ČESKÁ SPOLEČNOST PRO JAKOST

Novotného lávka 5, 116 68 Praha 1

60. SEMINÁŘ
ODBORNÉ SKUPINY PRO SPOLEHLIVOST

pořádaný výborem Odborné skupiny pro spolehlivost
k problematice

PREDIKTIVNÍ ANALÝZY SPOLEHLIVOSTI A MOŽNOSTI JEJICH VYUŽITÍ

Materiály z 60. semináře
odborné skupiny pro spolehlivost

Brno, červen 2015

Odborný garant semináře: doc. Ing. David Vališ, Ph.D.

OBSAH:

Sborník přednášek: **Prediktivní analýzy spolehlivosti a možnosti jejich využití**
Vydání 1., Česká společnost pro jakost
Brož
ISBN: 978-80-7231-965-7
Kolektiv autorů
47 stran

ÚVOD DO PREDIKTIVNÍCH ANALÝZ SPOLEHLIVOSTI – ÚČEL A ZÁKLADNÍ CHARAKTERISTIKY

prof. Ing. Zdeněk VINTR, CSc., dr.h.c.
e-mail: zdenek.vintr@unob.cz

pplk. doc. Ing. David VALIŠ, Ph.D.
e-mail: david.valis@unob.cz

1. Úvod

Cílem příspěvku je seznámit čtenáře se základy a úvodními principy metod prediktivních analýz spolehlivosti. Prediktivní analýzy spolehlivosti se používají k přezkoumání a předpovědi ukazatelů bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti systému. Analýzy spolehlivosti se provádí zejména v etapě volby koncepce a stanovení požadavků, v etapě návrhu a vývoje a v etapě provozu a údržby a to především pro vyhodnocení a stanovení ukazatelů spolehlivosti a pro posouzení zda byly splněny specifikované požadavky.

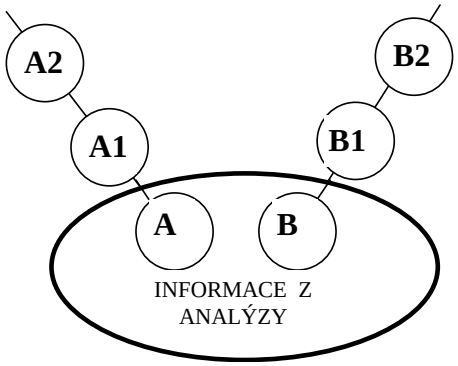
2. Cíle prediktivní analýzy spolehlivosti systému

Analýza spolehlivosti systému je proces, jehož podstatou je získávání, zkoumání a uspořádávání informací specifických a významných pro daný systém a potřebných pro rozhodování o něm a o stanovených cílech. Zkoumání probíhá obvykle na modelu systému. Konečným produktem tohoto procesu je soubor informací o vlastnostech modelu systému. Model může být v průběhu analýzy modifikován. V souladu s touto definicí je primárním cílem analýzy systému získávání informací o něm. Analýza musí být provedena podle jasně stanovených pravidel a postupů, tak aby proces analýzy byl opakovatelný a vždy vedl ke stejným výsledkům (dvě nezávisle provedené analýzy jednoho systémů nemůžou dospět ke vzájemně rozporným výsledkům.

Informace, které jsme schopni z analýzy získat, nemusí být na první pohled a na jejím začátku zcela zřejmé. Vysvětlení poskytuje Obrázek 1.1. Kruh představuje informace, které musí být získány proto, aby analýza systému splnila svůj účel. Analytik, který se zaměřuje na typ problémů A začíná svůj výzkum v této oblasti a vyřešení řady problémů které ho zajímají, jej může dovést do oblasti A1; objasnění těchto problémů jej může dále přivést do oblasti A2; atd. Jiný analytik, zaměřený na skupinu problémů B může obdobně dospět k oblastem B1, B2 atd.

Pro ilustraci problému uvažujme např. elektronický bezpečnostní systém ochrany důležitého průmyslového podniku. Analytik začíná výzkum jeho spolehlivosti identifikací a popisem rozhraní systému, možných příčin a důsledků poruch jeho externího napájecího systému, rozborem poruch vlastního napájecího systému, pokračuje rozborem příčin a důsledků poruch interní elektrické instalace a nakonec jednotlivých výkonných prvků

bezpečnostního systému. Uvážit musí vazby mezi prvky a důsledky kombinace poruch jednotlivých prvků na výslednou spolehlivost systému ve všech předpověditelných režimech provozu.



Obrázek 1.1 Oblasti informací, získávaných analýzou spolehlivosti.

3. Metodologické přístupy k analýze

Existují dva rozdílné metodologické postupy při provádění analýzy spolehlivosti systému: induktivní a deduktivní.

Induktivní postup: je založen na provádění analýzy od specifických a elementárních problémů k obecnějším a globálnějším problémům. Od analýzy funkcí a poruch prvků (a jejich kombinací) na nejnižší úrovni členění systému se postupuje k analýze poruch a jejich důsledků na nadřazené systémy až k poruchám celého systému. Tento postup se uplatňuje například v metodě FMEA, kde se posuzují důsledky poruch prvků na funkci nadřazených systémů. Při zkoumání důsledků poruch se tedy uplatňuje induktivní postup.

Deduktivní postup: je založen na provádění analýzy od globálních (obecných) problémů k problémům elementárním. Od analýzy poruch systému na nejvyšší úrovni členění se postupuje k analýze jejich příčin a podílu poruch elementárních prvků na těchto poruchách. Při zkoumání příčin vzniku poruch se tedy uplatňuje deduktivní postup. Tento postup se uplatňuje například v metodě stromu poruch.

4. Základní metody analýzy spolehlivosti

Tak jak se vyvíjela spolehlivost jako vědní obor, rozvíjely se i metody analýzy spolehlivosti. Dnes jsou nejvýznamnější metody analýzy spolehlivosti již standardizovány a návody k jejich použití jsou k dispozici ve formě národních, mezinárodní či vojenských norem. V současné praxi se při provádění analýz spolehlivosti můžeme setkat zejména s následujícími metodami:

- Předběžná analýza nebezpečí (PHA).
- Analýza způsobů a důsledků poruch (FMEA).
- Analýza způsobů, důsledků a kritičnosti poruch (FMECA).
- Metoda grafů a blokových diagramů bezporuchovosti (RBD).

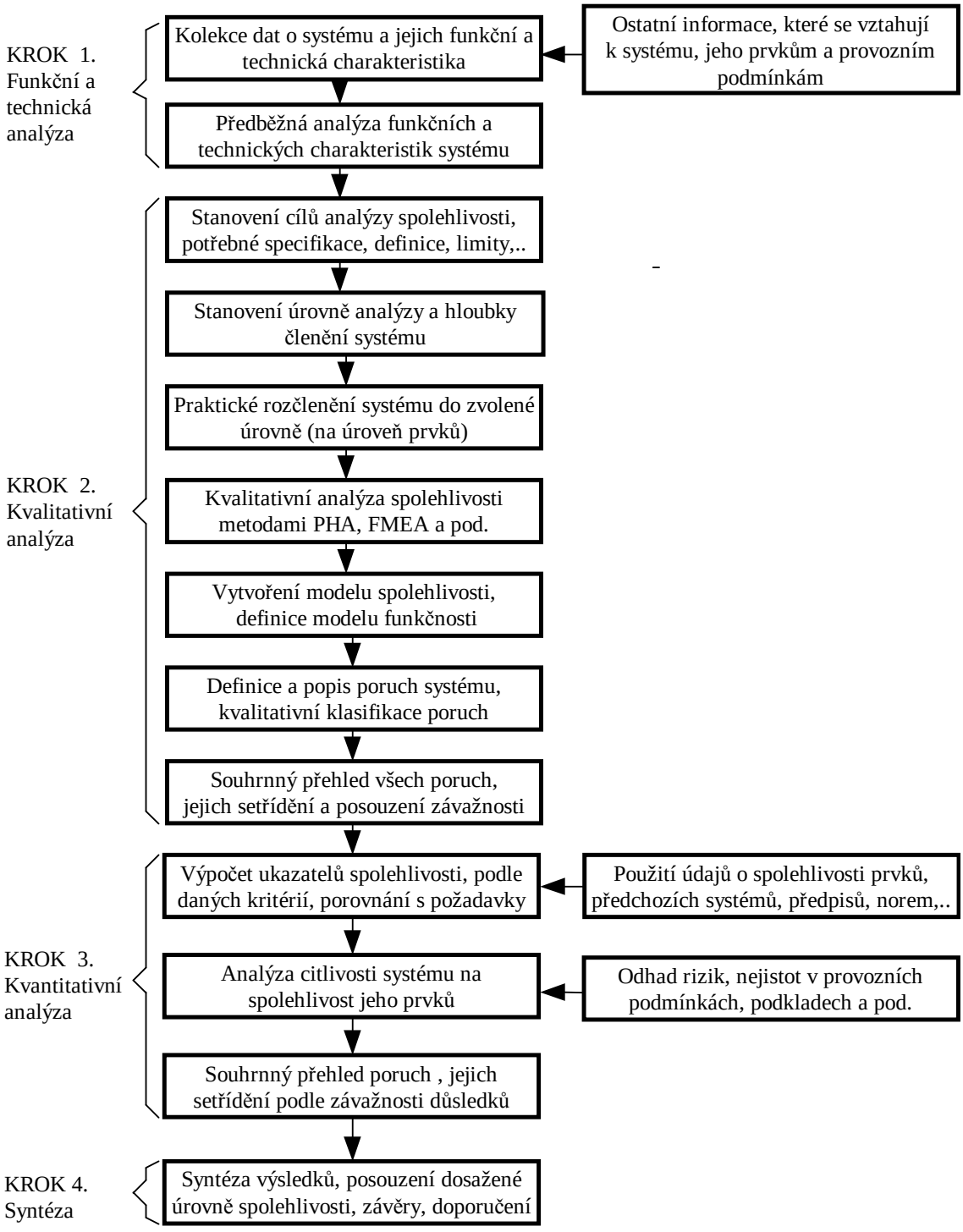
- Metoda pravdivostní tabulky.
- Metoda orientovaných stromů událostí (FTA, ETA, aj.).
- Markovovy metody (MA).
- Simulační metody.

5. Hlavní kroky a charakteristiky prediktivní analýzy

V principu existují čtyři hlavní kroky (etapy) při provádění prediktivní analýzy spolehlivosti a to:

- Funkční a technická analýza.
- Kvalitativní analýza.
- Kvantitativní analýza.
- Syntéza výsledků analýzy.

Vzájemná návaznost těchto etap a přehled základních úkolů, které jsou v rámci každé etapy realizovány je znázorněn na Obr. 1.2.

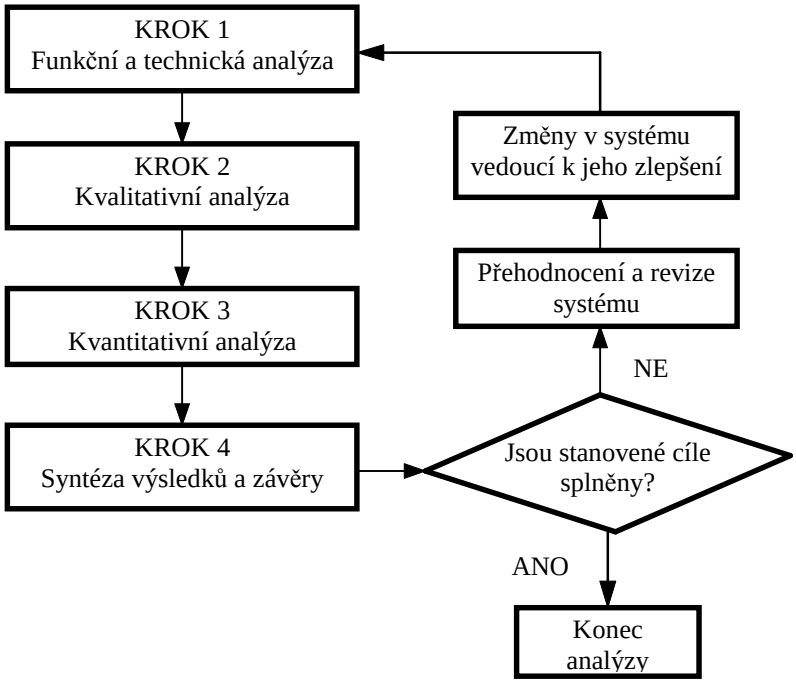


Obrázek 1.2 Prediktivní analýza spolehlivosti systému

Mezi hlavní charakteristiky prediktivních analýz patří:

Interaktivní povaha analýzy: Pro snadnější pochopení podstaty a cílů analýzy spolehlivosti byl postup jejího provádění rozdělen do čtyř samostatných a relativně nezávislých kroků. Ve skutečnosti ovšem toto dělení a nezávislost kroků nemá ostré hranice. Pro každý reálný systém, který má být definován, vyvinut a vyroben mají jednotlivé etapy, jimiž jeho vznik prochází v prováděných činnostech vzájemné průniky.

Iterativní povaha analýzy: Ze své povahy má analýza spolehlivosti iterativní charakter. Je integrální součástí všech vývojových prací na systému, přináší náměty a návrhy na změny systému, které jsou důsledkem odhalených nedostatků. První závěry z analýzy vedou ke změnám v systému a ke zvýšení jeho spolehlivosti. Vliv těchto změn a modifikací vyvolává potřebu opakování (aktualizaci) analýzy až do té doby, dokud nejsou splněny na začátku projekčních prací stanovené cíle. Iterativní aspekty, obsažené v analýze spolehlivosti ukazuje Obrázek 1.3.



Obrázek 1.3 Iterativní povaha analýzy spolehlivosti

6. Závěr

Kvalitativní modelování, které je implicitní součástí analýzy má v sobě i kvantitativní aspekty. Identifikace a definice možných poruch, jejich projevů, důsledků a rizika jejich vzniku mají vždy stochastickou povahu a nesou v sobě i jistou chybu v odhadu. Proto vždy můžeme v analýze pouze předpokládat vznik poruch a jejich důsledků a to obvykle na základě zkušeností získaných empiricky z provozu stejných nebo příbuzných systémů.

Syntéza informací a závěry z kvalitativní a kvantitativní analýzy např. přesně ukáže ty poruchy a jejich kombinace, na nichž je nejvíce závislá spolehlivost systému, odhalí nejkritičtější prvky systému nebo nejvýznamnější funkce systému. Tímto způsobem lze rozhodnout o takových technických či technologických opatřeních, která nejúčinnějším a nejrychlejším způsobem povedou ke zvýšení spolehlivosti, konkrétně bezporuchovosti, bezpečnosti, pohotovosti, udržovatelnosti a jiných vlastností systému. Ze závěrů analýzy je možné usoudit, zda systém splnil nebo nesplnil požadavky na jeho spolehlivost a bezpečnost. Stejně tak analýza může posloužit i k jiným praktickým krokům:

- ke zvýšení úrovně spolehlivosti prvků;
- ve změnách v zálohování prvků;

- ke zdůvodnění nezbytnosti dodatečného zálohování prvků;
- k odstranění nadbytečného zálohování;
- k dodatečné ochraně nebo monitorování funkcí prvků;
- k nezbytnosti zabudování ochrany systému před poruchou společných prvků;
- k nezbytnosti předepsat kontrolu správné funkce prvků se skrytými poruchami;
- k úpravě preventivních údržbových operací;
- ke změnám charakteru a period kontrolních zkoušek;
- k minimalizaci rizika vlivu lidského faktoru na spolehlivou funkci systému apod.

Analýza poskytuje celou řadu dalších užitečných informací, využitelných při organizaci, řízení a kontrole provozu. Dává též první podklady pro objektivní plánování systému logistické podpory budoucího provozu.

Použité zdroje

[1] DHILLON, B. S. *Design reliability: Fundamentals and applications.* Boca Raton: CRC Press, 1999. ISBN 0-8493-1465-8.

[2] HOLUB, R. – VINTR, Z. *Spolehlivost letadlové techniky* [Elektronická učebnice]. Brno: VUT v Brně, 2001.

[3] HOLUB, R. – VINTR, Z. *Základy spolehlivosti*. Brno: VA v Brně, 2002.

[4] MATĚJČEK, J. Stručný přehled norem z oblasti spolehlivosti. In *Úvod do spolehlivosti.* Praha: Česká společnost pro jakost, 2014, s. 18–26. ISBN 978-80-02-02514-6.

[5] MURTHY, D.N.P. – RAUSAND, M. – ØSTERÅS, T. *Product reliability: Specification and performance.* London: Springer-Verlag, 2008. ISBN 978-1-84800-270-8.

[6] MYKISKA, A. Systém managementu spolehlivosti. In *Normy z oblasti managementu spolehlivosti a rizik.* Praha: Česká společnost pro jakost, 2006, s. 11–18.

[7] VINTR, M. Oborové normy ve spolehlivosti. In *Mezinárodní a národní normalizace ve spolehlivosti.* Praha: Česká společnost pro jakost, 2012, s. 29–36. ISBN 978-80-02-02421-7.

[8] ČSN IEC 60050/192. Mezinárodní elektrotechnický slovník – Část 192: Spolehlivost. Praha: UNMZ, 2015.

[9] ČSN EN ISO 9000:2006. *Systémy managementu kvality – Základy, zásady a slovník.* Praha: ČNI, 2006.

[10] ČSN EN ISO 9001:2009. *Systémy managementu kvality – Požadavky.* Praha: ÚNMZ, 2009.

