

RIZIKO V PODNIKU

Prípadová štúdia 1

Dr. h. c. prof. RNDr. Michal Tkáč, CSc., Ing. Michal Tkáč, PhD.

Tento učebný text je venovaný hlavne študentom I. ročníka II. stupňa Podnikovohospodárskej fakulty, Ekonomickej univerzity v Bratislave. Text obsahuje prípadovú štúdiu k predmetu Riziko v podniku zameriavajúcu sa na rozhodovacie stromy.

Analýza stromu porúch Fault Tree Analysis (FTA) je metóda, ktorá na základe grafického riešenia štruktúry problému pomáha k pochopeniu vzťahov a nadväznosti analyzovaných chýb. Pri riešení danej problematiky sa najčastejšie používajú dva prístupy.

Prístupy, ktoré môžeme použiť na analýzu kauzálnych vzťahov medzi zlyhaniami prvkov a zlyhaním systému:

1. **Induktívna analýza** začína s množinou podmienok zlyhaní prvkov a postupuje dopredu identifikujúc možné následky, čo predstavuje prístup „čo sa stane ak?“.
2. Analýza stromu porúch je príkladom **deduktívneho prístupu**, „čo môže spôsobiť študovaný stav?“ a používa sa na identifikáciu kauzálnych vzťahov vedúcich k špecifickému druhu systémového zlyhania.

Analýza stromu porúch je metóda, podľa ktorej osobitný druh systémového zlyhania môže byť vyjadrený v súvislosti s druhmi zlyhania jednotlivých prvkov a činností operátorov. Druh systémového zlyhania sa nachádza vo vrchole zvanom koreň, odkiaľ smerom nadol rozširujúce sa vetvy poukazujú na možné príčiny. Týmto spôsobom udalosti reprezentované stromom sú ďalej predefinované vzhľadom na predchádzajúce udalosti. Tento postup prerušíme, ak narazíme na udalosti spôsobujúce zlyhanie prvkov, ktoré sa ďalej nedajú deliť, tieto nazývame základne udalosti a sú nedeliteľné. Analýzu stromu porúch spravidla dopĺňa informácia o pravdepodobnosti základných udalostí.

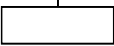
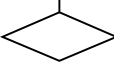
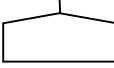
Každý strom porúch vyšetruje iba jeden z mnohých možných druhov zlyhaní systému, a preto počas hodnotenia akéhokoľvek systému je nutne spravidla zostrojiť viac ako jeden strom porúch. Vrcholy stromu porúch okrem udalostí prezentujú aj logické spojenia nazývané hradlá. Tieto vrcholy neopisujú udalosti, ale logickú väzbu medzi jednotlivými vetvami. Nasledovná tabuľka (Tab. 1) opisuje najčastejšie používané hradlá, ich tvar, názov, a význam.

Hradlá umožňujú alebo zabraňujú postupu logickej chyby v stromovej štruktúre a ukazujú vzťah medzi udalosťami potrebnými pre vznik vyššej udalosti. Kategórie zlyhania prvkov:

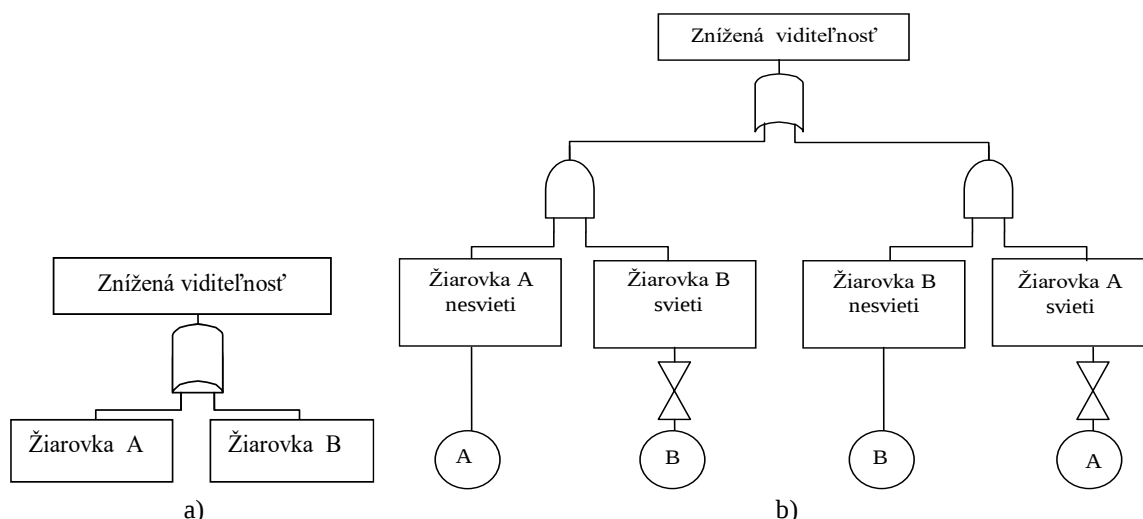
- **Chyba verzus zlyhanie** - všetky zlyhania sú chyby, ale nie všetky chyby sú zlyhania.

