ANALÝZA SPOLEHLIVOSTI SYSTÉMU S VYUŽITÍM STROMU PORUCHOVÝCH STAVŮ

Jiří Stodola[1]
[1]Univerzita obrany Brno, jiri.stodola@unob.cz

SYSTEM RELIABILITY ANALYSIS USING A FAULT TREE

Abstract: *Fault Tree Analysis (FTA) is an effective reliability analysis technique used to identify factors that can lead to an undesirable so-called peak event (fault, failure). Causal factors are identified deductively, are organized in a logical manner, and are represented using a tree diagram that shows the causal factors and their logical relationship to the peak event. Factors in a fault tree can include events related to hardware component failures, human errors, or any other sub-events that lead to an undesirable event. A fault tree can be used qualitatively to identify possible causes and paths leading to a failure, or quantitatively to calculate the probability of a peak event. FTA can be used in the system design phase to identify possible causes of failures and to choose between different design options. It can be used in the operation phase to identify how a significant failure can occur and to determine the importance of different paths leading to a peak event. FTA can also be used to analyze a failure that has occurred, with the aim of graphically illustrating the way in which various events came together to cause the failure.*

Key words: *reliability, safety, solution methods, fault trees*

ÚVOD

Spolehlivostní analýzy velmi často využívají metodu stromu poruchových stavů FTA (Fault Tree Analysis) pro posuzování spolehlivosti a bezpečnosti komplexních technických systémů. Jedná se o deduktivní metodu umožňující zkoumat logické vztahy mezi nežádoucí vrcholovou událostí, což je porucha (selhání) systému a příčinami, které k této poruše vedou [1]. Metoda má relativně dlouhou historii, byla vytvořena v 60. letech 20. století v USA při analýzách raketových systémů. Později metodu zdokonalila společnost Boeing, která vyvinula první software pro kvalitativní a kvantitativní vyhodnocení stromů poruch v souvislosti s analýzami bezpečnosti letecké techniky. FTA je v současné době široce rozšířena a využívána v náročných oborech, jako jsou jaderná energetika, kosmonautika, letectví nebo zbrojní průmysl aj. Svým charakterem patří FTA mezi orientované grafy mající speciální vlastnosti (kořen, listy, větve, hrany, směr aj.), podrobnosti např. v [2] aj. V současné době je FTA standardizována mezinárodní normou IEC 61025, resp. ČSN EN 61025 [3]. V praxi se standardně využívá při návrhu a rovněž v průběhu celého životního cyklu složitých systémů, k identifikaci potenciálních příčin poruch, odhadu pravděpodobnosti kritických selhání, posouzení spolehlivosti, bezpečnosti a rizik [4-6]. Cílem tohoto příspěvku je velmi stručně představit metodiku FTA (charakteristiku, tvorbu stromu poruch, metody kvalitativní a kvantitativní analýzy, praktické

užití), což lze s jistým zjednodušením ukázat na praktickém příkladu analýzy selhání brzd vozidla Land Rover Defender.

TEORETICKÁ VÝCHODISKA METODY FTA

FTA je deduktivní metoda analýzy (shora-dolů) spolehlivosti, bezpečnosti a rizik. Základem je definování vrcholové události (poruchy, selhání) a systematická analýza možných příčin, které k této události mohly vést. Výsledkem je strom poruchových stavů, který graficky znázorňuje logické vazby mezi vrcholovou událostí a jejími základními příčinami. FTA využívá nejčastěji statické logické hradlo (logický člen) OR (≥ 1), které vyjadřuje situace, kdy pouze jedna jakákoliv událost vede k vrcholové události. Toto hradlo reprezentuje logický součet, jehož výstup je pravdivý, pokud bude alespoň jeden z jeho vstupů pravdivý. FTA dále využívá statické logické hradlo (logický člen) AND (&), které znázorňuje současné spolupůsobení mnoha vlivů. Používá se tam, kde je třeba kombinace chyb, aby došlo k poruše. Toto hradlo reprezentuje logický součin, jehož výstup je pravdivý, jestliže jsou pravdivé všechny jeho vstupy. Samozřejmě kromě základních logických prvků jsou definovány další symboly, podmíněné a přenosové, např. pro členění stromu do dílčích stromů aj. Jedná se o další hradla (K/N neboli NAND, NOT, OR, NOR, XOR, Priority AND, INHIBIT, SEQ, aj.), podrobnosti v [1-2]. Např. ve srovnání s metodou FMEA (analýza způsobů a důsledků poruch), která zkoumá možné následky jednotlivých poruch prvků zdola-nahoru, umožňuje FTA analyzovat vícenásobné kombinace poruch s využitím booleovských výpočtů [1]. Booleovské výpočty (algebra) jsou základním nástrojem pro práci s pravdivostními hodnotami (pravda/nepravda, 1/0) a tvoří základy pro užití logických operací uvedených výše. Hlavní výhodou FTA je skutečnost, že znázorňuje logiku rozvoje poruchy, odhaluje kauzální vazby mezi prvky systému a poruchou pro příslušnou úroveň složitosti systému. Vlastní praktickou realizaci metod FTA lze rozčlenit na následující základní kroky:

1) Přípravná fáze – sběr informací, což zahrnuje detailní znalost analyzovaného systému a jeho funkcí. Analytik nejprve vymezuje systémové hranice, popíše funkce systému a dílčích subsystémů, identifikuje možné režimy selhání, poruchové stavy jeho prvků, zohlední provozní podmínky a vlivy okolí.
2) Definice vrcholové události, která musí být zcela přesná a jednoznačná; znamená to analýzu nežádoucího stavu a jeho exaktní definici (ohrožení bezpečnosti, poškození životního prostředí, ztráta funkce systému, porucha rozhodujícího subsystému, pokles důležité funkce pod určitou mez aj.). Pokud je to možné, je potřebné událost přesně kvantifikovat (např. pokles výkonu motoru pod určitou mez, porucha hlavního brzdového válce aj.) [3-4].
3) Konstrukce stromu poruchových stavů začíná definováním vrcholové události, následně postupuje směrem dolů hledáním logických vazeb mezi příčinami a událostí. Příčiny vrcholové události se zapisují do stromu pomocí grafických symbolů a propojují je logickými hradly. Každá událost je analyzována z hlediska toho, zda ji lze dále rozvíjet. V případě, že ne označuje se jako základní událost – konečný bod analýzy, který nemá další známé příčiny. Rozvoj stromu pokračuje obdobným způsobem, dokud nejsou všechny větve zakončeny základními nebo jinými konečnými typy událostí. Pokud se některá událost ve stromu opakuje, používají se tzv. transfery, které umožňují pouze jednu analýzu a přenos výsledků

do dalších míst výskytu [3-4]. Konečný strom tvoří diagram logických vztahů mezi příčinami a následky, slouží jako podklad pro další kvalitativní nebo kvantitativní analýzu spolehlivosti, bezpečnosti a rizik systému.

4) Kvalitativní analýza stromu má za cíl identifikaci kombinací podmínek a poruch, které mohou vést k vrcholové události. Základním výstupem jsou minimální kritické řezy (MKR), což jsou nejmenší množiny elementárních událostí (poruchy, lidské selhání aj.), jejichž společný výskyt vede k vrcholové události. Každý MKR představuje podmínku nutnou a postačující pro vznik události. Aby bylo možno zjednodušit relativně komplexní strukturu stromu poruch využívá se Booleovská redukce, umožňující přepsat logiku stromu do výrazu složeného průniky elementárních událostí. Celý proces je zejména při větším počtu událostí mimořádně náročný, proto se používají specializované softwarové nástroje. Hodnocení závažnosti jednotlivých MKR probíhá podle jejich „řádu“ tj. počtu událostí a typu jevů.
5) Kvantitativní analýza stromu poruch se provádí tehdy, pokud jsou známy spolehlivostní data (pravděpodobnosti) jednotlivých elementárních událostí. Cílem je potom stanovení pravděpodobnosti výskytu vrcholové události v daném časovém intervalu. K tomu se kromě jednoduchých případů využívají specializované softwary pracující s využitím matematických metod. V praxi se obvykle používají tři hlavní metody výpočtu:

1. Metoda přímého výpočtu, která je vhodná pouze pro stromy, kde se každá elementární událost vyskytuje pouze jednou. Pomocí známých níže uvedených vztahů se vypočítává pravděpodobnost výskytu událostí od nejnižší úrovně stromu směrem k vrcholové události. Typ použitého logického hradla určuje způsob výpočtu.

