ČESKÁ SPOLEČNOST PRO JAKOST
Novotného lávka 5, 116 68 Praha 1

ÚLOHA
A APLIKAČNÍ MOŽNOSTI METODY FMEA
PŘI ZABEZPEČOVÁNÍ SPOLEHLIVOSTI

MATERIÁLY Z 5. SETKÁNÍ
ODBORNÉ SKUPINY PRO SPOLEHLIVOST

Praha, listopad 2001

OBSAH

Princip a možnosti aplikace metody FMEA/FMECA 2
Doc. Ing. A.Mykiska, CSc., ing. Votava

Aplikace metody FMEA procesní v SGS Hořovice 12
Milan Polák, SGS Hořovice

Provedení FMECA pro zařízení provozované na cvičném letadle L159 19
Ing. Čech, ITC

Využití metody FMEA při analýze bezpečnosti dopravního letounu 34
Doc.ing.Vintr, CSc.

Komplexní hodnocení spolehlivosti varovného systému 41
Ing. Fuchs, CSc.

PRINCIP A MOŽNOSTI APLIKACE METODY FMEA/FMECA

Doc. Ing. Antonín Mykiska, CSc. - Ing. Pavel Votava

Metoda **Analýza druhů poruchových stavů a jejich důsledků** (**FMEA** - Fault Modes and Effects Analysis) je metoda systematické analýzy možných druhů a důsledků poruchových stavů a jejich uspořádání podle stupně závažnosti. Rozšířením metody FMEA o hodnocení kritičnosti důsledků s uvážením pravděpodobností (nebo četností) jejich výskytu je metoda **Analýza druhů, důsledků a kritičnosti poruchových stavů** (**FMECA** - Fault Modes, Effects and Criticality Analysis). V praxi se často provádí metoda FMECA, avšak používá se označení FMEA.

*Pozn. 1: Významově rovnocenné k termínu „**poruchový stav**“ se používají termíny „**porucha**“ a „**vada**“.*

Pozn. 2: Vedle uvedeného českého názvu metody podle ČSN IEC 300-3-1:1993 se běžně používají další česká názvy:

- *„Analýza způsobů a důsledků poruch“ (ČSN IEC 812:1992),*
- *„Analýza možností vzniku vad a jejich následků“ (český překlad VDA 3.2),*

Metodu FMEA/FMECA lze obecně charakterizovat jako postup (proces) systematické a podrobné analýzy vznikající konstrukce, resp. návrhu výrobního procesu výrobku z hlediska vzniku, důsledků a příčin všech potenciálně možných poruch (vad), jež mají původ v samotné konstrukci, resp. v návrhu výrobního procesu. Takto uplatňovaný postup analýz umožňuje identifikovat potenciálně možné poruchy (vady), jejich příčiny a zhodnotit jejich důsledky z pohledu zákazníka. Volbou vhodných nápravných opatření pak umožňuje preventivně odstranit nejvýznamnější z nich. Využívá se při tom zkušeností z konstrukcí a výrobních procesů výrobků předchozích generací. Při systematickém dlouhodobějším využívání metody a současné realizaci zpětné vazby z období výroby a provozu umožňuje zkušenosti odborných pracovníků (konstruktérů, návrhářů, technologů atd.) kumulovat, zvyšovat a uchovávat.

Metodu FMEA je nutno chápat jako metodu týmovou, jeden pracovník sám ji může jen obtížně kvalitně provádět, neboť by chyběly pohledy na problematiku z dalších profesních oblastí. Metoda FMEA při svém provádění musí být provázána s řídícími zásahy v podobě nápravných opatření k odstranění příčin identifikovaných nejzávažnějších potenciálně možných poruchových stavů (vad). K její úspěšné aplikaci je proto nezbytné manažerské zajištění (vymezení pravomocí, odpovědností, přidělení zdrojů atd.). Z tohoto pohledu lze metodu FMEA/FMECA charakterizovat jako jeden z nástrojů managementu jakosti, resp. managementu spolehlivosti.

Metoda FMEA/FMECA patří mezi nejpoužívanější kvalitativní metody analýzy bezporuchovosti. V současné době je často vnímána (a řadou výrobců finálních výrobků, zejména v automobilovém a leteckém průmyslu, vyžadována od jejich dodavatelů) jako nástroj řízení a zlepšování jakosti v předvýrobních etapách – tj. jako metoda kontinuálního zlepšování úrovně jakosti návrhu výrobku. V těchto případech je méně vnímána jako kvalitativní analýza bezporuchovosti a zpravidla se pro ní používá jen označení FMEA!

1. Podstata metody FMEA

Základem metody jsou tedy postupy systematického zkoumání a analýz objektu (konstrukce, návrhu výrobního procesu) v předvýrobních etapách životního cyklu výrobku (chápaného jako systém) z hlediska jeho potenciálně možných poruchových stavů (vad) materiálu, součástek, zařízení apod., jejich mechanismů a závažnosti jejich důsledků, projevujících se na nejbližší vyšší funkční úrovni výrobku. Příčiny těchto potenciálně možných poruchových stavů (vad) se zjišťují v závislosti na vznikající konstrukci, resp. v další etapě v závislosti na vznikajícím návrhu výrobního procesu. Primárním výsledkem je identifikace nejzávažnějších druhů poruchových stavů (vad) z hlediska jejich důsledků a zkoumání jejich příčin. Na tuto část bezprostředně navazuje návrh a provedení vhodných nápravných opatření k jejich odstranění (nebo alespoň potlačení), včetně stanovení odpovědností a termínů jejich provedení. Umožňuje tedy provést vhodná opatření s minimálními ztrátami již v předvýrobních etapách životního cyklu výrobků (ve stádiu návrhu konstrukce výrobku nebo procesu).

Při aplikaci metody se používá induktivní postup "zdola nahoru", tj. analýza začíná na "nejnižší" úrovni, u každého identifikovaného potenciálně možného poruchového stavu se zkoumá a usuzuje, jaké může mít důsledky na vlastnosti na nejblíže vyšší úrovni systému. Výsledný důsledek se stane druhem poruchového stavu na následující vyšší úrovni systému. Postupným opakováním tohoto postupu až k nejvyšší úrovni se zjišťují a hodnotí všechny jednotlivé potenciálně možné poruchové stavy konstrukce či procesu výrobku jako celku.

2. Základní způsoby aplikace metody

Metoda má zhruba tři základní způsoby užití:

I. V období vznikajícího návrhu, konstrukce, projektu slouží k identifikaci a analýze všech potenciálně možných poruchových stavů, které na základě inženýrských zkušeností mohou uvažovaným konstrukčním řešením nastat, v následné analýze závažnosti jejich následků a hledáním všech jejich příčin, které náleží do samotné konstrukce výrobku, s cílem odstranit je nebo potlačit změnou či úpravou konstrukčního řešení - tzv. **FMEA konstrukční.**

II. Při návrhu procesu (nejčastěji výrobního či montážního procesu, jímž se bude navržená konstrukce či projekt výrobku realizovat) slouží k identifikaci a analýze všech jeho potenciálně možných poruchových stavů, které mohou vést k neshodnému výrobku na jeho výstupu, jejichž příčiny mohou spočívat ve vlastním navrhovaném postupu procesu (jednotlivé výrobní a kontrolní operace a činnosti) s cílem umožnit návrh nápravných opatření k jejich odstranění (nebo potlačení) úpravou nebo změnou jeho návrhu (tj. změnou nebo úpravou činností a způsobu jejich provádění výrobního či montážního postupu, jímž je proces realizován) - tzv. **FMEA procesní (výrobní)**. FMEA procesní by měla navazovat na provedenou FMEA konstrukční a provádí se jako závěrečná ve fázi schvalování technické přípravy výrobního nebo montážního postupu.

III. Rozšířením analýz na vzájemné funkční souvislosti jednotlivých dílů při FMEA/FMECA konstrukční, resp. jednotlivých operací procesů, včetně jejich analýzy z hlediska všech "zúčastněných" prvků (člověk - stroj - materiál - prostředí) při FMEA/FMECA procesní se dospělo k jejich komplexnějšímu pojetí, které je označováno jako tzv. **FMEA systémová** (výrobková).

Pozn.: Takto je FMEA systémová prezentována a podrobněji definována ve VDA 4.2 a ve VDA 3.2 jako nástroj analýzy spolehlivosti (přesněji vzato bezporuchovosti), zatímco FMEA konstrukční a FMEA procesní jsou svým charakterem více vnímány jako nástroje neustálého zlepšování jakosti konstrukce a procesů souvisejících se vznikem objektu.

Používání metody FMEA se rozšířilo zejména v posledním desetiletí pod tlakem výrobců finálních zařízení (obzvláště automobilů) na své dodavatele. Díky tomu se stala především FMEA procesní jedním z běžnějších nástrojů zabezpečování a zlepšování jakosti v předvýrobních etapách.

3. Obecný postup úspěšné a efektivní aplikace metody FMEA

Praktická **aplikace metody** se uskutečňuje postupným **vyplňováním** určitým způsobem **normalizovaných tabulek FMEA,** čímž je její provedení rovněž **dokumentováno**. Postup aplikace metody FMEA ilustruje tab. 1. Položky 1. až 8. v tab. 1 jsou identifikační parametry aplikace metody na analýzu konkrétního objektu (návrh jeho konstrukce nebo procesu) a uvádějí se v záhlaví tabulek FMEA.

Vlastní provádění metody pak zahrnuje čtyři charakteristické skupiny činností:

1. Identifikují se jakékoliv myslitelné, potenciálně možné poruchové stavy (často označované též "vady") a analyzují se jejich možné projevy, důsledky a příčiny (položky 9 až 13 v tab. 1); provádění tohoto kroku analýzy vyžaduje pro ně stanovit:
   - místo a/nebo popis;
   - projev;
   - důsledek;
   - příčinu.

2. Hodnotí se současný stav tzv. rizikovým číslem MR/P (přesněji míra rizika/priorita) – položky 15 až 18 v tab. 1:

$$MR/P = Výsk \times Význ \times Odhal, \quad \ldots (1)$$

kde Výsk - bodové ohodnocení pravděpodobnosti (četnosti) výskytu (tj. vzniku) poruchového stavu,

Význ - bodové ohodnocení významu následku (tj. závažnosti z hlediska nepříznivých důsledků pro zákazníka),

Odhal - bodové ohodnocení odhalitelnosti (tj. detekce) příčiny, resp. následku poruchového stavu před dodáním zákazníkovi.

Bodová ohodnocení se nejčastěji získávají roztříděním výskytu, významu a odhalitelnosti vždy do deseti tříd podle zvolených klasifikačních tabulek, jejichž příklady jsou uvedeny v tab. 2 až 4. Např. pro činitel Význ v (1) je hodnota 10, resp. 9 přiřazena případům, kdy vzniká bezpečnostní riziko, resp. riziko nesplnění zákonných předpisů, resp. úplné neschopnosti plnit požadované funkce (u automobilu např. jeho nepojízdnost), hodnota 1 je přiřazena případům, kdy má následek poruchového stavu (vady) jen malý význam pro konečného uživatele (např. velmi malé omezení funkcí, rozeznatelné jen odborníkem).

3. Navrhnou se opatření k nápravě (změna či úprava konstrukčního řešení, návrhu výrobního postupu apod.) s vymezením termínů a odpovědností – viz položky 19, 20 v tab. 1.
4. Po realizaci opatření k nápravě se provede opakovaně analýza podle 2. bodu postupu včetně hodnocení rizikovým číslem MR/P zlepšeného stavu (položky 21, 22 v tab. 1).

Metoda je užitečná zejména při analýze nových a nevyzkoušených systémů, součástek a procesů s jednodušší strukturou, u nichž platí princip kauzality, což bývá splněno u většiny technických systémů (elektrická, mechanická, hydraulická, resp. kombinovaná technická zařízení, systémově pojaté technologické výrobní a montážní procesy apod.).

Při aplikaci FMEA se vychází z technicko-inženýrské "kolektivní" zkušenosti a proto je nezbytné k tomu účelu vytvořit **řešitelský tým**. Jeho vhodné sestavení a zejména dobré vedení je jedním z důležitých předpokladů úspěšného využívání metody v podmínkách konkrétní organizace.

Má-li se metoda v organizaci stát rutinně a systematicky používaným nástrojem zlepšování a zabezpečování spolehlivosti (a obecněji jakosti) v předvýrobních etapách, je prakticky nezbytná její **počítačová podpora**. Příslušný software pro její počítačovou podporu by měl být schopen zejména:

- usměrňovat činnost řešitelského týmu ve smyslu systematičnosti a úplnosti jeho postupu,
- umožňovat efektivní a rychlý postup aplikace metody v daném konkrétním případě,
- umožňovat takové ukládání zkušeností v podobě výsledků, k nimž je snadný a rychlý přístup při dalších aplikacích,
- dokumentovat výsledky v podobě, která umožňuje jejich efektivní prezentaci při jednáních se zákazníky, při externích auditech, při oficiálním přezkoumání návrhu apod.

4. Postup při aplikaci metody FMEA v podmínkách konkrétní organizace

Postup při systematické aplikaci metody v podmínkách konkrétní organizace (podniku) lze obecně charakterizovat těmito kroky:

⇒ Vrcholové vedení rozhodne o používání metody FMEA v organizaci, jmenuje odpovědného pracovníka za vypracování podnikové směrnice pro aplikaci FMEA, která stanovuje postup analýzy, odpovědnosti a pravomoci spojené s řešením a další náležitosti, které mají charakter vazeb v příslušném systému jakosti organizace.

⇒ Jmenovaný pracovník, odpovědný za provádění metody FMEA, navrhne členy řešitelské skupiny (týmu), kteří po schválení vrcholovým vedením jsou jmenováni do týmu pro vlastní

<table>
<tr><td>FMEA konstrukce:
Název a popis rubriky</td><td>FMEA procesu:
Název a popis rubriky</td></tr>
<tr><td colspan="2">1. MODEL - TYP:
Označí se typ a druh výrobku, na který se rozbor provádí</td></tr>
<tr><td colspan="2">2. ČÍSLO DOKUMENTU:
Uvede se pořadové číslo listu dokumentu rozboru jedné skupiny/dílu analyzovaného objektu</td></tr>
<tr><td colspan="2">3. ČÍSLO DÍLU (OBJEKTU):
Uvede se číslo nebo stanovený kód analyzovaného skupiny/dílu objektu</td></tr>
<tr><td colspan="2">4. NÁZEV DÍLU (OBJEKTU):
Uvede se název dílu, skupiny výrobku, které jsou předmětem analýzy</td></tr>
<tr><td colspan="2">TECHNICKÉ ZMĚNY:
Uvede se číslo, resp. kód uskutečněných technických změn</td></tr>
<tr><td colspan="2">5. ZPRACOVAL:
Uvede se jméno, oddělení a telefon zpracovatele analýzy</td></tr>
<tr><td colspan="2">6. DATUM ZPRACOVÁNÍ:
Uvede se datum zpracování analýzy</td></tr>
<tr><td colspan="2">7. DATUM PŘEPRACOVÁNÍ:
Uvede se datum přepracování, event. doplnění předkládané analýzy</td></tr>
<tr><td colspan="2">8. DODAVATEL: Uvede se dodavatel, event. subdodavatel analyzovaného objektu</td></tr>
<tr><td>9. SYSTÉM / ZNAK:
Popis místa výskytu nebo vzniku potenciálně možného poruchového stavu (vady). Zpravidla se uvádí popisem užitné funkce, resp. vlastností objektu.</td><td>9. SYSTÉM / ZNAK:
Popis místa výskytu nebo vzniku potenciálně možného poruchového stavu (vady), zpravidla název technologické operace ve výrobním postupu
Pozn.: Někdy označení názvu technologické operace může být příliš rozsáhlé a proto je nevhodné pro označení systému</td></tr>
<tr><td>10. MOŽNÉ DRUHY PORUCH (VAD):
Postupně se uvedou všechny potenciálně možné druhy poruch (vad), které mohou nastat u analyzovaného dílu, resp. konstrukční skupiny. Je vhodné čerpat ze zkušeností získaných na podobných postupech u předešlých konstrukcí; dalšími zdroji jsou zprávy o poruchách dílu v provozu, při laboratorních zkouškách apod. Je nutné uvažovat i poruchy, které mohou nastat i při různých netypických provozních podmínkách.</td><td>10. MOŽNÉ DRUHY PORUCH (VAD):
Postupně se uvedou všechny potenciálně možné druhy poruch (vad), které mohou nastat v jednotlivých krocích analyzovaného procesu. Vychází se z předpokladu jeho potenciálně možného vzniku a je přitom vhodné čerpat ze zkušeností získaných na podobných postupech</td></tr>
<tr><td colspan="2">11. MOŽNÉ NÁSLEDKY DRUHŮ PORUCHOVÝCH STAVŮ (DRUHŮ PORUCH, VAD):
Pro daný druh poruchového stavu, resp. typ poruchy (vady) se uvede jejich následek z hlediska uživatele. Musí být použito označování v pojmech vlastností výrobků - systému nebo subsystému</td></tr>
<tr><td colspan="2">12. KONTROLNÍ POLOŽKY:
Znakem se označí vybrané díly a materiály, které podléhají zvláště stanovenému systému kontroly z důvodu bezpečnosti, zvláštní důležitosti pro funkci výrobku apod.</td></tr>
</table>

13. MOŽNÉ PŘÍČINY DRUHŮ PORUCHOVÝCH STAVŮ (DRUHŮ PORUCH, VAD): Uvádějí se všechny možné příčiny konstrukčního charakteru daného typu poruchy. U příčin poruch konstrukčně upravovaných součástí se vychází z příčin, vyskytujících se u předešlé konstrukce. U nových konstrukcí se předpokládá co nejvíce příčin poruchy.	13. MOŽNÉ PŘÍČINY DRUHŮ PORUCHOVÝCH STAVŮ (DRUHŮ PORUCH, VAD): Uvádějí se všechny možné příčiny poruch výrobního charakteru.
14. KONTROLNÍ OPATŘENÍ (ČINNOSTI): Uvede se přehled běžných kontrolních činností, které jsou doporučeny k zabránění vzniku poruchy, případně mají její vznik detekovat. Za běžné kontrolní činnosti (výrobní předpisy, systém kontroly jakosti apod.) se považují takové, které jsou standardně užívány u podobných procesů. Je-li potřebné uvažovat jakékoliv další kontroly, uvedou se do doporučených činností a doplní se do technických podmínek (TP). Pro zcela nové procesy prakticky běžné kontroly neexistují a odpovědný pracovník musí odhadnout, které z ověřených běžných kontrol je možné užít	
15. VÝSKYT (VÝSK): Provede se odhad pravděpodobnosti (resp. četnosti) výskytu typu poruchy (vady) a jeho zatřídění do tříd 1 - 10 podle klasifikační tabulky "stupeň výskytu". Výskytem poruchy (vady) u FMEA konstrukce se rozumí pravděpodobnost (resp. četnost), s níž se konstruktér dopustí při své konstrukční činnosti stanovené vady, resp. vady téměř shodné. Rozsah termínu "téměř shodné" stanoví podniková směrnice pro aplikaci FMEA	15. VÝSKYT (VÝSK): Provede se odhad pravděpodobnosti (nebo četnosti) výskytu typu poruchy (vady) a jeho zařazení do tříd 1 - 10 podle klasifikační tabulky "stupeň výskytu". Do toho se zahrne i vliv kontrolních činností, které mají zabránit výskytu příčin poruchy
16. VÝZNAM (VÝZN): Provede se odhad významu projevu a důsledku poruchy z hlediska uživatele a jeho zařazení do tříd 1 - 10 podle příslušné klasifikační tabulky. Zatřídění podle závažnosti může být změněno pouze na základě úprav technologického postupu apod. a nelze je ovlivnit běžnými kontrolami; zařazení do tříd je bezprostředně vázáno na důsledek poruchy, proto všechny příčiny poruchy vztahující se ke stejnému typu poruchy mají stejnou třídu závažnosti	
17. ODHALITELNOST (ODHAL): Provede se odhad pravděpodobnosti (četnosti) odhalení (detekce) příčiny poruchy dříve, než se výrobek dostane k uživateli, a zatřídění ve stupních 1 - 10 podle příslušné klasifikační tabulky. Tím se rozumí pravděpodobnost, resp. četnost, se kterou bude odhalena příslušná vada schvalovacím řízením dané konstrukce	17. ODHALITELNOST (ODHAL): Provede se odhad pravděpodobnosti (četnosti) jevu, že neshodný díl na výstupu procesu pro jeho každou příčinu poruchy lze odhalit kontrolami dříve než opustí výrobní linku (náhodné kontrolní úkony nejsou schopny jednotlivé neshody odhalit
18. MÍRA RIZIKA - PRIORITA (MR/P): Rizikové číslo MR/P je součin tříd výskytu, významu a odhalitelnosti. Stanovuje se zvlášť pro každou příčinu poruchy a slouží zejména k identifikaci prioritních příčin poruch, u kterých je nutno stanovit a realizovat nápravné činnosti	

19. DOPORUČENÁ NÁPRAVNÁ OPATŘENÍ: Stručný popis doporučených nápravných opatření pro zlepšení stavu s jejich přesným určením - např. konstrukční změny; důraz je nutno klást na prevenci vzniku poruchy a na její určování.	19. DOPORUČENÁ NÁPRAVNÁ OPATŘENÍ: Stručný popis doporučených nápravných opatření, která sníží rizikové číslo dané příčiny poruchy. Nápravná opatření mohou být v oblasti výrobní a jejich zaměření vyplývá z analýzy příčin poruchy.
20. ODPOVĚDNOST: Uveden útvar, resp. pracovník, který je zodpovědný za provedení nápravné činnosti	
21. PROVEDENÁ OPATŘENÍ: Po realizaci nápravných opatření se uvede jejich popis, výsledek, datum ověření apod.; provede se nový odhad tříd výskytu, významu a odhalitelnosti poruchy při zlepšeném stavu	
22. VÝSLEDNÉ RIZIKOVÉ ČÍSLO, MÍRA RIZIKA - PRIORITA (MR/P): Vypočteme výsledné rizikové číslo po ukončené nápravné činnosti	

Tab. 1 – Příklad systematického dokumentovaného postupu provádění metody FMEA (levý sloupec - FMEA konstrukční, pravý sloupec FMEA procesní)

provádění analýzy. Obvykle bývá stanoven „koordinátor FMEA“ (tzv. zmocněnec pro FMEA), který zpravidla vede konkrétní práci týmu a je tedy bezprostředně vedoucím řešitelské skupiny.

