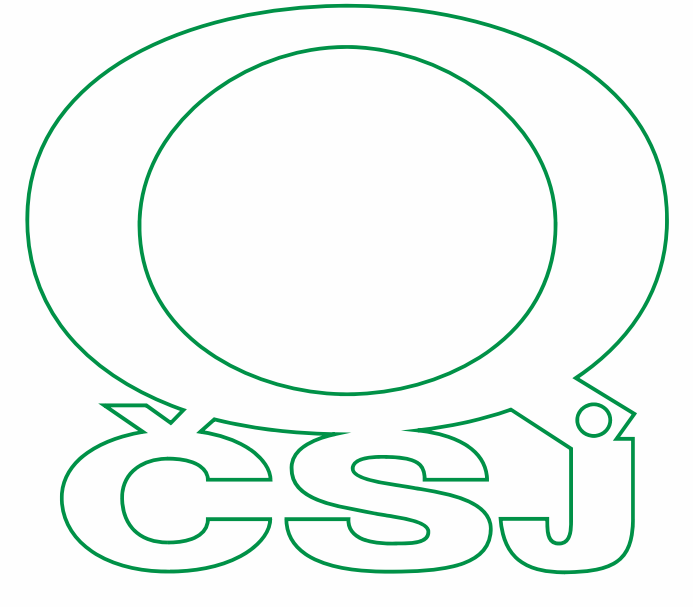
Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1



Aplikované techniky spolehlivosti v automobilovém inženýrství

Materiály ze 75. semináře Odborné skupiny pro spolehlivost
konaného dne 11. 6. 2019 na Univerzitě obrany v Brně

Odborní garanti semináře:
prof. Ing. Zdeněk Vintr, CSc., dr.h.c.
Ing. Michal Vintr, Ph.D.

Obsah

Sledování provozní spolehlivosti u vozidel používaných AČR

Ing. Jiří CHALOUPKA, Ph.D.

Vojenský technický ústav, s.p. oz VTÚPV

jiri.chaloupka@vtusp.cz

1. Úvod

V posledních letech AČR pořizuje novou pozemní techniku a zbraňové systémy a součástí akvizice je také hodnocení nákladů na životní cyklus. Mimo pořizovací náklady se na celkových nákladech akvizice pozemní techniky podílejí náklady na provoz v délce 20-30 let podle zadání. Výše nákladů na provoz pozemní techniky je velkou měrou ovlivněna její spolehlivostí, resp. počtem poruch, tzn. parametr bezporuchovost, a cenou potřebných náhradních dílů k provedení oprav.

Do sledování spolehlivosti resp. bezporuchovosti vojenské pozemní techniky byly zařazeny automobily, lehká obrněná vozidla, kolová bojová vozidla a těžká bojová technika. Informace o provozu a počtu poruch pro hodnocení provozní spolehlivosti byly získány péčí AČR.

2. Sledování

Sledování provozní spolehlivosti probíhalo podle jednotné metodiky [1] na jednotlivých typech vojenské pozemní techniky zavedených do používání v AČR. Hodnocení provozní spolehlivosti bylo provedeno po ročním provozu v roce 2016. Cílem sledování provozní spolehlivosti bylo vyhodnotit plnění stanovených požadavků na spolehlivost, stanovit parametry spolehlivosti jednotlivých skupin vozidla, normativ náhradních dílů (ND), pracnost oprav a údržby a navrhnout opatření ve vztahu k reálně dosaženým parametrům provozní spolehlivosti.

Celkem tak bylo sledováno a hodnoceno přes 3 000 ks vojenské pozemní techniky. Sběr informací potřebných k vyhodnocení provozní spolehlivosti byl náročný na organizaci, aby byly zajištěny relevantní informace. Některé typy vojenské techniky byly již dříve sledovány a nové poznatky přispěly pouze k aktualizaci dřívějších informací.

3. Informační systém

Byl vytvořen informační systém mezi Agenturou logistiky zastupující uživatele a pracovištěm pro vyhodnocení provozní spolehlivosti. Informace byly získány z informačního systému používaného v AČR, do kterého uživatel vojenské techniky zadává provozní data o technice (ujeté kilometry, spotřeba PHM, provedení preventivní údržby) informace o poruše, nepojízdnosti a termíny o odstranění poruchy.

Informace o poruše jsou vkládány do samostatné databáze, s datem vložení a jménem vkladatele informace, tzn. uživatele předmětné techniky. Evidenční informace o typu vojenské techniky a jejím provozu jsou automatickou cestou do této databáze vkládány. Dále se v čase do systému doplňují informace, které popisují průběh a způsob odstranění poruchy, tzn. provedení nápravné údržby.

Tyto informace mohou být určitým vodítkem k řešení obdobné poruchy u stejného typu vojenské techniky a k analytickému vyhodnocení schopností dílenských specialistů, rychlosti provedení opravy, dob prostojů a případně vhodnosti úprav normativů náhradních dílů.

Pokud lze poruchu jednoznačně definovat, lze specifikovat poškozený díl, ujasněn postup provedení opravy a zajištění náhradního dílu, rozhodne se o způsobu odstranění poruchy v možnostech:

- prostředky praporu (prostory a dílenští specialisté);
- prostředky nadřízeného (prostory a dílenští specialisté);
- prostředky externího opravce (může být využito vojenského prostoru, nebo prostoru externího opravce, ale dílenští specialisté jsou vždy od externího opravce).

Pokud nelze přesně specifikovat poškozený díl je nutné nejdříve vyžádat specialisty výrobce k provedení defektace a získání bližších informací pro rozhodnutí o dalším postupu. Následně může být rozhodnuto o způsobu opravy.

V případě rozhodnutí o provedení opravy silami logistického celku praporu, lze dále vysledovat termín přijetí do opravy, jméno dílenského specialisty určeného k provedení opravy, počet náhradních dílů a pracovní kapacity nutné k odstranění poruchy.

V případě využití prostředků opravce lze využít fakturu s přílohami, které mohou specifikovat vyměněný díl a dobu práce na opravě.

Obdobný model je uplatněn i pro realizaci preventivní údržby vojenské techniky. Rozsah preventivní údržby je definován v dokumentaci výrobce/dodavatele vojenské techniky a její správné a odborné provádění má celkem zásadní vliv na poruchovost vojenské techniky. V informačním systému jsou uvedeny provozní hodnoty, které jsou vztahovány k termínům provedení údržby, a systém automaticky upozorňuje na nutnost provedení údržby. Opět je možné dohledat záznamy o provedení preventivní údržby jako je termín přijetí k provedení preventivní údržby, jméno dílenského specialisty a pracovní kapacity nutné k provedení preventivní údržby.

V informačním systému AČR a další vedené dokumentaci lze výše uvedený postup realizace preventivní a následné údržby vysledovat. V současné době informační systém zatím neprovádí automatickou cestou hodnocení spolehlivosti nebo nákladů potřebných k zajištění provozu.

4. Provozní podmínky

Provozní podmínky vojenské techniky v AČR jsou specifikovány množstvím provozních jednotek (ujetých kilometrů, vystřelených nábojů, spotřebou provozních hodin, spotřebou PHM, množstvím pokládek/nakládek apod.) v kalendářním roce. Dále se informačně sleduje provádění preventivní údržby, legislativních revizí, STK a dalších činností spojených s provozem.

Tyto informace o provozu AČR průběžně sleduje a vyhodnocuje ve vztahu ke skladovanému množství náhradních dílů a predikci k zajištění potřebného množství a sortimentu jednotlivých komodit.

Z hlediska provozu lze rozčlenit vojenskou techniku na vozidla, která zajišťují dopravní a zabezpečovací úkoly jednotlivých armádních celků a vojenská speciální vozidla, která plní úkoly výcviku nebo plní úkoly při nasazení v zahraničních operacích.

4.1 Provozní podmínky zabezpečovací techniky

Provoz vozidel zajišťujících dopravní a zabezpečovací úkoly byl až na dílčí výkyvy jednotlivých roků celkem ustálený. Nicméně byl zaznamenán trend ve snížení celkového provozu této techniky.

Také všechna tato zabezpečovací technika se nevyužívá každým rokem. Tento aspekt ve využití vojenské techniky platí pro každou armádu. Hodnocením provozních dat lze konstatovat, že pouze cca 17 % zabezpečovací techniky ujede více 2 000 km ročně. Celkem cca 83% zabezpečovací techniky ujede maximálně do 2 000 km nebo je dlouhodobě uloženo bez provozu.

Provoz do 2 000 km u zabezpečovací techniky není nijak zásadní z hlediska opotřebení a lze konstatovat, že se u této techniky promítá spíše hledisko stárnutí techniky, zejména pryžových částí jako jsou těsnící elementy, hadice apod.

Průměrná spotřeba paliva u zabezpečovacích vozidel na 100 km se pohybovala na tabulkové spotřebě paliva v AČR. Z těchto hodnot spotřeby paliva lze uvažovat o odpovídajícím stavu pohonných soustav této techniky. Dále tato vozidla podléhají ve většině STK, což znamená, že technický stav těchto vozidel odpovídá legislativnímu standardu v ČR.

4.2 Provozní podmínky speciální vojenské techniky

Vojenská speciální, resp. bojová technika má samozřejmě nižší provoz než zabezpečovací technika. Provoz u této techniky je určen plněním pouze výcvikových úkolů nebo úkolů spojených s nasazením v zahraničních operacích, které jsou pro daný rok naplánovány. Pro výcvik se opět využívá pouze nezbytná technika a tak tato vozidla nejsou provozována vždy v plném počtu.

