MATEMATICKÉ ZÁKLADY PRO ANALÝZU STROMEM PORUCH

prof. Ing. Radim Briš, CSc.

Vysoká škola báňská - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

Ostrava 2021

ANALÝZA SPOLEHLIVOSTI SYSTÉMU METODOU STROMŮ PORUCH

- **Analýza stromem poruch - historie**
- **Konstrukce stromu poruch**
- **Pravidla pro konstrukci a popis stromu poruch**
- **Kvalitativní vyhodnocení stromu poruch**
- **Využití Booleovy algebry -**

  výpočet pravděpodobností jednoduchých složených událostí
- **Kvantitativní vyhodnocení stromu poruch**
- **Typy vyhodnocení stromu poruch**
  - **Přímá metoda pomocí pravdivostní tabulky**
  - **Analytické vyhodnocení**

ANALÝZA STROMEM PORUCH - HISTORIE

- Systémová analýza pomocí stromu poruch (FTA - Fault Tree Analysis) patří bezesporu k nejčastěji používaným způsobům pro vyhodnocování spolehlivosti složitých systémů. Tento postup poskytuje stručný, uspořádaný a přehledný popis různých možných příhod uvnitř systému, které mohou vést k předem definované „nežádoucí události“. Právě tyto vlastnosti udržují stálou popularitu a perspektivnost této metody ve srovnání s obecnějšími a účinnějšími metodami.

- Metoda stromů poruch byla vyvinuta laboratoří Bell Telephone pro provedení bezpečnostní analýzy odpalovacího zařízení Minuteman. Postupně byla tato metoda aplikována i na digitální systémy. Využití metody bylo zpočátku v hlavní míře soustředěno na **elektronické systémy**, širokou popularizaci a následné rozpracování této metody v oblasti **jaderných** zařízení přineslo zpracování známé rozsáhlé Rassmussenovy studie (Reactor Safety Study) v r. 1975.

- **Strom poruch** lze definovat jako „uspořádaný systém logicky svázaných vstupních událostí vedoucích k předem determinované nežádoucí události“. Terminologie a symbolika stromů poruch není zatím stoprocentně ujednocena a často se liší nejen podle národních zvyklostí, ale odlišuje se i u jednotlivých autorů a institucí. Při studiu i při aplikaci této metody je proto třeba této skutečnosti věnovat zvýšenou pozornost. V převážené míře je dnes přijímána dnes terminologie a symbolika americké literatury, kde dosáhla tato metoda největšího rozvoje a využití.
- Je třeba uvést, že zde je pozornost soustředěna na uvedení do dané problematiky a přehled nejzákladnějších pojmů a principů a zdaleka nepokrývá dnes již obrovský komplex literatury věnované tomuto tématu. Budou uvedeny základy analýzy stromem poruch, jeho kvalitativní a kvantitativní vyhodnocení, přehled výpočtových programů a aplikační příklady.

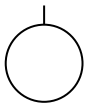
Konstrukce stromu poruch

- **Terminologie a symbolika**

Strom poruch zpracováváme graficky, k vyjádření logiky „nebo“ (příp. OR) a „a“ (příp. AND) využíváme symbolů nazývaných hradla. Pro vyjádření stromu jsou dále užívány symboly pro primární události (resp. „meziudálosti“) a symboly přenosu.

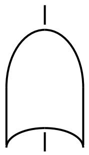
- **Značení primárních událostí**

U primárních událostí uvažujeme pět možných typů



Základní událost - událost, kterou nelze dále dělit (porucha prvku)

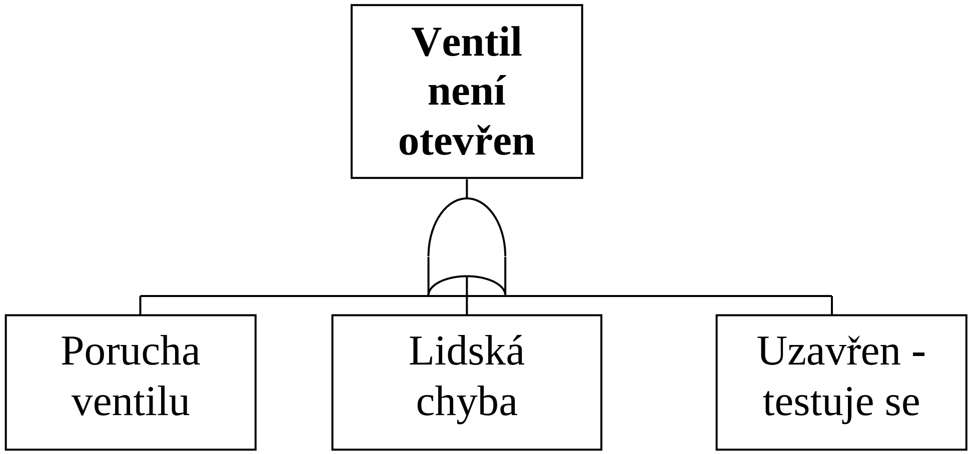
- **Značení a funkce základních hradel: OR, AND a „výběrové“**



Hradlo „OR“ (disjunkce) - k výstupní události dojde tehdy, dojde-li alespoň k jedné (nebo více) ze vstupních událostí.

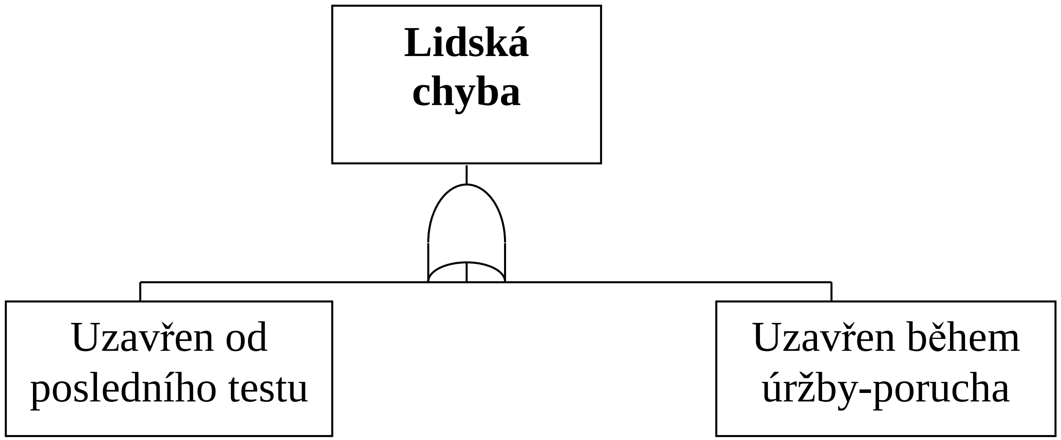
Mezi vstupními a výstupními událostmi neplatí příčinná vazba, tzn. výstupní porucha není nikdy vyvolána vstupními, ale je jejich pomocí pouze více specifikována.