- **Vznik verzus existencia** - ak vznikne (uskutoční sa) neopraviteľná chyba, existuje, od jej vzniku. Rozdiel medzi „existenciou“ a „vznikom“ musíme robiť pri opraviteľnej chybe z dôvodu správnej kvantifikácie nevzniknutia vrcholnej udalosti počas časovej periódy.

Tab. 1 Zoznam najčastejšie používaných symbolov - FTA

	Symbol udalosti	Význam symbolu
1	 Obdĺžnik	Prostredná udalosť ďalej rozvíjaná hradlom
2	 Kruh	Základná udalosť
3	 Kosoštvorec	Nerozvinutá udalosť
4	 Elipsa	Podmienená udalosť používaná spolu s inhibičným hradlom
5	 Dom	Domová udalosť. Buď sa uskutoční alebo nie – s pravdepodobnosťami 0 alebo 1
6	 Trojuholníky	Symbole prenosu používajúce sa pri výskyte nejakej udalosti vo viac ako 1 vetve stromu

Uvedieme príklad: Použitie „výhradného hradla“ naznačuje prítomnosť tretieho logického operátora (NIE). Výstupná udalosť, v tomto prípade „Znížená viditeľnosť“ v tmavej miestnosti s dvomi žiarovkami nastane, keď nejaká, ale nie obe z 2 nezávislých žiaroviek zlyhá (Obr. 1a). Ak by zlyhali obe, potom nastane úplná tma, čo nepredstavuje výstupnú udalosť na vrchole stromu. Výhradné ALEBO je skratkou zobrazujúcou danú situáciu. Môže byť nahradené štruktúrou na Obr. 1b vyžadujúcou operátory A, ALEBO a NIE.



Obr. 1 Príklad „tmavá miestnosť s dvoma žiarovkami“

Opísanie tej istej situácie pomocou hradíel nemusí byť jednoznačné. Nahradenie výhradného hradla hradlami A, ALEBO a NIE je opísané v Tab. 1. Jednoduchý strom opisuje základnú udalosť. Strom sa nezaobrá úplnou neviditeľnosťou. Úplná tma neznamenaá zníženú viditeľnosť. To by bol iný príklad. Ak **vznikne** (uskutoční sa) neopraviteľná chyba, **existuje** od jej vzniku.

Rozdiel medzi „existenciou“ a „vznikom“ musíme robiť pri opraviteľnej chybe z dôvodu správnej kvantifikácie nevzniknutia vrcholnej udalosti počas časovej periódy.

Pasívne verzus aktívne prvky

Sledované systémy sa spravidla skladajú z prvkov, ktoré sa rôznym spôsobom podieľajú na vzniku chyb. Rozdeľujeme ich preto na pasívne a aktívne. Pasívny prvok predstavuje spravidla prenášač signálu napr. drôt. Na rozdiel od pasívnych prvkov aktívne prvky sa podieľajú na systéme vo všeobecnosti menia tento systém napr. ventil, transformátor. Aktívne prvky orientujú alebo menia signály, ktoré pasívne prvky prenášajú. Aktívne prvky obyčajne vyžadujú uskutočnenie vstupného signálu. Ak zlyhá aktívny prvok, môže to byť spôsobené aj nevyhovujúcim stupňom signálu. Dôvod rozdelenia na aktívne a pasívne prvky spočíva v miere ich zlyhania. Pasívne prvky majú vo všeobecnosti radovo 2 až 3 násobne nižšiu mieru zlyhania ako aktívne prvky v tom istom systéme.