⇒ Při každém svolání týmu je přesně stanoven obsah řešené problematiky. Je nutné, aby se práce v týmu účastnili odborníci, kteří mohou svými poznatky a zkušenostmi přispět ke zdárnému řešení.

⇒ Vedoucí řešitelské skupiny seznámí členy s předmětem analýzy a musí dbát na to, aby se mohli všichni členové řešitelské skupiny (týmu) k řešenému problému vyjádřit a shodnout se na optimalizovaném řešení problematiky. Vlastní pracovní činnost týmu je vhodné organizovat postupem řízeného brainstormingu. Členové řešitelské skupiny se na zasedání týmu připravují, využívají výsledků jednodušších analytických metod (např. Ishikawova diagramu) a výsledků statistických metod (např. SPC, Paretovy analýzy apod.), výsledků z řízení o neshodných výrobcích (vnějších i vnitřních) atd. Vedoucí týmu dbá, aby žádný závažný problém nebyl zapomenut.

⇒ Členové řešitelské skupiny realizují analýzu postupným hledáním a nacházením řešení tak, aby mohl být řádně a úplně vyplněn formulář FMEA v souladu s obsahem definic položek. Doporučuje se stanovit jednotlivé možnosti vzniku míst poruch, jejich druhů, následků a příčin (tedy v těchto položkách, které mají stromovou strukturu, postupovat nejprve vertikálně); potom ke každému druhu a příčině poruchy vyplnit další položky (tzn. dále postupovat horizontálně).

⇒ U položky „Kontrolní opatření (současný stav)“ a „Odpovídá“ je nezbytné údaj doplnit příslušným datem. U položky „Kontrolní opatření“ datum, ke kterému dni je toto opatření uskutečňováno, u položky „Odpovídá“ datem, do kdy je odpovědný pracovník povinen zabezpečit realizaci příslušného opatření.

⇒ V položkách „Význ“, Výsk“ a „Odhal“ je nutné vyjádřit předepsaným bodovým hodnocením význam, výskyt a odhalitelnost poruchového stavu. Komplexní hodnocení pak vyjadřuje součin těchto tří veličin bodového hodnocení, který se nazývá „Rizikové číslo“ (MR/P = Míra rizika na poruchu). Pokud hodnota MR/P překročí předem stanovenou hodnotu, je nezbytné stanovit nápravné (resp. preventivní) opatření. Hodnota MR/P je tedy klíčem k rozhodnutí, zda-li je nezbytné při daném hodnocení výskytu, významu a odhalitelnosti nápravné opatření stanovit či nikoliv.

⇒ Je nutné průběžně kontrolovat plnění úkolů, které vzešly z analýzy, a údaje neustále aktualizovat opakovanými optimalizačními analýzami. Pouze tak bude FMEA „živým dokumentem“.

Podle toho, zda již byla provedena aplikace FMEA na analyzovaný objekt (dílec/sestavu), lze rozlišit dva případy:

1. FMEA na nový dílec, tj.

a) na dílec, který je již vyráběn, ale na který dosud FMEA nebyla aplikována - analýza možností vzniku vad, jejich možných příčin a následků nebyla provedena, možné vady, jejich možné příčiny a následky nebyly detekovány a ohodnoceny body (jedná se zpravidla o případy nového zavádění metod při budování systému řízení jakosti v praxi),

b) na zcela nově vyvíjený objekt (dílec/sestavu). Aplikace FMEA by měla být součástí návrhové fáze procesu, nikoliv až po provedení hodnocení schvalovacího řízení jako „následný“ doplněk výrobního procesu;

2. FMEA optimalizační - provádí se na objekt (dílec/sestavu), na který již v minulosti byla FMEA aplikována. V této fázi se jedná v podstatě o provedení hodnocení navržených opatření a jejich realizace (tedy zhodnocení současného stavu, který vychází z dříve přijatých opatření zlepšující předchozí stav).

Případ 1b) a 2) jsou případy, kdy organizace metodu FMEA již provádí a existují s její aplikací již určité zkušenosti (není to však podmínkou). Tyto případy plně respektují hlavní myšlenku FMEA. Případ 1a) zásadní myšlenku FMEA zcela nerespektuje v tom smyslu, že je aplikována FMEA na objekt (dílec/sestavu), který jej již vyráběn. Organizace si je ale vědoma nutnosti začít s používáním FMEA a tak ji „dodatečně“ aplikuje na výrobní dílec. Je to jakýsi „přechodný, záběhový proces“ zavedení metody v organizaci, kde sestavený tým získává praktické zkušenosti s jejím používáním. Jde o častý případ zavádění FMEA ve výrobních organizacích. Je nutné, aby tým odborníků se naučil s FMEA běžně pracovat, chápal FMEA jako způsob práce, nikoliv jako ztrátu diskusí nad problémy. To tato fáze zavádění FMEA umožňuje a proto je přínosná při jejím zavádění.

Podrobnější zásady řízení postupu musí stanovit příslušná podniková směrnice pro aplikaci FMEA.

6. Využití výsledků metody FMEA

Metoda FMEA je metoda kvalitativní – je pro ni charakteristické vznik výsledků v podobě verbálních popisů druhů, příčin a následků poruchových stavů a případných doporučených opatření.

Kritérium klasifikace výskytu poruchy (vady)	**Odhad četnosti**	**Třída**
Není pravděpodobné, že porucha (vada) nastane	0	1
Velmi malá: Jedná se o proces s ojedinělým výskytem poruchy (vady)	1/5000 1/2000 1/1000 1/500	2 3 4 5
Střední: Odpovídá procesům, kde obvykle dochází k náhodným poruchám (vadám), ale v menší míře	1/200	6
Vysoká: Odpovídá výrobním procesům s častými poruchami (vadami)	1/100 1/50	7 8
Velmi vysoká: z hlediska uživatele je téměř jistý výskyt poruchy (vady)	1/20 1/10	9 10

Tab. 2 – Příklad klasifikační tabulky výskytu poruchových stavů (vad)

Kritérium klasifikace významu poruchy (vady)	**Třída**
Zanedbatelná: podstata poruchy (vady) je taková, že neovlivní schopnosti systému - výrobku, tj. uživatel pravděpodobně nezaznamená její výskyt	1
Nízká: porucha (vada) vyvolá uživateli pouze potíže, nepozorují se poškozené funkce objektu – výrobku	2 3
Střední: porucha (vada) vyvolá obtíže uživateli snížením pohodlí při užívání - porucha (vada) obtěžuje při ovládání, manipulaci. Uživatel zaznamená určité zhoršení vlastností výrobku	4 5 6
Vysoká: porucha (vada) vyvolá značné obtíže uživateli, resp. způsobí vážné poškození, špatné vlastnosti výrobku; neovlivňuje však bezpečnost výrobků	7 8
Velmi vysoká: porucha (vada) ovlivňuje bezpečnost výrobků, jeho nezpůsobilost k provozu z hlediska zákonných předpisů	9 10

Tab. 3 – Příklad klasifikační tabulky významu poruchových stavů (vad)

Kritérium klasifikace odhalitelnosti poruchy (vady)	**„Průchod“ poruchy (vady) k uživateli [%]**	**Třída**
Velmi vysoká: pravděpodobnost, že porucha (vada) by byla detekována kontrolou nebo při montáži	0 až 5	1
Vysoká: pravděpodobnost, že porucha (vada) se dostane k uživateli bez detekce - podle pravděpodobnosti průchodu poruchy k uživateli	6 až 15 16 až 25	2 3
Střední: pravděpodobnost, že porucha (vada) se dostane k uživateli bez detekce - podle pravděpodobnosti průchodu poruchy (vady) k uživateli	26 až 35 36 až 45 46 až 55	4 5 6
Nízká: pravděpodobnost, že porucha (vada) se dostane k uživateli bez detekce - podle pravděpodobnosti průchodu poruchy (vady) k uživateli	56 až 65 65 až 75	7 8
Velmi vysoká: pravděpodobnost, že porucha (vada) se dostane k uživateli bez detekce - podle pravděpodobnosti průchodu poruchy (vady) k uživateli	76 až 85 86až 100	9 10

Tab. 4 – Příklad klasifikační tabulky odhalitelnosti poruchových stavů (vad)

Existují tři významné a přitom základní okruhy výsledků FMEA, které slouží jako základní podklad k dalšímu zpracování. Jedná se o toto následné zpracování:

a) stanovení ztrát ze vzniku následků potencionálních poruchových stavů: je vhodné přizvat na jednání týmu zástupce ekonomického úseku, který se zabývá analýzou nákladů na jakost pro stanovení odhadu ztrát v případě výskytu analyzovaného poruchového stavu a ke stanovení finančních zdrojů na uskutečňování doporučovaného nápravného opatření ve vazbě na hodnocení nákladů na (ne)jakost,
b) stanovení opatření k nápravě a preventivních opatření jako základního prvku zlepšování systému jakosti v organizaci: výsledky FMEA jsou vhodnými podklady a jedním ze zdrojů ke stanovení opatření k nápravě/prevenci v souladu se zavedeným systémem jakosti. Na základě posouzení závažnosti druhu poruchového stavu, resp. jeho následku ve vazbě na velikost rizika/priority (MR/P) se příčina poruchového stavu buď odstraní operativní nápravou nebo při vyšší hodnotě MR/P se na základě doporučeného opatření z analýzy stanoví např. formou vystavení karty opatření k odstranění příčiny poruchového stavu,
c) zásadní podklad pro souhrnné hodnocení účinnosti systému jakosti: výsledky analýzy metodou FMEA lze s výhodou použít jako dílčí podklad do celkového souboru informací, které slouží k vyhodnocení účinnosti systému jakosti v organizaci.

Metoda FMEA, resp. formuláře FMEA, pomocí nichž se metoda prakticky aplikuje, jsou tzv. „živým“ dokumentem, který odráží vývoj analyzovaného objektu a procesu (v obecném smyslu slova). Tento vývoj a jeho posuzování v čase umožňuje horizontální dimenze záznamu ve formuláři FMEA. Záznamy ve vertikální dimenzi umožňují analýzu obohacovat o stále nově zjištěné příčiny, druhy a následky poruchových stavů.

Vzájemným posuzováním a srovnáváním zjištěných údajů za stanovené časové období lze dospět ke zhodnocení dílčího stavu, které je vhodné promítnout jako dílčí část do celkového hodnocení účinnosti systému jakosti. Vhodné je vyhodnocovat účinnost realizovaného doporučeného opatření poměrem MR/P ve dvou různých časových horizontech pro každou jednu příčinu poruchového stavu.

Závěr

V příspěvku jsou uvedeny základní principy metody FMEA/ FMECA, postup její aplikace a základní možnosti využívání jejich výsledků. Výsledků však lze využívat i v řadě dalších činnostech ve vazbách na další metody řízení a zlepšování jakosti a zejména řízení a zlepšování bezporuchovosti a/nebo bezpečnosti. Při komplexních analýzách spolehlivosti platí všeobecná zkušenost, že zpravidla nepostačí využívat jednu metodu analýzy spolehlivosti, protože žádná jednotlivá metoda analýzy není natolik vyčerpávající, aby zvládla všechny možné složité modely pro hodnocení konkrétního systému. Bývá proto nutné použít několika metod, což teprve umožní zvládat potřebné a požadované vyhodnocení vlastností různých druhů praktických systémů. Metoda FMEA i při požadované kvantitativní analýze spolehlivosti, kdy se pracuje s ukazateli spolehlivosti, má často své uplatnění jako jedna z použitých metod kvalitativních analýz s využitím výše uvedených možností jejich výsledků.

Literatura:

[1] VOTAVA, P.: ***Analýza druhu poruchových stavů a jejich důsledků (FMEA) dvourychlostního stěrače PAL, a.s.*** Diplomová práce (vedoucí DP A. Mykiska). Fakulta strojní ČVUT –KAŘ, Praha 1994 (60 str., 20 příloh)

[2] MYKISKA, A.: ***Spolehlivost technických systémů.*** Vydavatelství ČVUT, Praha 2000 (177 str.)

[3] VOTAVA, P.: ***Metody FMEA a FMECA při analýze bezporuchovosti***. In: Sborník mezinárodní konference JAKOST 2000. Dům techniky Ostrava 2000

[4] MYKISKA, A. – VOTAVA, P.: ***Metody analýz spolehlivosti a jejich výběr.*** In: Materiály k setkání odborné skupiny pro spolehlivost Zabezpečování spolehlivosti. Česká společnost pro jakost, Praha, září 2001 (str. 3 - 9)

APLIKACE METODY FMEA PROCESNÍ V SGS HOŘOVICE

Milan Polák, SGS Hořovice

I. ÚVOD

I. 1 Krátké seznámení s podnikem SGS ČR - Hořovice

Organizace Saint – Gobain SEKURIT (SGS) je v současné době největším výrobcem automobilových skel a v roce 1995 vstoupila na český trh prostřednictvím své dceřinné společnosti – Saint – Gobain SEKURIT ČR s.r.o.

Přehled vývoje podniku:

1995 – stavba budovy a infrustruktury (ukončeno 15.12.1995);

1996 – zahájení výroby čelních skel (5.2.1996). Celkem 60 zaměstnanců, vyrobeno 70 000 ks skel;

1997 – v polovině roku zahájen tří směnný provoz. Celkem 130 zaměstnanců, vyrobeno 240 000 ks skel;

1998 – od začátku roku nepřetržitý provoz. Velké investice, výroba také skel pro autobusy. Celkem 190 zaměstnanců, vyrobeno 320 000 ks skel a 550 ks skel pro autobusy.

1999 – náběh nových technologií, rozšíření výroby. Celkem 280 zaměstnanců, vyrobeno 442 447 ks skel a 1 046 ks skel pro busy.

2000 – rozšíření výroby vč. náběh nových technologií pro výrobu vyhřívaných čelních skel. Celkem 285 zaměstnanců, vyrobeno 510 000 Ks skel a 5 135 ks skel pro busy

2001 – schválena nová investic , nové technologie,

I. 2 Stav používání metody FMEA v podniku

Od roku 1996 byl vývoj soustředěn jen centrálně v SGS International (SGSI) v Německu. Od roku 1997 se započalo s připravováním modelů (jen pro náhradní díly) již v Hořovicích. Během roku 1998 – 1999 se již pracovníci přípravy výroby (kam spadá vývoj) zúčastňovali pravidelných FMEA pořádaných firmou Škoda Auto, a.s. při vývoji nového modelu Škoda Fabia. V roce 2000 začal vývoj nového modelu pro automobilku Jaguár (model X400). I zde se intenzivně pracovalo s metodou FMEA a to jak s FMEA návrhu (pod vedením konstruktéra z firmy Jaguár), tak s FMEA procesu (vedené přímo v podniku SGS Hořovice).

Do tohoto roku se metoda FMEA používala jen v omezené formě. Nebylo využíváno všech možností, které metoda FMEA poskytuje. Chybělo také dostatečné provázání s výrobou a nedostatečně se reagovalo na různé problémy a přání ze strany zákazníků.

II. ANALYTICKÁ ČÁST

II.1 FMEA a její historický vývoj

Pojem FMEA – v německém originále „Fehler-Möglichkeits-und Einfluss-Analyse“ - znamená v češtině – Analýza možností vzniku vad a jejich následků. Byla jako metoda vyvinuta NASA v USA v šedesátých letech pro projekt Apollo. Po zavedení metody v letectví a kosmických letech jakož i v jaderné technice nalezla brzo využití v automobilním průmyslu. Nato se metoda FMEA rozšířila celosvětově. Dnes je základním metodickým nástrojem managementu systémů jakosti u mnoha výrobců automobilů a jejich dodavatelů.

Cíle metody FMEA se odvozují od faktorů působících na odvětví, např. na automobilní průmysl, které se v minulosti silně měnily. Se stoupajícími nároky zákazníků na jakost působí nutná optimalizace nákladů na výrobky a zákonem požadovaná odpovědnost výrobce za výrobek.

II. 2 Cíle metody FMEA

Dosažení dále uvedených podnikových cílů podporuje mimo jiných nástrojů právě metoda FMEA:

- **zvyšování bezpečnosti funkcí a spolehlivosti výrobků,**
- snižování záručních a servisních nákladů,
- zkrácení procesu vývoje,
- náběhy sérií s menšími vadami,
- lepší termínová kázeň,
- hospodárná výroba,
- lepší služby,
- lepší vnitropodniková komunikace.

Aby se předcházelo vadám, musí být používání metody FMEA zahájeno ve velmi raném stádiu procesu výrobku (např. při stanovení požadavků), k přezkoušení k okamžitému stavu vývoje a plánování, aby mohla být zavedena preventivní opatření k předcházení možným vadám.

Obecně lze metodu FMEA charakterizovat jako týmovou metodu k minimalizaci rizik vývojových a plánovacích procesů, vyžadující interdisciplinární spolupráci zúčastněných útvarů již od samého počátku prací. Navíc poskytuje dokumentované podnikové expertní vědění.

V minulosti docházelo při používání metody FMEA obzvláště k následujícím nedostatkům:

- při konstrukční FMEA se vady zkoumaly pouze na úrovni dílu,
- nezkoumaly se vzájemné funkční souvislosti jednotlivých dílů,
- při procesní FMEA se možné vady zkoumaly jen v jednotlivých operacích procesu,
- neprováděla se systematicky členěná potřebná analýza.

II. 3 Základní rozdělení FMEA

FMEA se rozděluje na dvě základní skupiny: FMEA návrhu (konstrukce) a FMEA výrobku (procesu).

II. 3. 1 FMEA návrhu (konstrukce)

Jedná se o analytickou podobu metody FMEA používanou především k tomu, aby se odpovědný návrhář (konstruktér) co nejvíce ujistil, že byly vzaty v úvahu a řešeny všechny možné druhy vad a s nimi spojené příčiny . Musí být vyhodnoceny všechny prvky spolu se všemi souvisejícími systémy, podsystémy a díly.

V prvotní formě je metoda FMEA návrhu (konstrukce) souhrnem poznatků návrháře a týmu o tom jak je součást, podsystém či systém navržen (včetně analýzy prvků, které by mohly podle zkušeností a minulých případů selhat). Tento systematický přístup uspořádává, formalizuje a dokumentuje duševní postupy , kterými návrhář normálně prochází při procesu navrhování.

Aplikace metody FMEA návrhu (konstrukce) podporuje proces navrhování s omezováním rizika vzniku vad pomocí:

- objektivního vyhodnocení požadavků návrhu a alternativ návrhu,
- stanovení prvotních podmínek pro výrobu a montáž,
- zvýšení pravděpodobnosti, že možné vady a jejich důsledky na systém a funkci výrobku budou uvažovány již ve fázi návrhu (vývoje),
- poskytnutí doplňkových informací pro pomoc při plánování důsledných a účinných zkoušek a programu vývoje,
- zpracování seznamu možností vad uspořádaného podle jejich účinku na zákazníka, což vytváří systém priorit pro zlepšení návrhu a vývojové zkoušky,
- poskytnutí souboru otevřených otázek pro doporučení a realizaci aktivit ke snížení rizik,

- poskytnutí podkladů pomáhajících analyzovat budoucí události v provozu, vyhodnocovat změny návrhu a připravovat náročnější návrhy.

