Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1

Funkční bezpečnost v automobilovém průmyslu

Materiály z 80. semináře Odborného centra Spolehlivost
konaného dne 7. 12. 2021 online

Odborný garant semináře:
Ing. Michal Vintr, Ph.D.

Obsah

Úvod do funkční bezpečnosti

Ing. Michal Vintr, Ph.D.

Nezávislý expert na spolehlivost, bezpečnost a RAMS/LCC

mvintr@mvintr.cz – www.mvintr.cz

1 Úvod

Cílem článku je uvést čtenáře do problematiky funkční bezpečnosti a do obecných principů jejího zajišťování v různých průmyslových oborech.

V článku jsou vysvětleny základní pojmy z oblasti funkční bezpečnosti a představeny základní standardy obsahující požadavky na funkční bezpečnost. Dále je v článku nastíněno, co obnáší zajišťování funkční bezpečnosti. Na závěr jsou stručně představeny metody z oblasti funkční bezpečnosti (FMEA a FTA), které jsou uplatněny v dalších dvou článcích.

Funkční bezpečnost byla dosud předmětem několika jednotlivých příspěvků na seminářích Odborného centra Spolehlivost (OCS) (dříve Odborné skupiny pro spolehlivost), např.:

- 46. seminář: Případové studie realizace projektů spolehlivosti;
- 53. seminář: Bezpečnost a spolehlivost nových technologií;
- 66. seminář: Nejčastější mýty ve spolehlivosti.

První a dosud jediný seminář OCS zaměřený výhradně na oblast funkční bezpečnosti proběhl v roce 2018:

- 70. seminář: Funkční bezpečnost – Normy a řešení v praxi.

Dosud žádný seminář Odborného centra Spolehlivost nebyl monotematicky zaměřen na funkční bezpečnost v automobilovém průmyslu. Tématem se dosud zabýval pouze jeden příspěvek:

- Introduction to ISO 26262 and its limitations with regards to ADAS [3] – v rámci 75. semináře Aplikované techniky spolehlivosti v automobilovém inženýrství.

2 Funkční bezpečnost

Funkční bezpečnost / functional safety / funktionale Sicherheit / sécurité fonctionnelle.

Funkční bezpečnost je v dnešní době především odborným pojmem používaným v mnoha průmyslových oblastech, kde elektrické/elektronické/programovatelné elektronické (E/E/PE) systémy plní funkce, jejichž selhání mohou negativně ovlivňovat bezpečnost (průmysl automobilový, procesní, železniční, letecký a další).

Funkční bezpečnost je také samostatnou inženýrskou disciplínou a je náplní práce mnoha odborníků v uvedených průmyslových oborech. Funkční bezpečnost je také předmětem komerčního vzdělávání a certifikací jak osob, tak systémů.

Podobně jako spolehlivost a bezpečnost, funkční bezpečnost jako „vlastnost“ existovala dlouho před tím, než ji odborníci pojmenovali a začali se jí zabývat. Předmětem zájmu se funkční bezpečnost stala v 80. letech minulého století, zejména v souvislosti s rozvojem programovatelné elektroniky a software.

Problematika funkční bezpečnosti nezůstala stanou pozornosti mezinárodních standardizačních organizací a v roce 1995 byla vydána pracovní verze standardu IEC 1508 Functional Safety: Safety-Related Systems. Na základě zkušeností a připomínek k tomuto standardu bylo v letech 1998 až 2000 postupně vydáno 7 částí standardu IEC 61508.

K výraznému rozvoji v oblasti funkční bezpečnosti došlo v posledních cirka 20 letech. Jedním z dokladů může být porovnání stavu a množství mezinárodních standardů funkční bezpečnosti před 20 lety a dnes.

I přes náročnost požadavků na funkční bezpečnost v jednotlivých průmyslových odvětvích, množství a složitost používaných metod, postupů a výpočtů, je třeba nezapomenout, že jediným a hlavním cílem „zajišťování“ funkční bezpečnosti je **redukce rizika**.

3 Bezpečnost a riziko

Jednou ze základních charakteristik systémů je jejich bezpečnost, kterou obecně chápeme jako jejich schopnost neohrožovat při plnění požadovaných funkcí své okolí (osoby, životní prostředí či další systémy) či sama sebe. To, že systém může ohrožovat své okolí, v mnoha případech vyplývá přímo z podstaty systému a funkcí, které jsou u něj požadovány. Například vozidlo (např. při nevhodném způsobu řízení) může ohrožovat životy a zdraví jak pasažérů, tak dalších účastníků silničního provozu. V oblasti bezpečnosti však předmětem zájmu není to, jak systémy můžou ohrožovat své okolí v situaci, kdy fungují tak jak je požadováno, ale to, zda se nestávají nebezpečnými poté, co jejich schopnost fungovat tak, jak je požadováno, zanikne, tedy poté co u nich dojde k poruše.

Bezpečnost je ve standardech [5] definována jako absence nepřijatelného rizika. Přičemž obecně je *riziko* definováno jako účinek nejistoty na dosažení cílů [11]. V oblasti spolehlivosti a bezpečnosti je *riziko* konkrétněji definováno jako kombinace pravděpodobnosti výskytu újmy (fyzického zranění nebo poškození osoby, majetku a živého inventáře) a závažnosti této újmy [5].

Symbolicky lze uvedenou definici vyjádřit následujícím vztahem:

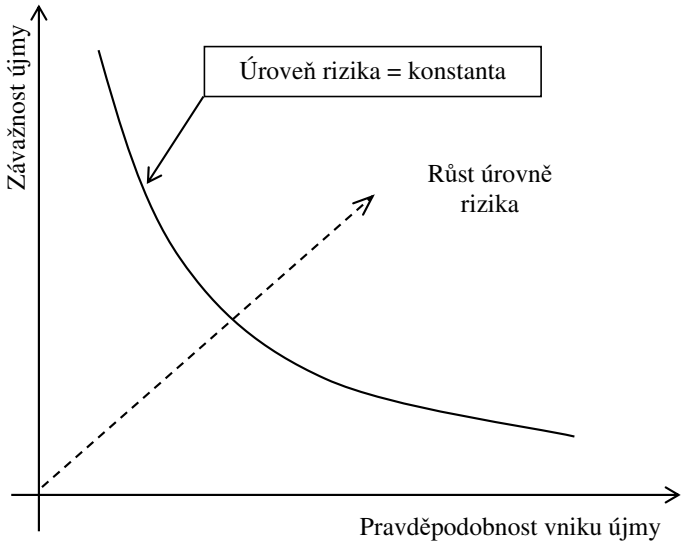
$$R = P \times C$$

kde: P – pravděpodobnost výskytu újmy;
C – závažnost újmy.

S využitím tohoto vztahu lze dobře znázornit základní filozofii hodnocení rizik (viz Obr. 1).

Z tohoto pohledu je nezbytné rizika spojená s poruchami systematicky vyhledávat, hodnotit a posuzovat, zda jsou přijatelná či nikoli a v případě, že se jako nepřijatelná ukážou, hledat cesty k jejich odstranění, nebo alespoň k jejich snížení na přijatelnou úroveň. Aby tento proces byl efektivní, je třeba ho uplatňovat především v předvýrobních etapách životního cyklu systému [1].

S bezpečností úzce souvisí pojem *nebezpečí*, které je definováno jako zdroj potenciálního poškození nebo újmy [11]. V oblasti spolehlivosti a bezpečnosti za takový zdroj potenciálního poškození považujeme poruchy systémů, případně chyby a omyly obsluhy systémů.



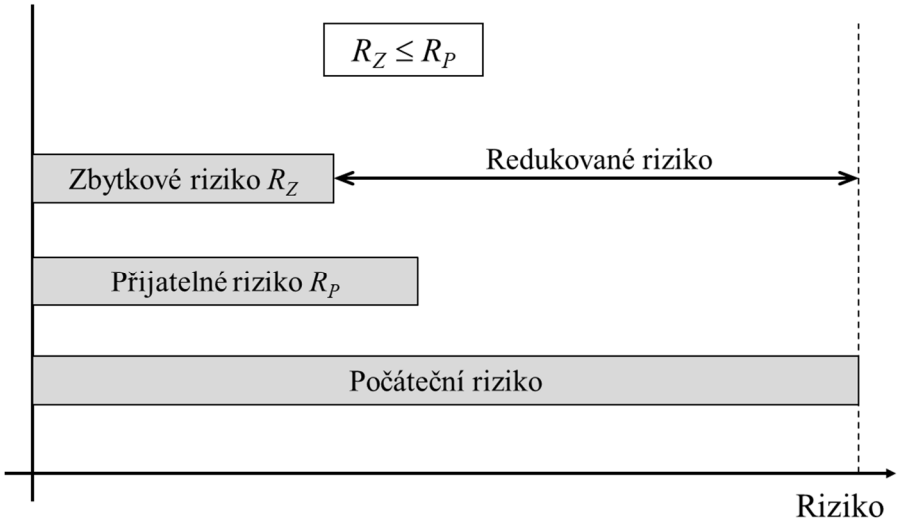
Obr. 1: Hodnocení rizika

Se snížením rizika na přijatelnou úroveň souvisí *přijetí rizika*, které je ve standardech [11] definováno jako vědomé rozhodnutí převzít určité riziko. Riziko, které je vědomě přijato (akceptováno), je v daném kontextu považováno za riziko přijatelné. Úroveň akceptovatelného rizika může být stanovena normou (předpisem, zákonem či obdobným dokumentem), rozhodnutím nebo pocitem. Rozhodnutím se stanovuje úroveň akceptovatelného rizika, pokud neexistuje odpovídající standard. Například, v rámci dodavatelsko-odběratelských vztahů, kdy požadavky na bezpečnost stanovuje odběratel. Pocitem se stanovuje akceptovatelná úroveň rizika zpravidla v rámci rozhodování jednotlivců (co se může zdát bezpečné pro jednu osobu, může být z pohledu jiné osoby spojeno s nepřijatelnými riziky). *Přijatelné (akceptovatelné) riziko* je ve standardech [5] označováno jako *tolerovatelné riziko* a definováno jako riziko, které je přijímáno v daném kontextu založeném na aktuálních hodnotách společnosti.

Snížení rizika na přijatelnou úroveň se dosahuje prostřednictvím *ošetření rizika*, které je ve standardech [11] definováno jako proces pro modifikování (změnu) rizika. Ošetření rizika se zpravidla aplikuje v těch případech, kdy z hodnocení rizika vyplyne, že dané riziko pro nás není akceptovatelné. Obecně ošetření rizika spojeného s poruchami systému může zahrnovat následující opatření:

- odstranění zdroje rizika (např. použitím jiné konstrukční technologie, u které nemůže dojít k danému typu poruchy nebo rozhodnutím realizovat zamýšlenou funkci systému jiným způsobem);
- snížením četnosti výskytu dané poruchy (např. použitím odolnějších konstrukčních materiálů, předimenzováním součástí, použitím zálohování, pravidelnou kontrolou a údržbou apod.);
- zmírněním nežádoucích důsledků poruchy (např. změnou konstrukce, použitím ochranných prvků pro obsluhu systému, provozními opatřeními) [1].

V rámci ošetření rizika zpravidla není dosaženo úplného odstranění rizika, ale je pouze snížena jeho úroveň na úroveň tzv. *zbytkového rizika* (R_Z), které je ve standardech [11] definováno jako riziko zbývající po ošetření rizika. Žádoucí je, aby toto zbytkové riziko mělo nižší úroveň než riziko v daném kontextu považované za přijatelné (R_P). Tento koncept je graficky znázorněn na Obr. 2.



Obr. 2: Ošetření rizika [1]

Zajišťování funkční bezpečnosti je jedním ze způsobů, jak redukovat riziko.

4 Základní pojmy

V následujících podkapitolách jsou vysvětleny vybrané základní pojmy z oblasti funkční bezpečnosti. Definice dalších pojmů lze nalézt v platných standardech, zejména v [8].

4.1 Funkce, funkční bezpečnost, integrita bezpečnosti a SIL

Funkce systému je chápána jako činnost, respektive způsob činnosti, prostřednictvím které systém plní svůj účel. Je to důvod, pro který systém existuje nebo má existovat. Funkce lze rozdělovat např. na hlavní funkce, vedlejší funkce, podpůrné funkce, informační funkce a funkce rozhraní.

Hlavní funkce vyjadřují podstatu existence systému. Pro realizaci těchto funkcí byl systém navržen a zejména plnění těchto funkcí se od něj očekává. Vedlejší funkce specifikují u systému další funkční vlastnosti, které zpravidla umožňují plnění hlavních funkcí a doplňují hlavní funkce o konkrétní vlastnosti. Podpůrné funkce jsou takové, které zpravidla nejsou pro vlastní výkon hlavních funkcí nezbytně nutné, ale které zvyšují užitnou hodnotu systému [2].