Konštrukcia stromu porúch – špecifikácia rozmedzia systému

Na začiatku analýzy je spravidla potrebné určiť akýsi rámec t.j. spravidla podsystém, ktorý bude predmetom analýzy. Veľa systémov má totiž extrémne zdroje (ako napríklad dodávka vody) a preto je potrebné v hodnotení systému definovať tzv. extrémne rozmedzie tj. podsystém, v ktorom budeme daný problém skúmať. Extrémne rozmedzie je vhodné definovať

aj v časovom horizonte, keďže napr. podmienky pri rozbiehaní stroja sú odlišné od normálneho chodu, čo má za následok kvalitatívne iné príležitosti pre vznik poruchy v závislosti od analyzovaného času.

Pri analýze nejakého zariadenia, alebo procesu budeme chápať niektoré prvky ako nedeliteľné dodávka, ventil resp. jeho časť. Je dôležité rozvíjať analýzu na podsystém alebo na jeho prvky.

Je potrebné stanoviť aj **hranicu analýzy**, po ktorú sa analýza bude rozvíjať odpovedaním na otázku „je dôležité rozvíjať analýzu na úroveň podsystému alebo až na úroveň prvkov?“ Kým výber hranice analýzy určuje ako detailne sa budeme zaoberať jednotlivými prvkami. Hranice analýzy (interné hranice) môžu tiež vyplývať z uskutočniteľnosti a cieľa analýzy.

Základné vrcholné pravidlá konštrukcie stromu porúch

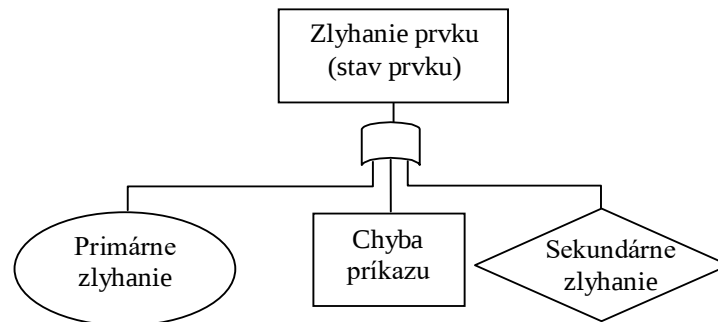
Po definovaní systému a vybratí druhu systémového zlyhania ako vrcholnej udalosti stromu, vytvárame strom porúch určením **stredných, nevyhnutných a dostatočných** príčin pre jeho vznik. Ide o zásadné rozdelenie príčin. (Tieto príčiny nepredstavujú udalosti na úrovni základných prvkov, sú to stredné príčiny). Ďalej ich potom vyšetrujeme ako subvrcholové udalosti tým, že určíme ich stredné, nevyhnutné a dostatočné príčiny. Takýmto spôsobom je nutné strom rozvíjať, aby bol presnejší v detailoch, čím dosahujeme lepšie riešenie problému., Strom považujeme za kompletný, ak dosiahneme predtým určenú hranicu analýzy. Postup pri konštrukcii stromu porúch:

1. Stanovujeme presne chybu, ktorú chceme analyzovať.
2. Ak je chyba spôsobená zlyhaním prvku (ďalej nedeliteľná porucha), klasifikujeme ju ako porucha stavu prvku Obr. 2. V opačnom prípade klasifikujeme udalosť ako poruchu stavu systému (zloženého z ďalších prvkov resp. podsystémov). Pri poruche stavu prvku konštrukcia stromu porúch spravidla zodpovedá obrázku. Pri poruche stavu systému pokračujeme ďalej hľadaním stredných, nevyhnutných a dostatočných príčin, v ktorých súvislosti opisujeme pomocou vhodných hradiel.

Primárne zlyhanie – zlyhanie prvku ako takého

Sekundárne zlyhanie – zlyhanie prvku z dôvodu prevádzky v neprimeraných podmienkach alebo spôsobené zlyhaním iných prvkov systému.