U vojenských speciálních vozidel bylo provozováno (5 – 30 % po typech) a ostatní vozidla (95 – 70 %) nebyla provozována nebo jejich provoz byl zanedbatelný. Lze usuzovat o vyšším využití trenažérové a simulační techniky vedoucí také k odpovídající vycvičenosti jednotek, ale při snížení nákladů na výcvik.

Tato vozidla sice nepodléhají provádění STK, ale průměrná spotřeba paliva na 100 km se pohybovala na tabulkové spotřebě paliva pro jednotlivé typy těchto vozidel v AČR. Z těchto hodnot spotřeby paliva lze uvažovat o relativně odpovídajícím stavu pohonných soustav u této techniky.

Provoz vojenské speciální techniky se v roce 2016 u některých typů snížil a u jiných typů mírně zvýšil. Z hlediska dlouhodobého provozu je nutné již plánovat u některých typů této techniky termíny provedení oprav vyššího rozsahu nebo revizí po 10 letech a k tomu upravit i hodnotu provozu.

Celkově lze vyhodnotit provozní podmínky sledované techniky jako odpovídající a také technický stav sledované techniky v návaznosti na prováděnou preventivní a následnou údržbu jako relativně uspokojivý. Nicméně je možné definovat oblasti, které jsou plněny lépe nebo oblasti kde byly zjištěny deficity, na které se bude nutné v dalších letech zaměřit. Úspěšné vyřešení oblastí s deficity nejen zvýší schopnosti logistického zabezpečení, ale kladně se promítnou i do hodnot bezporuchovosti sledované techniky. Jedná se počty dílenských specialistů, jejich vycvičenost a obměnu dílenské technologie, která není ve všech případech na standardní nebo odpovídající úrovni. Znamená to samozřejmě realizovat i investiční náklady, které se promítnou do rozpočtu AČR v následujících letech.

5. Výsledky sledování provozní spolehlivosti

Během provozu vojenské techniky bylo zjišťováno neplnění funkce, čímž byla specifikována porucha, která byla klasifikována v souladu se zadáním akvizice nebo podle technických podmínek výroby daných vozidel. Jednoznačné specifikování parametrů spolehlivosti v dokumentaci je stav posledních let.

U starších typů vojenských vozidel nebylo běžné jednoznačně definovat hodnotu spolehlivosti včetně definování charakteru provozu, případně kategorizovat poruchy. Pouze novější typy vojenské techniky mají již tyto parametry spolehlivosti takto uvedeny.

Nicméně i v současnosti byl zaznamenán stav, že některé typy vojenské techniky, jejichž akvizice vzhledem k velikosti nákladů na pořízení byla sledována, mají hodnoty parametrů spolehlivosti lépe specifikovány než jiné typy vojenské nebo speciální techniky, jejichž akvizice jako málo početných vozidel s nižšími náklady na pořízení, nemá parametry spolehlivosti jednoznačně uvedeny.

Tento stav se promítá do možnosti objektivního vyhodnocení parametrů spolehlivosti ve vztahu k zadání. Z tohoto důvodu je hodnoceno u těchto typů vojenských vozidel pouze dosažení reálných parametrů spolehlivosti v jednotlivých letech a při dlouhodobém sledování lze následně vysledovat trendy nebo průměrné hodnoty dosahovaných parametrů spolehlivosti, resp. bezporuchovosti vojenské techniky.

Takové sledování parametrů u velkého počtu vojenské techniky dislokované u velkého počtu organizačních celků je náročné na verifikaci zjištěných informací a jednotný přístup, způsob řešení, kategorizace poruch apod. Analytická práce v tomto případě je zásadní pro správnou interpretaci výsledků a přijetí odpovídajících opatření vedoucích ke zvyšování parametrů spolehlivosti (udržovatelnost, bezporuchovost a zajištěnost údržby).

Určitým nedostatkem sledování a hodnocení spolehlivosti bylo různé stáří sledované vojenské techniky (nová, starší, jednodušší nebo složitější) bez dřívější kontinuální návaznosti, což v prvním roce sledování pouze hodnotu parametru spolehlivosti matematicky vypočítá, ale pokud není pro danou vojenskou techniku hodnota parametru spolehlivosti ani zadána, lze pouze konstatovat zjištěný výsledek. U speciální techniky, která nemá zadané parametry spolehlivosti nelze hodnotu spolehlivosti ani porovnat s jinými typy protože příbuznost této techniky je velmi malá. A informace o spolehlivosti techniky z ostatních armád nejsou běžně dostupné.

Nejen malá příbuznost vojenské techniky se projevuje při hodnocení parametrů spolehlivosti, ale také různý stupeň zajištění údržby u jednotlivých typů vojenské techniky. Tyto aspekty lze samostatně vyhodnotit, ale v jednom roce sledování je obtížné definovat míru vzájemného vlivu na celkové parametry spolehlivosti a navrhnout směry, které budou zlepšovat zjištěné výsledky. Lze objektivně vyhodnotit pouze dosažené parametry spolehlivosti v daném roce sledování, případně náklady spotřebované v daném roce po jednotlivých typech. Nelze hodnotit optimálnost spotřebovaných nákladů.

Poruchy pro hodnocení parametrů spolehlivosti byly převzaty z databáze informačního systému, který vlastní AČR. Na vkládání potřebných informací o poruchách jednotlivých vozidel do informačního systému je vytvářen potřebný tlak a relevantnost údajů se neustále zlepšuje. Do budoucna se předpokládá také rozšíření informačního systému v této oblasti, které přispěje ke zlepšení analytických prací při hodnocení spolehlivosti vojenské techniky. Z toho lze usuzovat, že představitelé AČR si uvědomují, že podrobné informace o spolehlivosti ve všech aspektech (bezporuchovost, údržba a zajištěnost údržby) u vojenské techniky jsou důležité pro další predikci potřeb logistického zabezpečení.

5.1 Provozní spolehlivost zabezpečovací techniky

Vojenská zabezpečovací technika je oproti bojové technice méně složitá a lze vysledovat i technickou příbuznost těchto vozidel. Ale z hlediska různého stáří a složitosti konstrukce jednotlivých typů zabezpečovací techniky nelze tuto příbuznost plně využít. Spolehlivost zabezpečovací vojenské techniky byla sledována po jednotlivých typech.

Některé typy již byly v minulosti sledovány, ale u některých typů proběhlo sledování poprvé v délce jednoho roku. U dlouhodobě sledovaných vojenských vozidel byl zjištěn nárůst vážných poruch, zejména u brzdové soustavy. Tyto poruchy samozřejmě ovlivnily hodnotu MTBF (Střední doba mezi poruchami) dosahovanou v jednotlivých letech. I přes snížení hodnoty MTBF, lze konstatovat, že vojenská zabezpečovací vozidla plní zadané požadavky, pokud byly jednoznačně zadány.

Hodnota MTBF u zabezpečovacích vozidel, která v minulosti nebyla sledována, a parametry spolehlivosti u ní ani nebyly zadány, byla tato hodnota pouze zjištěná bez podrobných aspektů a v příštích letech sledování bude možné tuto dosaženou hodnotu dále hodnotit. Hodnota MTBF se u jednotlivých typů pohybovala od 20 000 km do 100 000 km, což je pro vojenská zabezpečovací vozidla celkem odpovídající hodnota. Celkově bylo možné jednotně hodnotit vojenskou zabezpečovací techniku ve větších počtech s porovnáním po typech. Zároveň byly zjištěny informace i o typech zabezpečovací techniky, která dosud nebyla sledována a zjištěné hodnoty parametrů spolehlivosti jsou pro hodnocení spolehlivosti prvotní.

5.2 Provozní spolehlivost speciální vojenské techniky

Některá vojenská vozidla (speciální) byla také v minulosti sledována a hodnocena z hlediska parametrů provozní spolehlivosti, ale u některých typů této vojenské techniky toto sledování a hodnocení spolehlivosti ještě neproběhlo. U již sledovaných vojenských vozidel byly informace zjištěné v roce 2016 porovnány s dřívějšími hodnotami parametrů spolehlivosti. Porovnáním dosažených hodnot bylo zjištěno snížení hodnoty MTBF v kilometrech provozu. Provoz této vojenské speciální techniky sice klesl, ale i snížené počty poruch hodnotu MTBF v kilometrech snížily. Nejlepších hodnot MTBF bylo dosaženo při dvojnásobném provozu oproti stávajícímu provozu. Hodnota MTBF v kilometrech byla při hodnotě průměrného provozu 1500 km na vojenské speciální vozidlo přes 15 000 km.

Hodnota MTBF u vojenské speciální techniky je plněna v souladu se zadáním. Nicméně byl zachycen trend, který ukazuje, že se při zvyšujícím stářím těchto vozidel i při snižování hodnoty provozu hodnota MTBF v kilometrech u této techniky stále snižuje. Lze vyhodnotit, že nižší hodnota provozu vojenské speciální techniky je pro hodnocení parametru spolehlivosti méně výhodná a také náklady spojené s odstraněním poruch nepřináší úspory.

Poruchovost některé vojenské speciální techniky, která byla v roce sledování a hodnocení spolehlivosti provozována již po dobu 11 let a MON (Mezi Opravní Norma) pro tuto techniku byla nastavena na 10 let, není pro standardní hodnocení parametrů spolehlivosti zcela objektivní. Lze spíše hodnotit zbytkovou hodnotu spolehlivosti, než dojde k provedení vyššího stupně opravy.