Pro metodu FMEA návrhu (konstrukce) není „zákazníkem“ jenom konečný uživatel, ale také výroba, montáž, servis.

Při plném uplatnění se metoda FMEA návrhu (konstrukce) musí provádět pro všechny nové díly, změněné díly a díly dříve použité, ale nasazené v nových aplikacích či prostředí. Během počáteční aplikace procesu FMEA návrhu (konstrukce) se očekává přímé zapojení všech představitelů dotčených oblastí (montáž, výroba, jakost, materiály, služby, dodavatelé). Metoda FMEA má být katalyzátorem výměny myšlenek mezi příslušnými útvary a tím podněcovatelem týmového přístupu.

Metoda FMEA návrhu (konstrukce) je živým dokumentem a má být zahájena před nebo při finalizaci konceptu návrhu, soustavně aktualizována podle náběhu změn nebo objevení se nových informací v průběhu fází vývoje výrobku a konečně kompletována před uvolněním výrobních výkresů pro přípravu výroby. Metoda FMEA návrhu (konstrukce) bere v úvahu technická omezení v procesu výroby:

- potřebné obrysové náčrty,
- mezní jakost povrchu,
- montážní značky,
- způsobilost / výkon procesů,

Možné druhy vad a mechanismy, které mohou vzniknout v průběhu výroby nebo procesu montáže, jejichž identifikace, důsledek a kontrola je pak zahrnuta do FMEA procesu.

II. 3. 2 Průběh provádění metody FMEA návrhu (konstrukce):

Proces začíná sestavením seznamu toho co se od návrhu očekává a co nikoliv. Musí být zahrnuta očekávání a potřeby zákazníka, dokumenty s požadavky na vozidlo, známé požadavky na výrobek, požadavky výroby a požadavky montáže. Čím lépe jsou požadované charakteristiky definovány, tím lehčeji se pro nápravná opatření identifikují možné způsoby vad.

Nejlépe je začít blokovým diagramem systému (tok informací, energie , materiálu atd.). Cílem je porozumět vstupům do bloku , přeměně procesu a výstupům z bloku. Diagram ilustruje primární vztahy a stanovuje logické pořadí analýzy.

Metoda FMEA návrhu (konstrukce) je živým dokumentem a měla by odpovídat poslednímu stavu návrhu jakož i nejnovějším odpovídajícím opatřením, včetně těch , která se objevila po zahájení výroby.

II. 3. 3 FMEA výrobku (procesu)

FMEA procesu je analytickou metodou používanou především k tomu, aby se odpovědný tým co nejvíce ujistil, že byly vzaty v úvahu a řešeny všechny možné druhy vad a s nimi spojené příčiny. V prvotní formě je FMEA výrobku (procesu) souhrnem poznatků technologů a týmu o průběhu vývoje procesu (včetně analýzy prvků, které by mohly selhat, prováděné na základě zkušeností a minulých problémů. Tento systematický přístup uspořádává a formalizuje duševní postupy, kterými technologové obvykle procházejí při procesu plánování výroby.

Použití metody FMEA procesu:

- identifikuje způsoby vad procesu, které by mohly ovlivnit hotový výrobek,

- oceňuje působení vady na zákazníka,

- identifikuje možné příčiny v procesu výroby nebo montáže a identifikuje proměnné procesu, na něž je nutno pro omezení nebo zjištění podmínek vzniku vad zaměřit úkony řízení,
- sestavuje a uspořádává seznam možných způsobů vad a tím sestavuje systém priorit pro zdůvodnění nápravných opatření
- dokumentuje výsledky výrobního nebo montážního procesu.

Při plném zavedení se metoda FMEA procesu musí provádět pro všechny nové díly (procesy), změněné díly (procesy) a díly (procesy) dříve použité, nasazené v nových aplikacích či prostředí.

Na počátku aplikace metody FMEA procesu se od odpovědného pracovníka za její používání očekává, že přímo a aktivně zapojí představitele všech dotčených oblastí. Mezi těmito oblastmi by měly být: návrh, vývoj, montáž, výroba, materiály, jakost, služby a dodavatelé. Používání metody FMEA musí podporovat týmový přístup.

Metoda FMEA procesu je živým dokumentem a její použití má být zahájeno před etapou nebo při etapě studie realizovatelnosti, před zajišťováním nástrojů pro výrobu a mělo by se zde uvažovat o všech výrobních a kontrolních operacích. Včasné prověrky a analýzy nových nebo revidovaných procesů slouží k předvídání, řešení nebo monitorování možných problémů procesu již v etapách připravování výroby nového modelu nebo dílu. Aplikace metody FMEA procesu předpokládá, že výrobek byl navržen podle zámyslu návrhu. Možné vady, které mohou vzniknout pro nedostatky návrhu, nemusí ale mohou být zahrnuty do provádění metody FMEA procesu. Jejich důsledky a vyvarování se jim je však třeba zahrnout do FMEA návrhu.

Pro předcházení možným nedostatkům procesu se provádění metody FMEA procesu nespoléhá jen na změny návrhu výrobku, ale bere v úvahu znaky navrhovaného výrobku ve vztahu k procesu výroby, tak aby výsledný produkt splňoval potřeby a očekávání zákazníka.

Aplikace metody FMEA procesu má začít sestavením analýzy rizik celého procesu. Zde mají být identifikovány všechny charakteristiky procesu příslušné každé operaci. Mají být připojeny všechny důsledky vad výrobku z odpovídající FMEA návrhu, pokud je k dispozici. Pro usnadnění dokumentování analýzy možných vad a jejich následků se používá vyvinutý formulář FMEA.

Při vlastní aplikaci metody FMEA výrobku (procesu) je důležité vypsat pro jednotlivé operace každý možný projev vad, který může, ale nutně nemusí vzniknout. Vždy je nutné položit si otázky:

- jakým způsobem může díl (proces) porušit specifikaci,
- co může zákazník (konečný uživatel) bez ohledu na technické požadavky považovat za nežádoucí.

Doporučuje se vycházet z porovnání obdobných procesů a názorů zákazníka ve vztahu k obdobným dílům.

Pracovník odpovědný za proces odpovídá za zajištění toho, že jsou uplatňována nebo příslušně směřována všechna doporučená opatření. Metoda FMEA výrobku (procesu) je živým dokumentem a měla by vždy odpovídat poslednímu stavu návrhu jakož i nejnovějším odpovídajícím opatřením, včetně těch, která se objevila po zahájení výroby.

III. NAVRHOVÁ ČÁST

III. 1 Výběr optimálního software pro aplikaci metody FMEA

Jelikož se při aplikaci metody FMEA jedná o problematiku rozsáhlou analytickou činnost, prostupující od vstupu materiálu až po výstup do skladu, je nanejvýš účelné k zmapování všech možných příčin vady vhodný software. Požadavky na tento software jsou především:

- přehlednost,
- jednoduchost,
- přizpůsobivost,
- finanční nenáročnost,
- možnost dalšího rozšiřování.

Jsou tři možnosti, jak takový software získat:

1) Nákup již hotového softwaru od některé z tuzemských firem.
2) Přesun FMEA softwaru od některé firmy z koncernu v Evropě.
3) Vytvoření vlastního softwaru.

Po analýze a zhodnocení všech možných kladů a záporů konkrétních možností uvedených třech případů jsem se rozhodl o vytvoření vlastního softwaru. K tomuto rozhodnutí mě vedla hlavně myšlenka využít jen některé zajímavé myšlenky jak z nabídek tuzemských firem, tak z existujícího softwaru firem z koncernu. Tyto myšlenky jsem dále rozvinul o specifické problémy v naší výrobě.

III. 2 Popis vytvořeného software

Při tvorbě softwaru jsem využil „kostru“ formuláře předepisující VDA. Software jsem přizpůsobil tak, aby bylo možné jednoduchým filtrováním v zanesených datech pracovat vždy s daty již pro konkrétní model (typ právě vyráběného automobilového skla). V praxi to znamená, že existuje „nekonečný“ seznam možných příčin vad zpracovaný na každou operaci a pro každou linku ve výrobě. Ke každému typu vyráběného automobilového skla se vada váže či nikoliv (dle složitosti typu skla). Jelikož jsou data zapisována v MS Excel, lze pak jednoduchým filtrováním otevřít vždy možné vady pro konkrétní vyráběný model.

Odpovědný pracovník za používání metody FMEA procesu odpovídá také za zajištění toho, že jsou uplatňována nebo příslušně směřována všechna doporučená opatření. Metoda FMEA je živým dokumentem a měla by vždy odpovídat poslednímu stavu návrhu jakož i nejnovějším odpovídajícím opatřením, včetně těch, která se objevila po zahájení výroby.

III. 3 Vytvoření teamů FMEA

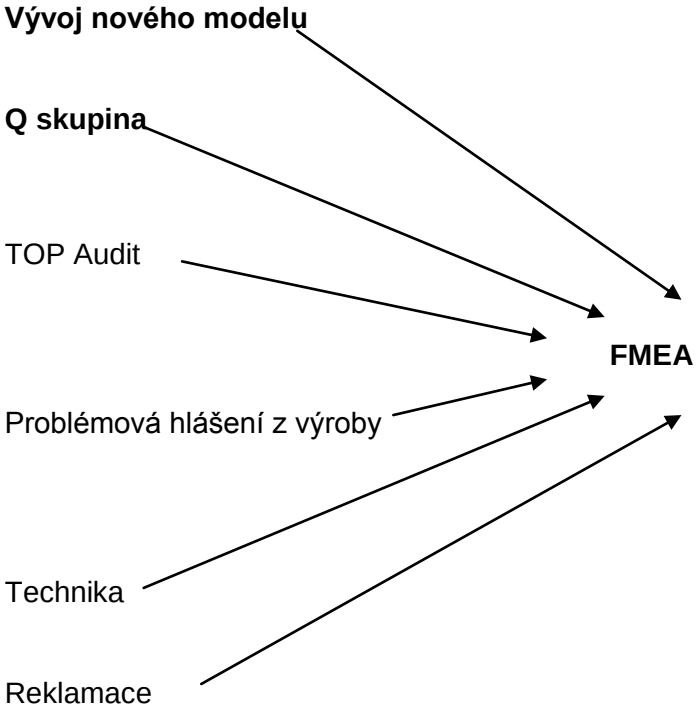
Pro úspěšné používání metody FMEA v našem podniku bylo velmi důležité vytvoření pracovních teamů. Zde bylo rozhodnuto vytvořit team pro každou výrobní linku zvlášť. Důležité bylo zvolit optimální složení všech pracovních teamů. V každém teamu byl zástupce:

- předák konkrétní linky,
- pracovník přípravy výroby zodpovědný za tuto linku,
- údržbář zodpovědný za tento úsek,
- produktauditor – pracovník oddělení kvality.

Za koordinaci všech teamů FMEA a pro práci se software byl určen pracovník přípravy výroby.

Dalším krokem bylo určení pravidelných schůzek všech teamů FMEA. Zde byl stanoven termín min. 1x měsíčně pro každý team (ze začátku a při aktuálních problémech se team scházel častěji).

III. 4 Popis sběru informací a systém práce s FMEA v našem podniku



Na obr. je schématicky uvedeno šest základních zdrojů, z kterých získává pracovník zodpovědný za FMEA podněty, připomínky a poznatky, které dál zapracovává do používaného softwaru.

1) Vývoj nového modelu: před začátkem každého vývoje nového modelu nebo před počátkem přesunu výroby modelu z některého ze závodů koncernu Saint – Gobain Sekurit se schází postupně všechny teamy FMEA, kde se detailně diskutuje nad možnými problémy, které mohou nastat
2) Q skupina : jedná se o pravidelnou pracovní poradu (1x za 14 dní) nazvanou – Q skupina. Zde se probírají např. opatření z interních nebo externích auditů v našem podniku.
3) TOP audit: je schůzka (1x týdně), kde se nad hotovým výrobkem náhodně odebraným ze skladu rozebírají případné nalezené neshody.
4) Problémové hlášení z výroby: jedná se o písemně podané problémové hlášení z výroby, kde se řeší nedostatky zjištěné během sériové výroby.
5) Technika: toto je schůzka (1x za 14 dní), kde se schází vedoucí pracovníci oddělení Techniky (Příprava výroby, Logistika, Údržba, Výroba atd.). Zde se řeší problémy tohoto oddělení.
6) Reklamace: zde jsou dva zdroje informací a poznatků pro FMEA:
    a) oficiální reklamace od zákazníků,
    b) neoficiální reklamace od zákazníků (doporuční, přání atd.).

IV. VYHODNOCENÍ

IV.1 Ekonomický přínos pro podnik

V průmyslu hraje vztah mezi náklady a užitkem důležitou roli. O použití takových nástrojů jako je metoda FMEA je možné rozhodnout teprve po vytvoření představy o nákladech a očekávaném prospěchu. Je nutno vzít v úvahu, že se investovaný kapitál bude vracet až v průběhu určité doby, a že bez této investice hrozí riziko velkých finančních ztrát.

Je jisté, že se metoda FMEA musí použít pro každý výrobek, na nějž se vztahují bezpečnostní předpisy. Proti nákladům na zavedení a systematické provádění metody FMEA stojí

prospěch, možnost včasného, preventivního a systematického rozpoznávání možných vad a možnost formulovat vhodná nápravná opatření. Užitek z nasazení se dále zvyšuje tím, že se účinek plánovaných a uskutečněných zlepšení dá měřit kvantitativně.

Po zavedení navrženého a vytvořeného softwaru bylo provedeno přehledné vyčíslení úspor v podniku. Zjistily se úspory při zavádění nového modelu na nákladech vývojové série a tím i nákladech při zavádění do sériové výroby až 50%. Tím je zřejmé, že používáním metody FMEA dojde k odhalení několika problémů, které by nás finančně zatížily při prvních sériích ve výrobě.

IV.2. Využití metody FMEA v dalších odděleních podniku

Metodu FMEA lze úspěšně používat i v dalších odděleních podniku. U nás v závodě se dál rozšířila do oblasti výroby ohýbacích forem a výroby přípravků.

Dále je možné používat metodu FMEA v oddělení nákupu, kde lze odhalit problém ještě před dodáním materiálu do výroby a tím ušetřit jak peníze, tak kapacitu výroby.

Další možnosti je využít metodu FMEA v oddělení Investic, kde již při plánování velkých investic tato metoda může velmi pomoci. Takto by bylo možné projít oddělení za oddělením, kde by metoda FMEA přinesla velké úspory jak finanční, tak časové.

V. Závěr

Budoucnost metody FMEA celkově pro další vývoj společnosti je dosti vysoká. Hlavně v automobilovém průmyslu, kde jde vývoj obrovskými kroky je budoucnost této metody veliká. V naší zemi se tato metoda bohužel používá dost zřídka, ale postupně jí zde zavádějí západní podniky, kde je více rozšířená.

Literatura:

[1] Polák, M.: Zavedení metody FMEA v podniku Saint-Globain Sekurit Hořovice. Závěrečná semestrální práce za 2. semestr vyššího managerského studia. ČVUT v Praze Masarykův ústav vyšších studií – ISQ PRAHA, Praha 2001

[2] Franke, D. W.: FMEA – Analýza možnosti vzniku vad a jejich následků. Česká společnost pro jakost. Praha 1993

[3] VDA 4.2 Management jakosti v automobilovém průmyslu. Zabezpečování jakosti před sériovou výrobou. Systémová FMEA. VDA – ČSJ, Praha 1997

PROVEDENÍ FMECA PRO ZAŘÍZENÍ PROVOZOVANÉ NA CVIČNÉM LETADLE L159

Ing. Karel Čech, Institut pro testování a certifikaci, a. s., divize 4 - MESIT QM,

Uherské Hradiště

Společnost Institut pro testování a certifikaci, a. s., se sídlem ve Zlíně má bohaté zkušenosti s prováděním činností autorizovaných, akreditovaných zkušebních i kalibračních v mnoha oborech (viz materiály písemné, resp. informace na webových stránkách www.itczlin.cz).

Součást společnosti - divize 4 - MESIT QM, Uherské Hradiště také již dlouhou dobu provádí analýzy bezporuchovosti elektronických zařízení. Jedná se o zařízení z různých oblastí: letectví, železnice, automobilový průmysl aj.

Pro ilustraci Vás seznámím s analýzou bezporuchovosti soupravy pro měření podélného vyvážení na letounu L159 - vysílač LUN 1756 a ukazovatele LUN 1755 metodou FMECA.

1 ZÁKLADNÍ ÚDAJE

Cílem analýzy **soupravy pro měření podélného vyvážení - vysílač LUN 1756 a ukazovatel LUN 1755** bylo určení kritických konstrukčních uzlů, které zásadním způsobem ovlivňují bezporuchovost celé soupravy. V rámci analýzy je také provedeno ověření správné volby součástek, jejich zatížení a určení nejméně spolehlivých prvků.

Součástí analýzy je také výpočet intenzity poruch, resp. střední doby bezporuchového provozu soupravy pro měření podélného vyvážení metodou sériového poruchového modelu s využitím normy MIL 217 F (z 2. prosince 1991).

Pro potřeby analýzy byla shromážděna následující dokumentace o přístroji:

- technické podmínky TPF - MSP 01-7088-96X pro ukazovatel podélného vyvážení LUN 1755,
- technické podmínky TPF - MSP 01-7090-96X pro vysílač podélného vyvážení LUN 1756,
- schéma zapojení soupravy pro měření podélného vyvážení,
- seznam součástek,
- technické listy všech použitých polovodičových prvků.

V příspěvku jsou použity následující pojmy:

objekt analýzy - analyzovaný přístroj (souprava pro měření podélného vyvážení),
modul - funkční část soupravy pro měření podélného vyvážení podle blokového schéma,
prvek - nejnižší analyzovaná součást - v případě soupravy pro měření podélného vyvážení se jedná o jednotlivé součástky, ze kterých jsou uvedené moduly složeny,
funkční výstup - projev činnosti soupravy pro měření podélného vyvážení.

2 DEFINICE OBJEKTU ANALÝZY, POŽADAVKY

2.1 Objekt analýzy

Objektem analýzy je *souprava pro měření podélného vyvážení - jeden vysílač LUN 1756 (437 P6) a jeden ukazovatel LUN 1755 (218 P1)* pro letoun L 159. Souprava je určena k přesnému nastavování podélného vyvážení letounu L159 a k indikaci nastavené hodnoty podélného a příčného vyvážení.

Vysílač (potenciometrický vysílač polohy) pracuje jako převodník úhlové výchylky mechanismu podélného vyvážení letounu na elektrické napětí, úměrné této výchylce. Potenciometr vysílače je napájen stabilizovaným napětím z ukazovatele podélného vyvážení.

Pohyb od mechanismu podélného vyvážení letounu je přenášen na převodník - potenciometr - pomocí ramena, které je k ose potenciometru připevněno stahovacím kroužkem.

Elektrická vývodka je na tělesu vysílače tvořena zásuvko - vidlicovým spojem. Těleso je uzavřeno víčkem a utěsněno těsněním.

Ukazovatel podélného vyvážení letounu se skládá z těchto základních částí:
- kryt ukazovatele se sklem naneseným antireflexní vrstvou,
- základna s vidlicí,
- krokový motor nesoucí ručku ukazovatele,
- elektronické obvody pro řízení kroku motoru, mikroprocesoru, zesilovače vstupních signálů a zdrojové jednotky, umístěné na plošných spojích,
- číselník zhotovený z polymetylmetakrylátu, jehož stupnice je prosvětlená integrálním systémem osvětlení s použitím žárovek se zeleným filtrem,
- signalizace příčného vyvážení letounu je realizována žárovkou se zeleným filtrem, umístěnou v pravém horním kvadrantu číselníku,
- signalizace výpadku napájení je realizována oranžovým praporkem, který je ovládán magnetoelektrickým indikátorem napětí. Signalizace je umístěna v pravé polovině číselníku,
- číselník a kryt ukazovatele jsou naneseny černým matným emailem; stupnice číselníku je bílá,
- propojení ukazovatele s vysílačem podélného vyvážení je provedeno přístrojovou vidlicí MS 3470W12-10P a kabelovou zásuvkou MS 3476W12-10S s vývodkou M 85049/52-S-12W.

Princip činnosti ukazovatele: měřený signál (ss napětí) je z potenciometrického vysílače přes spojovací vedení přiveden do osmibitového A/D převodníku ADC 0833 a odtud již v číselné podobě zpracováván mikroprocesorem AT89C2051. Mikroprocesor je doplněn minimálním počtem vnějších prvků - řídícím krystalem a obvodem RESET. Výstupní signály procesoru (signály počtu impulsů a signál směru) jsou řídícími veličinami obvodu pro díl ovládání krokového motoru. S hřídelí krokového motoru je pevně spojena ručka ukazovatele. Součástí ukazovatele je zdroj napětí (DC/DC měnič), která jsou potřebná pro napájení mikroprocesorového systému a krokového motoru.

