}$$

$$T_{2N} = \frac{t_{nesviti}}{A_{FN}} = \frac{7{,}2 \cdot 10^4}{805} = 90[h] \tag{6.7}$$

kde:
T_{2S} - doba trvání zkoušky, světlo pod napětím [h],
T_{sviti} - požadavek na dobu svícení (práce pod napětím) [h],
A_{FS} - faktor zrychlení, světlo pod napětím [-],
T_{2N} - doba trvání zkoušky, světlo není pod napětím [h],
$T_{nesviti}$ - požadavek na dobu, kdy světlo nesvítí [h],
A_{FN} - faktor zrychlení, světlo není pod napětím [-],



Zdroj: autor

Obr. 6.10 Schéma zkoušky LED světla

Dílčí závěr:

Doba trvání druhé části zkoušky musí být realizována nejméně v délce 340 hodin, nejméně 5 ks bloků LED z deseti musí být v bezporuchovém stavu. Schéma průběhu zkoušky je obr. 6.7.

Diskuze k obdrženým výsledkům:

Obě části zkoušky vyžadují řádově rozdílné doby trvaní. Je zjevné, že požadavky na bezporuchovost z hlediska životního cyklu jsou velmi „měkké“ oproti požadavkům na bezpečnost na úrovni ASIL. Je zde značný prostor pro optimalizaci architektury hardware, kde by byly důsledně odděleny obvody související s bezpečností od ostatních. Tím by bylo možné docílit stavu, kdy bezpečnostní obvody, nutně vyžadující kvalitní a proto i dražší součástky, budou navrženy a zkušeny dle požadavků na funkční bezpečnost a ostatní obvody realizovány z běžně dostupných a proto i levnějších součástek. Problematika optimalizace nabízí prostor pro pokračování řešeného tématu.

7 Závěr

Obsahem této disertační práce je problematika funkční bezpečnosti v oblasti silničních vozidel, zvláště pak využití vhodných metod, postupů a modelů, v návaznosti na novou situaci spojenou se zaváděním nových norem.

Práce byla zaměřena na návrh vhodných postupů a využití kvalitativní a kvantitativní analýzy spolehlivosti vybraných systémů silničních vozidel, jež významně ovlivňují bezpečnost silničního provozu. Pro ověření skutečné úrovně vybraných parametrů spolehlivosti zařízení byl navržen program zkoušek spolehlivosti.

Pro hodnocení funkční bezpečnosti byly zvoleny postupy a nástroje, jež vycházejí z principů funkční bezpečnosti elektrických/elektronických systémů souvisejících s bezpečností, popsaných v normě ČSN EN 61508 a ISO 26262.

7.1 Zhodnocení dosažených výsledků a návrhy na další postup ve výzkumu

Zhodnocení výsledků dosažených v teoretické části práce je provedeno v následujících bodech:

- V úvodu teoretické části práce jsou přehledně zpracovány a rozvinuty základní principy používané v oblasti funkční bezpečnosti. Cílem bylo zpracovat principy takovým způsobem, aby byly zřejmé vzájemné souvislosti a návaznost činností a procedur směrem k praktickému využití. Bez této části práce je praktické uplatnění postupů funkční bezpečnosti pro výrobce vozidel velmi složité.
- V teoretické části práce byl vytvořen nový postup pro klasifikaci rizik pro silniční vozidla, který zjednodušuje proces posuzování rizik a přiřazení úrovně integrity bezpečnosti. Dosaženým výsledkem práce je značné zjednodušení postupů posuzování rizik s výstupy plně srovnatelnými s doporučeními uvedenými v normě ISO 26262.
- V teoretické části práce byly dále vybrány, popsány a rozpracovány metody pro kvalitativní a kvantitativní hodnocení funkční bezpečnosti. Dosaženým výsledkem je výběr vhodných metod s ohledem na potřeby průmyslové praxe, tedy využití metod co nejjednodušších z hlediska výrobců komponent vozidel, a současně metod poskytujících dostatečně kvalitní výstupy.

Praktická část práce byla zaměřena na uplatnění postupů a metod navržených v teoretické části práce. Byly aplikovány na systém vstupních dveří autobusu a přední světlomet automobilu. Zhodnocení dosažených výsledků významných pro praxi je provedeno v následujících bodech:

- Dosaženým výsledkem je provedení kvalitativního hodnocení spolehlivosti s využitím postupu ASAM, analýzy stromů poruch (FTA) a analýzy způsobů a důsledků poruch (FMEA). Byly identifikovány jednotlivé funkce vstupních dveří autobusu a způsoby jejich selhání. Výsledkem této části práce je návrh opatření vedoucích ke snížení rizika na společensky přijatelnou úroveň. Zbytková rizika vyhovují požadavkům na úroveň integrity bezpečnosti ASIL.
- Dosaženým výsledkem kvantitativní analýzy světlometu osobního automobilu je vytvoření teoretického modelu bezporuchovosti pro náhodné poruchy hardware, na jehož základě by bylo možné výpočtem určit konkrétní číselné hodnoty ukazatelů funkční bezpečnosti. Na základě predikce intenzit poruch tvořících prvků hardware byla určena číselná hodnota ukazatele cílové míry poruch. Obvodová řešení byla analyzována a byla navržena taková opatření, která splňují požadavky na cílovou míru poruch dané úrovní ASIL. Dále bylo provedeno hodnocení kvality obvodového návrhu LED světla pomocí tří parametrů, a to parametrem odolnosti SPM, parametrem odolnosti LFM a parametr diagnostického pokrytí DC_{RF}. Dosažené hodnoty odolnosti SPM, odolnosti LFM a parametr diagnostického pokrytí DC_{RF} vyhovují požadované úrovni ASIL.
- Dalším výsledkem je návrh zrychlené zkoušky LED světla a ověření, zda je splněna hodnota cílové míry poruch a zda světlo odpovídá požadavkům na bezporuchovost z hlediska profilu životního cyklu. Dle výsledků výpočtového modelu zkoušky musí být doba trvání zkoušky pro splnění hodnoty cílové míry poruch ukončené bez poruchy realizována v délce nejméně 3450 hodin.