Příklad 1: *„porucha ventilu, protože není otevřen“*

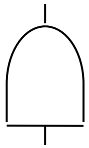


Příklad hradla „OR“

Tyto meziudálosti je možno samozřejmě ještě dále rozvíjet, např.



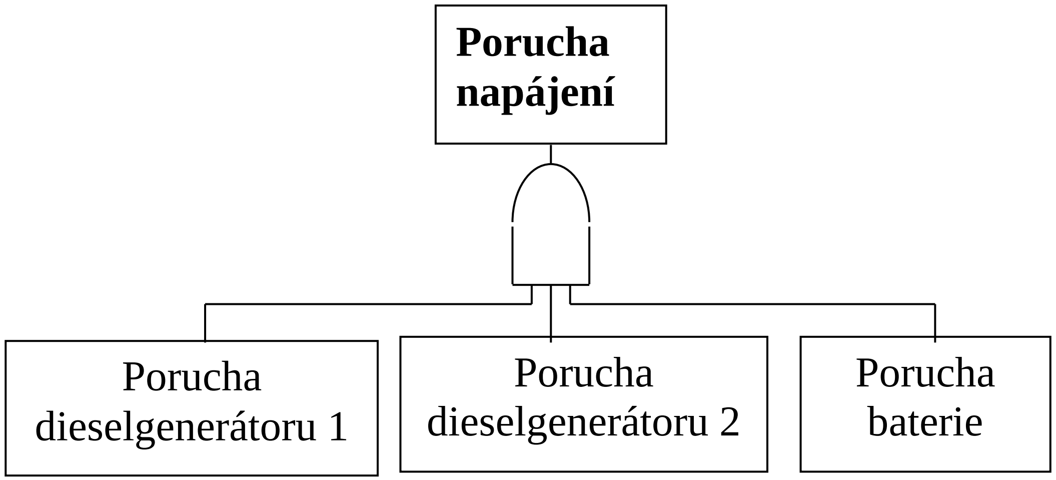
Další rozvoj dané meziudálosti – „Lidská chyba“



Hradlo „AND“ (konjunkce) - k výstupní události dojde pouze tehdy, jestliže dojde ke všem vstupním událostem.

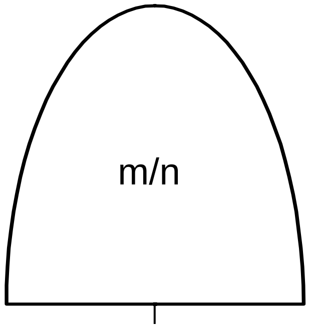
Mezi vstupními a výstupní událostí existuje příčinný vztah, tj. vstupní poruchy kolektivně reprezentují příčinu výstupní události.

Příklad 2: *Porucha dvou dieselgenerátorů a baterie, které vedou k poruše napájení*



Příklad hradla „AND“

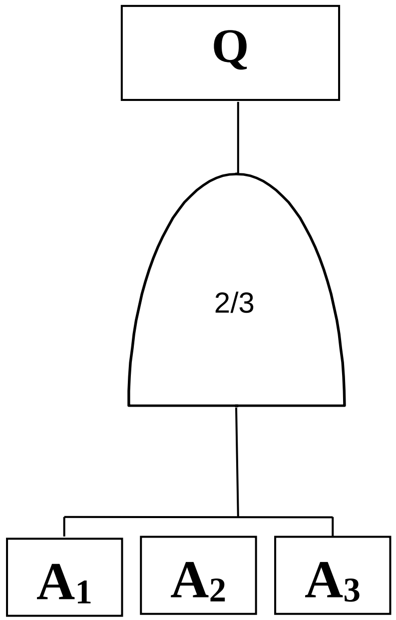
Výběrové hradlo: lze samozřejmě jinak rozepsat pomocí hradel OR a AND.



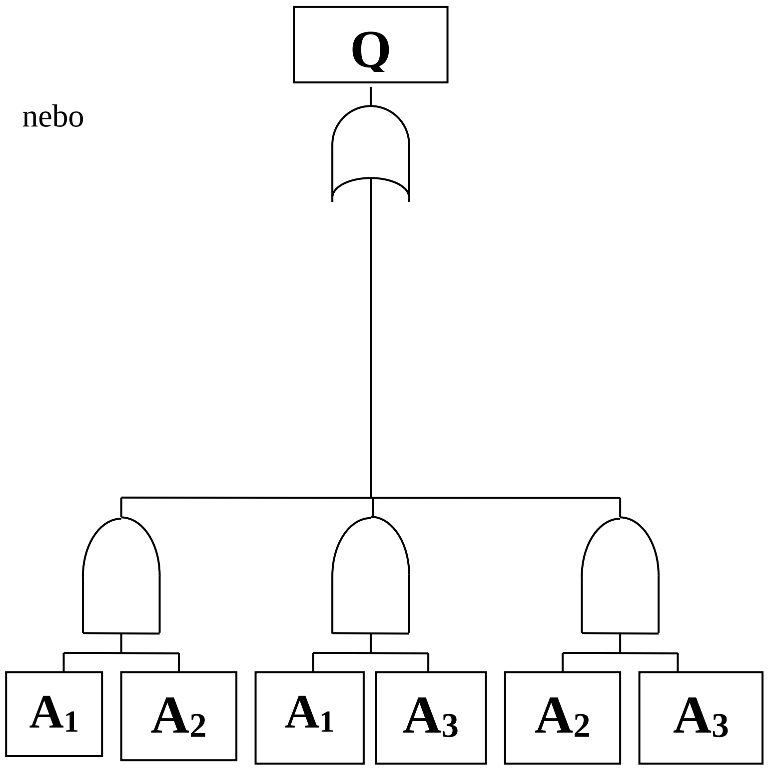
Hradlo „výběrové“ - k výstupní události dojde tehdy, jestliže nastane alespoň „m z n“ vstupních událostí ($m < n$)

Příklad 3: *Příkladem výběrového systému může být systém signálů n čidel vyvolávající zásah bezpečnostního systému jaderného reaktoru. V případě zásahu bezpečnostního systému na každý signál by došlo k řadě zbytečných zásahů (bezpečná porucha) při falešném signálu. Naopak při zásahu až při všech signálech současně by už při poruše jednoho čidla či přenosové trasy mohlo dojít k „nebezpečné poruše“.*

Příklad: *Systém „dva ze tří“, který omezuje výskyt bezpečných poruch a současně připouští poruchu signálu při nebezpečné poruše. Porucha nastává, není-li přenesen signál z libovolných dvou čidel. Lze též rozepsat pomocí hradel OR a AND.*

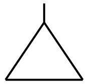


nebo

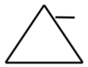


Příklad „výběrového“ hradla pro systém „dva ze tří“

• Symboly pro pokračování stromu poruch



Symboly pokračování se používají pro přehlednější kreslení stromů poruch (např. neopakování již popsaných podstromů) nebo pro vstup.