[11] ČSN EN 60300-1. *Management spolehlivosti – Část 1: Systémy managementu spolehlivosti.* Praha: ČNI, 2004.

[12] ČSN EN 60300-2. *Management spolehlivosti – Část 2: Směrnice pro management spolehlivosti.* Praha: ČNI, 2005.

[13] IEC 60300-1/Ed3. *Dependability management – Part 1: Guidance for management and application (Final draft – 56/1550/FDIS)*. Geneva: International Electrotechnical Commission, 2014.

[14] MIL-STD-785B. Reliability Progam for Systems and Equipment Development and Production. Washington: Department of Defense, 1980.

[15] NASA-STD-8729.1. *Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program.* Washington: NASA, 1998.

[16] SAE JA1000. *Reliability Program Standard.* Warrendale: Society of Automotive Engineers, 1998.

[17] SAE JA1000/1. *Reliability Program Standard Implementation Guide.* Warrendale: Society of Automotive Engineers, 1999.

[18] SAE JA1010. *Maintainability Program Standard.* Warrendale: Society of Automotive Engineers, 2011.

[19] SAE JA1010/1. *Maintainability Program Standard Implementation Guide.* Warrendale: Society of Automotive Engineers, 2011.

[20] VDA 3.1. *Zabezpečení spolehlivosti u výrobců automobilů a dodavatelů.* Praha: Česká společnost pro jakost, 2002.

POSTUP ANALÝZY ZPŮSOBŮ, DŮSLEDKŮ A KRITIČNOSTI PORUCH – FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS (FME(C)A)

Ing. Michal VINTR, Ph.D.
Expert na spolehlivost a bezpečnost produktů
e-mail: mvintr@mvintr.cz

Ing. Lenka VINTROVÁ
Honeywell – HTS CZ

1. Úvod

Cílem příspěvku je seznámit čtenáře s metodu FME(C)A. V příspěvku je stručně popsána metoda FME(C)A, její historie, normy a návody pro její provádění. V příspěvku je dále uveden seznam zdrojů s informacemi o analýze a výčet rozšířených softwarových produktů pro podporu provádění analýzy. Hlavní část příspěvku je věnována postupu provádění analýzy. Dále je v příspěvku popsáno, které informace je třeba před započetím analýzy získat a které během analýzy zaznamenávat.

FME(C)A je jednou z nejčastěji používaných metod pro analýzu spolehlivosti a bezpečnosti technických systémů. V mnoha případech není analýza prováděna samostatně, ale je součástí celého souboru analýz spolehlivosti a bezpečnosti, z nichž některé jsou popsány v ostatních příspěvcích v tomto sborníku.

2. Zkratky FMEA a FMECA

V normách, literatuře a praxi se lze setkat s používáním následujících dvou zkratek, které vychází z anglických názvů:

- FMEA – Failure Modes and Effects Analysis;
- FMECA – Failure Modes, Effects and Criticality Analysis.

Ve většině cizích jazyků se používají zkratky FMEA a FMECA. Výjimkou je francouzština, která používá zkratky francouzských názvů:

- AMDE – Analyse des modes de défaillance et de leurs effets;
- AMDEC – Analyse des modes de défaillance, de leurs effets et de leur criticité.

Dle platné normy ČSN EN 60812 [7] jsou tyto názvy překládány jako:

- Analýza způsobů a důsledků poruch;
- Analýza způsobů, důsledků a kritičnosti poruch.

Je však možno se setkat i s jinými pojmenováními, např.: Analýza druhů poruchových stavů a jejich důsledků nebo Analýza možností vad a jejich následků.

3. Historie a standardizace FME(C)A

Metoda FME(C)A byla vytvořena v 50. letech 20. století Armádou Spojených Států Amerických. Ta v roce 1949 vydala první armádní proceduru pro použití metody:

- *MIL-P-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis.*

Metoda byla v počátcích používána zejména v oblasti letectví a ozbrojených sil jako nástroj umožňující určovat důsledky poruch systémů a jejich komponent.

K výraznému rozšíření metody FME(C)A došlo v 60. letech minulého století v souvislosti s potřebou zabezpečovat spolehlivost nových technických systémů, které se vyznačovaly značnou složitostí a jejichž selhání mohlo vést ke katastrofickým důsledkům značného rozsahu. Jednou z prvních známých aplikací metody FMECA bylo její použití v agentuře NASA při realizaci projektu APOLLO. Metoda se osvědčila a její použití se rychle rozšířilo do celé řady dalších oborů lidské činnosti. Jako výsledek vývoje byl Armádou USA v roce 1974 poprvé vydán vojenský standard:

- *MIL-STD-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis*,

který zobecnil získané zkušenosti a zformuloval základní zásady pro provádění a použití metody. Poslední verze normy pochází z roku 1980 [11].

Metoda nezůstala stranou zájmu mezinárodních standardizačních organizací. V roce 1985 Mezinárodní elektrotechnická komise IEC vydala normu *IEC 812 Procedure for Failure Mode and Effects Analysis*, která byla v roce 1992 zavedena také v ČR jako ČSN IEC 812. V současné době je platná aktualizovaná verze normy:

- *ČSN EN 60812 Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA),*

která byla vydána v roce 2007 [7].

V současné době IEC pracuje na vydání již 3. edice normy IEC 60812. V době vydání příspěvku se příprava nacházela v etapě návrhů komise a byl vydán „Committee draft“ [9].

Metoda se také rozšířila v oblasti automobilového průmyslu. V roce 1994 byla v USA Sdružením pro automobilní inženýrství SAE poprvé vydána norma SAE J1739. V současné době je platná revize z roku 2009:

- *SAE J1739 Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)* [14].

Norma je určena pro použití zejména v automobilovém průmyslu. SAE také vydalo v roce 2001 normu:

- *SAE ARP5580 Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications* [13],

která je určena pro použití mimo oblast automobilového průmyslu.

Metoda nezůstala stranou pozornosti ani Sdružení automobilového průmyslu VDA, které v roce vydalo normu:

- *VDA 4 Zajišťování kvality před sériovou výrobou, kapitola: FMEA produktu a procesu*.

Norma byla naposledy vydána v roce 2012 také v českém jazyce [15].

V USA je automobilovém průmyslu také používána norma vydaná organizací AIAG:

- *AIAG FMEA-4 – Potential Failure Mode & Effects Analysis.*

V oblasti leteckého a kosmického průmyslu bylo vydáno několik norem definujících pravidla pro provádění analýzy FME(C)A:

- *SAE ARP4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* [12]*;*
- *ANSI/AIAA S-102.2.4-2009. Performance-Based Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements* [6]*;*
- *ECSS-Q-ST-30-02C. Space Product Assurance – Failure Modes, Effects (and Criticality) Analysis (FMEA/FMECA)* [8].

Přičemž použití normy SAE ARP4761 při analýzách spolehlivosti a bezpečnosti je doporučeno leteckými předpisy.

4. Volně dostupné zdroje informací o analýze

Informace, doporučení a příklady provádění analýzy FME(C)A lze nalézt také na internetu, přičemž informace jsou často volně (bezplatně) dostupné.

V českém jazyce jsou kvalitním informačním zdrojem sborníky ze seminářů Odborné skupiny pro spolehlivost zaměřené na analýzy spolehlivosti a metodu FME(C)A, např.:

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

Sborníky jsou dostupné na webových stránkách: http://www.csq.cz/spolehlivost/

V anglickém jazyce lze na internetu nalézt nespočet webových stránek s informacemi o metodě FME(C)A. Uveďme tři nejpřínosnější z pohledu autorů příspěvku:

- FMEA and FMECA Information: http://www.fmea-fmeca.com/
- FMEA Info Centre: http://www.fmeainfocentre.com/
- Effective FMEAs: http://www.effectivefmeas.com/

5. Softwarová podpora analýzy

V současné době je na trhu relativně velké množství softwarových produktů zaměřených na analýzu FME(C)A. Jedná se zejména o produkty od renomovaných producentů software zaměřených na podporu spolehlivosti a bezpečnosti systémů. Mezi rozšířené softwarové produkty patří zejména následující:

- Modul FMEA a FMECA software Reliability Workbench od producenta Isograph;
- Windchill FMEA od producenta PTC (dříve Relex);

- Xfmea od producenta Reliasoft;
- FMECA modul software ITEM ToolKit od producenta ITEM Software;
- Moduly FMEA a FMECA software RAM Commander od producenta ALD;
- ASENT od producenta Raytheon.

Většina producentů dodává software pro FME(C)A samostatně. Často je software pro FME(C)A začleněn (nebo může být začleněn) do kompletního balíku software pro podporu spolehlivosti a bezpečnosti. Tím je umožněno provázat FME(C)A s dalšími analýzami, jako jsou např. analýza blokového diagramu bezporuchovosti (RBD), analýza stromu poruchových stavů (FTA) a analýza stromu událostí (ETA).

6. Charakteristika a oblasti použití analýzy

Metoda FMEA je strukturovaná, kvalitativní analýza sloužící k identifikaci způsobů poruch systémů, jejich příčin a důsledků. Metoda FMECA je logickým rozšířením metody FMEA spočívajícím v tom, že jsou do ní zahrnuty prostředky pro klasifikaci závažnosti způsobů poruch.

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

Metoda FMEA je dle způsobu použití nejčastěji rozdělována na:

- konstrukční FMEA (Design FMEA), někdy také nazývána FMEA návrhu, která se používá pro potřeby analýzy produktu, respektive technického návrhu produktu;
- procesní FMEA (Process FMEA), která se používá pro potřeby analýzy procesu;

V dostupných zdrojích se lze setkat i s dalšími způsoby použití analýzy, např.:

- systémová FMEA (System FMEA), někdy také nazývána funkční FMEA (Functional FMEA, která se používá pro analýzu funkcí na úrovni systému;
- FMEA konceptu (Concept FMEA), která se používá v prvotní etapě životního cyklu produktu pro analýzu jeho konceptu.

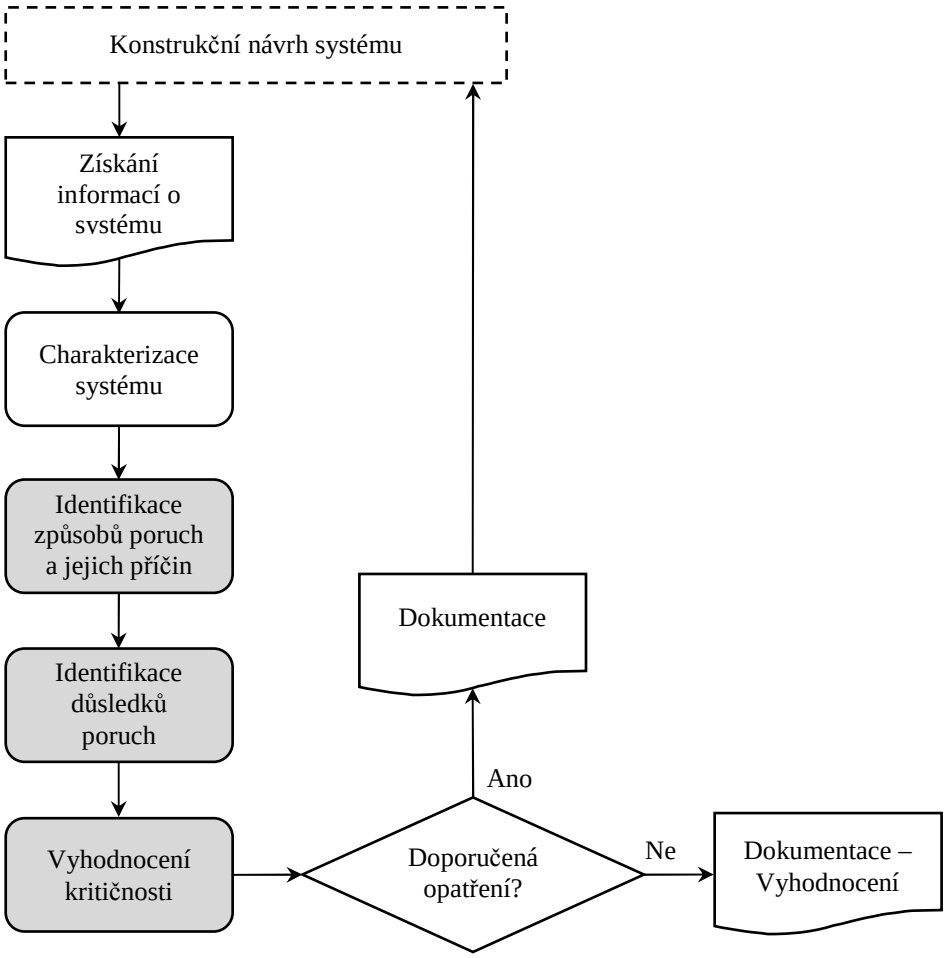
Tento příspěvek je primárně zaměřen na FMEA konstrukční.

7. Postup provádění analýzy

Postup provádění konstrukční FME(C)A lze rozdělit do tří základních částí:

- přípravná část;
- vlastní FME(C)A jednotlivých komponent systému;
- vyhodnocení analýzy.

Zjednodušený postup provádění analýzy FMECA je graficky znázorněn na obrázku 2.1. Jednotlivé kroky postupu jsou podrobně popsány v následujících podkapitolách.



Obrázek 2.1 – Postup analýzy FMECA

7.1 Přípravná část

Obsahem této části je shromáždění informací a podkladů potřebných pro provedení vlastní analýzy. K základním informacím, které jsou k provedení analýzy nezbytné, patří zejména:

- Účel a cíle analýzy.
- Termíny provedení analýzy.
- Požadovaná hloubka analýzy.
- Požadavky na spolehlivost a bezpečnost systému (technické a legislativní požadavky).
- Informace o struktuře a funkcích systému.
- Informace o provozních podmínkách (specifikace podmínek provozu, dob a fází provozu).
- Informace o systému údržby (systém preventivní a nápravné údržby).
- Informace o podmínkách prostředí.
- Požadavky na využití softwarové podpory.

Účel a cíle analýzy

Musí být přesně vymezeno, k jakému účelu je analýza prováděna. Například se analýza provádí proto, aby:

- Bylo možné prokázat, že systém splňuje požadavky na spolehlivost a bezpečnost.
- Byly vyspecifikovány kritické komponenty systému z hlediska nepříznivých důsledků jejich poruchy pro plnění základních funkcí systému.
- Poskytla vstupní informace pro návrh optimálního systému technické údržby a diagnostiky systému.

Požadovaná hloubka analýzy

Je nezbytné stanovení nejnižší úrovně, která je předmětem analýzy. Všechny komponenty na této úrovni jsou potom pro potřeby analýzy považovány za dále nedělitelné prvky, které plní jasně definované funkce a mají jednoznačně vymezené způsoby poruch. Při volbě nejnižší úrovně analýzy je třeba brát v úvahu zejména:

- stanovený účel a cíle analýzy;
- složitost analyzovaného systému;
- úroveň znalostí o funkcích a způsobech poruch (případně intenzitách poruch) systému na jednotlivých úrovních struktury systému;
- specifikovanou nebo zamýšlenou úroveň nápravné a preventivní údržby;
- možnosti symbolického znázornění (modelování) funkcí systému na jednotlivých úrovních jeho struktury;
- možnosti software použitého pro analýzu.

Obecně lze říci, že nejnižší úroveň analýzy musí být zvolena tak, aby na ní bylo možno věrohodně identifikovat funkce jednotlivých prvků, způsoby jejich selhání a v případě kvantitativního hodnocení i stanovit hodnoty intenzity poruch těchto prvků. Z tohoto pohledu může v rámci jednoho analyzovaného systému prvek představovat jak jednotlivou součást, tak i složitý subsystém. Při analýze je potom každý prvek na zvolené úrovni analýzy považován za tzv. „černou skříňku“, jejíž vnitřní struktura a funkce již nejsou předmětem analýzy.

Informace o struktuře a funkcích systému

Musí být k dispozici slovní popisy konstrukčního uspořádání a použitého technologického řešení systému, doplněné o podrobnou výkresovou dokumentaci, schémata, grafy apod.

K dispozici musí být také podrobný výčet všech důležitých funkcí systému a komponent, které musí plnit a které musí být podrobeny analýze. Funkce musí být definovány tak, aby bylo možné studovat (modelovat) jejich vzájemné souvislosti, podmíněnost, posloupnost, vazby na provozní podmínky systému. Z definice musí být možné odvodit závažnost důsledků jejich neplnění, možnosti vzájemné oddělitelnosti jednotlivých funkcí apod.

V návaznosti na funkce systému musí být definováno funkční členění systému, které specifikuje, do jakých funkčních subsystémů se systém člení a to až do požadované hloubky analýzy. Funkční členění může být shodné nebo podobné konstrukčnímu členění, ale není to

pravidlem. Funkční a konstrukční členění systému je nutné odlišovat, protože produkt jednoho konstrukčního typu může plnit celou řadu odlišných funkcí a tomu musí být přizpůsobeno i odpovídající funkční členění.

Musí být přesně definováno rozhraní systému, které vymezuje hraniční body a komponenty, kde dochází ke vzájemné interakci s okolními systémy nebo s vnějším okolím systému. V nich potom musí být vymezeny okrajové podmínky pro analýzu systému. Definice rozhraní má za cíl vyloučit průniky více systémů tak, aby se stejné analyzované funkce, poruchy apod. neopakovaly vícekrát v různých systémech.