Stěžejní témata pro další rozvoj problematiky jsou dle názoru autora následující:

- Další využití je možné vidět v definování zásad pro metodiku konstrukce mechanických systémů, zajišťujících bezpečnostní funkce a v rozvoji způsobů jejich validace

- Vzhledem k tomu, že mnohé technické systémy se jeví jako systémy mechatronické a část bezpečnosti spočívá také na straně mechanické části systému, rozšířit a rozpracovat problematiku o hodnocení schopnosti mechanického systému splňovat požadavky integrity bezpečnosti jako celku
- další zrychlení průběhu zkoušek spolehlivosti jejich realizací při časově proměnlivém tepelném zatížení nebo při větším počtu zrychlujících zatížení (vibrace, vlhkost apod.), v této souvislosti vytvoření matematických modelů těchto zkoušek.

7.2 Přínos pro vědní obor a praxi

Těžiště přínosu práce pro vědní obor spolehlivost je uveden v následujících bodech:

- Byla zdokonalena metodika pro hodnocení rizik. Přínosem je značné zjednodušení postupu pro hodnocení rizik oproti metodice uvedené v normě ISO 26262. Obdržené výsledky s použitím navržené metodiky hodnocení rizik plně odpovídají kvalitativním požadavkům dle ISO 26262.
- Byl navržen výpočetní model zrychlené zkoušky spolehlivosti založený na principu Arrheniových vztahů pro rychlost chemické reakce. Navržený profil zkoušky umožňuje současně ověřit dosaženou intenzitu poruch z hlediska požadavků ASIL a ověřit dosaženou intenzitu poruch z hlediska očekávaného životního cyklu světlometu. Je tak možné původně dvě izolované zkoušky provést současně, což má značný přínos z hlediska úspory nákladů a času při vývoji světlometu u výrobce.
- Využití výsledků této disertační práce je možné vidět v univerzitní pedagogické praxi, a to implementací poznatků do výuky předmětů spojených s konstrukcí, spolehlivostí a bezpečností dopravních prostředků v bakalářském, magisterském a doktorském studiu. Přínos teoretické části práce představuje stěžejně problematika funkční bezpečnosti dopravních prostředků, kterou je možno dle názoru autora považovat za novou a tedy v prostředí České republiky pro studenty (a nejen je) neznámou. Experimentální část disertační práce může být využita jako didaktický příklad aplikace principů funkční bezpečnosti v oblasti silničních vozidel. S využitím vhodných příkladů mohou být představeny a aplikovány metody a postupy analýzy a hodnocení spolehlivosti a bezpečnosti vycházející z požadavků normy ISO 26262 a ČSN EN 61508.

Conclusions

The content of this doctoral thesis is the functional safety of road vehicles, in particular the use of appropriate methods, procedures and models in relation to the new situation, associated with the implementation of new standards.

The thesis was focused on the design of appropriate procedures and utilization qualitative and quantitative reliability analysis of selected systems of road vehicles that significantly affect road safety. To verify the actual level of selected reliability parameters of equipment the program of reliability tests has been designed.

For functional safety assessment procedures and tools have been selected, which are based on the principles of functional safety of electric / electronic safety-related systems, as described in the standards EN 61508 and ISO 26262.

Evaluation of the achieved results and proposals for further progress in research

Evaluation of the results achieved in the theoretical part of the thesis is performed in the following points:

- In the beginning of the theoretical part of the thesis the basic principles used in the field of functional safety have been clearly processed and developed. The aim was to design principles in such a way that makes clear the mutual relations and sequences of activities and procedures toward the practical use. The practical application of functional safety procedures for vehicle manufacturers without this part of this the thesis is very difficult.
- In the theoretical part a new procedure for the classification of risk for road vehicles have been created, which simplifies the process of risk assessment and the assignment of safety integrity levels. The achieved result is considerable simplification of procedures for risk assessment with outputs fully comparable with the recommendations of ISO 26262.
- In the theoretical part of the thesis were selected, described and developed methods for qualitative and quantitative evaluation of functional safety. The obtained result is the selection of appropriate methods to meet the needs of industrial practice, thus the use of methods as simple as possible in terms of vehicle component manufacturers, and concurrently methods, providing sufficient quality outputs.

The practical part focuses on the application of the procedures and methods proposed in the theoretical part. Procedures and methods have been applied to the bus entrance door and headlight of the car. Evaluation of the achieved results significant for practice is performed in the following points:

- The achieved result is to perform the qualitative assessment of reliability using the ASAM process, fault tree analysis (FTA) and the failure mode and effect analysis (FMEA). Each functions of bus entry door and the modes of their failures have been identified. The result of this is design of measures to reduce the risk to a socially acceptable level. Residual risks meet the requirements for safety integrity level ASIL.
- The achieved result for the quantitative analysis of the car headlight is to create a theoretical model of reliability for hardware random failures. On the basis of this model is possible calculate the specific numerical values of the functional safety indicator. On the basis of failure rate prediction of hardware forming elements was determined numerical value of the target failure rate. The circuit schemes have been analyzed and such measures were designed, that meet the target failures rate at given level of ASIL. In addition an evaluation of LED circuit scheme quality with three parameters has been performed, namely parameter SPM, parameter LFM and diagnostic coverage DC_{RF}. The achieved values of parameter SPM, LFM and DC_{RF} meet the required level of ASIL.
- Another result is a LED headlight accelerated reliability test and verification of the target failure rate and reliability requirements for the life cycle profile. Depending on the results of the test computational model shall be the test duration meet at least 3,450 hours without failure.

The key issues for further development:

- Other possibilities of using can be seen in the definition of principles for the methodology of design of safety-related mechanical systems and the development of validation methods.
- Because that many of the technical systems appears as mechatronic systems and part of the safety is linked to the mechanical parts of the system, is possible to expand and develop the problems of assessing the ability of the mechanical system meet the requirements of safety integrity as a whole.

- Further acceleration of the reliability tests by the realization in time-varying thermal loads or in larger number of accelerating loads (vibration, humidity, etc.). In this context, the creation of mathematical models of these tests.

