ČESKÁ SPOLEČNOST PRO JAKOST

Nejčastější mýty ve spolehlivosti

Materiály z 66. semináře Odborné skupiny pro spolehlivost,
konaného dne 7. 2. 2017 v Praze

Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1, www. csq.cz

Obsah

Nejčastější chyby v terminologii spolehlivosti

Ing. Jan Kamenický, Ph.D.

Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií, Studentská 2, Liberec 461 17

e-mail: jan.kamenicky@tul.cz, http://osr.mti.tul.cz

Abstrakt

Při specifikování požadavků na spolehlivost objektu je vhodné, ne-li nezbytné, aby všechny strany, které s těmito požadavky přijdou do styku, mluvili jednotným jazykem a pod jednotlivými pojmy chápali stejné parametry. Z tohoto důvodu vznikl Mezinárodní elektrotechnický slovník, Část 192: Spolehlivost [1]. Přesto v reálném životě nastávají situace, kdy terminologie není dodržována. V takových případech mohou nastat dvě možnosti - A) obě strany znají a používají termín, odlišný od normalizovaného a domluví se spolu nebo B) jedna strana v dobré víře použije nesprávný termín, ovšem strana druhá se bude striktně držet standardizované terminologie a potom dojde k neporozumění a často i k soudním sporům. Příspěvek si neklade za cíl popsat vyčerpávajícím způsobem všechny nejasnosti v terminologii, spíše chce popsat možné typy neporozumění a podat k nim vysvětlení.

1 Nejčastější chyby v terminologii spolehlivosti

Spolehlivost vs. Pohotovost

V textu příspěvku Odborné skupiny pro spolehlivost se samo nabízí uvést nejprve na pravou míru, co je to *spolehlivost*. *Spolehlivost* je definována jako „schopnost fungovat tak, jak je požadováno, a tehdy, když je to požadováno“. Proto je zcela zcestné ptát se, jak hodně je nějaké zařízení spolehlivé, protože tato vlastnost není kvantifikovatelná, minimálně ne jedním číselným ukazatelem. Mnoho lidí si myslí, že terminologicky správnější a tím pádem odbornější je bavit se o *pohotovosti*, kterou již podle nich je možné vyjádřit číselně. Co se však píše v [1]? *Pohotovost* je „schopnost objektu být ve stavu, kdy funguje tak, jak je požadováno“. Tedy pozor, *pohotovost* je opět vlastnost! Ovšem je pravda, že pohotovost lze kvantifikovat pomocí různých ukazatelů, viz dále.

Pohotovost vs. Funkce okamžité pohotovosti vs. Ustálená pohotovost

Jak bylo popsáno výše, v běžné praxi se pojem *pohotovost* používá spíše pro popis číselného vyjádření pravděpodobnosti, že objekt funguje. Toto je vlastně definice *funkce okamžité pohotovosti*, která přesně zní: „pravděpodobnost, že objekt je ve stavu, kdy v daném okamžiku funguje tak, jak je požadováno“. Samozřejmě, pokud se ztotožníme s provozovatelem nějakého zařízení, zajímá nás právě tato hodnota, protože nám říká, jaká je šance, že stroj bude fungovat, když to budeme potřebovat. Ovšem je třeba si uvědomit, že takováto hodnota je vztažená pouze k danému okamžiku a tedy je vhodné ji používat pouze pro objekty, které nepracují v nepřetržitém režimu. Vysvětlení je jednoduché - okamžitá pohotovost je důležitá u zařízení, která čekají na vyžádání funkce, jako jsou např. záložní čerpadla nebo zabezpečovací zařízení.

Oproti tomu u zařízení, která pracují v nepřetržitém režimu vyžádání, je vhodné udávat tzv. *ustálenou pohotovost*. Ta je definována jako „limita, existuje-li, funkce okamžité pohotovosti, když se doba blíží nekonečnu. Proto pokud budeme uvažovat o nepřetržitém používání nějakého zařízení, právě hodnota *ustálené pohotovosti* nám řekne, jaký je poměr mezi dobami

použitelného a nepoužitelného stavu objektu. Tím je mj. také dáno, kolik procent času bude nutné věnovat údržbě zařízení. Je však nutné mít na zřeteli, že doba údržby zařízení závisí na dvou faktorech; na ochotě zařízení nechat se udržovat, tzv. *udržovatelnost* objektu a na schopnosti organizace objekt udržovat, tzv. *zajištěností údržby*. Je tedy zřejmé, že *okamžitou* i *ustálenou pohotovost* je možné ovlivňovat právě údržbou.

Dostupnost vs. Pohotovost

Termín *dostupnost* je v praxi často používán pro označení pravděpodobnosti, že je objekt v provozuschopném stavu. Názvoslovná norma 60050-192 [1] však tento termín vůbec nezná. Významově nejblíže jsou *dostupnosti* ukazatele *pohotovosti*, které byly zmíněny v předchozí kapitole. Zde pouze pro upřesnění uveďme, že *pohotovost*, resp. *nepohotovost*, v teorii spolehlivosti označovaná jako *A*, resp. *U*, bývá běžně počítána podle následujících vztahů:

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

$$U = \frac{MTTR}{MTBF + MTTR} \qquad (2)$$

Pokud se však budeme striktně řídit normalizovanými výrazy [1], potom vztah pro *ustálenou pohotovost* je obsažen v poznámce 1 k heslu 192-08-07 *ustálená pohotovost* jako podíl *střední doby použitelného stavu* a součtu *střední doby použitelného stavu* a *střední doby nepoužitelného stavu*. Vyjádřeno vzorcem dostáváme:

$$A = \frac{MUT}{MUT + MDT} \qquad (3)$$

Analogicky pro *ustálenou nepohotovost* platí:

$$U = \frac{MDT}{MUT + MDT} \qquad (4)$$

Jaký je však rozdíl mezi vztahy, používanými v praxi a těmi normovanými? Opět se budeme držet výkladu názvoslovné normy spolehlivosti [1] a pokusíme se objasnit význam jednotlivých členů všech vzorců. Nejprve však uveďme definice jednotlivých výrazů.
MTBF je definována jako „očekávaná hodnota doby provozu mezi poruchami“,
MTTR je definována jako „očekávaná hodnota doby do obnovy“,
MUT je definována jako „očekávaná hodnota doby použitelného stavu“ a

MDT je definována jako „očekávaná hodnota doby nepoužitelného stavu“.

Pro objasnění rozdílu porovnejme nejprve *MTBF* a *MUT*. Rozdíl spočívá zejména ve skutečnosti, že *MTBF* předpokládá, že stroj skutečně pracuje, tj. vykonává funkci, zatímco *MUT* operuje se skutečností, že objekt je schopen fungovat (ale např. nejsou zabezpečeny vnější zdroje, není požadována jeho funkce atp.). Oba ukazatele jsou tedy totožné, pouze pokud zařízení využíváme nepřetržitě a zabezpečujeme mu podmínky pro úspěšné plnění funkce.

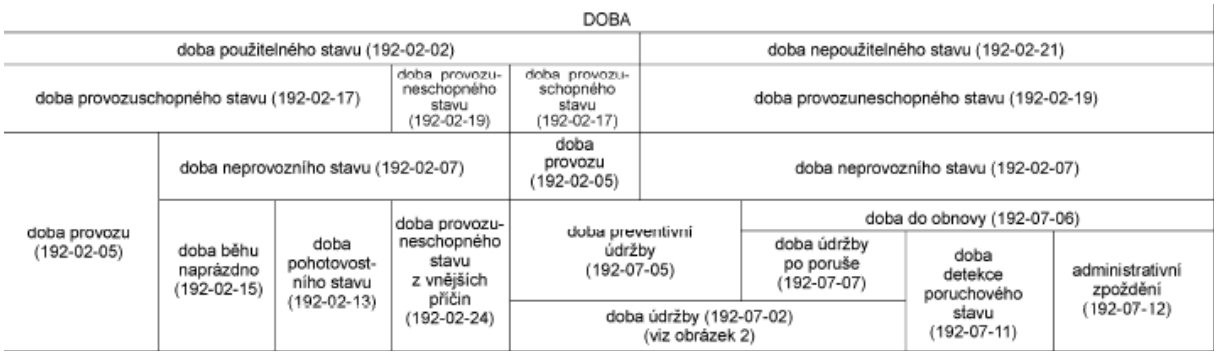
Při detailnějším pohledu na rozdíl mezi *MTTR* a *MDT* lze konstatovat, že *MTTR* v sobě zahrnuje celkovou dobu od výskytu poruchy až do obnovení funkce. Bohužel tato doba není ve většině případů závislá pouze na zkoumaném objektu, ale patří do ní *doba údržby po poruše*, *doba detekce poruchového stavu* a *administrativní zpoždění*, a proto by logicky neměla být používána pro popis vlastností objektu. *MDT* oproti tomu v sobě kumuluje pouze dobu „kdy objekt není schopen fungovat tak, jak je požadováno, v důsledku vnitřního poruchového stavu nebo preventivní údržby“. Proč však došlo k tomu, že praxe používá zástupné hodnoty? Podle názoru autora je to dáno tím, že hodnoty *MTBF* a *MTTR* jsou v praxi snáze dostupné, než hodnoty *MUT* a *MDT*. Kromě toho vlastníka (provozovatele) zařízení zajímá reálná doba, kdy bude zařízení opět fungovat, tudíž do *doby nepoužitelného stavu* zahrnují i doby na dodání náhradních dílů, vlastní opravu, čekání na volného údržbáře atp. Této hodnotě je potom bližší právě *MTTR*.

Porucha vs. Poruchový stav

Porucha je v [1] definována jako „ztráta schopnosti fungovat tak, jak je požadováno“. *Poruchový stav* je tamtéž definován jako „neschopnost fungovat tak, jak se požadováno, v důsledku vnitřního stavu“. Tato dvojice termínů patří v běžné praxi k těm, kdy všichni zúčastnění mluví o odlišném termínu, ale domluví se spolu. V praxi všichni mluví o *poruše*, ovšem mají na mysli *poruchový stav*. Pro vysvětlení uveďme, že o *poruše* se mluví zejména v souvislosti s jejími příčinami a následky. Pokud mluvíme o příčinách, pak správně používáme termín *porucha*, protože zjišťujeme, jaké jsou kořenové příčiny poruchy, tedy co způsobilo např. výpadek stroje. Je třeba si uvědomit, že *porucha* je jevem, tedy něčím, co nemá žádnou dobu trvání, jedná se o přechod objektu ze stavu použitelného do stavu nepoužitelného, resp. poruchového. A už tady nastává drobný rozpor v termínech. Nepoužitelný stav totiž může nastat i v důsledku pravidelné preventivní údržby. *Poruchový stav* je ovšem něčím, co má i časovou osu své existence. Takže pokud se bavíme o následcích poruchy, často jimi rozumíme i následky *poruchového stavu*. Těmito následky bývá zejména ztráta produkce, což je dominantní složka následků. Přesto lze konstatovat, že i když se v praxi bavíme o následcích *poruchy*, myslíme tím i následky *poruchového stavu* a nedochází k nepochopení.

Preventivní údržba vs. plánovaná údržba

Možná záměna těchto dvou termínů spočívá ve skutečnosti, že si mnoho lidí stále neumí představit jinou, než časově plánovanou preventivní údržbu. Přitom podle definice je *preventivní údržba* jakákoliv „údržba prováděná ke zmírnění degradace a snížení pravděpodobnosti poruchy“, tedy se může jednat i o *údržbu podle stavu*, *odloženou údržbu*, atd. Oproti tomu *plánovaná údržba* je „údržba prováděná v souladu se specifikovaným časovým plánem“. Kdo tedy chápe *preventivní údržbu* pouze jako *plánovanou údržbu*, dopouští se omezení významu tohoto pojmu. Ještě jedna otázka k zamyšlení - *plánovaná údržba* nemůže být podle [1] plánována jinak, než podle časového plánu. Tím je ovšem omezeno plánování údržby podle najetých kilometrů, vytěžených barelů, vyrobených kusů atp. I toto plánování se ale v praxi běžně používá a bývá označováno za *plánovanou údržbu*. Velmi dobře jsou doby, týkající se provozu a údržby, zpracovány v [1], viz obrázek 1.



Obrázek 1: Doby týkající se provozu a údržby [1]

Životnost vs. Užitečná doba života

Oba pojmy se týkají doby, po kterou se předpokládá používání objektu. Pojem *životnost* se ve své definici na *užitečnou dobu života* odvolává, když tato zní „schopnost fungovat tak, jak je požadováno, v daných podmínkách používání a údržby do konce užitečné doby života“. Z tohoto vyplývá, že *životnost* není kvantifikovatelná, nýbrž jedná se, jako v případě *spolehlivosti*, o obecnou vlastnost, kvantifikovanou mj. i *užitečnou dobou života*. Ovšem i *užitečná doba života* má určité nedokonalosti. V definici *užitečné doby života*, která zní „časový interval od prvního použití do doby, kdy již nejsou požadavky uživatele nadále plněny z důvodu hospodárnosti provozu a údržby nebo z důvodu zastarání“ není exaktně zakotvena hranice, která by jednoznačně identifikovala konec *užitečné doby života*. Naopak, je velmi dobře možné, že hranice *užitečné doby života* bude pro každého provozovatele jiná, protože závisí na plnění požadavků uživatele. *Z* tohoto důvodu je nemožné přesně specifikovat oba popisované parametry, což vede mj. k tomu, že *životnost*, resp. *užitečná doba života* není právně vymahatelná ani v případě, že je ukotvena ve smluvním vztahu mezi dodavatelem a odběratelem.