Činnost procesoru a celého přístroje je řízena souborem programů, uložených v paměti procesoru. Jednotlivé programy zajišťují v podstatě dvě funkce přístroje:
1 Cyklické zobrazování naměřené hodnoty ručkou ukazovatele, které je zajištěno sadou podprogramů pro obsluhu jednotlivých periferních obvodů (A/D převodníku, ovládače krokového motoru) a pro provádění matematických operací.
2 Autodiagnostiku ukazovatele, která je jeho integrální součástí. Autodiagnostiku je třeba popisovat současně s popisem funkce ukazovatele jako celku.

Po zapnutí ukazovatele (přivedení napájecího napětí) je provedena autokontrola procesoru a následně kontrola celého měřícího řetězce ukazovatele. Tuto kontrolu lze provést i bez připojeného vysílače. Bude-li ukazovatel s vysílačem bez poruchy, ručka vykoná diagnostický pohyb na bílý oblouk umístěný v pravém dolním kvadrantu číselníku a následně zaujme polohu definovanou polohou vysílače. Nebude-li připojen vysílač, zůstane ručka při diagnostickém pohybu na bílém oblouku trvale.

V průběhu normálního provozu procesor (kromě obsluhy měřícího řetězce) provádí jak průběžnou diagnostiku vysílače a spojovacího vedení, tak diagnostiku chodu programu. Diagnostika vysílače zahrnuje 9 poruchových stavů vysílače a vedení typu zkrat a přerušení. Poruchové stavy se zobrazí pohybem ručky na bílý oblouk. Diagnostika chodu hlavního programu je zajištěna kontrolními body a systémem WATCHDOG, který při zjištění chyby provede RESET procesoru. Po každém RESETu proběhne již uvedená autodiagnostika jako při zapnutí přístroje. Současně je kontrolován počet provedených RESETů.

Jednotlivé kroky činnosti soupravy:
a) Po zapnutí napájení soupravy měření podélného vyvážení letounu se oranžový praporek, signalizující výpadek napájení, zasune pod štítek s nápisem TRIM a ručka ukazovatele přeběhne na bíle vyznačený oblouk mimo stupnici (signalizující poruchu ukazovatele, vysílače nebo vedení) a vzápětí naběhne do polohy odpovídající aktuálnímu měření. Jestli-

že nebyly v soupravě od vypnutí prováděny žádné změny, bude poloha ručky po zapnutí odpovídat poloze ručky před vypnutím soupravy.

b) V pracovním režimu bude postavení ručky sledovat polohu vysílače, spojeného s mechanismem řízení podélného vyvážení letounu.

c) Po vypnutí napájení soupravy zůstane ručka ukazovatele v poloze posledního platného měření. Pokud ručka po vypnutí není v ose pólových nástavců krokového motoru, může vlivem vybití kapacitorů vykonat krátký pohyb ve směru nejbližších pólových nástavců.

d) Při poruše ukazovatele, vysílače nebo vedení (jak po zapnutí, tak v pracovním režimu) přeběhne ručka ukazovatele na vyznačený bílý oblouk mimo stupnici a zastaví se. Z této polohy lze po odstranění poruchy ručku ukazovatele přesunout vypnutím a opětovným zapnutím napájecího napětí.

Vnitřní osvětlení je napájeno jmenovitým napětím U = 28 V, I_{max} = 0,05 A.

Souprava je napájena jmenovitým napětím U = 28 V, I_{max} = 1,0 A.

2.2 Pracovní prostředí objektu

Jednotlivé součásti soupravy pro měření podélného vyvážení letounu musí vyhovovat z hlediska působení vnějších vlivů požadavkům následujících dokumentů a norem (viz uvedené TPF):

- dokument RTCA/DO - 160C, ze dne 4. 12. 1989,
- dočasně dokument RTCA/DO - 160B, kapitola 20, kategorie Z, ze dne 20. 6. 1984,
- norma ISO 2678, Category D, ze dne 15. 5. 1985.

Z hlediska klimatického namáhání vyhovuje souprava parametrům uvedeným v tab. 1, z hlediska mechanického namáhání parametrům uvedeným v tab. 2.

Tab. 1

klimatické namáhání	**vysílač**	**Ukazovatel**
nízká provozní teplota	-55 °C	-20 °C
nízká neprovozní teplota	-55 °C	-55 °C
vysoká provozní teplota	+70 °C	+55 °C
vysoká neprovozní teplota	+85 °C	+85 °C
krátkodobá vysoká provozní teplota	+70 °C	+70 °C
vlhkost	zhoršené vlhké prostředí (kategorie B) - min. 95 % relativní vlhkost při 65 °C	Zhoršené vlhké prostředí (kategorie B) - min. 95 % relativní vlhkost při 65 °C

Tab. 2

mechanické namáhání	**vysílač**	**Ukazovatel**
provozní rázy	60 $m.s^{-2}$	60 $m.s^{-2}$
havarijní rázy	150 $m.s^{-2}$	150 $m.s^{-2}$
trvalé zatížení (lineární)	120 $m.s^{-2}$	120 $m.s^{-2}$
vibrace	standardní náhodné kapitola 8, kategorie C (4,12 gms)	Standardní náhodné kapitola 8, kategorie B (0,7 gms)

2.3 Požadavky na bezporuchovost (viz tab. 3)

Tab. 3

parametr	**vysílač**	**Ukazovatel**
celkový technický život	8 000 letových hodin	8 000 letových hodin
střední doba mezi poruchami	20 000 letových hodin	8 000 letových hodin

2.4 Využití objektu v praxi a provozní zatížení

Souprava pro měření podélného vyvážení letounu je v činnosti po celou dobu letu a její informace mohou být také trvale využívány. Pilot může prostřednictvím ručky ukazovatele trvale zjišťovat podélné nebo prostřednictvím světelného symbolu příčné vyvážení letounu.

2.5 Podmínky a požadavky na údržbu objektu

Ukazovatel i vysílač soupravy podélného vyvážení letounu nevyžadují během letu obsluhu a jsou udržováni podle jejich stavu.

Ukazovatel vyžaduje po záletu letounu nebo při výměně vysílače seřízení.

V době mezi předepsanými středními opravami nevyžaduje souprava údržbu.

V průběhu celkového technického života soupravy jsou kontrolní prohlídky prováděny periodicky po (2 000 $\pm$ 100) letových hodinách nebo po osmi rocích používání.

2.6 Definice poruchy a minimálních provozních požadavků

Pro analyzovanou soupravu pro měření podélného vyvážení letounu je možné definovat následující funkce:
- převést úhlovou výchylku mechanismu podélného vyvážení letounu na elektrické napětí, úměrné této výchylce,
- analogově zobrazit úhlovou výchylku mechanismu podélného vyvážení letounu na ukazovateli,
- indikovat příčné vyvážení letounu,
- indikace poruchy soupravy na vyznačeném oblouku mimo stupnici,
- vysunutím oranžového praporku signalizuje výpadek napájení,
- provádět autodiagnostiku ukazovatele.

Poruchou se pro účel analýzy rozumí stav, kdy souprava pro měření podélného vyvážení letounu nevyhodnotí správnou výchylku mechanismu podélného, resp. příčného vyvážení letounu, neprovede autodiagnostiku ukazovatele, nezobrazí správnou výchylku mechanismu podélného vyvážení letounu a nebo neindikuje předepsané stavy soupravy.

3 ANALÝZA PORUCH VNITŘNÍ STRUKTURY SOUPRAVY PRO MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LETOUNU

3.1 Stanovení úrovně analýzy

Při analýze soupravy pro měření polohy podélného vyvážení letounu byla zvolena nejnižší možná úroveň a to úroveň jednotlivých součástek.

3.2 Rozdělení objektu na funkční celky a vytvoření blokových schémat

Pro potřebu analýzy bylo vytvořeno blokové schéma soupravy pro měření podélného vyvážení letounu. Blokové schéma bylo zpracováno na základě rozboru činnosti soupravy pro měření podélného vyvážení letounu podle schématu zapojení.

3.3 Vytvoření pracovního formuláře

Podoba pracovního formuláře je přizpůsobena účelu analýzy a má za cíl stanovit rizikové číslo RN pro jednotlivé předvídané poruchy. Pomocí rizikového čísla je možno zjistit obvody nebo prvky, které zásadním způsobem ovlivňují bezporuchovost celé soupravy pro měření podélného vyvážení letounu.

Pracovní formulář obsahuje následující informace:
- název modulu podle blokového schématu,
- popis funkce příslušného modulu,
- předvídané poruchy, které mohou způsobit nesprávnou funkci modulu,
- důsledek poruchy na činnost celé soupravy pro měření podélného vyvážení letounu,

- rizikové faktory F_1, F_2, F_3, F_4,
- výsledné rizikové číslo RN.

Jednotlivé faktory F_1, F_2, F_3, F_4 mají následující význam:

F_1 - faktor, vyjadřující míru pravděpodobnosti vzniku poruchy,
F_2 - faktor, vyjadřující míru závažnosti poruchy na celý systém,
F_3 - faktor, vyjadřující míru obtížnosti detekce poruchy ve výrobním procesu,
F_4 - faktor, vyjadřující míru rizika započetí letového úkolu bez zjištění funkčního stavu přístroje, resp. vyjadřující míru obtížnosti detekce poruchy v předletové přípravě,
RN - rizikové číslo, tvořené součinem všech čtyř rizikových faktorů.

Za nebezpečné jsou považovány všechny ty poruchy, jejichž rizikové číslo je větší než střední hodnota uvažovaných rizikových čísel, přičemž jsou pro kvalifikovaný odhad kritické hodnoty rizikového čísla brány v úvahu také zkušenosti z výroby a provozu stávající, resp. analogické letecké techniky.

3.4 Definice rizikových faktorů kritičnosti

Hodnoty faktoru kritičnosti F_1: Hodnotící kritérium: ***intenzita výskytu poruchy za život objektu (pravděpodobnost vzniku dané poruchy)***

Hodnota kritéria vyjádřená slovně	**F_1**
Zanedbatelná velikost intenzity výskytu poruch (vznik dané poruchy je velmi nepravděpodobný).	1
Nízká hodnota intenzity výskytu poruch (vznik dané poruchy je možný s malou pravděpodobností).	2 ÷ 3
Střední hodnota intenzity výskytu poruch (vznik dané poruchy je pravděpodobný).	4 ÷ 6
Vysoká hodnota intenzity výskytu poruch (vznik dané poruchy je velmi pravděpodobný).	7 ÷ 8
Velmi vysoká hodnota intenzity poruch (vznik dané poruchy je téměř jistý).	9 ÷ 10

*Pozn. Intenzita výskytu poruch byla zjišťována **výpočtem** (sériový poruchový model) nebo **na základě praktických zkušeností se spolehlivostí použitých prvků v provozu na analogických přístrojích** z výroby MESIT přístroje spol. s r. o., provozovaných v leteckém provozu.*

Hodnoty faktoru kritičnosti F_2: Hodnotící kritérium: ***závažnost projevu poruchy z hlediska důsledků pro uživatele***

Hodnota kritéria vyjádřená slovně	**F_2**
Porucha nemá pro zákazníka pozorovatelný důsledek, zákazník ji pravděpodobně ani vůbec nezjistí, zanedbatelná závažnost.	1
Porucha vyvolá jen lehké obtíže, nejsou pozorovány významnější změny v chování objektu.	2 ÷ 3
Porucha vyvolá znatelné obtíže, je pozorováno určité zhoršení vlastností objektu, nejsou dotčeny základní funkce.	4 ÷ 6
Porucha vyvolá značné obtíže, ale nedochází k ohrožení bezpečnosti provozu, objekt neplní základní funkce, vysoká závažnost poruchy.	7 ÷ 8
Porucha způsobuje neplnění požadavků přepisů, je možné ohrožení bezpečnosti provozu, velmi vysoká závažnost poruchy.	9 ÷ 10

Pozn. V případě poruchy, která způsobí úplný výpadek funkce soupravy pro měření podélného vyvážení letounu, byla zvolena hodnota faktoru F2 = 8. Při vyhodnocení bylo předpokládáno, že ztráta činnosti funkce soupravy pro měření podélného vyvážení letounu nemá přímý vliv na bezpečnost letu.

Hodnoty faktoru kritičnosti F_3: Hodnotící kritérium: ***pravděpodobnost toho, že v případě vzniku poruchy nebude tato odhalena při výrobě, zkouškách nebo na výstupní kontrole (pravděpodobnost, že se porucha dostane k zákazníkovi)***

Hodnota kritéria vyjádřená slovně	**F_3**
Pravděpodobnost, že vznik poruchy nebude odhalen při kontrolách, montáži nebo zkouškách je zanedbatelná, porucha se k zákazníkovi téměř jistě nedostane, porucha je zjevná bez dalšího zkoušení.	1
Pravděpodobnost, že vznik poruchy nebude odhalen při kontrolách, montáži nebo zkouškách je nízká a pravděpodobnost expedice vadného výrobku malá.	2 ÷ 3
Pravděpodobnost, že vznik poruchy nebude odhalen při kontrolách, montáži nebo zkouškách je střední a pravděpodobnost expedice vadného výrobku střední.	4 ÷ 6
Pravděpodobnost, že vznik poruchy nebude odhalen při kontrolách, montáži nebo zkouškách je velká a pravděpodobnost expedice vadného výrobku vysoká.	7 ÷ 8
Pravděpodobnost, že vznik poruchy nebude odhalen při kontrolách, montáži nebo zkouškách je velmi velká a pravděpodobnost expedice vadného výrobku velmi vysoká.	9 ÷ 10

Hodnoty faktoru kritičnosti F_4: Hodnotící kritérium: ***pravděpodobnost toho, že v případě vzniku poruchy nebude tato odhalena před započetím letového úkolu, resp. vyjadřuje míru obtížnosti detekce poruchy v předletové přípravě (pravděpodobnost, že uživatel vzlétne s poruchou)***

Hodnota kritéria vyjádřená slovně	**F_4**
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je zanedbatelná (0% ÷ 5%), uživatel s poruchou téměř jistě nevzlétne, porucha je zjevná bez dalšího zkoušení.	1
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je velmi nízká (6% ÷ 15%).	2
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je nízká (16% ÷ 25%).	3
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je střední (26% ÷ 35%).	4
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je střední (36% ÷ 45%).	5

Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je vyšší (46% ÷ 55%).	6
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je vysoká (56% ÷ 65%).	7
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je vysoká (66% ÷ 75%).	8
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je velmi vysoká (76% ÷ 85%).	9
Pravděpodobnost, že vznik poruchy nebude odhalen při předletové přípravě je velmi vysoká (86% ÷ 100%).	10

3.5 Určení funkcí jednotlivých funkčních celků

Popis funkce jednotlivých funkčních celků (modulů) soupravy pro měření podélného vyvážení letounu je uveden přímo v pracovním formuláři.

3.6 Výpočet střední doby bezporuchového provozu

Při výpočtu intenzity poruch λ, resp. střední doby bezporuchového provozu T_0 *vysílače soupravy pro měření podélného vyvážení letounu LUN 1756 a ukazovatele* soupravy *pro měření podélného vyvážení letounu LUN 1755* byla použita metoda náhradního sériového modelu. Mechanické části jednotlivých částí soupravy nejsou při tomto výpočtu uvažovány.

Pro stanovení rozsahu hodnoty intenzity poruch pro 1 poruchu je možné stanovit 90-ti %-ní konfidenční interval z hodnot vypočtených pro vysílač a ukazovatel. Po jeho určení lze konstatovat, že parametry bezporuchovosti jednotlivých dílů soupravy pro měření podélného vyvážení letounu se budou s 90-ti %-ní pravděpodobností nacházet pod horní hranicí spočítaného konfidenčního intervalu (v případě intenzity poruch) či nad spodní hranicí konfidenčního intervalu (v případě střední doby bezporuchového provozu). Uvažované hranice dosahují následující hodnoty:

pro vysílač soupravy pro měření podélného vyvážení letounu LUN 1756:

$$\lambda_H = 1{,}325 * 10^{-6}\ h^{-1}, \text{ resp.}$$
$$\underline{T_{0D} = 754\,447\ h,}$$

pro ukazovatel soupravy pro měření podélného vyvážení letounu LUN 1755:

$$\lambda_H = 8{,}762 * 10^{-5}\ h^{-1}, \text{ resp.}$$
$$\underline{T_{0D} = 11\,413\ h.}$$

Na základě těchto skutečností lze předpokládat, že uvedené díly soupravy pro měření podélného vyvážení letounu LUN 1755 a LUN 1756 trvale překračují požadované hodnoty λ a T_0.

4 VÝSLEDKY ANALÝZY PORUCH VNITŘNÍ STRUKTURY SOUPRAVY PRO MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LETOUNU

Celkem bylo vyšetřováno 74 možných typů poruch na celkem 62 pozicích. Jako významné byly vyhodnoceny ty poruchy, jejichž rizikové číslo RN je větší než 200. Jedná se o následující poruchy:

* porucha portu mikroprocesoru DD2 (AT89C2051-S) v modulu 4 RN = 480
* porucha převodníku DD5 (ADC08034CIW) v modulu 4 RN = 480
* porucha čítače DD3 (PC74HCT93T) v modulu 7 RN = 420

*	přerušení diody
D1 ÷ D4 (11DF6) v modulu 5	RN = 392
*	změna hodnoty
trimru R4 (SMD3314 - 10k) v modulu 4	RN = 360
*	změna hodnoty
trimru R9 (CONTELEC - 10k) v modulu 4	RN = 360
*	zkrat rezistoru
R1 (SMD 1206 - 8k2) v modulu 4	RN = 324
*	přerušení kapa-
citoru C1 (CF5 - 220 nF) v modulu 6	RN = 294
*	přerušení kapa-
citoru C2 (CF5 - 220 nF) v modulu 6	RN = 294
*	zkrat kapacitoru
C4 (SR201C - 47 nF) v modulu 6	RN = 294
*	zkrat diody VD1
(1N5400) v modulu 6	RN = 256
*	přerušení diody
D5, D6 (BZX84C5V1) v modulu 4	RN = 256

Analýzou bezporuchovosti bylo vybráno celkem 12 možných poruch, které je možno označit jako závažné. Jedná se o poruchy aktivních i pasivních součástek. Pravděpodobnost vzniku těchto poruch je možno snížit použitím prvků se zaručovanou bezporuchovostí (tzv. součástky kategorie M, určené výhradně pro použití ve speciální technice).

Význam všech vyhodnocených poruch není možné snížit pouhou záměnou součástek za spolehlivější, jelikož použité typy jsou vesměs vhodné pro použití ve speciální technice a žádná není významněji zatěžována. Použitím součástek pro „speciál“ a zároveň pečlivým sekundárním tříděním všech polovodičových prvků při zatížení můžeme dosáhnout podstatné redukce období časných poruch a tím následně zmenšení možnosti oprávněné reklamace v počátcích provozu analyzované soupravy.

Celkovým rozborem schématu zapojení nebyl zjištěn žádný obvod, ve kterém by mohly vznikat poruchy typu „**skrytá porucha**“ (tzn. porucha, která se neprojeví v době svého vzniku, ale až po určité době nebo při určitých měřených hodnotách). Existují však případy, kdy by mohlo za určitých okolností dojít k poruše dalšího prvku náhodně v závislosti na typu poruchového mechanismu (přerušení diody D1 ÷ D4 (11DF6) v modulu 5 a následně porucha řadiče motoru DD6 (NMB SDI-C403) v tomtéž modulu nebo v modulu 6 případ možnosti vzniku rušení).

Zatížení jednotlivých pasivních i aktivních součástek není v převážné většině případů větší než 50%, zatížení integrovaného obvodu je v povolených mezích. Nebylo zjištěno použití žádné klimaticky nevhodné součástky.

Dále je třeba zdůraznit, že ztráta funkce ukazovatele se nevztahuje a nemá vliv na indikaci příčného vyvážení.

Srovnáním stanovených parametrů bezporuchovosti pro vysílač a ukazovatel soupravy pro měření podélného vyvážení letounu (viz kap. 2.3 - požadovaná střední doba mezi poruchami je 20 000 letových hodin pro vysílač a 8 000 letových hodin pro ukazovatel) s vypočtenými parametry bezporuchovosti (viz kap. 3.6) je možné konstatovat následující:

Dolní mez 90-ti %-ního konfidenčního intervalu střední doby bezporuchového provozu pro jednotlivé části soupravy pro měření podélného vyvážení letounu podstatně převyšuje hodnotu střední doby mezi poruchami, požadovanou v technických podmínkách TPF - MSP 01-7088-96X či v TPF - MSP 01-7090-96X. Existuje tedy reálný předpoklad, že požadavky na dosažení stanovené hodnoty parametrů bezporuchovosti budou s velkou pravděpodobností splněny, lépe řečeno překročeny.

