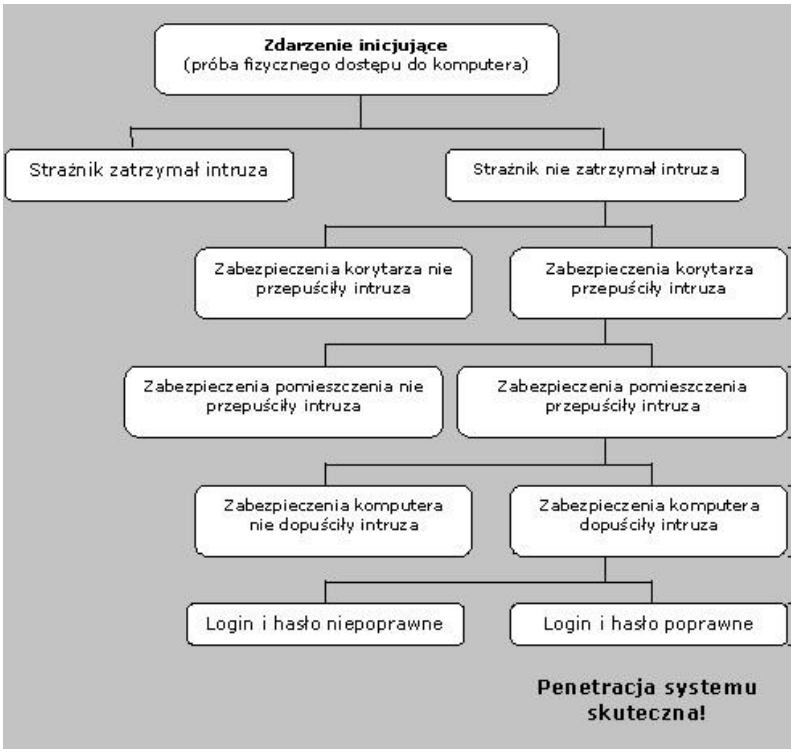
Ocena ryzyka awarii systemu za pomocą analizy drzewa usterek (FTA)



„Analiza drzewa usterek (FTA akronim od angielskiego *Fault Tree Analysis*) to metoda używana do analizy przyczyn usterek (defektów). Technika modeluje wizualnie związki logiczne pomiędzy błędami człowieka, defektami, awariami i zewnętrznymi zdarzeniami. Przykładem może być usterka kanadyjskiej maszyny do radioterapii nowotworów Therac-25. Metoda FTA (*Fault Tree Analysis*) jest zaawansowaną, dedukcyjną techniką do identyfikacji i analizy czynników, które mogą być przyczyną niepożądanych zdarzeń. Analiza drzewa błędów FTA jest graficznym modelem zależności przyczynowo-skutkowych i jest budowana w przeciwnym kierunku niż drzewo zdarzeń ETA (drzewo zdarzeń). Dzięki schematowi FTA zostają zilustrowane przyczyny, których skutek określany jest jako niepewne zdarzenie bądź ryzyko.” [5]

1. Wprowadzenie do problemu

Proces analizy ryzyka za pomocą metody drzewa usterek rozpoczyna się od identyfikacji zdarzenia szczytowego. W dalszej kolejności pozwala nam na znalezienie ścieżek krytycznych prowadzących do powstania usterki. Można wyróżnić następujące czynności związane z projektowaniem drzewa usterek opisującego awarię w systemie informatycznym, o czym mówi blog o ryzyku (pozycja [5]):

1. „Identyfikację zdarzeń zagrażających i prowadzących do powstania zdarzenia szczytowego, tzw. zdarzenia pośrednie;

2. Ustalenie hierarchicznej struktury drzewa usterek, w której brane są pod uwagę wszystkie zdarzenia pośrednie oraz powiązanie tych zdarzeń z logicznymi bramkami wyboru;
3. Określenie zdarzeń podstawowych, będących źródłem zdarzenia szczytowego;
4. Usterki najniższego poziomu drzewa usterek uznawane są jako podstawowe i kluczowe czynniki decydujące o powstaniu zdarzenia szczytowego. Na nich właśnie projekt powinien skupić szczególną uwagę i podjąć działania, które nie dopuszczą do powstania tego zdarzenia;
5. Na podstawie pojedynczych usterek oblicza się prawdopodobieństwo wystąpienia zdarzenia szczytowego. Każda usterka powinna być indywidualnie rozpatrywana."