   Pro hradlo OR platí

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

   Pro hradlo AND platí

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

2. Metoda minimálních kritických řezů (MKR) vychází ze znalosti všech kritických řezů stromu, což představuje kombinaci událostí, jejichž současný výskyt způsobí vrcholovou událost. Tyto řezy lze převést do sériově-paralelního blokového diagramu a dále řešit inspekční metodou [7-8] nebo pravdivostní tabulkou [5]. Výsledný logický výraz lze upravit do disjunktního tvaru, což usnadní výpočet celkové pravděpodobnosti vrcholové události.
3. Simulační metody (Monte Carlo aj.) lze využít s podporou výpočetní techniky. Jsou vhodné pro složité systémy s relativně velkým množstvím událostí a jejich kombinací. Simulační metody obvykle využívají náhodné generování událostí a statistické vyhodnocování výsledků.

PŘÍKLAD APLIKACE FTA

Příklad zahrnuje využití FTA pro vrcholovou událost, kterou je závažné selhání brzdového systému u vozidla off-road Land Rover Defender. Cílem analýzy bylo identifikovat a logicky strukturovat potenciální příčiny kritického stavu, při kterém vozidlo zcela ztratí schopnost účinně

brzdit, a to za běžných provozních podmínek. Hranice analyzovaného systému byly pro řešený příklad vymezeny tak, aby zahrnovaly pouze vybrané hlavní komponenty brzdové soustavy, tvoří je:

- hydraulický systém (hlavní brzdový válec, posilovač brzd, rozvod kapaliny, spojovací prvky, aj.),
- mechanická soustava (brzdové kotouče a třmeny, brzdové obložení, písty aj.),
- elektronický systém ABS (snímače otáček, brzdový váleček, hydraulická jednotka, hlavní brzdový válec, řídící jednotka aj.),
- brzdová kapalina (předepsané množství, doporučené kvalitativní vlastnosti, kontaminace kapaliny, obsah vzduchu v soustavě, aj.).

Pro standardních provozní podmínky (silniční a terénní provoz, pravidelná údržba v předepsaných intervalech) můžeme vrcholovou událost definovat jako stav, kdy vozidlo po sešlápnutí pedálu nebrzdí. Jedná se o kritické selhání (brzdný účinek je ztracen, popř. omezen tak, že není možné vozidlo bezpečně zastavit nebo masivně zpomalit). Vrcholová událost má za následek selhání účinku brzdné síly, prodloužení brzdné dráhy, resp. výpadek aktivních bezpečnostních prvků aj. Přitom vrcholová událost není způsobena chybou řidiče, není důsledkem vnějších podmínek (smyk na zledovatělé vozovce aj.), není důsledkem kolize nebo mechanického poškození vozidla při nehodě, ale jeho příčinou je pouze technické selhání brzdové soustavy vozidla.

KVANTITATIVNÍ A KVANTITATIVNÍ ANALÝZA

Konstrukce stromu poruchových stavů zahrnuje vyjádření vrcholové události, která je logickou kombinací bezprostředních příčin této události. Příčiny selhání a jejich označení jsou uvedeny v tab. 1. Strom poruchových stavů je uveden na obr. 1.

Tab. 1 Příčiny selhání brzdové soustavy a jejich označení

Označení	Příčina selhání	Označení	Příčina selhání
G	Vozidlo po sešlápnutí pedálu nebrzdí	G1	Selhání hydraulického systému
G2	Selhání brzdových komponent	G3	Vadná brzdová kapalina
G4	Selhání ABS	G5	Selhání 1. brzdového okruhu
G6	Selhání 2. brzdového okruhu	A	Únik brzdové kapaliny 1. okruhu
B	Zavzdušněný 1. okruh brzd	C	Neprůchodný 1. okruh brzd
D	Únik brzdové kapaliny 2. okruhu	E	Zavzdušněný 2. okruh brzd
F	Neprůchodný 2. okruh brzd	H	Opotřebené brzdové kotouče
I	Opotřebené brzdové čelisti	J	Nepohyblivý brzdový třmen
K	Nevhodná brzdová kapalina	L	Znečištěná brzdová kapalina
M	Chemické změny brzdové kapaliny	N	Nefunkční čidlo kol
O	Porucha řídící jednotky	P	Nefunkční ventil modulu ABS