Contribution to science and experience.

The focus of the contribution of doctoral thesis for scientific field reliability is given in the following points:

- The risk assessment methodology has been improved. The benefit is a significant simplification of the procedure for risk assessment methodology compared to ISO 26262. The obtained results using the proposed methodology of risk assessment fully comply with quality requirements according ISO 26262.
- Mathematical model of accelerated reliability tests based on the principle of Arrhenius formulas for the rate of a chemical reaction has been designed. The proposed test profile allows you to simultaneously verify the achieved failure rate in terms of the ASIL requirements and verify compliance failure rate in terms of the expected life cycle of the headlight. This makes it possible previously two isolated tests performed simultaneously, resulting in substantial benefits in terms of cost and time savings in the development phase of the headlight.
- The results of this thesis can be used in university pedagogical practice, by implementation of knowledge in the courses related to the design, reliability and safety of transport means in the bachelor's, master's and doctoral programs. The Key contribution of the theoretical part is an issue of vehicles functional safety, which can be considered, according to the author, as a new and therefore for the students in the Czech Republic (and not only them) unknown. By using appropriate examples can be presented and applied methods and procedures for analysis and evaluation of the reliability and safety based on the requirements of ISO 26262 and ČSN EN 61508.

Seznam použité literatury

[1] BRIŠ, Radim. *Teorie spolehlivosti : učební text pro Fakultu aplikované informatiky, UTB Zlín* [online]. Ostrava : VŠB - TU Ostrava, 2007 [cit. 2009-11-06]. Dostupné z WWW: <http://am.vsb.cz/bris/>.

[2] BRIŠ, Radim; LITSCHMANNOVÁ, Martina. *Statistika I. pro kombinované a distanční studium* [online]. Ostrava : VŠB - TU Ostrava, 2004 [cit. 2009-11-06]. Dostupné z WWW: <http://am.vsb.cz/bris/>.

[3] FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. *Teorie údržby* [online]. Ostrava : VŠB - TU Ostrava, 2007 [cit. 2009-11-21]. Dostupné z WWW: <http://homel.vsb.cz/~krz011/>. ISBN 978-80-248-1509-1.

[4] HOLUB, Rudolf. *Zkoušky spolehlivosti (Stochastické metody)*. Brno : Vojenská akademie v Brně, 1992. 226 s. S-1590.

[5] HOLUB, Rudolf; VINTR, Zdeněk. *Spolehlivost letadlové techniky (elektronická učebnice)* [online]. Brno : VUT v Brně, 2001 [cit. 2009-11-21]. Dostupné z WWW: <http://lu.fme.vutbr.cz/download.php>.

[6] KECECIOGLU, Dimitri. *Reliability & Life Testing Handbook, Volume 2*. Englewood Cliffs : PTR Prentice Hall, 1994. 859 s. ISBN 0-13-772369-5.

[7] KRZYŽANEK, Radek. *Stanovení spolehlivostních charakteristik nové generace modulu automatického vedení vlaku*. Ostrava: VŠB – TU Ostrava 2011. Disertační práce. Vysoká škola báňská - Technická univerzita Ostrava. Fakulta strojní. Institut dopravy

[8] LÁNSKÝ, Milan. *Systémová diagnostika a její fenomenologie*. 2011. Univerzita Pardubice. Dopravní fakulta Jana Pernera, 205 s. ISBN 0-13-772369-5.

[9] STODOLA, Jiří. *Aplikace zrychlené zkoušky Bezporuchovosti u mechanických prvků*. Zrychlené zkoušky bezporuchovosti a možnosti jejich praktické aplikace. Materiály z 39. setkání odborné skupiny pro spolehlivost Brno. Česká společnost pro jakost. Praha. 2010, s. 27-53. ISBN 978-80-02-02062-2

[10] *Accelerated Life Testing Analysis* [online]. [cit. 2009-11-16]. Dostupné z WWW: <http://www.weibull.com/acceltestwebcontents.htm>.

[11] ISO 26262-1. *Road vehicles – Functional safety – part 1: Vocabulary*. ICS 43.040.10 , 2011. International Organization for Standardization

[12] ISO 26262-2. *Road vehicles – Functional safety – part* 2: *Management of functional safety*. ICS 43.040.10 , 2011. International Organization for Standardization

[13] ISO 26262-3. *Road vehicles – Functional safety – part 3*: *Concept phase*. ICS 43.040.10 , 2011. International Organization for Standardization

[14] ISO 26262-4. *Road vehicles – Functional safety – part 4*: *Product development at the*

system level. ICS 43.040.10 , 2011. International Organization for Standardization

[15] ISO 26262-5. *Road vehicles – Functional safety – part 5*: *Product development at the hardware level*. ICS 43.040.10 , 2011. International Organization for Standardization

[16] ISO 26262-6. *Road vehicles – Functional safety – part 6*: *Product development at the software level*. ICS 43.040.10 , 2011. International Organization for Standardization

[17] ISO 26262-7. *Road vehicles – Functional safety – part 7*: *Production and operation*. ICS 43.040.10 , 2011. International Organization for Standardization

[18] ISO 26262-8. *Road vehicles – Functional safety – part 8*: *Supporting processes*. ICS 43.040.10 , 2011. International Organization for Standardization

[19] ISO 26262-9. *Road vehicles – Functional safety – part* 9: *Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*. ICS 43.040.10 , 2011. International Organization for Standardization

[20] ISO 26262-10. *Road vehicles – Functional safety – part 10*: *Guideline on ISO 26262*. ICS 43.040.10 , 2012. International Organization for Standardization

[21] ČSN EN 61508-1. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky.* Praha :Český normalizační institut, 2002. 60 s.

[22] ČSN EN 61508-2. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností.* Praha :Český normalizační institut, 2002. 76 s.

[23] ČSN EN 61508-4. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 4: Definice a zkratky.* Praha : Český normalizační institut, 2002. 32 s.

[24] ČSN EN 61508-5. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 5: Příklady metod určování úrovní integrity bezpečnosti.* Praha : Český normalizační institut, 2002. 32 s.