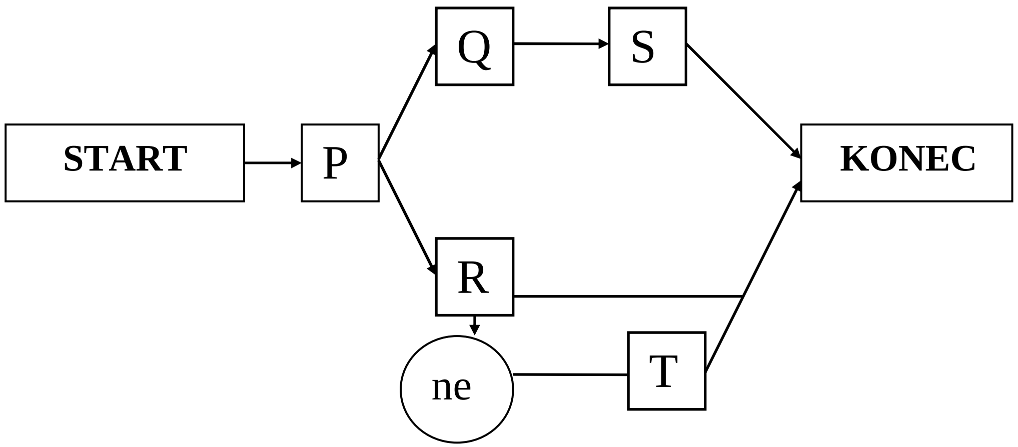
Možnost rozkreslení stromů poruch na několik částí. Označení pokračovacích symbolů si musí vzájemně odpovídat.

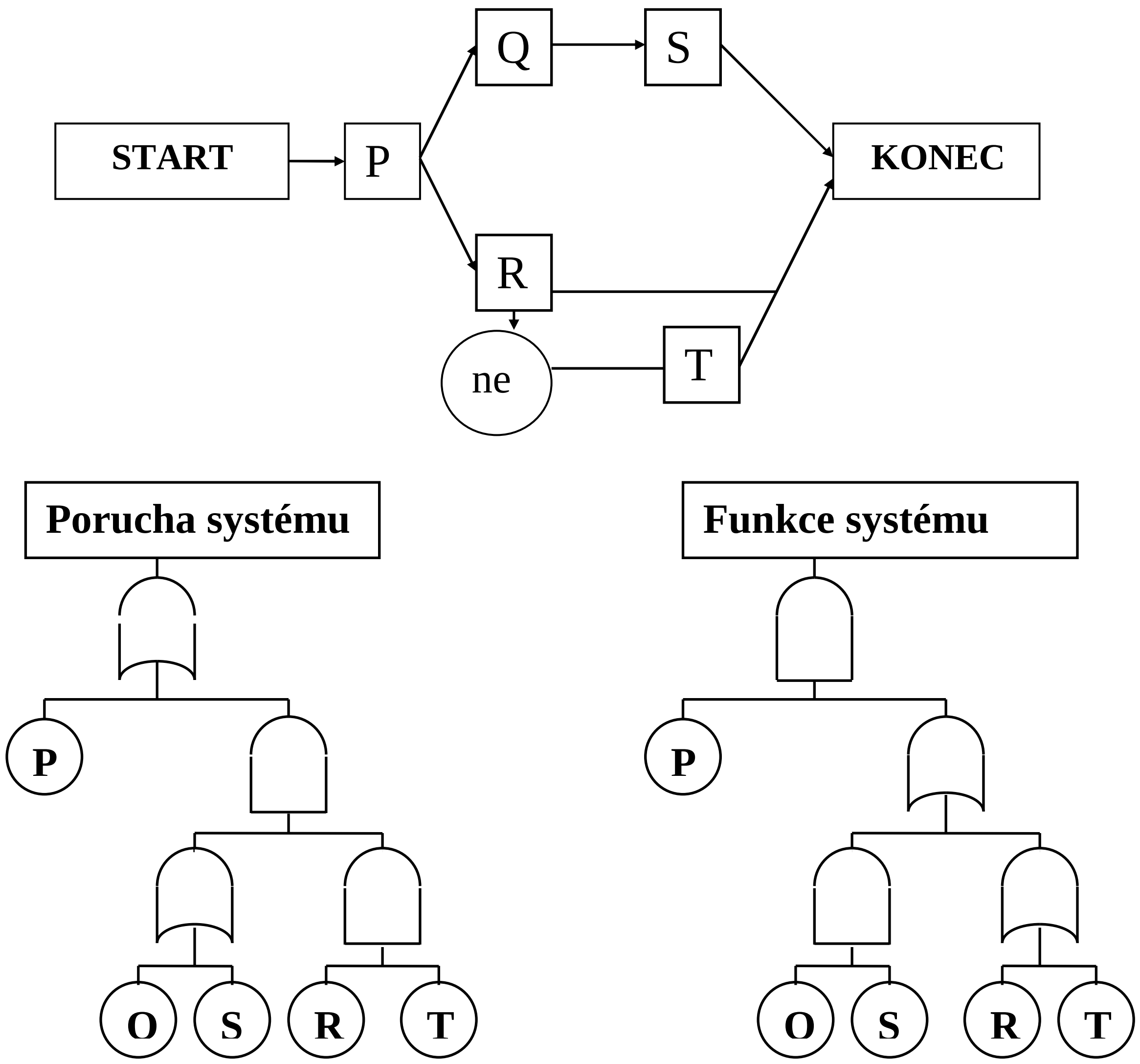
výstup

Příklad

Příklad přechodu od blokového schématu (funkci sledujeme jako průchod signálu schématem; jednotlivé prvky se chovají binárně - tj. zadrží či propustí signál) ke stromu poruch

Blokové schéma





Vytvoření stromu poruch a stromu úspěchu na základě blokového schématu

Přechod od stromu úspěchu ke stromu poruch a naopak vzniká záměnou hradel typu AND a OR.

Vrcholová událost

Vrcholovou událostí (TOP) označujeme událost, při které systém není schopen své funkce, nebo která je pro nás nežádoucí. Volba vrcholové události je zásadní věcí při konstrukci stromu poruch a je třeba jí věnovat patřičnou pozornost. Rozvoj vrcholové události - ve smyslu hledání příčin jejího vzniku, je třeba provádět postupně až do úrovně příčin, které nejsou dále rozvíjeny, jejichž pravděpodobnost jsme schopni kvantifikovat. Tyto „konečné příčiny“ nazýváme zpravidla prvky (primární, prvotní, vstupní či základní události, elementy, komponenty, podsystémy, součástky, listy ap.)