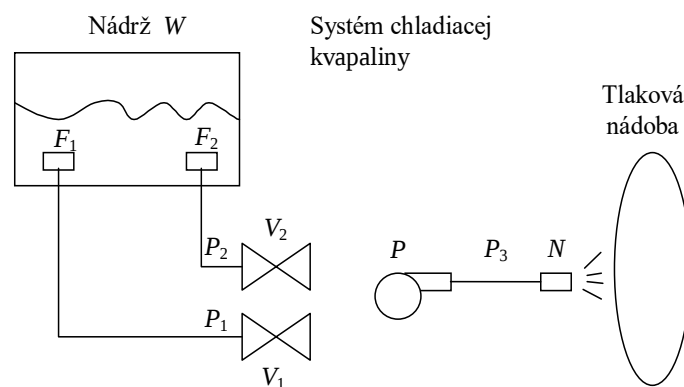
Chyba príkazu – prvok nebol v stave činnosti z dôvodu nevhodného riadiaceho signálu.



Obr. 2 Chyba spôsobená zlyhaním prvku

3. Je potrebné brať do úvahy všetky možné zdroje prípadných porúch. Analýza stromu porúch môže byť iba vtedy funkčná, ak je komplexná a kompletná t.j. ak v nej nechýbajú žiadne možné príčiny vzniku chýb.
4. Je potrebné dbať na to, aby všetky vstupy boli jasne a zrozumiteľne definované pred ich ďalšou analýzou.
5. Ak sa v strome porúch vyskytne susedstvo dvoch za sebou idúcich hradiel, ide spravidla o neefektívne zvolené hradlo. Je možné skupinu hradiel nahradiť jediným hradlom. Ako príklad uvedieme systém chladiacej kvapaliny:

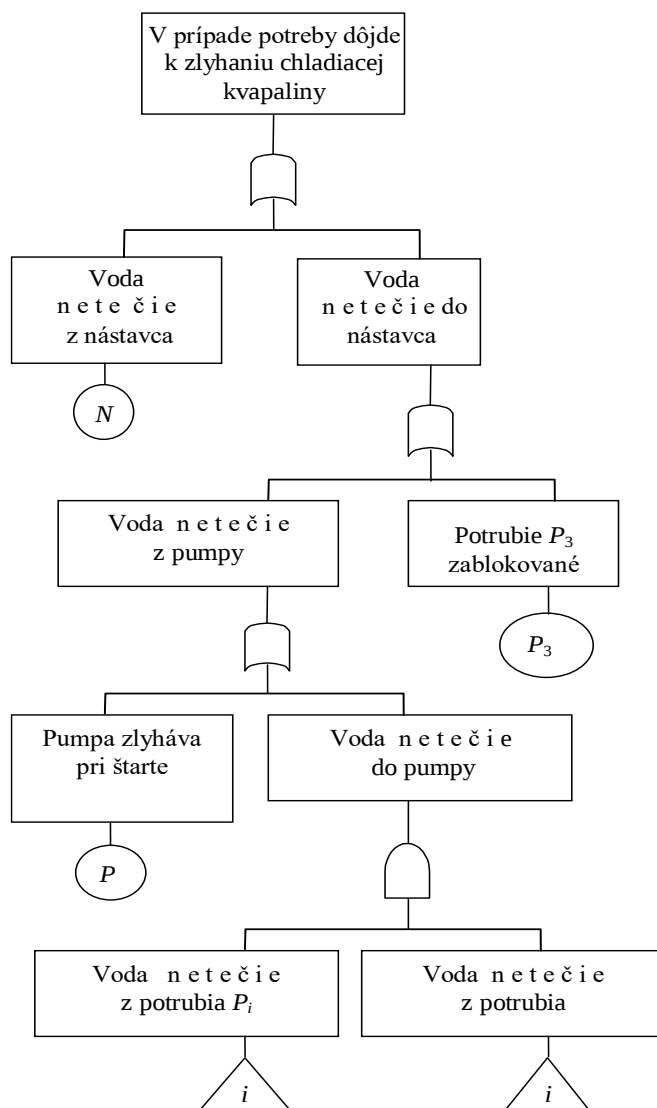
Vrcholnú udalosť predstavuje zlyhanie systému chladiacej kvapaliny, požadovanej v prípade vysokej teploty v tlakovej nádobe (Obr. 3).



Obr. 3 Príklad „systém chladiacej kvapaliny“

Senzory monitorujú teplotu nádoby a v prípade prehriatia aktivujú pumpu P . Systém monitorovania teploty predpokladá 100% spoľahlivosť. Voda preteká dvoma potrubiami P_1 a P_2 s filterami F_1 a F_2 na ich koncoch. Ventily V_1 a V_2 sú za normálnych okolností otvorené, zatvorené sú v prípade údržby, keď musí byť pumpa odstránená. Voda je privádzaná do tlakovej nádoby cez nástavec N namontovaný na potrubí P_3 .