O všech komponentech systému, až do zvolené úrovně, která je určena požadovanou hloubkou analýzy, musí být k dispozici alespoň následující informace:

- jednoznačná identifikace komponent – mohou to být například čísla výkresů, katalogová čísla, čísla prvků na schématech a výkresech apod.;
- popis funkcí komponent;
- popis možných způsobů poruch komponent;
- popis důsledků poruch komponent;
- intenzity (pravděpodobnosti) jednotlivých způsobů poruch komponent (pokud je požadováno provedení kvantitativní analýzy);
- zdroj informací o intenzitách poruch (vyžaduje obvykle zákazník).

7.2 Vlastní FMECA jednotlivých komponent systému

Při vlastní analýze se u každého komponentu (prvku) systému (na zvolené nejnižší úrovni) realizují zejména tyto základní kroky:

- identifikace způsobů poruch prvku, jejich důsledků a pravděpodobných příčin;
- identifikace metod a opatření k detekci a izolaci poruch;
- kvalitativní posouzení významnosti poruch a alternativní opatření;
- vyhodnocení pravděpodobnosti poruch (v případě kvantitativního hodnocení);
- určení kritičnosti poruch (v případě kvantitativního hodnocení).

Tento základní rozsah analýzy může být podle potřeby rozšířen o další kroky, v rámci kterých se budou účelově zjišťovat (analyzovat) další informace, potřebné pro posouzení spolehlivosti či bezpečnosti systému.

Jednotlivé kroky vlastní analýzy je vhodné zaznamenávat do uspořádaných pracovních formulářů, případně s využitím specializovaného software. Použití formulářů nebo software, mimo jiné, vytváří předpoklady proto, že analýza bude provedena systematicky, tj. nic nebude opomenuto (každá položka musí být vyplněna). V současnosti neexistuje žádný závazný předpis, upravující obsah a uspořádání pracovního formuláře pro realizaci analýzy. Uspořádání formuláře může být proto velice různorodé. Některá doporučení a návrhy jsou součástí norem [7], [9], [11], [14]. Vždy by však obsah a uspořádání mělo odpovídat specifickým cílům analýzy a charakteru analyzovaného systému.

Na základní úrovni by měl pracovní formulář nebo software umožňovat zaznamenání následujících informací.

Identifikační číslo prvku

Musí zajistit jednoznačnou identifikaci prvků v systému a zajistit sjednocení údajů v dokumentaci analýzy s výrobní dokumentací. Vhodné je využít systém identifikace prvků použitý při návrhu systému (např. pozice prvků na výkresu sestavy). Identifikační číslo by mělo umožnit bezpečné rozlišení konstrukčně různých prvků se stejným názvem a identifikaci konstrukčně shodných prvků použitých v různých částech systému. Vedle identifikačního čísla je možno použít další upřesňující údaje, např. čísla výrobních výkresů, sériová čísla, výrobní čísla, označení prvků podle katalogu náhradních dílů, označení prvků v blokových diagramech.

Název prvku

Měl by korespondovat s názvem použitým ve výrobní dokumentaci tak, aby se předešlo možným nedorozuměním. Spolu s identifikačním číslem musí zajistit naprosto jednoznačnou identifikaci každého prvku. Pokud je používán pro konstrukčně rozdílné prvky stejný název, musí být název vždy používán s dalšími doplňujícími údaji, které ho jednoznačně identifikují a odlišují od ostatních prvků.

Funkce prvku

Funkci prvku je třeba chápat jako činnost, prostřednictvím které plní svůj účel. Je to důvod, pro který existuje. Proto je definice a popis funkcí klíčovou částí analýzy a je nutné definicím funkcí věnovat velkou pozornost. Je nutné definovat jak očekávané a přijatelné způsoby činnosti systému jako celku a základních prvků, z nichž se skládá, tak i charakteristiky činností, které jsou považovány za nepřijatelné a jsou poruchou, chybovou funkcí nebo mezním stavem. Popis funkcí by měl zahrnovat definici přijatelné činnosti pro všechny požadované nebo stanovené charakteristiky při všech provozních i mimo provozních stavech, pro všechna uvažovaná časová období a pro všechny podmínky prostředí. Funkce prvků musí být definovány jak ve vztahu k nadřazenému systému tak i k celému systému.

Součástí definice funkcí je i definování podmínek prostředí a požadavků předpisů. Prostředí (teplota, vlhkost, vibrace, atd.), v němž se předpokládá, že bude systém pracovat, by mělo být jasně definováno i s jeho vlivem na funkce systému a prvků. U systémů řízených a obsluhovaných člověkem by se měly uvážit i vlivy, spojené s lidským faktorem. Do pracovních formulářů se funkce zapisují výstižným a co nejjednodušším způsobem (obvykle jednoslovným, nebo holou větou). Správná formulace funkcí prvku usnadňuje stanovení možných způsobů selhání prvku.

Způsob poruchy

Způsob poruchy je definován jako jev, prostřednictvím něhož je porucha na prvku pozorována. Vhodným způsobem se tedy zaznamenávají všechny způsoby, kterými se selhání prvků projeví. Pro každý prvek může být definováno více než jen jeden způsob poruchy, pokud je to žádoucí. Pro zjednodušení celé analýzy a zvýšení srozumitelnosti výsledků analýzy je vhodné provést klasifikaci způsobů poruch, která definuje použitelné způsoby popisu selhání prvků. Příklad klasifikace způsobů poruch lze nalézt v normách (např. [14]).

Důležité je, aby při analýze byly do úvahy vzaty všechny možné způsoby poruch prvku a žádný nebyl dopředu z analýzy vylučován jen proto, že je krajně nepravděpodobný. Otázka pravděpodobnosti nastoupení jednotlivých způsobů poruch v této části analýzy není podstatná, jediným rozhodujícím kritériem pro zařazení každého způsobu poruchy do analýzy je zde předpoklad možnosti a předpověditelnosti takového způsobu poruchy (bez ohledu na

praktickou pravděpodobnost poruchy). To, že do analýzy jsou zahrnuty všechny předpověditelné a reálně možné způsoby poruchy každého prvku je podstatným základem analýzy.

Při definování způsobů poruch je možné využít databázi *FMD-97 – Failure Mode/Mechanism Distributions* [10] (Rozložení způsobů poruch), která obsahuje údaje o pravděpodobnosti výskytu jednotlivých způsobů poruch u konkrétních elektronických, elektrických, elektromechanických a mechanických prvků. V nedávné době byla databáze aktualizována a je dostupná jako *FMD-2013*. Je také možné použít konkurenční produkt, a to databázi *SPIDR™ – System and Part Integrated Data Resource* (Integrovaný zdroj dat o systémech a prvcích) vydanou v roce 2006.

Příčina poruchy

Stanovení příčiny poruchy není původním, ani prioritním cílem analýzy a někdy bývá z analýzy zcela vypuštěno. Je nezbytné stanovit všechny pravděpodobné (možné) příčiny spojené s každým daným způsobem poruch. Identifikace potenciálních příčin každého způsobu poruch se provádí především proto, aby bylo možné odhadnout zdroj jejich výskytu, aby se odhalily sekundární důsledky a aby bylo možné doporučit soubor nápravných opatření. Jelikož způsob poruchy může mít více než jednu příčinu, musí být stanoveny a popsány všechny možné nezávislé příčiny pro každý způsob poruchy.

Důsledky poruchy

Analýza důsledků poruch je prioritním cílem analýzy. Zjistí se, vyhodnotí a zaznamenají důsledky všech předpokládaných způsobů poruch jak na činnost, funkci a stav vlastního prvku systému, tak i na všechny vyšší úrovně systému až po úroveň systému jako celku. Podle zvolených kritérií se potom každému důsledku přiřadí stupeň závažnosti. Obvykle se rozlišují důsledky místní (na úrovní prvků) a konečné (na úrovni systému).

V rámci lokálního důsledku se analyzují důsledky poruchy na vlastní prvek. Vyhodnocení těchto důsledků poskytuje výchozí informace pro vyhodnocení alternativních opatření nebo pro doporučení nápravných opatření. V některých případech neexistuje jiný lokální důsledek než sám způsob poruchy.

Pro posouzení konečného důsledku poruchy, tedy důsledku poruchy prvku na činnost, funkci a stav celého systému je nutné vyhodnotit důsledky každé poruchy na všech nižších úrovních. Přitom je nutné brát v úvahu všechny možné kombinace s dalšími poruchami systému, protože porucha jednoho prvku, která sama o sobě může mít nezávažné důsledky, může v kombinaci s jinou poruchou vést ke katastrofickým důsledkům. Proto v pracovních formulářích musí být tyto důsledky vyplývající z násobných poruch také uvedeny.

Metody detekce poruch

Je třeba popsat možné způsoby detekce poruch a prostředky, jejichž pomocí je uživatel nebo údržbář informován o poruše. Informace z této části analýzy jsou důležité pro návrh případných preventivních opatření, jakými mohou být například návrhy na vybavení systému přístroji palubní diagnostiky, nebo návrhy do oblasti údržby systému. Zvláštní pozornost je třeba věnovat tak zvaným „skrytým poruchám“ o kterých obsluha není včas informována zabudovaným systémem signalizace a varování a které by mohly svojí existencí způsobit selhání systému až v okamžiku, kdy se od něj očekává plnění jeho funkce.

Klasifikace závažnosti poruchy

Klasifikace závažnosti poruchy je posouzení významnosti důsledku způsobu poruchy pro provoz objektu. K tomu je vhodné vytvořit systém kategorizace důsledků poruch, který by pokrýval všechny předpověditelné důsledky jednotlivých poruch systému a umožňoval jednoznačné zařazení každé poruchy do některé z navržených kategorií. Systém kategorizace důsledků poruch, je vždy třeba přizpůsobit konkrétnímu systému a podmínkám jeho použití.

Pravděpodobnost výskytu poruchy

Pro každý způsob poruchy se uvede pravděpodobnost jejího výskytu. Odhad této pravděpodobnosti může být proveden řadou způsobů, například s využitím:

- údajů od výrobců;
- dat z provozu stejného (srovnatelného) prvku;
- zkoušek spolehlivosti stejného (srovnatelného) prvku;
- metodik predikce bezporuchovosti prvků (MIL-HDBK-217F, PRISM, 217Plus, FIDES, IEC/TR 62380, Telcordia SR-332, …);
- databází informací o bezporuchovosti prvků (NPRD-2011, EPRD-2014, SPIDR, …);
- expertních odhadů.

Údaje uvedené v této části slouží jako vstupní údaje pro hodnocení kritičnosti poruch a pro případný výpočet pravděpodobností jednotlivých způsobů poruch celého systému, nebo jeho částí. Pokud má analýza ověřit, jestli systém vyhovuje kvantitativním požadavkům na spolehlivost a bezpečnost je znalost pravděpodobnosti jednotlivých způsobů poruch všech prvků systému nezbytná.

Kritičnost poruchy (riziko)

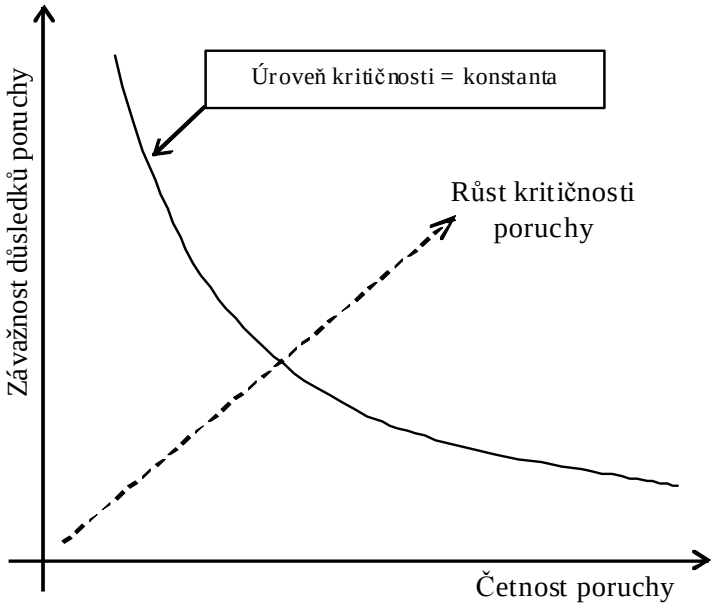
Jedním z možných přístupů k hodnocením kritičnosti poruchy je „ohodnocení“ závažnosti důsledků daného způsobu poruchy při uvažování jeho četnosti (pravděpodobnosti vzniku). Filozofie uvedeného hodnocení kritičnosti poruchy je naznačena na Obrázku 2.2.

Odlišným přístupem k hodnocení kritičnosti je způsob používaný zejména v automobilovém průmyslu. Ten je založen na určení tzv. čísla priority rizika (RPN – Risk Priority Number) [7]:

$$RPN = S \times O \times D,$$

kde S (Severity) je bezrozměrné číslo, které klasifikuje závažnost důsledků poruchy; O (Occurrence) klasifikuje pravděpodobnost výskytu způsobu poruchy (často uváděna formou kategorie četnosti namísto skutečné pravděpodobnosti); D (Detection) klasifikuje detekci (odhad naděje, že se porucha zjistí a eliminuje před tím, než se projeví důsledek).

Podrobně je problematika určování RPN popsána v normách [7], [9], [14].



Obrázek 2.2 – Filosofie hodnocení kritičnosti poruch [3]

7.3 Vyhodnocení analýzy

Vyhodnocení analýzy musí směřovat k přijetí souboru účinných nápravných opatření, zaměřených na odstranění příčin nejzávažnějších typů poruch nebo na snížení stupně jejich závažnosti. Výsledky analýzy se vždy porovnávají s požadavky stanovenými v normách a předpisech (pokud existují) nebo s požadavky, které byly stanoveny pro daný produkt (např. zákazníkem).

Na základě výsledků tohoto porovnání a dalších poznatků získaných při realizaci analýzy se navrhnou konkrétní nápravná opatření. Ke každé poruše a jejím příčinám, pokud to je třeba, se navrhnou taková opatření, která povedou:

- k úplnému odstranění příčin poruchy;
- ke snížení pravděpodobnosti vzniku poruchy;
- ke snížení stupně kritičnosti důsledků poruchy.

Mimo to je možné na základě výstupů z analýzy, pokud je to požadováno, navrhnout:

- zdůvodněný program potřebných zkoušek spolehlivosti kritických prvků;
- účelný systém údržby, zaměřený na předcházení vzniku závažných poruch;
- účelný systém technické diagnostiky, zaměřený na včasné odhalení příčin vzniku poruch.

8. Závěr

V příspěvku byla představena a popsána jedna z nejpoužívanějších metod pro analýzu spolehlivosti a bezpečnosti – FME(C)A. V příspěvku také byly uvedeny četné zdroje s informacemi o metodě, zejména normy a webové stránky.

Použité zdroje

[1] BORGOVINI, R. – PEMBERTON, S. – ROSSI, M. *Failure Mode, Effects and Criticality Analysis (FMECA).* Rome: Reliability Analysis Center (RAC), 1993.

[2] FAJMONOVÁ, L. *Analýza zařízení metodou FMEA.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2003. 55 s. Vedoucí diplomové práce prof. Ing. František Babinec, CSc.

[3] HOLUB, R. – VINTR, Z. *Spolehlivost letadlové techniky* [Elektronická učebnice]. Brno: VUT v Brně, 2001.

[4] VINTR, M. Oborové normy ve spolehlivosti. In *Mezinárodní a národní normalizace ve spolehlivosti.* Praha: Česká společnost pro jakost, 2012, s. 29–36. ISBN 978-80-02-02421-7.

[5] VINTR, M. Metoda FMECA jako nástroj analýzy bezpečnosti a spolehlivosti komponent systému. In *Analýzy spolehlivosti a bezpečnosti v praxi*. Praha: Česká společnost pro jakost, 2009, s. 35–50. ISBN 978-80-02-02156-8.

[6] ANSI/AIAA S-102.2.4-2009. *Performance-Based Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements.* Reston: American Institute of Aeronautics and Astronautics, 2009.

[7] ČSN EN 60812 (01 0675). *Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA).* Praha: Český normalizační institut, 2007.

[8] ECSS-Q-ST-30-02C. *Space Product Assurance – Failure Modes, Effects (and Criticality) Analysis (FMEA/FMECA).* Noordwijk: ESA Requirements and Standards Division, 2009.

[9] IEC 60812/Ed3. *Failure Mode and Effects Analysis (FMEA) (Committee draft – 56/1579/CD).* Geneva: International Electrotechnical Commission, 2014.

[10] *FMD-97. Failure Mode/Mechanism Distributions.* Rome: Reliability Analysis Center (RAC), 1998.

[11] MIL-STD-1629A. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis.* Washington: Department of Defense, 1980.

[12] SAE ARP4761. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* Warrendale: Society of Automotive Engineers, 1996.

[13] SAE ARP5580. *Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications.* Warrendale: Society of Automotive Engineers, 2001.

[14] SAE J1739. *Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA).* Warrendale: Society of Automotive Engineers, 2009.

[15] VDA 4. *Zajišťování kvality před sériovou výrobou (kapitola: FMEA produktu, FMEA procesu)*. Praha: Česká společnost pro jakost, 2006.

ANALÝZA STROMU UDÁLOSTÍ – EVENT TREE ANALYSIS (ETA)

pplk. doc. Ing. David VALIŠ, Ph.D.
Univerzita obrany v Brně
e-mail: david.valis@unob.cz

1. *Úvod*

Technika ETA se v literatuře uvádí jako vhodná metoda pro všeobecné posuzování spolehlivosti. Tato metoda se též používá pro studie analýzy rizika a bezpečnosti. Principy analýzy stromu událostí (ETA – Event Tree Analysis) se využívají k popisu a modelování následků iniciační události, jakož i pro kvalitativní a kvantitativní analyzování těchto následků v kontextu ukazatelů týkajících se spolehlivosti a rizika.