Označíme-li pravděpodobnost vrcholové události F_{TOP} (což může být např. distribuční funkce doby do první poruchy systému, funkce bezporuchovosti systému, popř. funkce okamžité pohotovosti, apod.) a nalezneme-li, že závisí na poruchovém chování *n* prvků (o pravděpodobnostech F_i) pak hledáme vyjádření:

$$F_{TOP} = \Phi(F_i : i = 1, 2, ..., n)$$

Pravidla pro konstrukci a popis stromu poruch

Strom poruch pro účely matematického zpracování

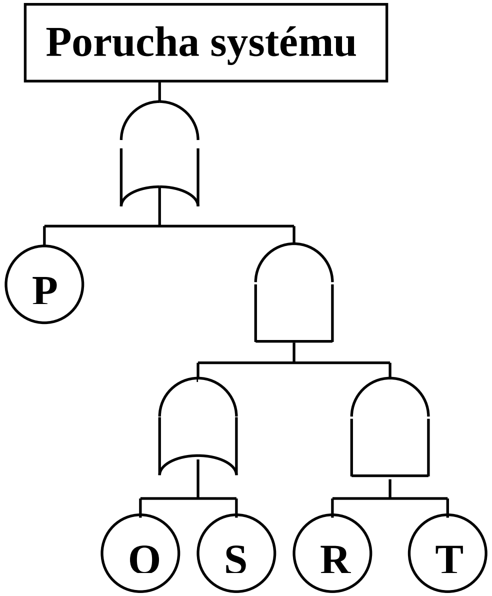
Po ukončení konstrukce stromu poruch přicházíme k jeho matematickému zpracování. Pro tento účel, zpravidla už se znalostí počtu primárních událostí a hradel, strom očíslujeme (už s uvážením potřeb dále použité metodiky vyhodnocení, tj. např. číslování pouze primárních událostí či všech - zpravidla zleva doprava a zdola nahoru; rozepsání stromu tak, aby do každého hradla vstupovaly pouze dvě události atd.). Nejběžněji je používán zápis pomocí Booleovy algebry (viz dále):

Strom poruch je popsán jako logická funkce základních událostí ψ

$$\mathrm{TOP} = \psi\,(A_1, A_2, \ldots, A_n)$$

kde Booleova logika zachycuje vliv hradel a funkce je tedy tvořena jen primárními událostmi A_i.

Příklad: Jednoduchý strom poruch



TOP = (Q ∪ S) ∩ (R ∩ T) ∪ P **nebo** **TOP = (Q + S) . (R . T) + P**

V případě komplikovaného stromu postupujeme tak, že vycházíme od vrcholové události a postupně popisujeme jednotlivá značená hradla na nižších úrovních. Postupnou substitucí dostáváme nakonec žádanou logickou funkci. Při úpravách je žádoucí využívat základních pravidel Booleovy algebry (viz další výklad), pro zjednodušení. Operátory mezi událostmi jsou v souladu s definovanými logickým součtem a součinem (OR, AND).

Kvalitativní vyhodnocení stromu poruch

Sestrojený strom poruch přechází v této etapě na matematický model popsaný graficky, resp. matematickým zápisem. Jeho vyhodnocení lze provést ručním způsobem nebo pomocí počítače a různých typů výpočtových programů. **Cílem kvalitativního vyhodnocení je najít strukturní funkci stromu**, tj. vyjádřit vrcholovou událost jako funkci jednotlivých prvků tak, abychom po dosazení příslušných pravděpodobností primárních událostí v daném čase získali přímo pravděpodobnost vrcholové události. Kvantitativní vyhodnocení v případě neschůdnosti tohoto postupu může přejít na odhad, tj. vyčíslení horních resp. i dolních mezí této pravděpodobnosti.

Pojem minimální řez

V počítačovém zpracování přechází zpravidla kvalitativní analýza na nalezení souboru minimálních řezů (anglicky *minimal cut set*). Takovýmto **minimálním řezem** rozumíme nejmenší možnou kombinaci primárních prvků stromu, které nastanou-li současně, vyvolají vrcholovou událost. Počet prvků v řezu pak určuje **řád** tohoto **řezu**.

Pojem minimální dráha

Přejdeme-li od stromu poruch ke stromu úspěchu (někdy nazývaný též duální strom poruch; tj. provedeme záměnu hradel, přechod z Booleovského popisu stromu pomocí de Morganových vztahů, čímž budeme hledat doplňek vrcholové události) pak řez tohoto stromu nazveme minimální dráhou (*minimal path*). Analogicky **minimální dráhou** rozumíme nejmenší možnou kombinaci primárních událostí, které musí zároveň nastat, aby nedošlo k vrcholové události stromu poruch (tzn., které komponenty si musí zachovat svou funkci, aby nebyla ohrožena funkceschopnost vyšetřovaného systému).

Koherence stromu poruch

Při rozboru stromu poruch je třeba prověřit, zda se jedná o koherentní strukturu. Koherencí rozumíme takovou vlastnost systému, kdy při náhlé poruše resp. opravě prvku nedojde k opačnému chování vrcholové události, tj. obnovení funkce systému, resp. jeho poruše.

Závislost stromu poruch

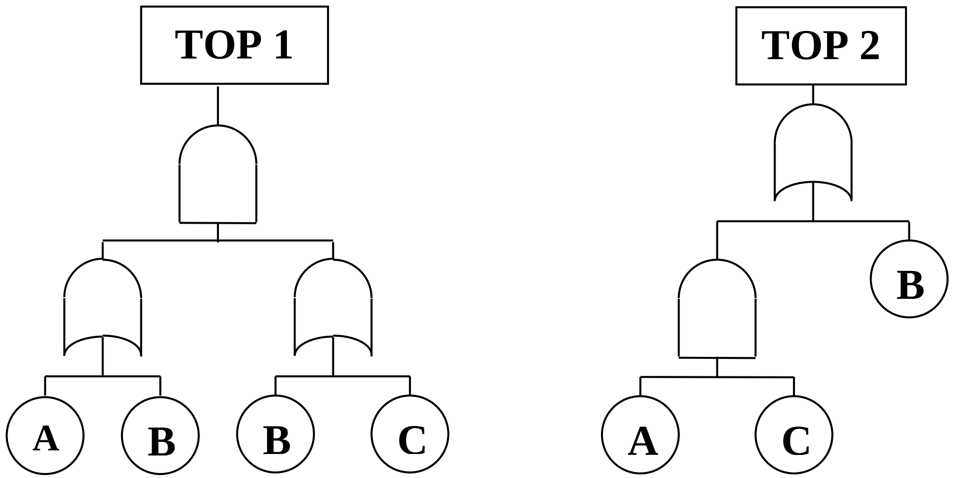
I když o primárních událostech předpokládáme, že jsou nezávislé, mohou se ve stromu poruch některé primární události či podstromy **opakovat**. Při přímém vyhodnocení se pak snadno můžeme dopustit chyby.