Podľa pravidla 1 vrcholnú udalosť definujeme ako poruchová udalosť – „v prípade potreby zlyhá chladiaci systém“ (Obr. 3.4).



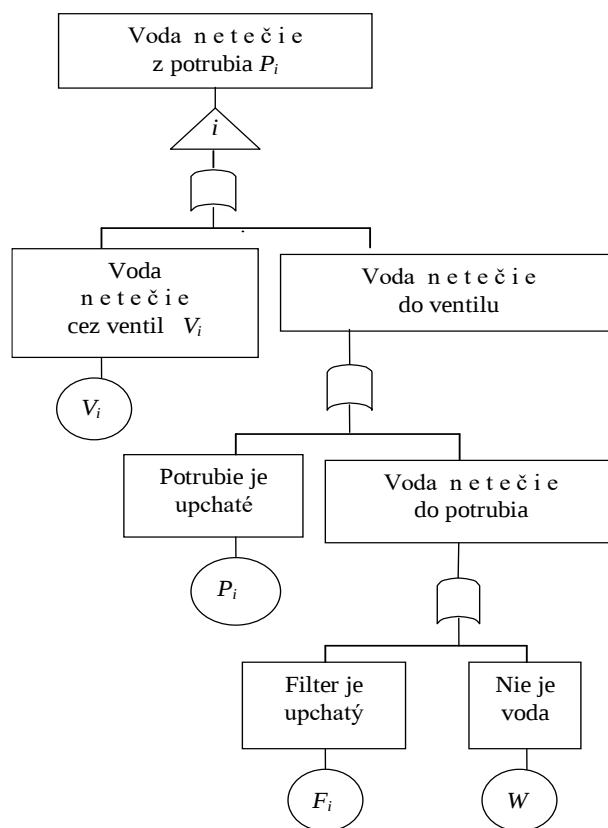
Obr. 3.4 Poruchová udalosť v prípade zlyhania chladiacej kvapaliny

V strome porúch zaznamenávame len primárne zlyhania a chyby príkazu, sekundárne zlyhania boli pre tento prípad ignorované. Platí, že $i = 1, 2$.

V prípade sekundárneho zlyhania (ak pravdepodobnosť sekundárneho vplyvu je štatisticky významná), posudzujeme každý prvok, u ktorého sekundárne zlyhanie pripadá do úvahy osobitne. Napríklad pre pumpu P posudzujeme nasledovne možné sekundárne vplyvy ako (Obr. 5):

- Zlyhanie kvôli podmienkam mimo tolerancie, napr. mechanické vibrácie, nevhodné elektrické napájanie zo zdroja neprípustná teplota, atd.

- Nevhodná údržba – neadekvátne mazanie motorových ložísk, nevhodná obsluha, zlyhanie ľudského faktoru, atď.



Obr. 5 Príklad „voda netečie z potrubia P_i “

Kvalitatívna analýza stromu porúch

Každý špecifický spôsob, akým môže systém zlyhať, predstavuje istý **druh zlyhania systému**. Tento môže pozostávať zo zlyhania individuálnych prvkov alebo zlyhania kombinácie prvkov.

Pri analýze systému a eliminácii najpravdepodobnejších príčin zlyhania je žiadúce najprv každý spôsob zlyhania identifikovať. Spôsoby systémového zlyhania môžeme definovať pomocou tzv. reznej množiny. Rezná množina predstavuje súbor istých základných udalostí. Základnou vlastnosťou takýchto udalostí je, že ak vzniknú, potom sa uskutoční aj vrcholná udalosť. Iným duálnym prístupom je tzv. množina ciest. Ide o súbor základných udalostí s vlastnosťou, že ak pre nich nenastane zlyhanie, potom nevznikne ani vrcholná udalosť (t.j. ide o prvky, ktorých fungovanie zabezpečuje úspešné fungovanie systému vzhľadom na danú vyšetrovanú vrcholnú udalosť).

Existuje množstvo rezných množín a každá môže pozostávať z množstva udalostí možného zlyhania prvku (aj irelevantných, ktoré neovplyvňujú vznik vrcholnej udalosti). My

sa však sústredíme len na druhy zlyhania prvkov, ktoré sú **nevyhnutné** a súčasne **postačujúce** na to, aby spôsobili zlyhanie systému. Zameriame sa teda na minimálne rezné množiny spĺňajúce dane predpoklady.