Funkce může být také *požadovaná*, tj. považovaná za nezbytnou ke splnění daného požadavku. Požadovaná funkce může být stanovená nebo samozřejmě předpokládaná (tj. to, co by odběratel oprávněně očekával). Do požadované funkce se samozřejmě zahrnuje též to, co systém nesmí dělat. Za požadované funkce též považujeme zásadně důležité vnitřní funkce systému, které nemusejí být pro uživatele viditelné.

V oblasti funkční bezpečnosti se používá pojem *bezpečnostní funkce*, což je dle standardů [8] funkce, která má být realizována systémem E/E/PE souvisejícím s bezpečností, nebo jiná opatření snižující riziko, která jsou určena pro zajištění nebo udržení bezpečného stavu řízeného zařízení s ohledem na určitou nebezpečnou událost. V železničním průmyslu standard [6] definuje *bezpečnostní funkci* jako funkci jejíž jediný účel je zajistit bezpečnost.

Bezpečnost je ve standardech [5] definována jako absence nepřijatelného rizika (podrobnosti viz kapitola 3).

Funkční bezpečnost je ve standardech [8] definována jako část celkové bezpečnosti týkající se řízeného zařízení a systému řízení řízeného zařízení, které závisí na správném fungování systémů E/E/EP souvisejících s bezpečností a na jiných opatřeních pro snížení rizika. V železničním průmyslu standard [6] definuje *funkční bezpečnost* jako část celkové bezpečnosti, která závisí na funkčních a fyzických jednotkách, které fungují správně v reakci na jejich vstupy.

Z uvedeného je zřejmé, že funkční bezpečnost je „pouze" částí celkové bezpečnosti. Zjednodušeně lze tvrdit, že bezpečnost (celková) se zabývá „všemi" riziky (ochranou proti všem nebezpečím) a funkční bezpečnost se zabývá riziky souvisejícími s nesprávnou funkcí (ochranou proti nebezpečím způsobeným nesprávnou funkcí).

Pro potřeby popisu vlastností systémů z hlediska funkční bezpečnosti byl stanoven pojem *integrita bezpečnosti*, která je definována ve standardech [8] jako pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu. V železničním průmyslu standard [6] definuje *integritu bezpečnosti* jako schopnost systému souvisícího s bezpečností dosáhnout požadovaných bezpečnostních funkcí za všech uvedených podmínek v rámci daného provozního prostředí a v rámci stanovené doby trvání.

Integrita bezpečnosti se kvantifikuje s využitím *úrovně integrity bezpečnosti* (safety integrity level – SIL), která je definována ve standardech [8] jako diskrétní úroveň (jedna ze čtyř možných) odpovídající rozsahu hodnot integrity bezpečnosti, kde úroveň integrity bezpečnosti 4 má nejvyšší úroveň integrity bezpečnosti a úroveň 1 nejnižší. V železničním průmyslu standard [6] definuje *úroveň integrity bezpečnosti* jako jedno z čísel z definovaných diskrétních úrovní pro stanovení požadavků na integritu bezpečnosti pro funkce se vztahem k bezpečnosti, které mají být přiděleny systémům se vztahem k bezpečnosti.

Základní standardy funkční bezpečnosti pracují se SIL1 až SIL4. Oborově specifické standardy pracují i s jinými úrovněmi integrity bezpečnosti (SIL0, BI) nebo jinak označovanými (ASIL, SAS atd.).

Je třeba zdůraznit, že z technického hlediska úroveň integrity bezpečnosti (SIL) není vlastností systému. SIL je třeba vztahovat k funkcím (bezpečnostním funkcím), nikoliv k systémům jako celkům. Pokud je systém (technicky nesprávně) označen za SIL*n* systém, znamená to, že systém je schopen podporovat (některé) bezpečnostní funkce s úrovní integrity až *n*.

Již bylo řečeno, že hlavním cílem zajišťování funkční bezpečnosti je redukce rizika. Z tohoto pohledu lze zjednodušeně tvrdit, že dosažení určité SIL dokladuje snížení rizika řádově následovně:

- SIL1: redukce rizika 10×;
- SIL2: redukce rizika 100×;
- SIL3: redukce rizika 1000×;
- SIL4: redukce rizika 10000×.

Uvedená škála je orientační, určená pro ilustraci situace.

4.2 Porucha, selhání

Porucha, či selhání, je událost charakteristická tím, že po ní daný systém přestává plnit požadované funkce, či je začíná plnit jen v omezeném rozsahu. Uvedené samozřejmě platí i pro bezpečnostní funkce. V oblasti funkční bezpečnosti je poruchám věnována značná pozornost.

Porucha (selhání), je definována jako ztráta schopnosti fungovat tak, jak je požadováno [4]. Ve standardech funkční bezpečnosti [8] je *porucha* definována jako ukončení schopnosti funkční

jednotky plnit požadovanou funkci nebo provoz funkční jednotky jiným než požadovaným způsobem.

Poruchy (selhání) se mohou vyskytovat u hardware i software. U software je, pro přesnější popis, častěji používán pojem *selhání software*, které je definováno jako selhání, které je projevem neaktivní softwarové vady [4]. Selhání softwaru se může opakovat, dokud není softwarová vada, která je za něj odpovědná, odstraněna. *Softwarová vada* je stav softwarového objektu, který mu zabraňuje, aby fungoval tak, jak je požadováno [4]. Softwarové vady jsou vady způsobené specifikací, vady způsobené návrhem, vady zanesené kompilátorem nebo vady zanesené během údržby softwaru. Softwarová vada může být neaktivní, dokud nebude aktivována specifickým spouštěčem (např. vnitřním stavem systému, zpracovávanými daty, zásahem obsluhy, podmínkami prostředí).

V oblasti funkční bezpečnosti jsou poruchy rozdělovány na náhodné a systematické. Přičemž náhodné poruchy se mohou vyskytovat jen u hardware (nikoliv u software). Ve standardech [8] je proto definován pojem *náhodná hardwarová porucha*, tj. náhodně se objevující porucha, která je způsobena jednou nebo několika možnými degradacemi mechanismu hardwaru. Četnost náhodných poruch lze „předvídat“ a jejich výskyt lze statisticky kvantifikovat. K tomu lze využít vhodné metody z oblasti spolehlivosti. Zjednodušeně lze tvrdit, že náhodné hardwarové poruchy jsou „důsledkem“ bezporuchovosti hardware.

Systematická porucha je ve standardech [8] definována jako porucha, kterou jednoznačně způsobila určitá příčina a kterou je možné odstranit jen změnou návrhu (konstrukce) nebo výrobního procesu, provozních postupů, dokumentace nebo jiných souvisejících činitelů. Systematické poruchy nelze statisticky kvantifikovat. Systematické poruchy se mohou vyskytovat u hardware i software a jsou způsobeny lidskými chybami během životního cyklu hardware nebo software.

Rozdělení na náhodné a systematické poruchy je důležité, protože k ošetření rizik souvisejících s náhodnými nebo systematickými poruchami se používají odlišné metody a postupy.

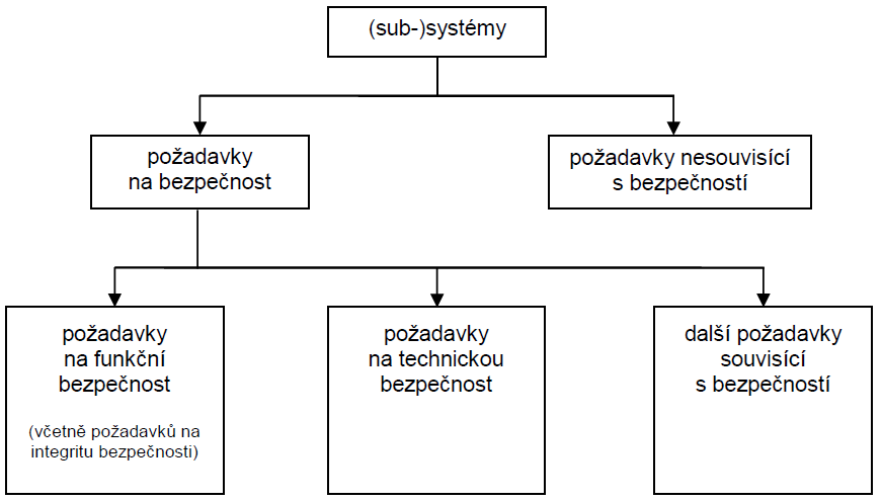
5 Požadavky a standardy v oblasti funkční bezpečnosti

5.1 Požadavky na funkční bezpečnost

Z hlediska bezpečnosti lze požadavky kladené na systémy rozdělit na požadavky související s bezpečností a nesouvisející s bezpečností. Požadavky na bezpečnost lze dále rozdělit na požadavky na funkční bezpečnost, na technickou bezpečnost, na kontextuální bezpečnost (další požadavky). Uvedené rozdělení je znázorněno na Obr. 3.

Požadavky na technickou bezpečnost jsou spojeny s technickým návrhem a implementací systému. Vztahují se k nebezpečím (potenciálním zdrojům újmy) jako např. nebezpečí požáru, přítomnost vysokého napětí, přítomnost škodlivých látek apod.

Kontextuální (další) požadavky na bezpečnost se vztahují k požadavkům na provoz a údržbu. Tyto požadavky mají zajistit provozní bezpečnost a bezpečnost při údržbě. Zahrnují např. požadavky na dokumentaci, školení, personál apod.



Obr. 3: Požadavky na bezpečnost systémů [6]

Požadavky na bezpečnost systémů (technickou a kontextuální) jsou v jednotlivých průmyslových odvětvích stanoveny v legislativních dokumentech. Ty se mohou, a často také odkazují na standardy. Požadavky na funkční bezpečnost systémů jsou stanoveny ve standardech funkční bezpečnosti platných pro dané průmyslové odvětví.

5.2 Standardy funkční bezpečnosti

Základním standardem pro oblast funkční bezpečnosti je standard:

- IEC 61508-x:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.

Standard má 7 částí. Poprvé byl vydán v letech 1998 až 2000 a v současné době je platná druhá revize z roku 2010.

V ČR byl standard vydán jako:

- ČSN EN 61508-x. Ed.2 (2011) Funkční bezpečnost elektrických/ elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1 až 7.

IEC 61508 je generický standard platný pro E/E/PE systémy související s bezpečností napříč průmyslovými odvětvími. Nicméně pro některá průmyslová odvětví byly vytvořeny oborově specifické standardy funkční bezpečnosti, které více, či méně vychází ze základního standardu IEC 61508. Příklady takových standardů jsou:

- ISO 26262-x:2018: Road vehicles – Functional safety.
- IEC 61511-x:2016: Functional safety – Safety instrumented systems for the process industry sector.
- IEC 62061:2005: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.
- IEC 61513:2011: Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.
- ISO 13849-x:2015: Safety of machinery – Safety-related parts of control systems.
- EN 50128:2011: Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.
- EN 50129:2018: Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling.

Pokud pro dané průmyslové odvětví (resp. typ systému) existuje oborově specifický standard, je nanejvýš vhodné (nikoliv povinné) použít jej namísto generického standardu IEC 61508.

6 Zajišťování funkční bezpečnosti

Zajišťování funkční bezpečnosti systému musí probíhat v souladu se standardy funkční bezpečnosti. Je třeba mu věnovat pozornost systematicky a ve všech etapách životního cyklu systému. Činnosti spojené se zajišťováním funkční bezpečnosti systému musí být přiměřeně organizované a plánované.

Zajišťování funkční bezpečnosti ve vztahu k úrovni integrity bezpečnosti (SIL) lze rozdělit na tři základní kroky:

- Určení, jaké SIL má být dosaženo – jakou SIL požadujeme (specifikace, alokace).
- Realizace návrhu a vývoje (a také definování podrobností nasazení, provozu a údržby) tak, aby byla dosažena požadovaná SIL.
- Hodnocení, jaké SIL bylo dosaženo (dokazování).

6.1 Určení požadované úrovně integrity bezpečnosti (SIL)

Určení SIL znamená stanovení, jaké SIL má být dosaženo. Tj. jakou SIL požadujeme. Proces určení se nazývá buď specifikace (pokud je požadavek na funkce systému nově specifikován) nebo alokace (pokud je požadavek na funkce systému rozdělován z nadřazeného požadavku).

Požadavky na funkční bezpečnost (resp. na SIL) specifikuje:

- Odběratel (provozovatel) – u systému na zakázku. Předpokládá se, že pouze zákazník ví, jaká je pro něj akceptovatelná úroveň rizika, a tudíž jakou SIL má požadovat.
- Dodavatel (výrobce) – u systému, který není na zakázku (je určen pro trh). Dodavatel musí mít představu o akceptovatelné úrovni rizika a o tom, jaké SIL má být dosaženo.