6. Závěr

V praxi se potvrdilo, že sledovaná vozidla AČR z hlediska spolehlivosti, resp. bezporuchovosti jsou z dlouhodobého provozu na předpokládané hodnotě dle zadání. Provoz techniky v AČR v minulých letech klesl, ale aktuálně se již zvyšuje a tento trend ovlivňuje dosahované hodnoty bezporuchovosti. Rozsah ročního provozu u sledované techniky se

pohybuje na polovičních hodnotách, než se předpokládalo při pořizování těchto vozidel do AČR. Parametry provozní spolehlivosti, resp. bezporuchovosti zjištěné sledováním vojskového provozu vybraných vozidel jsou na požadované úrovni, která je obvyklá pro obdobné typy vozidel i u jiných armád.

Sledování velkého počtu techniky, analytické zpracování výsledků parametrů provozní spolehlivosti a správná interpretace zjištěných výsledků vyžaduje soustředění vyššího počtu odborných pracovníků. Také vstupní informace a jejich relevantnost jsou zásadní pro správné vyhodnocení. AČR resp. představitelé logistické podpory tak mají k dispozici informace, které dosud předpokládali, ale neměli k dispozici požadovaný analytický materiál. Díky spolupráci s ALog vznikl analytický materiál, který rozšířil stávající znalosti hodnot parametrů provozní spolehlivosti jak u zpracovatele analýzy, tak u zadavatele.

Také důležitost sledování a hodnocení oblasti spolehlivosti vojenské techniky v AČR se potvrzuje dalšími požadavky na činnost v této oblasti v následujících letech. S předpokládanými úpravami informačního systému, který bude následně disponovat podrobnějšími informacemi pro analýzu parametrů spolehlivosti, získá jak zpracovatel, tak zadavatel přesnější hodnoty, což bude velmi přínosné.

Použitá literatura

[1] CHALOUPKA Jiří, Zdeněk VINTR, a Michal VINTR. *Metodika pro sledování a vyhodnocení spolehlivosti nově zaváděné mobilní pozemní techniky AČR*. Metodika, ev. č. J-4-6100/01, VOP-026 Šternberk s.p., divize VTÚPV Vyškov, 2007.

[2] CHALOUPKA Jiří a Ľubomír BÁRDY. *Analýza spolehlivosti pozemní vojenské techniky*. Zpráva, čj. VTÚ/VTÚPV-1345-3/2016, Vyškov, 2016.

[3] KUTIL Robert a kolektiv. *Analýza aktuálního stavu logistické podpory techniky v rezortu MO.* Analýza, čj. VTÚ/VTÚPV-1187-11/2017, Vyškov, 2017.

Zrychlené zkoušky elektronických prvků vozidel

prof. Ing. Zdeněk VINTR, CSc., dr.h.c.; Ing. Xuan Phong CU

Fakulta vojenských technologií, Univerzita obrany, Brno

zdenek.vintr@unob.cz

1. Úvod

Typickým znakem moderních vozidel je stále narůstající využívání různých elektronických systémů sloužících jak k podpoře a realizaci základních funkcí automobilu, tak i ke zvýšení bezpečnosti přepravovaných osob a jejich komfortu. Masívní nasazení elektronických systémů je také základním předpokladem rozvoje vozidel ve dvou nejprogresivnějších oblastech, a to v oblasti elektrického pohonu vozidel a oblasti praktického využití autonomních vozidel. Oprávněně tak lze očekávat, že jedním ze základních rysů všech budoucích vozidel bude rozsáhlé využití elektronických vozidel. Zvláště intenzivně se tento trend projevuje u vojenských vozidel, kde právě využití vyspělých elektronických systémů a digitalizace rozhodujícím způsobem přispívá ke zvyšování bojové efektivnosti těchto vozidel. Tato skutečnost, mimo jiné, vedla i ke vzniku zcela nové technické oblasti označované jako VETRONIKA (složenina z anglických slov Vehicle a Electronics), která se systematicky zabývá rozvojem, standardizací a praktickou aplikací elektronických systémů právě u vojenských vozidel.

Z uvedených trendů je zřejmé, že celková úroveň spolehlivosti vozidel je dnes podstatným způsobem ovlivňována právě úrovní spolehlivosti použitých elektronických systémů, jejichž případná selhání mohou často vést ke ztrátě základních funkcí vozidel. Základním předpokladem pro zajištění požadované úrovně spolehlivosti elektronických systémů je přitom použití kvalitních elektronických komponent s vysokou úrovní bezporuchovosti. Žádoucí přitom je, aby skutečná úroveň bezporuchovosti jednotlivých prvků byla před praktickou aplikací ve vozidlech adekvátním způsobem ověřena. Jistý problém zde představuje skutečnost, že vzhledem k dynamickému vývoji v oblasti elektroniky, nejsou zpravidla při návrhu nových systémů k dispozice věrohodné informace o bezporuchovosti aplikovaných součástek z předchozího provozu. Jedinou cestou, jak úroveň bezporuchovosti součástek ověřit, tak velmi často je pouze provedení odpovídajících zkoušek bezporuchovosti. Zde je však třeba se vyrovnat s dalším problémem, který představuje požadovaná vysoká úroveň bezporuchovosti, jejíž ověření, či prokázání vyžaduje realizaci časově velmi náročných zkoušek. Právě z těchto důvodů jsou v oblasti ověřování bezporuchovosti elektronických prvků velmi populární tak zvané zrychlené zkoušky bezporuchovosti (ART – Accelerated Reliability Testing), jejichž aplikace umožňuje podstatné zkrácení doby potřebné k provedení zkoušky.

Předložený článek přináší základní informace o ART využitelných při zkouškách bezporuchovostí prvků elektronických systémů vozidel a demonstruje jejich praktické využití na příkladu elektroluminiscenčních diod (LED).

2. Základní principy zrychlených zkoušek bezporuchovosti

Podstatou zrychlených zkoušek je využití obecně známé a ověřené zkušenosti, že při vyšších hodnotách namáhání dochází k poruchám výrobků dříve než při hodnotách nižších. Tato inverzní (nepřímo úměrná) závislost mezi úrovní namáhání a úrovní jeho bezporuchovosti je obecným principem všech zrychlených zkoušek.

Během zkoušky zatěžujeme zkoušený prvek na vyšší úrovni, než jaká se předpokládá v běžném provozu. Díky tomu se poruchy projevují častěji a za kratší dobu lze získat informace nezbytné pro vyhodnocení zkoušky. Při realizaci zrychlených zkoušek je třeba řešit dva základní problémy. Prvním je stanovení zatížení prvku při zkoušce. Zatížení by mělo být podstatně vyšší než předpokládané zatížení v provozu (aby bylo dosaženo žádoucího zrychlení), ale na druhé straně nesmí být překročeny konstrukční limity zkoušeného prvku, protože by to vedlo ke vzniku poruch jiného charakteru než při běžném provozním zatížení a tím i ke zkreslení výsledků zkoušky.

Při stanovení zatížení při zkoušce se tak vychází jednak z předpokládaných provozních podmínek prvku a z analýzy jeho konstrukčních limitů. Obecně lze zvýšit zatížení prvku při zkoušce buď zvyšováním provozního zatížení (zvyšování působících sil, momentů, proudů, napětí, …) nebo zhoršováním podmínek prostředí (zvyšování teploty, vlhkosti, vibrací, …).

Zrychlená zkouška je obecně charakterizována tak zvaným faktorem zrychlení, který vyjadřuje vztah mezi hodnotou sledovaného ukazatele (střední doba do poruchy, technický život, …) vyhodnoceného z výsledků zrychlené zkoušky (pří zvýšeném zatížení prvku) a hodnotou stejného ukazatele stanoveného při běžném provozním zatížení prvku. Faktor zrychlení A lze vyjádřit následujícím vztahem:

$$A = \frac{L(S_{Use})}{L(S_{Test})} \tag{1}$$

kde: $L(S_{Use})$ - je technický život jako funkce namáhání v běžném provozním použití,

$L(S_{Test})$ - je technický život jako funkce namáhání použitého ve zkoušce.

Velmi podrobně je problematika zrychlených zkoušek popsána ve sborníku z 39. setkání Odborné skupiny pro spolehlivost [1], který je spolu se sborníky z dalších setkání volně dostupný na stránkách Odborné skupiny pro spolehlivost (https://www.csq.cz/spolehlivost/). Z tohoto důvodu zde není celá problematika zrychlených zkoušek podrobně popisována a dále je pouze stručně vysvětlen Arrheniův model, který se velmi často využívá při zrychlených zkouškách bezporuchovosti elektronických prvků, kdy se zatížení prvku při zkoušce zvyšuje aplikací vyšší provozní teploty. Arrheniův model je založen na vyjádření intenzity reakce jako funkce typu zkoušeného prvku a absolutní teploty T. Tento model předpokládá, že reakce je proporcionálně vztažená k teplotě. Faktor zrychlení A_T lze v tomto případě vyjádřit následujícím vztahem:

$$A_T = \frac{L(T_{Use})}{L(T_{Test})} = e^{\frac{E_a}{k_B}\cdot\left(\frac{1}{T_{Use}} - \frac{1}{T_{Test}}\right)} \tag{2}$$

kde: E_a - aktivační energie (eV);

k_B - Boltzmanova konstanta = 8,617385E-5 eV/K,

$L(T_{Use})$ - je technický život jako funkce teploty při běžném provozním použití,

$L(T_{Test})$ - je technický život jako funkce teploty použité při zkoušce.