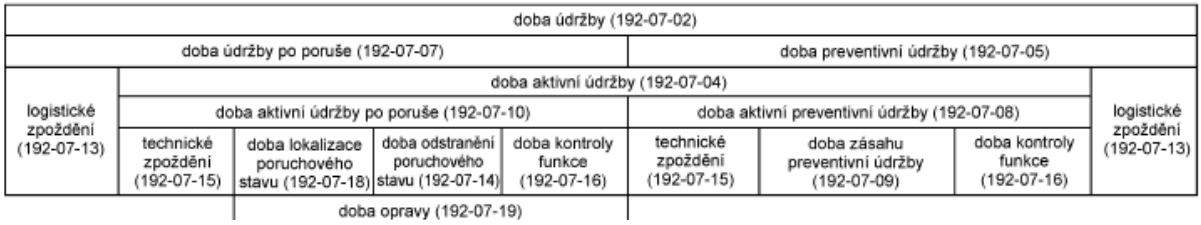
Bezporuchovost vs. Pravděpodobnost bezporuchového provozu

V případě těchto dvou pojmů je situace podobná, jako u *pohotovosti* a *funkce okamžité pohotovosti*. *Bezporuchovost* je totiž vlastnost objektu, konkrétně se jedná o „schopnost fungovat v daných podmínkách během daného časového intervalu bez poruchy tak, jak je požadováno“. Zajímavý na této definici je fakt, že definice bezporuchovosti není splněna i v situaci, kdy objekt bez problémů plní svou funkci, ale došlo na něm k nějaké poruše. Další nejistotou v uvedené definici jsou „dané podmínky“. Znamená to, že dvě naprosto totožná zařízení mohou dosahovat rozdílných ukazatelů bezporuchovosti právě v závislosti na tom, jakým způsobem jsou objekty využívány (doba provozu, úroveň namáhání, ale i preventivní údržba). Pro úplnost doplňme ještě definici *pravděpodobnosti bezporuchového provozu*, která zní „pravděpodobnost fungování za daných podmínek v časovém intervalu (t_1, t_2) tak, jak je požadováno“. Touto pravděpodobností se tedy kvantifikuje obecná vlastnost objektu, *bezporuchovost*. Nicméně v praktickém životě se běžně oba pojmy chápou stejně. Poslední poznámkou k pojmům, týkajícím se *bezporuchovosti*, je skutečnost, že časový interval může být udáván i v jiných jednotkách, než je kalendářní čas, resp. doba. V závislosti na charakteru objektu se může udávat např. v ujetých kilometrech, počtu sepnutí, provozních cyklech, aj.

Z historického hlediska budiž uvedeno, že anglický termín pro *bezporuchovost*, tedy *Reliability*, byl v minulosti používán pro *spolehlivost*, a proto se ještě v dnešní době občas oba termíny pletou, zejména v případě neodborných překladů spolehlivostních textů.

Udržovatelnost vs. Zajištěnost údržby

Pojmy *udržovatelnost* a *zajištěnost údržby* nepatří mezi ty, které se ve spolehlivosti často pletou. Ovšem do textu příspěvku byly zařazeny z toho důvodu, že si málo lidí uvědomuje jejich vzájemnou provázanost. Provozovatelé zařízení často berou nějaké zařízení jako problémové z toho důvodu, že na něj jsou např. nesnadno k sehnání náhradní díly, je potřeba speciální nářadí atp. Tím ovšem takovému zařízení nespravedlivě zhoršují spolehlivostní charakteristiky. *Udržovatelnost* je totiž vlastnost objektu, podle [1] jde o „schopnost objektu v daných podmínkách používání a údržby být udržen ve stavu nebo být navrácen do stavu, kdy funguje tak, jak je požadováno“, zatímco *zajištěnost údržby* je „efektivnost organizace s ohledem na podporu údržby“. Je tedy zřejmé, že pokud organizace nebude schopná zajistit potřebné zdroje pro správnou údržbu a funkci objektu, potom se to podepíše nejen na delší *době do obnovy*, ale i na zpoždění, předcházejícím vlastní údržbě, jak je zřejmé z obrázku 2 [1]. Stejné zařízení tedy bude mít různé spolehlivostní ukazatele v závislosti na organizaci, která ho provozuje.



Obrázek 2: Doby údržby [1]

2 Zamyšlení nad pojmem „kritičnost“

Motivací tohoto textu byly časté dotazy pracovníků vedení na to, jak zefektivnit proces optimalizace údržby. Nosnou myšlenkou managementu bylo, že na dražších komponentách je možné více ušetřit, proto by se mělo začít s úpravou plánu údržby u nich. V průběhu finančního ohodnocování jednotlivých strojů se však přišlo na to, že dražší stroje mají většinou vyšší všechny složky svých nákladů (pořizovací cena, náklady na provoz, náklady na údržbu, vliv na navazující technologii, atd.). Kromě toho tato dražší zařízení mají většinou i propracovanější systém údržby, a tedy že není snadné tyto náklady dále snižovat. Otázkou však nadále zůstává, jak definovat kritičnost zařízení tak, aby podle jednoho ukazatele bylo možné rozhodnout o potenciální neefektivnosti zařízení a tím o jeho vhodnosti pro zařazení do optimalizačního procesu. Protože je příspěvek inspirován zkušenostmi z praxe, jsou také všechna kritéria vztahována k možnosti finanční úspory změnou systému údržby.

V úvodu dokumentu je vhodné zmínit i pojem „riziko“, které je pro účely tohoto článku chápáno obecně jako kombinace finančního vyjádření ztráty z důsledku poruchy a četnosti této poruchy. Pro umožnění porovnání různých rizik je nezbytné převést riziko na shodnou časovou jednotku, kterou bude pro naše potřeby jeden rok. Roční riziko tedy bude mít fyzikální rozměr [Kč/rok].

Kritičnost standardizovaná

Podle Mezinárodního elektrotechnického slovníku, Část 192: Spolehlivost je *kritičnost* „závažnost účinku poruchového stavu nebo poruchy s ohledem na specifikovaná kritéria poruchy“. Z této definice vyplývá, že prvek (stroj, komponenta, výrobní linka, ...) nemusí mít pouze jednu kritičnost, nýbrž že kritičnost závisí na *specifikovaných kritériích poruchy*. Další podstatnou skutečností, kterou lze z definice vyčíst, je fakt, že do velikosti kritičnosti se promítne nejen samotná *porucha* (tedy jev, kdy se zařízení porouchá), ale i *poruchový stav* komponenty (tedy v prvé řadě doba, po kterou bude prvek v poruchovém stavu; dále pak

náklady na odstranění poruchového stavu aj.) Pojďme se nyní pokusit popsat různé pohledy na *kritičnost*.

Kritičnost první - bezpečnostní

V současné době se stalo velmi módním úsloví „safety first“, česky řečeno „bezpečnost až na prvním místě“. Jistě nebudeme rozporovat, že zařízení musí být bezpečné, ovšem stanovení úrovně bezpečnosti je otázkou více faktorů. V prvé řadě jde o interakci stroje s člověkem - u bezobslužných strojů nehrozí poškození zdraví nebo života obsluhy během standardního provozu. Jiná situace nastává při údržbě, kdy musí dojít ke kontaktu člověka se strojem. Je to ale kontakt na časově omezenou dobu, navíc často jde o kontakt s „mrtvým“ strojem, jehož energie jsou odpojeny. Úroveň bezpečnosti je dále podle ČSN 13849 definována závažností potenciálního zranění a možností vyhnout se nežádoucí události. Závažnost zranění jde ovlivnit jen těžko, ovšem možnost vyhnout se zranění je ovlivnitelná např. použitím osobních ochranných pomůcek, vhodným označením nebezpečných částí stroje nebo administrativním opatřením, např. sepsáním kvalitního návodu k obsluze/údržbě. Tím je vlastně řečeno, že bezpečnostní kritérium při stanovení kritičnosti zařízení musíme brát v úvahu, ovšem je ovlivnitelné i jinak, než údržbou, a proto je obtížné pomocí tohoto kritéria rozhodovat o zařazení zařízení do plánů optimalizace údržby.

Jinou otázkou zůstává, kolik financí je nutné, resp. vhodné investovat do bezpečnostních opatření daného zařízení. Provozovatel má povinnost eliminovat všechna bezpečnostní rizika, ovšem pouze pokud je to technicky možné a ekonomicky odůvodnitelné. Není předmětem tohoto příspěvku zabývat se otázkou ekonomického ohodnocení zdravotních rizik, plynoucích z provozování jakékoliv technologie, ale neodpustím si poznámku, že nebezpečí zranění nelze u většiny strojů zcela eliminovat, zůstávají tzv. zbytková rizika. A je čistě věcí managementu, jak vysoká tato rizika budou - samozřejmě za dodržení legislativních opatření.

Stejná situace, jako byla popsána v oblasti bezpečnosti, je v případě, že zařízení ohrožuje svým provozem nebo poruchovým stavem životní prostředí. Jistě každý provozovatel bude chtít provozovat zařízení bez ohrožení životního prostředí, ovšem některé technologie neumožňují 100% eliminaci environmentálních rizik. Tedy ani kritérium ovlivnění životního prostředí není pravděpodobně vhodné pro rozhodnutí o vhodnosti optimalizace údržby za účelem úspory finančních prostředků.

Kritičnost druhá - ovlivnění navazující technologie

Některá zařízení mohou vyvolat při svém výpadku zastavení produkce navazující technologie. Je snadno představitelné, že výpadek zapříčiní ztráta hlavní funkce nějakého zařízení, ovšem mnohem častější jsou výpadky výroby, způsobené tzv. bezpečnou poruchou bezpečnostního systému. Při bezpečné poruše dojde k zafungování bezpečnostního systému, přestože nenastala nebezpečná událost. Závažnost tohoto problému je dána zejména množstvím komponent, které bezpečnostní systém tvoří. Paradoxem je, že bezpečnostní systém může být i při nebezpečné poruše ve stavu schopném vykonávat svou bezpečnostní funkci. Pozitivem je, že komponenty, případně celé trasy bezpečnostního systému mohou být zálohované, čímž se sníží nejen riziko nefunkčnosti bezpečnostního systému v případě výskytu nežádoucí události, ale lze tímto způsobem také minimalizovat počet bezpečných poruch a tím i počet výpadků navazujících technologických celků.

Je zřejmé, že omezit se při hodnocení kritičnosti zařízení pouze na to, jaké nastanou vyvolané náklady z výpadku navazující technologie, by byla chyba. Nicméně umístění zařízení v procesu výroby a následky jeho poruchy mají vliv na důležitost zařízení a tomu je třeba přizpůsobit i systém údržby. To znamená, že dvě naprosto totožné komponenty mohou mít

stanovenu rozdílnou ideální úroveň údržby v závislosti na svém umístění ve výrobním procesu.

Kritičnost třetí - zařízení bez údržby

V průběhu analýz optimalizace údržby se velmi často začíná z tzv. nulového stavu, tedy ze stavu, kdy na zařízení není aplikována žádná údržba. Myšlenka, vedoucí k této strategii je zřejmá - jestli mám investovat do údržby zařízení, chci vědět, jaká je návratnost této investice, jinými slovy kolik ušetřím na snížené poruchovosti udržovaného zařízení. Problém je také zřejmý - dosud žádný podnik neposkytl svoje vybavení pro testování, jak dlouho vydrží fungovat bez údržby. Z toho vyplývá značná nejistota v odhadu spolehlivostních parametrů neudržovaného zařízení, zejména jeho střední doby mezi poruchami.

Na druhou stranu je na tomto místě nutné zmínit, že z porovnání ročních rizik neudržovaných zařízení můžeme určit ta „kritická“, která by v případě ukončení údržbových aktivit vykazovala nejvyšší roční ztráty. Tento postup je možné využít pro argumentaci v případě tlaku na snižování ročního rozpočtu oddělení údržby tak, že vedoucí údržby má možnost vytipovat zařízení, která v režimu „bez údržby“ vykazují relativně nízké náklady, které se ovšem předpokládají vyšší, než součet nákladů na údržbu a tzv. zbytkového rizika, tedy potenciálních následků poruchy i v případě řádného vykonávání preventivní údržby.

Kritičnost čtvrtá - zařízení s existující nebo doporučenou údržbou

Obdobným myšlenkovým postupem, jako kritičnost zařízení bez údržby, je možné odhadnout kritičnost zařízení s údržbou. V tomto případě jde vlastně o součet dvou nákladů (samozřejmě za jednotné časové období, ideálně 1 rok). Tím prvním jsou náklady na prováděnou preventivní údržbu a druhým nákladem je riziko poruchy při stávajícím, resp. doporučeném systému údržby. Tím, že obě složky kritičnosti převedeme na jednotného jmenovatele, tedy Kč/rok, můžeme je sčítat, aniž se dopustíme matematické chyby. Po sečtení již můžeme snadno porovnat kritičnost zařízení s údržbou s kritičností bez údržby. Tím dostaneme informaci o tom, zda se ekonomicky vyplatí údržbu provádět či nikoliv.