Základem určení požadované SIL je znalost tolerovatelného (akceptovatelného) rizika. Akceptovatelnou úroveň rizika lze stanovit s využitím přístupů jako jsou ALARP, MEM apod. Výchozím bodem je posuzování rizika a v případě, kdy z hodnocení rizika vyplyne, že dané riziko pro nás není akceptovatelné, přistupuje se k určení požadované úrovně integrity bezpečnosti (SIL).

Pro určování požadované SIL se používají následující metody:

- kvalitativní (diagramy rizika a rozhodovací diagramy);
- semi-kvantitativní (semi-kvantitativní výpočtové vztahy, kombinace diagramů a výpočtových vztahů);
- kvantitativní (výpočtové vztahy).

Podrobné informace o uvedených metodách lze nalézt ve standardech funkční bezpečnosti.

6.2 Realizace návrhu a vývoje pro dosažení SIL

Realizace návrhu a vývoje (a také definování podrobností nasazení, provozu a údržby) tak, aby byla dosažena požadovaná úroveň integrity bezpečnosti (SIL), je nejnáročnějším krokem zajišťování funkční bezpečnosti.

Při návrhu a vývoji je třeba splnit požadavky (související s požadovanou SIL) definované v příslušných standardech funkční bezpečnosti. Požadavky na funkční bezpečnost lze rozdělit do dvou skupin:

- požadavky na integritu vůči systematickým poruchám (hardware a software);
- požadavky na integritu vůči náhodným poruchám (hardware).

Požadavky na integritu vůči systematickým poruchám mají kvalitativní formu. Cílem splnění kvalitativních požadavků je minimalizace výskytu systematických poruch hardware a software. Tohoto cíle se dosahuje aplikováním různých postupů a opatření v závislosti na tolerovatelném riziku (resp. požadované SIL).

Požadavky na integritu vůči náhodným poruchám mají kvantitativní formu. Cílem splnění kvantitativních požadavků je „omezení" výskytu náhodných poruch hardware. Naplnění tohoto cíle zahrnuje provedení předpovědi pravděpodobnosti poruch hardware a porovnání výsledků s požadavkem na tolerovatelné riziko. Pokud není požadavek splněn, jsou nezbytné úpravy designu (případně redefinování podrobností nasazení, provozu a údržby), dokud není požadavek splněn.

Konkrétní kvalitativní a kvantitativní požadavky pro jednotlivé SIL jsou podrobně a obsáhle definovány ve standardech funkční bezpečnosti.

6.3 Hodnocení dosažené SIL

Posledním krokem je hodnocení, jaké SIL bylo dosaženo. Jde o proces dokazování (prokazování), že požadavky související danou úrovni integrity bezpečnosti (SIL) byly a jsou splněny. Konkrétně se hodnotí (dokazuje) splnění kvalitativních požadavků a kvantitativních požadavků. V kontextu standardu IEC 61508 se jedná o odhad funkční bezpečnosti.

Podstatou prokázání splnění kvalitativních požadavků na funkční bezpečnost (resp. SIL) je prokázat dodržení organizačního uspořádání, postupů, metod, opatření apod.

Podstatou prokázání splnění kvantitativních požadavků je prokázat splnění kvantitativních požadavků definovaných pro danou SIL. Při tom se používají nejrůznější analytické metody z oblasti spolehlivosti a bezpečnosti (např. FMEA a FTA).

Dosažení určité úrovně integrity bezpečnosti (SIL) „systému" se dokazuje:
- posouzením nezávislou osobou (nezávislým posuzovatelem bezpečnosti);
- nebo certifikací SIL „systému".

7 Metody analýzy v oblasti funkční bezpečnosti

V dalších článcích v tomto sborníku jsou zmíněny dvě metody často používané v oblasti funkční bezpečnosti. Jedná se o metody FMEA a FTA. Následující podkapitoly mají za cíl nasměrovat čtenáře, kteří nejsou podrobně obeznámeni s těmito metodami.

7.1 FMEA

Analýza způsobů a důsledků poruch, označovaná stručně jako FMEA (Failure Modes and Effects Analysis) je strukturovaná, kvalitativní analýza sloužící k identifikaci způsobů poruch systémů a procesů, jejich příčin a důsledků. Analýza způsobů, důsledků a kritičnosti poruch, označovaná stručně jako FMECA (Failure Modes, Effects and Criticality Analysis) je logickým rozšířením metody FMEA spočívajícím v tom, že jsou do ní zahrnuty prostředky pro určení kritičnosti způsobů poruch. Metoda FMECA nepředstavuje samostatný způsob analýzy systémů a procesů, ale je pouze logickým rozšířením metody FMEA [1].

FME(C)A (dále jen FMEA) je metodou induktivní, která umožňuje provádět kvalitativní a kvantitativní analýzu bezpečnosti a spolehlivosti systému od nižší k vyšší úrovni členění systému a zkoumá, jakým způsobem mohou systémy na nižší úrovni selhat a jaký důsledek mohou mít tato selhání pro vyšší úrovně systému [1].

V oblasti funkční bezpečnosti se používá tzv. konstrukční FMEA (design FMEA). Někdy také nazývána FMEA návrhu, která se používá pro potřeby analýzy systému, respektive technického návrhu systému.

Provedení FMEA představuje logicky navazující kroky, které lze rozdělit do tří částí:

- přípravná část analýzy;
- vlastní FMEA jednotlivých prvků systému;
- vyhodnocení analýzy.

Při vlastní FMEA se, u každého prvku systému (na zvolené nejnižší úrovni) realizují zejména tyto základní kroky [1]:

- identifikace způsobů poruch prvku;
- identifikace důsledků poruch;
- identifikace příčin poruch;
- identifikace metod detekce poruch a existujících opatření.

Při provádění FMECA se navíc realizují následující kroky [1]:

- stanovení závažnosti konečných důsledků poruch;
- odhad pravděpodobnosti výskytu;
- určení kritičnosti způsobů poruch.

Tento základní rozsah analýzy může být podle potřeby rozšířen o další kroky, v rámci nichž se budou účelově identifikovat a analyzovat další informace, potřebné pro posouzení spolehlivosti či bezpečnosti systému [1].

Jednotlivé kroky vlastní analýzy je nezbytné zaznamenávat do uspořádaných pracovních formulářů, případně s využitím specializovaného software.

Vozidlo: Systém:			**FMECA** **Analýza způsobů, důsledků a kritičnosti poruch**						Vypracoval: Datum:	
Řád.	Prvek	Popis funkce	Způsob poruchy	Důsledek pro systém	Důsledek na vozidlo	Způsob detekce	Intenzita poruch	Závažnost důsledků	Kritičnost poruchy	Pozn.

Obr. 4: Příklad hlavičky formuláře FMEA [1]

Podrobné informace o jednotlivých krocích realizace analýzy lze nalézt ve standardech:

- ČSN EN 60812 ed. 2 Analýza způsobů a důsledků poruch (FMEA a FMECA);
- MIL-STD-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis;
- SAE J1739 Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA).

V českém jazyce jsou kvalitním informačním zdrojem vydané sborníky ze seminářů Odborného centra Spolehlivost zaměřené, mimo jiné, na metodu FME(C)A, např.:

- 5. seminář: Úloha a aplikační možnosti metody FMEA při zabezpečování spolehlivosti;
- 28. seminář: Spolehlivost tradiční i netradiční;
- 35. seminář: Analýzy spolehlivosti a bezpečnosti v praxi;
- 60. seminář: Prediktivní analýzy spolehlivosti a možnosti jejich využití.

7.2 FTA

Metoda analýzy stromu poruchových stavů, označovaná stručně jako FTA (Fault Tree Analysis), se dle [10] zabývá identifikací a analýzou podmínek a faktorů, které způsobují nebo mohou potenciálně způsobit výskyt nebo přispívat k výskytu specifikované vrcholové události.

Metoda analýzy stromu poruchových stavů (FTA) je deduktivní metodou a svým charakterem patří mezi speciální orientované grafy. Strom poruchových stavů má podobu logického diagramu, který znázorňuje logické vztahy mezi potenciální vrcholovou událostí (jevem) a mezi příčinami vzniku tohoto jevu. Příčiny mohou být v provozních podmínkách, v běžných očekávaných poruchách prvků systému, v lidských chybách, v odchylkách (chybách) provozních parametrů prvků apod. Správně zkonstruovaný strom poruchových stavů reprezentuje (ilustruje) všechny rozumné kombinace „nežádoucích" událostí (jevů), které mohou vést ke vzniku specifikované vrcholové události [1].

Při aplikaci metody stromu poruchových stavů lze použít dva základní přístupy – kvalitativní a kvantitativní [10]. Při kvalitativním přístupu se pravděpodobnost (či jiný ukazatel) události a faktorů, které k ní přispívají (základních událostí), nebo jejich četnost výskytu nesleduje. Tento přístup je znám jako kvalitativní nebo tradiční FTA. Druhý přístup je kvantitativní, při kterém se pomocí FTA modeluje celý systém a základní události mají v modelu nějakou pravděpodobnost výskytu (či jiný ukazatel) stanovenou pomocí jiných metod než FTA. V tomto případě je konečným výsledkem pravděpodobnost výskytu vrcholové události během definovaného časového intervalu [1].

Vlastní realizace analýzy představuje provedení jisté logické posloupnosti kroků, kterou lze rozdělit do následujících základních částí [1]:

- přípravná část;
- definování vrcholové události;
- tvorba stromu poruchových stavů;
- kvalitativní analýza stromu poruchových stavů;
- kvantitativní analýza stromu poruchových stavů;
- vyhodnocení analýzy.

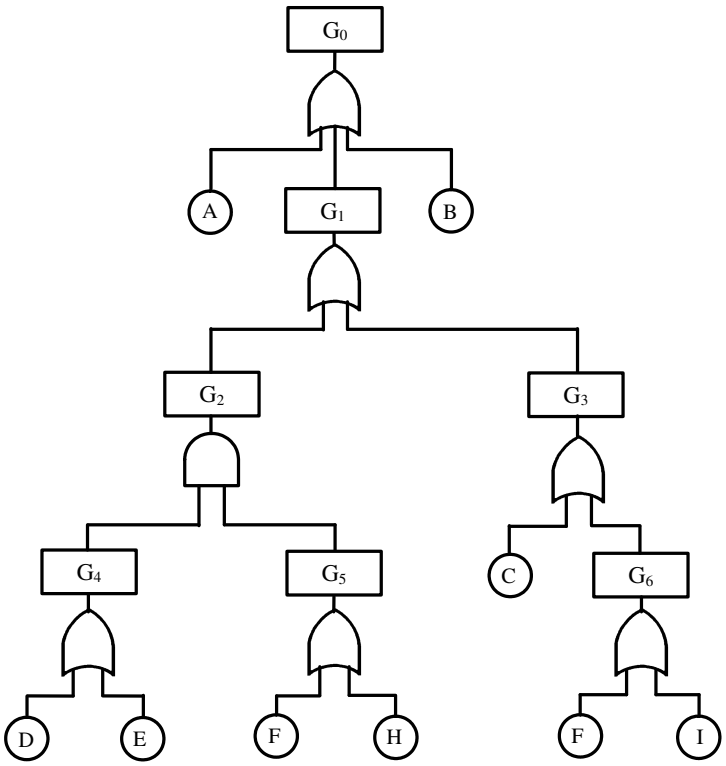
Příklad vytvořeného stromu poruchových stavů je uveden na Obr. 5.

Podrobnosti o jednotlivých krocích realizace analýzy lze nalézt ve standardech:

- ČSN EN 61025 Analýza stromu poruchových stavů (FTA);
- NUREG-0492 Fault Tree Handbook;
- NASA Fault Tree Handbook with Aerospace Application.

V českém jazyce jsou kvalitním informačním zdrojem vydané sborníky ze seminářů Odborného centra Spolehlivost zaměřené, mimo jiné, na metodu FTA, např.:

- 35. seminář: Analýzy spolehlivosti a bezpečnosti v praxi;
- 60. seminář: Prediktivní analýzy spolehlivosti a možnosti jejich využití.



Obr. 5: Příklad stromu poruchových stavů [1]

8 Závěr

Článek je třeba chápat jako základní úvod do problematiky funkční bezpečnosti. Článek se snažil informace podat co nejstručněji. Avšak, vzhledem ke komplexnosti problematiky funkční bezpečnosti, bylo třeba některé části vysvětlit podrobněji.

V článku bylo charakterizováno nebezpečí a riziko, byly popsány základní pojmy z oblasti funkční bezpečnosti a představeny základní standardy obsahující požadavky na funkční bezpečnost. Dále byly nastíněny obecné principy zajišťování funkční bezpečnosti v různých průmyslových odvětvích. Na závěr článku byly stručně představeny dvě často používané metody z oblasti funkční bezpečnosti (FMEA a FTA).