Pro stanovení faktoru zrychlení je nutná znalost aktivační energie E_a, která se zpravidla určuje experimentálně, nebo se využívají její hodnoty uváděné v odborné literatuře. Například u polovodičových prvků používaných v automobilovém průmyslu se často využívá zjednodušený vztah pro faktor zrychlení, který již nepracuje se Boltzmanovou konstantou k_B a aktivační energií E_a, ale přímo vyjadřuje závislost faktoru na rozdílu mezi teplotou použitou u při zkoušce a předpokládanou teplotou v běžném provozu [2]:

$$A_T = 2^{\frac{\Delta T}{10}} \tag{3}$$

kde $\Delta T = T_{Test} - T_{Use}$.

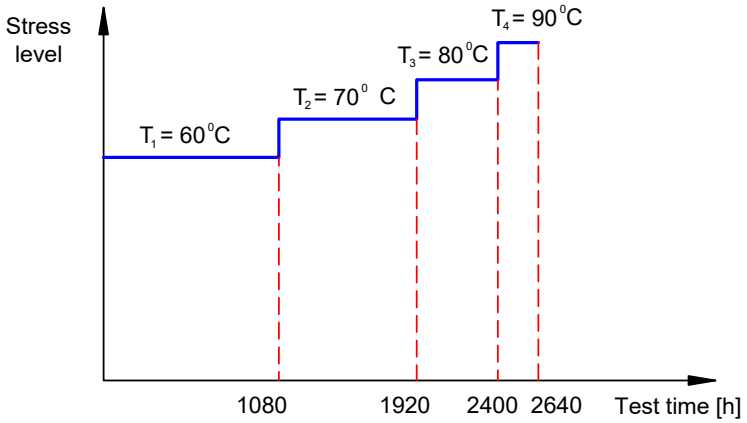
Ze vztahu je patrné, že každé zvýšení zkušební teploty o 10 °C vede ke zdvojnásobení intenzity poruch zkoušeného prvku.

3. Zrychlená zkouška bezporuchovosti LED

Principy zrychlených zkoušek bezporuchovosti byly prakticky využity pro ověření vhodnosti vybraných typů LED pro použití ve vojenských vozidlech. Zkoušeny byly dva typy vysoce výkonných LED. První typ s deklarovaným příkonem 3 W a druhý typ s příkonem 10 W. Cílem zkoušky bylo určení technického života LED. V rámci zkoušky byly monitorovány dva typy poruch LED – úplná ztráta funkce (LED nesvítí) a pokles svítivosti LED pod stanovenou mez.

Pro LED je typickým jevem, že v průběhu jejich provozu postupně dochází k poklesu generovaného světelného toku. Proto je někdy účelné za poruchu považovat i pokles světelného toku pod jistou úroveň.

Vlastní experiment byl proveden s využitím klimatické komory Vötsch VC3 7034, přičemž celý experiment byl proveden tak, že zkouška byla zahájena při zkušební teplotě 60 °C a potom vždy po určitém časovém úseku byla teplota skokově zvýšena o dalších 10 °C až na konečnou teplotu 90 °C (viz Obr. 1).

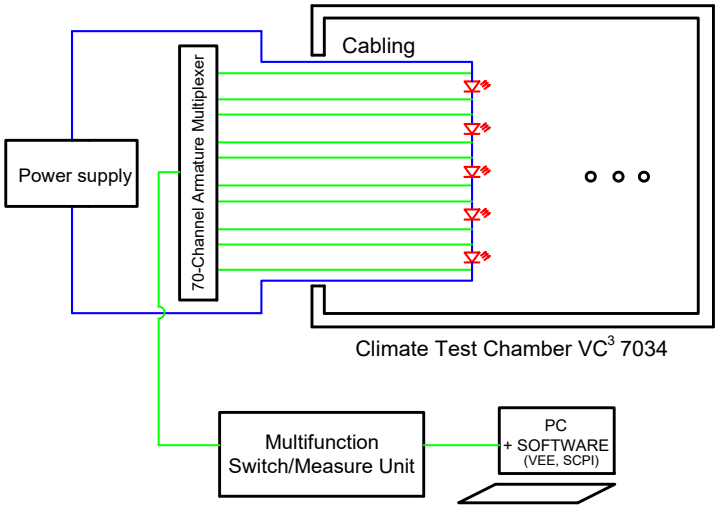


Obr. 1 Zvyšování teploty během zkoušky

Uvedený postup byl zvolen proto, že reálná vnitřní teplota LED je vždy výrazně vyšší než teplota okolí a je tak obtížné určit maximální přípustnou teplotu ve zkušební komoře tak, aby nedošlo k překročení konstrukčních limitů daného typu LED. Zkouška tedy měla také za cíl určit, při jaké teplotě ve zkušební komoře případně dojde k překročení daných konstrukčních limitů. Doba zkoušení se při jednotlivých teplotách postupně zkracuje, protože se zvýšením teploty se vždy zvyšuje i faktor zrychlení.

Obr. 2 Klimatická komora s měřící aparaturou

Na Obr. 2 je zkušební klimatická komora s měřící a napájecí aparaturou. Schéma zapojení měřící aparatury a napájení LED při experimentu je znázorněno na Obr. 3.



Obr. 3 Schéma zapojení měřící apartury

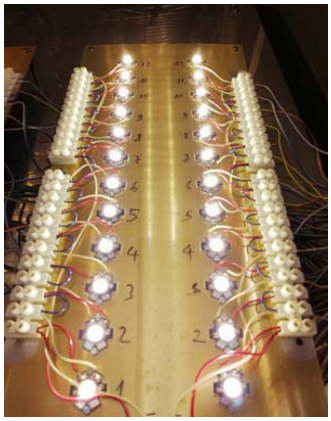
V Tabulce 1 je uveden přehled dob trvaní jednotlivých fází zkoušky, hodnot faktorů zrychlení odpovídajících daným zkušebním teplotám a ekvivalent. dob provozu za běžných provozních podmínek. V daném případě výpočty vychází z běžné provozní teploty na úrovní 35 °C.

Tabulka 1 Časový průběh zkoušky

Teplota při zkoušce (°C)	**Faktor zrychlení**	**Doba zkoušky (h)**	**Ekvivalentní doba provozu při běžné provozní teplotě (h)**
60	5,656	1080	6 109
70	11,134	840	9 504
80	22,627	480	10 861
90	45,254	240	10 861
Celková simulovaná doba provozu			**37 333**

4. Vyhodnocení výsledků zrychlené zkoušky bezporuchovosti LED

V jedné ze zkoušených sad (viz Obr. 4) bylo u 9 z celkového počtu 24 LED zaznamenána v průběhu zkoušky porucha spočívající v úplné ztrátě funkce. U každé poruchy byl měřící aparaturou zaznamenán čas poruchy, který byl pro potřeby dalšího zpracování převeden na ekvivalentní dobu provozu při běžné teplotě (35 °C). V Tabulce 2 je uveden přehled zaznamenaných časů poruch.



Obr. 4 Sada 24 LED instalovaných na hliníkové desce ve zkušební komoře

K vyhodnocení souboru informací ze zkoušky byl použit výpočet dolní meze jednostranného konfidenčního intervalu střední doby do poruchy dle normy [3]. Protože se jednalo o zkoušku ukončenou časem, realizovanou bez nahrazování, byl výpočet proveden s využitím následujícího vztahu:

$$MTTF_L = \frac{2T_{oE}}{\chi^2_\alpha(\nu)}, \tag{4}$$

kde: $\chi^2_\alpha(\nu)$ - kvantil rozdělení chí-kvadrát pro ν stupňů volnosti a konfidencí úroveň α,

T_{oE} - ekvivalentní doba zkoušky (součet všech dob provozu zkoušených výrobků, v tomto případě přepočtených na běžnou provozní teplotu).

Počet stupňů volnosti ν se pro každý jednotlivý případ vyhodnocení stanoví dle následujícího vztahu [3]:

$$\nu = 2r + 1 \tag{5}$$

kde *r* je počet zaznamenaných poruch u příslušného vzorku.

Tabulka 2 Přehled zaznamenaných poruch

Číslo poruchy	Čas poruchy přepočtený na normální provozní teplotu (h)
1	27651
2	27922
3	28330
4	29099
5	30547
6	30773
7	32086
8	34710
9	35435

Ekvivalentní doba zkoušky se stanoví s využitím vztahu:

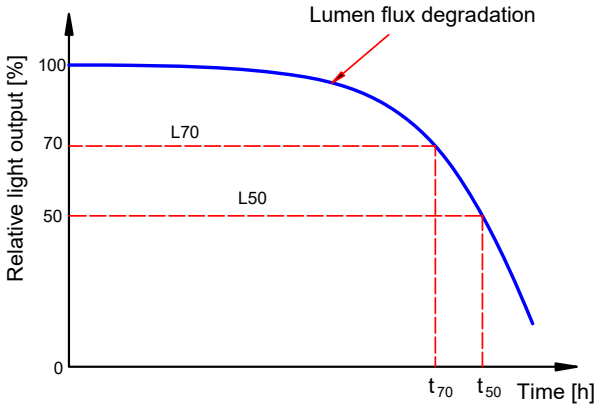
$$T_{OE} = \sum_{i=1}^{r} t_i + (n - r) \cdot \tau \qquad (6)$$

Kde: t_i - doba do i-té poruchy,
n - počet zkoušených LED (24 ks),
r - počet zaznamenaných poruch (r = 9),
τ - celková doba zkoušky přepočtená na normální teplotu (τ = 37 333 hodin).

V prezentovaném případě bylo vyhodnocení provedeno na úrovni konfidence α = 0,95 a s použitím uvedených vztahů byla dolní mez střední doby do poruchy odhadnuta na hodnotu: $MTTF_L$ = 55 586 hodin (tj. 6,34 roku nepřetržitého svícení).