Zápisy obsahují symboly průniku a sjednocení, resp. pro zjednodušení znaménka „krát“ a „plus“.

$$G = G1 + G2 + G3 + G4$$

Následně do rovnice za jev G1 dosadíme logický výraz vyjadřující tento jev jako logickou kombinaci jeho bezprostředních příčin a vztah dále upravujeme, dokud logický výraz nebude tvořen pouze

elementárními jevy. Výsledný logický výraz upravíme tak, aby vyjadřoval prosté sjednocení průniku jevů.

$$G = (G5 \cdot G6) + (H + I + J) + (K + L + M) + (N + O + P)$$

$$G = [(A + B + C) \cdot (D + E + F)] + (H + I + j) + (K + L + M) + (N + O + P)$$

Tento výraz lze zjednodušit a napsat ve tvaru

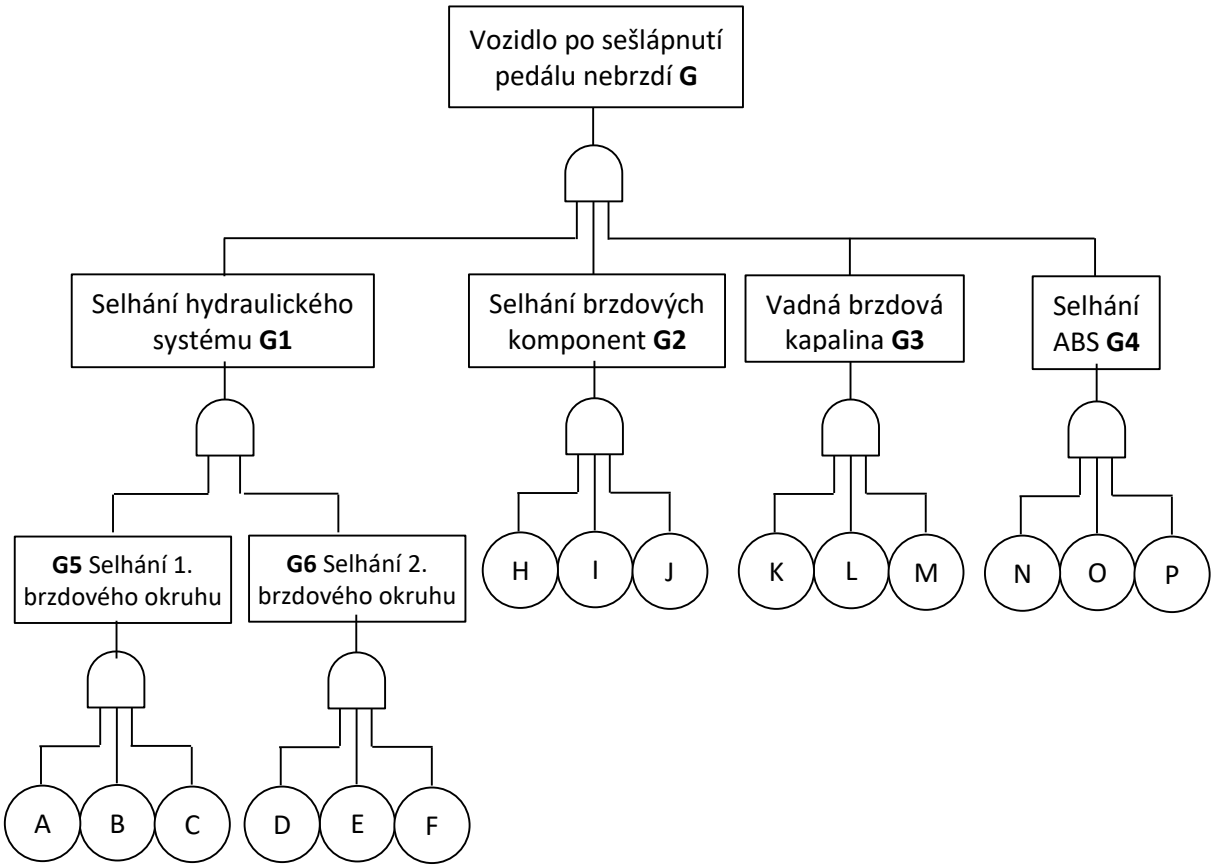
$$G = AD + AE + AF + BD + BE + BF + CD + CE + CF + H + I + J + K + L + M + N + O + P$$