Celý článek, a zejména kapitola číslo 6 (Zajišťování funkční bezpečnosti), stručně vyjadřuje pohled autora na problematiku funkční bezpečnosti. Autor nepopírá, že jeho pohled je výrazně ovlivněn praktickými zkušenostmi z oblasti železničního průmyslu.

Použité zdroje

[1] SMITH, David J., and Kenneth G. L. SIMPSON. *Functional Safety: A Straightforward Guide to Applying IEC 61508 and Related Standards*. 2nd ed. Oxford: Elsevier, 2004. ISBN 978-0750662697.

[2] VINTR, Zdeněk, David VALIŠ a Michal VINTR. *Základy spolehlivosti technických systémů.* Brno: Univerzita obrany v Brně, 2020. ISBN 978-80-7582-303-8.

[3] HUDEC, Marek. Introduction to ISO 26262 and its limitations with regards to ADAS. In *Aplikované techniky spolehlivosti v automobilovém inženýrství.* Brno: Univerzita Obrany v Brně, 2019, s. 19–29. ISBN 978-80-7582-102-7.

[4] ČSN IEC 60050-192. *Mezinárodní elektrotechnický slovník – Část 192: Spolehlivost.* Praha: ÚNMZ, 2016.

[5] ČSN IEC 60050-903. *Mezinárodní elektrotechnický slovník – Část 903: Posuzování rizik.* Praha: ÚNMZ, 2014.

[6] ČSN EN 50126-1 ed. 2. *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 1: Generický proces RAMS.* Praha: ÚNMZ, 2019

[7] ČSN EN 50126-2. *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) – Část 2: Systémový přístup k bezpečnosti.* Praha: ÚNMZ, 2019.

[8] ČSN EN 61508-x ed. 2. Funkční bezpečnost elektrických/ elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1 až 7. Praha: ÚNMZ, 2011.

[9] ČSN EN IEC 60812 ed. 2. *Analýza způsobů a důsledků poruch (FMEA a FMECA)*. Praha: ÚNMZ, 2019.

[10] ČSN EN 61025. *Analýza stromu poruchových stavů (FTA).* Praha: ČNI, 2007.

[11] TNI 01 0350 *Management rizik – Slovník* (Pokyn 73). Praha: ÚNMZ, 2010.

Functional safety on the vehicle level in accordance with ISO 26262

Ing. Marek Hudec, Carlos Sierra

marek.hudec@porsche-engineering.cz

1. Introduction

The functional safety discipline in the automotive domain deserves a domain-specific treatment. This led the leading experts in the industry to define the automotive-specific functional safety standard, nowadays known as ISO 26262:2018. The principles originate from the general standard IEC 61508:2010, still the automotive domain is specific in its mass production as well as risk acceptance and role of the driver. The driver presence and other factors lead the experts to consider the aspect of controllability and today, even widely used, it is the most difficult factor of the risk evaluation since it should be based on a very good understanding of the targeted drivers' behavior. The original intention to incorporate the controllability factor into the risk evaluation is questionable in the context of autonomous driving systems, especially if the driver is not a human driver, but it is "replaced" by an electric/electronic function. A brief overview of the automotive functional safety on the vehicle level in terms of ISO 26262-2 and ISO 26262-3 is provided as well as its relation to the conventional failure analysis methods like FMEA and FTA. Furthermore, the above-mentioned influence of the development of the autonomous driving systems onto safety is commented including the main challenges.

2. ISO 26262 as the main functional safety standard for automotive

2.1 Origin of ISO 26262 and its relation to its parent standard IEC 61508

Prior to the publishing of ISO 26262 in 2011, automotive industry had difficulties applying the parent standard IEC 61508. The parent standard (see Figure 1), which was introduced in 1998 (first draft in 1995 as IEC 1508), is not domain-specific and thus also does not reflect specific approaches of the automotive industry. IEC 61508 states, that in case there is a domain-specific standard for functional safety, it shall be followed as a replacement of IEC 61508. Prior to 2011, unfortunately, there was no such domain-specific standard for the automotive industry and thus, IEC 61508 had to be applied. It posed certain difficulties, starting with the general framework of deriving safety integrity levels (SIL), as IEC 61508 claims not to be domain-specific, but its derivation of SIL is much more suitable for the needs of process industry instead of mass production of road vehicles. Therefore, the publication of ISO 26262 had on one hand a huge impact (in terms of additional effort and workforce) on the automotive industry, placing new requirements on the development of automotive E/E systems, but on the other hand the new domain-specific standard was a relief for every functional safety engineer bringing not only automotive-tailored approaches, but also numerous practical examples and application guidelines (most importantly the Part 10 of ISO 26262: Guidelines on ISO 26262 [2], [3]).

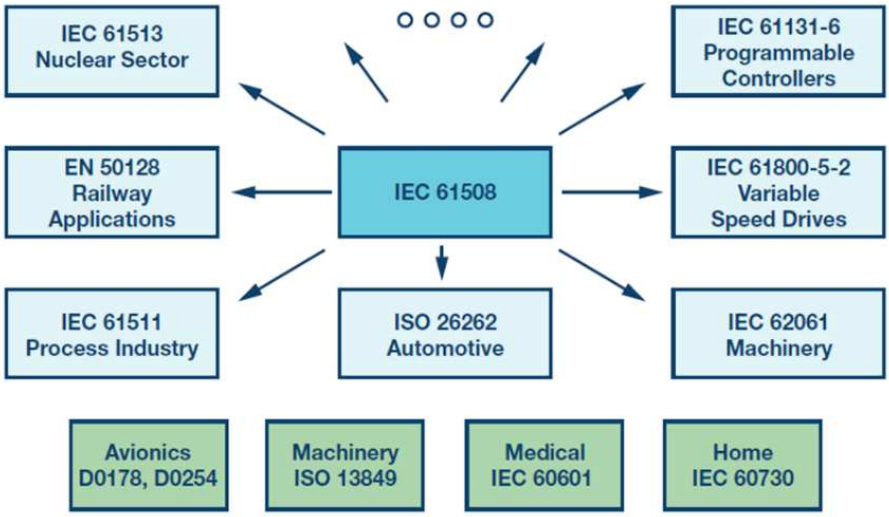


Figure 1: Relation of IEC 61508 to domain-specific standards for functional safety [5].

2.2 Automotive specific approaches in ISO 26262

As already mentioned, the application of IEC 61508 in the automotive industry is not satisfactory due to various automotive-specific approaches. Therefore, in this clause, three examples of such approaches will be given including its resolution in the sense of ISO 26262.

The mostly appreciated automotive-tailored approach prescribed in ISO 26262 is the consideration of vehicle controllability including its validation in the vehicle. The introduction of controllability during safety goal (top-level safety requirements) derivation in the hazard analysis and risk assessment (HARA) allows functional safety engineers to directly influence the resulting safety integrity level (called ASIL in the sense of ISO 26262 = Automotive SIL) by consideration of the controllability of a potential hazardous situation coming up from a malfunction of a particular E/E system. More details on this approach will be given in Chapter 3.

Another example of an automotive specific approach is mapping of the safety activities and work products as defined in ISO 26262 onto the V-model, due to the vast usage of this development model in the automotive industry.

As a third example of automotive specific considerations in ISO 26262 in comparison with its parent standard IEC 61508 can be a set of rules focused on distributed developments, especially on the customer-supplier interface. Since in the automotive industry it is very common to have very long supplier chains (sub-supplier, sub-sub-supplier, etc.), the standard comprises a number of rules for the distribution of safety activities and work products defined in ISO 26262 as well as other rules, e. g. with regards to safety assessments or safety audits.

3. Overview of the safety lifecycle as required by ISO 26262

In this chapter, a very brief overview of ISO 26262, its definition of the safety lifecycle consisting of a broad range of safety activities and work products, will be given.

3.1 Safety lifecycle of ISO 26262 and timeline definition

As mentioned above, ISO 26262 is heavily oriented on the V-model (see Figure 2). Based on the V-model, the standard defines safety activities and work products that have mutual relations in the sense that one work product serves as a pre-requisite for another work product (for example to create a functional safety concept, derived safety goals must be existing). Although ISO 26262 does not prescribe any milestones or deadlines for individual work products and/or activities (apart from stating that functional safety of a specific function has to be achieved prior to its release to public roads), it is clear from its context that the safety lifecycle of a product (e. g. vehicle stability system) necessarily have to start as soon as the product is defined in its very early stage. Should the safety lifecycle start very late in the project, there is a huge risk that necessary safety requirements cannot be respected with regards to the system architecture or cannot simply be fulfilled due to the late stage of the project. Therefore, to prevent costly changes in the late development stages (due to the advancing product maturity), it is highly recommended to carry out the safety activities as soon as the necessary inputs are available.

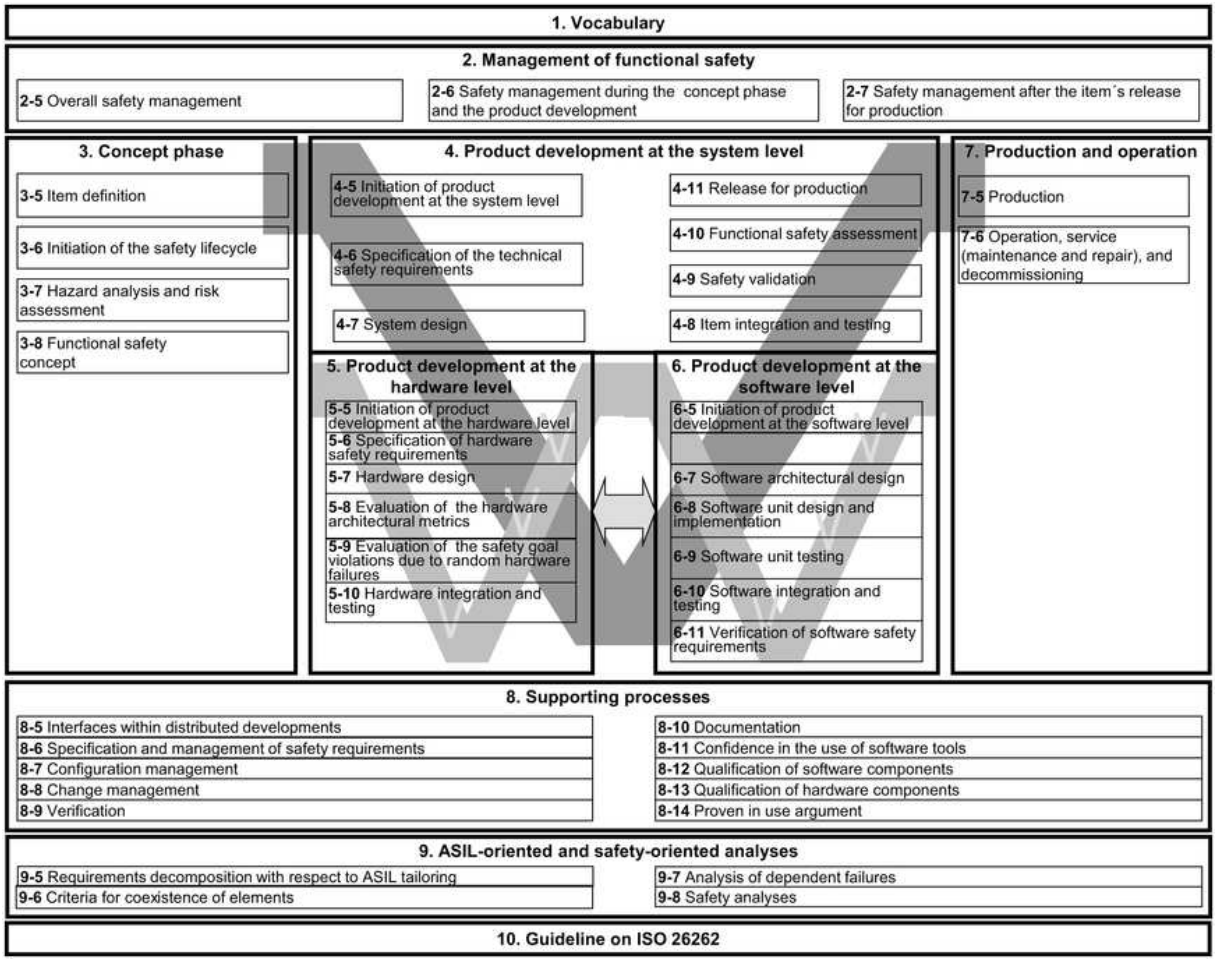


Figure 2: Structure of ISO 26262:2011 [2].