Odpowiednio przeprowadzona analiza FTA jest niezwykle użyteczna podczas wstępnej fazy projektowania systemów informatycznych. Jest ona narzędziem oceny ryzyka wprowadzenia modyfikacji w projekcie. Po tym, jak produkt jest dostępny na rynku, analiza FTA może być natomiast zastosowana jako narzędzie do rozwiązywania problemów. Dzięki analizie produkt może być przestudiowany zarówno pod kątem niezawodności, jak i możliwości wystąpienia uszkodzenia. Z punktu widzenia niezawodności, analiza FTA może pomóc w oszacowaniu, czy produkt spełni wymagania dotyczące niezawodności eksploatacyjnej. Analiza drzewa usterek, zgodnie z pozycją [6], może być użyta do:

1) Analizy funkcjonalnej wysoce skomplikowanych systemów;
2) Obserwacji efektów jednoczesnego, niekrytycznego zdarzenia na zdarzenie szczytowe;
3) Określenia wymogów i specyfikacji bezpieczeństwa;
4) Określenia niezawodności systemu;
5) Określenia działań ludzkich;
6) Określenia interfejsu oprogramowania;
7) Zidentyfikowania potencjalnych wad projektowych i zagrożeń bezpieczeństwa;
8) Określenia potencjalnych czynności naprawczych.

W celu zrozumienia idei FTA w następnym rozdziale zostaną podane wybrane definicje i własności prawdopodobieństwa.

2. Elementy teorii prawdopodobieństwa

W celu zrozumienia idei FTA w następnym rozdziale zostaną podane wybrane definicje i własności prawdopodobieństwa:

Definicja 1. [7] Jeśli Ω jest ustalonym zbiorem, to rodzinę F złożoną z jego podzbiorów nazywamy Б – ciałem (sigma - ciałem) podzbiorów zbioru, jeżeli spełnione są następujące warunki:

A1) $\emptyset \in F$,

A2) Jeśli $A \in F$ to również $A' \in F$,

A3) Suma przeliczalnie wielu zbiorów należących do F również należy do F,

oraz

Definicja 2. [7] Prawdopodobieństwem nazywamy dowolną funkcję P określoną na Б – ciele zdarzeń $F \subset 2^{\Omega}$, która spełnia warunki:

B1) $P(A) \geq 0$,

B2)$P(\Omega) = 1$,

B3) Jeśli $A_n \in F, n \in N$ oraz $A_i \cap A_j = \emptyset$ dla $i \neq j$, to $P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i)$.

Z wyżej podanych definicji wynikają następujące własności prawdopodobieństwa:

W1) $0 \leq P(A) \leq 1$,

W2) $P(\emptyset) = 0$,

W3) $P(A') = 1 - P(A)$,

W4) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

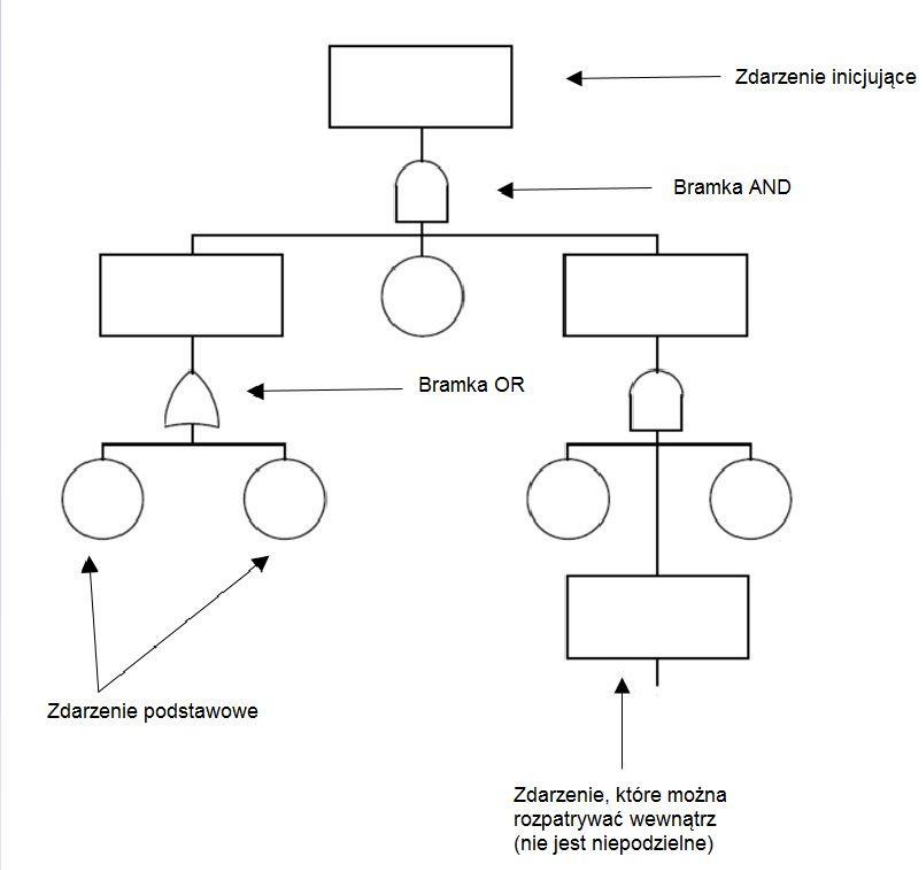
Zbiory A oraz B nazywane są **zdarzeniami**. Przy analizie drzewa usterek ważne jest pojęcie niezależności zdarzeń, dla których obliczane jest prawdopodobieństwo.