5. Vyhodnocení degradace LED s využitím výsledků zrychlených zkoušky

Charakteristickým rysem činnosti LED je postupná degradace světelného toku (viz Obr. 5). Proto se v technických aplikacích často pro LED stanovuje maximální akceptovatelná úroveň degradace (poklesu generovaného světelného toku), jejíž překročení signalizuje, že příslušná LED již neplní svoji funkci požadovaným způsobem. Překročení daného limitu je potom považováno za dosažení mezního stavu LED a vnímáno jako její porucha.

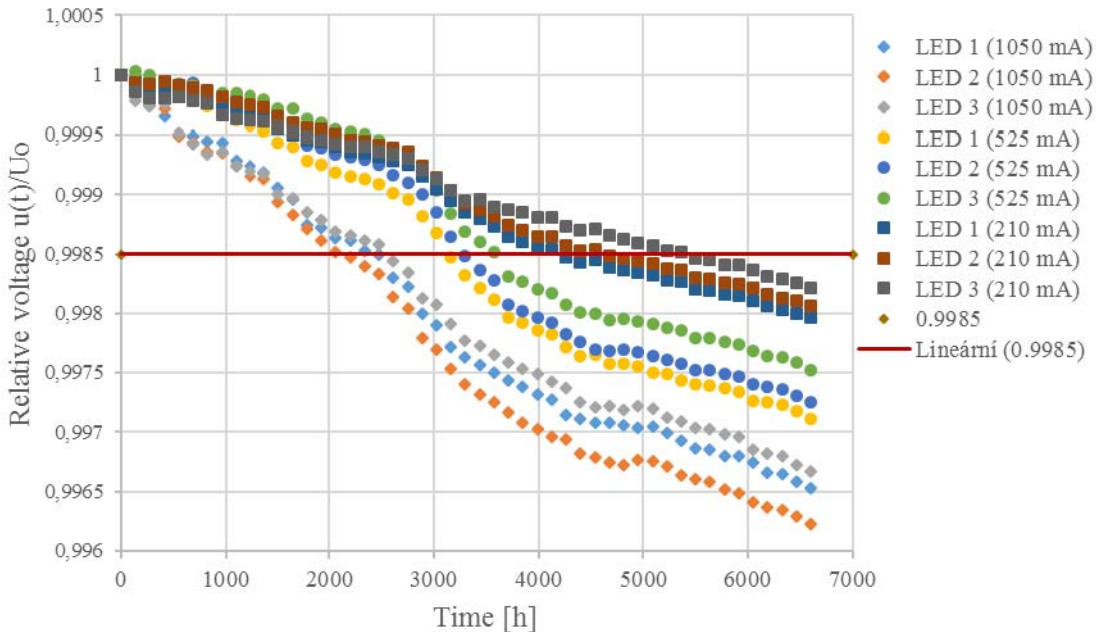


Obr. 5 Závislost světelného toku LED na době provozu

V rámci realizovaného experimentálního výzkumu byl, mimo jiné zkoumán vliv výkonového zatížení LED na její degradaci. To bylo zkoumáno tak, že od každého typu LED byly do zkoušky nasazeny tři sady LED a každá z nich byla zkoušena při aplikování jiné hodnoty proudu. Jedna sada byla provozována pří nominální proudové hodnotě (uvedené v technické specifikaci LED), druhá s proudem na úrovní 50 % nominální hodnoty a třetí sada s proudem na úrovni 25 % nominální hodnoty. Testovací aparatura byla navržena tak, že napájecí zdroj udržoval hodnotu proudu po celou dobu na konstantní úrovni. Degradace LED se pak v průběhu zkoušky projevovala poklesem napětí na jednotlivých LED.

Degradaci LED je tedy možné zprostředkovaně monitorovat měřením napětí na svorkách LED (při aplikaci konstantního proudu). V rámci provedeného experimentu tak byl průběžně sledován a automaticky zaznamenáván pokles napětí na svorkách jednotlivých LED. Na Obr. 6 je graficky znázorněn zaznamenaný pokles napětí na třech vybraných LED pro každou ze tří úrovní proudových zatížení. Z obrázku je patrné, že proudové zatížení zásadním způsobem ovlivňuje rychlost degradace.

Pro podrobnější posouzení byla zvolena jistá úroveň poklesu napětí na svorkách LED jako limitní hodnota a čas dosažení tohoto limitu byl u každé LED vyhodnocen jako čas do poruchy (viz Obr. 6).



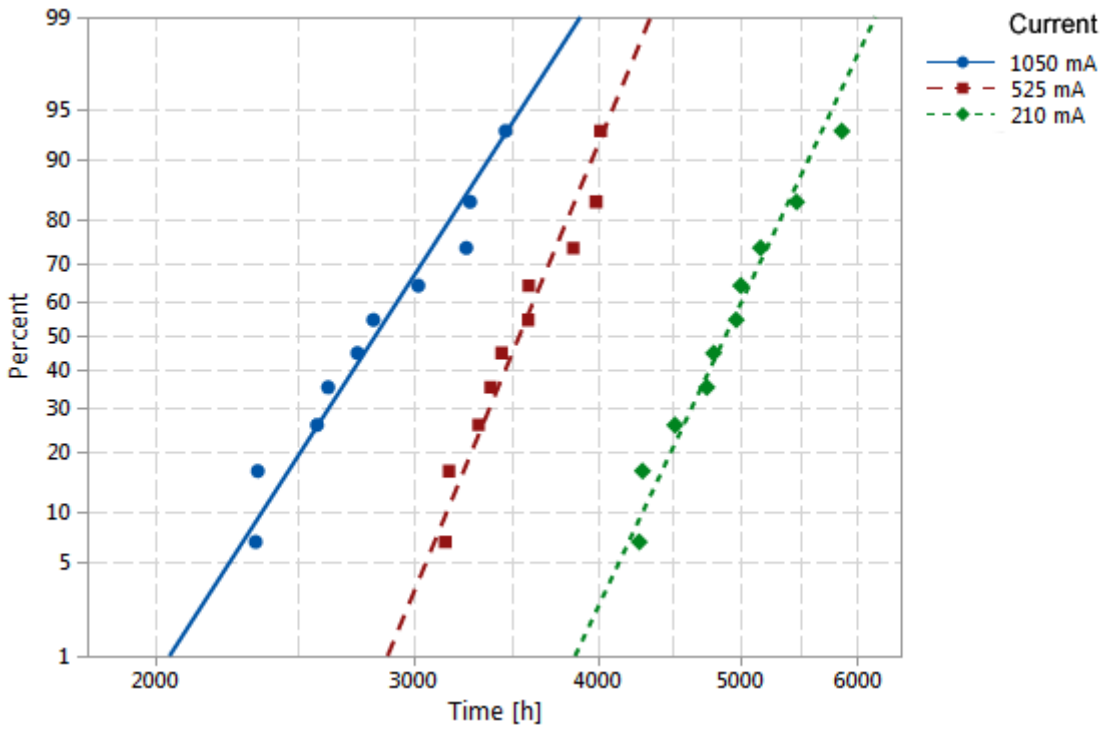
Obr. 6 Degradace LED v závislosti na čase a aplikovaném proudovém zatížení

V rámci popsaného experimentu byly zkoušeny 3 sady LED, každá s 10 kusy LED shodného typu. První sada byla napájena proudem 1050 mA (100 % nominální hodnoty), druhá sada proudem 525 mA (50 % nominální hodnoty) a třetí sada proudem 210 mA (25 % nominální hodnoty. U každé LED byl zaznamenán čas dosažení stanovené limitní hodnoty poklesu napětí na svorkách příslušné LED. Přehled zaznamenaných dob je uveden v Tabulce 3.

Tabulka 3 Přehled dob provozu LED do dosažení mezního stavu

Číslo LED	**Doba do poruchy [h]**		
	I_1 = 1050 mA	I_2 = 525 mA	I_3 = 210 mA
1	2339	3147	4263
2	2347	3165	4285
3	2575	3316	4408
4	2620	3378	4637
5	2643	3437	4789
6	2712	3582	4861
7	2917	3585	4896
8	3152	3844	5154
9	3172	3984	5452
10	3358	4012	5812

Získaná data byla podrobena statistické analýze, při které byl hledán vhodný typ rozdělení náhodné proměnné, kterou v tomto případě je doba do dosažení mezního stavu LED. Tento proces vyústil do závěru, že jako nevhodnější se jeví logaritmicko-normální rozdělení (viz Obr. 7).



Obr. 7 Logaritmicko-normální rozdělení dob do dosažení mezního stavu

Pro každou skupinu zkoušených LED potom byly s využitím známých postupů [4] stanoveny odpovídající parametry logaritmicko-normálního rozdělení a proveden odhad střední doby do dosažení mezního stavu pro jednotlivé úrovně proudového zatížení. Výsledky statistického zpracování jsou uvedeny v Tabulce 4.