Kritičnost pátá - souhrn nákladů na provoz a údržbu

Při zjišťování kritičnosti zařízení, tedy obecně nákladů, které toto zařízení odčerpává z rozpočtu provozovatele za účelem vykonávání své funkce, je vhodné se soustředit nejen na stránku poruchovosti, ale i na náklady, spojené s provozem zařízení, jako např. elektrická energie, ale třeba i pravidelné výměny katalyzátorů, atp. Tyto provozní náklady jsou nedílnou součástí celkových nákladů na provoz a údržbu zařízení a proto je vhodné s nimi počítat, přestože v praxi je často provozní a údržbářský rozpočet oddělen.

Kritičnost šestá - poměr nákladů na provoz a údržbu k pořizovací ceně zařízení

Navažme na předchozí kapitolu, ve které jsme kritičností rozuměli součet ročních nákladů na provoz a údržbu, včetně údržby poruchové. Vnímavý čtenář si jistě uvědomil, že pro určité účely není vhodné porovnávat mezi sebou absolutní hodnoty nákladů. Je evidentní, že malé zařízení, např. teploměr, bude mít odlišné (nižší) náklady na provoz a údržbu, než zařízení velké, např. čerpadlo, a to i přesto, že teploměr může být poruchovější. Pro snížení těchto nedokonalostí je možné normovat celkové náklady na provoz a údržbu zařízení (preventivní i poruchovou) např. pořizovací cenou zkoumaného zařízení. Tím dostaneme kritičnost jako bezrozměrnou veličinu, podobně jako např. FMECA má své bezrozměrné rizikové číslo. Takováto hodnota slouží zejména k porovnání zařízení a nalezení těch, která vykazují nejvyšší kritičnost bez ohledu na její absolutní hodnotu. Potom je již možné aplikovat např.

všeobecně známou Paretovu analýzu a zahájit proces snižování kritičnosti (a tím ekonomické náročnosti provozování) analyzovaného seznamu majetku.

Literatura

[1] ČSN IEC 60050-192, *Mezinárodní elektrotechnický slovník - Část 192: Spolehlivost*, Praha, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016

[2] ČSN EN 61703 (010607) *Matematické výrazy pro ukazatele bezporuchovosti, pohotovosti, udržovatelnosti a zajištěnosti údržby*, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2002

Použití ordinálních a semikvantitativních postupů ve spolehlivosti

Ing. Jaroslav Zajíček, Ph.D.

Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií, Studentská 2, Liberec 461 17

e-mail: jaroslav.zajicek@tul.cz, http://osr.mti.tul.cz

1. Úvod

Pro efektivní řízení rizika je třeba umět riziko správně posuzovat. V technické praxi se řízení rizik stává jedním ze základních prostředků k zajištění bezpečnosti, snížení nákladů nebo splnění legislativních požadavků. Aby bylo možné riziko efektivně řídit, je nutné ho nejprve identifikovat a zjistit jeho velikost. Tuto velikost (úroveň) rizika je možné stanovit kvantitativně, semikvantitativně nebo pomocí rozhodovacích schémat apod. Zatímco v případě kvantitativního výpočtu bývá problémem především přesnost vstupních dat, u ostatních přístupů může zásadní nepřesnost vzniknout už díky samotnému modelu pro stanovení rizika. Příspěvek se zaměřuje na posouzení postupů, které nejsou založeny na plně kvantitativním vyjádření rizika.

2. Výskyt nekvantitativních postupů vyjádření rizika

V běžné praxi je velmi rozšířeno používání matice rizika, někdy označované jako matice kritičnosti. Jedná se o jednoduchý nástroj, který pomocí dvourozměrné matice, která má na jedné ose pravděpodobnost a na druhé ose následky, stanovuje úroveň rizika. Matice rizik mají většinou rozměr od 3x3 do 5x5 (nemusí být čtvercové) a jednotlivá pole jsou označena (obarvena) úrovní rizika.

Metoda FMECA stanovuje tzv. rizikové číslo RPN (Risk Priority Number) pro jednotlivé identifikované způsoby poruch. Jedná se o semikvantitativní metodu. Vstupní data pro vyčíslení RPN jsou bodová ohodnocení 3 faktorů, a to pravděpodobnosti, odhalitelnosti a následků nežádoucí události (způsobu poruchy). Na základě výsledné hodnoty RPN jsou pak hledána vhodná nápravná opatření pro snížení rizika.

Další výskyty nekvantitativních postupů vyjádření rizika jsou v oblasti funkční bezpečnosti. Prvním krokem při snižování rizika pomocí bezpečnostních systémů je stanovení úrovně rizika provozovaného zařízení. Stanovení této úrovně je realizováno pomocí rozhodovacích diagramů nebo kombinací semikvantitativního výpočtu a matice rizika. Daný způsob je závislý na typu zařízení a případně oboru, ve kterém se používá. Za základní normy funkční bezpečnosti jsou považovány IEC 61508-5 [1] a IEC 61511-x [2]. Jejich principy pak přejímají další normy z různých průmyslových odvětví se vztahem k funkční bezpečnosti, např. IEC 62061 [3], ISO 13849 [4], IEC 61513 [5], EN 50129 [6] nebo směrnice německého drážního úřadu [7].

3. Matice rizika

Matice kritičnosti/rizika je velmi jednoduchým nástrojem pro zběžné určení rizika. Jedná se o dvourozměrné pole. Z toho je zřejmé, že se vždy omezujeme na hodnocení dvou faktorů, tedy pravděpodobnosti a následků. Sestrojení vícerozměrné matice je pochopitelně teoreticky

možné, pro praxi však téměř nepoužitelné. Vícerozměrnou matici je tak vhodné nahradit například výpočtem RPN apod.

Existuje mnoho variant matic pro hodnocení rizika, které se liší v počtu stupňů pro stanovení pravděpodobnosti a následků, ale dokonce i v principu obarvování jednotlivých polí. Stupňům pravděpodobnosti jsou často přiřazeny konkrétní zástupné hodnoty nebo intervaly hodnot, stupně následků pak mají pouze slovní popis.

Četnost výskytu důsledku poruchy	**Úrovně závažnosti**			
	1 Nevýznamná	**2 Nízká**	**3 Kritická**	**4 Katastrofická**
5: Častý výskyt	Nežádoucí	Nepřípustné	Nepřípustné	Nepřípustné
4: Pravděpodobný výskyt	Přípustné	Nežádoucí	Nepřípustné	Nepřípustné
3: Občasný výskyt	Přípustné	Nežádoucí	Nežádoucí	Nepřípustné
2: Velmi slabý výskyt	Zanedbatelné	Přípustné	Nežádoucí	Nežádoucí
1: Nepravděpodobný výskyt	Zanedbatelné	Zanedbatelné	Přípustné	Přípustné

Obr. 1: Matice kritičnosti

Matice kritičnosti z obr. 1, která je obsažena v normě ČSN EN 60812**,** rozděluje výsledné riziko do 4 oblastí: zanedbatelné, přípustné, nežádoucí a nepřípustné. Pokud se stupňům pravděpodobnosti přiřadí namísto intervalu uvedeného v normě jedna konkrétní zástupná hodnota a stupňům následků charakter stupnice, je možné určit, zda obarvení polí odpovídá riziku spočteného ze zástupných hodnot, tzn., že riziko méně závažně ohodnocené události nepřesáhne riziko události se závažnějším ohodnocením. Stupnice následků se bude opět předpokládat jako geometrická, v tomto případě však s neznámým kvocientem q. Zástupné hodnoty pravděpodobnosti a následků byly přiřazeny následujícím způsobem.

Tab. 1: Přiřazení zástupných hodnot hodnotícím stupňům

Hodnotící stupeň	**Pravděpodobnost**	**Následky**
1	0,0005	$k \cdot q^1$
2	0,005	$k \cdot q^2$
3	0,05	$k \cdot q^3$
4	0,15	$k \cdot q^4$
5	0,5	nedefinováno

Jednoduchým porovnáním hodnot výsledného rizika bylo zjištěno, že způsob obarvení matice z obr. 1 je korektní pouze pro hodnoty $q \in \{6, 7, 8, 9, 10\}$, pokud se omezíme na $q \in Z$.

Například pro $q = 3$ a zanedbání konstanty ($k = 1$) není stávající obarvení matice korektní, protože „zanedbatelné“ riziko u kombinace „Velmi slabý výskyt nevýznamné závažnosti“ má

vyšší hodnotu zástupného rizika než „přípustné“ riziko u kombinace „Nepravděpodobný výskyt kritické závažnosti“.

Četnost výskytu důsledku poruchy	Úrovně závažnosti			
	1 Nevýznamná	2 Nízká	3 Kritická	4 Katastrofická
5: Častý výskyt	0,5	1,5	4,5	13,5
4: Pravděpodobný výskyt	0,15	0,45	1,35	4,05
3: Občasný výskyt	0,05	0,15	0,45	1,35
2: Velmi slabý výskyt	0,005	0,015	0,045	0,135
1: Nepravděpodobný výskyt	0,0005	0,0015	0,0045	0,0135

Legenda	Zanedbatelné	Přípustné	Nežádoucí	Nepřípustné

Obr. 2: Riziko spočtené ze zástupných hodnot pro $q = 3$

Použití matice kritičnosti/rizika lze doporučit v případech, kdy je dostačující hodnocení dvou parametrů. Pro obarvení matice rizikovými stupni je nezbytné, aby bylo navrženo na základě jednotlivých stupňů pro hodnocení kritérií, nikoliv intuitivně. Matice uvedená v normě ČSN EN 60812 je na základě výše uvedené analýzy použitelná bez úpravy za předpokladu geometrického charakteru stupnice s kvocientem v rozmezí 6 až 10 včetně krajních hodnot. Tento předpoklad však norma neuvádí a je zřejmý až po detailní analýze, kterou většina uživatelů tohoto nástroje neprovádí.

4. RPN v analýze FMECA

Obdobným způsobem můžeme analyzovat další nekvantitativní přístupy stanovení rizika, tzn. i rizikové číslo RPN v analýze FMECA. Pro srovnání kvantitativního rizika a rizika vypočteného pomocí bodových stupnic musí být každé bodové hodnotě všech stupnic přiřazena zástupná kvantitativní hodnota reprezentující celý interval. Stupnice pro analýzu níže byly použity z normy ČSN EN 60812, jedná se o stupnice pravděpodobnosti, odhalitelnosti a následků, přičemž všechny stupnice mají 10 úrovní (1-10) a výsledné rizikové číslo se počítá jako součin jednotlivých bodových ohodnocení.

$$RPN = P \cdot O \cdot N$$

U stupnice pravděpodobnosti je její zástupná hodnota jednoznačně přiřazena. U stupnic odhalitelnosti a následků je nutné strukturu stupnice odvodit ze slovního hodnocení. Vzhledem k tomu, že prostřední ohodnocení na stupnici odhalitelnosti mají v popisu kritéria „střední šance odhalení“, lze je transformovat na cca 50% pravděpodobnost odhalení. Ostatní stupně již není možné takto přiřadit, lze se však domnívat, že je stupnice přibližně aritmetická, tedy stupeň 1 odpovídá 95% šanci odhalení, stupeň 2 odpovídá 85% šanci odhalení atd.

Zatímco hodnoty pravděpodobnosti a odhalitelnosti mohou nabývat pouze hodnot v intervalu $< 0; 1 >$, hodnocení následků není obecně shora omezené. Stupnice pro hodnocení následků navíc nemá ve slovním popisu jednotlivých bodových stupňů kvantifikaci (kromě stupňů 2, 3 a 4, ve kterých se píše o počtu zákazníků, kteří zpozorují skřípající nebo chrastící objekt).