5 ANALÝZA PORUCH VÝSTUPNÍCH FUNKCÍ SOUPRAVY PRO MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LETOUNU

Analýza poruch výstupních funkcí soupravy pro měření podélného vyvážení letounu, která byla provedena na základě analýzy poruch vnitřní struktury soupravy pro měření podélného vyvážení letounu, akceptovala všechny rozborované prvky. To znamená, že byly uvažovány všechny součásti, ze kterých se souprava pro měření podélného vyvážení letounu skládá. Z provedeného rozboru vyplývá, že 12 poruch, výše označených jako **významné,** by se v reálném provozu projevily následujícím způsobem:

porucha portu mikroprocesoru DD2 v modulu 4	ztráta funkce - nesprávný údaj ukazovatele
porucha převodníku DD5 v modulu 4	ztráta funkce - nesprávný údaj ukazovatele
porucha čítače DD3 (PC74HCT93T) v modulu 7	bez vlivu na funkci ukazovatele (při překročení určitého počtu RESETů nastane definovaný stav - ručka na bílém oblouku)
přerušení diody D1 ÷ D4 (11DF6) v modulu 5	bez vlivu na funkci ukazovatele (možnost poruchy obvodu DD6)
změna hodnoty trimru R4 v modulu 4	ztráta funkce - nesprávný údaj ukazovatele
změna hodnoty trimru R9 v modulu 4	ztráta funkce - nesprávný údaj ukazovatele
zkrat rezistoru R1 (SMD 1206 - 8k2) v modulu 4	bez vlivu na funkci ukazovatele (nelze vypnout funkci diagnostiky)
přerušení kapacitoru C1 (CF5 - 220 nF) v modulu 6	bez vlivu na funkci ukazovatele (možnost rušení)
přerušení kapacitoru C2 (CF5 - 220 nF) v modulu 6	bez vlivu na funkci ukazovatele (možnost rušení)
zkrat kapacitoru C4 v modulu 6	bez vlivu na funkci ukazovatele (možnost rušení)
zkrat diody VD1 (1N5400) v modulu 6	bez vlivu na funkci ukazovatele
přerušení diody D5, D6 (BZX84C5V1) v modulu 4	bez vlivu na funkci ukazovatele

6 VÝSLEDKY ANALÝZY PORUCH VÝSTUPNÍCH FUNKCÍ SOUPRAVY PRO MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LETOUNU

Vzhledem k definici poruch výstupních funkcí (viz bod 2.6), vzhledem k počtu vyšetřovaných poruch a k jejich následnému rozboru je možné určit procentuální podíl intenzit určených poruch na celkové intenzitě poruch soupravy pro měření podélného vyvážení letounu (viz tab. 4). Vzhledem k tomu, že jednotlivé mechanické díly mají vůči elektronickým součástkám zanedbatelnou intenzitu poruch, je za celkovou intenzitu poruch soupravy považována hodnota vypočtená pro ukazovatel a vysílač soupravy.

Tab. 4

Definice poruchy výstupních funkcí	**Počet určitých vyšetřovaných poruch**	**Intenzita poruch určitého typu poruchy**	**Procentuální podíl na celkové intenzitě**
Ztráta funkce - ukazovatel bez funkce	60 x	$1{,}718 * 10^{-5}$	52,6 %
Ztráta funkce - nesprávný údaj ukazovatele	4 x	$5{,}477 * 10^{-6}$	16,6 %
Ztráta funkce - nefunguje indikace příčného vyvážení	4 x	$2{,}412 * 10^{-6}$	7,2 %
bez vlivu na funkci ukazovatele	38 x	$7{,}340 * 10^{-6}$	22,3 %
bez vlivu na indikaci příčného vyvážení	3 x	$5{,}169 * 10^{-8}$	1,3 %

Projevy výše analyzovaných 12-ti **významných** poruch byly následující:

- ztráta funkce - nesprávný údaj ukazovatele 4 x
- bez vlivu na funkci ukazovatele (při překročení určitého počtu RESETů nastane definovaný stav - ručka na bílém oblouku) 1 x

- bez vlivu na funkci ukazovatele (možnost poruchy obvodu DD6) 1 x
- bez vlivu na funkci ukazovatele (nelze vypnout funkci diagnostiky) 1 x
- bez vlivu na funkci ukazovatele (možnost rušení) 3 x
- bez vlivu na funkci ukazovatele 2 x

Z tab. 4 vyplývá, že procentuální podíl intenzity definovaných poruch na celkové intenzitě poruch soupravy pro měření podélného vyvážení letounu není úměrný počtu jednotlivých poruch, ale závisí na úrovni bezporuchovosti (tj. intenzitě poruch) součásti, která danou poruchu vyvolá.

Jak vyplývá z údajů, projevuje se u osvětlení (žárovky typu ALBA) intenzita poruch, která podstatně ovlivňuje celkovou intenzitu poruch soupravy pro měření podélného vyvážení letounu. Tento fakt je vysvětlen následovně. Během provozu v letech 1986 ÷ 1991 byly žárovky ALBA reklamovány v minimálním počtu (vzhledem k počtu provozovaných). Ve srovnání s touto zanedbatelnou hodnotou jsou výrobcem zajišťované, resp. vypočtené parametry bezporuchovosti (intenzita poruch) žárovek ALBA nepoměrně vyšší. Jak však vyplývá z údajů, **nezařazuje velikost rizikového čísla RN** (RN = 32) **pro žárovky ALBA** tyto prvky mezi **závažné**.

7 ZÁVĚRY A DOPORUČENÍ

7.1 Závěry

Cílem analýzy bezporuchovosti soupravy pro měření podélného vyvážení letounu - vysílač LUN 1756 a ukazovatel LUN 1755 - pro letoun L 159 bylo odhalit kritická místa v konstrukci vysílače a přijímače, určit nejméně spolehlivé prvky, které se mohou rozhodující měrou podílet na poruchovosti přístroje (viz kap. 3 - „Analýza poruch vnitřní struktury soupravy pro měření podélného vyvážení letounu“) a definovat poruchy výstupních funkcí soupravy pro měření podélného vyvážení letounu, včetně jejich rozboru (viz kap. 5 - „Analýza poruch výstupních funkcí soupravy pro měření podélného vyvážení letounu“). Výsledky analýzy jsou uvedeny v kap. 4 (včetně doporučených nápravných opatření), resp. v kap. 6.

Hodnoty střední doby bezporuchového provozu jsou uvedeny v kap. 3.6. Z výsledků vyplývá, že požadavek Technických podmínek na jednotlivé části soupravy pro měření podélného vyvážení letounu: technické podmínky TPF - MSP 01-7090-96X pro vysílač podélného vyvážení letounu LUN 156 a technické podmínky TPF - MSP 01-7088-96X pro ukazovatel podélného vyvážení letounu LUN 1755 (viz kap. 2.3 - „Požadavky na bezporuchovost“) bude s postačující rezervou splněn, lépe řečeno překračován. Je možno tedy konstatovat, že souprava pro měření podélného vyvážení letounu splňuje všechny požadavky na ni kladené, a to jak po stránce technické, tak po stránce spolehlivostních parametrů.

Z výsledků vyplývá, že požadavek Technických podmínek TPF - MSP 01-7090-96X pro vysílač a TPF - MSP 01-7088-96X pro ukazovatel bude s postačující rezervou splněn. Je možno konstatovat, že souprava pro měření podélného vyvážení letounu splňuje všechny požadavky na ni kladené, a to jak po stránce technické, tak po stránce parametrů bezporuchovosti.

7.2 Doporučení

Doporučení ke změně součástek nejsou. Pro zaručení dané bezporuchovosti a pro snížení období časných poruch se jeví jako potřebné **sekundární třídění polovodičových prvků při funkčním a klimatotechnologickém zatížení a použití prvků v *military* provedení.**

Dalšího podstatného zkrácení období časných poruch (a následně redukce počtu oprávněných reklamací v počátcích provozu analyzované soupravy) bude dosaženo realizací **zahořování jednotlivých přístrojů** (podle racionálně stanoveného režimu).

Jako nezbytné se však jeví **sledování bezporuchovosti** (důsledná realizace již ověřeného informačního systému ISJS), a to jak **při montáži a na výstupní kontrole (vnitřní**

ISJS), tak v provozu na letounu (vnější ISJS). Získané informace je nutno průběžně vyhodnocovat a porovnávat se zadanými požadavky na bezporuchovost soupravy pro měření podélného vyvážení letounu. Bez naznačené zpětné vazby informací o výrobě a provozu analyzovaného objektu nelze zajišťovat ani ověřovat dosažení požadovaných parametrů bezporuchovosti.

Při prováděné analýze bylo zjištěno dublované značení součástek v jednotlivých modulech soupravy. Pro jednoznačnou identifikaci jednotlivých prvků je nutné tento nedostatek odstranit.

LITERATURA

[1] Technické podmínky TPF - MSP 01-7088-96X pro ukazovatel podélného vyvážení letounu LUN 1755
[2] Technické podmínky TPF - MSP 01-7090-96X pro vysílač podélného vyvážení letounu LUN 1756
[3] Schéma zapojení ukazovatele LUN 1755
[4] Analýza spolehlivosti použitím metod FMEA a FMECA. Příručka fy BREN, s. r. o., březen 1993
[5] ČSN IEC 812:1992 Metody analýzy spolehlivosti systému. Postup analýzy způsobů a důsledků poruch (FMEA)
[6] Katalog elektronických součástek, konstrukčních dílů, bloků a přístrojů, díly 1 až 5. TESLA ELTOS, 1988
[7] Katalogové listy použitých polovodičových prvků
[8] Vojenská norma MIL-HDBK-217 F:1991
[9] Letecká norma RTCA/DO 160C:1989

PRACOVNÍ FORMULÁŘ FMECA PRO SOUPRAVU MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LUN 1755 A LUN 1756

Název modulu	Popis funkce modulu	Předvídané poruchy	Možné následky poruchy	F_1	F_2	F_3	F_4	RN
1. Osvětlení ukazovatele	Zajišťuje čitelnost údajů ukazovatele zeleným světlem.	- porucha žárovky ALBA Ž1 ÷ Ž2	- bez vlivu na funkci ukazovatele - zhoršení čitelnosti údajů stupnice	4	4	1	2	32
		- prasklé sklo	- bez vlivu na funkci ukazovatele	2	3	1	1	6
2. Indikace příčného vyvážení	Zobrazuje funkci příčného vyvážení, které není přímo součástí soupravy.	- porucha žárovky ALBA Ž3	- ztráta funkce - nesvítí indikace příčného vyvážení	4	5	1	2	40
		- zkrat diody VD2, VD3 (KY132/300)	- bez vlivu na funkci indikace příčného vyvážení	4	1	5	8	160
		- přerušení diody VD2 (KY132/300)	- nefunguje indikace příčného vyvážení	4	3	2	2	48
		- přerušení diody VD3 (KY132/300)	- nefunguje test indikace příčného vyvážení (žárovky)	4	2	3	4	96
		- přerušení diody VD2 a VD3 (KY132/300)	- nebude svítit žárovka indikace příčného vyvážení	2	3	2	2	24
3. Krokový motor	Ve spojení s ručkou indikuje podélné vyvážení letounu na stupnici ukazovatele.	- porucha krokového motoru	- ztráta funkce - nefunguje indikace podélného vyvážení letounu	3	7	1	2	42
		- uvolnění ručky ukazovatele	- ztráta funkce - ukazovatel bez funkce	1	7	2	2	28
		- poškození ručky ukazovatele	- bez vlivu na funkci ukazovatele - zhoršení čitelnosti údajů stupnice ukazovatele	2	4	1	2	16
4. Mikroprocesor s A/D převodníkem	Zpracovává a vyhodnocuje informaci o stavu podélného vyvážení od vysílače.	- přerušení napájení mikroprocesoru DD2 (AT89C2051-S)	- ztráta funkce - ukazovatel bez funkce	4	7	1	2	56
		- porucha portu mikroprocesoru DD2 (AT89C2051-S)	- ztráta funkce - nesprávný údaj ukazovatele (v případě vyhodnocení hodnoty jako pravděpodobné)	4	8	3	5	480
		- porucha portu mikroprocesoru DD2 (AT89C2051-S)	- ztráta funkce - definovaný stav (v případě vyhodnocení hodnoty jako nepravděpodobné - ručka na bílém oblouku)	4	7	2	2	112
		- porucha převodníku DD5 (ADC08034CIW)	- ztráta funkce - nesprávný údaj ukazovatele (v případě vyhodnocení hodnoty jako pravděpodobné)	4	8	3	5	480
		- porucha převodníku DD5 (ADC08034CIW)	- ztráta funkce - definovaný stav (v případě vyhodnocení hodnoty jako nepravděpodobné - ručka na bílém oblouku)	4	7	2	2	112
		- porucha krystalu X1 (11.059 MHz)	- ztráta funkce - ukazovatel bez funkce	4	7	1	2	56
		- porucha kapacitoru C10 (SMD 0805-33 pF)	- ztráta funkce - ukazovatel bez funkce	3	7	1	2	42
		- porucha kapacitoru C11 (SMD 0805-33 pF)	- ztráta funkce - ukazovatel bez funkce	3	7	1	2	42
		- přerušení rezistoru R1 (SMD 1206-8k2)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat rezistoru R1 (SMD 1206-8k2)	- bez vlivu na funkci ukazovatele (nelze vypnout funkci diagnostiky)	3	3	6	6	324

PRACOVNÍ FORMULÁŘ FMECA PRO SOUPRAVU MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LUN 1755 A LUN 1756

Název modulu	Popis funkce modulu	Předvídané poruchy	Možné následky poruchy	F1	F2	F3	F4	RN
4. Mikroprocesor s A/D převodníkem	Zpracovává a vyhodnocuje informaci o stavu podélného vyvážení od vysílače.	- přerušení kapacitoru C16 (SMDD - 68 μF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C16 (SMDD - 68 μF)	- ztráta funkce – ručička se nepohybuje	3	7	1	2	42
		- přerušení kapacitoru C17 (SMDD - 33 μF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C17 (SMDD - 33 μF)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- přerušení kapacitoru C18(SMD1206-47nF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C18 (SMD 1206 - 47 nF)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- porucha zdroje refer. napětí NR1 (TL431)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- přerušení rezistoru R2 (SMD 1206 - 249 R)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- zkrat rezistoru R2 (SMD 1206 - 249 R)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- přerušení trimru R4 (SMD 3314 - 10 k)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- zkrat trimru R4 (SMD 3314 - 10 k)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- změna hodnoty trimru R4 (SMD 3314-10k)	- ztráta funkce – nesprávný údaj ukazovatele (v případě vyhodnocení hodnoty jako pravděpodobné)	3	8	3	5	360
		- změna hodnoty trimru R4 (SMD 3314-10k)	- ztráta funkce – definovaný stav (v případě vyhodnocení hodnoty jako nepravděpodobné - ručka na bílém oblouku)	3	7	2	2	84
		- porucha rezistoru R5,6,7,8,10 (SMD1206)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	3	7	1	2	42
		- změna hodnoty trimru R9 (CONTELEC-10k)	- ztráta funkce – nesprávný údaj ukazovatele (v případě vyhodnocení hodnoty jako pravděpodobné)	3	8	3	5	360
		- změna hodnoty trimru R9 (CONTELEC-10k)	- ztráta funkce – definovaný stav (v případě vyhodnocení hodnoty jako nepravděpodobné - ručka na bílém oblouku)	3	7	2	2	84
		- přerušení diody D5, D6 (BZX84C5V1)	- bez vlivu na funkci ukazovatele	4	1	8	8	256
		- zkrat diody D5, D6 (BZX84C5V1)	- ztráta funkce – definovaný stav (ručka na bílém oblouku)	4	7	1	2	56
5. Obvod pro ovládání krokového motoru	Řídí krokový motor dle informací mikroprocesoru.	- porucha řadiče motoru DD6 (NMB SDI - C403)	- ztráta funkce – ručička se nepohybuje	4	7	1	2	56
		- porucha kapacitoru C7 (SMD0805 - 4n7)	- ztráta funkce – ručička se nepohybuje	3	7	1	2	42
		- přerušení kapacitoru C8,C9 (SMDD-47 μF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C8, C9 (SMDD - 47 μF)	- ztráta funkce – ukazovatel bez funkce	3	7	1	2	42
		- přerušení rezistoru R13,14(SMA0207-4R7)	- ztráta funkce – ručička se nepohybuje	3	7	1	2	42
		- zkrat rezistoru R 13, 14 (SMA 0207 - 4R7)	- ztráta funkce – poškození krokového motoru	3	7	2	3	126
		- přerušení diody D1 ÷ D4 (11DF6)	- bez vlivu na funkci ukazovatele (možnost poruchy DD6)	4	2	7	7	392
		- zkrat diody D1 ÷ D4 (11DF6)	- ztráta funkce – ručička se nepohybuje	4	7	1	2	56

PRACOVNÍ FORMULÁŘ FMECA PRO SOUPRAVU MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LUN 1755 A LUN 1756

Název modulu	Popis funkce modulu	Předvídané poruchy	Možné následky poruchy	F1	F2	F3	F4	RN
6. Zdroj napětí	Napájí ukazovatel podélného vyvážení včetně vysílače.	- porucha převod. DC/DC - NR1(TEP2411)	- ztráta funkce – chybí napětí (ukazovatel bez funkce)	4	7	1	2	56
		- porucha stabilizátoru NR2 (78L15)	- ztráta funkce – nízké napětí (ukazovatel bez funkce)	4	7	1	2	56
		- přerušení diody VD1 (1N5400)	- ztráta funkce – definovaný stav - ručka na bílém oblouku	4	7	1	2	56
		- zkrat diody VD1 (1N5400)	- ztráta funkce – ukazovatel bez funkce	4	7	1	2	56
		- přerušení kapacitoru C1 (CF5 - 220 nF)	- bez vlivu na funkci ukazovatele	4	1	8	8	256
		- zkrat kapacitoru C1 (CF5 - 220 nF)	- bez vlivu na funkci ukazovatele (možnost rušení)	3	2	7	7	294
		- přerušení kapacitoru C2 (CF5 - 220 nF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C2 (CF5 - 220 nF)	- bez vlivu na funkci ukazovatele (možnost rušení)	3	2	7	7	294
		- přerušení kapacitoru C3 (SXE 50 -330 μF)	- ztráta funkce – ukazovatel bez funkce	3	7	1	2	42
		- zkrat kapacitoru C3 (SXE 50 - 330 μF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- přerušení kapacitoru C4 (SR201C - 47 nF)	- bez vlivu na funkci ukazovatele (i když C3 shoří)	3	1	8	8	192
		- zkrat kapacitoru C4 (SR201C - 47 nF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- přerušení kapacitoru C5 (SR201C - 47 nF)	- bez vlivu na funkci ukazovatele (možnost rušení)	3	2	7	7	294
		- zkrat kapacitoru C5 (SR201C - 47 nF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- porucha tlumivky L1 (314 - 293E1)	- ztráta funkce – definovaný stav - ručka na bílém oblouku	3	7	1	2	42
7. Diagnostické prostředky	Hlídají napájecí napětí, obsluhují RESET, „optickou závoru“	- porucha čítače DD3 (PC74HCT93T)	- bez vlivu na funkci ukazovatele (při překročení určitého počtu RESETů nastane definovaný stav - ručka na bílém oblouku)	4	3	7	5	420
		- porucha obvodu DD4 (DS1232LPSN - 2)	- ztráta funkce – buď trvalý RESET nebo žádný RESET i když by měl	4	8	2	2	128
		- porucha optické závory CNY 70	- ztráta funkce – nezorientuje se na číselníku ukazovatele	4	8	1	2	64
		- přerušení rezistoru R11, R11a (SMD 1206 - 715R)	- ztráta funkce – nesynchronizuje se ručička a nastane definovaný stav – ručka na bílém oblouku	3	7	1	2	42
		- zkrat rezistoru R11 nebo R11a (SMD 1206 - 715R)	- ztráta funkce – nesynchronizuje se ručička a nastane definovaný stav – ručka na bílém oblouku	3	7	1	2	42
		- přerušení rezistoru R12 (SMD 0805 - 22k)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat rezistoru R12 (SMD 0805 - 22k)	- ztráta funkce – definovaný stav - ručka na bílém oblouku	3	7	1	2	42
		- přerušení kapacitoru C1 ÷ C6 (SMD 1206 - 47 nF)	- bez vlivu na funkci ukazovatele	3	1	8	8	192
		- zkrat kapacitoru C1÷C6 (SMD1206-47 nF)	- ztráta funkce – ručička stojí	3	8	1	2	48

PRACOVNÍ FORMULÁŘ FMECA PRO SOUPRAVU MĚŘENÍ PODÉLNÉHO VYVÁŽENÍ LUN 1755 A LUN 1756

Název modulu	Popis funkce modulu	Předvídané poruchy	Možné následky poruchy	F 1	F 2	F 3	F 4	RN
8. Vysílač	Snímá výchylku podélného vyvážení a převádí ji na elektrické napětí.	- porucha potenciometru RP11/500F - porucha připojovacího konektoru	- ztráta funkce – souprava bez funkce - ztráta funkce – souprava bez funkce	3 1	8 8	1 1	2 2	48 16
9. Připojovací konektory		- porucha připojovacího konektoru	- ztráta funkce – souprava bez funkce	1	8	1	2	16

VYUŽITÍ METODY FMEA PŘI ANALÝZE BEZPEČNOSTI DOPRAVNÍHO LETOUNU

Doc. Ing. Zdeněk VINTR, CSc.