[25] ČSN EN 61508-6. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3.* Praha : Český normalizační institut, 2002. 72 s.

[26] *ReliaSoft's Xfmea Version 5 : Software Training Guide* [online]. Tucson : ReliaSoft Corporation, 2006 [cit. 2010-04-02]. Dostupné z WWW: <http://Xfmea.ReliaSoft.com>.

[27] *System Analysis Reference: Reliability, Availability and Optimization* [online]. RBDs and Analytical System Reliability [cit. 2010-05-12]. Dostupné z WWW: <http://www.weibull.com/systemrelwebcontents.htm>.

[28] *System Analysis Reference: Reliability, Availability and Optimization* [online]. RBDs and Analytical System Reliability [cit. 2010-05-12]. Dostupné z WWW: <http://www.weibull.com/systemrelwebcontents.htm>.

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

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

[31] ČSN EN 61078. *Techniky analýzy spolehlivosti - Blokový diagram bezporuchovosti a booleovské metody*. Praha : Český normalizační institut, 2007

[32] MAREK, Pavel; GESTAR, Milan; ANAGNOS, Thalia. *Simulation-based Reliability Assessment for Structural Engineer.,*CRC Press, Boca Raton, 1996, 365 s. ISBN 0-8493-8286-6.

Seznam vybraných publikací doktoranda

[1] FAMFULÍK, J., MÍKOVÁ, J., LÁNSKÁ, M., RICHTÁŘ, M. *A stochastic model of the logistics actions required to ensure the availability of spare parts during maintenance of railway vehicles.* Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 0954409712465695, first published on November 15, 2012 as doi:10.1177/0954409712465695, IF 0,573

[2] ŠMIRAUS, J., RICHTÁŘ, M: *Design of Motorcyle Active Chassis Geometry Change System.* Perners Contacts, Number IV, Volume V 2012, Univerzita Pardubice, s. 279-288, ISSN 1801-674X

[3] DRESLER, P., RICHTÁŘ, J: *Simulation Model of the Singlecylinder Combustioun Engine MZ 125*. Perners Contacts, Number IV, Volume V 2012, Univerzita Pardubice, s. 80-88, ISSN 1801-674X

[4] KUTĚJ, L., RICHTÁŘ M. *Aerodynamic interaction of two vehicles in selected drive modes*, Perners Contacts,Number IV, Volume V, December 2010, 300 pages, 104-110, ISSN 1801-674X

[5] GALVAS, P., RICHTÁŘ M. *Utilization possibilities of the hybrid drive In land transport*, Perners Contacts,Number IV, Volume V, December 2010, 300 pages, 51-61, ISSN 1801-674X

[6] MÍKOVÁ, J., RICHTÁŘ, M. *Maintenance costs modeling of small road vehicle fleet.* Advanced Logistic Systems: Theory and Practice, University of Miskolc, 2009, s. 143-146, ISSN 1789-2198

[7] BOROVEC, K.; RICHTÁŘ, M.; KŘIVDA, V.; OLIVKOVÁ, I. *N_2O Emissions from the Mobile Sources.* Perner's Contact - January 2008, Number I. Volume III, 8/2008 [14. 1. 2008]. Elektronický odborný časopis o technologii a logistice v dopravě. Dostupné na WWW: <http://pernerscontacts.upce.cz/>. ISSN 1801-674X

[8] KŘIVDA, V.; RICHTÁŘ, M.; OLIVKOVÁ, I. *Essential Dynamical Traffic Flow Characteristic Surveillance Using Counting Facility Viacount II*. Sborník vědeckých prací FS. Ostrava: VŠB-TU Ostrava, 2008, s. 153-158. ISBN 978-80-248-1633-3, ISSN 1210-0471

[9] RICHTÁŘ, M.; OLIVKOVÁ, I.; KŘIVDA, V.; MATĚJKA, R. *Vybrané aspekty problematiky zavedení dlouhých a těžkých jízdních souprav*. Zdvihací zařízení v teorii a praxi. II/2006, Elektronický odborný časopis o konstrukci a provozu zdvihacích, manipulačních a transportních zařízení a dopravních prostředků. VŠB-TU Ostrava 2006, s. 47-56. ISSN 1802-2812

[10] RICHTÁŘ, M., *Advanced numerical reliability characteristics of vehicles***,** Second international konference "Reliability, safety and diagnostics of transport structures and means 2005", University of Pardubice, Czech Republic, 7-8 July 2005, ISBN 80-7194-769-5

Skripta, knihy, vysokoškolské učebnice domácí

[1] KŘIVDA, V; OLIVKOVÁ, I; RICHTÁŘ, M; PALO, J. *Dopravní telematika*. Kniha – vysokoškolská učebnice, 2009, 345 s. ISBN 978-80-8070-981-5.

[2] OLIVKOVÁ, I; KŘIVDA, V; RICHTÁŘ, M; KRAJČÍR, D. *Dopravní telematika II*. Skripta VŠB-TU Ostrava, 2008, 156 s. ISBN 978-80-248-1932-7.

[3] SUROVEC, P; MATĚJKA R; ŠKAPA, P; ROJÍČEK E; OLIVKOVÁ, I; KŘIVDA, V; RICHTÁŘ, M; KRAJČÍR, Dušan. *Manažer silniční dopravy*. Vydáno v rámci vzdělávacího projektu ESF "Zvyšování kvalifikace v oblasti Doprava". 1. vyd. Ostrava: VŠB - Technická univerzita Ostrava, 2007, 211 s. ISBN 978-80-248-1447-6

[4] ŠKAPA, P; KŘIVDA, V; OLIVKOVÁ, I; RICHTÁŘ, M; KRAJČÍR, D. *Základy dopravy*. Vydáno v rámci vzdělávacího projektu ESF č. CZ.04.01.3/.2.15.2/0326 "E-learningové prvky pro podporu výuky odborných a technických předmětů". 1. vyd. Ostrava: VŠB - Technická univerzita Ostrava, 2007, 492 s. ISBN 978-80-248-1499-5