Charakter stupnice tedy nelze exaktně určit. Absolutní rozdíly mezi sousedními úrovněmi stupnice nejsou konstantní, např.:

2 - Skřípající a chrastící objekt, vadu zpozorují nároční zákazníci

3 - Skřípající a chrastící objekt, vadu zpozoruje 50% zákazníků

oproti

8 - Objekt není provozuschopný (ztráta základní funkce)

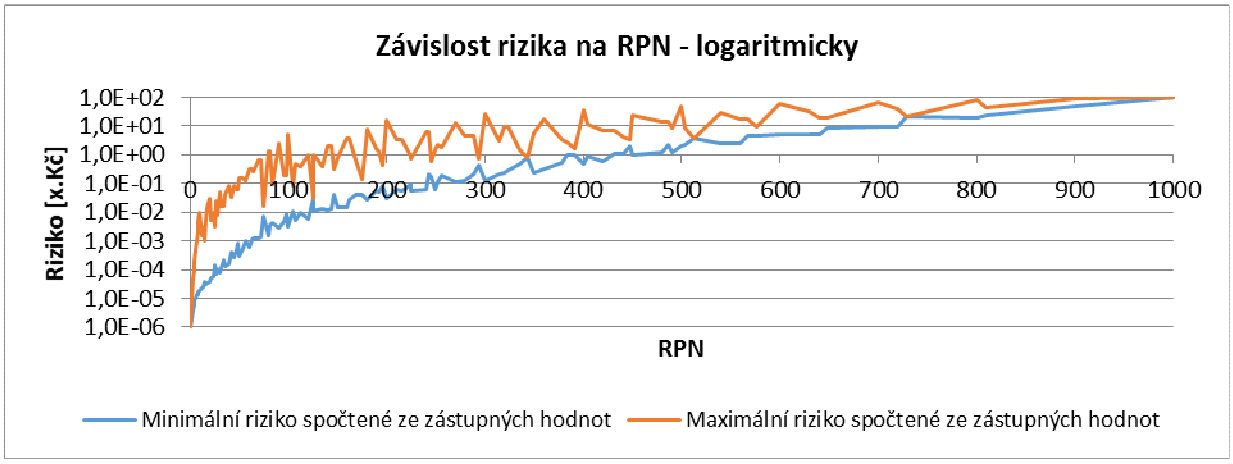
9 - Způsob poruchy ovlivňuje bezpečnost nebo způsobí nesoulad s vládními předpisy

čímž je možné vyloučit, že stupnice je daná aritmetickou posloupností. Zda se jedná o stupnici danou geometrickou posloupností nelze potvrdit ani vyvrátit, záleží i na interpretaci jednotlivých stupňů samotným analytikem. Pro další část práce budeme uvažovat stupnici danou geometrickou posloupností s kvocientem $q = 2$, tzn., že událost ohodnocená stupněm 4 bude mít přibližně $2\times$ větší následky než událost ohodnocená stupněm 3, či $4\times$ větší následky než událost ohodnocená stupněm 2.

Tab. 2: Přiřazení zástupných hodnot bodovým klasifikacím stupnic

Klasifikace	Pravděpodobnost	Odhalitelnost	Následky [Kč]
1	1,0E-05	0,95	$k \cdot 2^1$
2	1,0E-04	0,85	$k \cdot 2^2$
3	5,0E-04	0,75	$k \cdot 2^3$
4	1,0E-03	0,65	$k \cdot 2^4$
5	2,0E-03	0,55	$k \cdot 2^5$
6	5,0E-03	0,45	$k \cdot 2^6$
7	1,0E-02	0,35	$k \cdot 2^7$
8	2,0E-02	0,25	$k \cdot 2^8$
9	5,0E-02	0,15	$k \cdot 2^9$
10	1,0E-01	0,05	$k \cdot 2^{10}$

Grafy na obr. 3 zobrazují závislost rizika vypočteného ze zástupných hodnot na RPN vypočteném pomocí bodových ohodnocení. Protože jedno rizikové číslo RPN může vzniknout různými bodovými kombinacemi hodnocených faktorů, je vynesena křivka minimálního a maximálního rizika. Druhý graf (obr. 4) zobrazuje poměr maximální a minimální hodnoty rizika pro dané rizikové číslo RPN. Přestože je RPN diskrétní veličina, jsou následující funkce pro přehlednost zobrazeny jako spojité.



Obr. 3: Závislost rizika na RPN

Obr. 4: Poměr maximálního a minimálního rizika v závislosti na RPN

Na obr. 4 vidíme, že v první desetině rozsahu rizikových čísel RPN, tedy v intervalu $\{1, \dots, 100\}$, kde se v praxi vyskytuje nejvíce ohodnocených událostí, se vyskytují poměrově největší rozdíly mezi minimálními a maximálními možnými hodnotami rizika.

Z výše uvedených grafů je na první pohled zřejmé, že stávající postup hodnocení a vyhodnocení nežádoucích událostí dává velmi zkreslené výsledky v podobě RPN. K jednotlivým RPN není možné jednoznačně přiřadit hodnotu rizika, ale pouze jeho minimální a maximální hodnotu. Minimální ani maximální hodnota rizika v závislosti na rostoucím RPN není rostoucí funkcí, tím lze předem vyloučit schopnost RPN korektně porovnat dvě hodnocené události.

5. Identifikace rizika v oblasti funkční bezpečnosti

Důvodem, proč byly normativně popsány procesy a postupy aplikace funkční bezpečnosti, bylo řízení rizika, které plyne z ohrožení zdraví a života osob, na úroveň, která je společností přijatelná. Analýza rizika a hodnocení rizika probíhají v jednom kroku pomocí diagramů,

matic nebo semikvantitativních výpočtů, uvedených přímo v normativních dokumentech (informativních přílohách). Zjednodušeně řečeno, na základě určení pravděpodobnosti a následku nežádoucí události je přiřazena úroveň bezpečnostního systému tak, aby po jeho realizaci byla míra rizika přijatelná.

Níže budou stručně charakterizovány 4 přístupy při posuzování rizika, a to dle:

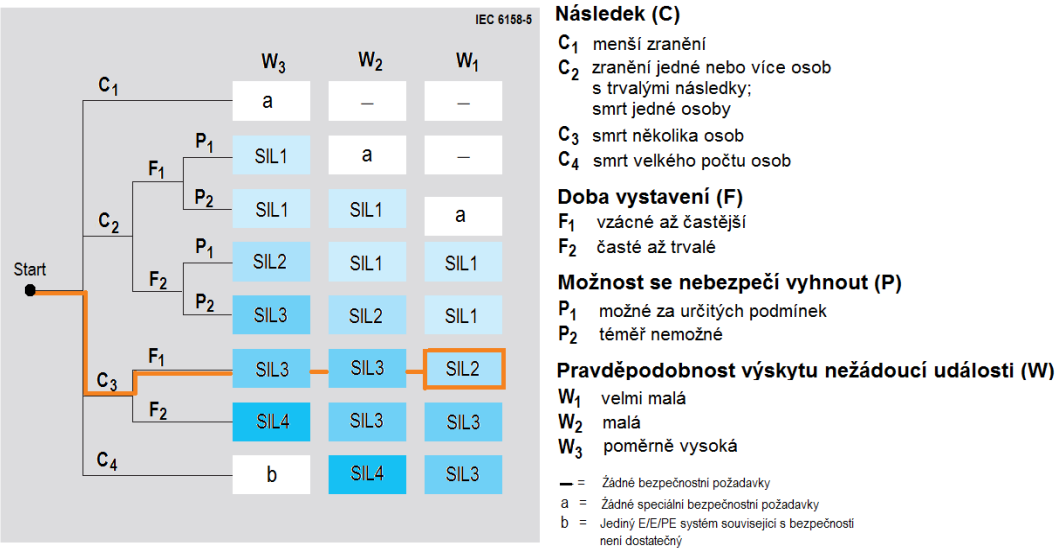
- IEC 61508-5 [1]

- IEC 62061 [3]

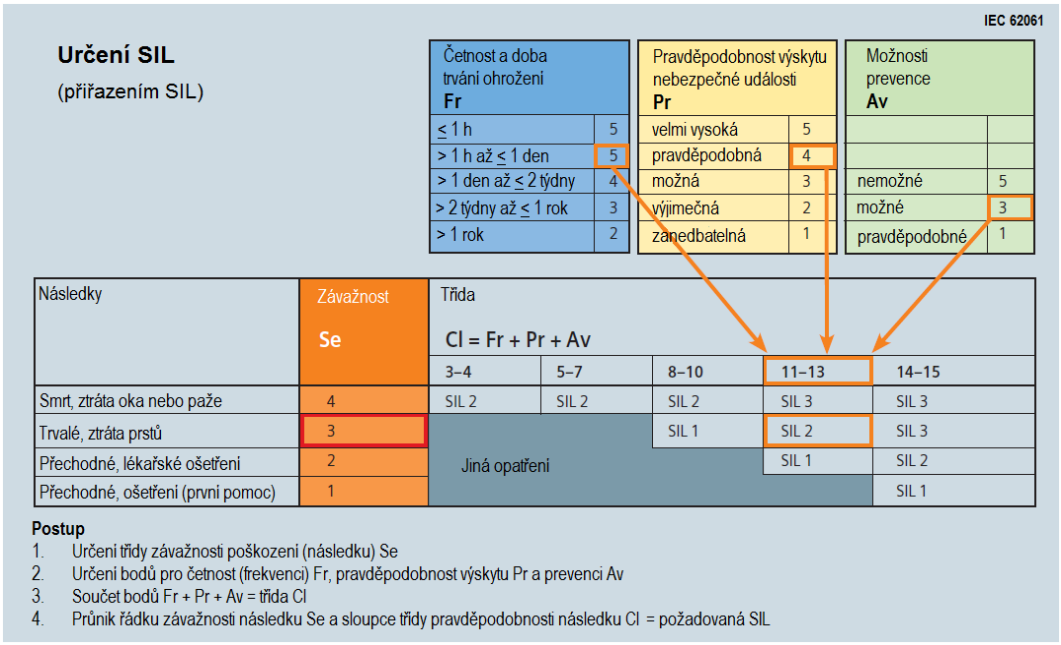
- ISO 13849-1 [4]

- SIRF 400 [7]

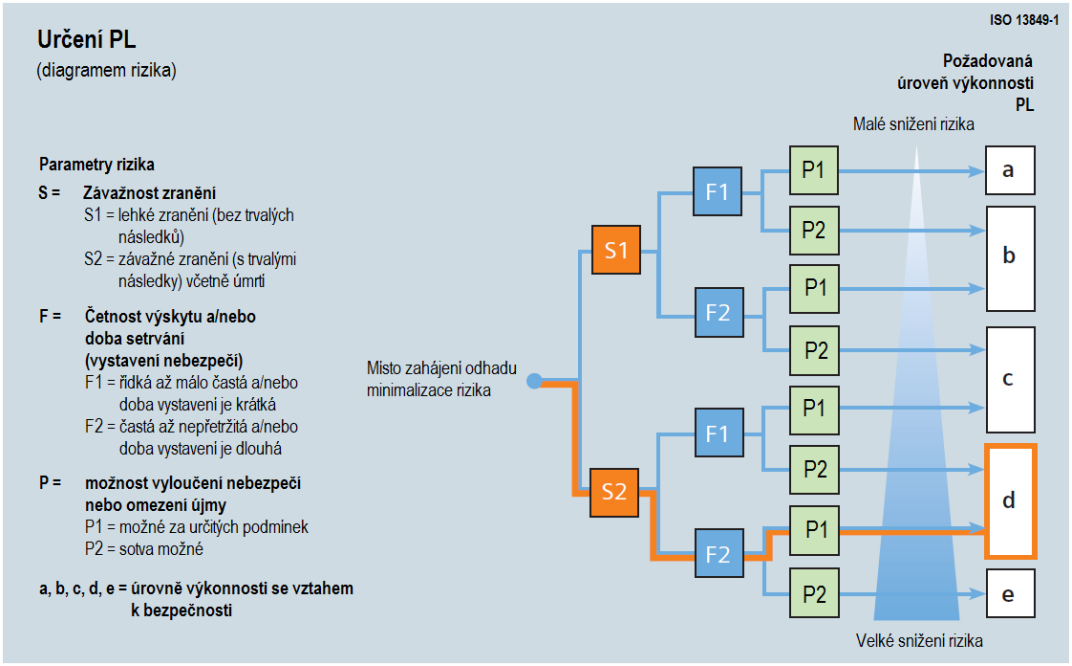
Uvedené dokumenty se poměrně zásadně liší v procesu posuzování rizika. Liší se množství hodnocených faktorů, jejich kvantifikace i výsledné zpracování pro stanovení potřebné úrovně spolehlivosti bezpečnostního systému. To, v čem se postupy shodují, je základní filosofie rizika, tedy jeho chápání jako kombinace složky pravděpodobnosti a následků. Dva z postupů používají semikvantitativního přístupu v posuzování, zbylé dva pak kvalitativního přístupu s využitím rozhodovacího schématu a ordinálních stupnic (lze určit pořadí).



Obr. 5: Postup dle IEC 61508-5



Obr. 6: Postup dle IEC 62061



Obr. 7: Postup dle ISO 13849-1

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

$$I = \frac{S_a \cdot S_v \cdot W \cdot E}{V}$$

klasifikační indikátor I	stupeň požadavku na bezpečnosti (SIL, něm. SAS)
0 - 21	= SAS 0
22 - 35	= SAS 1
36 - 72	= SAS 2
73 - 122	= SAS 3

Obr. 8: Postup dle SIRF 400

Pro porovnání uvedených postupů byly vytvořeny tabulky 3 až 5. První tabulka dělí postupy podle typu hodnotících stupnic, způsobu stanovení SIL, toho, jakým způsobem jsou úrovně požadované funkční bezpečnosti vůbec značeny, počtu hodnocených kritérií a počtu úrovní hodnotících stupnic.