Tabulka 4 Střední doba do dosažení mezního stavu

Zatěžující proud, I_s [mA]	**Střední doba do dosažení mezního stavu, L_s [h]**
1050	2846
525	3546
210	4902

Pokud začneme výsledky experimentu zkoumat z hlediska vlivu proudového zatížení LED na jejich životnost (střední dobu do dosažení mezního stavu), doporučuje odborná literatura v takovém případě využití inverzního mocninového zákona [5], jehož obecnou podobu lze vyjádřit vztahem:

$$L_S = \frac{C}{I_S^{\,n}} \tag{7}$$

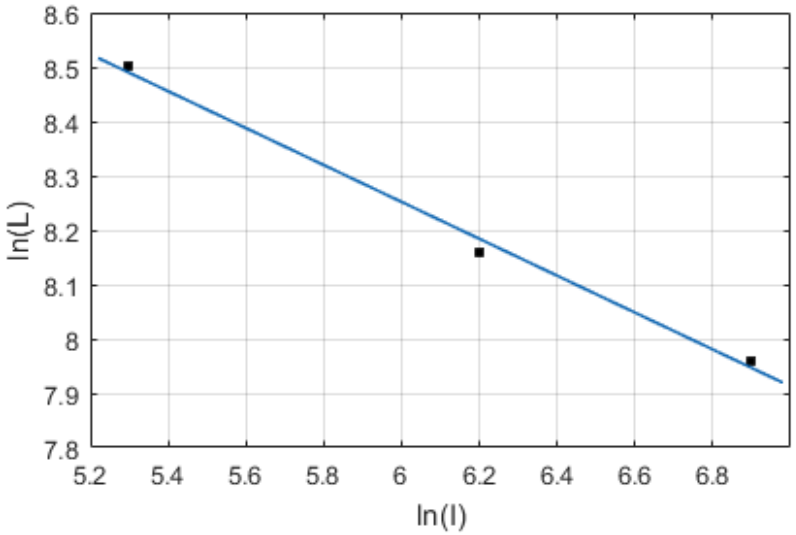
kde: L_S - střední doba do dosažení mezního stavu při proudovém zatížení I_S,

C, n - parametry rozdělení.

S využitím informací uvedených v Tabulce 4 lze odvodit, že v daném případě inverzní mocninový zákon platí v následující podobě:

$$L_S = \frac{30271}{I_S^{\,0,34}} \tag{8}$$

Graficky je tato závislost znázorněna v Obr. 8, kde je zřejmá velmi dobrá shoda s experimentálně určenými hodnotami střední doby do dosažení mezního stavu při třech sledovaných úrovních proudového zatížení LED.



Obr. 8 Závislost střední doby do dosažení mezního stavu na proudovém zatížení LED

S využitím rovnic (1) a (8) lze potom také odvodit vztah pro faktor zrychlení ve vztahu k proudovému zatížení:

$$A_I = \left(\frac{I_{Test}}{I_{Use}} \right)^{0,34} \tag{9}$$

kde: I_{Test} - proudové zatížení LED při zkoušce,

I_{Use} - proudové zatížení LED v běžném provozu.

Pokud tedy budeme v rámci zrychlené zkoušky LED současně uvažovat jak zatížení teplotou, tak i proudem, může být výsledný faktor zrychlení vyjádřen s ohledem na rovnice (3) a (9) vztahem:

$$A = A_T A_I = 2^{\frac{\left(T_{Test} - T_{Use}\right)}{10}} \left(\frac{I_{Test}}{I_{Use}} \right)^{0,34} \tag{10}$$

S využitím uvedeného vztahu lze potom určit faktor zrychlení pro libovolnou kombinaci tepelného a proudového zatížení (nepřekračující konstrukční limity LED). Případně lze také vztahu využít k přepočtu ukazatelů bezporuchovosti při změněně provozních podmínek.

6. Závěr

Předložený článek naznačuje možnosti využití zrychlených zkoušek při hodnocení bezporuchovosti elektronických systémů využívaných v konstrukci moderní vozidel. Přesto, že je zde řešena problematika zkoušek pro LED, lze prezentované metody a postupy efektivně přímo nebo v modifikované využívat i u jiných polovodičových prvků. Zvláště zajímavou možností je využití zrychlených zkoušek při monitorování a modelování různých forem degradace prvků.

Použitá literatura

[1] VALIŠ, D. Zrychlené zkoušky bezporuchovosti – základní principy a možnosti realizace. In: *Sborník z 39. setkání Odborné skupiny pro spolehlivost – Zrychlené zkoušky bezporuchovosti a možnosti jejich praktické aplikace*. Brno: Univerzita obrany, 2010, s. 1-20.

[2] GS 95003-1. *Electrical/Electronic assemblies in Motor vehicle, General information*. München: BMW Group Standard, 2010.

[3] ČSN IEC 60605-4 *Zkoušení bezporuchovosti zařízení – Část 4: Statistické postupy pro exponenciální rozdělení – Bodové odhady, konfidenční intervaly, předpovědní interval a toleranční interval.*

[4] ESCOBAR, L. A. and MEEKER, W. Q. *Statistical Methods for Reliability Data*. New York: John Wiley & Sons, 1998.

[5] ESCOBAR, L. A. and MEEKER, W. Q. A review of accelerated test models. *Statistical science*, Vol. 21(2006), No. 4, pp. 552-577.

Introduction to ISO 26262 and its limitations with regards to ADAS

Ing. Marek Hudec

Porsche Engineering Services, s.r.o., Praha

marek.hudec@porsche-engineering.cz

1. Introduction

It has been several years since the standard ISO 26262 was published as the main standard for functional safety – with the main focus on malfunctions of electric and/or electronic (E/E) systems – in the automotive industry in the year 2011. Nowadays (2019) the standard is heavily followed and respected in the automotive industry, offering much more automotive-specific approach in comparison with the predecessor and also parent standard IEC 61508. Furthermore, several improvements were made to the standard ISO26262, reflecting the needs of the industry, basically as improvements coming out of lessons learned in the practical usage of the standard. These improvements are introduced within the 2nd Edition of ISO 26262 released in the last year (2018). Even the scope of the standard was expanded to cover not only vehicles up to 3 500 kg (as in the 1st Edition of the standard), but to become valid for all series production vehicles of any mass and kind – such as passenger cars, motorcycles, trucks and buses. However the scope expansion is still limited to E/E system malfunction and poses a clear limitation regarding its application especially (but not only) in advanced driver assistance systems (ADAS). A brief overview of the automotive functional safety in terms of ISO 26262 as well as the above mentioned limitations are addressed in this article and shown on practical examples.

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]).

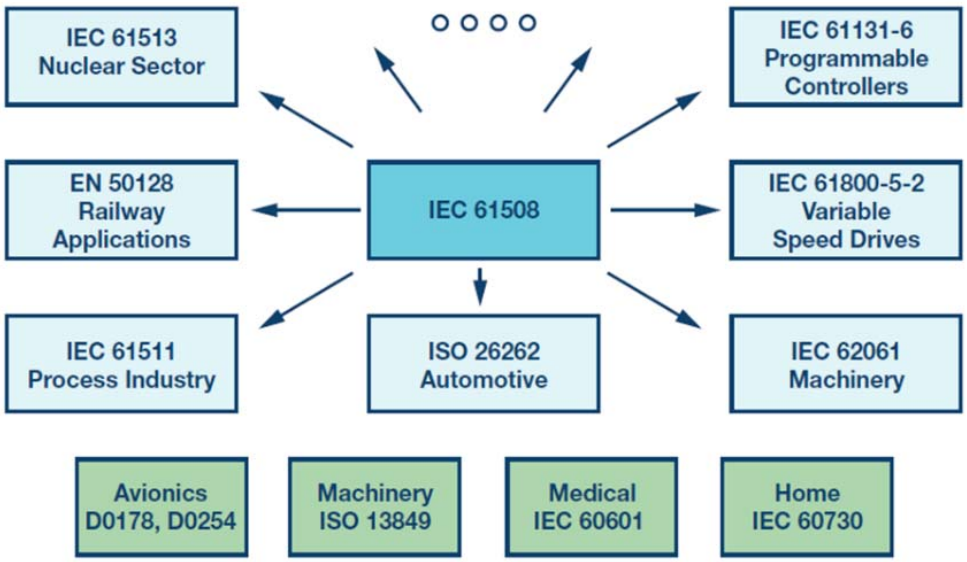


Figure 1: Relation of IEC 61508 to domain-specific standards for functional safety [5].

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. Due to the fact that 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 in order to create a functional safety concept, derived safety goals have to 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, in order 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.