Minimálna rezná množina je množina udalosti, ktorá ma vlastnosť, že ak by sme niektorú z nich vylúčili, vrcholná udalosť by nevznikla. Ide teda o najmenšiu kombináciu zlyhania prvkov, ktoré ak sa vyskytnú, spôsobia vznik vrcholnej udalosti. Až po správnom vyhodnotení minimálnej reznej množiny, môžeme pristúpiť ku kvantifikácii stromu porúch. Každému stromu porúch môžeme priradiť konečné množstvo minimálnych rezných množín, ktoré sú špecifické pre vrcholnú udalosť. Hovoríme, že dva stromy porúch zakreslené použitím rôznych prístupov sú logicky ekvivalentné, ak obsahujú identické minimálne rezné množiny. Ak existuje jednoprvková minimálna rezná množina (1. rádu) znamená to, že existuje v systéme jednoduché zlyhanie, ktoré spôsobuje vrcholovú udalosť. Dvojprvkové (k - prvkové) minimálne rezné množiny reprezentujú párové zlyhania (zlyhania n - tíc), ktoré spôsobia uskutočnenie vrcholných udalostí. Vo všeobecnosti, minimálne rezné množiny nižšieho rádu (k -relatívne malé) prispievajú k systémovému zlyhaniu vo väčšej miere. To znamená, že pri eliminácii porúch je potrebné sústrediť pozornosť hlavne na takéto rezné množiny.

Vyjadrenie skupiny minimálnych k - prvkových rezných množín pre vrcholnú udalosť môžeme zapísať nasledovným vzťahom:

$$T = K_1 + K_2 + K_3 + \dots + K_n,$$

kde K_i , $i = 1, 2, \dots, n$ sú minimálne rezné množiny (navyššie reprezentujú logické ALEBO). Každá minimálna rezná množina pozostáva z kombinácie zlyhaní prvkov, a preto vo všeobecnosti k_i - prvkovú reznú množinu vyjadríme ako:

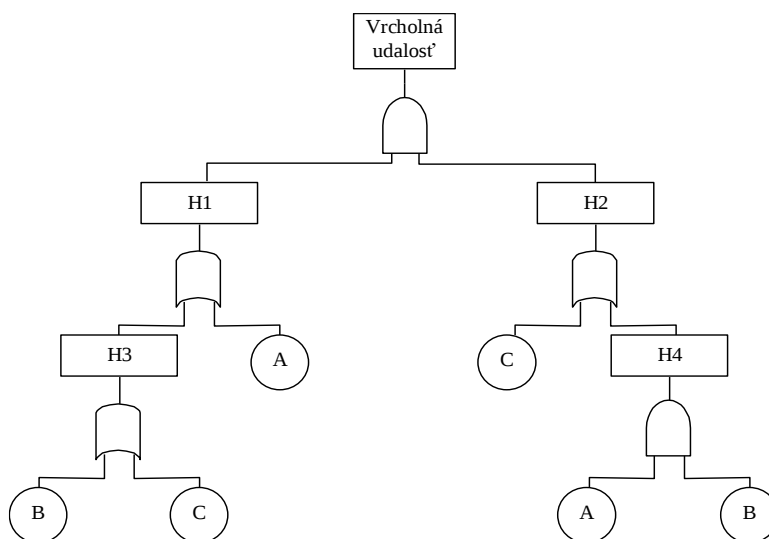
$$K_i = X_1 \cdot X_2 \cdot X_3 \cdot \dots \cdot X_{k_i},$$

kde $X_1, \dots, X_{k_i}$ sú základné zlyhania prvkov (reprezentuje logické A).

Napr. $T = A + B \cdot C + C \cdot D$ (predstavuje tri minimálne rezné množiny, z ktorých prvá je 1. rádu, obsahuje zlyhanie A, druhá je 2. rádu, predstavuje zlyhanie BC a tretia je 2. rádu CD).