Tab. 3: Způsoby dosažení požadované funkční bezpečnosti

	Typ stupnic	**Způsob stanovení SIL**	**Označení požadavku**	**Počet hodnocených kritérií**	**Počet úrovní hodnotících stupnic**
IEC 61508-5	Kvalitativní ordinální	Rozhodovací diagram	- a SIL1 SIL2 SIL3 SIL4 b	4	2 až 4

IEC 62061	Semikvantitativní	Kombinace semikvantitativního výpočtu a matice	SIL1 SIL2 SIL3	4	3 až 5
ISO 13849-1	Kvalitativní ordinální	Rozhodovací diagram	a b c d e	3	2
SIRF 400	Semikvantitativní	Semikvantitativní výpočet	SAS0 SAS1 SAS2 SAS3	5	2 až 3

Tab. 4: Porovnání značení úrovní funkční bezpečnosti a jejich kvantitativní význam

		IEC 61508-5	**IEC 62061**	**ISO 13849-1**	**SIRF 400**
Požadavek na průměrnou frekvenci nebezpečné poruchy bezpečnostní funkce [h^{-1}]	**žádné bezpečnostní požadavky**	-			SAS 0
	žádné speciální bezpečnostní požadavky	a			
	>1E-5 to <1E-4			a	
	>3E-6 to <1E-5	SIL 1	SIL 1	b	SAS 1
	>1E-6 to <3E-6			c	
	>1E-7 to <1E-6	SIL 2	SIL 2	d	SAS 2
	>1E-8 to <1E-7	SIL 3	SIL 3	e	SAS 3
	>1E-9 to <1E-8	SIL 4			SAS 4
	jediný bezpečnostní systém není dostatečný	b			

Tab. 5: Značení jednotlivých faktorů rizika

	Parametry pravděpodobnosti			**Parametr následků**	
	Výskyt	**Vystavení**	**Vyhnutí**	**Počet osob**	**Stupeň zranění**
IEC 61508-5	W	F	P	C	

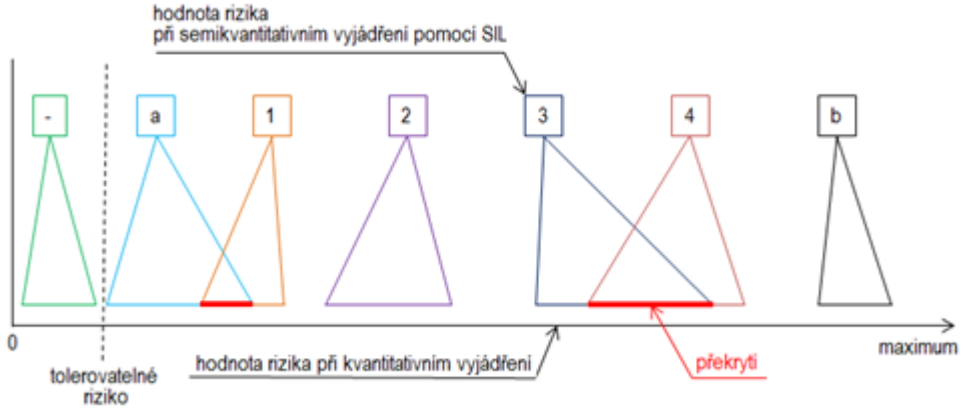
IEC 62061	Pr	Fr	Av		Se
ISO 13849-1		F	P		S
SIRF 400	W	E	V	Sa	Sv

Na základě takovéhoto stručného porovnání přístupů je evidentní, že uvedené metody se snaží dosáhnout stejného cíle různým způsobem. Ani jeden z postupů není plně kvantitativního charakteru, aby ho bylo možné snadno podrobit ověření - validaci. I bez dalšího podrobnějšího zkoumání je téměř jisté, že různé metody budou při posuzování stejné události dosahovat různých výsledků a tedy se budou lišit i v požadavku na úroveň funkční bezpečnosti.

5.1 Zásady posouzení postupů kvantitativním způsobem

Testování, zda doporučený model koresponduje s plně kvantitativním přístupem kvantifikace rizika, je založeno na přiřazení kvantitativních hodnot jednotlivým stupňům hodnotících stupnic. V tomto testování se omezujeme na přiřazení geometrických posloupností, tedy se předpokládá, že sousední úrovně stupnice se liší právě x-krát. Hodnota X je testována na intervalu <2; 20> a omezuje se na celočíselné hodnoty. Důležité je zmínit, že jednotlivé faktory (výskyt, vystavení, vyhnutí, počet osob a stupeň zranění) mohou mít tyto hodnoty (kvocienty geometrické posloupnosti) různé. Např. pro postup v normě IEC 61508-5, do kterého vstupují 4 hodnocené faktory, bylo testováno $19^4 = 130\ 321$ variant.

Následně je porovnáváno, zda pro nízké riziko není požadováno přísnějšího SILu než pro událost s vyšším rizikem. Kritériem tedy je, zda se kategorie rizika překrývají dle následujícího schématu. Překrytí přitom nemusí nastat pouze mezi přímo sousedícími kategoriemi, ale i přes několik kategorií.



Obr. 8: Pokrytí rizika prostřednictvím SIL

5.2 IEC 61508-5

Počet vstupních faktorů: 4

Množství testovaných variant: $19^4 = 130\ 321$

Tab. 6: Překrývání intervalů rizika pro IEC 61508-5

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**						
	0	**1**	**2**	**3**	**4**	**5**	**6**
Jedna (sousední) kategorie SIL	0	0	0	14	82	2 114	128 111
Dvě kategorie SIL	2	169	16 107	26 263	27 773	60 007	-
Tři kategorie SIL	2 995	4 695	50 819	57 508	14 304	-	-
Čtyři kategorie SIL	58 236	14 490	41 143	16 452	-	-	-
Pět kategorií SIL	108 870	0	21 451	-	-	-	-
Šest kategorií SIL	124 922	5 399	-	-	-	-	-

Význam zvýrazněné buňky: U 4 695 variací kvocientů se 1 dvojice intervalů rizika překrývá, dvojice je od sebe vzdálena 3 kategorie SIL. Příklad může být například situace, kdy minimum intervalu rizika úrovně SIL 4 může být nižší než maximum intervalu rizika úrovně SIL 1.

Informačně nejdůležitější buňka je v levém horním rohu tabulky, která vypovídá o počtu variant, kdy se intervaly rizika vůbec nepřekrývají. Za předpokladu geometrických stupnic a platnosti vzorce pro výpočet rizika, který je daný součinem pravděpodobnosti a následků, lze tedy konstatovat, že výsledky při aplikaci doporučeného schématu pro stanovení SIL nejsou v souladu s kvantitativním posuzováním a řízením rizika.

5.3 IEC 62061

Metoda stanovení úrovně integrity bezpečnosti je v této normě odlišná od metody uvedené v IEC 61508-5. Je založena na semikvantitativním hodnocení rizika. Používá 4 parametry (*Se*, *Fr*, *Pr*, *Av*), které jsou hodnoceny body a promítnuty do matice rizika, ve které se uskutečňuje stanovení SIL. Vzhledem k tomu, že se bodová ohodnocení pravděpodobnostních parametrů *Fr*, *Pr* a *Av* sčítají do jediného výsledného parametru *Cl*, je zde pravděpodobné použití geometrických stupnic se stejným kvocientem *Q*. Součet tedy vyplývá ze vztahu:

$$Q^{Fr} \cdot Q^{Pr} \cdot Q^{Av} = Q^{Fr + Pr + Av}$$

Počet vstupních faktorů: 4

Množství testovaných variant: $19^2 = 361$

Tab. 7: Překrývání intervalů rizika pro IEC 62061

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**			
	0	**1**	**2**	**3**
Jedna (sousední) kategorie SIL	0	11	15	335
Dvě kategorie SIL	4	79	278	-
Tři kategorie SIL	298	63	-	-

Výše uve

dená tabulka je menšího rozměru z důvodu, že norma IEC 62061 stanovuje pouze 3 kategorie SIL. Komentář je v souladu s hodnocením IEC 61508-5, opět neexistuje varianta, kdy by navržený model byl v souladu s plně kvantitativním hodnocením rizika.

5.4 ISO 13849-1

Počet vstupních faktorů: 3

Množství testovaných variant: $19^3 = 6\,859$

Tab. 8: Překrývání intervalů rizika pro ISO 13849-1

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**				
	0	**1**	**2**	**3**	**4**
Jedna (sousední) kategorie SIL	2 109	0	4 750	0	0
Dvě kategorie SIL	6 459	400	0	0	-
Tři kategorie SIL	6 859	0	0	-	-
Čtyři kategorie SIL	6 859	0	-	-	-

Z tabulky 6 je zřejmé, že zjednodušený přístup podle ISO 13849-1 je v porovnání s přístupy podle IEC 61508-5 a IEC 62061 mnohem robustnější ve smyslu jeho odolnosti proti nevhodnému způsobu sestavení stupnic parametrů rizika. To je zřejmé i z koncentrace hodnot ve sloupci "0". Ani tento způsob však není imunní proti jeho nesprávnému použití a nelze jej tedy považovat za zcela korektní - viz body zmíněné v závěru.

5.5 SIRF 400

Tento přístup využívá 5 hodnotících faktorů rizika. Z důvodu vysokých časových nároků na provedení simulací byly kvocienty generovány pouze na intervalu <2; 15>, a to opět celočíselné. Tato varianta je časově 5x méně náročná oproti původnímu intervalu <2; 20>.

Počet vstupních faktorů: 5

Množství testovaných variant: $14^5 = 537\,824$

Tab. 9: Překrývání intervalů rizika pro SIRF 400

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**				
	0	**1**	**2**	**3**	**4**
Jedna (sousední) kategorie SIL	12	32	636	18 020	519 124
Dvě kategorie SIL	80 110	68 610	47 973	341 131	-
Tři kategorie SIL	387 187	73 301	77 336	-	-
Čtyři kategorie SIL	519 147	18 677	-	-	-

Stejně jako u předchozího postupu v normě ISO 13849-1 existují jisté variace kvocientů, které požadovaných kritériím odpovídají. Důvody, proč ani tento postup nelze přímo označit jako korektní, jsou uvedeny v závěru.

6. Závěr

Cílem článku bylo představit nekvantitativní postupy v oblasti rizika, udělat jejich vzájemné porovnání a dále testovat, zda za jistých předpokladů jsou metody konzistentní s plně kvantitativním posuzováním a řízením rizika.

Použití matice rizika může dávat relevantní výstupy, pokud je vhodně navržena a jednotlivé kategorie ve stupnicích pravděpodobnosti a následků dostatečně detailně popsány.

Rizikové číslo RPN se jako vhodný nástroj neprokázal. Jednotlivé stupnice nejsou konzistentní. Aby vyhovoval standardní výpočet pomocí součinu, musely by všechny stupnice vykazovat charakter aritmetické posloupnosti.

Po provedení simulací na metodách funkční bezpečnosti je evidentní, že nejvíce robustní je stanovení potřebné úrovně SIL dle ISO 13849-1. To je způsobeno především tím, že do modelu vstupují pouze 3 faktory a intervaly rizika pro jednotlivé kategorie SIL jsou tedy užší.

Zkoumání a porovnání přístupů následně generuje další náměty a otázky k řešení:

- Jaký je důvod existence různých metod? Všechny postupy v závěru doporučují kategorie SIL, které mají konkrétní kvantitativní parametry. To by znamenalo, že různé standardy předpokládají různou míru přijatelného rizika.
- Jaká je tedy hodnota přijatelného rizika? Ani jeden z dokumentů se nezmiňuje o konkrétní hodnotě. Vzhledem k tomu, že se přístupy nejeví v souladu s plně kvantitativním hodnocením rizika, není možné je zpětně z postupů určit.
- Předpoklad použitý v tomto článku - geometrické stupnice - může být samozřejmě mylný. Stupnice stejně tak mohou být aritmetické nebo zcela obecné. Jakým způsobem byly normativní postupy vytvořeny? Chybí jakékoliv zdůvodnění navržených rozhodovacích diagramů, bodových hodnocení semikvantitativních stupnic atd. Stejný přístup, uplatňovaný různými analytiky, se pak může ve výsledcích diametrálně lišit. Například "vysoká" pravděpodobnost výskytu bude vnímána odlišně analytikem pracujícím standardně s mechanickými komponentami vykazující opotřebení a analytikem, který se standardně věnuje spolehlivé elektronice - a to v rozdílech až několika řádů.
- Rozdíl mezi kvantitativní hodnotou kategorie SIL je 1 řád. Toto kritérium nebylo zohledněno při překrývání intervalů. Varianty, které po simulaci vyšly bez překryvu intervalů, by tedy bylo vhodné dále podrobit testu, zda tyto intervaly, respektive středy těchto intervalů, jsou od sebe vzdáleny přibližně o jeden řád.

Využití plně kvantitativních přístupů posuzování a řízení rizika je mnohem efektivnější a prokazatelnější oproti zkoumaným metodám, a to i za předpokladu, že pro kvantitativní analýzu nejsou k dispozici přesná vstupní data a je třeba pracovat s expertními odhady.

Použitá literatura:

[1] ČSN EN 61508-5:2011, *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti.*

[2] ČSN EN 61511-x:2005, *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů.*

[3] ČSN EN 62061:2005, *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.*
[4] ČSN EN ISO 13849-1:2006, *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci*.
[5] ČSN IEC 61513:2003, *Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Všeobecné požadavky na systémy*.
[6] ČSN EN 50129:2003, *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy*.
[7] SIRF 400 - směrnice německého drážního úřadu

Interpretace pravděpodobnosti selhání ve funkční bezpečnosti drážních zařízení

doc. Ing. Pavel Fuchs, CSc.

Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií, Studentská 2, Liberec 461 17

e-mail: pavel.fuchs@tul.cz, http://osr.mti.tul.cz

1 Úvod

Obecný termín drážní zařízení pokrývá velmi různorodá zařízení dráhy a drážních vozidel. Složitost drážních zařízení je různá. Od jednoduchých jednoúčelových prvků až po strukturálně složitá zařízení. Technické požadavky na drážní zařízení specifikují příslušné technické normy a to včetně požadavků spojených s bezpečností. Postupy prokazování bezpečnosti jsou předmětem požadavků příslušné drážní legislativy a státní správy v oblasti drah (Drážní úřad).

Účelem tohoto příspěvku je podat užitečné informace použitelné v různé míře pro různá drážní zařízení, jejichž porucha může vést k funkčnímu selhání s dopadem na bezpečnost. Termín funkční bezpečnost je tedy v tomto příspěvku chápán v širším pojetí, není omezován jen na elektrické či elektronické bezpečnostní systémy a systémy související s bezpečností. Je zřejmé, že v příspěvku nelze vyčerpávajícím způsobem pokrýt celou šíři problematiky. Proto jsou jen naznačeny základní okruhy a postupy výpočtů pravděpodobnosti selhání některých zařízení.

Příspěvek je členěn do několika částí. V první části se zabývá pravděpodobnostními veličinami vstupujících do výpočtu rizika. Druhá část příspěvku prezentuje způsoby výpočtu pravděpodobnosti poruchy s ohledem na způsob fungování zařízení. Třetí část příspěvku se zabývá otázkou stanovení hodnoty přijatelného rizika.

2 Pravděpodobnostní veličiny při výpočtu rizika

Jedním z výsledků posuzování rizika je kvantitativní stanovení hodnoty rizika na základě provedené analýzy rizika. Podle hodnoty rizika se pak v dalším rozhodovacím procesu usuzuje na přijatelnost rizika a navrhují se případná opatření ke zmírnění rizika. Je zřejmé, že chybné vyčíslení rizika má za následek i chybné rozhodování. Předpokládejme, že všechny vstupní parametry výpočtu a ocenění nejistot spojených se stanovením jejich hodnot primárních jsou správné. Pak může chyba vzniknout chybnou analýzou rizika, nebo z neznalosti toho, co je vlastně počítáno. V mnoha odborných a vědeckých článcích se nesprávně interpretují jednotlivé veličiny a parametry vystupující ve výpočtech rizika. To má za následek, že předkládané výsledky výpočtů nejsou správné.

V české terminologii je pravděpodobnost zpravidla uvažována jako bezrozměrná veličina nabývající hodnot v intervalu 0 až 1. V angličtině je označována termínem probability. Avšak při výpočtu rizika se pro výskyt nežádoucí události používají i jiné pravděpodobnostní veličiny, než bezrozměrná pravděpodobnost. Angličtina operuje s termínem *likelihood*, což je

termín zavedený i v základním pokynu [1] pro používání termínů a definic v managementu rizik a příslušných normách. Tento termín je v českém překladu tohoto pokynu [2] uveden v definici 3.6.1.1 spolu s poznámkami takto:

> **možnost výskytu**
>
> **pravděpodobná možnost (výskytu)**
>
> možnost, že něco nastane
>
> POZNÁMKA 1 V terminologii managementu rizik se výraz „možnost výskytu“ používá k vyjádření možnosti, že něco nastane, ať již je tato možnost definována, měřena nebo objektivně či subjektivně, kvalitativně nebo kvantitativně stanovena a popsána s použitím obecných termínů, nebo je vyjádřena matematicky [jako je pravděpodobnost (3.6.1.4) nebo četnost (3.6.1.5) za dané časové období].
>
> POZNÁMKA 2 Anglický termín „likelihood“ nemá v některých jazycích přímý ekvivalent; místo něho se často používá ekvivalent termínu „probability“. V angličtině se však „probability“ často úzce interpretuje jako matematický termín. Nicméně v terminologii managementu rizik se „likelihood“ používá se záměrem, aby tento termín měl stejně širokou interpretaci, jako má termín "probability" v mnoha jiných jazycích, než je angličtina.

V následujícím textu bude podán výklad toho, jaké důsledky pro výpočet rizika má vyjádření pravděpodobnosti výskytu jevu (nežádoucí události) různou pravděpodobnostní veličinou [3]. Za tím účelem je třeba uvést seznam použitých symbolů, veličin a jejich jednotek.

Symbol	**Veličina**	**Jednotka**
C	následek (resp. následky)	viz text uvedený níže
F	frekvence výskytu (v obecném pojetí)	$[h^{-1}]$, $[km^{-1}]$, $[ks^{-1}]$
P	pravděpodobnost výskytu	[1]
R	riziko	viz text uvedený níže
U	nepohotovost, nedostupnost	[1]
p	očekávaný počet výskytů	[1]
t	doba	[h]
λ	intenzita poruch	$[h^{-1}]$
μ	intenzita oprav	$[h^{-1}]$

Při výpočtu rizika se zpravidla používá zápis rovnicí, kde se vyskytuje pravděpodobná možnost výskytu nežádoucí události a následky této nežádoucí události. Ale pravděpodobnou možnost výskytu je možné popsat odlišnými pravděpodobnostními veličinami. Namátkou lze uvést tyto pravděpodobnostní veličiny:

- pravděpodobnost výskytu (P),
- frekvence výskytu (F),
- intenzita výskytu (λ)
- očekávaný počet výskytů (p).

Při prezentaci výsledků výpočtu rizika je však třeba chápat, co je počítáno, aby nedošlo k nesprávné interpretaci. Vysvětlení rozdílů při výpočtu rizika a interpretaci výsledků je uvedeno v 2.1 – 2.4.

2.1 Pravděpodobnost výskytu

Při použití veličiny *pravděpodobnost výskytu* ve výpočtu rizika, je výpočet rizika zpravidla zapsán rovnicí (1).

$$R = P \cdot C \tag{1}$$

Pravděpodobnost výskytu P nežádoucí události je bezrozměrná pravděpodobnostní veličina s hodnotou v rozmezí 0 až 1. Hodnota této bezrozměrné pravděpodobnostní veličiny potřebuje doplňující popis, který vysvětluje, za jakých podmínek vypočítaná hodnota platí. Bez tohoto popisu by bylo možné vypočtenou hodnotu interpretovat nesprávně.

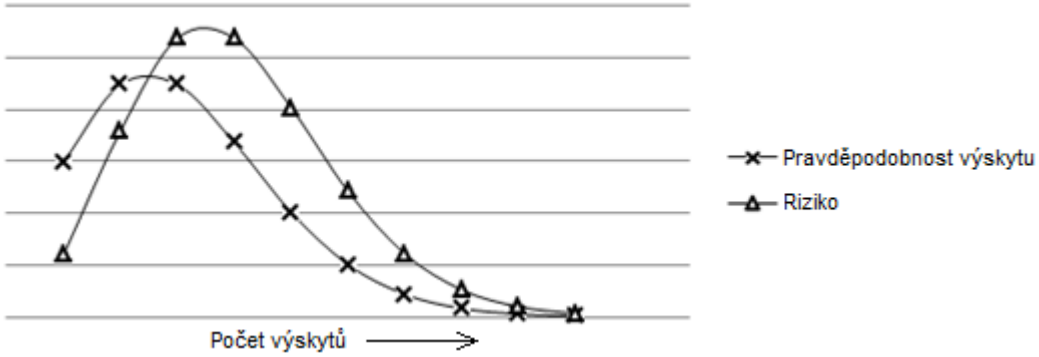
Příklad:
Pravděpodobnost výskytu náhodné nežádoucí události za dobu 100 let (vysvětlení podmínky) je 0,1 (bezrozměrná hodnota). Následek této události je smrt 20 osob. Riziko spojené s touto nežádoucí událostí lze snadno spočítat jako součin dvou hodnot v rovnici (1) a představuje smrt 2 osob. Doplňující popis pak specifikuje, že riziko je 2 úmrtí za dobu 100 let.

Je zřejmé, že při tomto výpočtu je hodnota rizika vyjádřena ve stejných jednotkách jako hodnota následků, tedy v počtu úmrtí.

Rovnici (1) však nelze použít, pokud se nežádoucí událost za dobu 100 let může vyskytnout více než jednou. Tam, kde náhodná nežádoucí událost se za uvažovanou dobu může vyskytnout opakovaně (1, 2, 3, …, n), je třeba použít rovnici (2).

$$R = \sum_{n=1}^{\infty} R_n = \sum_{n=1}^{\infty} P_n \cdot n \cdot C \tag{2}$$

Celková hodnota následků nežádoucích událostí $n.C$ se zvyšuje přímo úměrně s počtem nežádoucích událostí n. Ale pravděpodobnost výskytu nežádoucí události od určitého počtu výskytů rapidně klesá a tudíž klesá i hodnota rizika R_n, viz obr. 1.



Obr. 1: Průběh rizika v závislosti na očekávaném počtu nežádoucích událostí

Výpočet pravděpodobnosti výskytu právě n nežádoucích událostí není snadné. Nejjednodušší řešení je v případě exponenciálního rozdělení dob vzniku nežádoucí události, např. poruchy. V takovém případě je pravděpodobnost výskytu právě n událostí P_n za dobu (0; t) dána Poissonovo rozdělením s parametrem $t.\lambda$, viz rovnice (3).

$$P_n = \frac{(t \cdot \lambda)^n}{n!} \cdot e^{-t \cdot \lambda} \tag{3}$$

2.2 Frekvence výskytu

Obecně je frekvence (kmitočet) fyzikální veličinou. Jednotkou frekvence je hertz [Hz]. Jde o odvozenou jednotku, vyjádření v základních jednotkách soustavy SI je [s^{-1}]. V oboru spolehlivosti a rizika je však účelné vyjadřovat frekvenci výskytu nežádoucích událostí za delší časový interval nebo ve vztahu k jiným parametrům, např. k počtu vyrobených výrobků, ujeté vzdálenosti apod. Protože počet vyrobených výrobků do výskytu vadného výrobku je náhodný, stejně tak jako je náhodný počet kilometrů ujetých do vzniku poruchy, lze frekvenci výskytu chápat jako pravděpodobnostní veličinu. Frekvenci výskytu nežádoucí události lze tedy vyjadřovat např. v těchto jednotkách:

- [s^{-1}], resp. [h^{-1}], [rok^{-1}],
- [m^{-1}], resp. [km^{-1}],
- [1], v případě počtu objektů, jevů lze použít i doplňkový popis jednotky, např. [ks], [osoba], [úmrtí] aj.

Bez ohledu na to, v jakých jednotkách bude vyjádření frekvence, je pro výpočet rizika možné použít rovnici (4).

$$R = F \cdot C \tag{4}$$

Při použití frekvence výskytu je předpokládán opakovaný výskyt náhodné nežádoucí události, a tudíž odpadá problém složitého výpočtu. Rovněž jednotky rizika pak vyjadřují exaktně následky ve vztahu k frekvenci nežádoucí události bez nutnosti vysvětlujícího popisu.

Příklad:
Frekvence výskytu náhodné nežádoucí události je jednou za dobu 10 let, tedy 0,1 [rok^{-1}]. Následek této události je smrt 20 osob. Riziko spojené s touto nežádoucí událostí lze tak vyjádřit hodnotou 2 [úmrtí.rok^{-1}].

Je zřejmé, že při použití frekvence jako pravděpodobnostní veličiny, promítá se jednotka této veličiny přímo do jednotky rizika.

2.3 Intenzita výskytu

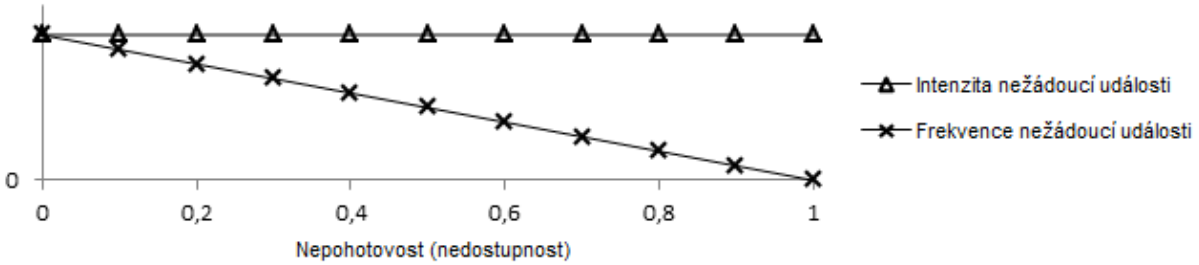
Intenzita poruch (resp. intenzita nežádoucích událostí) je definována jako limita, existuje-li, podílu podmíněné pravděpodobnosti, že porucha neopravitelného objektu nastane v časovém intervalu (t, $t + \Delta t$), a Δt, když se Δt blíží nule, za předpokladu, že v intervalu (0, t) nenastala porucha. Matematický zápis této definice je uveden v rovnici (5).

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P(t; t + \Delta t)}{\Delta t} \tag{5}$$

Jednotkou intenzity poruch (intenzity nežádoucích událostí) je [h^{-1}], tedy jednotka používaná pro frekvenci. Tato skutečnost vede k tomu, že se intenzita a frekvence často vzájemně zaměňují. Ale základní rozdíl mezi nimi spočívá v tom, že v případě intenzity poruch událost (porucha, nežádoucí událost) dosud nenastala, kdežto u frekvence se uvažuje její opakovaný výskyt.