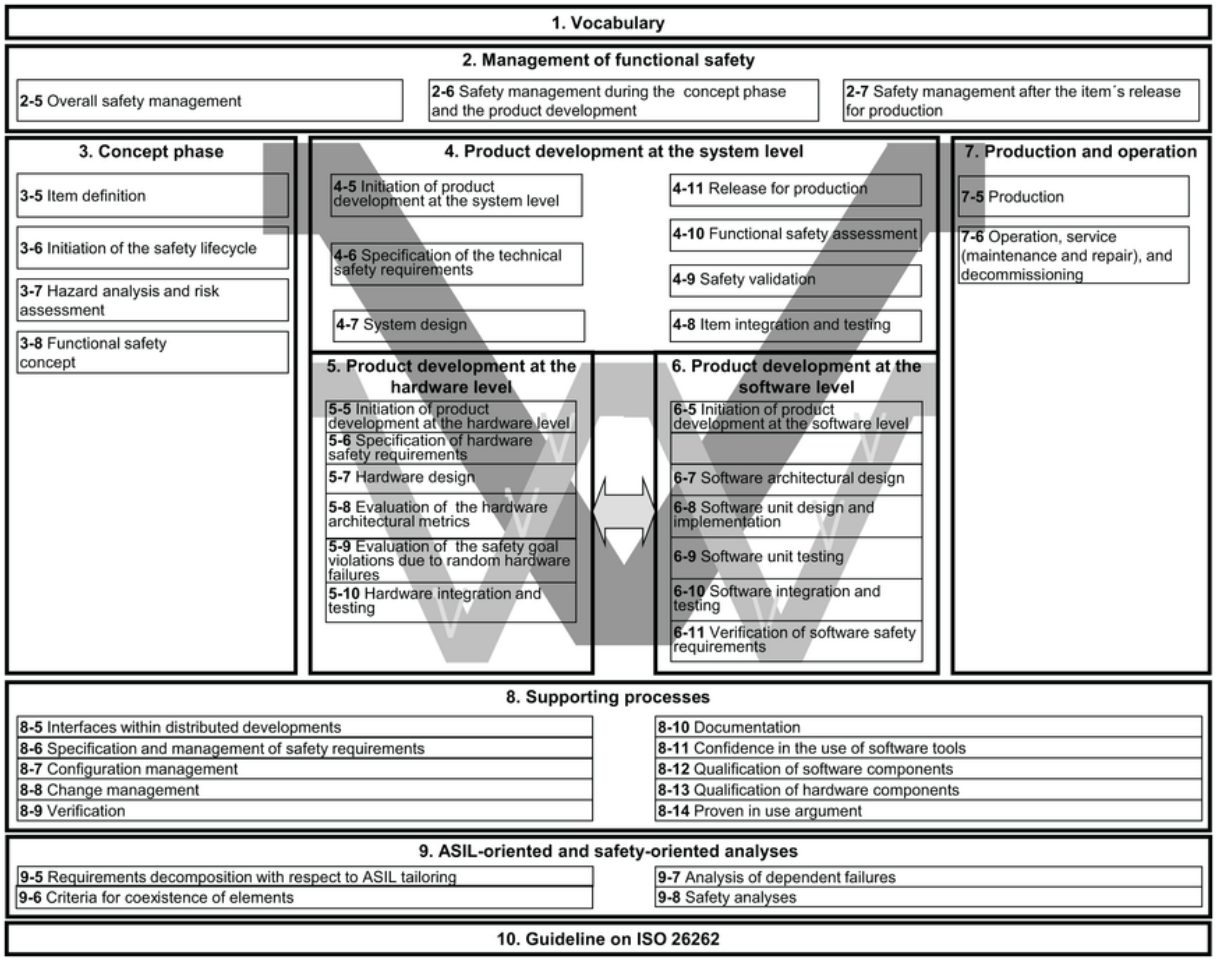


Figure 2: Structure of ISO 26262:2011 [2].

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 negligible in comparison with ASIL C or D. But regardless on the ASIL derived, for all ASILs it is absolutely 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).

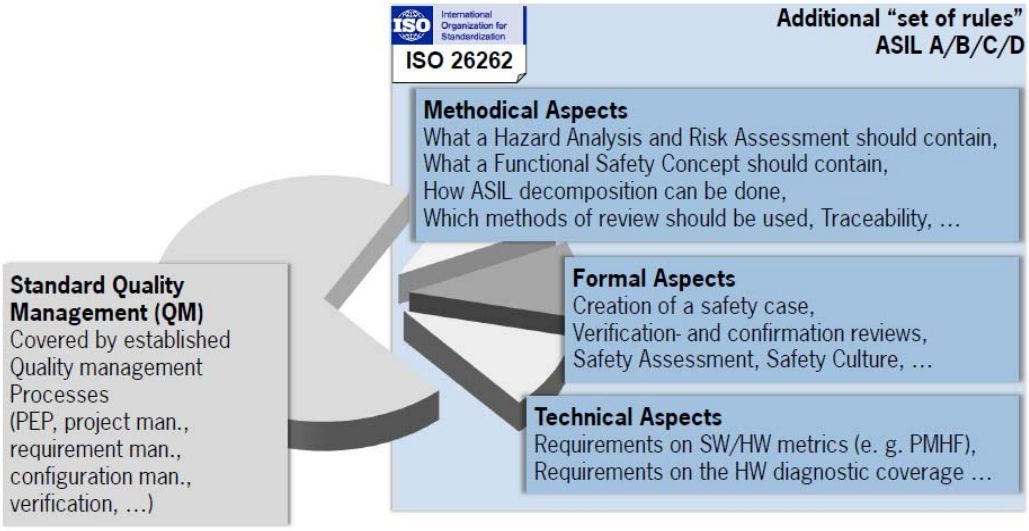


Figure 3: Means of risk reduction in the sense of ISO 26262 by considering additional "set of rules" during the development where effort to maintain these depends on the ASIL.

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

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 (top-level abstraction)

On the top level of abstraction, firstly so-called items are defined. These items comprise of one or more functions on the vehicle level (operable and perceivable by its user) which might be distributed across a number of systems (sensing, controlling or actuating). An example of a function might be car headlights, car wipers, a cruise control function or a stability control

function. A short and brief definition of the function and its systems is provided in a work product called item definition.

The functions defined in the item definitions are analyzed in a 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, in order 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, a 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 Part 4 of ISO 26262, which are described in the next clause of this chapter.

The derived safety goals as well as the functional safety requirements have to be validated on the right side of the V-model. For this purpose, 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 Functional safety on the system level (middle-level abstraction)

From the functional safety requirements derived in the FSC, technical safety requirements are derived, considering the system architecture (i. e. its sub-systems and/or components) up to the level of detail of individual HW or SW components. Although it is not clearly stated in ISO 26262 (improved however in the 2nd Edition of ISO 26262), this work product is commonly called as technical safety concept (TSC). It requires, similarly to the FSC, HW or SW monitoring and/or redundancies with the goal of prevention of the safety goal violation. In order to test the derived technical safety requirements, appropriate test cases are derived. These tests are typically carried out on the target HW such as HiL (hardware in the loop tests).

3.5 Functional safety on the component level (implementation)

On the level of individual components, the necessary safety activities depend on whether the component is a SW component or a HW component. For HW components, systematic as well random failures are relevant and both need to be prevented and/or detected. As an input for their detection and/or prevention, technical safety requirements allocated to HW are considered in the HW design (layout, selection of components, redundancies, etc.). The goal of their implementation and verification is to prevent safety-critical systematic failures and minimize safety goal violation due to random HW failures. Systematic failures are treated in the sense of additional (with regards to standard QM development) "set of rules" addressed by ISO 26262 considering reviews, testing, safety analyses (inductive, deductive), design and testing methods to be followed, etc. Random HW failures are reduced by implementation of monitoring mechanisms in the HW design or by employing SW to monitor certain HW elements, mitigating the number of undetected faults resulting in violation of the safety goals. Quantitative metrics are defined in ISO 26262 to measure the "level of mitigation" (see example of the target values in Figure 5).

ASIL	Random hardware failure target values
D	$<10^{-8}\ h^{-1}$
C	$<10^{-7}\ h^{-1}$
B	$<10^{-7}\ h^{-1}$
NOTE The quantitative target values described in this table can be tailored as specified in 4.1 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).	

Figure 5: Target values for random hardware failures leading to a violation of a safety goal rated with ASIL B, C or D [2].

For SW components, systematic failures have to be prevented only. Random failures are not introduced by pure SW components and are therefore not relevant for SW development. Similar to the HW design, systematic failures during the SW development are prevented by additional effort in terms of technical reviews, safety analyses, intensive testing on different levels (SW units, SW components or fully integrated SW), methods used for coding and testing, etc. Since all these mentioned requirements are addressed by common SW quality management standards (e. g. aSPICE), large overlaps with established QM processes might exist. This fact again emphasizes the necessity of established QM processes in a company carrying our safety-related developments.

3.6 Supporting processes and ASIL decomposition as per ISO 26262

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. These are however very similar or even referenced to other quality management standards.

Furthermore, ISO 26262 allows ASIL decomposition on any level of development (vehicle, system or component in the sense of this article). For that purpose, independence between the decomposed systems has to 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 has to be given), see Figure 6.

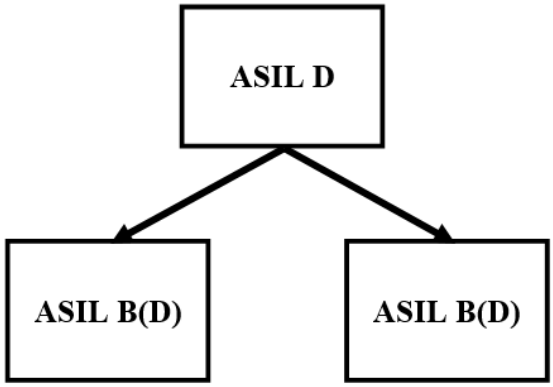


Figure 6: Example of an ASIL decomposition according to ISO 26262 Part 9.

3.7 Scope expansion in the 2nd Edition of ISO 26262 published in 2018

ISO 26262 was slightly adjusted and extended by the publication of its 2nd Edition in December 2018. This main extension is its validity also for vehicles over 3 500 kg and motorcycles. That means, that ISO 26262:2018 is valid for mass produced motorcycles, passenger cars, trucks and buses. For the application in the motorcycle development, ISO 26262:2018 keeps the same framework as for passenger cars. However in the HARA, MSILs (motorcycle safety integrity levels) instead of ASILs are derived. Nevertheless, MSILs are afterwards converted to ASILs (the conversion leads to reduction by one integrity level, see Figure 7) and ASIL safety goals and/or safety requirements are followed in the development. ASILs are also kept for the functional safety in trucks and buses, only additional guidance (for example with regards to the situation analysis in the hazard and risk analysis) is provided, but the framework remains.

MSIL D	ASIL C
MSIL C	ASIL B
MSIL B	ASIL A
MSIL A	QM
QM	QM

Figure 7: Mapping of MSIL to ASIL [3].

Further adjustments are focused on effectiveness of reviews and safety assessments. For example, in ISO 26262:2018 impact analyses are scope of an independent review, whereas in ISO 26262:2011 no such requirement exists, even though a whole project might be impacted (i.e. in worst case necessary safety activities not executed) by wrong assumptions in the impact analyses.