The effort needed for performing required safety activities is proportional to the ASIL of the corresponding safety goal. For instance, ASIL D safety goal requires the highest effort, whereas ASIL A requires elevated effort, but still lower n comparison with ASIL C or D. But regardless on the ASIL derived, for all ASILs it is necessary, that the company development

has a certain quality level established, called QM (quality management) in the language of ISO 26262. It comes from the fact that functional safety represents an additional "set of rules" on top of the standard quality processes. Therefore, it is required to have established QM processes on place as a basis for safety-relevant (meaning ASIL A, B, C or D) developments (see Figure 3).

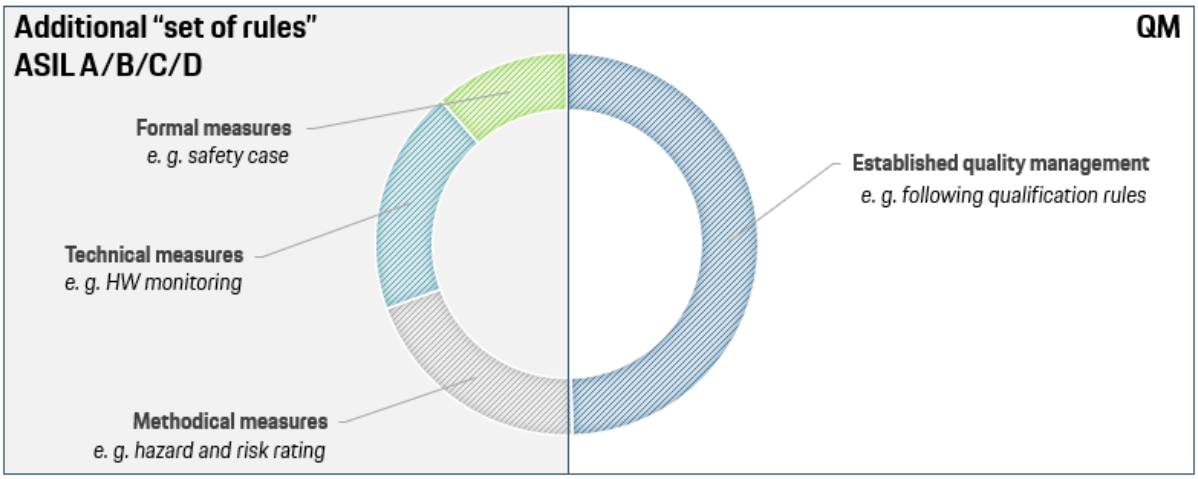


Figure 3: Means of risk reduction in the sense of ISO 26262 by considering additional "set of rules" during the development where effort to maintain these depends on the ASIL.

ISO 26262 contains methodical, formal, technical as well as process requirements (see Figure 3) which are grouped based on levels and parts of the V-model. Therefore, also the upcoming clauses in this chapter are based on these parts, covering the following topics: overall safety management, functional safety on the vehicle level, functional safety on the system level, functional safety on the component level, supporting processes.

3.2 Overall safety management as per ISO 26262-2

The part 2 of ISO 26262 describes general safety activities and work products that are required in every safety-relevant project, no matter on which level or how far in the supplier chain. It addresses safety culture of a company, responsibilities with regards to functional safety, project set-up, general planning and monitoring of safety activities as well as rules for technical (so-called verification) and independent (so-called confirmation) reviews of selected work products and rules for safety assessments and audits. It also addresses creation of a safety case which contains all information gathered during the safety lifecycle and thus provides evidence that the functional safety is achieved in the project in terms of ISO 26262. The requirements in the part 2 as well as in other parts of ISO 26262 are dependent on the safety goal with the highest ASIL, e. g. a safety assessment, checking achievement of functional safety by a complete independent party, must be performed only in case of ASIL C or D (for lower ASILs it is recommended, but not necessary). This scheme generates different effort in the development for different ASILs.

3.3 Functional safety on the vehicle level as per ISO 26262-3

The technical aspects of the functional safety start with the so-called item definition. The item definition describes (by the means of the functional description, user interface, rough vehicle architecture, interfaces to other items, performance, etc.) an item in scope of functional safety. An item can comprise of one or more functions on the vehicle level (operable and perceivable by its user) which might be distributed across several systems (sensing, controlling, or actuating). Examples of a function might be road lightning by beam lights, screen wiping by the car wipers, a cruise control function to assist the driver in terms of longitudinal vehicle control or a stability control function to assist the driver in terms of keeping the vehicle on the track.

The functions defined in the item definition are analyzed in the Hazard and Risk Analysis (HARA). For that purpose, all possible malfunctions of the functions defined are listed. For each of such malfunctions, all relevant vehicle operation situations are selected in which such malfunctions could cause a hazardous event. For each of these combinations of a malfunction with the relevant situation, an entry is created in the HARA. The corresponding situation is then rated with regards to its probability (parameter E – exposure). For probabilities, typically OEM catalogues of standard situations are used, where E parameters are already agreed on based on statistics and expert judgement. The entry is further rated with regards to its worst-case severity (parameter S) in case the hazard is not prevented by the affected traffic participants (so under the assumption that the driver, pedestrians and further affected parties do not take any actions). The third parameter is the controllability (parameter C), rating the traffic participant actions possibly preventing or reducing the severity of the hazardous event (e. g. driver can brake, pedestrian can run away). The controllability is the most difficult parameter to put rationale for as it is not simple to prove statistically. Typically, an expert judgement made by a team of experts is used on this place, to avoid subjective rating. In some cases, user surveys or studies are made to statistically support the rating. The entry in the HARA then results in a safety goal and the sum of all three parameters (E, C and S) results in an ASIL of the safety goal (see Figure 4).

		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	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 4: ASIL evaluation based on E, C and S parameters.

Based on the safety goals and further parameters such as safe state, acceptance criteria (tolerance) and fault tolerance time interval, derived in the HARA, the Functional Safety Concept (FSC) is created. The FSC takes the vehicle and/or system architecture into account and details the safety goals down to the level of detail of individual systems. This is practically done by deriving functional safety requirements from safety goals and allocation of these

requirements to the systems mentioned. The requirements derived within the FSC aim to reduce risks by employing safety monitoring mechanisms and/or redundancies, prescribe system degradation and warning concept in case of detected failures and the failure handling. At this level, the FSC is detailed down to the level of systems, allowing further steps following ISO 26262-4 (most importantly the Technical Safety Concept).

The safety requirements need to consider any single-point E/E failure and – depending on the ASIL rating – also multi-point failures. To achieve completeness in terms of the coverage of all these failures by the safety requirements, verification activities are performed. Verification is a mean of achieving technical completeness and correctness and since it is a technical discipling, it involves technical experts. It involves multiple experts or a team of experts who review each other's statements. Since also the Failure Mode and Effect Analysis (FMEA) is done in a team of experts who systematically analyze system architectures to find causes and their effects, the FMEA is understood as a very important verification means for the functional safety concept, especially for the single-point failures. In case of higher ASIL ratings with dual-point or even multi-point failures being in focus, the FMEA is supported by the Fault Tree Analysis (FTA).

The derived safety goals as well as the functional safety requirements shall be validated on the right side of the V-model. For this purpose, e. g. fault injection tests are derived that validate if the behavior is sufficiently safe and thus controllable by the driver. The validation of safety goals is carried out in the vehicle.

3.4 Supporting processes and ASIL decomposition as per ISO 26262-8 and ISO 26262-9

ISO 26262, specifically its Part 8, also gives requirements onto development supporting processes, e. g. change management, configuration management, documentation management, re-use of components, tool qualification. These are however very similar or even referenced to other quality management standards.

Furthermore, ISO 26262 allows ASIL decomposition at any level of the development (vehicle, system, or component). For that purpose, independence between the decomposed systems must be shown. That way, an ASIL D requirement could be for instance decomposed to two ASIL B(D) requirements (in parentheses, the original ASIL prior to decomposition must be given), see Figure 5.

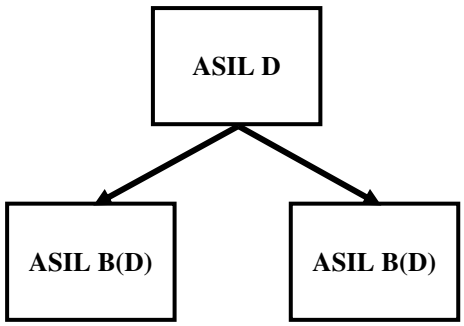


Figure 5: Example of an ASIL decomposition according to ISO 26262 Part 9.

4. The impact of autonomous driving onto system safety

4.1 Safety beyond ISO 26262

ISO 26262 satisfies safety objectives with regards to malfunctions of E/E systems and offers a very wide framework (or also "set of rules") in order to treat systematic as well as random failures with the goal of prevention of hazardous events ("accidents" in terms of road vehicles). However, the application of ISO 26262 to upcoming systems of high complexity under current development, comprising of various numbers of sensing, processing, and actuation elements, is not satisfactory. Firstly, other domains (such as mechanics, hydraulics, etc.) are not addressed in ISO 26262 – the standard states that safety requirements (no ASIL though) shall be derived for such domains in case these interface the E/E systems in scope of ISO 26262. Since most of the classical non-E/E domains were preceding E/E systems in the vehicle development (e. g. combustion engine without electronic control systems, hydraulic braking systems or mechanical chassis systems), assumption can be made that such systems are safe enough by applying state-of-the-art methods and domain-applicable standards for quality, reliability, and safety. However, sufficient safety of sensing systems in the way how they are designed, how they should be understood and relied on by the driver (e. g. role of driver assistance systems as E/E systems with the aim of supporting the driver) cannot be achieved by application of ISO 26262 only. The following aspects are typical for the nowadays and future electronic control systems of high complexity:

- Estimation of physical values instead of their measurement (some values even cannot be practically measured and need to be estimated based on models that take other physical values into account, e. g. road friction coefficient),
- estimation of the environment based on computer vision methods employing probabilistic approaches and machine learning,
- control algorithms intended to control a system of which the simplified model is used to define the control strategy in the algorithms implemented in the HW and SW.

The selection of the technology, the selection of the algorithm is therefore key to assuring safety of such control systems. We can never guarantee a 100 % functionally safe system (classical functional safety in accordance with ISO 26262), due to the nature of failure occurrence (true for both systematic and random HW failures). Similarly, we cannot guarantee a 100 % situational awareness of the autonomous driving systems (such safety objective is called safety of the intended functionality). For both, the classical functional safety as well as the safety of the intended functionality, we need to achieve reasonably low residual risks.

4.2 Controllability in the context of autonomous driving

Considering the classical functional safety domain, the autonomous driving has also a strong influence on this discipline. Due to the absence of the driver in the ego vehicle, the controllability factor relies on the traffic participants around the ego vehicle only. This typically results in less controllability ratings and therefore higher ASILs, since the human controllability and troubleshooting factor is removed. What might be controversial (however positive for the safety), is that the E/E function replacing the driver cannot be used as rationale in the controllability (the ISO 26262 in its current version does not include this influence). The E/E functions meant to replace humans in autonomous cars can – depending on the situation – perform better (in terms of failure rate) than humans, since humans are not failure free. However, assuming sufficient independency between the human replacement E/E function and

the function impaired by the failure, decomposition could be employed on the level of the safety concept. An example is shown in Figure 6. The decomposition could only be used in case both the decomposed paths fulfill the original requirement, i. e. prevent the partial brake loss from turning into an accident. This can be for example provided by the following technical measures:

- The E/E function replacing the driver can detect the partial loss of brake and compensate its effect on the stopping distance by increasing the autopilot ("driver") deceleration demand (e. g. 0,5 g instead of 0,2 g).
- The brake system can detect the partial loss of brake and compensate it by redirection of the driver deceleration demand to a second ("fallback") actuator.