Příklad: Logický model ilustrující eliminaci závislých poruch. Dva stromy poruch níže jsou zřejmě ekvivalentní. Logický výraz pro výslednou poruchu prvního stromu je

$$\text{TOP 1} = (A + B) \,.\, (B + C)$$

S použitím Booleovy algebry dále platí:

$\text{TOP 1} = AB + BB + AC + BC = AC + B \,.\, (A + C + B) = AC + B = \text{TOP 2}$



Modularizace stromu poruch

Rozsáhlý strom poruch bývá (zvláště pro kvantitativní vyhodnocení) často s výhodou modularizován. Tento postup snižuje počet primárních událostí vytvářením tzv. „makrokomponent“, které reprezentují podstromy. Tyto makrokomponenty musí být nezávislé jak vzhledem k ostatním primárním událostem, tak k ostatním vytvořeným makrokomponentám. S ohledem na následnou kvantifikaci jsou nejvýhodnější podstromy pouze s hradly OR. Při jejich vyhodnocení, za předpokladu použití exponenciálního modelu, se exponenciální model zachovává i u makrokomponenty.

Opakování: Reprodukční vlastnost Weibullova rozdělení

Jak jsme se dozvěděli, flexibilita Weibullova rozdělení umožňuje aproximovat širokou třídu rozdělení s monotónní intenzitou poruch. Takováto rozdělení se v technické praxi vyskytují poměrně často.

Věta:

Nechť $X_1, \ldots, X_n$ jsou nezávislé stejně rozdělené náhodné veličiny s rozdělením $W(\Theta, \beta)$. Potom náhodná veličina $X_{\min} = \min(X_1, \ldots, X_n)$ má rozdělení $W\left(\dfrac{\Theta}{n^{\frac{1}{\beta}}}, \beta\right)$.

Využití Booleovy algebry, výpočet pravděpodobností jednoduchých složených událostí

Booleova algebra je libovolná množina prvků, na které jsou definovány operace součet, násobení a inverze, která je dále uzavřená vůči těmto operacím, a která zachovává řadu algebraických zákonů (komutativní, asociativní, distributivní), vůči oběma operacím. Její základní pravidla uvádíme přehledně s matematickým i technickým značením v tabulce níže. Booleovské proměnné označené v tabulce čárkou (X') jsou komplementární doplňky (inverze) k původním proměnným X, symbol $\emptyset$ značí nulový prvek, symbol Ω značí jednotkový prvek, oba charakterizovány příslušnými vlastnostmi v tabulce. Platnost některých doplněných vztahů lze snadno ověřit (např. pomocí Vennových diagramů).

Pravidla Booleovské algebry

Matematická symbolika	Technická symbolika	Označení
(1a) $X \cap Y = Y \cap X$ (1b) $X \cup Y = Y \cup X$	$X \cdot Y = Y \cdot X$ $X + Y = Y + X$	Komutativní zákon
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$ $X (YZ) = (XY) Z$ $X + (Y + Z) = (X + Y) + Z$	Asociativní zákon
(3a) $X \cap (Y \cup Z) =$ $= (X \cap Y) \cup (X \cap Z)$ (3b) $X \cup (Y \cap Z) =$ $= (X \cup Y) \cap (X \cup Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$ $X (Y + Z) = XY + XZ$ $X + Y \cdot Z =$ $= (X + Y) \cdot (X + Z)$	Distributivní zákon
(4a) $X \cap X = X$ (4b) $X \cup X = X$	$X \cdot X = X$ $X + X = X$	Idempotentní zákon
(5a) $X \cap (X \cup Y) = X$ (5b) $X \cup (X \cap Y) = X$	$X \cdot (X + Y) = X$ $X + X \cdot Y = X$	Zákon absorbce

(6a) $X \cap X' = \emptyset$ (6b) $X \cup X' = \mathbf{\Omega}$	$X \cdot X' = \emptyset$ $X + X' = \mathbf{\Omega}$	Zákon komplementů
(7a) $(X \cap Y)' = X' \cup Y'$ (7b) $(X \cup Y)' = X' \cap Y'$	$(X \cdot Y)' = X' + Y'$ $(X + Y)' = X' \cdot Y'$	de Morganovy vzorce
(8a) $\emptyset \cap X = \emptyset$ (8b) $\emptyset \cup X = X$ (8c) $\mathbf{\Omega} \cap X = X$ (8d) $\mathbf{\Omega} \cup X = \mathbf{\Omega}$ (8e) $\emptyset' = \mathbf{\Omega}$ (8f) $\mathbf{\Omega}' = \emptyset$	$\emptyset \cdot X = \emptyset$ $\emptyset + X = X$ $\mathbf{\Omega} \cdot X = X$ $\mathbf{\Omega} + X = \mathbf{\Omega}$ $\emptyset' = \mathbf{\Omega}$ $\mathbf{\Omega}' = \emptyset$	Operace s $\emptyset$ a $\mathbf{\Omega}$
(9a) $X \cup (X' \cap Y) = X \cup Y$ (9b) $X' \cap (X \cup Y') = X' \cap Y' = (X \cup Y)'$	$X + X' \cdot Y = X + Y$ $X' \cdot (X + Y') = X' \cdot Y' = (X + Y)'$	Často užívané vztahy

Strom poruch pro účely matematického zpracování

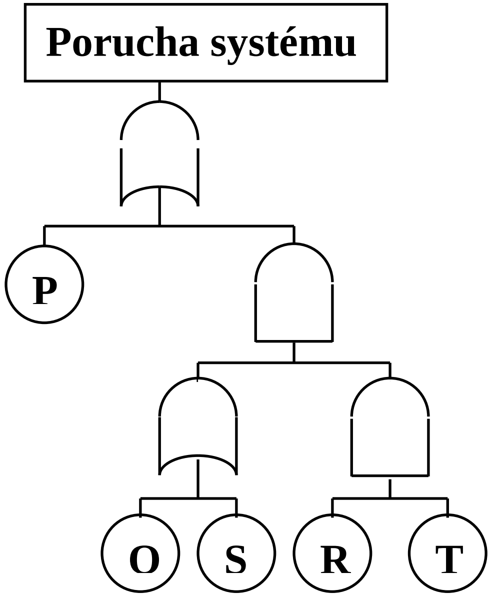
Se znalostí počtu primárních událostí a hradel, strom očíslujeme (už s uvážením potřeb dále použité metodiky vyhodnocení, tj. např. číslování pouze primárních událostí či všech - zpravidla zleva doprava a zdola nahoru; rozepsání stromu tak, aby do každého hradla vstupovaly pouze dvě události atd.). Nejběžněji je používán zápis pomocí Booleovy algebry:

Strom poruch je popsán jako logická funkce základních událostí ψ

$$\mathrm{TOP} = \psi\ (A_1, A_2, \ldots, A_n)$$

kde Booleova logika zachycuje vliv hradel a funkce je tedy tvořena jen primárními událostmi A_i.