Pro náš příklad stromu poruchových stavů jsme tak obdrželi soustavu osmnácti minimálních kritických řezů ve tvaru

$$\sum MKR =$$

$$\{AD\},\{AE\},\{AF\},\{BD\},\{BE\},\{BF\},\{CD\},\{CE\},\{CF\},\{H\},\{I\},\{J\},\{K\},\{L\}\{M\},\{N\},\{O\},\{P\}.$$

Kvalitativní analýza stanovila minimální kritické řezy (MKR), které představují nejmenší kombinace poruch vedoucích k vrcholové události. Tyto řezy stanovují komponenty (systémy), jejichž selhání má okamžitý a zásadní dopad na funkčnost brzdové soustavy [5]. Z kvantitativního hlediska analýza umožňuje vyhodnotit pravděpodobnost výskytu těchto kritických stavů, což je důležité pro rozhodování o preventivních opatřeních a údržbě. Na základě vyhodnocení lze doporučit pravidelné kontroly hydraulického systému a stavu brzdové kapaliny, preventivní údržbu mechanických částí brzd, diagnostiku a monitoring elektronických brzdových systémů (zejména ABS).



Obr. 1. Strom poruchových stavů

Za předpokladu, že jsou známy vstupní data a ukazatele spolehlivosti elementárních událostí lze realizovat kvantitativní analýzu FTA. Jejím cílem je určení pravděpodobnosti výskytu vrcholové

události během určeného časového intervalu [6]. Ruční provádění kvantitativní analýzy je možné pouze pro jednoduché případy. Složitější stromy poruchových stavů lze řešit pouze softwarovými nástroji. Pro praktické využití FTA jsou dostupné specializované komerční software (Isograph, CAFTA, FaultTree+, OpenFTA, Fault TreweAnalyser, RAM Commander, ITEM ToolKit, PTC Windchill Quality Solutions aj.) [9-12]. Pro náš příklad, za předpokladu, že všechny prvky mají stejnou pravděpodobnost nástupu, lze určit s využitím binomického vzorce a klasických operací s mnohočleny celkovou pravděpodobnost vzniku vrcholové události $P(G)$ následujícími vztahy

$$P(G1) = P(G5) \cdot P(G6) = (p^3 - 3p^2 + 3p) \cdot (p^3 - 3p^2 + 3p) = p^6 - 6p^5 + 15p^4 - \\ -18p^3 + 9p^2$$

$$P(G2) = 1 - \{[1 - P(H)] \cdot [1 - P(I)] \cdot [1 - P(J)]\} = 1 - [(1-p) \cdot (1-p) \cdot (1-p)] \\ = p^3 - 3p^2 + 3p$$

$$P(G3) = 1 - \{[1 - P(K)] \cdot [1 - P(L)] \cdot [1 - P(M)]\} = 1 - [(1-p) \cdot (1-p) \cdot (1-p)] \\ = p^3 - 3p^2 + 3p$$

$$P(G4) = 1 - \{[1 - P(N)] \cdot [1 - P(O)] \cdot [1 - P(P)]\} = 1 - [(1-p) \cdot (1-p) \cdot (1-p)] \\ = p^3 - 3p^2 + 3p$$

$$P(G5) = 1 - \{[1 - P(A)] \cdot [1 - P(B)] \cdot [1 - P(C)]\} = 1 - [(1-p) \cdot (1-p) \cdot (1-p)] \\ = p^3 - 3p^2 + 3p$$

$$P(G6) = 1 - \{[1 - P(D)] \cdot [1 - P(E)] \cdot [1 - P(F)]\} = 1 - [(1-p) \cdot (1-p) \cdot (1-p)] \\ = p^3 - 3p^2 + 3p$$

$$P(G) = 1 - \{[1 - P(G1)] \cdot [1 - P(G2)] \cdot [1 - P(G3)] \cdot [1 - P(G4)]\} = \\ = 1 - [(p^6 - 6p^5 + 15p^4 - 18p^3 + 9p^2) \cdot)p^3 - 3p^2 + 3p) \cdot (p^3 - 3p^2 + 3p) \cdot p^3 - 3p^2 + 3p] \\ = -p^9 + 9p^8 - 36p^7 + 81p^6 - 108p^5 + 81p^4 - 27p^3 + 1$$