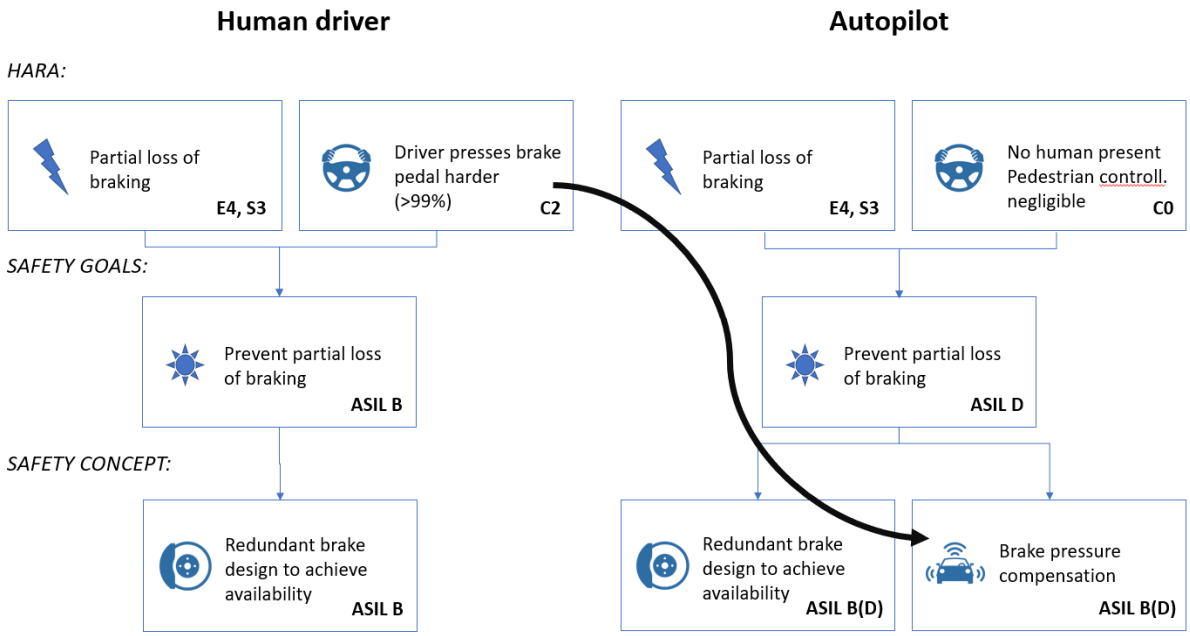


Figure 6: Controllability factor in autonomous driving systems.

4.3 Safe architecture in the context of autonomous driving

As mentioned in the previously, the lack of human driver in case of autonomous driving systems leads to higher ASIL ratings compared to the conventional systems with human drivers. Many essential functions in the conventional systems such as steering or braking are designed in the way, that there is a mechanical backup in case they fail (due to an E/E malfunction). The mechanical backup is part of the functional safety concepts of such functions. With autonomous driving systems, there is no human driver who could push on the brake pedal or steering wheel, which is a reason why the functional safety concepts of such systems cannot rely on any mechanical backup. Such systems must remain operational within the E/E domain and need to be designed in the way, that they are available. This means that the architecture of such system must continue operating in case of E/E malfunctions. Since the E/E malfunctions leading to a system non-availability due to their nature hardly reach target metrics defined in ISO 26262-5, the architecture needs to incorporate redundancy concepts with levels of degradation. All that at high speed, since losing control for several milliseconds can end up with a severe accident.

4.4 Safety of the intended functionality (SOTIF) standard ISO/PAS 21448

As you might have noticed in the example with the compensation of the brake loss as a requirement to the autonomous E/E function replacing the human driver, it would be irrelevant in case the autonomous E/E function does not correctly perceive the situation in which it should brake. It shall be designed in a way that it correctly understands its surroundings and deploys brakes whenever that is required in the respective driving situation. The target for this "correct understanding" is the failure rate of human drivers, i. e. the function shall miss less "braking evens" than an average human driver.

The SOTIF (Safety of the Intended Functionality) standard currently under development (currently in the DIS stage), addresses these topics. It mainly addresses the following safety issues in the design of automotive E/E systems interacting with environment (and thus also other domains different from E/E):

- Performance limitations (of sensing or actuating elements),
- Limitations of the human/machine interface (HMI),
- Limitations caused by decisions algorithms, e. g. machine learning algorithms,
- Limitations with regards to the user interaction, e. g. foreseeable misuse.

Although ISO/PAS 21448 references many methods of ISO 26262, it is very different to the functional safety standard. The main reason is the fact that in case of SW/HW development, systematic and random failures might occur, and the failure propagation might be complex, but it is still identifiable by the means of ISO 26262 (e. g. by the means of appropriate safety analyses such as FMEA or FTA), whereas in SOTIF many "dormant" hazards in the intended functionality are existing and are unknown by the time of its development. Therefore, the main goal of ISO/PAS 21448 is to identify such failures and reduce the number of the unknown ones, and of course reduce the number of known ones by design adjustments.

5. Conclusion

In this article, a very brief introduction to the functional safety according to ISO 26262 was given, especially with focus on its automotive specific approaches. Thanks to this automotive-specific standard, now even available in its 2nd edition as ISO 26262:2018, safety engineers have a clearly defined set of requirements that are to be applied on top of the established QM processes. However, based on a simple example it was shown that ISO 26262 has certain limitations, especially with regards to ADAS. In such systems, further approaches must be used in addition to ISO 26262, to reduce risks resulting not only from the E/E systems malfunctions, but also from its functionality insufficiencies. Such approaches are currently being developed and established in the automotive industry. The newly published standard ISO/PAS 21448 might serve as an example, addressing performance limitations in the intended functionality under the consideration of foreseeable misuse.

Sources

[1] ISO/PAS 21448:2019 *Road vehicles — Safety of the intended functionality.*

[2] ISO 26262:2011 Parts 1-10 *Road vehicles — Functional safety.*

[3] ISO 26262:2018 Parts 1-12 *Road vehicles — Functional safety.*

[4] IEC 61508:2010 Parts 1-7 *Functional safety of electrical/electronic/programmable electronic safety-related systems.*

[5] MEANY, T. *Functional Safety for Integrated Circuits*. USA: Analog Devices, Inc. (available online: https://www.analog.com/en/technical-articles/a54121-functional-safety-for-integrated-circuits.html)

Aplikace výpočetních postupů spolehlivosti HW dle standardů ISO 26262

doc. Ing. Jan Famfulík, Ph.D.

Ing. Michal Richtář, Ph.D.

Institut dopravy, Fakulta strojní, VŠB – Technická univerzita Ostrava,

jan.famfulik@vsb.cz

michal.richtar@vsb.cz

Abstrakt

Druhé vydání normy ISO 26262 v roce 2018 pro oblast funkční bezpečnosti v automobilovém průmyslu vyžaduje provést hodnocení HW s využitím cílové míry poruch P_{MHF} (Probabilistic Metric for random Hardware Failures). Norma velmi doporučuje využít k tomuto účelu analýzu stromu poruch, avšak neuvádí žádný konkrétní příklad výpočtu. V článku jsou proto popsány výpočetní postupy s odvozením a vysvětlením matematických vztahů pro různé typy architektur HW elektronických systémů. Uvedené vztahy uvažují vliv vícenásobných poruch a vliv self – testů, avšak jsou relativně jednoduché. To umožňuje jejich využití i v raných fázích vývoje HW, kdy se dají očekávat časté změny návrhu. Článek s připojenou case study je tak určen nejen pro vědce, ale především pro vývojáře elektronických systémů kritických z hlediska bezpečnosti v oblasti v automobilového průmyslu.

Klíčová slova: funkční bezpečnost automobilu; ISO 26262; P_{MHF}; analýza stromu poruch, FTA, ASIL

1 Úvod

Podobně jako v jiných oblastech průmyslu podíl elektronických systémů na konstrukci automobilů neustále roste. S tím úzce souvisí vznik a požadavky na zavádění oborových norem v oblasti funkční bezpečnosti, které vychází z principů uvedených v základní normě pro funkční bezpečnost EN 61508. V oblasti automobilového průmyslu jde o již zavedenou normu ISO 26262:2018 pro vozidla do hmotnosti 3.5 t, kde jedním z cílů této normy je upravení standardů pro hodnocení dosažené úrovně Automotive Safety and Integrity Level (ASIL).

Standardním požadavkem při validaci HW posuzovaného systému dle ISO 26262 je provedení kvantitativní analýzy s cílem prokázat splnění konkrétních číselných hodnot v závislosti na požadované úrovni ASIL ve dvou oblastech. První oblast se týká diagnostického pokrytí, tedy schopnosti dostatečně robustně a včas diagnostikovat nebezpečné poruchové stavy systému. Postupy pro oblast diagnostického pokrytí jsou v ISO 26262 dobře popsány a doplněny ukázkovým příkladem a usnadňují tak orientaci vývojářům při práci. Proto v článku bude tato problematika zmíněna jen v rozsahu nutném pro pochopení dalších textů.

Druhá oblast se principiálně týká dosažené spolehlivosti použitého HW řešení. Norma ISO 26262 však nijak nespecifikuje výpočetní postupy nutné k prokázání pravděpodobnosti náhodných poruch HW, což může vést k potížím. Použití různých výpočetních postupů může vést k vzájemně neporovnatelným hodnocením dosažené úrovně ASIL. Např. v [1] je pro řídící systém brzdy kalkulována maximální pravděpodobnost poruchy systému, kdežto v [2] výpočet pracuje se střední hodnotou pravděpodobnosti poruchy. Důsledkem je potlačení jednoho z důvodů zavedení ISO 26262, tj. možnosti vzájemného porovnání dosažené úrovně ASIL.

Výpočetní metody popsané v tomto příspěvku jsou založeny na aplikaci kvantitativní FTA analýzy [3]. V oblasti funkční bezpečnosti je metoda FTA rozpracována dle standardů EN 61508 v [4], pro oblast automotive je zmíněna v [Mader 5]. Použití FTA analýzy vede k relativně jednoduchým výpočetním vztahům a zjednodušuje tak postupy nutné k provedení kvalitativní analýzy posuzovaného systému. Jednoduchost výpočtu je žádoucí zejména v počátečních fázích vývoje, kdy se dají očekávat časté změny v designu HW a následně i změny v konfiguraci výpočtu.

2 Dílčí požadavky normy ISO 26262

Cílové požadavky na provedení kvalitativní analýzy HW jsou popsány [6]. Prvním cílem kvantitativní analýzy je prokázat v závislosti na požadované úrovni ASIL dostatečně vysoké diagnostické pokrytí poruch. Výpočet diagnostického pokrytí vychází z normou popsané kategorizace intenzit poruch tvořících prvků, jak ukazují vztahy (1), (2) převzaté z normy [6].

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S \tag{1}$$

$$\lambda_{MPF} = \lambda_{MPF,DP} + \lambda_{MPF,L} \tag{2}$$

kde:

λ_{SPF} - intenzita poruch přiřazená single-point poruchám hardwaru[h^{-1}]
λ_{RF} - intenzita poruch přiřazená reziduálním poruchám hardwaru [h^{-1}]
λ_{MPF} - intenzita poruch přiřazená multiple-point poruchám hardwaru [h^{-1}]
$\lambda_{MPF, DP}$ - intenzita poruch přiřazená pozorovaným nebo detekovaným multiple-point poruchám hardwaru [h^{-1}]
$\lambda_{MPF, L}$ - intenzita poruch přiřazená latentním poruchám hardwaru [h^{-1}]

Druhým cílem je prokázat dostatečně nízkou pravděpodobnost vzniku nebezpečné poruchy posuzovaného systému. Požadavky související normy na cílovou míru poruch P_{MHF} jsou uvedeny v tab. 1.

Tab. 1 Požadavky normy na cílovou míru poruch [6]

ASIL	Random hardware failure target values
D	**< 10^{-8}**
C	**< 10^{-7}**
B	**< 10^{-7}**

U posuzovaného systému je nutné výpočtem prokázat dosažené hodnoty P_{MHF} a porovnat je s požadavky normy uvedenými v tab. 1. Porovnáním se rozhodne, zda systém vyhovuje požadované úrovni ASIL.

3 Výpočet P_{MHF}

Norma ISO 26262, část 5 definuje P_{MHF} jako střední pravděpodobnost poruchy připadající na hodinu provozu. Této definici odpovídá vztah (3).

$$P_{MHF} = \frac{F_{AVG}}{t} \tag{3}$$

kde:

F_{AVG} - střední hodnota pravděpodobnosti poruchy [-]
t - doba provozu [h]

V oblasti funkční bezpečnosti reálně pracujeme s hodnotou pravděpodobnosti poruchy prvků F(t) <<1 a samozřejmě i omezenou dobou života prvku. Za těchto předpokladů je možné s dostatečnou přesností průběh pravděpodobnosti F(t) odpovídající exponenciálnímu rozdělení aproximovat přímkou a pravděpodobnost poruchy prvku F(t) je potom dána vztahem (4).

$$F(t) = \lambda \cdot t \qquad \lambda>0,\ t \geq 0 \tag{4}$$

kde:

F(t) - pravděpodobnost poruchy prvku [-]
λ - intenzita poruch prvku [h^{-1}]
t - doba provozu [h]

Potom pro P_{MHF} definovanou vztahem (3) s využitím uvedené aproximace získáme následující vztahy:

$$F_{AVG} = \frac{1}{t}\int_0^t (\lambda \cdot t)dt = \frac{1}{2}(\lambda \cdot t) \tag{5}$$

$$P_{MHF} = \frac{\lambda \cdot t}{2t} = \frac{\lambda}{2} \approx \lambda_{AVG} \tag{6}$$

kde:

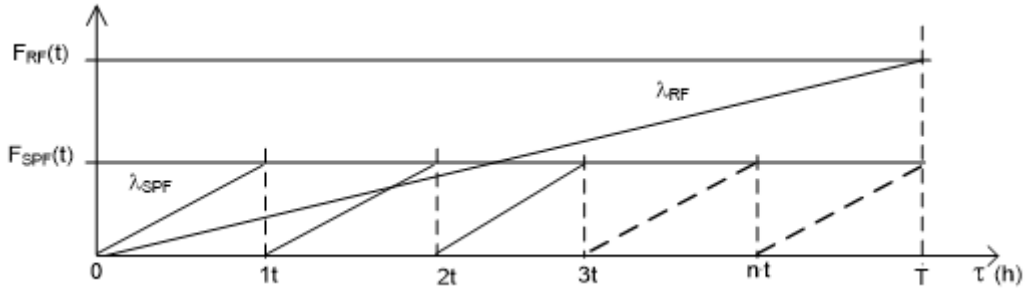
F_{AVG} - střední hodnota pravděpodobnosti poruchy prvku [-]
λ_{AVG} - střední hodnota intenzity poruch prvku [h^{-1}]

Získané rovnice (5) a (6) budou dále využity při detailní analýze vlivu diagnostického pokrytí na výpočet P_{MHF}.