Základní principy této metodiky se nezměnily od vypracování koncepce techniky ETA v šedesátých letech dvacátého století. ETA byla poprvé úspěšně použita v jaderném průmyslu ve studii vypracované americkou komisí U.S. Nuclear Regulatory Commission v tak zvané zprávě WASH 1400 v roce 1975.

V následujících letech se technice ETA rozšířila v podobě metodiky pro analýzu spolehlivosti a rizika. Tato technika se používá v rozmanitých průmyslových odvětvích sahajících od leteckého průmyslu, přes jaderná zařízení, automobilový průmysl, chemický zpracovatelský průmysl, těžbu ropy a plynu na pobřeží a v moři až po obranný průmysl a přepravní systémy.

Na rozdíl od jiných technik spolehlivosti, jako je například použití Markovova modelování, je ETA založena na relativně elementárních matematických principech. Implementace ETA však vyžaduje vysoký stupeň odborných znalostí při použití této techniky. To je zčásti způsobeno skutečností, že je nutné dávat zvlášť pozor na zacházení se závislými událostmi. Kromě toho je možné využít těsné příbuznosti mezi analýzou stromu poruchových stavů (FTA – *Fault Tree Analysis*) a kvalitativní a kvantitativní analýzou stromů událostí.

2. *Všeobecný popis metody ETA*

Analýza stromu událostí (ETA) je induktivní postup modelování možných výstupů, které by mohly vyplývat z dané iniciační události a stavu zmírňujících faktorů, jakož i postup identifikace a posouzení četnosti nebo pravděpodobnosti různých možných výstupů dané iniciační události.

Grafická reprezentace stromu událostí vyžaduje, aby byly značky, identifikátory a návěští užívány konzistentním způsobem. Jelikož se reprezentace stromů událostí mění podle toho, co preferuje uživatel. Například v příloze normy ČSN EN 62502 je uveden soubor obecně používaných grafických reprezentací pro ETA.

Počínaje od iniciační události se ETA zabývá otázkou "co se stane, když ...". Na základě této otázky analytik konstruuje strom různých možných výstupů. Je tedy zásadně důležité, aby byl sestaven vyčerpávající seznam iniciačních událostí a tudíž bylo zajištěno, že stromy událostí řádně zobrazují všechny důležité posloupnosti událostí uvažovaného systému.

S použitím této logiky může být ETA popsána jako metoda reprezentování zmírňujících faktorů v reakci na iniciační událost, přičemž se berou v úvahu vhodné zmírňující faktory.

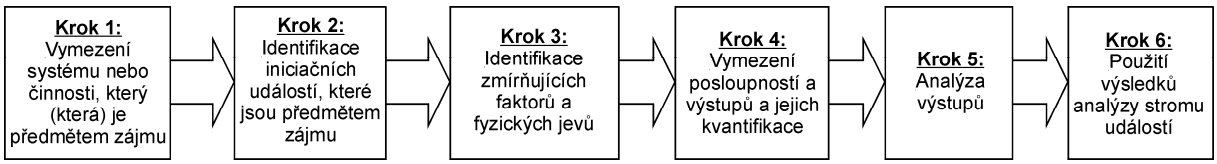
Z kvalitativního hlediska pomáhá ETA identifikovat všechny potenciální scénáře nehod (rozvětvující se jako strom s větvemi úspěchů nebo poruch/selhání) a potenciální slabiny návrhu nebo postupu. Větev úspěchu modeluje podmínku, že zmírňující faktor funguje, jak je zamýšleno. Jako u jiných technik analýzy, je i v ETA nutné věnovat zvláštní péči modelování závislostí, přičemž je nutné mít na paměti, že pravděpodobnosti používané pro kvantifikování stromu událostí jsou podmíněny posloupností událostí, ke kterým došlo před výskytem dotyčné události. Teoreticky by bylo možné pomocí stromu událostí modelovat vliv poruch (selhání) obsluhy nebo softwaru, tyto problémy jsou však rovněž pojednány např. v IEC 62508 a v IEC 62429.

Výhody analýzy ETA jako techniky týkající se spolehlivosti a rizika, jakož i její omezení, jsou rozebrány dále. Příkladem omezení analýzy ETA je nutnost pečlivě uvažovat časově závislý vývoj, protože s ním lze řádně zacházet pouze ve zvláštních případech. Toto omezení vedlo k vypracování silně souvisejících metod, jako je metoda analýzy dynamického stromu událostí (Dynamic Event Tree Analysis), která usnadňuje modelování časově závislých vývojů.

Analýza ETA úzce souvisí s analýzou FTA, přičemž vrcholové události FTA dávají podmíněnou pravděpodobnost pro konkrétní uzel ETA. Tato skutečnost je popsána analýzou vztahu příčina-následek (CCA – Cause-Consequence Analysis) a analýzou ochranných vrstev (LOPA – Layer of Protection Analysis). Při analýze CCA se kombinuje analýza příčiny a analýza následku a proto se používá deduktivní i induktivní přístup. Analýza LOPA byla vyvinuta ve zpracovatelském průmyslu jako speciálně přizpůsobená analýza ETA.

Jelikož jsou pro úspěch zásadně důležité první kroky a dobře sestavený přístup, je dále popsán rozvoj stromu událostí počínaje přesným vymezením systému. Kromě toho se dále zabýváme rovněž různými hledisky systému (technickým, provozním, lidským a funkčním), jakož i hloubkou analýzy. Dalším důležitým problémem je otázka, jak stanovit seznam relevantních iniciačních událostí.

Na obrázku 3.1 jsou zobrazeny hlavní kroky při provádění analýzy ETA. Ačkoliv se zdánlivě jedná o přímočarý proces, musí mít analytik na mysli, že je konstrukce stromu událostí velmi iterativní proces.



Obrázek 3.1 – Proces rozvoje stromů událostí

3. *Kroky v analýze ETA*

Krok 1: Vymezení systému nebo činnosti, které jsou předmětem zájmu - Specifikují se a jasně se vymezí hranice systému nebo činnosti, pro které se mají provést analýzy ETA.

Krok 2: Identifikace iniciačních událostí, které jsou předmětem zájmu - Provede se třídění, aby se identifikovaly události, které jsou předmětem zájmu, nebo kategorie událostí, na které se analýza zaměří.

Krok 3: Identifikace zmírňujících faktorů a fyzických jevů - Identifikují se různé zmírňující faktory, které mohou ovlivnit průběh iniciační události k jejím výstupům. Mezi tyto

zmírňující faktory se zahrnují jak technické systémy, tak lidské zásahy/rozhodnutí. Identifikují se též fyzické jevy nebo nahodilé události, jako je vznícení nebo meteorologické podmínky, které ovlivní průběh a nakonec výstup iniciační události.

Krok 4: Vymezení posloupností a výstupů a jejich kvantifikace - Pro každou iniciační událost se přesně stanoví různé výstupy (např. scénáře nehody), které mohou nastat, a provede se aktuální kvantitativní analýza na základě zkonstruovaného stromu událostí.

Krok 5: Analýza výstupů - Potom se analyzují různé výstupy s ohledem na jejich následky a jejich dopad na výsledky analýzy.

Krok 6: Použití výsledků analýzy ETA - Kvalitativní a kvantitativní výsledky analýzy se potom převedou na nutné zásahy.

4. *Přínosy a omezení analýzy ETA*

Analýza ETA má následující přednosti:

a) je použitelná pro všechny typy systémů;
b) poskytuje vizualizaci řetězců událostí následujících po iniciační události;
c) umožňuje posoudit více současně existujících poruchových stavů systému (stavů způsobujících neschopnost provádět požadovanou funkci, např. vadu kontrolního systému) nebo poruch (ukončení schopnosti provádět požadovanou funkci, např. událost zaseknutí otevřeného ventilu), jakož i jiných závislých událostí;
d) funguje současně v oblasti poruchy/selhání i úspěchu;
e) identifikují se při ní koncové událostí, které by jinak nemusely být předvídány;
f) identifikují se při ní potenciální jednobodové poruchy, oblasti zranitelnosti systému a protiopatření s malým přínosem. ETA poskytuje optimalizované rozmístění zdrojů a zlepšené řízení rizika pomocí zlepšených po-stupů a bezpečnostních funkcí;
g) poskytuje identifikaci a sledovatelnost cest šíření poruch v systému;
h) umožňuje provést rozklad velkých a složitých systémů na menší zvládnutelnější části jejich seskupením do menších funkčních jednotek nebo podsystémů.

Síla analýzy ETA ve srovnání s mnoha jinými technikami analýzy a technikami týkajícími se rizika spočívá ve schopnosti modelovat posloupnost a interakci různých zmírňujících faktorů, které následují po výskytu iniciační události. Systém a jeho interakce se všemi zmírňujícími faktory ve scénáři nehody se tedy stávají pro analytika viditelnými pro další hodnocení rizika.

Následující obecně platná omezení sdružená s technikami analýzy spolehlivosti platí též pro analýzu ETA:

a) iniciační události samotná analýza neodhalí; sestavit vyčerpávající seznam iniciačních událostí je analytickým úkolem pracovníků zapojených do používání metody;
b) sestavit vyčerpávající seznam možných provozních scénářů je úkolem pracovníků zapojených do procesu;
c) skryté závislosti systému by mohly být přehlédnuty, což by vedlo k nepřiměřeně optimistickým odhadům ukazatelů týkajících se spolehlivosti a rizika;
d) k zaměření se na správné zacházení s podmíněnými pravděpodobnostmi a závislými událostmi je nutné, aby měl analytik praktické zkušenosti jak s touto metodou, tak se zkoumáním předchozího systému.

Dále jsou uvedena omezení platná pro ETA:

e) časově závislými vývoji, do kterých jsou zahrnuty časové závislosti příslušných pravděpodobností, se lze zabývat pouze tehdy, jestliže příslušné systémy vykazují skutečně konstantní pravděpodobnost nebo intenzitu poruch nebo jestliže se v případě strategií zotavení a opravy předpokládá, že se rychle dosáhne ustálené nepohotovosti. S tímto hlediskem je třeba počítat při zacházení s periodicky testovanými systémy;

f) dalším obtížným hlediskem je hledisko časově závislých vývojů, do kterých jsou zahrnuty dynamické situace, např. jestliže se kritéria úspěchu pro zmírňující faktory mění v závislosti na tom, jak působily předchozí zmírňující faktory. K reflektování této situace se obvykle volí konzervativní předpoklad;

g) situace, kdy prodlévání v určitém stavu déle než po specifikovanou dobu může vést k poruchovému stavu. Tento stav (např. pomalé ucházení vzduchu z pneumatiky) lze ve stromu událostí obtížně modelovat;

h) závislosti ve stromu událostí, např. v důsledku závislostí mezi iniciační událostí a zmírňujícími faktory, je nutné pečlivě uvážit. Existuje však několik technik analýzy, které jsou samy vhodné pro zacházení se závislostmi (závislými poruchami). Pro zacházení s těmito hledisky se může jako výhodná osvědčit kombinace analýz FTA a ETA;

i) ačkoliv může být identifikováno několik posloupností vedoucích k poruše systému, nemusejí být různé závažnosti nehod sdružené s konkrétními výstupy rozlišitelné bez dodatečné analýzy; takovou potřebu analýzy je však nutné si uvědomit.

5. *Vztah ETA k jiným technikám analýzy*

V praxi se ETA někdy provádí jako samostatná analýza a v jiných případech se provádí v kombinaci s analýzou FTA. FTA se zabývá identifikací a analýzou podmínek a faktorů, které způsobují nebo potenciálně způsobují definovanou nežádoucí událost či přispívají k jejímu výskytu. Další podrobnosti viz IEC 61025. Kombinace analýz ETA a FTA (někdy nazývaná jako analýza vztahu příčina-následek CCA – *Cause-Consequence Analysis*) se všeobecně používá, FTA se např. může použít k vyhodnocení četnosti *f* iniciační události v ETA.

Při kombinování stromů událostí a stromů poruchových stavů lze volit mezi dvěma přístupy. Jeden přístup je takzvaný přístup LESF. Jestliže má strom událostí tendenci být nadměrně velký, může se použít přístup SELF.

Při přístupu LESF se ve stromech událostí explicitně objevují stavy všech systémů, které podporují analyzovaný systém a které jsou dále nazývány podpůrné systémy. K vrcholovým událostem stromů poruchových stavů jsou přidruženy okrajové podmínky, do kterých je zahrnut předpoklad, že jsou podpůrné systémy v určitém stavu vhodném k vyhodnocení posloupnosti událostí. Pro každou množinu okrajových podmínek se v daném systému používají samostatné stromy poruchových stavů.

Při přístupu SELF se nejprve rozvíjejí stromy událostí s iniciační událostí a zmírňujícími funkcemi vykonávanými rozmanitými zmírňujícími systémy uvedenými jako záhlaví a potom se rozšíří do podoby stromů událostí se statutem systémů první linie jako záhlavím. Modely stromu poruchových stavů systému první linie se rozvíjejí dolů až ke vhodným hranicím s podpůrnými systémy.

LOPA je zvláštní normalizovaná forma analýzy ETA, která se používá jako zjednodušený prostředek pro analýzu rizika přizpůsobenou pro konkrétní aplikační prostředí.

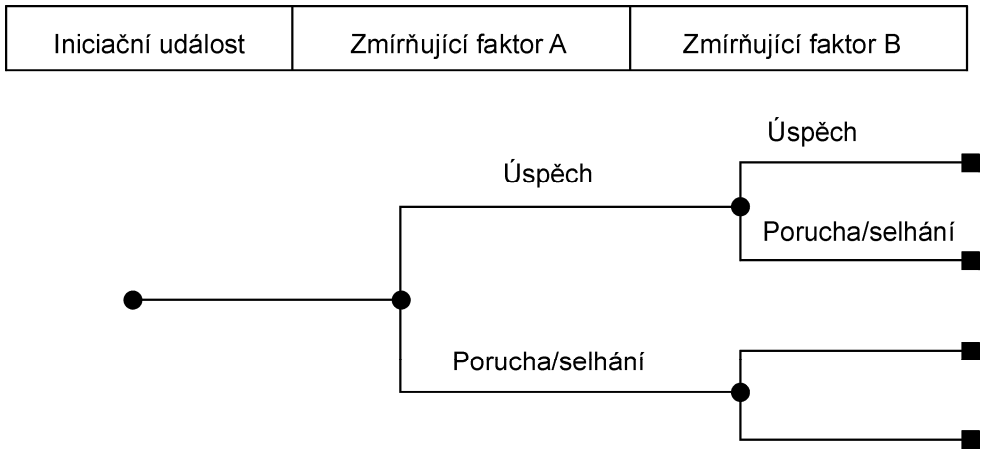
LOPA je organizována ve formě pracovního listu podobně jako při analýze způsobů adůsledků poruch (FMEA); iniciační události se zaznamenávají do řádků a různé ochranné vrstvy (představující normalizované zmírňující faktory) se zaznamenávají do sloupců. To znamená, že je možné s jakoukoliv posloupností událostí v analýze LOPA zacházet též jako v ETA. Pro účely analýzy rizika se do pracovního listu začleňují též úrovně závažnosti (nebo poškození).

Analýzu ETA je možné kombinovat s jinou technikou, která je užitečná pro odvození pravděpodobnosti úspěšnosti nebo selhání odpovídajících zmírňujících faktorů, např. s Markovovou technikou nebo s blokovými diagramy bezporuchovosti (RBD), avšak v těchto případech tyto jiné techniky pouze doplňují analýzu ETA.

6. *Grafická podoba metody ETA*

Před zahájením kvantitativní analýzy četnosti nebo pravděpodobnosti výstupů různých posloupností událostí je nutné pečlivě analyzovat kvalitativní hlediska modelu stromu událostí. Tato hlediska zahrnují závislosti událostí včetně iniciační události a vrcholových událostí, jakož i mezilehlých nebo základních událostí propojených stromů poruchových stavů.

Ke snadnějšímu znázornění základních principů vyhodnocení je na obrázku 3.2 pro ilustraci ukázána základní grafická reprezentace stromu událostí.



Obrázek 3.2 Oblasti informací, získávaných analýzou spolehlivosti.