Pro vysoce spolehlivé systémy s velmi nízkou hodnotou nepohotovosti U[1], je rozdíl v hodnotě intenzity a frekvence nepatrný a záměna intenzity s frekvencí nemá vliv na vypočtenou hodnotu rizika. Avšak s rostoucí hodnotou nepohotovosti U se rozdíl mezi hodnotou intenzity a frekvence zvětšuje. Vzájemný vztah mezi intenzitou a frekvencí nežádoucích událostí (např. selhání bezpečnostního systém) je uveden v rovnici (6) a graficky znázorněn na obr. 2. V rovnici (6) má frekvence jednotku [h^{-1}], ale v jiných případech může být vázána k jiné veličině, než je doba.

$$F(t) = \lambda(t) \cdot [1 - U(t)] \tag{6}$$



Obr. 2: Závislost frekvence na nepohotovosti při konstantní intenzitě

Z uvedeného vztahu je zřejmé, že při použití intenzity nežádoucí události se nadhodnocuje pravděpodobná možnost výskytu nežádoucí události a tedy zvyšuje konzervativnost výpočtu hodnoty rizika.

2.4 Očekávaný počet výskytů

Očekávaný počet výskytů nežádoucí události p nemá fyzikální jednotku. Podobně jako v případě pravděpodobnosti výskytu musí být u očekávaného počtu výskytů doplňující popis. Tento popis by měl obsahovat specifikaci časového intervalu (nebo počtu vyrobených kusů, ujetých kilometrů apod.) vztahujícího se k očekávanému počtu výskytů. Hodnotu rizika lze pak jednoduše vypočítat podle rovnice (7).

$$R = p \cdot C \tag{7}$$

Příklad:
Počet úmrtí na dálnicích ČR v roce 2014 byl 24. V roce 2015, tedy za dobu jednoho roku (specifikace podmínky), lze očekávaný počet výskytů úmrtí odhadnout na 25. Riziko spojené s dálničním provozem v ČR v roce 2015 se očekává 25 úmrtí.

Shodně jako v případě popsaném v 2.1, je při tomto výpočtu hodnota rizika vyjádřena ve stejných jednotkách, jako hodnota následků. Je vyjádřena v počtu úmrtí a výpočet vyžaduje doplňující popis.

3 Výpočet pravděpodobnosti selhání s ohledem na způsob fungování

Pro určování možnosti selhání komponent je třeba zjistit, jakým způsobem komponenty fungují. Podle způsobu fungování se pak přistupuje k výpočtu pravděpodobnosti selhání komponent. Výpočet lze provádět podle počtu namáhání, podle počtu otáček, podle počtu

[1] *Nepohotovost U je pravděpodobnost, že objekt v daném okamžiku nefunguje tak, jak je požadováno.*

sepnutí, podle doby fungování apod. Vždy je třeba respektovat charakter komponenty a způsob jejího využívání v provozu.

3.1 Výpočty podle namáhání

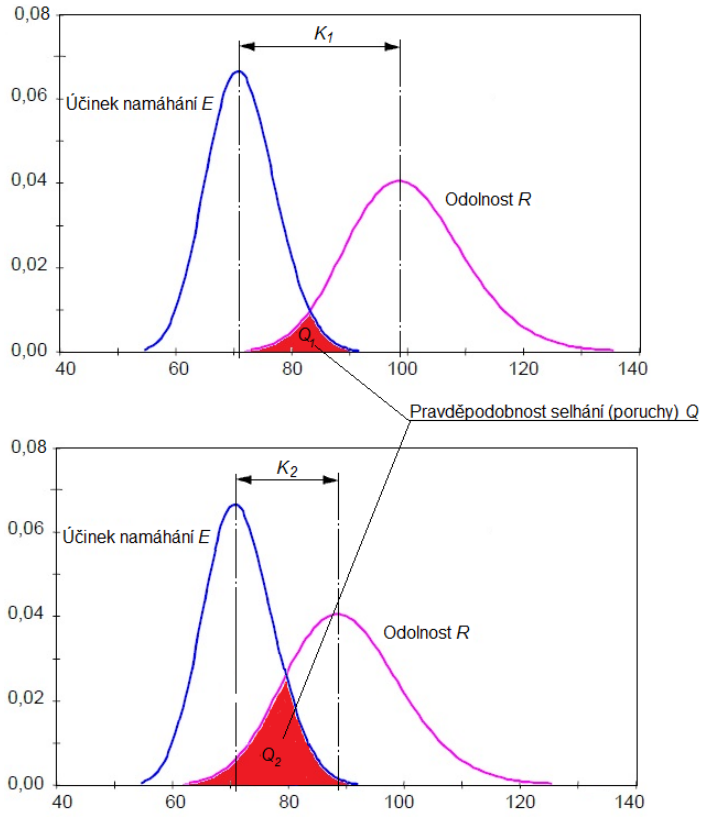
Výpočty pravděpodobnosti selhání při namáhání byly již na semináři Odborné skupiny pro spolehlivost prezentovány v roce 2004 [4]. Tyto postupy se běžně používají ve stavebnictví a v letectví, kde významnou rolu hraje životnost konstrukcí podrobených namáhání. Lze očekávat jejich postupné uplatnění i u kolejových vozidel, kdy bude požadován důkaz, že pravděpodobnost selhání konstrukce kolejového vozidla je na velmi nízké úrovni.

Při výpočtu pevnostně namáhaných konstrukcí lze uvažovat, že dominantním mechanismem, který vede k poruše konstrukce je ztráta pevnosti při namáhání. Zde bude třeba k predikci bezporuchovosti použít analýzu odolnost – namáhání, viz obr. 3. K tomu se používá hodnocení robustnosti konstrukce.

Robustností je míra odolnosti konstrukce vůči namáhání. Tuto robustnost (míru odolnosti) lze vyjádřit dvěma parametry:

a) součinitelem bezpečnosti *K*,
b) pravděpodobností selhání *P*.

První parametr je deterministický, druhý stochastický, přitom spolu vzájemně souvisejí a každý z nich postihuje jiný aspekt robustnosti konstrukce. Součinitel bezpečnosti *K* vyjadřuje odstup středních (průměrných) hodnot účinků namáhání *E* a odolnosti konstrukce *R*, viz obr. 3.



Obr. 3: Pravděpodobnost poruchy při namáhání

Pravděpodobnost selhání *P* pracuje s hustotou rozložení pravděpodobnosti účinků namáhání *E* a s hustotou rozložení pravděpodobnosti odolnosti konstrukce *R*. Na základě jejich znalosti je možné vypočítat pravděpodobnost selhání *P*. Čím menší bude hodnota pravděpodobnosti selhání *P*, tím robustnější bude navržená konstrukce. Tento přístup umožňuje kvantifikovat pravděpodobnostní složku rizika a vede k sofistikovanějším návrhům konstrukcí.

Pravděpodobnost selhání komponent vystavených namáhání lze určit podle následujících vztahů.

$$f_X(x) = \frac{1}{\sigma\sqrt{2\pi}} . e^{-\frac{(x-\mu)^2}{2\sigma^2}} = \frac{1}{\sigma} . \Phi(y) = \frac{1}{\sigma} . \Phi\left(\frac{x-\mu}{\sigma}\right) \qquad (8)$$

Kde

x je hodnota náhodné veličiny X (tedy hodnota pevnosti nebo hodnota namáhání),

μ je střední hodnota náhodné veličiny X (tedy střední hodnota z hodnot x, kterou může nabývat pevnost nebo namáhání),

σ^2 je rozptyl náhodné veličiny od střední hodnoty μ,

σ je směrodatná odchylka náhodné veličiny (tedy hodnoty pevnosti nebo hodnoty namáhání),

Φ je standardizované (normované) normální rozdělení.

Normální (Gaussovo) rozdělení hustoty pravděpodobnosti je dvouparametrické rozděleni s parametry (μ; σ^2). Standardizované (normované) normální rozdělení hustoty pravděpodobnosti má parametry (0;1) je dáno vztahem

$$\Phi(y) = \frac{1}{\sqrt{2\pi}} . e^{-\frac{y^2}{2}} \qquad y = \left(\frac{x-\mu}{\sigma}\right) \qquad (9)$$

$$\Phi(y) = \frac{1}{\sqrt{2\pi}} . e^{-\frac{y^2}{2}} = \Phi\left(\frac{x-\mu}{\sigma}\right) = \frac{1}{\sqrt{2\pi}} . e^{-\frac{\left(\frac{x-\mu}{\sigma}\right)^2}{2}} = \frac{1}{\sqrt{2\pi}} . e^{-\frac{(x-\mu)^2}{2\sigma^2}} \qquad (10)$$

Tento vtah je normovaný na střední hodnotu $\mu = 0$ a rozptyl $\sigma^2 = 1$ prostřednictvím převodu $(x - \mu)/\sigma$.

Normální rozdělení je vhodné pro náhodné veličiny s relativně malým rozptylem, tj. s hodnotou variačního koeficientu $CoV<0{,}3$. Variační koeficient $CoV = \sigma/\mu$. Tuto podmínku mechanické vlastnosti konstrukcí kolejových vozidel (pevnost) a zatížení za normálních provozních podmínek splňují.

Bezporuchovost konstrukce je charakterizována tzv. indexem spolehlivosti konstrukce β. Index spolehlivosti je konstrukce β při normálním rozdělením odolnosti konstrukce R a účinku zatížení E je dán vztahem

$$\beta = \frac{\mu R - \mu E}{\sqrt{\sigma_R^2 + \sigma_E^2}} \qquad (11)$$

Pravděpodobnost poruchy Q a pravděpodobnost bezporuchového stavu P lze stanovit podle následujících vztahů.

$$Q = \Phi(-\beta) = 1 - \Phi(\beta) = 1 - \frac{1}{\sqrt{2\pi}} . e^{-\frac{\beta^2}{2}} \quad (12)$$

$$P = 1 - Q = 1 - \Phi(-\beta) = \Phi(\beta) = \frac{1}{\sqrt{2\pi}} . e^{-\frac{\beta^2}{2}} \quad (13)$$

Hodnoty pravděpodobnosti stanovené tímto způsobem se vztahují na případ zatížení konstrukce statickým namáháním. Neuvažují však vliv cyklického namáhání komponent vedoucí k únavovým defektům.

Při opakovaném pevnostním namáhání komponent se zvažuje vliv cyklů namáhání na únavu materiálu. Aby komponenty odolaly cyklickému namáhání, určuje se funkční závislost mezi namáháním, počtem cyklů a hodnotou pevnosti materiálu komponenty. Výsledkem je stanovení mezní hodnoty dovoleného namáhání, kterému může být komponenta vystavena při dodržení požadované úrovně bezpečnosti. K tomu slouží pevnostní výpočty a analýzy podle příslušných norem. Při dosazení mezní hodnoty dovoleného namáhání do rovnice (8) až (13) získáme pravděpodobnost poruchy Q a pravděpodobnost bezporuchového stavu P komponenty pro počet cyklů namáhání, který byl uvažován při stanovení mezní hodnoty dovoleného namáhání. Jinými slovy řečeno jedná se o pravděpodobnost poruchy Q a pravděpodobnost bezporuchového stavu P komponenty za dobu její životnosti

Na základě hodnoty pravděpodobnosti poruchy Q pro uvažovaný počet cyklů namáhání n, lze stanovit pravděpodobnost poruchy komponenty vztažené na 1 namáhání a respektující únavu materiálu vztahem

$$\lambda = \frac{Q}{\mathrm{n}} \quad (14)$$

Kde

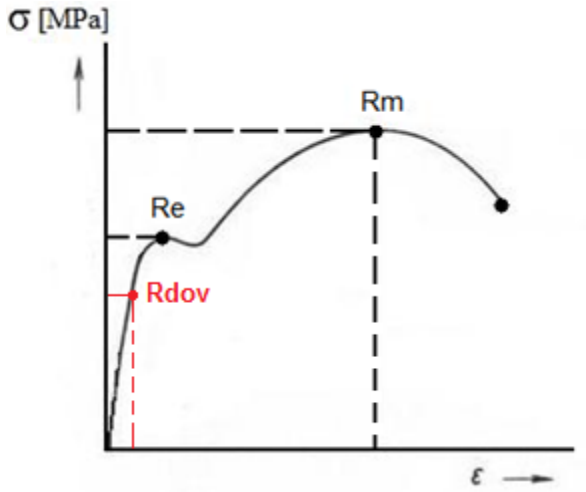
λ intenzita poruch na jedno namáhání [1/cykl],

n počet cyklů namáhání za životnost komponenty [1],

Q pravděpodobnost poruchy za životnost komponent [1].

Intenzita poruch λ reprezentuje podmíněnou pravděpodobnost poruchy. V praxi ji však lze chápat jako frekvenci poruch.

Při aplikaci výpočtu podle namáhání je však třeba jednoznačně vymezit definici selhání cyklicky namáhané komponenty. Selhání je zpravidla definováno jako dosažení či překročení mezního stavu, např. dovolené hodnoty namáhání. To lze zjednodušeně vysvětlit na obr. 4.



Obr. 4: Dovolená hodnota namáhání pro provozní zatížení

Dovolená hodnota namáhání pro provozní zatížení *Rdov* reprezentuje návrhovou odolnost *R*, která je stanovena pro cyklicky namáhané zařízení s ohledem na velikost provozního zatížení a počet cyklů uvažovaný za dobu životnosti zařízení.