Otázkám bezpečnosti leteckého provozu je v jednotlivých zemích i na mezinárodní úrovni věnována značná pozornost, protože případné selhaní techniky nebo lidského faktoru v této oblasti může vést k velkým materiálním ztrátám i ohrožení životů a zdraví značného počtu lidí. Z tohoto důvodu jsou všechny činnosti související s leteckým provozem poměrně přísně regulovány a v podstatě každá země má pro tuto oblast vytvořen soubor zákonů, směrnic a standardů, které usměrňují všechny činnosti s touto oblastí související.
Zvláštní místo v souborech těchto dokumentů mají předpisy stanovující technické požadavky na konstrukci letecké techniky. Tyto dokumenty mají zpravidla závazný charakter a každý výrobce, který chce leteckou techniku vyrábět, je musí akceptovat a jejich dodržení stanoveným způsobem prokazovat.
Velká pozornost je v leteckých předpisech věnována otázkám bezpečnosti letounu a jeho soustav. Jsou zde vymezeny jak požadavky, které musí letoun v této oblasti splňovat, tak i způsoby, kterými je možno splnění těchto požadavků prokázat. Za jeden ze základních způsobu průkazu bezpečnosti letounu jsou považovány analýzy inherentní spolehlivosti letounu, ve kterých nezastupitelnou roli sehrává *analýza způsobů a důsledků poruch* (metoda FMEA) [6], [7].
Cílem tohoto příspěvku je rámcově nastínit problematiku analýz spolehlivosti a bezpečnosti letecké techniky a vymezit místo, úlohu a zvláštnosti aplikace metody FMEA při predikci spolehlivosti dopravního letounu a jeho soustav.

1. Požadavky na bezpečnost dopravního letounu a jeho soustav

Požadavky na bezpečnost dopravních letounů představují poměrně rozsáhlý soubor technických specifikací, které velice podrobně vymezují kvalitativní a kvantitativní požadavky, které musí být u letounu pro zajištění jeho bezpečnosti splněny. Pro potřeby tohoto příspěvku se omezím pouze na nejvýznamnější z těchto požadavků, jejichž stručný (a zjednodušený) přehled je dále uveden.

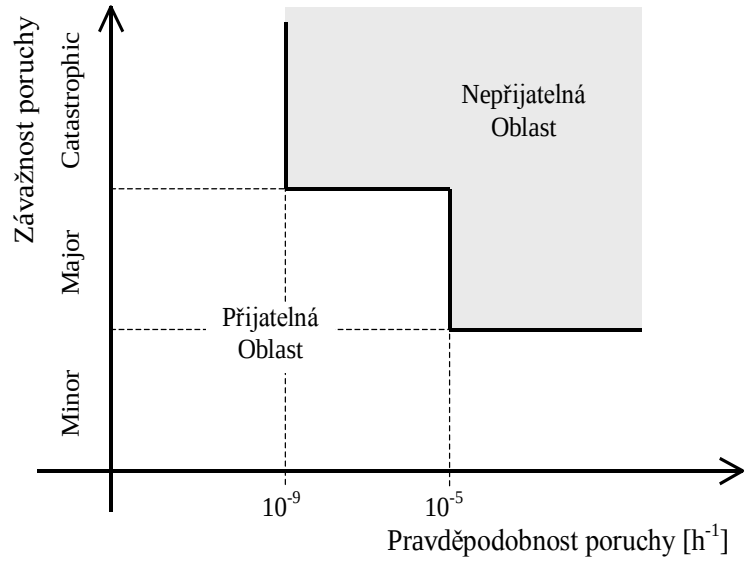
Podle leteckých předpisu [4], [5] musí být prvky a letadlové systémy z nich vytvořené uvažovány jednotlivě, ve vzájemném spojení i ve spojení s ostatními systémy letounu navrženy a zhotoveny tak, aby za všech předvídatelných podmínek provozu:

- výskyt jakéhokoliv poruchového stavu, který by mohl znemožnit pokračování bezpečného letu a přistání letounu byl extrémně nepravděpodobný (poruchové stavy tohoto typu jsou označovány jako katastrofické poruchové stavy - Catastrophic);
- výskyt jakéhokoliv poruchového stavu, který by mohl omezit (snížit, redukovat) schopnost letounu nebo posádky letounu zvládnout nepříznivé provozní podmínky byl nepravděpodobný (poruchové stavy tohoto typu jsou označovány jako závažné poruchové stavy - Major).

Poruchové stavy, které významně nesnižují bezpečnost letounu mohou být pravděpodobné (tyto poruchové stavy jsou označovány jako nezávažné – Minor). Jednotlivé poruchové stavy jsou podle předpisů [5] považovány za:

- pravděpodobné jestliže pravděpodobnost jejich výskytu je větší než $1{,}0 \cdot 10^{-5}$ za hodinu letu.
- nepravděpodobné jestliže pravděpodobnost jejich výskytu je menší než $1{,}0 \cdot 10^{-5}$ za hodinu letu ale větší než $1{,}0 \cdot 10^{-9}$;
- extrémně nepravděpodobné pokud pro pravděpodobnost jejich výskytu během jedné hodiny letu platí, že je menší než $1{,}0 \cdot 10^{-9}$.

V leteckých předpisech se tedy požaduje, aby každý poruchový stav měl pravděpodobnost nepřímo úměrnou jeho závažnosti. Grafické vyjádření tohoto požadavku – viz obr. 1.
Dále předpisy nepřipouští, aby poruchový stav, který je důsledkem pouze jediného druhu poruchy byl považován za extrémně nepravděpodobný. Jinak řečeno – je nepřijatelné, aby jednotlivá porucha některého z prvku letadlových systémů vedla ke katastrofickým důsledkům.



Obr. 1 Vztah mezi závažností poruchových stavů a jejich přípustnou pravděpodobností

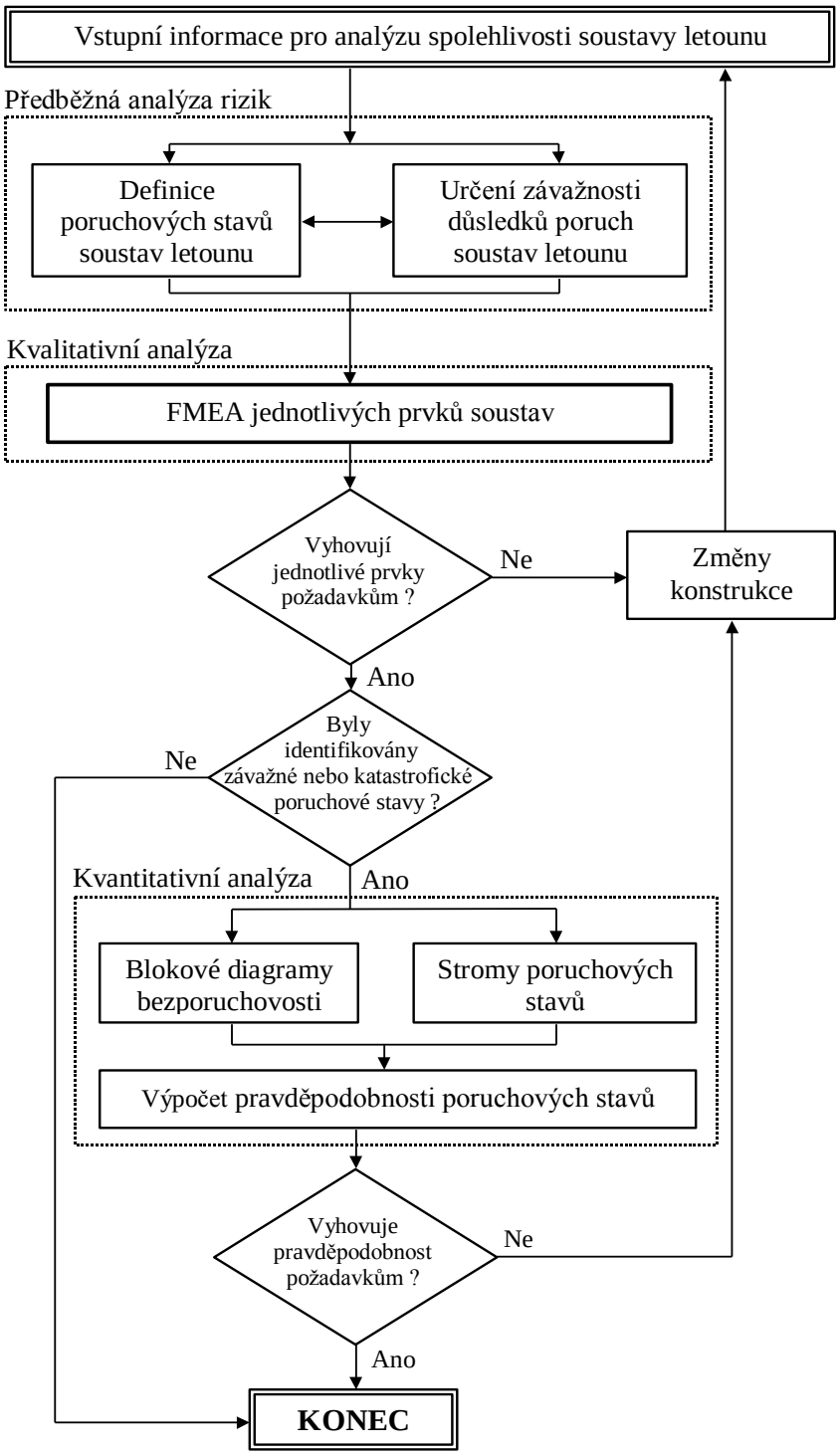
2. Analýza bezpečnosti letounu a jeho soustav

Splnění výše uvedených požadavků musí být podle leteckých předpisů prokázáno analýzou bezpečnosti a tam, kde je to nezbytně nutné, odpovídajícími pozemními, letovými nebo simulačními zkouškami. Za prioritní a hlavní metodu průkazu splnění požadavků je tedy považována analýza bezpečnosti, přičemž se požaduje aby tato analýza obsahovala:

- přehled všech možných způsobů poruch včetně způsobů selhání funkce a možných způsobů poškození z vnějších příčin a zdrojů;
- odhad (výpočet) pravděpodobnosti vzniku poruch prvků a kombinací poruch včetně, skrytých poruch;
- analýzu výsledného důsledku poruch na systém, na letoun a na posádku a cestující ve všech jednotlivých fázích letu a převídatelných provozních podmínkách;

- přehledný výčet výstražných a varovných signálů a pokynů pro posádku, požadovaných nápravných opatření a prostředků pro včasnou identifikaci poruchy.

Celý postup analýzy je vhodné uspořádat do logicky navazujících kroků, které zajistí splnění požadovaných cílů analýzy. Letecké předpisy striktně nevymezují jaké metody a postupy mají být při analýze použity a případ od případu se způsob provádění analýzy může lišit.
Dále bude prezentován obecný postup, který byl použit při analýzách dopravního letounu L-610 G v procesu jeho certifikace [1], [2] [3].
Prvním krokem postupu je provedení tzv. *hodnocení funkční nebezpečností* každé soustavy letounu. Jedná se v podstatě o modifikovanou *předběžnou analýzu rizik* (Preliminary Hazard Analysis), jejímž cílem je určení a klasifikace nebezpečných poruchových stavů letadlových soustav. V rámci této části analýzy by měly být identifikovány všechny závažné a katastrofické poruchové stavy každé soustavy. Vychází se přitom z analýzy funkcí soustavy a posouzení důsledků selhání těchto funkcí. Výsledky této analýzy vždy mají předběžný charakter a je třeba je doplňovat a verifikovat na základě výsledků dalších kroků analýzy.
Na hodnocení funkční nebezpečnosti navazuje kvalitativní analýza spolehlivosti prvků soustavy, kde se posuzuje zda jednotlivé prvky soustavy splňují příslušné požadavky. K realizaci tohoto kroku se využívá metod *FMEA*. Ta umožňuje identifikaci všech způsobů poruch jednotlivých prvků a posouzení jejich důsledků na jednotlivé subsystémy, systémy i letoun jako celek.
Dalším krokem postupu je kvantitativní analýza. Při ní se vychází z výsledků kvalitativní analýzy a s využitím takových metod, jako jsou *metoda analýzy stromu poruchových stavů* nebo *metoda blokového diagramu bezporuchovosti* se určí pravděpodobnosti všech závažných a katastrofických poruchových stavů soustavy a posoudí se zda tyto číselné hodnoty splňují příslušné požadavky.



Obr. 2 Postup analýzy bezpečnosti letadlové soustavy

Analýza každé letadlové soustavy může dospět k jednomu z následujících závěrů:

- letadlová soustava splňuje všechny požadavky na bezpečnost – potom se analýza může předložit jako průkaz splnění příslušných požadavků;
- letadlová soustava nesplňuje požadavky – potom se na základě výsledků analýzy navrhnou příslušné konstrukční úpravy k odstranění zjištěných nedostatků (po realizaci změn je třeba celý postup analýzy opakovat).

Logický postup analýzy a vzájemná návaznost jednotlivých kroků je zřejmá z vývojového diagramu na obr. 2.

3. Místo a úloha metody FMEA při analýze bezpečnosti letadlové soustavy

Místo metody FMEA v celém systému analýzy bezpečnosti letounu je dobře zřejmé z obr. 2. Metoda zde slouží k provedení kvalitativní analýzy soustavy s cílem:

- identifikovat všechny možné způsoby poruch prvků;
- posoudit důsledky a posloupnosti jevů pro každý zjištěný způsob poruchy prvků a to na různých úrovních soustavy;
- určit závažnosti každého způsobu poruchy s ohledem na bezpečnost soustavy a letounu;
- zpracovat vstupní podklady k provedení kvantitativní analýzy.

Vlastní analýza se provádí standardním způsobem, proto zde celá procedura nebude podrobně popisována a vysvětlována. Dále budou zmíněny pouze některé zvláštnosti aplikace metody, které se při analýze bezpečnosti letounu objevují a nejsou zcela běžné [5].

Při hodnocení závažnosti poruchových stavů se uplatňují tři základní hlediska:

- Důsledky poruchy pro letoun jako jsou snížení rezerv bezpečnosti, zhoršení výkonnosti, ztráta schopnosti provádět určité letové činnosti nebo potenciální, popřípadě následné důsledky pro celistvost konstrukce.
- Důsledky pro členy posádky, jako je zvětšení jejich obvyklého pracovního zatížení, ovlivňujícího jejich schopnost zvládnout nepříznivé podmínky provozu nebo vnějšího prostředí, popřípadě následné poruchy.
- Důsledky pro osazenstvo – tj cestující a členy posádky, jako je snížení pohodlí či ohrožení životů a zdraví.

Při uplatnění těchto hledisek je třeba u každého poruchového stavu jednoznačně stanovit jeho závažnost a určit zda se jedná o poruchový stav *nezávažný, závažný či katastrofický*. Při třídění poruch musí být vždy přihlédnuto ke všem závažným činitelům, jako jsou funkční vlastnosti soustavy, vliv lidského činitele, podmínky provozu či vnějšího prostředí. Zvláště důležité je brát v úvahu ty činitele, které snižují, nebo zvyšují závažnost poruchového stavu.

Příkladem činitele snižujícího závažnost poruchového stavu je pokračující výkon totožných nebo provozně podobných funkcí jinými systémy, které nejsou dotčeny zkoumaným poruchovým stavem. Příkladem činitelů zvyšujících závažnost poruchového stavu mohou být povětrnostní nebo jiné nepříznivé podmínky provozu a vnějšího prostředí, případně poruchy jiných nesouvisejících systémů nebo funkcí, které by snižovaly schopnost posádky zvládnout poruchový stav.

Zvláštní pozornost je třeba při analýze věnovat *poruchám skrytým* a *poruchám se společnou příčinou*.

Skrytou poruchou rozumíme takovou poruchu, která nebude zjištěna v okamžiku kdy se vyskytne. Za významnou skrytou poruchu je považována porucha, která ve spojení s dalšími poruchami, případně událostmi bude mít za následek závažný nebo katastrofický poruchový stav. V případě identifikace takových poruch je třeba navrhnout vhodná opatření v oblasti kontrol a inspekcí, které by snížily pravděpodobnost existence takové poruchy, navrhnout vhodný způsob monitorování a signalizace, případně doporučit změnu konstrukce.

Poruchami (událostmi) se společnou příčinou rozumíme takové poruchy (události) které mohou poškodit nebo jinak nepříznivě ovlivnit více než jeden ze vzájemně se zálohujících kanálů systému nebo více než jeden systém plnicí provozně podobné funkce. Mezi takové potencionální poruchy (událostí) se společnou příčinou můžeme například zahrnout rychlé uvolnění energie z koncentrovaných zdrojů, jakými jsou nezachycené poruchy rotačních částí a tlakových nádob, ztráta ochrany proti vnějšímu prostředí, poškození ohraničenými požáry, ztráta zdrojů energie, chyby lidského činitele, podmínky vnějšího prostředí apod.

Z uvedeného je patrné, že se v tomto případě nepožaduje pouze zkoumání důsledku poruchy jednotlivých prvků jako takových, ale je nezbytné zkoumat důsledky poruch prvků i v kombinaci s poruchami jiných prvků.

Výsledky analýzy se průběžně zaznamenávají do pracovního formuláře, který by měl zahrnovat následující položky u každého prvku systému: označení prvku a jeho jednoznačná identifikace, název prvku, popis funkce, možné způsoby poruchy, fáze letu, důsledek poruchy pro systém a letoun, hodnocení závažnosti poruchy a další potřebné údaje. Pro potřeby

následné kvantitativní analýzy je vhodné do formuláře uvést i příslušné číselné hodnoty ukazatelů bezporuchovosti.

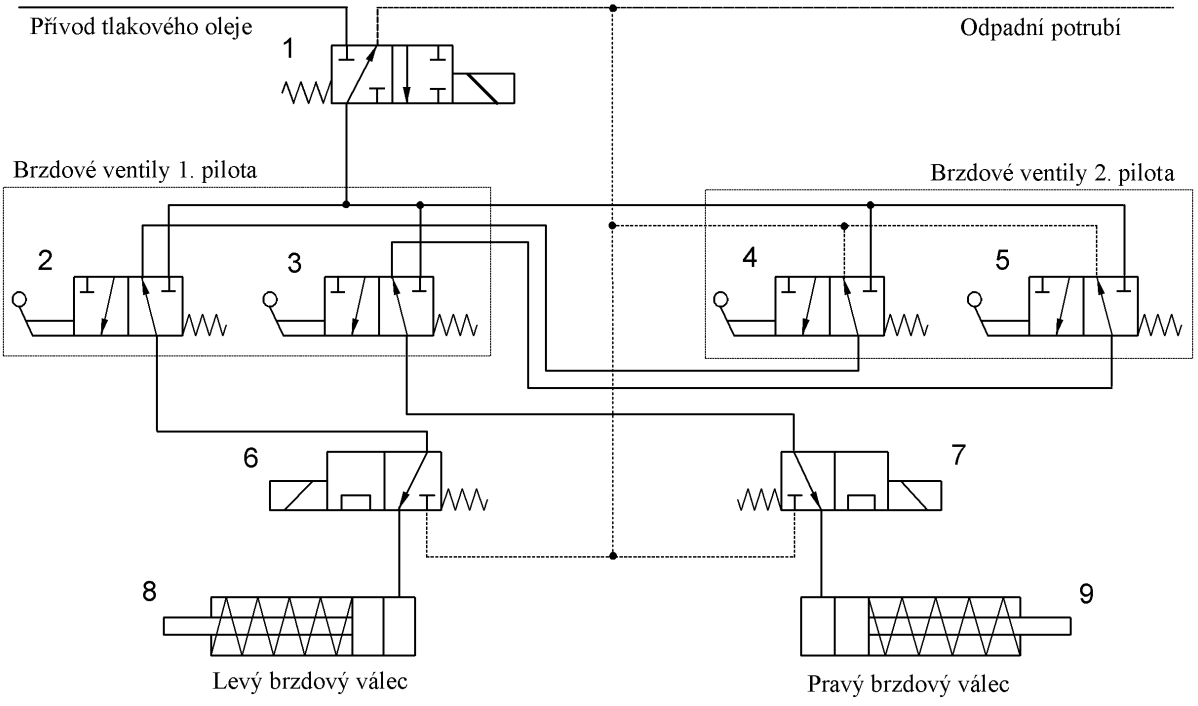
4. Příklad použití metody FMEA při analýze bezpečnosti brzdové soustavy letounu

Podrobněji bude aplikace metody FMEA při analýze bezpečnosti dopravního letounu ukázána na příkladu brzdové soustavy letounu. Na obr. 3 je znázorněna část této soustavy a to hydraulický systém ovládání brzd letounu. V rámci předběžné analýzy rizik byly u této části soustavy identifikovány, mimo jiné, dva následující poruchové stavy [1]:

- přistání letounu se zabrzděnými koly;
- selhání brzdové soustavy při pohybu letounu po zemi.