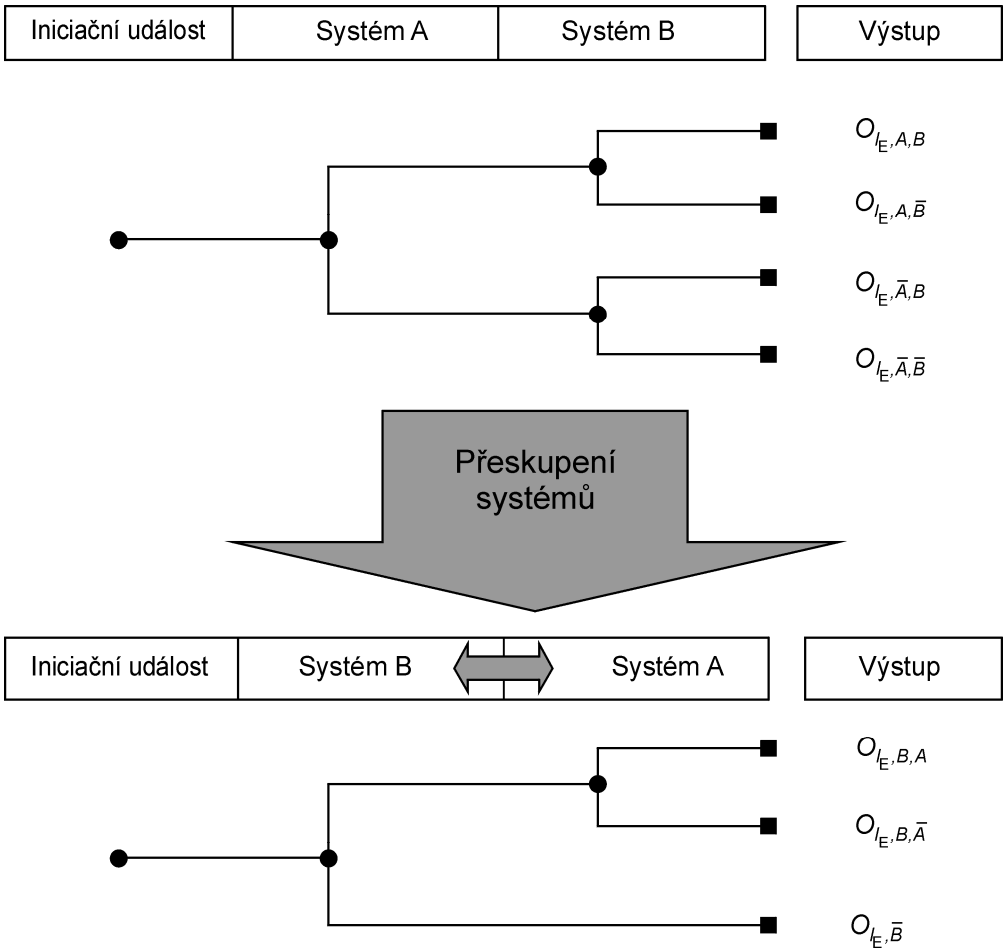
Funkční závislosti:

Řazení různých zmírňujících faktorů v posloupnosti stromu událostí není ovládáno pouze jejich časem zásahu jako možných zmírňujících faktorů, ale též jejich logickým pořadím. Je nutné vzít v úvahu, zda je úspěšný zásah zmírňujícího faktoru závislý na úspěšném zásahu jiného. To by se mohlo stát, jestliže například

- jeden zmírňující faktor reprezentuje podpůrný systém pro jiný faktor, nebo
- dojde k takovým změnám parametrů prostředí, že to ovlivní úspěch či selhání jiného zmírňujícího faktoru.

Uvažme například strom znázorněný na obrázku 3.3, kde následná selhání systémů A a B (zmírňujících faktorů) vedou k ukázaným výstupům. V tomto příkladu je systém A podporován systémem B.

Po přeskupení (změně pořadí) systémů A a B ve stromě událostí (viz obrázek 3.3) není zapotřebí větev následující po poruše systému B dále rozložit na dvě větve pro systém A, protože porucha systému B znamená, že systém A nemůže vykonávat svou funkci. To umožňuje provést tak zvané prořezání stromu událostí. Jelikož se toto provádí většinou pomocí počítačových programů, hlavním příspěvkem analytika je uvážit různé závislosti modelu.



Obrázek 3.3 Funkční závislosti ve stromech událostí

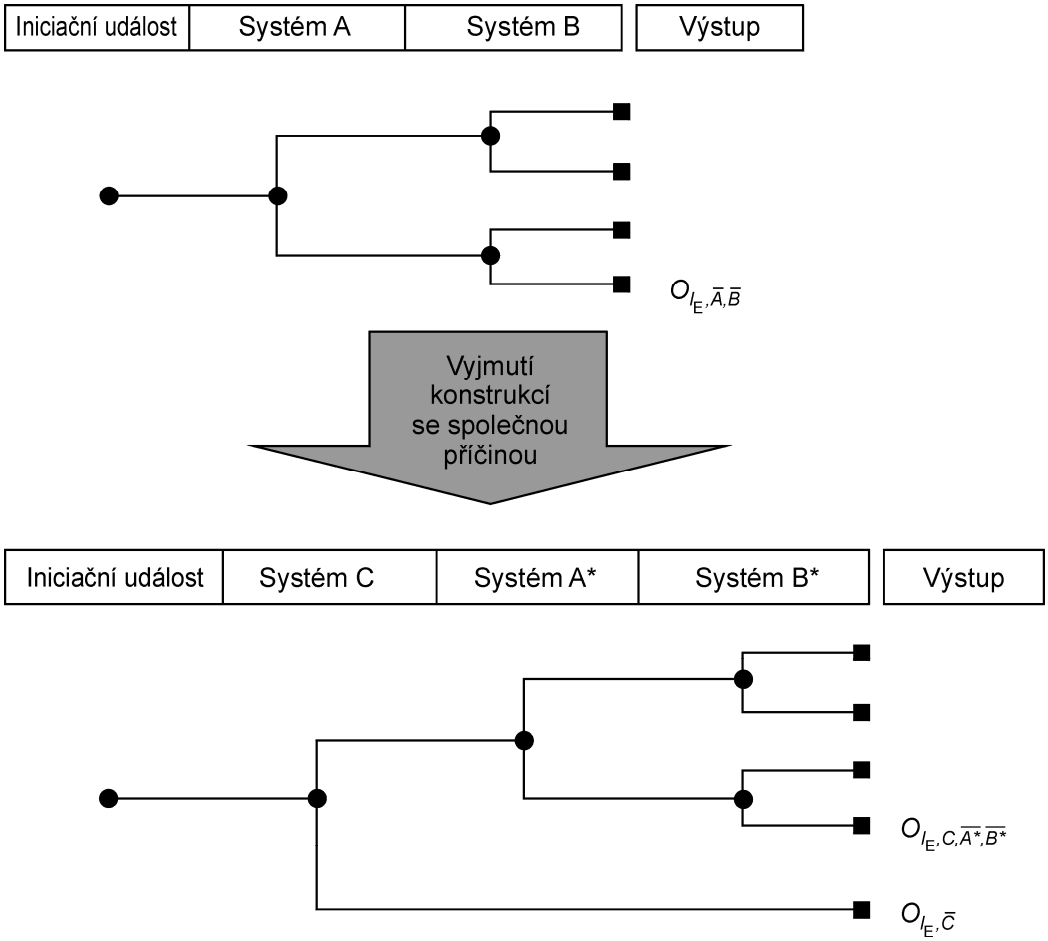
Konstrukční nebo fyzické závislosti:

Konstrukční nebo fyzické závislosti obecně vedou k poruchám se společnou příčinou a takové poruchy vedou k vícenásobným událostem. Příklady poruch se společnou příčinou jsou případy způsobené událostmi, jako jsou požáry, zemětřesení, orkány, poruchy technických systémů (např. rozsáhlá porucha dodávky elektrické energie nebo výbuchy – ať již jsou iniciovány interně nebo externě) nebo zásahy člověka, jako jsou lidské chyby nebo sabotáže.

Provádí se tudíž analýza společné příčiny, aby se stanovila citlivost různých zmírňujících faktorů na poruchu/selhání pocházející z externích nebo interních podmínek, systémů nebo funkcí. Hledisko, které je třeba objasnit, je, zda výskyt iniciační události (např. zemětřesení) ovlivňuje podmíněné pravděpodobnosti výskytu všech vrcholových událostí propojených stromů poruchových stavů.

Další krok kvalitativní analýzy se skládá z identifikování společných systémů nebo společných funkcí, které ovlivňují různé zmírňující faktory. Uvažujme například strom událostí, kde porucha systému A, za kterou následuje porucha systému B, vede

k nežádoucímu výstupu. Jestliže systém A k tomu, aby řádně fungoval za účelem úspěšného splnění funkce, spoléhá na části systému B, mohla by se "společná část" vyjmout a uvažovaly by se tři systémy: systém A* a systém B*, což jsou systémy A a B bez společných částí, a systém C, který reprezentuje společné části používané oběma systémy A a B. Tento scénář je znázorněn na obrázku 3.4.

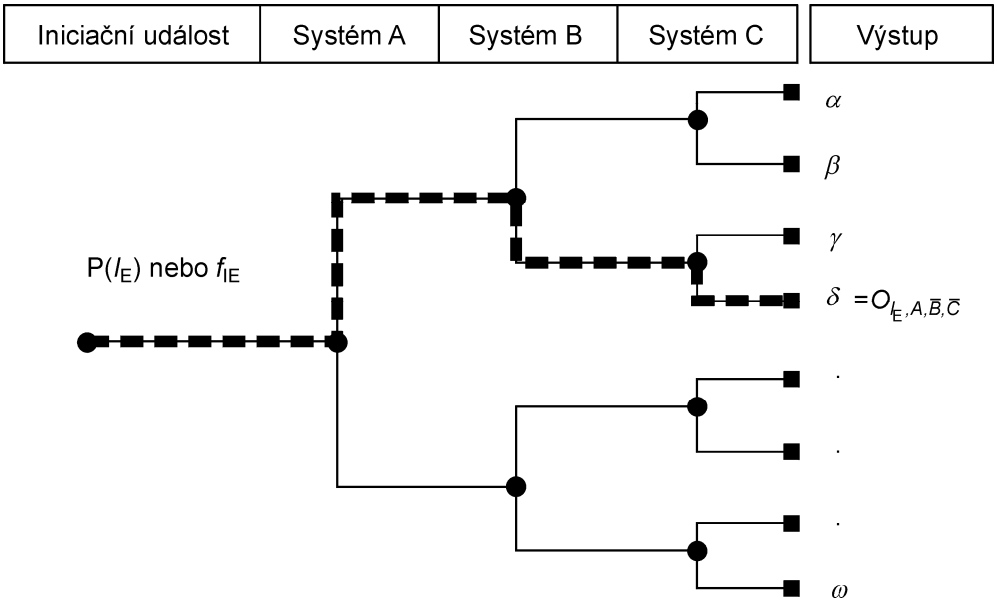


Obrázek 3.4 Modelování konstrukčních nebo fyzických závislostí

Kvantitativní analýza – nezávislá posloupnost událostí

Když jsou všechny podmíněné pravděpodobnosti úspěchu nebo selhání zmírňujících faktorů navzájem nezávislé, stává se kvantitativní analýza velmi jednoduchou.

Uvažujme strom událostí se třemi zmírňujícími faktory – systémy A, B a C. Na obrázku 3.5 je znázorněna zvláštní posloupnost ve výsledném stromu událostí (znázorněná přerušovanou čarou), kde systém A funguje, zatímco systémy B a C mají poruchu. V následujících odstavcích jsou vysvětleny základní principy vyhodnocování četnosti nebo pravděpodobnosti výstupu této konkrétní posloupnosti δ.



Obrázek 3.5 Posloupnost událostí

K napsání rovnice (1) pro pravděpodobnost $P(\delta)$ této konkrétní posloupnosti δ lze použít teorém podmíněné pravděpodobnosti a definice uvedené v kapitole 3.

$$P(\delta) = P\left(I_E \cdot A \cdot \overline{B} \cdot \overline{C}\right) = P(I_E) \cdot P\left(A \middle| I_E\right) \cdot P\left(\overline{B} \middle| I_E \cdot A\right) \cdot P\left(\overline{C} \middle| I_E \cdot A \cdot \overline{B}\right), \qquad (1)$$

kde

$P(I_E)$ je rovno pravděpodobnosti výskytu iniciační události I_E,

$P(A|I_E)$ je rovno pravděpodobnosti úspěchu systému A za předpokladu, že nastala iniciační událost I_E (podmíněná pravděpodobnost).

Jestliže jsou úspěchy a poruchy jednoho systému nezávislé na úspěších a poruchách jiných systémů, lze použít pravděpodobnosti podmíněné výhradně výskytem události I_E. Vzorec (1) lze tudíž zjednodušit, jak je uvedeno dále, s $P(I_E)$ jako pravděpodobností výskytu iniciační události:

$$P(\delta) = P(I_E) \cdot P\left(A \middle| I_E\right) \cdot P\left(\overline{B} \middle| I_E\right) \cdot P\left(\overline{C} \middle| I_E\right). \qquad (2)$$

Iniciační událost může být popsána buď bezrozměrnou pravděpodobností výskytu $P(I_E)$, nebo četností f_{IE} (1/čas). Jestliže je pozornost zaměřena na pojem četnost, může se tento matematický model použít též k výpočtu četnosti f_δ výskytu posloupnosti δ v rovnici (3) s četností iniciační události f_{IE}:

$$f_\delta = f_{IE} \cdot P\left(A \middle| I_E\right) \cdot P\left(\overline{B} \middle| I_E\right) \cdot P\left(\overline{C} \middle| I_E\right). \qquad (3)$$

7. *Dokumentace analýzy ETA*

Dokumentace analýzy ETA má obsahovat některé základní položky, jak je uvedeno dále. Pro zvýšení srozumitelnosti, zejména u složitých systémů, mohou být poskytovány další a doplňkové informace. Klíčovým bodem je, že dokumentace musí zevrubně zachytit provedené kroky. Minimální části dokumentace jsou následující:

a) cíl a rozsah platnosti analýzy;
b) popis systému:
   - popis návrhu;
   - provoz systému;

- podrobné vymezení hranic systému;

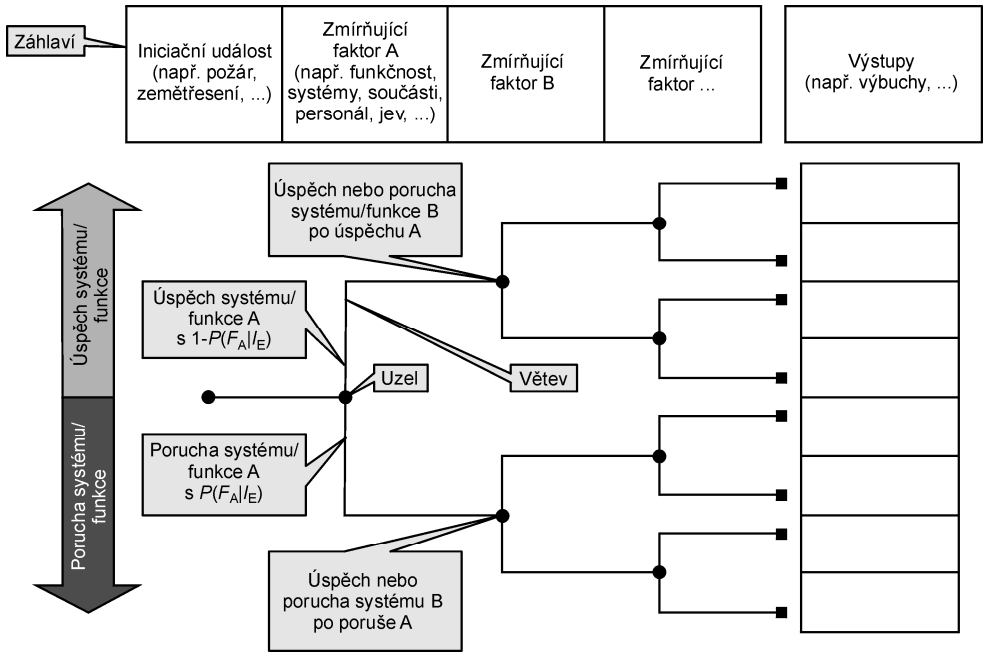
c) předpoklady:
   - předpoklady o návrhu systému;
   - předpoklady o provozu, údržbě, zkouškách a kontrolách;
   - předpoklady o modelování bezporuchovosti a pohotovosti;

d) analýza ETA (B.2.5), (B.2.6):
   - důvody a zdroje pro seznam iniciačních událostí;
   - analýza včetně grafické reprezentace;
   - použité zdroje dat;

e) výsledky, závěry a doporučení (B.2.7).

8. *Příklady provedení grafické reprezentace ETA*

Často používaná grafická reprezentace stromu událostí je uvedena na obrázku 3.6.



Obrázek 3.6 Často používaná grafická reprezentace stromů událostí

Příklad použití analýzy pro požár v elektrárně

Zkušenosti za posledních 40 let ukazují, že je při analyzování přispívajících faktorů k celkovému riziku vážných nehod nutné počítat s riziky požáru v jaderné elektrárně.

Dále je uveden příklad pravděpodobnostní analýzy rizika požáru prováděné s dvojím cílem:

a) pomocí vhodného procesu třídění musejí být identifikovány kritické zóny elektrárny, které představují největší příspěvek k celkové pravděpodobnosti poškození aktivní zóny reaktoru jaderné elektrárny;

b) musejí se stanovit posloupnosti událostí požáru, které odrážejí důsledky výskytu požáru, detekci požáru, izolaci místnosti, hašení a poškození zařízení vlivem hasicího prostředku.

Při kvantitativní analýze ETA se musí stanovit četnost iniciačních událostí způsobených požárem a různé stavy poškození aktivní zóny reaktoru.

Hlavní úkoly jsou provést kvantitativní analýzu a realizovat proces kvalitativního třídění pro identifikaci kritických požárních úseků, jak je popsáno dále.

Třídicí analýza

V prvním kroku se provede podrobný sběr dat ve všech místnostech elektrárny, aby se místnosti klasifikovaly podle své důležitosti a funkce. Dále uvedené termíny jsou příklady ze specifické analýzy.

Hasební obvod je definován jako budova nebo část budovy, která je dostatečně chráněna požárními bariérami, které brání šíření požáru do přilehlých budov nebo částí budov.