3.1 Analýza vlivu diagnostického pokrytí na P_{MHF}

Dosud jsme ve výpočtu uvažovali intenzitu poruch λ popsanou rovnicí (1), která je složena s dílčích hodnot spojených s diagnostickým pokrytím poruch prvku. To znamená, že část poruch bude diagnostikována, zde konkrétně s intenzitou poruch λ_{SPF} a $\lambda_{MPF,\,DP}$ a část poruch bude nediagnostikovaná s intenzitou poruch λ_{RF} a $\lambda_{MPF,\,L}$. Diagnostika poruch úzce souvisí s použitím diagnostických testů a jejich intervaly. Některá část systému může být diagnostikována kontinuálně, jiná část v rámci self-test při startu vozidla až po situaci, kdy testování není prováděno vůbec. Je proto nutné upravit vztah (6), kde P_{MHF} bude záviset na intenzitě diagnostikovaných a nediagnostikovaných poruch a posouzení vlivu intervalů diagnostických testů.

V případě použití automatického diagnostického testu předpokládáme, že diagnostikovaný prvek je v bezporuchovém stavu a pravděpodobnost poruchy v tento okamžik je proto nula. Po provedení testu pravděpodobnost poruchy narůstá s intenzitou poruch λ_{SPF} až do okamžiku provedení dalšího diagnostického testu v čase *t*, kdy pravděpodobnost poruchy bude $F_{SPF}(t)$, jak ukazuje (obr.1). Vedle toho není část poruch pokryta tímto automatickým diagnostickým testem, a proto narůstá pravděpodobnost poruchy $F_{RF}(t)$ s intenzitou poruch λ_{RF} až do okamžiku testování v údržbě v čase *T*. V extrémním případě může doba *T* představovat celkovou dobu života prvku.



Obr. 1 Vliv použití automatického diagnostického testu

Ke střední hodnotě pravděpodobnosti poruchy prvku F_{AVG} budou přispívat dvě dílčí hodnoty pravděpodobnosti poruch. První příspěvek $F_{SPF}(t)$ je od diagnostikované poruchy a druhý $F_{RF}(t)$ od nediagnostikované poruchy. Protože diagnostikované a nediagnostikované poruchy jsou vzájemně disjunktní jevy, je možné dílčí pravděpodobnosti poruchy sčítat a $F_{AVG,}$ je dána vztahy (7), (8).

$$F_{AVG,S} = F_{AVG}^{(SPF)} + F_{AVG}^{(RF)} \tag{7}$$

$$F_{AVG,S} = \frac{1}{2} \cdot t \cdot \lambda_{SPF} + \frac{1}{2} \cdot T \cdot \lambda_{RF} \qquad \lambda_{SPF};\ \lambda_{RF} > 0,\ t \geq 0 \tag{8}$$

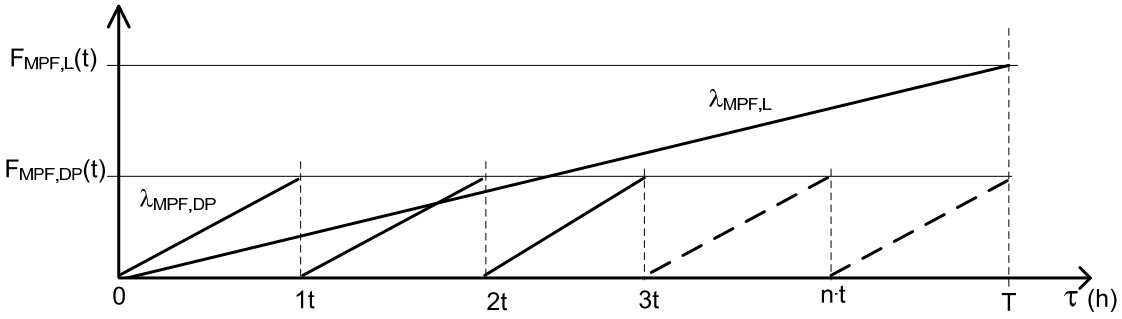
kde:

$F_{AVG,\,S}$ - střední pravděpodobnost vzniku single poruchy prvku [-]
t - interval automatického diagnostického testu prvku [h]
T - interval údržby zaměřené na detekci nediagnostikovaných poruch, případně životnost prvku [h]

Dále je dle požadavku normy nutno posoudit vliv vícenásobných a latentních poruch. Vznik latentní, tedy první poruchy, neznamená bezprostřední poruchu prvku, tato vznikne až v okamžiku souběhu s nějakou další poruchou jiného prvku, tedy druhou poruchou. U složitých

systémů může být takových kombinací velmi mnoho a úloha se tak stává velmi obtížně řešitelnou. Navíc v raných fázích vývoje HW se dají očekávat i časté změny návrhu a složitý postup výpočtu rozhodně není žádoucí. Zjednodušení výpočtu dosáhneme tak, že zvážíme logiku vzniku vícenásobné poruchy. Při vniku latentní poruchy (s pravděpodobností rovné jedné, protože porucha již nastala), je pravděpodobnost vzniku vícenásobné poruchy dána pravděpodobností vzniku druhé poruchy.

Obdobně jako v předchozím případě předpokládáme použití automatického diagnostického testu pro zjišťování vícenásobné poruchy. Na obr. 2 jsou znázorněny průběhy pravděpodobnosti vícenásobné poruchy $F_{MPF,\,DP}$ a $F_{MPF,\,L}$ za situace, kdy self-test je zaměřen i na pokrytí vícenásobné poruchy.



Obr. 2 Vliv vícenásobných diagnostikovaných a nediagnostikovaných poruch

Protože diagnostikované a nediagnostikované vícenásobné poruchy jsou vzájemně disjunktní jevy, je možné dílčí pravděpodobnosti poruchy sčítat a pravděpodobnost poruchy $F_{AVG,\,M}$ je dána vztahy (9), (10).

$$F_{AVG,M} = F_{AVG}^{(MPF,DP)} + F_{AVG}^{(MPF,L)} \tag{9}$$

$$F_{AVG,M} = \frac{1}{2} \cdot t \cdot \lambda_{MPF,DP} + \frac{1}{2} \cdot T \cdot \lambda_{MPF,L} \qquad \lambda_{MPF,\,DP};\ \lambda_{MPF,\,L} > 0,\ t \geq 0 \tag{10}$$

kde:

$F_{AVG,\,M}$ - střední hodnota pravděpodobnosti vícenásobné poruchy [h]
t - interval automatického diagnostického testu prvku [h]
$\lambda_{MPF,\,DP}$ - intenzita diagnostikovaných nebo pozorovaných latentních poruch prvku [h^{-1}]
T - interval údržby zaměřené na detekci nediag. latentních poruch, případně životnost prvku [h]
$\lambda_{MPF,\,L}$ - intenzita nediagnostikovaných latentních poruch prvku [h^{-1}]

Je nutné poznamenat, že uvedené zjednodušení výpočtu bude hodnotit vliv vícenásobných poruch konzervativně. Skutečně dosažené hodnoty budou vždy lepší, ale tento defenzivní přístup může být v raných fázích vývoje HW naopak přínosem.

Spojením modelů jednotlivých a vícenásobných poruch popsaných vztahy (9) a (10) získáme střední hodnotu pravděpodobnosti F_{AVG} jednoho prvku (11).

$$F_{AVG} = \frac{1}{2} t \cdot (\lambda_{SPF} + \lambda_{MPF,DP}) + \frac{1}{2} T \cdot (\lambda_{RF} + \cdot \lambda_{MPF,L}) \tag{11}$$

Dále je nutné rovnici (11) upravit ve smyslu definice P_{MHF} dle vztahu (3), to znamená příspěvek od diagnostikovaných poruch dělit dobou t a podobně příspěvek od nediagnostikovaných poruch dělit dobou T. Získáme tak hledanou hodnotu P_{MHF} danou vztahem (12).

$$P_{MHF} = \frac{1}{2}\left[\left(\lambda_{SPF} + \lambda_{MPF,DP}\right) + \left(\lambda_{RF} + \lambda_{MPF,L}\right)\right] \approx \lambda_{AVG} \tag{12}$$

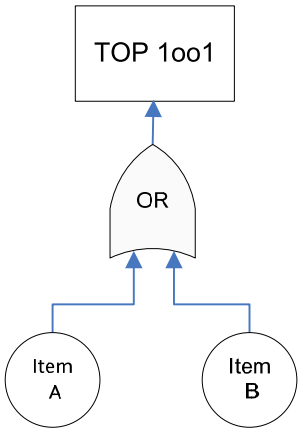
Model P_{MHF} jednoho prvku dle vztahu (12) je dostatečně jednoduchý pro použití v počátečních fázích návrhu systému, kdy lze očekávat časté změny návrhu systému na úrovni tvořících prvků (součástek).

3.2 Výpočet P_{MHF} soustav

Jednotlivé prvky, subsystémy nebo i celé systémy mají samozřejmě různé funkční vazby, a proto i různou architekturu. Potom pravděpodobnost poruchy systému bude záviset nejen na pravděpodobnosti poruchy tvořících prvků, ale i na architektuře systému. Prvky mohou být řazeny za sebou (sériová architektura), vedle sebe (paralelní architektura), tato problematika je ve funkční bezpečnosti známa jako „architektura HW“. V další části článku je ukázáno odvození vztahů pro nejčastěji používané architektury elektronických systémů automobilů.

Architektura 1001 – sériová soustava

Tuto architekturu tvoří nejméně dva prvky A a B řazené sériově a jsou tedy vázány hradlem OR. U sériové soustavy porucha jednoho prvku znamená poruchu celé soustavy. Sériová soustava, složená ze dvou prvků A a B, je schématický znázorněna na obr. 3, kde TOP jev představuje poruchu soustavy s architekturou 1001.



Obr. 3 Architektura 1001 – schématické zobrazení FTA

Výpočtu soustavy s architekturou 1001 provedeme s použitím pravidla, že výsledná intenzita poruch soustavy je dána součtem intenzit poruch tvořících prvků (13).

$$\lambda^{1001} = \lambda^{A} + \lambda^{B} \tag{13}$$

Dále, pokud zvážíme pravidlo, že součet středních hodnot je střední hodnota, můžeme do vztahu (17) dosadit střední hodnoty intenzit poruch prvků A a B a získat tak střední hodnotu intenzity poruch soustavy s architekturou 1001 danou vztahem (14).

$$\lambda_{AVG}^{1001} = \lambda_{AVG}^{A} + \lambda_{AVG}^{B} \tag{14}$$

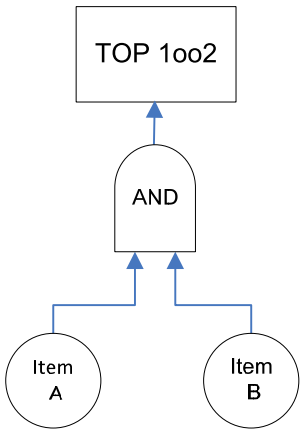
Jak bylo ukázáno ve vztahu (12), hodnota intenzity poruch λ_{AVG} jednoho prvku odpovídá Probabilistic Metric for random Hardware Failures P_{MHF} tohoto prvku. Potom dosazením (12) do vztahu (14) a zobecněním pro soustavu tvořenou *N* prvky získáme hledaný vztah P_{MHF} pro soustavu s architekturou 1001:

$$P_{MHF}^{1001} = \sum_{i=1}^{N} P_{MHF,i} \tag{15}$$

Vztah (15) je velmi jednoduchý, protože stačí sečíst hodnoty P_{MHF} tvořících prvků, což je výhodné v počátečních fázích návrhu systému, kdy lze očekávat časté změny konfigurace.