Další poruchové stavy, které byly u soustavy identifikovány zde nejsou uváděny, protože jejich znalost není pro uváděný příklad podstatná.

K přiblížení vlastního řešení je nezbytné alespoň základní objasnění funkce systému. Hydraulická kapalina je do systému přiváděna přes elektromagnetický rozvaděč 1, který je otevřen pokud je podvozek letounu zatížen (letoun se pohybuje po zemi). Vlastní brždění je řízeno buď prvním pilotem brzdovými ventily 2 a 3, nebo druhým pilotem brzdovými ventily 4 a 5. Při ovládání brzdových ventilů má prioritu první pilot. Z brzdových ventilů kapalina proudí do brzdových válců 8 a 9, které přímo ovládají kotoučové brzdy hlavního podvozku letounu. Mezi brzdové ventily a brzdové válce jsou vloženy elektromagnetické ventily 6 a 7, které plní funkci akčních členů systému ABS a které zajišťují krátkodobé přerušování brždění v případě zablokování a prokluzu kol.



Obr. 3 Zjednodušené schéma hydraulického ovládání brzd letounu

Pro hodnocení závažnosti poruchových stavů jsou důležité také následující informace. Přistání se zabrzděnými koly je považováno za katastrofický poruchový stav a selhání brzd při pohybu letounu po zemi za nezávažný poruchový stav (u letounu existují jiné možnosti brždění).

Vzhledem k omezenému prostoru, který je pro tento příspěvek k dispozici, nebude zde ukázána analýza všech prvků systému, ale jen jednoho z nich. Z hlediska bezpečnosti se v popisovaném systému jako kritický prvek jeví elektromagnetický rozvaděče 1. Proto bude postup analýzy demonstrován právě pro tento prvek.

Záznamy zachycující průběh analýzy prvku zde budou účelově pojaty poněkud podrobněji, aby z nich byl dobře patrný postup analýzy i úvahy, které ji provází. Výsledky analýzy proto nebudou zaznamenávány do pracovního formuláře, jak je to obvyklé, ale formou volného textu.

1) Funkce prvku

- Pokud je na svorkách elektromagnetu rozvaděče napětí, rozvaděč propouští tlakovou kapalinu do brzdového systému.
- Pokud na svorkách elektromagnetu rozvaděče není napětí, rozvaděč uzavírá přívod tlakové kapaliny do brzdového systému.

(Do otevřené polohy je rozvaděč přestavován silou elektromagnetu, do uzavřené polohy se vrací působením síly pružiny. Elektrický signál, který řídí otevírání a zavírání rozvaděče je generován v jiném systému letounu a na kontakty rozvaděče je přiváděn vždy, když jsou zatíženy podvozkové nohy letounu, tj, po celou dobu, kdy se letoun pohybuje po zemi.)

2) Způsoby poruchy

a) Rozvaděč po přivedení napětí na jeho svorky neotevře přívod tlakové kapaliny do brzdového systému, nebo v době kdy je napětí na jeho svorky přiváděno se samovolně uzavře.
b) Rozvaděč po přerušení přívodu napětí na jeho svorky neuzavře přívod tlakové kapaliny do brzdového systému, nebo v době kdy na jeho svorkách není napětí se samovolně otevře.

3) Důsledky poruchy pro soustavu:

ad a) V brzdovém systému není tlak v době kdy je to požadováno.
ad b) V brzdovém systému je tlak v době kdy je to nežádoucí.

4) Důsledky poruchy pro letoun

ad a) Nelze brzdit letoun provozními brzdami. (Nedotčena zůstává možnost brzdit nouzovou brzdou a reverzací tahu motorů)
ad b) Potenciální možnost přistání se zabrzděnými koly. Tato možnost může nastat pouze v kombinaci s jinými poruchami nebo událostmi. Letoun přistane se zabrzděnými koly jestliže současně s analyzovaným poruchovým stavem:
- nastane porucha způsobující vnitřní netěsnost některého z brzdových ventilů 2, 3, 4 nebo 5.
- některý z pilotů během přistání otevře brzdové ventily před tím, než dojde k plnému zatížení podvozků letounu.

Svým charakterem se jedná o skrytý poruchový stav, který se nijak navenek neprojeví (pokud nedojde k souběhu výše popsaných událostí).

5) Závažnost poruchového stavu

ad a) Jedná se o poruchový stav *nezávažný*. Situaci je posádka schopna vyřešit při využití běžných postupů. Letoun je možno zabrzdit s využitím nouzové brzdy a reverzací tahu motorů.
ad b) Sám o sobě je tento poruchový stav *nezávažný*, protože bezprostředně nevede k žádným závažným důsledkům. Avšak při souběhu s jinými událostmi může vyústit až do *katastrofického poruchového stavu.* Při hodnocení závažnosti je nutné vzít v úvahu že se jedná o skrytý poruchový stav, který se projeví právě až v okamžiku souběhu s událostmi vedoucími k potenciální letecké katastrofě. S ohledem na to je nutné tento poruchový stav označit jako katastrofický a naznačené konstrukční řešení soustavy klasifikovat jako nevyhovující.

6) Závěr analýzy

Z výše naznačených výsledků analýzy elektromagnetického rozvaděče je patrné, že analyzovaná konstrukce brzdového systému nesplňuje požadavky leteckých předpisů. V tomto konkrétním případě lze situaci vyřešit poměrně jednoduchou konstrukční změnou. Do soustavy bude zabudována výstražná signalizace, která bude piloty informovat o existenci příslušného poruchového stavu, tedy o tom, že v době kdy nejsou podvozkové nohy zatíženy (za letu) je brzdový systém pod tlakem. Realizací tohoto opatření zkoumaný poruchový stav

ztratí skrytý charakter a je možno ho považovat za *nezávažný*. Po této úpravě již soustava bude splňovat požadavky leteckých předpisů.
Zde je třeba podotknout, že poruchový stav se stejnými důsledky (tlak v brzdové soustavě za letu) může být způsoben také poruchou řady dalších prvků, které se podílí na řízení elektromagnetického rozvaděče (generují a přenáší signál o zatížení podvozků). Zavedením výstražné signalizace se tak sníží závažnost i všech těchto dalších poruchových stavů.

5. Závěr

Metoda FMEA je v současnosti v oblasti bezpečnosti letecké dopravy považována za jednu z nejdůležitějších metod analýzy bezpečnosti leteckých konstrukci. Nicméně na závěr je třeba zdůraznit alespoň dva závažné aspekty související s její aplikací:

- Analytik, který metodu aplikuje musí dokonale znát jak použití vlastní metody, tak i soustavu kterou analyzuje, proto musí při vlastní analýze úzce spolupracovat s celou řadou dalších odborníků – konstruktérů, pilotů, provozních techniků atd. Jedině tak lze zajistit, aby nic závažného při vlastní analýze nebylo opomenuto.
- Metoda sama o sobě není všemohoucí, ale vždy při analýze bezpečnosti letounu musí být používána v kombinaci s jinými standardními analytickými postupy se kterými se vzájemně doplňuje.

Použitá literatura:

[1] HOLUB, R. a VINTR, Z.: *Analýza spolehlivosti a bezpečnosti systému ovládání brzd s protiblokovacím zařízením letounu L-610 G*. [Výzkumná zpráva]. Brno: Vojenská akademie 1995.

[2] HOLUB, R. and VINTR, Z.: Integrated Safety Program of L-610G Transport Aeroplane Development. In: *PSAM 5 - Probabilistic Safety Assessment and Management – Proceedings of 5th International Conference on Probabilistic Safety Assessment and Management*. Tokyo: Universal Academy Press 2000.

[3] HOLUB, R. and VINTR, Z.: The Reliability/Safety Analyses of Transport Aeroplane Systems in Process of their Certification. In: *Safety and Reliability in Transport - Proceeding of the 16th ESReDA Semminar.* Luxembourk: European Communities 2000.

[4] Federal Aviation Regulations – FAR Part 25. Washington: Federal Aviation Administration 1988.

[5] Advisory Circular 25.1309-1A: System Design and Analysis. Washington: Federal Aviation Administration 1988.

[6] MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects, and Criticality.

[7] ČSN IEC 812 – Metody analýzy spolehlivosti systémů. Postup analýzy způsobů a důsledků poruch (FMEA). Praha: ČSNI 1992.

KOMPLEXNÍ HODNOCENÍ SPOLEHLIVOSTI VAROVNÉHO SYSTÉMU

Ing. Pavel Fuchs, CSc.

Úvod

Při hodnocení spolehlivosti systémů je FMEA, resp. FMECA, používána často na různých úrovních řešené úlohy. Jedním ze zajímavých příkladů z praxe je hodnocení spolehlivosti varovného systému. Zajímavost prezentovaného příkladu spočívá v tom, že názorně předvádí různé aspekty spojené s hodnocením spolehlivosti, včetně těch, které byly vyvolané nedostatečnou pozorností věnované spolehlivosti varovného systému v jednotlivých etapách vývoje, výroby a předávání zákazníkovi.

Z důvodu, který bude zřejmý při sledování postupu řešení uváděného příkladu, byla úloha rozčleněna na dvě vzájemně související části. V první části je obsažena analýza spolehlivosti varovného systému, ve druhé části je uvedeno ověření spolehlivosti varovného systému na základě hodnocení jeho provozu.

S ohledem na smluvní závazky spojené s uveřejňováním těchto informací je uvedený příklad prezentován obecně a číselné hodnoty ukazatelů spolehlivosti jsou jen informativní.

1 Analýza spolehlivosti varovného systému

1.1 Formulace zadání úlohy

Na základě objednávky průmyslového podniku byl dodavatelem vyvíjen systém pro varování obslužného personálu v případě havárie spojené s únikem nebezpečných látek. Objednatel požadoval od zhotovitele hodnocení spolehlivosti varovného systému, ten požadavek akceptoval a vybral vhodného řešitele. Řešitel formuloval zadání úlohy a její řešení do těchto kroků:

- stanovení požadavků na spolehlivost varovného systému,
- analýza poruch varovného systému,
- predikce hodnot ukazatelů spolehlivosti varovného systému.

Řešitel zahájil analýzu varovného systému za situace, kdy koncepce systému již byla navržena a moduly systému byly ve fázi výroby prototypů.

1.2 Popis varovného systému

Varovný systém je tvořen ze 160 vnitřních sirén umístěných v objektech areálu průmyslového podniku. Ovládání sirén se realizuje prostřednictvím dvojice počítačů třídy PC (vysílačů) přes komunikační síť. Pomocí modulů (jednotek) opakovače je struktura komunikační sítě rozdělena do 16 sekcí. Ke každé sekci lze připojit nejvýše 10 sirén. Signály vysílače jsou přes modul opakovače předávány přijímači sirény. Při požadavku (příkaz autorizované osoby) vysílač aktivuje sirénu. Sirény je možno ovládat individuálně nebo po skupinách.

Režim činnosti varovného systému lze rozdělit na periodické testování stavu systému (vyjma zkoušky spouštění sirén) a na generování povelu pro spuštění sirén (ostrý poplach nebo zkouška sirén). Periodické testování stavu systému je založeno na cyklickém testování stavu vysílačů a přijímačů. Jeden z vysílačů je navolen jako hlavní, druhý je záložní. Hlavní i záložní vysílač provádějí cyklicky v intervalu nepřesahujícím 10 s autodiagnostiku vlastního stavu, diagnostiku periferií (tiskárny) a vzájemnou komunikací si sdělují stav vlastní a ověřují stav druhého vysílače. Hlavní vysílač řídí v dotazovacím režimu provoz na společné síti varovného systému. Záložní vysílač pouze sleduje zprávy na této síti, provádí paralelně s hlavním vysílačem jejich dekódování, třídění a archivaci. Za normálního provozu (nepožaduje se spuštění sirén) se hlavní vysílač cyklicky v intervalu 3 s dotazuje na stav všech přijímačů. Získaná data průběžně vyhodnocuje a v případě závady nebo změny stavu přijímače

tento stav ohlásí na monitoru, vypíše na připojenou tiskárnu a zaznamená do trvalého archivního souboru na disk.

Spuštění sirén (ostrý poplach na všech sirénách nebo na jedné adresované siréně, test všech sirén nebo test jedné adresované sirény) může provést jen autorizovaná osoba z hlavního vysílače. Při spouštění ze záložního vysílače se tento vysílač automaticky stává hlavním. Iniciaci sirén může zrušit pouze autorizovaná osoba z hlavního vysílače. Test sirén se předpokládá dvakrát do roka, případně čtvrtletně.

1.3 Požadavky na spolehlivost varovného systému

Na varovný systém je třeba pohlížet jako na ochranný systém. U tohoto systému je třeba následující stavy:

- bezporuchový stav - systém je schopen plnit požadovanou funkci,
- stav bezpečné poruchy - systém neoprávněně generuje varovný signál (není havarijní situace) a dochází k falešnému poplachu,
- stav nebezpečné poruchy - systém není schopen vyslat varovný signál.

Oba poruchové stavy je třeba potlačit, neboť ve svých důsledcích snižují účinnost varování a tedy i ochrany osob. Stav nebezpečné poruchy tuto účinnost snižuje přímo. Stav bezpečné poruchy snižuje účinnost ochrany zprostředkovaně, neboť časté falešné poplachy vedou k diskreditaci varovného systému a tím k nežádoucímu chování osob v případě skutečného poplachu. Protože neexistuje norma nebo předpis, který by předepisoval pro varovné systémy hodnoty ukazatelů spolehlivosti, byla jeho spolehlivost hodnocena na základě:

- analýzy funkcí varovného systému,
- přiměřenosti požadované ochrany osob ve vztahu k technickým prostředkům a k možnosti varování osob dalšími prostředky.

Analýzou funkcí systému se rozumí analýza funkce vydání varovného signálu jednou sirénou, skupinou sirén jedné sekce varovného systému nebo všemi sirénami varovného systému. Přiměřeností požadované ochrany se rozumí stanovení takové úrovně spolehlivosti varovného systému, která **je adekvátní četnosti výskytu havarijní události a jejím následkům, hardwarovým a softwarovým prostředkům dostupným pro realizaci varovného systému a možnosti vyrozumění osob o nastalé havarijní situaci prostřednictvím dalších prostředků nebo kanálů**.

Pro hodnocení spolehlivosti varovného systému byly doporučeny tyto ukazatele spolehlivosti:

$T_{stř}$ - střední doba provozu mezi poruchami (ČSN IEC 50(191), def. 191-12-09) pro bezpečnou poruchu,

U - součinitel nepohotovosti (ČSN IEC 50(191), def. 191-11-08) pro nebezpečnou poruchu.

Hodnoty ukazatelů spolehlivosti varovného systému byly doporučeny podle hodnot uvedených v tab. 1.

Tab. 1: Doporučované hodnoty ukazatelů spolehlivosti varovného systému

Hodnocená funkce	**Bezpečná porucha $T_{stř}$ [h]**	**Nebezpečná porucha U [1]**
varovný signál od 1 sirény varovného systému	1.10^6	1.10^{-2}
varovný signál od skupiny sirén jedné sekce varovného systému	$1{,}5.10^6$	1.10^{-3}
varovný signál od všech sirén varovného systému	2.10^5	1.10^{-4}

Požadované hodnoty ukazatelů spolehlivosti byly stanoveny s přihlédnutím k těmto skutečnostem:

- četnost úniku nebezpečných látek je $n = 2.10^{-3} - 1.10^{-6}$ rok^{-1},
- hodnota ukazatelů spolehlivosti běžné technolog. ochrany je $T_{stř} = 1.10^5$ h, $U = 4.10^{-4}$,
- do jedné sekce varovného systému lze zapojit nejvýše 10 sirén,

- varovný systém bude obsahovat až 160 sirén,
- při selhání varovného signálu z jedné či více sirén lze v areálu podniku předpokládat předání informace o havarijní situaci jinými prostředky (telefon, osobní styk apod.).

1.4 Analýza poruch systému a predikce hodnot ukazatelů spolehlivosti

Při analýze spolehlivosti varovného systému bylo přistoupeno k hodnocení jeho spolehlivosti na základě hodnocení jeho funkčně ucelených částí. Hodnocení bylo provedeno pro:

- dvojici vysílačů včetně napájení,
- modul opakovače,
- napájení skříně opakovačů,
- přijímač včetně napájení a siréna,
- modul oddělovače včetně napájení,
- komunikační trasu.

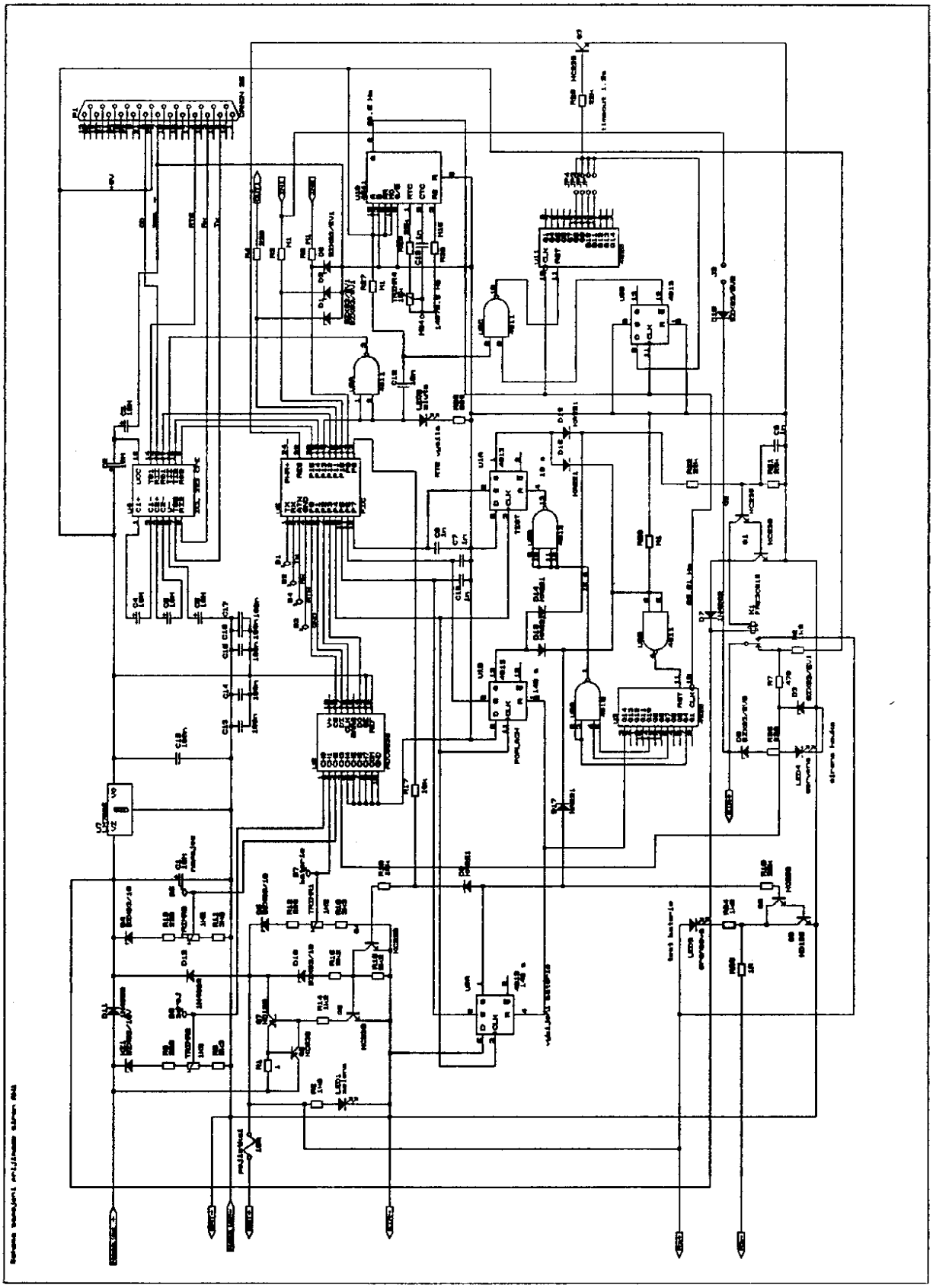
Z důvodu omezeného rozsahu příspěvku je stručně uvedena jen analýza spolehlivosti přijímače, který se projevil jako kritická část varovného systému.