[5] DANĚK, A., RICHTÁŘ M, RUBÁČ I., *Opravárenství silničních vozidel II***,** VŠB-Technická Universita Ostrava, Ostrava, 2004, 1. Vydání, stran 116, ISBN 80-248-0539-1

[6] DANĚK, A., RICHTÁŘ M, *Cvičení z teorie obnovy dopravních prostředků***,** VŠB - Technická Universita Ostrava, Ostrava, 2003, 1. Vydání, Počet stran 90, ISBN 80-248-0249-X

Patenty, vynálezy

Patent P 303473: 2011-292 - realizovaný patent

Název: Zavěšení předního kola jednostopého vozidla s aktivní změnou geometrie
Majitel: Vysoká škola báňská – Technická univerzita Ostrava
Původce: Bc. Jakub Šmiraus (podíl 50%)
Ing. Michal Richtář (podíl 25%)
Ing. Jana Míková, Ph.D. (podíl 25%)
(http://isdv.upv.cz/portal/pls/portal/portlets.rejst.detail)

Funkční vzorek 064/24-10-2011 F

Název: Zavěšení předního kola jednostopého vozidla s aktivní změnou geometrie
Majitel: Vysoká škola báňská – Technická univerzita Ostrava
Původce: Bc. Jakub Šmiraus (podíl 50%)
Ing. Michal Richtář (podíl 25%)
Ing. Jana Míková, Ph.D. (podíl 25%)
(http://isdv.upv.cz/portal/pls/portal/portlets.rejst.detail)

Užitný vzor UV 22413: 2011-24355

Název: Zavěšení předního kola jednostopého vozidla s aktivní změnou geometrie
Majitel: Vysoká škola báňská – Technická univerzita Ostrava
Původce: Bc. Jakub Šmiraus (podíl 50%)
Ing. Michal Richtář (podíl 25%)
Ing. Jana Míková, Ph.D. (podíl 25%)
(http://isdv.upv.cz/portal/pls/portal/portlets.rejst.detail)

Užitný vzor UV 22158: 2011-23805

Název: Pohybový mechanizmus simulátoru vozidel
Majitel: Vysoká škola báňská – Technická univerzita Ostrava
Původce: Ing. Jan Famfulík, Ph.D. (podíl 50%)
Ing. Jana Míková, Ph.D. (podíl 25%)
In. Michal Richtář (podíl 25%)
(http://isdv.upv.cz/portal/pls/portal/portlets.rejst.detail)

Užitný vzor UV 21203: 2010-22983

Název: Lapač nečistot pro silniční vozidla se zábranou proti vytržení
Majitel: Vysoká škola báňská – Technická univerzita Ostrava
Původce: Ing. Jan Famfulík, Ph.D. (podíl 50%)
Ing. Jana Míková, Ph.D. (podíl 30%)
Ing. Michal Richtář (podíl 20%)
(http://isdv.upv.cz/portal/pls/portal/portlets.pts.lst)

Projekty

Projekt: SP2012/198 s názvem „Vývoj zařízení pro měření parametrů motocyklu na dynamometrické válcové zkušebně“.
Zodpovědný řešitel: Ing. Jana MÍKOVÁ, Ph.D.
Řešitelé: Ing. Jan FAMFULÍK, Ph.D., Ing. Michal Richtář,
Ing. Jakub Šmiraus, Ing. Pavel Dresler,
Bc. Zuzana Galvasová
Období: 2012

Projekt: SP 2011/58 s názvem „Řešení aktivní změny geometrie motocyklu“.
Zodpovědný řešitel: Ing. Michal Richtář
Řešitelé: Ing. Jana MÍKOVÁ, Ph.D., Ing. Jakub Šmiraus
Období: 2011

Mobility

RICHTÁŘ M, *Warranty prediction problematic of vehicles*, Lecture, Vilnius Gediminas Technical University, Teaching Staff Mobility – Socrates Erasmus program, 6. -10. 6. 2006

RICHTÁŘ M, *Economy of Passengers Transport Service in Regions*, Lecture, Vilnius Gediminas Technical University, Teaching Staff Mobility – Socrates Erasmus program, 6. -10. 6. 2006

Seznam obrázků

Seznam tabulek

Příloha I. – MANAGEMENT BEZPEČNOSTI

INSTITUT DOPRAVY VŠB-TU OSTRAVA	MANAGEMENT BEZPEČNOSTI

Název projektu	
Zákazník	

Cíle projektu

Management projektu				
Funkce	**Jméno**	**Odpovídá za činnosti**	**Datum a podpis**	**Poznámka**
Vedoucí projektu		Souhrn požadavků na produkt, koncepce řešení, rozdělení činností na pracovníky, kontrola plnění úkolů, vypracování zprávy o posouzení bezpečnosti.		
Komunikace se zákazníkem		Souhrn požadavků na produkt, koncepce řešení, rozdělení činností na pracovníky, kontrola plnění úkolů.		
Vedoucí mechanické konstrukce		Koncepce řešení, rozdělení činností na pracovníky, kontrola plnění úkolů.		
Vedoucí elektrické konstrukce		Koncepce řešení, rozdělení činností na pracovníky, kontrola plnění úkolů.		
Projektant, analytik RAMS		Analýzy FMEA a FTA, stanovení požadavků na ASIL a MTBF.		
Komunikace se subdodavateli		Rozdělení činností na pracovníky, kontrola plnění úkolů, požadavky na produkt		

Zpráva o posouzení bezpečnosti				
Funkce	**Jméno**	**Odpovídá za činnosti**	**Datum a podpis**	**Poznámka**
Navrhovatel		Vypracování zprávy o posouzení bezpečnosti.		
Posuzující tým		Posouzení managementu projektu.		
		Posouzení záznamů o nebezpečí, posuzovaná nebezpečí a analýza rizik.		
		Posouzení úplnosti dokumentace, posouzení průběhu validace.		