3.2 Výpočty podle otáček a zatížení

Při výpočtu bezporuchovosti komponent, jejichž mechanismus degradace je dán počtem otáček a zatížení (např. ložiska, převodovky) se uplatňuje znalost počtu otáček a zatížení, což jsou základní faktory, které ovlivňují trvanlivost. Základní trvanlivost ložiska podle ISO 281:2007 je vyjádřena pomocí hodnoty L_{10} v miliónech otáček nebo L_{10h} v provozních hodinách. Hodnota L_{10} a L_{10h} vyjadřuje počet otáček či počet provozních hodin, při kterém dojde k poruše 10 % zkoušených komponent.

S ohledem na degradaci ložisek vlivem opotřebení se rozdělení dob do poruchy popisuje dvouparametrickým Weibullovo rozdělením s distribuční funkcí:

$$F(t) = 1 - \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \tag{15}$$

Kde

$F(t)$ distribuční funkce rozdělení dob do poruchy (funkce poruchovosti),

t doba [h],

α parametr polohy rozdělení (parametr měřítka, charakteristický život) [h],

β parametr tvaru rozdělení (parametr sklonu) [1],

Pravděpodobnost bezporuchového provozu se určí podle vztahu

$$R(t) = 1 - F(t) = \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \tag{16}$$

Při výpočtu pravděpodobnosti bezporuchového provozu je třeba znát hodnotu parametru α a hodnotu parametru β. Parametr α udává dobu, při kterých došlo k poruše u 63,2 % komponent. Parametr β charakterizuje vliv stárnutí na poruchovost komponent.

Pro ložiska se běžně uvažuje hodnota parametru β = 1,5. Tato hodnota je přiměřeně konzervativní k tomu, aby dostatečně zohlednila vliv opotřebení ložisek, který se projeví vzrůstem hodnoty intenzity poruch[2]. Hodnota parametru α se u ložisek neudává. Nahrazuje ji hodnota L_{10h}. S ohledem na rozdíl mezi dobou poruchy 10 % ložisek a dobou poruchy 63,2 % ložisek se provádí úprava rovnice (16).

Náhodnou veličinou X je doba do poruchy. Pravděpodobnost, že ložisko přežije bez poruchy dobu t, je dána funkcí přežití doby t.

$$R(t) = \Pr(X \geq t) = \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \tag{17}$$

Doba, která bude přežita je dána hodnotou základní trvanlivosti ložiska L_{10h}. Je to doba, která bude přežita a s pravděpodobností $R\,(L_{10h}) = 0{,}9$.

$$R(L_{10h}) = \exp\left[-\left(\frac{L_{10h}}{\alpha}\right)^{\beta}\right] = 0{,}9 \tag{18}$$

$$\left(\frac{L_{10h}}{\alpha}\right)^{\beta} = -\ln 0{,}9 \tag{19}$$

$$\alpha^{\beta} = -\frac{L_{10h}^{\beta}}{\ln 0{,}9} \tag{20}$$

Vztah (20) představuje transformaci parametru α z 63,2 % poruch ložisek na 10 % poruch ložisek. Pod dosazení do vztahu (17) lze vyjádřit pravděpodobnost bezporuchového stavu ložiska za dobu t vztahem

$$R(t) = \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] = \exp\left[-\frac{t^{\beta}}{\alpha^{\beta}}\right] = \exp\left[-\frac{t^{\beta}}{\left(-\frac{L_{10h}^{\beta}}{\ln 0{,}9}\right)}\right] = \exp\left[(\ln 0{,}9)\cdot\left(\frac{t}{L_{10h}}\right)^{\beta}\right] \tag{21}$$

Hodnota intenzity poruch není při Weibullovo rozdělení konstantní. Proto se pro praktické aplikace určuje střední (průměrná, konstantní) hodnota intenzity poruch za specifickou dobu provozování (fungování) ložiska podle vztahu:

$$\lambda_c = \frac{-(\ln 0{,}9)\cdot\left(\frac{T_f}{L_{10h}}\right)^{\beta}}{T_f} \tag{22}$$

Kde

λ_c intenzita poruch pro trvalý provoz [1/h],

T_f doba trvalého provozování (fungování) ložiska [h],

[2] *Vždy je třeba ověřit, zda pro konkrétní provozní nasazení je uvedený předpoklad správný.*

L_{10h} základní trvanlivost ložiska v hodinách počet provozních hodin, při kterém dojde k poruše 10 % ložisek [h].

3.3 Výpočty podle počtu cyklů sepnutí a rozepnutí

Při výpočtu bezporuchovosti komponent, jejichž mechanismus degradace je dán počtem sepnutí (komponenty typu spínačů, ovládačů, relé apod.) se uplatňuje znalost počtu pracovních cyklů, kterým je počet sepnutí. Pro přepočet počtu sepnutí na intenzitu poruch lze využít vhodné postupy uvedené v příslušných normách, např. pomocí hodnoty B_{10}. Hodnota B_{10} udává dobu nebo počet sepnutí, při kterém dojde k poruše 10 % zkoušených prvků. Podle EN 62061, odstavec 6.7.8.2.1 lze intenzitu poruch pro trvalý (nepřerušovaný) provoz určit podle vztahu:

$$\lambda_c = \frac{0{,}1 \cdot C}{B_{10}} \tag{23}$$

Kde

λ_c intenzita poruch pro trvalý provoz [1/h],

C počet provozních cyklů (počet sepnutí/rozepnutí) za hodinu [1/h],

B_{10} počet sepnutí, při kterém dojde k poruše 10 % zkoušených komponent [1].

3.4 Výpočty podle doby fungování

U trvale provozovaných komponent je úroveň bezporuchovosti dána hodnotou intenzity poruch $\lambda(t)$, která je funkcí času. Tam, kde se uvažuje, že intenzita poruch není závislá na namáhání, otáčkách či postupné degradaci materiálových vlastností se počítá s konstantní hodnotou intenzity poruch $\lambda(t) = \lambda$.

V případě, že zařízení není trvale v provozu, se u komponent konzervativně předpokládá, že i v době mimo provoz podléhají komponenty určité míře degradace či podléhají určitému šoku při změně režimu (provozní režim, odstávka). Tato složka poruchovosti se odhaduje na 10% hodnoty intenzity poruch trvalého provozu[3]. Proto pro zařízení, které bývá provozováno jen po část kalendářní doby, se používá přepočet hodnoty intenzity poruch na hodnotu ekvivalentní intenzity poruch podle následujícího vztahu.

$$\lambda = \frac{\lambda_c . T_f + 0{,}1 . \lambda_c . T_{nf}}{T_f + T_{nf}} \tag{24}$$

Kde

λ_c intenzita poruch pro trvalý provoz [1/h],

λ intenzita poruch pro přerušovaný provoz [1/h],

T_f doba fungování [h],

T_{nf} doba bez fungování (doba bez namáhání, bez napětí) [h].

[3] *Vždy je třeba ověřit, zda pro konkrétní provozní nasazení je uvedený předpoklad správný.*

4 Hodnota přijatelného rizika

Stávající normy platné pro drážní zařízení neuvádějí hodnotu přijatelného rizika. Pouze doporučují aplikovat některé známé přístupy řízení rizika (ALARP, MEM, GAMAB). Při použití matice rizika doporučují provést její kalibraci, tj. stanovit přiřazení hodnot pravděpodobnosti a závažnosti následků a stanovit v této matici hranici mezi přijatelným a nepřijatelným rizikem. O nevhodném přístupu k sestavení stupnic pravděpodobnosti a následků podle informativních příloh norem k funkční bezpečnosti a různých doporučení již bylo v rámci seminářů Odborné skupiny pro spolehlivost několikrát pojednáno. Z toho důvodu je v této kapitole jen stručně pojednáno o kritériu přijatelného rizika podle společné bezpečnostní metody (CSM).

Prováděcí nařízení Komise (EU) č. 420/2013 o společné bezpečnostní metodě pro hodnocení a posuzování rizik bylo upraveno dalším prováděcím nařízením Komise (EU) 2015/1136. Z úprav je pro hodnocení rizik důležité zpřesnění pojmů týkajících se pravděpodobnost nehody a úrovně závažnosti následků. To je podstatné pro použití kalibrované matice rizika publikované Evropskou agenturou pro železnice (ERA) v dokumentu *Soubor příkladů posuzování rizik a některých možných nástrojů podporujících nařízení CSM* (dokument ERA/GUI/02-2008/SAF). Tuto matici rizika zachycuje obr. 5.

Četnost výskytu nehody (způsobené nebezpečím)	Úroveň rizika			
Častá (10^{-4} za hodinu)	Nepřípustné	Nepřípustné	Nepřípustné	Nepřípustné
Pravděpodobná (10^{-5} za hodinu)	Nepřípustné	Nepřípustné	Nepřípustné	Nepřípustné
Příležitostná (10^{-6} za hodinu)	Přijatelné	Nepřípustné	Nepřípustné	Nepřípustné
Mizivě pravděpodobná (10^{-7} za hodinu)	Přijatelné	Přijatelné	Nepřípustné	Nepřípustné
Nepravděpodobná (10^{-8} za hodinu)	Přijatelné	Přijatelné	Přijatelné	Nepřípustné
Krajně nepravděpodobná (10^{-9} za hodinu)	Přijatelné	Přijatelné	Přijatelné	Přijatelné
	Nevýznamné	Okrajové	Kritické	Katastrofální
	Úrovně závažnosti důsledků nebezpečí (tj. nehody)			

Hodnocení rizika	Omezení/usměrnění rizika
Nepřípustné	Riziko musí být odstraněno.
Přijatelné	Riziko je přijatelné. Je třeba provést nezávislé posouzení.

Obr. 5: Typický příklad kalibrované matice rizika (převzato z ERA/GUI/02-2008/SAF)

Katastrofickou nehodou se rozumí nehoda, jež se obvykle dotýká velkého množství osob a jejímž důsledkem je více smrtelných nehod.

Kritickou nehodou se rozumí nehoda, jež se obvykle dotýká velmi malého množství osob a jejímž důsledkem je nejméně jedna smrtelná nehoda.

Vysoce nepravděpodobným se rozumí výskyt selhání s četností nižší nebo rovnou 10^{-9} za hodinu provozu.

Nepravděpodobným se rozumí výskyt selhání s četností nižší nebo rovnou 10^{-7} za hodinu provozu.

Další upřesnění k tomu, jak chápat pojem katastrofická a kritická nehoda, přináší dokument *Guideline for the application of harmonised design targets (CSM-DT)for technical systems as defined in (EU) Regulation 2015/1136within the risk assessment process of Regulation 402/2013* (dokument ERA-REC-116-2015-GUI), který byl vydán 12/2016.

Lze tedy konstatovat, že pro hodnocení přijatelnosti rizika drážních zařízení je k dispozici kritérium přijatelnosti. Toto kritérium lze však aplikovat jen v případě, kdy je proveden kvantitativní výpočet rizika.

Společná bezpečnostní metoda však uplatnění kritéria přijatelnosti rizika omezuje **jen pro navrhování elektrických, elektronických a programovatelných elektronických technických systémů** za účelem vzájemného uznávání těchto zařízení v rámci EU. Pro ostatní zařízení vyžaduje použití kodexů správné praxe či použití referenčního systému. To však nemění nic na skutečnosti, že toto kritérium je obecně platné a lze je použít i pro systémy založené na mechanických, pneumatických či hydraulických prvcích. Není rozdíl mezi rizikem způsobeným selháním elektronického, mechanického či jiného zařízení.

5 Závěr

Postupy založené na pravděpodobnostním posouzení rizika nacházejí stále širší uplatnění. Funkční bezpečnost není omezena jen na úzce vymezené bezpečnostní systémy či zabezpečovací zařízení. Obecně se funkční bezpečnost chápe jako bezpečnost zařízení při jeho fungování. A všechny poruchy či jiné nežádoucí události, které vedou ke vzniku nebezpečných situací jsou tedy předmětem posuzování rizik. K tomu je však třeba znalost postupů pro výpočet pravděpodobnosti selhání a porozumění tomu, co je výsledkem výpočtu pravděpodobnosti selhání.

Literatura

[1] ISO GUIDE 73:2009 Risk management – Vocabulary

[2] TNI 01 0350 Management rizik – Slovník (Pokyn 73)

[3] ZAJÍČEK, J. – KAMENICKÝ, J. – FUCHS, P.: Odlišné způsoby výpočtu rizika. *In: Bezpečnostní technologie, Systémy a Management 2015*, UTB Zlín.

[4] HOLICKÝ, M.: Pravděpodobnostní metody navrhování stavebních konstrukcí. *In: Spolehlivost ve stavebnictví. Sborník z 15. setkání Odborné skupiny pro spolehlivost*. Česká společnost pro jakost, Praha, 2004. Dostupné z WWW:

http://www.csq.cz/uskutecneneseminarespolehlivost/

ISBN 978-80-02-02709-6

Nejčastější mýty ve spolehlivosti

Sborník přednášek
kolektiv autorů
1. vydání
rok vydání 2017, Česká společnost pro jakost
vazba brožovaná, 38 stran