Požární úsek je rozdělení hasebního obvodu do takových sekcí, aby se nežádoucí následky nešířily na jiné sekce.

Základní požární úsek obsahuje buď zařízení týkající se provozu na výkonu, zařízení vztahující se k bezpečnosti, nebo trvale či dočasně umístěné hořlaviny.

Kritický požární úsek je základní požární úsek, ve kterém v případě, že požár poškodí nejméně jednu součást či systém vztahující se k bezpečnosti, způsobí to iniciační událost týkající se bezpečnosti v jaderné elektrárně.

Proces třídění začíná identifikací všech místností, u nichž je splněno nejméně jedno z následujících tří kritérií:

a) požární zatížení >7 kWh/m^2;

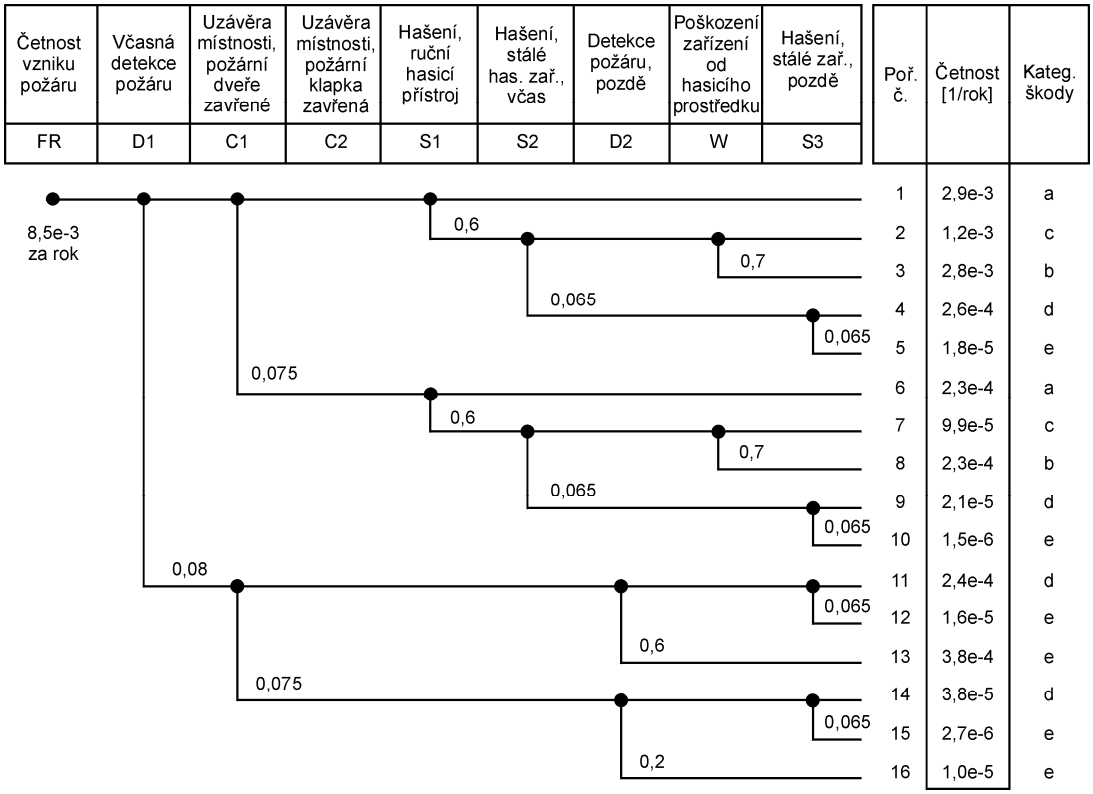
b) místnost obsahuje zařízení vztahující se k bezpečnosti nebo kabely takového zařízení;

c) místnost obsahuje provozní nebo snímací zařízení ochranného systému reaktoru (bezpečnostní řídicí systém).

Místnosti, u nichž jsou současně splněna všechna tři kritéria, se identifikují jako základní požární úseky.

Kvantitativní analýza

Pro každý kritický požární úsek nebo místnost se vypracuje strom událostí s uzlem pro vznik požáru, větrání místnosti, detekci požáru, hašení a šíření požáru. Všechny zmírňující faktory ve stromě událostí se považují za vzájemně nezávislé. Na obrázku 3.7 je ukázán typický strom událostí pro požár nafty v místnosti dieselového generátoru.



Obrázek 3.7 Strom událostí pro typický požární incident v budově dieselového generátoru

Pro četnost vzniku požáru a různé uzly je nutné použít vhodná data. Taková data mají být pokud možno specifická pro danou elektrárnu. V případě nedostatku dat specifických pro danou elektrárnu je však možné použít mezinárodní databáze, jako jsou nejnovější publikovaná data o elektrárnách USA. K výpočtu četnosti požáru pro jednu místnost v budově je nutné mít dodatečné váhové faktory založené na množství zdrojů vznícení, váze izolace kabelů, počtu příslušných požárních úseků a na speciálních faktorech pro zdroje vznícení.

Výstupy jsou rozlišovány do pěti kategorií škody (a), (b), (c), (d) a (e), s nejhorší kategorií definovanou jako (e) "totální škoda a šíření", ke které dojde, když všechny protipožární prostředky k zabránění šíření do přilehlých místností selžou. Všechna zařízení související s bezpečností umístěná v sousedních místnostech jsou poškozena.

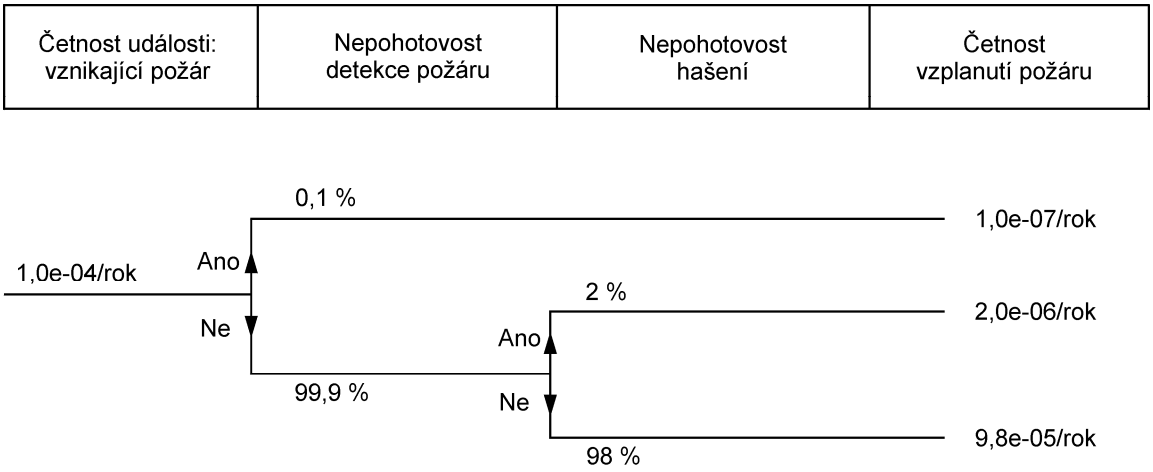
Pro každý kritický požární úsek se získají následující výsledky:

a) četnost a povaha přechodových dějů iniciovaných požárem v jaderné elektrárně;

b) seznam poškozených zařízení kategorizovaných podle kategorie škody (a) až (e);

c) četnost kategorií škody.

Na obrázku 3.8 je uvedena zjednodušená verze stromu událostí. Četnost vzplanutí požáru iniciovaného vznikajícím požárem a následnou nepohotovostí detekce požáru se odvodí vynásobením četnosti iniciační události 1,0e-4 za rok pravděpodobností nepohotovosti detekce požáru 1,0e-3 za rok. To dává výslednou četnost nežádoucí události vzplanutí požáru 1,0e-7 za rok.



Obrázek 3.8 Zjednodušený strom události pro vznik požáru

9. *Závěr*

Analýza ETA poskytuje vhodný nástroj k sestavení katalogu, vyhodnocení a rozboru možných nedostatků a k nastavení priorit i opatření pro zlepšení principů ochrany.

Na základě těchto výsledků mohou být provedeny dodatečné studie nákladů a přínosů. Stejně jako ostatní analýzy spolehlivosti patří metoda ETA k neopomenutelným nástrojům, pomocí kterých je možné naplňovat požadavky na spolehlivosti systému. To rovněž především standardizované podobě této metody.

Poděkování

Vznik tohoto příspěvku byl podpořen projektem pro institucionální rozvoj K-202 Univerzity obrany v Brně.

Použité zdroje

[1] HOLUB, R. – VINTR, Z. Spolehlivost letadlové techniky [Elektronická učebnice]. Brno: VUT v Brně, 2001.

[2] MATĚJČEK, J. Stručný přehled norem z oblasti spolehlivosti. In Úvod do spolehlivosti. Praha: Česká společnost pro jakost, 2014, s. 18–26. ISBN 978-80-02-02514-6.

[3] VINTR, M. Oborové normy ve spolehlivosti. In Mezinárodní a národní normalizace ve spolehlivosti. Praha: Česká společnost pro jakost, 2012, s. 29–36. ISBN 978-80-02-02421-7.

[4] ČSN IEC 60050/192. Mezinárodní elektrotechnický slovník – Část 192: Spolehlivost. Praha: UNMZ, 2015.

[5] ČSN EN 62502:2011. Techniky analýzy spolehlivosti – Analýza stromu událostí (ETA). Praha: ÚNMZ, 2011.

[6] Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, Rep. WASH-1400-MR (NUREG-75/014), Washington, DC, 1975.

[7] IEC 62429:2007, Reliability growth – Stress testing for early failures in unique complex systems.

[8] IEC 62508:2010, Guidance on human aspects of dependability.

ANALÝZA STROMU PORUCHOVÝCH STAVŮ – FAULT TREE ANALYSIS (FTA)

prof. Ing. Zdeněk VINTR, CSc., dr.h.c.
Univerzita obrany v Brně
e-mail: zdenek.vintr@unob.cz

1. Úvod

Metoda analýzy stromu poruchových stavů (Fautl Tree Analysis – FTA) byla poprvé použita v roce 1962 firmou Bell Telephone Laboratories v souvislosti s vývojem bezpečnosti startovacího systému rakety Minuteman. Později byla tato metoda zdokonalena ve firmě Boeing, kde také byly navrženy první výpočtové programy umožňující kvalitativní i kvantitativní vyhodnocení stromu poruchových stavů s využitím výpočetní techniky. Poměrně rychle začala tato metoda nacházet uplatnění především tam, kde předmětem analýzy byly složité technické systémy, například v jaderné energetice [1], kosmonautice [2], letectví, ve zbrojním průmyslu [3] a jiných exponovaných oborech. Postupem doby se použití metody dále rozšiřovalo i do řady jiných oblastí lidské činnosti. V technické oblasti se metoda stala jednou z nejrozšířenějších technik analýzy spolehlivosti, bezpečnosti, odhadu možných příčin poruch a hodnocení rizika a důsledků poruch složitých systémů.

Tento rychlý rozvoj použití metody se odrazil i v oblasti standardizace a v roce 1990 Mezinárodní elektrotechnická komise IEC vydala normu IEC 1025 – Fault Tree Analysis [4], ve které jsou zobecněny zkušenosti z praktického použití metody a zformulovány principy a postupy pro tvorbu a vyhodnocení stromu poruchových stavů. V roce 1993 byla tato mezinárodní norma také vydána jako česká technická norma ČSN IEC 1025 – Analýza stromu poruchových stavů [5]. Obě normy byly později zásadním způsobem přepracovaný a jsou dostupné jak ve formě mezinárodní normy [6], tak i normy české [7].

V současné době je na trhu nabízena celá řada vysoce výkonných softwarových produktů, které značně zjednodušují praktické použití metody, což vytváří předpoklady pro její další rozšiřování. Zde je však třeba zdůraznit, že i při využití nejmodernějšího programového vybavení může tuto metodu analýzy správně a efektivně použít pouze vysoce kvalifikovaný odborník, s poměrně širokým technickým rozhledem. Proto je také výuka této metody analýzy spolehlivosti zavedena na mnoha technických universitách.

2. Charakteristika, cíle a postup provádění metody

Metoda stromu poruchových stavů je deduktivní metodou a svojí povahou patří mezi speciální orientované grafy. Strom poruch má podobu logického diagramu, který znázorňuje logické vztahy mezi potenciální vrcholovou událostí (jevem), zvaným kořen stromu a mezi příčinami vzniku tohoto jevu. Příčiny mohou být v provozních podmínkách, v běžných očekávaných poruchách prvků systému, v chybách obsluhy, v náhodných diskrétních poruchách, v odchylkách (chybách) provozních parametrů prvků apod. Správně zkonstruovaný strom poruch reprezentuje (ilustruje) všechny rozumné kombinace poruch prvků a poruchových jevů, které mohou vést ke vzniku specifikovaného vrcholového jevu.

Výhodou techniky stromu poruch je hlavně to, že donutí tvůrce stromu (analytika poruchy) představit si a znázornit (přesně popsat) logiku rozvoje poruchy v systému, odhalit všechny kauzální vazby mezi prvky a poruchou a to až do zvolené úrovně složitosti systému. V důsledku toho většina slabých míst v systému může být včas odhalena a to především již v etapě návrhu a vývoje systému.

Strom poruch je deduktivní metoda. Rozvíjí se od vrcholové události k dalším jevům nižší úrovně, přičemž se posuzují možné příčiny vzniku nadřazeného poruchového jevu. Posuzuje se, jaké by mohly být příčiny poruchového jevu. Popis příčin poruchového jevu na každé úrovni by měl odpovídat na otázky: Co? Kde? Kdy? a Proč?

V současné době se technika stromu poruch stále zdokonaluje a zdokonalila se již tak, že umožňuje též analýzu dynamických systémů, jako regulovaných systémů, systémů s funkcemi ovládanými spínači na povel (na vyžádání), systémů podílejících se na různých fázích činnosti systémů, systémů podřízených složitým strategiím údržby apod. Vlastní realizace metody představuje provedení jisté logické posloupnosti kroků, kterou lze rozdělit do pěti základních částí:

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

Analýza stromu poruch poruchových stavů může být provedena buď kvalitativně, kvantitativně nebo obojím způsobem v závislosti na cílech analýzy. Výstupem z analýzy tedy muže být:

- Soupis (přehled) možných kombinací faktorů provozních podmínek, nebo podmínek prostředí, chyb lidského faktoru, normálních provozních poruch prvků takových, které by mohly jednotlivě nebo v kombinaci vést ke vzniku nežádoucí vrcholové události;
- Pravděpodobnost s jakou nežádoucí vrcholová událost může v provozu nastat během specifikovaného časového intervalu.

3. Přípravná část analýzy

Základním předpokladem pro úspěšné provedení analýzy je dokonalá znalost systému, jeho funkcí a podmínek jeho použití. Výchozím krokem řešení tedy musí být shromáždění všech nezbytných informací o systému, které umožní vlastní provedení analýzy. Jedná se především o následující informace:

- konstrukční uspořádání systému;
- popis funkcí systému;
- vymezení rozhraní, které systém odděluje od okolí a charakter interakcí systému s okolím;
- předpokládané provozní režimy systému;
- předpokládaný systém údržby;
- vliv lidského faktoru na činnost systému apod.

Při shromažďování těchto informací se vychází z dostupné technické dokumentace, např. výkresů, specifikací, technických popisů, provozních příruček apod. Analýze stromu

poruchových stavů také často předchází provedení analýzy spolehlivosti systému jinými metodami např. metodou FMEA nebo FMECA. V takovém případě je výhodné využít při shromažďování podkladů i výsledků těchto analýz.

Dalším krokem v přípravné části analýzy je definování vrcholové události, která bude předmětem analýzy. Takovou událostí obvykle bývá:

- událost, která může znamenat začátek vzniku nebo existenci nebezpečných podmínek;
- událost představující neschopnost systému plnit požadované funkce.

Za vrcholovou událost také může být zvolen provozuschopný stav systému. V takovém případě se nezkoumají příčiny selhání funkce systému, ale naopak podmínky, které jsou nutné pro realizaci požadované funkce systému. Z praktického hlediska je však výhodnější modelovat poruchový stav, protože to zpravidla vede ke snadnější kvantitativní a kvalitativní analýze. Vrcholová událost musí být definována (vymezena) jasně a jednoznačně. V případě, že tomu tak není, analýza je omezena ve svých výstupech. Protože cílem celé analýzy je nalezení všech možných příčin vrcholové události, je třeba vrcholovou událost definovat tak aby tento cíl byl splnitelný.

Definice vrcholové události proto musí jednoznačně popisovat událost, přesně vymezovat jakého systému nebo jeho části se týká a v jaké fázi provozu a za jakých podmínek nastala. Příliš obecná definice události (například „motorové vozidlo nelze zastavit“) není vhodná, protože může vést k nejasným závěrům se spekulativním charakterem. Naopak příliš specifické definování události může nežádoucím způsobem omezit rozsah analýzy a vést k opomenutí některých důležitých prvků systému či systémových vazeb. Například definice „vozidlo nelze zastavit pro poruchu hlavního brzdového válce“ již dopředu z analýzy vylučuje další prvky brzdového systému vozidla, které ovlivňují jeho schopnost brzdit.

Vrcholová událost musí být definována takovým způsobem, aby vždy bylo možné, s ohledem na uvažovaný stav systému a jeho prvků, jednoznačně určit zda by vrcholová událost mohla nastat či ne. Z tohoto důvodu je také vhodné, pokud to charakter systému a vrcholové události umožňuje, vrcholový jev specifikovat kvantitativními ukazateli.