Schéma přijímače je uvedeno na obr. 1. Úkolem přijímače je zabezpečení komunikace s vysílači, kontrola napájení, kontrola stavu akumulátoru a nabíjecí soustavy, kontrola stavu vedení k siréně, kontrola přítomnosti sirény, ovládání silového výstupu pro sirénu. Protože přijímač může být zdrojem falešného signálu, bylo analyzováno, které prvky při své poruše mohou způsobit vznik nebezpečné a bezpečné poruchy funkce přijímače. Na obr. 1 jsou barevně značeny prvky a obvodové struktury přijímače, jejichž porucha způsobí poruchu přijímače. Barevné značení rozlišuje, zda označený prvek nebo obvod vyvolá bezpečnou nebo nebezpečnou poruchu přijímače. Přehled prvků, jejichž porucha způsobí bezpečnou a nebezpečnou poruchu a hodnoty ukazatelů spolehlivosti těchto prvků jsou uvedeny v tab. 2 a 3. Pro výpočet ukazatelů spolehlivosti přijímače byla uvažována konzervativně celková intenzita poruch prvku bez rozlišení, který typ poruchy prvku způsobí bezpečnou a nebezpečnou poruchu přijímače.

Z analýzy poruch přijímače vyplynulo, že ke vzniku falešného signálu může dojít jednak při normálním klidovém režimu přijímače a jednak při zkoušce sirén. Tab. 2 rozděluje prvky do dvou kategorií. V první kategorii (horní část tabulky) jsou prvky, jejichž porucha způsobí generování falešného signálu při běžném režimu přijímače. V druhé kategorii jsou prvky, jejichž porucha se projeví generováním falešného signálu při testu sirén tím způsobem, že zkouška sirén není ukončena v předepsané době a sirénu nelze vypnout. I když se porucha některého z těchto prvků projeví až při testu sirén, není pravděpodobnost poruchy prvků tímto testem omezena (je ovlivněn pouze okamžik, kdy se porucha může projevit).

Tab. 2: Přehled prvků, které způsobí bezpečnou poruchu přijímače a hodnoty ukazatelů spolehlivosti

Prvek	Počet ks	Intenzita poruch λ [h^{-1}]
mikrořadič	1	7.10^{-6}
klopný obvod	2	1.10^{-6}
tranzistor	2	1.10^{-7}
dioda	1	3.10^{-8}
generátor hodinového kmitočtu	1	4.10^{-6}
čítač impulsů	1	2.10^{-6}
logické hradlo	3	1.10^{-7}
kondenzátor	1	2.10^{-8}
dioda	1	3.10^{-8}
trimr	1	2.10^{-7}
odpor	3	1.10^{-8}
spínací relé sirény	1	1.10^{-6}



Obr. 1: Schéma přijímače

Na základě hodnot intenzity poruch prvků a jejich zapojení v přijímači byla pro bezpečnou poruchu přijímače stanovena hodnota střední doby provozu mezi poruchami, které mají za následek generování falešného signálu, $\mathbf{T_{stř}} = \mathbf{5{,}9.10^4\ h}$ (cca 7 let).

Uvedená hodnota střední doby pro bezpečnou poruchu přijímače je nepřiměřeně nízká. Ve svém důsledku znamená, že při předpokládané instalaci 160 poplachových sirén v areálu průmyslového podniku bude vyvolán falešný poplach od jedné sirény přibližně každých 15 dnů ($5{,}9.10^4$ h : 160 sirén). Řešit tuto situaci bylo možné změnou konstrukce přijímače nebo náhradou prvků uvedených v tab. 2, které jsou běžné komerční jakosti, prvky s vysokou spolehlivostí používané pro průmyslové a speciální účely. Nejlepšího výsledku se dosáhne kombinací obou přístupů.

Z analýzy poruch přijímače vyplynulo, které prvky mají vliv na nebezpečnou poruchu přijímače. Tyto prvky jsou uvedeny v tab. 3.

Tab. 3: Přehled prvků, které způsobí nebezpečnou poruchu přijímače a hodnoty ukazatelů spolehlivosti

Prvek	Počet ks	Intenzita poruch λ [h^{-1}]	Střední doba neschopnosti provozu T_o [h]	Součinitel nepohotovosti U [-]
patice CANNON	1	5.10^{-8}	12	6.10^{-7}
modem PATTON	1	8.10^{-6}	12	1.10^{-4}
sériové rozhraní	1	3.10^{-6}	12	4.10^{-5}
mikrořadič	1	7.10^{-6}	12	8.10^{-5}
obvod W-D	1	1.10^{-6}	12	1.10^{-5}
kondenzátor sériového rozhraní	5	2.10^{-8}	12	2.10^{-7}
stabilizátor 5 V	1	8.10^{-7}	24	2.10^{-5}
kondenzátor stabilizátoru	2	2.10^{-8}	24	5.10^{-7}
tranzistor	3	1.10^{-7}	2200	2.10^{-4}
kondenzátor	1	2.10^{-8}	2200	4.10^{-5}
odpor	2	1.10^{-8}	2200	2.10^{-5}
spínací relé sirény	1	1.10^{-6}	2200	2.10^{-3}
klopný obvod	1	1.10^{-6}	---	---
dioda	1	3.10^{-8}	---	---

Aby bylo možno stanovit vliv poruchovosti prvků na nebezpečnou poruchu přijímače, bylo na jednotlivé prvky pohlíženo jako na opravované prvky (prvky se v praxi při poruše vyměňují za nové a obnova je tedy vztahována k funkci prvku). To umožnilo přiřazovat prvkům (respektive jejich funkcím) součinitel nepohotovosti. Doba neschopnosti provozu prvku po poruše se skládá z doby potřebné k zjištění poruchy prvku (závisí na četnosti testu) a z doby potřebné k odstranění poruchy. Tab. 3 rozděluje prvky podle doby obnovy do tří kategorií.

V první kategorii střední doba neschopnosti provozu nepřesahuje 24 h. Do této kategorie patří prvky, které jsou softwarově cyklicky testovány v intervalu 3 s. Porucha je zjištěna okamžitě, střední doba neschopnosti provozu se shoduje s reálnou dobou opravy a má hodnotu 12 h (s přihlédnutím ke všem zpožděním, která se v průmyslovém provozu vyskytují mezi dobou detekce poruchy a provedením opravy). Do této kategorie řadíme i prvky, které jsou testovány jednou denně (obvody napájení). Střední doba zjištění poruchy činí v tomto případě 12 h a spolu s reálnou dobou opravy 12 h je střední doba neschopnosti provozu 24 h.

Do druhé kategorie náleží prvky, které nejsou softwarově testovány. Porucha těchto prvků je zjištěna až při testu sirény. Při předpokladu, že sirény jsou testovány 2x ročně, je střední doba neschopnosti provozu dána intervalem mezi výskytem poruchy prvku a jejím odhalením při testu, tj. asi 2200 h. Dobu provedení opravy lze ve srovnání s hodnotou 2200 h zanedbat.

Třetí kategorii tvoří prvky, které nejsou testovány. Jejich porucha by byla zjištěna při ostrém poplachu nebo při revizi zařízení, pokud by tyto prvky byly zkoušeny. Střední dobu neschopnosti provozu nelze vyčíslit a pravděpodobnost poruchy těchto prvků roste s časem.

Na základě uvedených skutečností byly formulovány tyto **závěry**:

1. Prvky první kategorie mají malý podíl na pravděpodobnosti nebezpečné poruchy. Jejich příspěvek k nepohotovosti přijímače činí cca 3.10^{-4}.
2. Prvky druhé kategorie přispívají k nepohotovosti přijímače hodnotou $2{,}5.10^{-3}$. V této hodnotě má dominantní podíl spínací relé sirény hodnotou $2{,}2.10^{-3}$. U dobře navrženého přijímače by právě hodnota nepohotovosti spínacího relé měla představovat horní mez pravděpodobnosti nebezpečné poruchy jedné sirény varovného systému.
3. Ze dvou prvků třetí kategorie je zásadní příčinou vysoké pravděpodobnosti nebezpečné poruchy klopný obvod spouštění 140 s ostrého poplachu. **Pravděpodobnost poruchy klopného obvodu za dobu prvního roku provozu je $8{,}8.10^{-3}$ a s přibývající dobou dále roste.**

Uvedená skutečnost byla důvodem k tomu, že varovný systém byl považován za nevyhovující a dodavatel varovného systému byl nucen realizovat nápravná opatření ke zvýšení spolehlivosti varovného systému doporučená řešitelem:

- aplikace elektronických součástek se zvýšenou spolehlivostí u prvků, které kritickým způsobem ovlivňují spolehlivost varovného systému,
- změna konstrukce přijímače (společný klopný obvod pro oba signály (test sirén, ostrý poplach),
- softwarová diagnostika prvků klopného obvodu a dalších prvků přijímače.

Po realizaci nápravných opatření byly hodnoty ukazatelů spolehlivosti varovného systému uspokojivé a vyhovovaly stanoveným požadavkům na spolehlivost varovného systému.

2 Ověření spolehlivosti varovného systému

2.1 Vymezení problému

Z analýzy spolehlivosti varovného systému vzešlo doporučení na aplikaci elektronických součástek se zvýšenou spolehlivostí, změnu konstrukce přijímače a softwarovou diagnostiku. Zhotovitel doporučení realizoval a systém instaloval u objednatele. Objednatel odmítl varovný systém převzít do užívání (a zaplatit), protože zhotovitel nebyl schopen hodnověrně doložit, že použil elektronické součástky se zvýšenou spolehlivostí. Proto byl požádán řešitel (zpracovatel analýzy spolehlivosti varovného systému) o nalezení východiska z dané situace.

Spolehlivost zařízení je možno prokazovat dvěma základními způsoby - zkouškami spolehlivosti nebo analýzou spolehlivosti. Oba přístupy je možno kombinovat a jejich použití je ovlivněno řadou faktorů (např. velikostí a strukturální komplikovaností zařízení, počtem zařízení uváděných do provozu nebo již provozovaných, informacemi o vlivu provozního zatížení na poruchovost zařízení apod.). Řešitel proto navrhl k použít prokázání spolehlivosti varovného systému kombinaci obou způsobů v závislosti na druhu funkce varovného systému, která se bude hodnotit.

Zkouška spolehlivosti byla použita k prokázání hodnoty ukazatelů spolehlivosti pro hodnocení funkce individuálních sirén. Spolehlivost této funkce je rozhodující měrou určena spolehlivostí přijímače a sirény. Zkouška byla založena na sledování provozu a poruch, které se u varovného systému vyskytly během zkušebního provozu. Bylo třeba zvolit dostatečně dlouhou dobu zkušebního provozu, aby výsledky zkoušky byly věrohodné. U vysoce spolehlivých systémů, mezi které lze řadit varovný systém, vyžaduje zkouška spolehlivosti velmi dlouhou dobu zkušebního provozu. Pro hodnocení funkce individuálních sirén byla navržena vzhledem k počtu sirén (doba zkušebního provozu v délce 10 měsíců

K prokázání spolehlivosti funkce "varovný signál od skupiny sirén jedné sekce varovného systému " a funkce "varovný signál od všech sirén varovného systému" by doba zkušebního provozu byla neúměrně dlouhá. Velikost hodnoceného souboru je malá (16 sekcí a 1

systém) a potřebná délka doby zkušebního provozu výrazně roste (řádově roky). Ve spolehlivosti funkce skupiny sirén jedné sekce a všech sirén systému se však poruchy přijímačů a sirén uplatňují jen minimálně a v ostatních částech systému nebylo použití elektronických součástek se zvýšenou spolehlivostí předepsáno. Proto k prokázání spolehlivosti funkce skupiny sirén jedné sekce a od všech sirén systému vnitřního varování byly proto použity hodnoty ukazatelů spolehlivosti stanovené analýzou spolehlivosti.

2.2 Zkušební provoz

Jako zkušební provoz bylo využito období 10 měsíců, kdy byl varovný systém instalován, oživen, vyzkoušen a objednatelem protokolárně uznán za plně funkční. Stav systému v období zkušebního provozu byl pravidelně vyhodnocován a autodiagnostikou evidované poruchy prvků systému opravovány. Pro zjištění stavu prvků nesledovaných autodiagnostikou (spínací relé sirény, siréna) byl prováděn opakovaný test sirén.

Příklady záznamů o poruchách, které se vyskytly u varovného systému v jednotlivých obdobích zkušebního provozu a při zkouškách sirén, jsou uvedeny v tab. 4 a tab. 5.

Tab. 4: Stav přijímačů sirén dle výpisu z archivu poruch (zjištěno autodiagnostikou při běžném režimu)

Přijímač	**Text poruchy**	**Příčina poruchy**	**Vliv na bezpečnou poruchu**	**Vliv na nebezpečnou poruchu**
AY9160	siréna nepřítomna	chybějící pojistky u linek sirén	ne	Ano
AY9164	neodpovídá	vadný kontakt v komunikační lince 1 - nedotažená svorka	ne	Ano
AY7149	neodpovídá	výpadek adresy přijímače - vadná EPROM	ne	Ano
AY7117	siréna nepřítomna	zkrat na hlídači vedení	ne	Ano
AY7127	napájení mimo meze	přijímač nedobíjí baterii - vadná Zenerenova dioda	ne	Ne
AY7129	napájení mimo meze	přijímač nedobíjí baterii - vadný tranzistor	ne	Ne
AY7131	napájení mimo meze	nízké napětí 12 V baterie - výměna baterie	ne	Ne
AY4107	siréna nepřítomna	chybně nastaven jumper na hlídači vedení	ne	Ne
AY0181	siréna nepřítomna	zemní spoj na krytu sirény	ne	Ne
AY0180	siréna nepřítomna	ulomený spoj na přívodu hlídače vedení	ne	Ano
AY9139	neodpovídá	přerušená pojistka zdroje	ne	Ne
AY9154	siréna nepřítomna	poškozen jumper hlídače vedení	ne	Ne
AY9165	neodpovídá	po havárii technologie zaplaveno vodou	nehodn.	Nehodn.

Tab. 5: Stav přijímačů sirén dle výpisu z archivu poruch (zjištěno autodiagnostikou při zkoušce sirén)

Přijímač	Text poruchy	Příčina poruchy	Vliv na bezpečnou poruchu	Vliv na nebezpečnou poruchu
AY1170	siréna nepřítomna	pojistka	ne	Ano
AY3140	siréna nepřítomna	vadný hlídač vedení	ne	Ano
AY0180	siréna nepřítomna	vadný hlídač vedení	ne	Ano
AY9168	siréna nepřítomna	pojistka	ne	Ano

2.3 Dosažené hodnoty ukazatelů spolehlivosti

Při vyhodnocení zkušebního provozu varovného systému se vycházelo z velikosti sledovaného souboru (počtu sirén) a doby zkušebního provozu. Protože byla hodnocena funkce individuálních sirén varovného systému byla velikost souboru dána počtem sirén instalovaných v systému. Doba zkušebního provozu byla stanovena v délce t = 7552 h.

Hodnoty pro bezpečnou poruchu

Při výpočtu ukazatelů spolehlivosti pro bezpečnou poruchu systému vnitřního varování bylo použito postupů uvedených v **ČSN IEC 605-4 Zkoušky bezporuchovosti zařízení. Část 4: Postupy pro stanovení bodových odhadů a konfidenčních mezí z určovacích zkoušek bezporuchovosti zařízení**. Protože varovný systém je z valné části tvořen elektronickými prvky, byl přijat předpoklad, že intenzita poruch prvků je konstantní. Protože zkušební provoz systému vnitřního varování představuje zkoušku ukončenou časem, je bodový odhad intenzity poruch proveden podle čl. 5.1.1 normy. Bodový odhad (pozorovaná hodnota) intenzity poruch je dán vztahem

$$\hat{\lambda} = \frac{r}{T^*}$$

kde **r** je počet poruch a **T*** je kumulovaná platná doba zkoušky. V tomto případě **T*** je skutečná kumulovaná doba provozuschopného stavu sirén $\mathbf{T^* = T = 1{,}08.10^6\ h}$. Protože během zkoušky nebyly pozorovány žádné bezpečné poruchy systému (falešné signály sirén a majáků) doporučuje se při **r = 0** pro bodový odhad intenzity poruch v čl. 5.1.1 normy vztah

$$\hat{\lambda} = \frac{1}{3T^*} = \frac{1}{3.1{,}08.10^6\ h} = 3{,}1.10^{-7}\ h^{-1}$$

Z uvedeného vztahu plyne bodový odhad střední doby mezi poruchami

$$\hat{T}_{stř} = 3T^* = 3.1{,}08.10^6\ h = 3{,}2.10^6\ h$$

Není-li pozorována žádná porucha, může se stanovit pouze jednostranný konfidenční interval (90%) s horní mezí podle čl. 5.1.2 normy

$$\lambda < 2.10^{-6}\ h^{-1}$$
$$T_{stř} > 5.10^5\ h$$

Hodnoty pro nebezpečnou poruchu

Při výpočtu hodnot ukazatelů spolehlivosti pro nebezpečnou poruchu varovného systému není možno aplikovat postupy uvedené v **ČSN IEC 1070 Postupy ověřovacích zkoušek pro součinitele ustálené pohotovosti** protože hodnocený objekt je posuzován jako třístavový (bezporuchový stav, stav bezpečné poruchy a stav nebezpečné poruchy). Proto byly hodnoty ukazatelů spolehlivosti (pohotovost, resp. nepohotovost) vypočítány ze střední doby

provozu mezi poruchami (vyhodnocené dle ČSN IEC 605-4) pro nebezpečnou poruchu a doby uvažované pro obnovu provozuschopnosti v analýze spolehlivosti. Při výpočtu hodnot ukazatelů spolehlivosti byly zváženy tyto skutečnosti:

- všechny poruchy zaznamenané ve výpisech z archivu poruch byly zjištěny autodiagnostikou systému. Odstranit tyto poruchy bylo možné v průměru za 24 h od doby jejich zjištění,
- poruchy vzniklé při zkoušce sirén se vyskytly u diagnostikovaných prvků a bylo je možné odstranit do 24 h,
- při zkoušce sirén nebyl zaznamenán žádný případ poruchy nediagnostikovaného prvku (spínací relé sirény, siréna apod.),
- z výpisu z archivu poruch byly uvažovány pouze poruchy, které znemožnily vykonat bezpečnostní funkci (vydat varovný signál),
- nebyly uvažovány poruchy zaviněné špatnou montáží (nedotažené svorky, ulomený spoj, chybějící pojistky), neboť se nejedná o náhodné poruchy prvků. Po odstranění se tyto poruchy již neobjevují.

Skutečná kumulovaná doba provozuschopného stavu sirén je shodná s hodnotou použitou při výpočtu ukazatelů spolehlivosti pro bezpečnou poruchu, tj. $\mathbf{T^* = 1{,}08.10^6\ h}$. Počet nebezpečných poruch odvozený z poruch prvků je **r = 17**. Při předpokladu konstantní intenzity poruch je bodový odhad intenzity poruch podle čl. 5.1.1 ČSN IEC 605-4

$$\hat{\lambda} = \frac{r}{T^*} = \frac{17}{1{,}08.10^6\ h} = 1{,}6.10^{-5}\ h^{-1}$$

a bodový odhad střední doby mezi poruchami

$$\hat{T}_{stř} = \frac{T^*}{r} = \frac{1{,}08.10^6\ h}{17} = 6{,}4.10^4\ h$$

Dvoustranný konfidenční interval (90%) podle čl. 5.1.2 ČSN IEC 605-4

$$1.10^{-5}\ h^{-1} < \lambda < 2{,}4.10^{-5}\ h^{-1}$$

Při předpokladu konstantní intenzity poruch platí, že $T_{stř} = 1/\lambda$ a dvoustranný konfidenční interval (95%) pro $T_{stř}$ má hodnotu

$$1.10^5\ h > T_{stř} > 4{,}2.10^4\ h$$

Při uvažované době obnovení provozuschopného stavu $\mathbf{T_o = 24\ h}$ platí, že $\mathbf{T_o << T_{stř}}$, proto lze bodový odhad součinitele nepohotovosti vyjádřit vztahem

$$\hat{U} = \frac{T_o}{\hat{T}_{stř}} = \frac{24\ h}{6{,}4.10^4\ h} = 3{,}8.10^{-4}$$

Při uvažování dvoustranného konfidenční intervalu pro $T_{stř}$, lze stanovit hodnotu součinitele nepohotovosti

$$2{,}4.10^{-4} > U > 5{,}7.10^{-4}$$

Na základě provedeného hodnocení bylo konstatováno, že varovný systém splňuje v plném rozsahu požadavky kladené objednatelem na jeho spolehlivost a systém lze převzít do plného provozu.