ZÁVĚR

Analýza stromu poruchových stavů (FTA) představuje masivní nástroj pro identifikaci a pochopení příčin selhání komplexních technických systémů. FTA umožňuje zcela systematicky odhalovat relevantní příčiny poruch a logické vazby mezi nimi. Hlavním přínosem je odhalení takových kombinací selhání, které by jinak mohly zůstat opomenuty, např. odhalení skutečnosti, že i zdánlivě nevýznamná závada spolu s další může vést k vážné poruše až k celkovému selhání. Na kvalitativní úrovni FTA poskytuje seznam kritických scénářů (minimálních řezů), což pomáhá odhalit slabá místa systému. Kvantitativní vyhodnocení navíc umožňuje odhadnout pravděpodobnosti nežádoucích stavů a kvantifikovat vliv jednotlivých příčin, což je velmi cenné při rozhodování o nápravných opatřeních. Příklad selhání brzdové soustavy vozidla Land Rover Defender demonstroval, že pomocí FTA lze již v návrhu či při provozní analýze odhalit potenciální příčiny kritických selhání a přijmout opatření dříve, než k těmto poruchám dojde. Lze konstatovat, že metoda FTA je nedílnou součástí analýzy rizik, spolehlivosti a bezpečnosti. Umožňuje konstruktérům i provozovatelům pochopit detailní příčinné vazby vedoucí k poruše a cíleně posilovat kritické části systému. Pro zachování objektivity je potřebné konstatovat, že existují rovněž určitá omezení metody FTA spočívající v tom, že tato metoda představuje pouze statický model, který není zaměřen na vzájemné časové závislosti. FTA se ze své podstaty může zabývat pouze binárními stavy (má

poruchu/nemá poruchu) a metoda neumožňuje spolehlivě analyzovat možné domino efekty nebo podmíněné poruchy, které se rovněž v praxi vyskytují.

LITERATURA

[1] Vališ, D., Breznická, A., Stodola, J. Management rizik. Univerzita obrany v Brně, 2020. ISBN 978-80-7582-349-6, 116 s.

[2] Vintr, Z., Vališ, D., Vintr, M. Základy spolehlivosti technických systémů. Univerzita obrany v Brně, 2020. ISBN 978-80-7582-346-5, 183 s.

[3] ČSN EN 61025 (010676) Analýza stromu poruchových stavů (FTA). Český normalizační institut Praha, 2018.

[4] ČSN IEC 60300-3-1 Management spolehlivosti. Část 3-1 Pokyn k použití techniky analýzy spolehlivosti. Metodický pokyn. Český normalizační institut Praha, 2003.

[5] Breznická, A., Chovanec, A., Stodola, J. Metódy analýzy spoľahlivosti. Trenčianska univerzita Alexandra Dubčeka v Trenčíne, 2015. ISBN 978-80-8075-699-4, 227 s.

[6] Nožička, J. Aplikace řešící spolehlivost systémů metodou stromu poruchových stavů (FTA). DP. Technická univerzita Liberec, 2016. 64 s.

[7] Kamenický, J. Blokové diagramy – bezporuchovost sériových a paralelních systémů. Materiály 59. semináře odborné skupiny pro spolehlivost ČSJ. Praha, 2015. s 3-9.

[8] ČSN EN 61078 Techniky analýzy spolehlivosti. Blokový diagram bezporuchovosti a booleovské metody. Český normalizační institut Praha, 2006.

[9] ALD Profile, service, reliability, safety, quality. [online]. [cit. 2025-06-10]. Dostupné z: http://aldservice.com/Company/ald-profile.html

[10] ETA (Event tree analysis) - analýza stromu událostí [online]. [cit. 2025-05-11]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysisanalyza-stromu-udalosti

[11] FMEA (Failure Mode and Effect Analysis) [online]. [cit. 2024-12-19]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

[12] Fault Tree Analysis (FTA) Basics [online]. [cit. 2025-03-20]. Dostupné z: http://www.weibull.com/basics/fault-tree/

Poděkování

Tento příspěvek vznikl s podporou projektu Vojenské robotické a autonomní systémy (DZRO VAROPS), University obrany Brno, Česká republika