Pri určovaní minimálnej reznej množiny môžeme postupovať niekoľkými spôsobmi, najčastejšie používame postup zhora nadol, zdola nahor, alebo pomocou tabuľky. Na zjednodušenie vyjadrení je výhodné použiť zákony Booleovej algebry. V ďalšom pri opise kvalitatívnych hodnotení a stromov budeme spravidla využívať, také stromy porúch, ktoré obsahujú hradla A, ALEBO, NIE, VÝHRADNÉ ALEBO. Ide o stromy, ktoré na úkor efektívnosti v používaní hradiel sú ľahšie interpretovateľné. Kombinácie základných udalostí, ktoré spôsobujú vrcholné udalosti sa nazývajú „implikátory“. V ďalšom opíšeme základné

postupy produkujúce úplný zoznam minimálnych rezných množín. Poznamenávame, že pri konvenčnom spracovaní stromu porúch nie je nevyhnutne vytvárať úplný zoznam primárnych implikátorov.



Obr. 6 Vznik vrcholnej udalosti

Uvažujme jednoduchý strom porúch, pri ktorom sú tri základné udalosti vytvárajú celkovo $2^3 = 8$ stavov základných prvkov. Použitím stromu porúch a logickým posúdením určíme, či môže vzniknúť z každej možnej množiny stavov prvkov vrcholná udalosť alebo nie (Obr. 6). Zostrojíme logickú tabuľku zobrazujúcu všetky možné výstupy systému. V tejto Tab. 2 znak *P* označuje pravdivosť výroku (funkčnosť systému) a znak *N* nepravdivosť výroku (nefunkčnosť systému resp. zlyhanie). Z 8 možných stavov systému 3 spôsobujú, že systém je v stave fungovania (nevznikla vrcholná udalosť) a 5 v stave zlyhania. Ignorujúc stavy, kedy je systém úspešný a zvažujúc iba tie kombinácie, ktoré spôsobujú zlyhanie systému, uvažujeme o reznej množine, teda o zlyhaniach prvkov vedúcich k zlyhaniu systému.

Tab. 2 Riešenie pomocou logickej tabuľky

	A	B	C	Systém
1	P	P	P	P
2	P	P	N	N
3	P	N	P	P
4	P	N	N	N
5	N	P	P	P
6	N	P	N	N
7	N	N	P	N
8	N	N	N	N

Na základe princípov Booleovej algebry až polovica riadkov môže predstavovať taký spôsob zlyhania systému, ktorý je nezávislý na zlyhaní istej podskupiny skúmaných prvkov. Kontrolou môžeme zistiť, že vždy, keď systém je v stave zlyhania, je v tomto stave aj prvok C . Takýto vzťah neplatí pre prvok A aj B . Ak zavedieme v tabuľke novú premennú ‘–’ pre “nepodstatný” stav daného prvku vzhľadom na zlyhanie systému, potom vo všetkých riadkoch, kde C zlyhalo, môžeme stavy prvkov A a B nahradiť touto premennou ‘–’. Polovica riadkov predchádzajúcej tabuľky môže byť nahradená, čo charakterizuje nasledujúca Tab. 3. Skutočne nezávisí od toho, v akom stave je A resp. B , pretože ak C zlyhá, potom sa vrcholná udalosť uskutoční (t.j. zlyhá aj systém).

Tab. 3 Upravená tabuľka novou premennou ‘–’

A	B	C	Systém
P	P	P	P
-	-	N	N
P	N	P	P
N	P	P	P
N	N	P	N

Uvažujeme o spoločnom zlyhaní prvkov A aj B . Z tabuľky je zrejmé, že ak A a B zlyhajú, stav C je irelevantný (nepodstatný). Môžeme teda opäť pristúpiť k redukcii tabuľky. Kombinácia zlyhaní prvkov, ktoré spôsobujú zlyhanie systému je tak reprezentovaná v nasledujúcej Tab. 3.4 dvoma riadkami.

Tab. 3.4 Upravená tabuľka po redukcii

A	B	C	Systém
-	-	N	N
N	N	-	N

Z takto upravenej tabuľky môžeme jednoducho určiť minimálne rezné množiny $\{C\}$ a $\{AB\}$. Takýto postup pre hľadanie minimálnych rezných množín je názorný, ale ťažko využiteľný v prípadoch ak je tabuľka príliš rozsiahla, hoci len s relatívne málo prvkami. Preto v praxi častejšie pristupujeme k postupu zhora nadol, pri ktorom využívame základné zákony Booleovej algebry.

Literatúra

Tkáč, M. (1999-2000). Matematická štatistika a teória pravdepodobnosti Projekt Tempus - Phare IB_JEP-13406-98, SjF, Technická univerzita v Košiciach, 1999-2000, ISBN 80-7099-536-X.