Příklad: Jednoduchý strom poruch



$\mathbf{TOP = (Q \cup S) \cap (R \cap T) \cup P}$ **nebo** $\mathbf{TOP = (Q + S) \;.\; (R \,.\, T) + P}$

V případě komplikovaného stromu postupujeme tak, že vycházíme od vrcholové události a postupně popisujeme jednotlivá značená hradla na nižších úrovních. Postupnou substitucí dostáváme nakonec žádanou logickou funkci. Při úpravách se využívá základních pravidel Booleovy algebry pro zjednodušení. Operátory mezi událostmi: OR, AND.

Kvantifikace SP

- **Jak využít Booleovu algebru k úpravě a zjednodušení stromu poruch?**

S ohledem na stromy poruch nám komutace dovoluje zaměňovat pořadí prvků v hradlech, asociace různé grupování v sérii hradel stejného typu a distribuce nám dovoluje manipulovat s kombinacemi, kde se vyskytují jak AND tak OR hradla. Uvedené zákony i doplněné vztahy umožňují postupnou úpravu a zjednodušování Booleovsky popsaného stromu poruch.

- **Booleovský popis hradel**

Hradlo OR je v Booleovské algebře ekvivalentní sjednocení, či součtu, obecně pro hradlo s n vstupy $A_1, A_2, \ldots, A_n$ platí

$$Q = A_1 + A_2 + \ldots + A_n$$

Pro pravděpodobnost $P(Q)$ pak pro hradlo se dvěma vstupy A, B lze zapsat

$$P(Q) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A)\, P(B/A)$$

Pro **vzájemně se vylučující** události ($P(A \cap B) = 0$) je

$$P(Q) = P(A) + P(B)$$

Jsou-li A, B **nezávislé**, pak $P(B/A) = P(B)$ a tudíž

$$P(Q) = P(A) + P(B) - P(A)\, P(B)$$

resp. $$P(Q) = 1 - (1 - P(A))\, .\, (1 - P(B))$$ a zobecníme:

Obecně pro n vstupů: $$P(Q) = 1 - \prod_{i=1}^{n}\left(1 - P\left(A_i\right)\right)$$

Bereme-li vztah pro vylučující se události: $P(Q) = P(A) + P(B)$

jako aproximativní, pak je ve všech případech konzervativní, neboť

$$P(A) + P(B) \geq P(A) + P(B) - P(A \cap B)$$

a při jeho použití se už při pravděpodobnostech $P(A) < 10^{-1}$, $P(B) < 10^{-1}$ dopouštíme malé chyby (max. 5%).

Hradlo AND je v Booleovské algebře ekvivalentní průniku, či součinu, pro hradlo s *n* vstupy obecně platí

$$Q = A_1 \,.\, A_2 \,.\; \ldots \;.\, A_n$$

a pro pravděpodobnosti u hradla se dvěma vstupy platí

$$P(Q) = P(A)\,.\,P(B/A) = P(B)\,.\,P(A/B)$$

V případě **nezávislých událostí** dostaneme

$$P(Q) = P(A)\,.\,P(B)$$

a obecně pro *n* vstupů:

$$P(Q) = \prod_{i=1}^{n} P(A_i)$$

K vyjádření **pravděpodobnosti události na výstupu výběrového hradla** zaveďme pravděpodobnosti vstupních událostí $p_1, p_2, \ldots, p_n$ a $T(n, j)$ pravděpodobnost vzniku j nebo více událostí ze skupiny událostí $A_n, A_{n-1}, \ldots, A_1$. V případě $p_1 = p_2 = \ldots = p_n = p$, tj. stejné pravděpodobnosti vzniku všech vstupních událostí, lze snadno dokázat, že platí

$$T(n, j) = \sum_{r=j}^{n} \binom{n}{r} p^r (1-p)^{n-r}$$

Pivotální dekompozice Booleovské funkce (stromu poruch)

Tato metoda vyjadřuje Booleovskou funkci ve standardizované formě, rozvinuje obecnou Booleovskou funkci $\psi(A_1, A_2, \ . \ . \ . \ , A_n)$, představující nějaký strom poruch. Předpokládáme, že pro $A_i = 1$ se událost vyskytla a pro $A_i = 0$ se nevyskytla. Rozvinutí pak provádíme následovně

$$\psi(A_1, A_2, \ . \ . \ . \ , A_n) = A_1 \ . \ \psi(1, A_2, \ . \ . \ . \ , A_n) + (1- A_1) \ \psi(0, A_2, \ . \ . \ . \ , A_n)$$

Rozvíjet lze postupně pro všechny proměnné až získáme 2^n vzájemně se vylučujících kombinací.