	Zpracoval	**Schválil**
funkce		
jméno		
podpis		
Datum		

Příloha II. – HODNOCENÍ NEBEZPEČÍ – Elektricky ovládané dveře

INSTITUT DOPRAVY VŠB-TU OSTRAVA ©MR	INSTITUT DOPRAVY, Fakulta strojní, VŠB TU - Ostrava Hodnocení nebezpečí	Dokument č.	
		Změna č.	
Výrobek:	**Vstupní dveře s elektrickým pohonem**	**Požadavek č.**	
Číslo výkresu:		**Název projektu :**	
Předkladatel:	**Ing. et Ing. Michal Richtář**	**Datum:**	
Zaznamenal:	**Ing. et Ing. Michal Richtář**	**Datum:**	
Pracovník odpovědný za navržená opatření:		**Datum:**	
Schválil:		**Datum:**	

				Hodnocení nebezpečí podle ASAM						
No.	**Nebezpečí**	**Popis nebezpečí - následky nebezpečí**	**Příčiny nebezpečí, uzly, zařízení**	**Škody počet (SA)**	**Škody zranění (SV)**	**Pravděpodobnost výskytu (W)**	**Doba vystavení (E)**	**Zamezení (V)**	**Klasifikační indikátor (I)**	**ASIL**
H1	Náhlé uvolnění (otevření, odpadnutí) vstupních dveří	1 a více osob (u dveří může stát pouze jedna osoba, popřípadě se na dveře může tlačit více osob) - lehké zranění (vypadnutí při nízké rychlosti na vozovku nebo na ostrůvek), těžká zranění (vypadnutí při vysoké rychlosti na vozovku, nebo na ostrůvek) smrt	1) násilím došlo k zničení zámku dveří, 3) dveře odpanou poškozením závěsu, 4) selže elektronika, 5) funkční nouzové ovládání (dveře se jím daly otevřít), 6) dveře odpadnou poškozením závěsu - vysoké zatížení šroubů, držící dveře v závěsu	5,00	9,00	1,70	1,30	1,00	99	C
H2	Vozidlo nejde opustit dveřmi - standardní situace, dveře se neotevřely: výstup, nástup cestujících na zastávce	1 a více osob, vznikne panika - lehká zranění (v důsledku tlačenice k jiným dveřím), nezávažné nebezpečí	1) selhání elektroniky, 2) nedošlo k mechnickému oblokování dveří, 3) zamrznutí dveří, 4) dveře byly z důvodu poruchy odstaveny (nebyly označeny)	5,00	2,00	1,70	1,00	1,00	17	0
H3	Vozidlo nejde opustit dveřmi - nouzová situace, dveře se neotevřely, nejdou otevřít po nehodě : výstup	1 a více osob, vznikne panika - těžká zranění (např. oheň v blízkosti cestujících, avšak možnost úniku z vozidla), smrt (oheň v bezprostřední blízkosti dveří, kde cestující stojí a kde dveře nejdou otevřít), závažné nebezpečí	1) selhání nouzového ovládání dveří, 2) násilné poškození dveří - zničení zámku, 3) pohon způsobil neotevření dveří	5,00	9,00	1,70	1,30	1,70	59	B
H4	Osoba (cestující) je dveřmi přivřena : nástup, výstup	1, popř. 2 osoby (do dveří může vcházet pouze jedna osoba, ale i matka s dítětem nebo se mohou předhánět školáci)- těžká zranění (amputace některé části těla), smrt (nevšimnutí si přivřené osoby a následně dojde k rozjetí vozidla), nezávažné nebezpečí	1) selhání elektroniky, 2) neopartnost cestujícího, 3) řidič si nevšiml nastupujícícho cestujícího	3,00	9,00	1,70	1,00	1,00	46	B
H5	Nezavření (nedovření) dveří, vozidlo se rozjede	1 a více osob (při jízdě dojde k nečekanému otevření dveří) - lehká zranění (dojde k otevření dveří při nižší rychlosti - přiskřípnutí cestujících poblíž dveří), těžké zranění (otevření dveří při vysoké rychlosti - zlomeniny, rozdrcení kostí) : pokračuje	1) zaklíněný předmět ve dveřích (schválně) - nemístný žert, 2) náhodně zaklíněný předmět, 3) nefunkční jedna část mechanického zavírání, 4) elektronika	5,00	9,00	1,70	1,30	1,00	99	C
H6	Vznícení (požár) dveří	1 a více osob - těžké zranění (cestující má možnost se vzdálit od ohniska požáru a zachránit se), nezávažné nebezpečí	1) zkrat nebo jiné poškození el. Instalace, 2) vysoká venkovní teplota, 3) intenzivní sluneční záření	5,00	2,00	1,00	1,30	1,00	13	0
H7	Zabití, zranění elektrickým proudem	1 osoba - zranění (jedná se o 24V) smrt 1 i více osob (na dveře spadne trolej), závažné nebezpečí	1) špatné ukostření 2) špatné izolační kabely	5,00	9,00	1,00	1,30	1,00	59	B

Příloha II. – HODNOCENÍ NEBEZPEČÍ – Návrh LED světlometu

INSTITUT DOPRAVY VŠB-TU OSTRAVA ©MR	INSTITUT DOPRAVY, Fakulta strojní, VŠB TU - Ostrava Hodnocení nebezpečí	Dokument č.	
		Změna č.	
Výrobek:	LED světlo automobilu	Požadavek č.	
Číslo výkresu:		Název projektu :	
Předkladatel:	Ing. et Ing. Michal Richtář	Datum:	
Zaznamenal:	Ing. et Ing. Michal Richtář	Datum:	
Pracovník odpovědný za navržená opatření:		Datum:	
Schválil:		Datum:	