Architektura 1002 – paralelní soustava

Tuto architekturu tvoří dva prvky řazené vedle sebe a jsou tedy vázané hradlem AND. Porucha celé soustavy nastane při poruše obou prvků. Schematicky soustava, složená ze dvou prvků A a B, znázorněna na obr. 4, kde TOP jev představuje soustavy s architekturou 1oo2.



Obr. 4 Architektura 1002 – schématické zobrazení FTA

Exaktní výpočet pravděpodobnosti poruchy paralelní soustavy, složené ze dvou prvků, je dán vztahem (16).

$$F(t) = F_A(\mathrm{t}) \cdot F_B(\mathrm{t}) \tag{16}$$

kde:
F(t) - je pravděpodobnost poruchy soustavy 1002 složené z prvků A a B
F_A(t) - je pravděpodobnost poruchy prvku A
F_B(t) - je pravděpodobnost poruchy prvku B

Dosazením lineárního průběhu distribuční funkce popsané vztahem (4) do rovnice (16) získáme pravděpodobnost poruchy soustavy dané vztahem (17). Dále integrací vztahu (17) získáme střední hodnotu pravděpodobnosti poruchy soustavy s architekturou 1oo2, popsanou vztahem (18).

$$F(t) = (\lambda_A \cdot t) \cdot (\lambda_B \cdot t) \tag{17}$$

$$F_{AVG}^{1oo2} = \frac{1}{t}\int_0^t (\lambda_A \cdot t) \cdot (\lambda_B \cdot t)dt = \frac{1}{3} \cdot \lambda_A \cdot \lambda_B \cdot t^2 \tag{18}$$

kde:
F_{AVG}^{1oo2} - střední hodnota pravděpodobnosti poruchy soustavy s architekturou 1002
t - doba provozu soustavy
λ_A, λ_B - intenzity poruch prvků A a B

Soustava 1oo2 je tvořena dvěma prvky s intenzitou diagnostikovaných poruch λ_{SPF} a $\lambda_{MPF,\,DP}$ a intenzitou nediagnostikovaných poruch λ_{RF} a $\lambda_{MPF,\,L}$. Oba prvky jsou automatickým diagnostickým testem testovány s intervalem *t* a nediagnostikované poruchy jsou zjišťovány v intervalu T. Je tedy možné stanovit střední hodnotu pravděpodobnosti výskytu obou typů diagnostikovaných a nediagnostikovaných poruch s využitím vztahu (18). Dosazením intenzit diagnostikovaných poruch prvků λ_{SPF} a $\lambda_{MPF,\,DP}$ do (18) získáme vztah (19) a analogicky pro nediagnostikované vícenásobné poruchy vztah (20).

$$F_{AVG,DD}^{1oo2} = \frac{1}{3} \cdot t^2 \cdot \left(\lambda_{SPF}^A + \lambda_{MPF,DP}^A\right) \cdot \left(\lambda_{SPF}^B + \lambda_{MPF,DP}^B\right) \tag{19}$$

$$F_{AVG,DU}^{1oo2} = \frac{1}{3} \cdot T^2 \cdot \left(\lambda_{RF}^A + \lambda_{MPF,L}^A\right) \cdot \left(\lambda_{RF}^B + \lambda_{MPF,L}^B\right) \tag{20}$$

kde:

$F_{AVG,DD}^{1oo2}$ - střední hodnota pravděpodobnosti diagnostikované poruchy soustavy architekturou 1oo2 [-]

$F_{AVG,DU}^{1oo2}$ - střední hodnota pravděpodobnosti nediagnostikované poruchy soustavy s architekturou 1oo2 [-]

Protože diagnostikované a nediagnostikované poruchy jsou vzájemně disjunktní jevy, je možné jejich pravděpodobnosti sčítat. S uvážením vztahu (19) a (20) získáme vztah (21), dále úpravou vztahu (20) ve smyslu definice P_{MHF} získáme hledaný výraz (22) pro architekturu 1oo2.

$$F_{AVG}^{1oo2} = \frac{1}{3}\left[t^2 \cdot \left(\lambda_{SPF}^A + \lambda_{MPF,DP}^A\right) \cdot \left(\lambda_{SPF}^B + \lambda_{MPF,DP}^B\right) + T^2 \cdot \left(\lambda_{RF}^A + \lambda_{MPF,L}^A\right) \cdot \left(\lambda_{RF}^B + \lambda_{MPF,L}^B\right)\right] \tag{21}$$

$$F_{MHF}^{1oo2} = \frac{1}{3}\left[t \cdot \left(\lambda_{SPF}^A + \lambda_{MPF,DP}^A\right) \cdot \left(\lambda_{SPF}^B + \lambda_{MPF,DP}^B\right) + T \cdot \left(\lambda_{RF}^A + \lambda_{MPF,L}^A\right) \cdot \left(\lambda_{RF}^B + \lambda_{MPF,L}^B\right)\right] \tag{22}$$

V praxi se často setkáme se situací, kdy oba prvky soustavy jsou totožné a mají proto i stejné hodnoty intenzit poruch. Potom je možné vztah (22) zjednodušit a získáme tak vztah (23).

$$F_{MHF}^{1oo2} = \frac{1}{3}\left[t \cdot \left(\lambda_{SPF} + \lambda_{MPF,DP}\right)^2 + T \cdot \left(\lambda_{RF} + \lambda_{MPF,L}\right)^2\right] \quad (23)$$

Obecně architektura typu *koom*

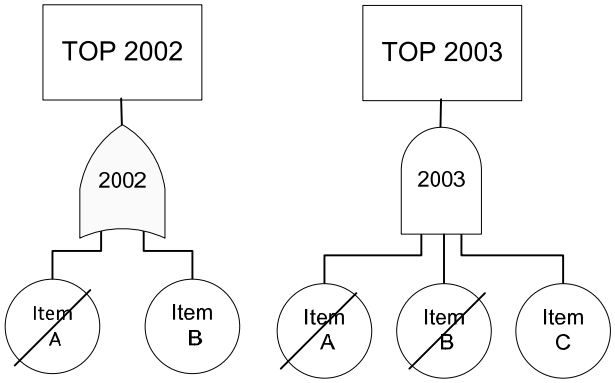
Soustava s architekturou typu *koom* je složena celkem z m prvků a pokud je k prvků v bezporuchovém stavu, je v bezporuchovém stavu celá soustava. Můžeme se tak setkat s konkrétním uspořádáním architektury typu 1oo3, 2oo2 nebo 2oo3 apod. Každá z uvedených variant má pro konkrétní návrh HW své výhody, ale analýza vlastností těchto soustav např. z hlediska diagnostického pokrytí je mimo rozsah tohoto článku. Proto se dále omezíme na výpočet P_{MHF} těchto soustav.

Výpočet P_{MHF} soustav typu *koom* je možné provést stanovením počtu prvků, které musí být současně v poruše, aby byla v poruše celá soustava. Tento počet prvků dán vztahem (24).

$$h = m - k + 1 \quad (24)$$

kde:
h - počet prvků, které jsou současně v poruše
m - celkový počet prvků v soustavě
k - počet prvků v bezporuchovém stavu v soustavě

Jak je ukázáno na obr. 5, soustava typu 2002 bude v poruše, pokud se porouchá jeden prvek, potom h = 1 a soustava typu 2003 bude v poruše, pokud se současně porouchají dva libovolné prvky, potom h = 2.



Obr. 5 Vznik poruchy soustav typu 2002 a 2003

Elektronické systémy velmi často používají řešení, kdy použité prvky jsou identické, např. tři identické snímače tvoří soustavu s architekturou 2oo3. Za předpokladu použití identických prvků je sestaven vztah (25) s uvážením podmínky, že soustava typu *koom* je v poruše, pokud je současně v poruše právě h libovolných prvků.

$$F_{AVG}^{koom} = \binom{m}{h} \cdot \frac{1}{t}\int_0^t (\lambda \cdot t)^h dt = \frac{\lambda^h \cdot t^{h-1}}{h+1} \quad (25)$$

Vztah (25) obsahuje kombinační člen s ohledem na počet kombinací prvků, které způsobí poruchu soustavy. Např. u soustavy 2oo3 existují tři kombinace poruch, jak ukazuje obr. 5, poruchy dvojice (A, B), (A, C) a (B, C) a proto je nutné vztah (25) doplnit o kombinační člen.

Zobecněním vztahu (25), a to použitím intenzity diagnostikovaných poruch λ_{SPF} a $\lambda_{MPF,\,DP}$ a intenzity nediagnostikovaných poruch λ_{RF} a $\lambda_{MPF,\,L.}$ a jeho úpravou v souladu s definicí P_{MHF} obdržíme obecný vztah pro výpočet soustav typu *koom* (26).

$$P_{MHF}^{koom} = \binom{m}{h} \cdot \frac{1}{(h+1)} \cdot \left[t^{h-1} \cdot \left(\lambda_{SPF} + \lambda_{MPF,DP}\right)^{h} + T^{h-1} \cdot \left(\lambda_{RF} + \lambda_{MPF,L}\right)^{h} \right] \tag{26}$$

Doposud jsme uvažovali, že soustavy jsou tvořeny výhradně prvky. V reálné praxi však místo prvků mohou být použity další soustavy, tvořené mnoha prvky (součástkami). Například soustava s architekturou 2oo2 osahuje místo dvou prvků další dvě soustavy s vnitřní architekturou typu 1oo1. Vznikají tak kombinované soustavy. Pro nejčastěji se vyskytující případ, že prvky soustavy s architekturou *koom* jsou nahrazeny soustavami s architekturou typu 1oo1, je sestaven vztah (27). Do vztahu dosadíme součty intenzit poruch součástí tvořící jeden kanál a můžeme přímo vypočítat P_{MHF}^{koom} dle vztahu (27).

$$P_{MHF}^{koom} = \binom{m}{h} \cdot \frac{1}{(h+1)} \cdot \left[t^{h-1} \cdot \left(\sum_{i=1}^{n} \lambda_{i,SPF} + \lambda_{i,MPF,DP} \right)^{h} + T^{h-1} \cdot \left(\sum_{i=1}^{n} \lambda_{i,RF} + \lambda_{i,MPF,L} \right)^{h} \right] \tag{27}$$

Výše uvedené vztahy umožňují relativně jednoduchý postup výpočtu kombinovaných soustav.

4 Závěr

V článku jsou popsány postupy výpočtu Probabilistic Metric for random Hardware Failures dle standardů požadovaných v ISO 26262:2018. Výpočet je proveden s využitím FTA analýzy, která je ve zmíněné normě uvedena jako velmi doporučená metod. Výpočtové postupy jsou zejména vhodné pro rané fáze vývoje elektrických/elektronických systémů, kdy se dají očekávat časté z měny návrhu HW. Odvozené vztahy jsou proto relativně jednoduché a jejich praktické použití nevyžaduje specializovaný SW zaměřený na řešení úloh z oblasti matematické teorie spolehlivosti. Aplikace uvedených postupů umožňuje řešení celé řady prakticky používaných architektur HW, a to jen s malým omezením přesnosti výpočtu.

Použité zdroje

[1] Johansson D, Karllssom P, *Safety mechanisms for random ECU hardware failures in compliance with ISO 26262*. Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg, Sweden. June 2015

[2] Kleyner A. and Knoell R., *Calculating Probability Metric for Random Hardware Failures (P_{MHF}) in the New Version of ISO 26262 Functional Safety - Methodology and Case Studies,* SAE Technical Paper 2018-01-0793, 2018, doi:10.4271/2018-01-0793.

[3] *NASA. Fault Tree Handbook with Aerospace Applications,* NASA Office of Safety and Mission Assurance, Washington DC, 2002.

[4] Rausand M, Høyland A, System Reliability Theory: *Models, Statistical Methods, and Applications*. Wiley, Hoboken, New Jersey, 2nd edition, 2004, ISBN: 978-0471471332

[5] Mader R., Armengaud E., Grießnig G., Kreiner C. J. Steger, C. & Weiß, R. (2013). OASIS: *An automotive analysis and safety engineering instrument*. Reliability Engineering & System Safety, 120, 150-162. https://doi.org/10.1016/j.ress.2013.06.045

[6] ISO 26262 – 5, Road vehicles — Functional safety —Part 5: Product development at the hardware level, Second edition 2018-12, ISO 2018

ISBN 978-80-02-02963-2

Funkční bezpečnost v automobilovém průmyslu

Sborník přednášek
kolektiv autorů
1. vydání, rok vydání 2021, Česká společnost pro jakost
online vydání, formát pdf, 37 stran