4. Limitations of ISO 26262

4.1 Scope of ISO 26262 and its limitations

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. Considering the fact that 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. In the next clause, the reason is shown based on one practical example.

4.2 Practical example

As a practical example of the limitations of ISO 26262, a simple system called "emergency brake" (only an imaginary example) that should possibly bring more safety to the automotive sector can be presumed. The "emergency brake" system might have a following functional definition: in case the vehicle speed is over 30 km/h and an object is detected in front of the vehicle with a distance smaller than the possible vehicle braking distance (at full deceleration on a dry road), full deceleration shall be activated independent on the driver input). The system could be composed e. g. by the following components: distance sensor, control unit and a brake actuator, see Figure 8.

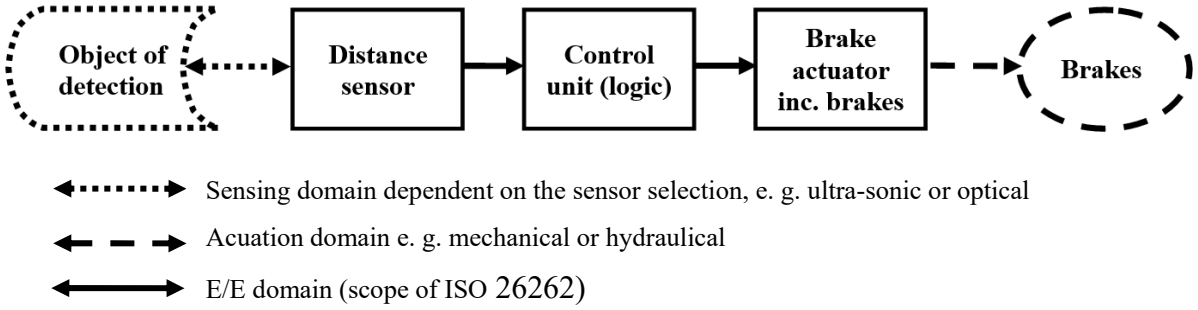


Figure 8: Example of a system implementing an "emergency brake" function.

The functional safety would now analyze every possible malfunction of the E/E system, focusing on prevention and/or detection of failures and prevention of violation of safety goals. Such safety goals might be for example: avoid erroneously triggered emergency braking (ASIL D), avoid missing emergency braking (QM). The overall safe state of the system (obvious due to criticality of the ASIL D safety goal) would be degradation or deactivation of the function, informing the driver. For the fulfillment of safety goals, safety requirements will be derived and implemented during the development, addressing for example the following failures: detect failure of analog/digital convertor in the distance sensor (requirement on the sensor), degrade the function in case of failure and warn the driver about non-availability of the function (requirement on the logic and the driver display unit).

Having the E/E system analyzed by the application of ISO 26262 and thus "free of" insufficient risks resulting from malfunctions of the E/E system, obviously further risks outside of the ISO 26262 scope are present in the system design. These are however not true malfunctions, but rather system design insufficiencies caused by the limitations of the components selected during the design. One example might be a wrongly detected object due to either weather conditions (e. g. heavy rain, fog etc.) or object that is actually present, but should not be evaluated as hazardous (e. g. flying plastic bag), misleading the decision algorithm and producing erroneous triggering of the emergency brake. The function design has to encounter and consider such limitations and for example degrade the function in case of heavy rain or when the sensor is covered by snow. Or a different way of sensing has to be selected, or it can be found insufficient to select one sensing technology only, so a sensor cluster have to be selected – comprising different sensing technologies (e. g. optical and ultra-sonic). In this example, not only the distance measurement is affected by the scope of the classical functional safety approach. Also the design of the speed measurement chain is not fully in the scope of ISO 26262 – it surely makes a difference if the speed is calculated based on the motor revolutions, wheel speeds or GNSS (global navigation satellite system, e. g. GPS) signals. Each of the sources certainly has performance limitations (motor might not be running, wheels might be slipping, GNSS might lose connection) which have essential impact on the function design and in the end also safety of the intended function.

It was shown on a practical example, that the safety scope of ISO 26262 is limited, especially with regards to design limitations. This is a publicly known issue and solutions are being sought in a prioritized manner, mainly due to emerging ADAS including autonomous driving systems. One example of the priority is publication of a new standard, which is actually still a draft, but made publicly available as ISO/PAS 21448 (PAS = public available specification) aimed for feedback collection resulting from practical usage "trials" in the automotive industry. The next clause of this chapter provides a brief summary with regards to the ISO/PAS 21448.

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

The SOTIF (safety of the intended functionality) standard under development was released as a public available specification early this year (2019). It mainly addresses 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 probably 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 "sleeping" 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. This fact is also reflected in the process flowchart of ISO/PAS 21448 (see Figure 9), where iterations (or loops) are proposed, very different to the framework of ISO 26262 where the classical approach based on V-model is used (see Figure 2). The iterations in the sense of the SOTIF standard aim at a continuous improvement of the intended functional design described by its various specifications. These iterations are strongly supported by verification and validation activities, pushing the development limits to identify all possible unknown hazardous events.

The iterative approach might be a challenge for the current way of development in the classical V-model sense, especially in distributed developments with various parties and long supplier chains. Therefore, it might be beneficial to rethink the processes in order to provide flexibility for such iterations. Such methods already exist in other industries, e. g. some of the agile development methods might be suitable.

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 have to be used in addition to ISO 26262, in order 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.

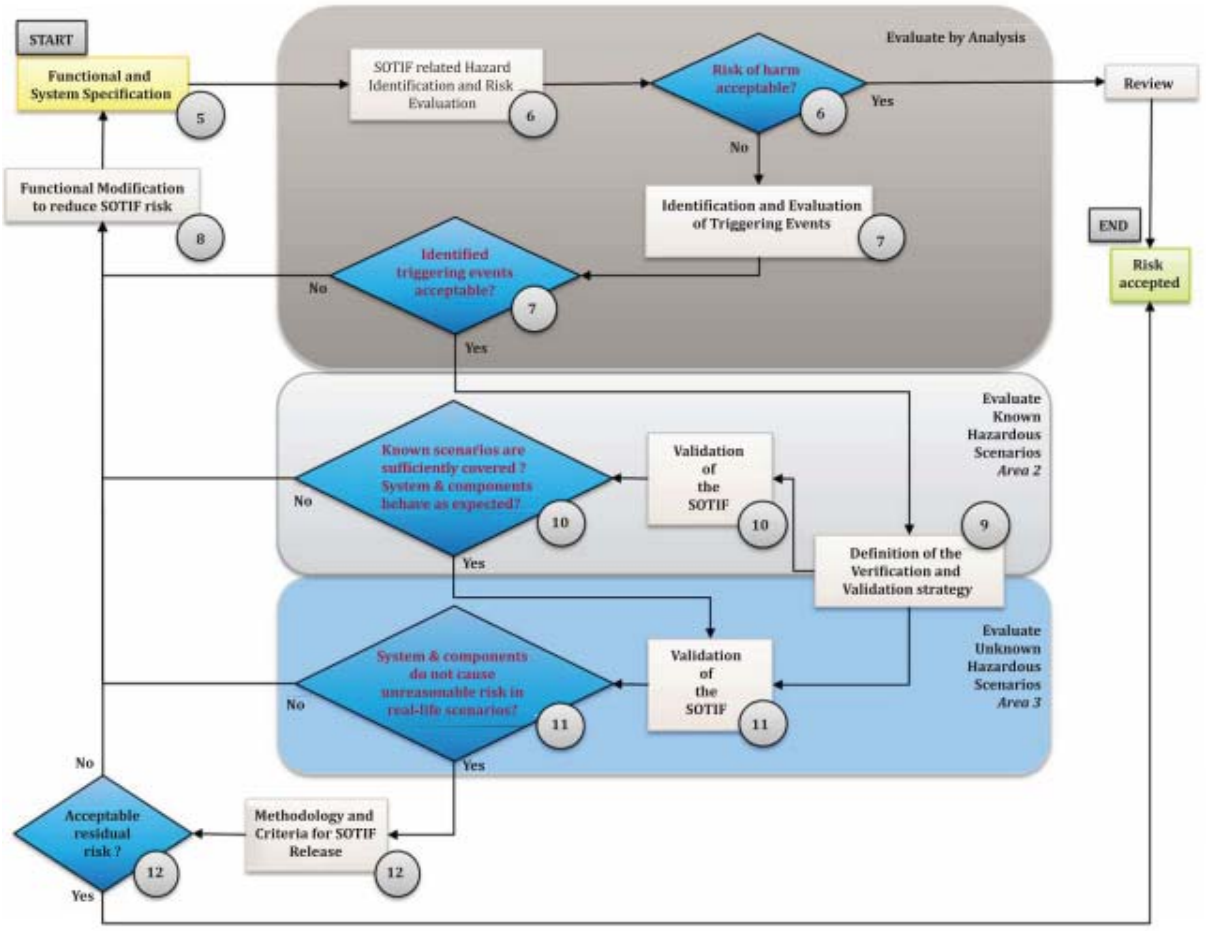


Figure 9: Process flowchart of ISO/PAS 21448 its numerous iteration cycles [2].

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)

Název:	Aplikované techniky spolehlivosti v automobilovém inženýrství
Autoři:	Kolektiv
Vydavatel:	Univerzita Obrany v Brně
Položka EP:	26/2019/2F
Tisk:	Oddělení vydavatelství a správy studijních fondů UO, Brno
Číslo zakázky:	
Náklad:	30 ks
Počet stran:	30
Rok vydání:	2019
Vydání:	první

Publikace neprošla jazykovou úpravou

ISBN 978-80-7582-102-7