Na závěr je třeba zdůraznit, že ke každému systému můžeme definovat celou řadu vrcholových událostí. Charakter popisované metody však neumožňuje analyzovat více vrcholových událostí současně. Pro každou jednotlivou vrcholovou událost je třeba vybudovat samostatný strom poruchových stavů a pro případný jiný jev celou analýzu opakovat.

4. Tvorba stromu poruchových stavů

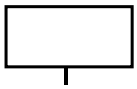
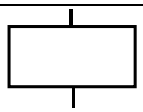
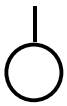
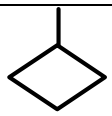
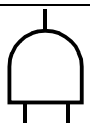
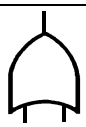
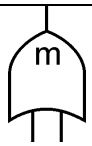
Tvorba stromu poruchových stavů začíná od vrcholové události. Další rozvoj stromu se děje postupnou analýzou kauzálního vztahu mezi vrcholovou událostí a jejími příčinami. Při této analýze hledáme odpověď na dvě základní otázky:

- Co by mohlo být příčinou (příčinami) vrcholové události?
- Jaká je logická vazba mezi vrcholovou událostí a jejími příčinami?

Cílem analýzy příčin vrcholového jevu je tedy identifikace všech událostí, které „by mohly být“ bezprostředními příčinami vrcholové události. Bezprostředními příčinami zde přitom rozumíme všechny bezprostředně nutné a dostačující příčiny vrcholové události. Výsledek této dílčí analýzy potom zaznamenáváme s využitím grafických značek, kdy vzájemnou logickou vazbu mezi událostí a jejími bezprostředními příčinami vyjadřujeme

pomocí tzv. hradel. Přehled vybraných značek používaných při tvorbě stromu poruch je uveden v *Tab. 4.1*.

Tab. 4.1 Často používané značky pro strom poruchových stavů

Doporučená značka	Název	Název a popis
	TOP EVENT (vrcholová událost)	Blok s názvem nebo popisem vrcholové události.
		Blok s názvem nebo popisem události (jevu), případně s uvedením pravděpodobnosti výskytu (pokud se to požaduje).
	BASIC EVENT (základní událost)	Událost na nejnižší úrovni, pro kterou jsou k dispozici pravděpodobnosti výskytu nebo informace o bezporuchovosti
	UNDEVELOPED EVENT (nerozvíjená událost)	Primární událost, která reprezentuje část systému, která dosud nebyla rozvíjena
		Přenos do – událost definovaná kdekoliv jinde ve stromu poruch.
		Přenos ven – opakovaná událost použitá kdekoli jinde ve stromu poruch.
	Hradlo AND	Hradlo AND (a) – událost nastane pouze tehdy, když současně nastanou všechny vstupní události.
	Hradlo OR	Hradlo OR (nebo) – událost nastane tehdy, když nastane kterákoliv vstupní událost, nebo jejich libovolná kombinace.
	Hradlo MAJORITY VOTE (majoritní hradlo)	Zálohovaná struktura – událost nastane tehdy, jestliže nastane minimálně m z n vstupních událostí.

V dalším postupu je třeba posoudit, zda bezprostřední příčiny vrcholové události představují tzv. základní (primární) události či ne. Základní událostí zde přitom rozumíme takovou událost, která se již dále nerozvíjí, to znamená, že její nastoupení nemůže být zapříčiněno žádnou jinou uvažovanou událostí v analyzovaném systému. Základní událost je obvykle vztažena k jednomu konkrétnímu prvku systému. Co bude při analýze považováno za základní událost je určováno požadovanou hloubkou analýzy. V některých případech může základní událost představovat poruchový stav jednotlivé součásti, jindy celého agregátu, podskupiny či subsystému. Jestliže se při hodnocení příčiny vrcholové události ukáže, že se

jedná o základní událost, zakreslí se příslušnou značkou do stromu poruch a dále se nerozvíjí. Jestliže se nejedná o základní událost, je v zásadě možný trojí postup:

- událost dále rozvíjet;
- označit událost jako nerozvíjenou událost (nemáme dostatek informací, nebo na dané úrovni rozpracovanosti projektu nebo členění systému to není možné nebo nutné);
- označit událost jako událost analyzovanou jinde a další rozvoj události v řešeném stromu neprovádět a událost analyzovat jinde v samostatném stromu poruch.

Zvolený postup vždy odpovídajícím způsobem zakreslíme do vytvářeného stromu poruch. V případě, že je některá z bezprostředních příčin vrcholové události dále rozvíjena, analyzují se její bezprostřední příčiny podobným způsobem, jako to bylo naznačeno u vrcholové události a výsledky tohoto kroku opět zakreslit do stromu poruch. Tento proces postupně úroveň po úrovni opakujeme (aplikujeme) pokud nedospějeme k událostem na nižší úrovni členění systému, tedy k základním událostem (případně k událostem nerozvíjeným a analyzovaným jinde). Tím je tvorba stromu poruchových stavů skončena.

V konstrukci stromu poruch se často používají tak zvané přenosy. Objevuje-li se na více místech stromu stejná dále rozvíjená událost, postačuje její vyřešení pouze na jednom z míst výskytu. Informace z tohoto řešení se potom na další místa výskytu události přenesou pomocí příslušných značek.

Každou událost ve stromu poruch je nutné jednoznačně identifikovat a označit tak, aby byly zřejmé vzájemné vztahy mezi stromem poruch a vyšetřovaným systémem. Jestliže se ve stromu poruch objevuje více různých událostí (poruchových stavů) vztahujících se k jednomu prvku systému, musí se tyto události označit tak, aby je bylo možné vzájemně rozlišit a přitom bylo vždy jasné, že se jedná o skupinu událostí, která se vztahuje k jednomu stejnému objektu. Jestliže se určitá událost, týkající se jednoho objektu objevuje na různých místech stromu poruch, případně v různých stromech poruch, je nutné všechny tyto výskyty označit stejně. Samozřejmě pokud se stejné události objevují na různých objektech, nesmí mít stejné označení.

V konečném stádiu vývoje je strom poruch diagram, ve kterém jsou všechny události spojené logickými hradly, přičemž každé hradlo má jednu výstupní událost a jednu či více vstupních událostí. Příklad finální struktury stromu poruchových stavů je uveden na *Obr. 4.1*. Z obrázku je také patrné použití různých značek používaných při vytváření stromu poruch.

5. Kvalitativní analýza stromu poruchových stavů

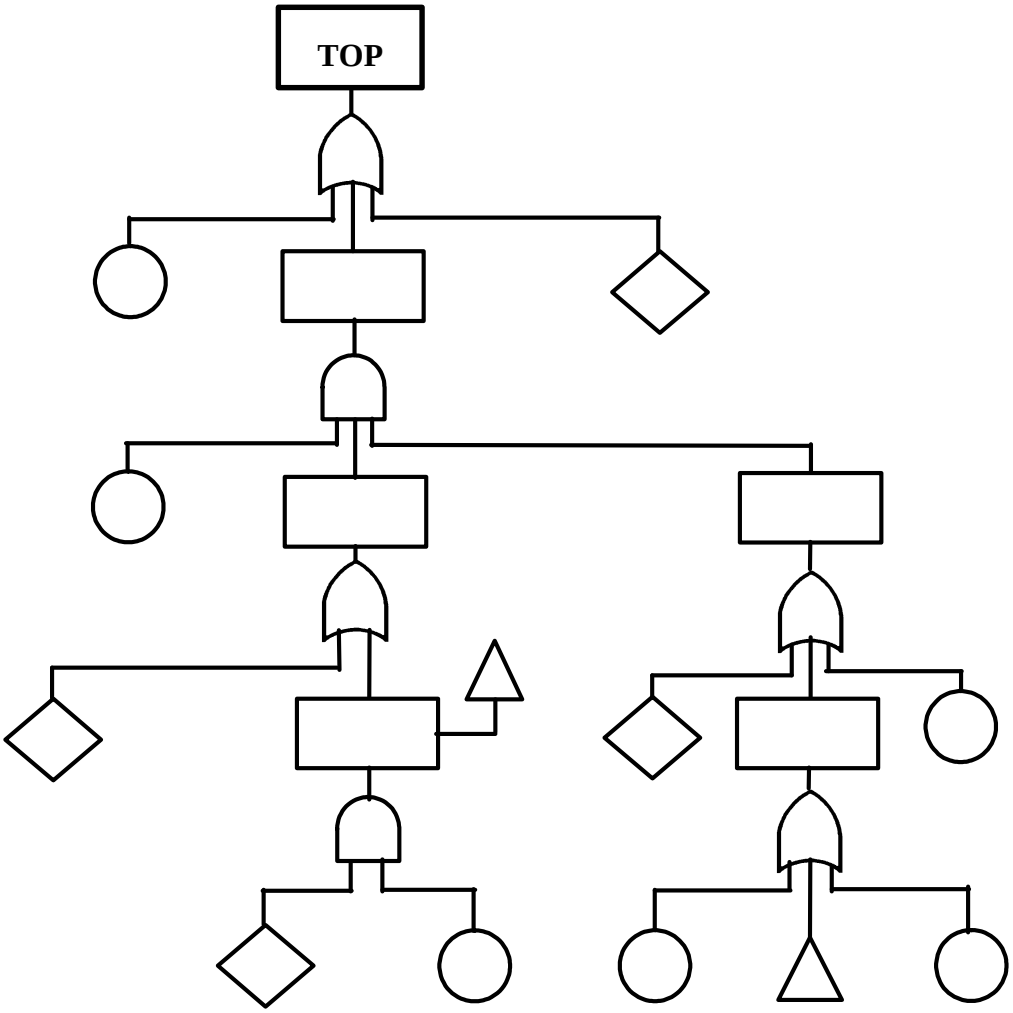
Cílem kvalitativní analýzy u stromu poruch je nalezení všech rozumně možných kombinací faktorů provozních podmínek, podmínek prostředí, chyb lidského faktoru a poruch prvků systému, které by mohly vést ke vzniku vrcholové události, zpravidla události nežádoucí (kritická porucha systému).

5.1 Kritické řezy stromu poruchových stavů

Z formálního hlediska je cílem analýzy stromu poruch nalezení množiny všech minimálních kritických řezů. Kritickým řezem stromu poruchových stavů přitom rozumíme takovou konečnou množinu základních, dále nerozvíjených a jinde analyzovaných událostí

(dále tyto události budeme souhrnně označovat jako události elementární) která, nastane-li současně, vede ke vzniku vrcholové události.

Minimálním kritickým řezem (MKR) stromu poruchových stavů dále rozumíme takovou konečnou množinu elementárních událostí, která je sama kritickým řezem, ale současně žádná její vlastní podmnožina kritickým řezem není.



Obr. 4.1 Příklad finální struktury stromu poruchových stavů

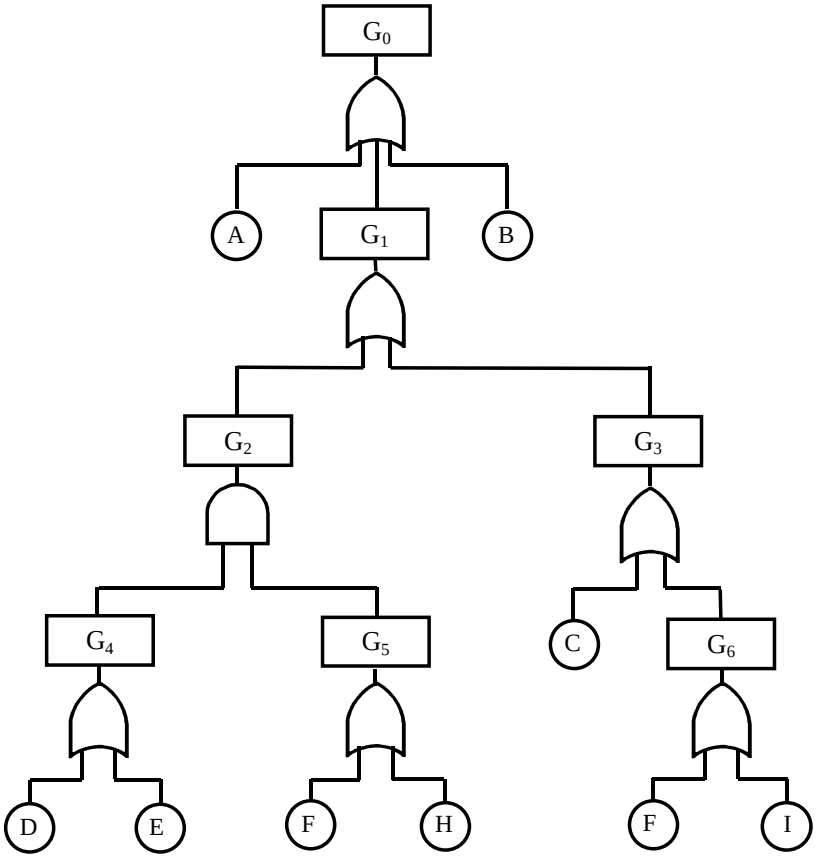
Jedním z hlavních dílčích cílů při řešení stromu poruch je nalezení úplné množiny minimálních kritických řezů (prakticky však množiny všech MKR do zvoleného „řádu“). To potom umožňuje analytikovi transformovat složitě strukturovanou logiku všech variant poruchy systému do relativně jednoduchého logického vztahu, který lze řešit standardními výpočtovými postupy.

Základní metodou pro určení množiny minimálních kritických řezů je Booleovská redukce, která je založena na jevovém popisu logických vazeb vyjádřených stromem poruch. Metoda je přímo použitelná i na stromy poruch, kde se stejné události objevují ve více větvích stromu. Metodu však nelze použít v případě, kdy je vrcholová událost závislá na časování

nebo posloupnosti jevů. Náročnost praktického použití metody rychle roste s počtem elementárních jevů ve stromu poruch.

Metoda spočívá v postupném vyjadřování logiky vrcholové události jako kombinace jednotlivých událostí vyjádřených ve stromu poruch. V prvním kroku vyjádříme vrcholovou událost jako logickou kombinaci událostí, které jsou bezprostřední příčinou vrcholové události. V dalších krocích stejným způsobem popisujeme události na nižších úrovních stromu poruch a takto postupujeme, dokud vrcholová událost není vyjádřena jako logická kombinace elementárních jevů.

Výsledný logický výraz potom s využitím pravidel Booleovké algebry upravíme tak, aby vyjadřoval prosté sjednocení průniků elementárních jevů. Jednotlivé průniky elementárních jevů v tomto logickém výraze potom představují minimální kritické řezy stromu poruch, přičemž všechny průniky jevů, které jsou v rovnici sjednocovány, představují množinu kritických řezů. Pokud z této množiny kritických řezů eliminujeme ty řezy, které sami o sobě nejsou minimálními kritickými řezy, obdržíme množinu všech minimálních kritických řezů.



Obr. 4.2 Příklad stromu poruchových stavů

Podrobněji si celý postup ukážeme na příkladu. Mějme strom poruchových stavů vyjádřený na *Obr. 4.2*. Nejdříve vyjádříme vrcholovou událost jako logickou kombinaci bezprostředních příčin této události. Pro zjednodušení zápisů zde budeme používat na místo symbolů pro průnik a sjednocení jevů znaménka „krát“ a „plus“:

$$G_0 = A + B + G_1$$

Potom do rovnice za jev G_1 dosadíme logický výraz vyjadřující tento jev jako logickou kombinaci jeho bezprostředních příčin a vztah tímto způsobem dále upravujeme, dokud logický výraz není tvořen výhradně elementárními jevy:

$$G_0 = A + B + (G_2 + G_3)$$

$$G_0 = A + B + [G_4 \cdot G_5 + (C + G_6)]$$

$$G_0 = A + B + \{(D + E) \cdot (F + H) + [C + (F + I)]\}$$

Výsledný logický výraz potom upravíme tak aby vyjadřoval prosté sjednocení průniků jevů:

$$G_0 = A + B + C + F + I + D \cdot F + D \cdot H + E \cdot F + E \cdot H$$

Tento výraz můžeme dále zjednodušit, uvážíme-li podstatu operace sjednocení jevů, ze které vyplývá že:

$$D \cdot F + E \cdot F + F = F$$

Výsledný logický výraz potom můžeme přepsat do tvaru:

$$G_0 = A + B + C + F + I + D \cdot H + E \cdot H$$

Pro řešený strom poruch jsme tak obdrželi následující soustavu sedmi minimálních kritických řezů:

ΣMKR = {A}, {B}, {C}, {F}, {I}, {D,H}, {E,H}

Výše presentovaný postup je vcelku jednoduchý a vede k jednoznačnému určení všech minimálních kritických řezů, ale při vysokých počtech elementárních jevů se stává ručně obtížně zvládnutelný. Z tohoto důvodu byla vyvinuta celá řada různých metod vyhledávání minimálních kritických řezů založených na různých logických postupech, které například uvažují jen kritické řezy do určitého řádu (viz následující kapitola) nebo přijímají jiné zjednodušující předpoklady. Tyto metody jsou obvykle založeny na snadno programovatelných algoritmech, které umožňují řešení stromů poruch s využitím počítačů.

K ručnímu řešení dnes přistupujeme jen v případě jednoduchých stromů poruch (obvykle jen do několika desítek elementárních jevů) a jinak využíváme speciální softwarové produkty určené k řešení stromů poruch, kterých je na současném trhu poměrně široká nabídka.