No.	Nebezpečí	Popis nebezpečí - následky nebezpečí	Příčiny nebezpečí, uzly, zařízení	Hodnocení nebezpečí podle ASAM						
				Škody počet (SA)	Škody zranění (SV)	Pravděp odobnost výskytu (W)	Doba vystavení (E)	Zamezení (V)	Klasifikační indikátor (I)	ASIL
H1	Světlo pro denní svícení nesvítí, nebo svítí málo.	Zhoršerná identifikace vozidla, svítí druhé světlo. Možnost vzniku nehody, smrt více osob. Řidič může použít potkávací světlo.	1) Porucha CPU, 2) porucha budičů	5,00	9,00	1,00	1,30	1,70	34	A
H2	Světlo pro denní svícení svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H3	Potkávací světlo nesvítí, nebo svítí málo.	Zhoršená identifikace překážek, zhorčená identifikace vozidla, svítí druhé světlo. Možnost vzniku nehody, nebo sražení chodců, cyklisty. Řidič nemůže světlo opravit.	1) Porucha CPU, 2) porucha budičů	5,00	9,00	1,00	1,30	1,70	34	A
H4	Potkávací světlo svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H5	Obrysové světlo nesvítí, nebo svítí málo.	Zhoršerná identifikace vozidla, svítí druhé světlo, nebo řidič může použít denní světlo. Bez následků, dále nehodnoceno.								0
H6	Obrysové světlo svítí nevyžádaně.	Bez následků, dále nehodnoceno.								0
H7	Dálkové světlo sesvítí nebo svítí málo.	Zhoršená identifikace překážek, ridič použije potkávací světla. Bez následků, dále nehodnoceno.								0
H8	Dálkové světlo svítí nevyžádaně.	Řidič vozidla nemůže reflektor vypnout. oslnění řidičů protijedoucích vozidel, Zranění nebo smrt více osob v důsledku nehody.	1) Porucha CPU, 2) porucha zdroje PSU 2, 3) porucha bezpečnostního obvodu.	5,00	9,00	1,00	1,30	1,00	59	B
H9	Vznícení (požár) světla	1 a více osob - lehké zranění, cestující má možnost se vzdálit od ohniska požáru a zachránit se.	1) zkrat nebo jiné poškození el. Instalace, 2) vysoká venkovní teplota.	5,00	2,00	1,00	1,30	1,70	8	0

Příloha III. – BEZPEČNOSTNÍ OPATŘENÍ - Elektricky ovládané dveře

INSTITUT DOPRAVY VŠB-TU OSTRAVA ©MR	ZÁZNAM O NEBEZPEČÍ 2/2 navržená bezpečnostní opatření			č. dokumentu: změna č:
Výrobek:	Vstupní dveře s elektrickým pohonem			
Číslo výkresu:				
Předkladatel:	Ing. et Ing. Michal Richtář		Datum:	
Zaznamenal:	Ing. et Ing. Michal Richtář		Datum:	

No.	Opatření technická	Opatření vnějším systémem	Opatření údržbová	Opatření organizační a legislativní	Související dokumenty
H1	BF1 - Uvedení řídící jednotky do bezpečného stavu. BF2 - Signalizace poruchy řidiči.	Není.	Kontrola obou bezpečnostních funkcí po 30000 km.	Typová zkouška	Pracovník odpovědný za Schválil termín
	Stav opatření	Stav opatření	Stav opatření	Stav opatření	
	Odpovídá výrobce.		Odpovídá provozovatel.	Odpovídá výrobce.	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	Související dokumenty Pracovník odpovědný za navržená opatření, termín
	Stav opatření	Stav opatření	Stav opatření	Stav opatření	Schválil termín
				Odpovídá provozovatel.	
H1	BF2 - Signalizace poruchy řidiči.	Není.	Kontrola bezpečnostní funkce po 30000 km.	Typová zkouška	Související dokumenty Pracovník odpovědný za navržená opatření, termín
	Stav opatření	Stav opatření	Stav opatření	Stav opatření	Schválil termín
	Odpovídá výrobce.		Odpovídá provozovatel.	Odpovídá výrobce.	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	Související dokumenty Pracovník odpovědný za navržená opatření, termín
	Stav opatření	Stav opatření	Stav opatření	Stav opatření	Schválil termín
				Odpovídá provozovatel.	
H1	Testování SW řídící jednotky dle ISO 26262-6.	Není.	Není.	Není.	Související dokumenty Pracovník odpovědný za navržená opatření, termín
	Stav opatření	Stav opatření	Stav opatření	Stav opatření	Schválil termín
	Odpovídá výrobce.				

No.	Opatření technická	Opatření vnějším systémem	Opatření údržbová	Opatření organizační a legislativní	
H1	Vhodné dimenzování mechanismu jištění, kontrola pomocí MKP.	Není.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Životnostní zkouška.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá výrobce.**	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
				Odpovídá provozovatel.	
H1	Motor s požadovanými technickými a spolehlivostními parametry.	Není.	Není.	Není.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.				
H1	BF2 - Signalizace poruchy řidiči. Snímač s požadovanými technickými a spolehlivostními parametry.	Není.	Kontrola bezpečnostní funkce po 30000 km.	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá provozovatel.**	
H1	Vhodné dimenzování mechanismu lineárního vedení, kontrola pomocí MKP.	Není.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Životnostní zkouška.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá výrobce.**	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
				Odpovídá provozovatel.	
H1	Vhodné dimenzování ramene dveří, kontrola pomocí MKP.	Není.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu po ujení 30000 km.	Životnostní zkouška.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá výrobce.**	

No.	Opatření technická	Opatření vnějším systémem	Opatření údržbová	Opatření organizační a legislativní	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
				Odpovídá provozovatel.	
H1	Vhodné dimenzování spojovacích součástí, utažení správným dotahovacím momentem.	Není.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola a dotažení spojovacích částí správným dotahovacím momentem po ujetí 30000km.	Životnostní zkouška.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá výrobce.**	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
				Odpovídá provozovatel.	
H1	Vhodné dimenzování křídla dveří, kontrola pomocí MKP.	Není.	Kontrola v rámci pravidelné údržby. Vizuální kontrola při denní prohlídce (500km). Podrobná kontrola mechanismu a mazání po ujení 30000 km.	Životnostní zkouška.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
	Odpovídá výrobce.		**Odpovídá provozovatel.**	**Odpovídá výrobce.**	
H1	–	–	–	Řidič postupuje dle předpisů provozovatele.	**Související dokumenty**
					Pracovník odpovědný za navržená opatření, termín
	Stav opatření	**Stav opatření**	**Stav opatření**	**Stav opatření**	**Schválil termín**
				Odpovídá provozovatel.	