Příklad

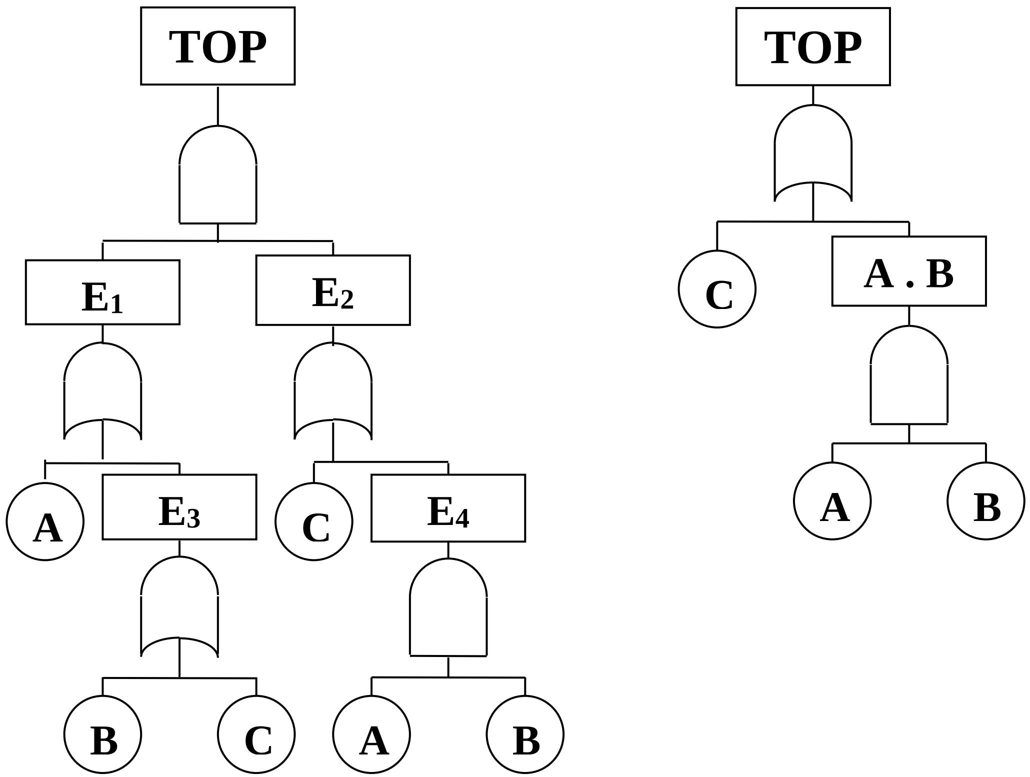
Proveďte pivotální dekompozici obecné Booleovské funkce tří proměnných.

$$\psi(A,B,C) = ABC\ \psi(1,1,1) + AB(1- C)\ \psi(1,1,0) + A(1- B)C\ \psi(1,0,1) + A(1- B)(1- C)\ \psi(1,0,0) + (1- A)BC\psi(0,1,1) + (1- A)B(1- C)\ \psi(0,1,0) + (1- A)\ (1- B)C\ \psi(0,0,1) + (1- A)\ (1- B)\ (1- C)\ \psi(0,0,0)$$

Určení souboru minimálních řezů

Úplný soubor minimálních řezů lze získat úpravou Booleovského popisu vrcholové události TOP = $\psi\ (A_1, A_2, \ldots, A_n)$ pomocí výše uvedených pravidel Booleovské algebry. Při těchto úpravách dochází ke zjednodušení a redukci stromu poruch.

Příklad: *Proveďte redukci stromu poruch z obrázku*



Řešení:

TOP = $E_1 \,.\, E_2 = (A + E_3)\,.\,(C + E_4) = (A + B + C)\,(C + A\,.B) =$

$= A\,.C + A\,.A\,.B + B\,.C + B\,.A\,.B + C\,.C + C\,.A\,.B =$

$= A\,.C + A\,.B + B\,.C + A\,.B + C + A\,.B\,.C =$

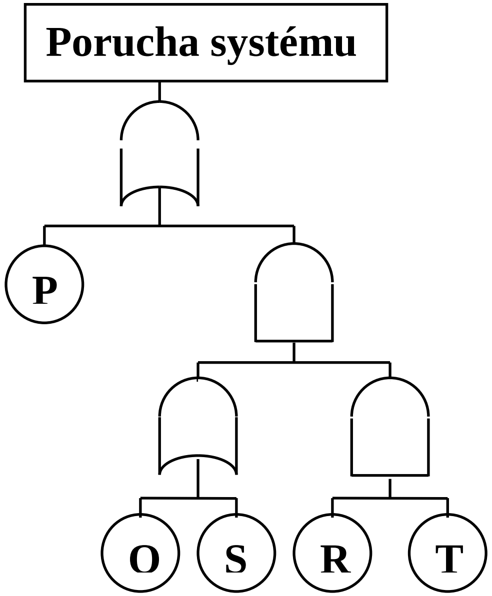
$= A\,.B + C$

K nalezení souborů minimálních řezů v současné době existuje řada počítačových algoritmů. Jejich znalost pak umožní vyčíslení pravděpodobnosti vrcholové události.

Kvantitativní vyhodnocení stromu poruch

Přímá metoda vyhodnocení: metoda založená na pivotální dekompozici.

Příklad



Respektujeme všechny stavy systému (viz následující tabulka, která reprezentuje strom poruch výše). Soustava nul a jedniček představuje „pracující“ či „porušený“ prvek nebo systém. Každý řádek reprezentuje jednu z možné kombinace stavů prvků *P*, *Q*, *R*, *S*, *T*. V posledním sloupci jsou uvedeny pravděpodobnosti jednotlivých stavů (kde pravděpodobnosti poruch jednotlivých prvků jsou: p,q,r,s,t), jejichž součet dává jednotku. Sečtením pravděpodobností těch stavů, kdy nastává vrcholová událost (systém = 1) dostáváme celkovou pravděpodobnost vrcholové události. Protože pro strom poruch s *n* prvky může nastat 2^n kombinací, stává se tento způsob pro větší *n* nepraktický.

Tabulka: Pravdivostní tabulka pro SP systému výše

Čís.	**Uzlový bod P Q R S T**	**Systém**	**Pravděpodobnost stavu**
1	0 0 0 0 0	0	(1-p)(1-q)(1-r)(1-s)(1-t)
2	0 0 0 0 1	0	(1-p)(1-q)(1-r)(1-s) t
3	0 0 0 1 0	0	(1-p)(1-q)(1-r) s (1-t)
4	0 0 0 1 1	0	(1-p)(1-q)(1-r) st
5	0 0 1 0 0	0	(1-p)(1-q) r (1-s)(1-t)
6	0 0 1 0 1	0	(1-p)(1-q) r (1-s) t
7	0 0 1 1 0	0	(1-p)(1-q) rs (1-t)
8	0 0 1 1 1	1	(1-p)(1-q) rst
9	0 1 0 0 0	0	(1-p) q (1-r)(1-s)(1-t)
10	0 1 0 0 1	0	(1-p) q (1-r)(1-s) t
11	0 1 0 1 0	0	(1-p) q (1-r) s (1-t)
12	0 1 0 1 1	0	(1-p) q (1-r) st
13	0 1 1 0 0	0	(1-p) qr (1-s)(1-t)

14	0 1 1 0 1	1	(1-p) qr (1-s) t
15	0 1 1 1 0	0	(1-p) qrs (1-t)
16	0 1 1 1 1	1	(1-p) qrst
17	1 0 0 0 0	1	p (1-q)(1-r)(1-s)(1-t)
18	1 0 0 0 1	1	p (1-q)(1-r)(1-s) t
19	1 0 0 1 0	1	p (1-q)(1-r) s (1-t)
20	1 0 0 1 1	1	p (1-q)(1-r) st
21	1 0 1 0 0	1	p (1-q) r (1-s)(1-t)
22	1 0 1 0 1	1	p (1-q) r (1-s) t
23	1 0 1 1 0	1	p (1-q) rs (1-t)
24	1 0 1 1 1	1	p (1-q) rst
25	1 1 0 0 0	1	pq (1-r)(1-s)(1-t)
26	1 1 0 0 1	1	pq (1-r)(1-s) t
27	1 1 0 1 0	1	pq (1-r) s (1-t)
28	1 1 0 1 1	1	pq (1-r) st
29	1 1 1 0 0	1	pqr (1-s)(1-t)
30	1 1 1 0 1	1	pqr (1-s) t
31	1 1 1 1 0	1	pqrs (1-t)
32	1 1 1 1 1	1	pqrst