5.2 Hodnocení závažnosti minimálních kritických řezů

Kvalitativní posouzení stromu poruch může být provedeno také na základě rozboru minimálních kritických řezů při uvážení různých kritérií závažnosti.

Prvním důležitým kritériem vyjadřujícím závažnost každého MKR je počet elementárních jevů řezu. Počet různých elementárních jevů v MKR se nazývá řád řezu. MKR prvního řádu je obvykle kritičtější (závažnější) než řezy druhého nebo vyšších řádů. Máme-li řez, sestávající pouze z jednoho elementárního jevu, potom vrcholová událost může nastat již tehdy, nastane-li samostatně tento jediný elementární jev. Sestává-li MKR ze dvou či více elementárních jevů, potom i vrcholová událost nastane až tehdy, nastoupí-li současně všechny jevy řezu současně, tedy dojde-li k jejich průniku.

Protože pravděpodobnost nastoupení průniku jevů je dána součinem pravděpodobností jednotlivých jevů, logicky platí, že čím více elementárních jevů je současně třeba k nastoupení vrcholové události, tím je jeho pravděpodobnost menší.

Jiným důležitým kritériem kvalitativního posouzení závažnosti MKR je typ uvažovaných elementárních jevů. Ze zkušeností vyplývá, že obecně můžeme elementární jevy podle jejich typu uspořádat (s ohledem na závažnost jejich důsledků a četnost výskytu) do následujícího pořadí:

- chyby lidského faktoru;
- poruchy aktivních prvků;
- poruchy pasivních prvků.

Pořadí je založeno na zkušenosti, že chyby lidského faktoru (selhání člověka) se vyskytují častěji než poruchy aktivních prvků a že aktivní prvky jsou náchylnější ke vzniku poruch než prvky pasivní. Např. čerpadlo, které je trvale v činnosti je vystaveno podmínkám generujícím jeho poruchu častěji než čerpadlo záložní, činné jen příležitostně, na požádání (samozřejmě pokud je udržované a pravidelně kontrolované).

Uvážíme-li toto pořadí závažnosti elementárních jevů, můžeme podobně sestavit pořadí kritičnosti i pro MKR 2. řádu, tj. řezy tvořené současně dvěma elementárními jevy:

a) chyba lidského faktoru + chyba lidského faktoru;
b) chyba lidského faktoru + porucha aktivního prvku;
c) chyba lidského faktoru + porucha pasivního prvku;
d) porucha aktivního prvku + porucha aktivního prvku;
e) porucha aktivního prvku + porucha pasivního prvku;
f) porucha pasivního prvku + porucha pasivního prvku.

Obdobně bychom mohli posoudit i závažnost minimálních kritických řezů vyšších řádů při znalosti charakteru elementárních jevů, které MKR tvoří.

Výše popsaná kritéria hodnocení závažnosti MKR mohou významně usnadnit celý proces kvalitativního hodnocení stromu poruch a následně i jeho hodnocení kvantitativní. Na základě těchto kritérií totiž můžeme kvalifikovaně rozhodnout o tom, jak podrobně je třeba analýzu provést bez toho, aby byla ohrožena věrohodnost výsledků.

Například se doporučuje vyhledání souboru MKR jen do určitého zvoleného řádu, (obvykle do třetího, případně čtvrtého). MKR vyšších řádů totiž již svojí nízkou pravděpodobností vzniku nepřispívají ke zpřesnění výsledků analýzy a z řešení se proto vylučují. Těchto principů často využívají moderní softwarové produkty určené k řešení rozsáhlých stromů poruch s rozsahem tisíc a více prvků a logických hradel.

6. Kvantitativní analýza stromu poruchových stavů

Pokud jsou známy parametry spolehlivosti elementárních jevů (vstupní údaje do stromu) je možné provést kvantitativní analýzu stromu poruch. Cílem této analýzy může být určení celé řady ukazatelů charakterizujících vrcholovou událost. Dále je uveden přehled vybraných ukazatelů, které při kvalitativní analýze stromu poruch mohou být určovány:

- pravděpodobnost že vrcholová událost nastane v zadaném intervalu provozu systému;
- pravděpodobnost že vrcholová událost nenastane v zadaném intervalu provozu systému;
- střední doba do prvního nastoupení vrcholové události;
- střední počet nastoupení vrcholové události v zadaném intervalu provozu systému a pod.

V dalším výkladu se zaměříme pouze na problematiku stanovení pravděpodobnosti vrcholové události. Určení dalších ukazatelů se realizuje analogickými postupy.

Hned na úvod je třeba konstatovat, že metody výpočtů stromu poruch jsou většinou velice komplikované (v závislosti na složitosti stromu poruch) a jejich ruční provedení přichází do úvahy pouze ve velice jednoduchých případech.

Metody výpočtů byly a stále jsou předmětem rozsáhlých výzkumných prací, které jsou dnes realizovány především u specializovaných softwarových firem, které se zabývají vývojem a produkcí programového vybavení v oblasti spolehlivosti.

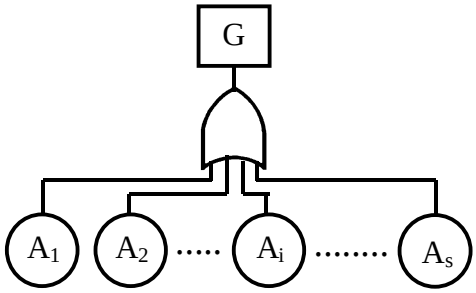
Nejčastěji jsou při výpočtech stromu poruch používány následující tři metody:

- metoda přímého výpočtu;
- metoda minimálních kritických řezů;
- simulační metody (Monte Carlo).

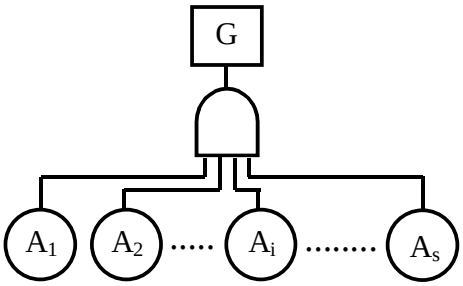
Simulační metody výpočtu jsou výhradně využívány při řešení stromů poruch na počítačích, kde je výpočet automatizován s využitím často velice komplikovaných algoritmů, jejichž popis přesahuje rámec tohoto článku. Z těchto důvodu zde simulační metody nebudou dále popisovány.

6.1 Metoda přímého výpočtu

Hned na úvod je třeba zdůraznit, že tato metoda je použitelná pouze pro stromy poruchových stavů, ve kterých se každý elementární jev objevuje pouze jednou. Při výpočtu postupujeme tak, že s využitím známých vtahů postupně určujeme pravděpodobnost jevů od nejnižší úrovně až po vrcholovou událost. Postupně zespodu (od listů) procházíme všechna logická hradla stromu poruch a podle jejich typu určujeme pravděpodobnost nastoupení jevů, které jsou těmito hradly logicky definovány. Například mějme jev G, složený s elementárních jevů A_i, které jsou jeho bezprostřední příčinou. V případě použití logického hradla typu OR (viz *Obr. 4.3*) se pravděpodobnost jevu G určí podle rovnice (1). V případě použití hradla AND (viz *Obr. 4.4*) se pravděpodobnost jevu G určí podle rovnice (2).



Obr. 4.3 Logické hradlo OR

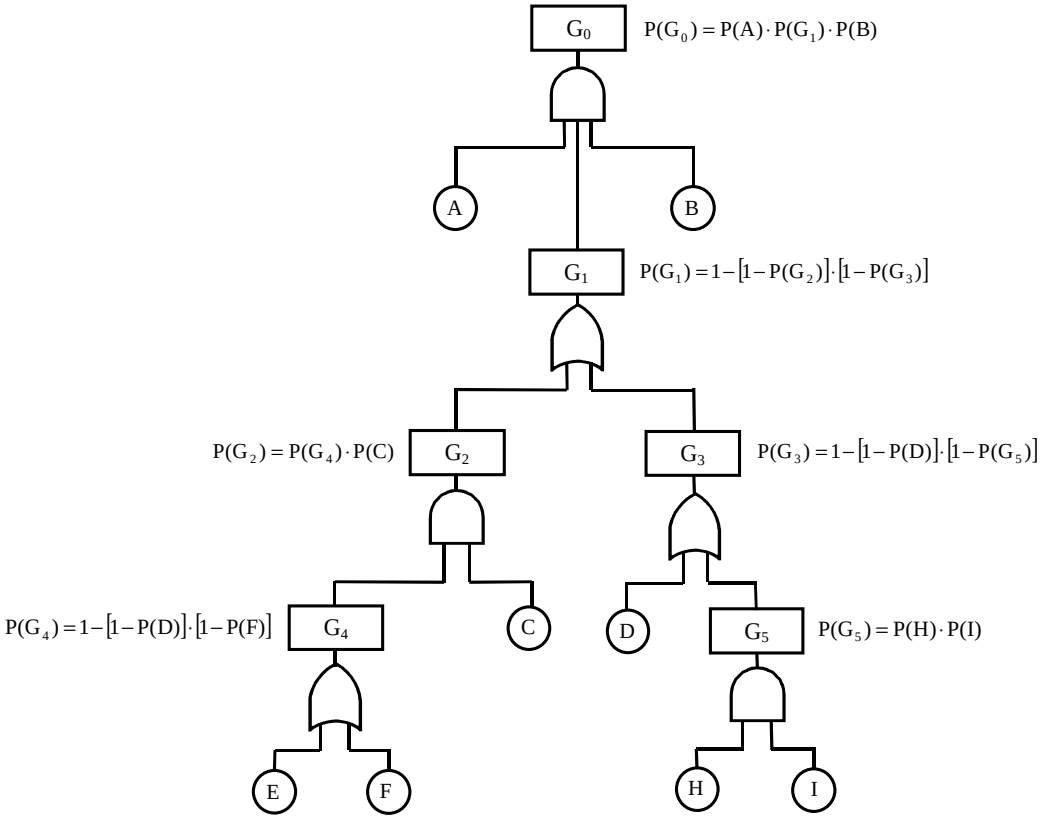


Obr. 4.4 Logické hradlo AND

$$P(G) = 1 - \prod_{i=1}^{i=s} [1 - P(A_i)] \tag{1}$$

$$P(G) = \prod_{i=1}^{i=s} P(A_i) \tag{2}$$

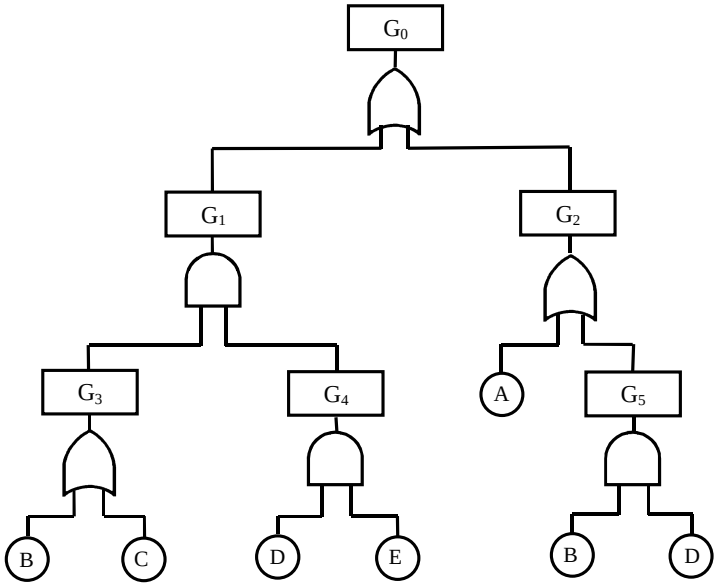
Postupnou aplikací výpočtového vztahu (1) respektive (2) tak můžeme určit pravděpodobnost všech neelementárních jevů, které se ve stromu poruch objevují včetně pravděpodobnosti vrcholové události. Příklad výpočtu stromu poruchových stavů přímou metodou je naznačen na *Obr. 4.5*.



Obr. 4.5 Příklad výpočtu stromu poruchových stavů přímou metodou

6.2 Metoda minimálních kritických řezů

Metoda je založena na předpokladu znalosti množiny všech minimálních kritických řezů stromu poruch. Jestliže je tato množina známa může být logika příslušného stromu poruchových stavů vyjádřena logickým vztahem, který představuje prosté sjednocení průniků jednotlivých jevů. Známými postupy potom lze spočítat pravděpodobnost nastoupení vrchového jevu s využitím tohoto logického výrazu. Tento postup bude dále demonstrován na ilustrativním příkladu.



Obr. 4.6 Ilustrativní příklad stromu poruchových stavů

Mějme strom poruchových stavů znázorněný na *Obr. 4.6*. Nejdříve vyšetříme minimální kritické řezy stromu. V prvním kroku si vyjádříme vrcholovou událost jako logickou kombinaci elementárních jevů:

$$G_0 = G_1 + G_2 = G_3 \cdot G_4 + A + G_5 = (B + C) \cdot D \cdot E + A + B \cdot D$$

Dále tuto rovnici upravíme tak aby představovala prosté sjednocení průniků elementárních jevů:

$$G_0 = B \cdot D \cdot E + C \cdot D \cdot E + A + B \cdot D$$

A s využitím adsorbčního zákona můžeme rovnici dále upravit do konečného tvaru:

$$G_0 = A + B \cdot D + C \cdot D \cdot E \qquad (3)$$

Řešený strom poruchových stavů tedy má tři minimální kritické řezy:

ΣMKR = {A}, {B,D}, {C,D,E}

Další postup se soustředí na určení pravděpodobnosti logického výrazu vyjádřeného rovnicí (3). To je možné provést mnoha způsoby [8]. Zde bude naznačen postup využívající převodu logického výrazu do disjunktního tvaru:

$$G_0 = A + B \cdot D + C \cdot D \cdot E = A + \overline{A} \cdot \left(B \cdot D + \overline{B \cdot D} \cdot C \cdot D \cdot E \right) =$$
$$= A + \overline{A} \cdot \left[B \cdot D + (\overline{B} + B \cdot \overline{D}) \cdot C \cdot D \cdot E \right] = A + \overline{A} \cdot B \cdot D + \overline{A} \cdot \overline{B} \cdot C \cdot D \cdot E$$

Jakmile je výraz převeden do disjunktního tvaru můžeme snadno určit jeho pravděpodobnost:

$$P(G_0) = P(A) + \left[1 - P(A)\right] \cdot P(B) \cdot P(D) + \left[1 - P(A)\right] \cdot \left[1 - P(B)\right] \cdot P(C) \cdot P(D) \cdot P(E)$$

Závěrem je třeba k metodě minimálních kritických řezů poznamenat, že možnost jejího použití je bezprostředně závislá na možnosti vlastního určení minimálních kritických řezů. To může být při velkém počtu elementárních jevů značný problém. Proto se zde často využívají různá zjednodušení, například se analýza omezí jen na kritické řezy do určitého řádu apod. Ruční aplikace této metody je možná (a racionální) jen při nízkých počtech elementárních jevů ve stromu poruch.

Naznačené principy metody však využívá řada softwarových produktů, které v kombinaci s výkonnou výpočetní technikou umožňují relativně rychlé řešení i poměrně rozsáhlých stromů poruchových stavů.

7. Vyhodnocení analýzy

Výsledky analýzy stromu poruchových stavů je vhodné shrnout do zprávy, která by měla zahrnovat alespoň:

- cíl a předmět analýzy;
- přehled použité technické dokumentace;
- popis systému (konstrukční popis, popis funkcí, vymezení hranic systému);
- uvažované provozní režimy a podmínky prostředí;
- uvažované aspekty působení lidského činitele;
- definici vrcholové události (událostí);
- vytvořený strom (stromy) poruchových stavů;
- výsledky kvalitativní analýzy (přehled uvažovaných kritických řezů a hodnocení jejich závažnosti, identifikace kritických prvků);
- výsledky kvantitativní analýzy (číselné hodnoty požadovaných ukazatelů);
- závěry analýzy (vyjádření zda systém splňuje stanovené požadavky, případně návrhy na změnu konstrukce systému, podmínek provozu či prostředí).

8. Závěr

Z výše uvedeného je zjevné, že metoda stromu poruchových stavů – FTA je systematickou a účelnou analýzou v rámci prediktivních i provozních procesů posuzování bezporuchovosti a bezpečnosti. Díky své standardizované podobě získala pevné místo mezi obvykle volenými a používanými technikami.

Poděkování

Vznik tohoto příspěvku byl podpořen projektem pro institucionální rozvoj K-202 Univerzity obrany v Brně.

Použitá literatura

[1] US Nuclear Regulatory Commission. *NUREG-0492 - Fault Tree Handbook*. Washington: NRC, 1981.

[2] NASA Office of Safety and Mission Assurance. *Fault Tree Handbook for Aerospace Applications*. Washington: NASA, 2002.

[3] U.S. Army Material Command. *Engineering Design (handbook) – Development Guide for Reliability*. Alexandria: U.S. Army Material Command, 1976.

[4] IEC 1025 *Fault tree analysis (FTA).* Geneva: International Electrotechnical Commission, 1990.

[5] ČSN IEC 1025 *Analýza stromu poruchových stavů*. Praha: ČNI, 1994.

[6] IEC 61025 *Fault tree analysis (FTA).* Geneva: International Electrotechnical Commission, 2006.

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

[8] HOLUB, R., VINTR, Z. *Základy spolehlivosti*. 1. vyd. Brno: Vojenská akademie v Brně, 2002.