Příloha IV. – PLÁN BEZPEČNOSTI

INSTITUT DOPRAVY VŠB-TU OSTRAVA	PLÁN BEZPEČNOSTI	č. dokumentu:
		změna:

Projekt - výrobek								
Předkladatel:	Jméno:						Datum:	
Shválil:	Jméno:						Datum:	
Fáze	**Etapa**	**Etapa - činnosti**	**Termín**	**Č. dokumentu**	**Splněno**	**Pracovník**	**Validace**	**Poznámka**
1. Volba koncepce	1.1	Požadavky zákazníka			ano	OM	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	1.2	Plán organizace projektu			ne	VŘP	Termín:	
	1.3	Management bezpečnosti			ano	VŘP, MRAMS	Pracovník:	
	1.4	Rámcový program RAMS projektu , Průkaz bezpečnosti			ne	VŘP, MRAMS		
2. Definice a podmínky použití	2.1	Specifikace požadavků - předběžné analýzy RAMS			ano	VŘP, MRAMS, OM, MTZ,TS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	2.2	Provozní podmínky a normy			ano	VŘP, MRAMS, OM,TS	Termín:	
	2.3	Definice kritérií bezpečnosti			ne	VŘP,MRAMS, OM,TS		
	2.4	Určení podmínek dlouhodobého provozu a údržby			ano	OM, MRAMS, TS	Pracovník:	
	2.5	Vypracování plánu bezpečnosti			ano	VŘP, MRAMS		
3. Analýza rizika	3.1	Analýza rizika sytému			ano	VŘP,TS, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	3.2	Chování při chybových podmínkách			ano	VŘP, TS, MRAMS	Termín:	
		Zpráva za etapu			ano	MRAMS	Pracovník:	
							Č. dokumentu:	
4. Požadavek na výrobek	4.1	Specifikace požadavků na RAMS a funkční požadavky			ano	VŘP,TS, MRAMS	Validace	požadavky na SIL
	4.2	Definice kritérií přejímky týkající se RAMS			ano	VŘP,TS, MRAMS	Termín:	požadavky na SIL
	4.3	Vypracování programu RAMS výrobku			ano	VŘP, MRAMS	Pracovník:	časový harmonogram
		Zpráva za etapu				MRAMS	Č. dokumentu:	Vstoupí do důkazů bezpečnosti
5. Rozdělení požadavků na výrobek	5.1	Alokace požadavků na RAMS subsystémů			ano	VŘP,TS, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	5.2	Požadavky na dodavatele subsystému Požadavky na výrobu			ne	VŘP,TS, MRAMS, MTZ, VŘ	Termín:	
	5.3	Aktualizace programu RAMS pro projekt			ne	VŘP, MRAMS	Pracovník:	
6. Návrh a zavedení	6.1	Návrh výrobku na požadovanou úroveň RAMS			ano	VŘP, TS, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	6.2	Realizace návrhu výrobku výrobou prototypu			ano	VŘP, TS, MRAMS	Termín:	
	6.3	zrušit			ano	VŘP, TS, MRAMS		
	6.4	Definovat a ověřovat výrobní proces			ne	VŘP, TS, MRAMS, VŘ	Pracovník:	
	6.5	Mapa dokumentace RAMS			ano	MRAMS		
7. Výroba	7.1	Ověření výrobního procesu z hlediska RAMS			ano	VŘP, VŘ, ŘKJ, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	7.2	Ověření oddolnosti výrobku na okolí			ne	VŘP, TS, ŘKJ, MRAMS	Termín:	
	7.3	Zkoušky výrobku pro zlepšení RAMS			ano	VŘP, TS, ŘKJ, MRAMS	Pracovník:	
	7.4	Zavedení systému hlášení poruch			ano	VŘP, TS, SE, MRAMS		
8. Instalace	8.1	Stanovit a zavést plán instalace			ano	VŘP, TS, SE, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	8.2	Připravit a zavést výcvik pracovníků údržby a obsluhy			ne	VŘP, TS, SE, MRAMS	Termín:	
	8.3	Stanovit program logistického zajištění údržby			ne	VŘP, TS, SE, MTZ, MRAMS	Pracovník:	
	8.4	Aktualizace plánu bezpečnosti			ano	VŘP, TS, MRAMS		
9. Validace	9.1	Validace subsystémů			ne	VŘP, TS, MRAMS	Validace	Zpráva za etapu Vstoupí do důkazů bezpečnosti
	9.2	Plán uvedení výrobku do provozu			ano	VŘP, TS, SE, MRAMS	Termín:	
	9.3	Důkaz bezpečnosti			ne	Předkladatel, MRAMS	Pracovník:	
		Zpráva za etapu			ano	MRAMS	Č. dokumentu:	
10. Přejímka	10.1	Aktualizovaná analýza rizika - přejímka			ano	VŘP, OM, TS, MRAMS	Termín: Pracovník:	Zpráva za etapu
11. Provoz a údržba	11.1	Aktualizovaná koncepce údržby a způsoby sledování provozu			ano	VŘP, SE, MRAMS	Termín:	Zpráva za etapu
	11.2	Aktualizace záznamu o nebezpečí			ano	VŘP, TS, MRAMS	Pracovník:	
		Zpráva za etapu			ano	MRAMS	Č.dokumentu:	
12. Sledování výkonnosti	12.1	Sběr dat - parametry RAMS			ano	VŘP, SE, MRAMS	Termín:	Zpráva za etapu
	12.2	Analýza a vyhodnocení parametrů RAMS			ano	VŘP, TS, MRAMS	Pracovník:	
13. Modifikace a regenerace	13.1	Plán modifikace, plán bezpečnosti a aktualizovaný program RAMS projektu			ano	VŘP, MRAMS, TS	Termín: Pracovník:	Zpráva za etapu
14. Vyřazení z provozu a	14.1	Vyřazení z provozu a likvidace			ano	MRAMS, Zákazník	Termín:	Zpráva za etapu
	14.2	Analýza výkonnosti životního cyklu výrobku			ano	VŘP, MRAMS	Pracovník:	