Analytické vyhodnocení

Při analytickém vyhodnocení vycházíme většinou z nalezeného souboru minimálních řezů, který kvantifikujeme. Pravděpodobnost výskytu jednotlivého řezu získáme vynásobením pravděpodobností výskytu událostí, které obsahuje (pracujeme s těmito událostmi, jako kdyby vstupovaly do hradla AND). Obecně lze vyčíslit pravděpodobnost výskytu vrcholové události dle aditivního teorému:

Aditivní teorém a jeho použití

Známe-li pravděpodobnosti výskytu minimálních řezů F_i ($i = 1, 2, \ldots, k$), pak pravděpodobnost výskytu alespoň jednoho z těchto řezů lze zapsat pomocí následujícího, který bývá často nazýván **aditivní teorém** nebo **věta o inkluzi a exkluzi**.

$$F_{TOP} = P\left(\bigcup_{j=1}^{k} F_j\right) = \sum_{j=1}^{k} P(F_j) - \sum_{\substack{i,j=1 \\ i\langle j}}^{k} P\left(F_i \bigcap F_j\right) + \ldots + (-1)^{k-1} P\left(\bigcap_{j=1}^{k} F_j\right)$$

Tento vztah vznikl pouze zobecněním již uvedeného výrazu: $P(Q) = P(A) + P(B) - P(A \cap B)$

pro k událostí. Pokud převedeme součet řezů $\bigcup_{j=1}^{k} F_j$ na součet vzájemně se vylučujících součinů, lze pravděpodobnost vrcholové události vyčíslit přímo, jako součet pravděpodobností těchto součinů (pravděpodobnosti průniků jsou nulové).

Příklad

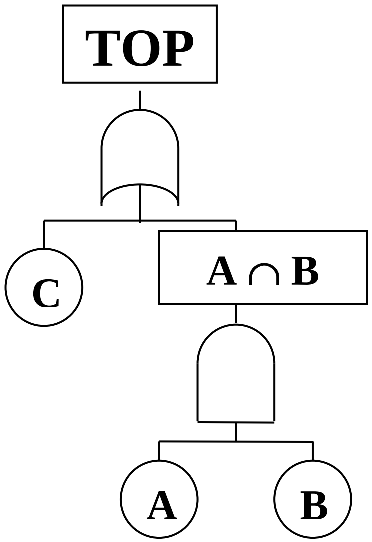
Kvantifikujte strom poruch z obr. tj. nalezněte pravděpodobnost vrcholové události F_{TOP}

Řešení

$F_{TOP} = P(\mathrm{C}) + P(A)\,.\,P(B)$

pokud

$P(\mathrm{C} \cap (\mathrm{A} \cap \mathrm{B})) = 0$



Přehled výpočetních programů pro analýzu stromem poruch současných i minulých

Pro vyhodnocení stromů poruch (kvalitativní, kvantitativní i citlivostní analýzu) byla sestavena celá řada výpočetních programů.

1. Item Software, http://www.itemsoft.com
2. BQR Reliability Engineering Ltd., Izrael, http://www.bqr.com
3. Risk Spektrum, Švédsko, http://www.riskspectrum.com/
4. Relex Software, USA, http://www.relexsoftware.com
5. IsographDirect, http://www.isographdirect.com
6. ITEM, http://www.itemuk.com

Většina těchto programových balíků je podrobně popsána v lit. [5].

Literatura

[1] Reactor Safety study (Appli. 2. Fault Tree), WASH-1400 USNRC, October 1975

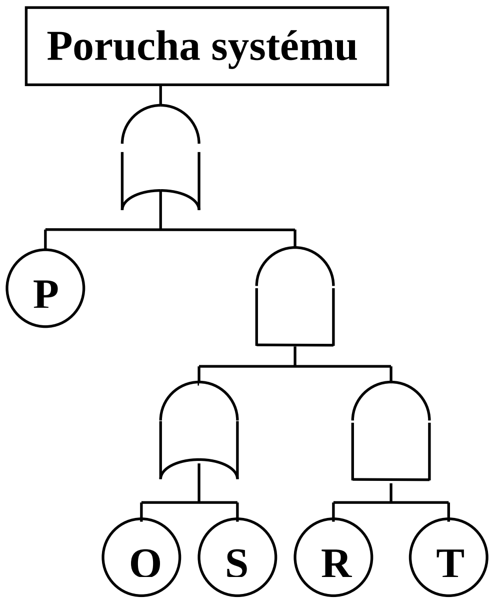
[2] W. E. Vesely at al., Fault Tree Handbook, NUREG-0492, January 1981

[4] R.E. Barlow, F. Proschan; Mathematical Theory of Reliability; SIAM 1996, ISBN 0-89871-369-2

[5] K.B. Misra, Reliability Analysis and Prediction, Elsevier 1992, ISBN 0-444-89606-6

Úloha k FTA:

1. Nalezte všechny minimální řezy pro strom poruch z obrázku.
2. Vypočítejte pravděpodobnost výstupní události z výběrového hradla „2 ze 3“ pro případ, kdy všechny vstupující události mají pravděpodobnost p = 0,3.



Řešení

1. Minimálním řezem rozumíme nejmenší možnou kombinaci primárních prvků stromu, které, nastanou-li současně, vyvolají vrcholovou událost. Počet prvků v řezu pak určuje řád tohoto řezu. Řezem 1.řádu je výskyt události P, řezy 2.řádu nejsou, řezy 3.řádu jsou: (Q,R,T), (S,R,T).

2. $T(n, j)$ je pravděpodobnost vzniku j nebo více událostí ze skupiny událostí A_n, A_{n-1}, . . . , A_1. V případě $p_1 = p_2 = \ldots = p_n = p$, tj. stejných pravděpodobností výskytu všech vstupních událostí, lze snadno dokázat, že platí

$$T(n, j) = \sum_{r=j}^{n} \binom{n}{r} p^r (1-p)^{n-r}$$

Dosadíme a dostáváme:

$$T(3,2) = \sum_{r=2}^{3} \binom{3}{r} (0{,}3)^r (0{,}7)^{3-r} = 0{,}216$$