Definicja 3. [7] Niech P będzie prawdopodobieństwem zdefiniowanym na Б – ciele F. Zdarzenia $A, B \in F$ są niezależne, jeśli $P(A \cap B) = P(A)P(B)$.

Zdarzenia opisane w drzewie usterek na ogół nie mają części wspólnej, czyli $P(A \cap B) = 0$. Mając przedstawione podstawowe pojęcia i własności związane z prawdopodobieństwem można zacząć projektować drzewo usterek, ale to wszystko prezentuje następny rozdział.

3. Symbole stosowane w FTA

Symbole stosowane w drzewie usterek mogą być różnie prezentowane. Jednak jego idea pozostaje zawsze taka sama. Nie jest ważny wygląd symboli opisujących zdarzenia (ponieważ może to być kwestia indywidualna systemu, np. typ przetwarzanych danych), lecz sposób połączenia i oddziaływania tych zdarzeń pomiędzy sobą za pomocą bramek logicznych. Model ten wzorowany jest na bramkach logicznych znanych z elektroniki, ale nie w 100% identycznych. W niniejszym artykule zastosowane zostaną symbole przedstawione na rysunku poniżej.



Rysunek 1: Przykładowy schemat drzewa usterek [opracowanie własne]

Uwaga! Zasada konstruowania drzewa usterek jest taka, że nie łączy się bramek ze sobą bezpośrednio. Pomiędzy bramkami muszą znajdować się zdarzenia. Często obliczenie prawdopodobieństwa awarii wiąże się z tym, że należy poprosić o pomoc eksperta z danej dziedziny. Metoda delficka to jednak nie jedyna ze stosowanych metod szacowania prawdopodobieństwa ryzyka awarii.

4. Obliczanie prawdopodobieństwa awarii za pomocą drzewa usterek

4.1. Bramka OR

Bramka OR realizuje funkcję prawdopodobieństwa sumy zdarzeń, które do niej wchodzą. Jeśli bramka OR ma dwa wejścia, które powiązane są ze zdarzeniami A oraz B, to na wyjściu tej bramki będzie wartość opisana następującym wzorem:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

W tym przypadku wymagana jest wiedza, jakie jest prawdopodobieństwo zdarzenia $A \cap B$. Jeśli bramka OR ma trzy wejścia związane ze zdarzeniami A,B oraz C, to na wyjściu pojawi się wartość obliczona wg wzoru:

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - [P(A \cap B) + P(A \cap C) + P(B \cap C)] + P(A \cap B \cap C).$$

Wyznaczenie prawdopodobieństwa sumy wielu wymaga znajomości rachunku zbiorów oraz zaawansowanej teorii prawdopodobieństwa. Jeśli zdarzenia A, B, C wykluczają się parami (nie mają części wspólnych), to

$$P(A \cup B \cup C) = P(A) + P(B) + P(C).$$

4.2. Bramka AND

Bramka AND realizuje funkcję prawdopodobieństwa iloczynu (części wspólnej) zdarzeń, które do niej wchodzą. Jeśli bramka AND ma dwa wejścia, które powiązane są ze zdarzeniami A oraz B (a takie na ogół występują w drzewie usterek), to na wyjściu tej bramki będzie wartość opisana następującym wzorem:

$$P(A \cap B) = P(A)P(B).$$

Jeśli bramka AND ma n wejść i wszystkie wchodzące zdarzenia A_i są niezależne, to ma miejsce wzór:

$$P(A_1 \cap \ldots \cap A_n) = P(A_1) \cdot \ldots \cdot P(A_n).$$

4.3. Bramka EX-OR

Czasami zdarza się, że drzewo usterek zawiera bramkę, którą jest nazywana **bramką EX-OR.** Ta bramka realizuje funkcję prawdopodobieństwa sumy zdarzeń, z tą różnicą, że prawdopodobieństwo na wyjściu bramki jest obliczane wg wzoru:

$$P(A \cup B) = P(A) + P(B) - 2P(A \cap B).$$

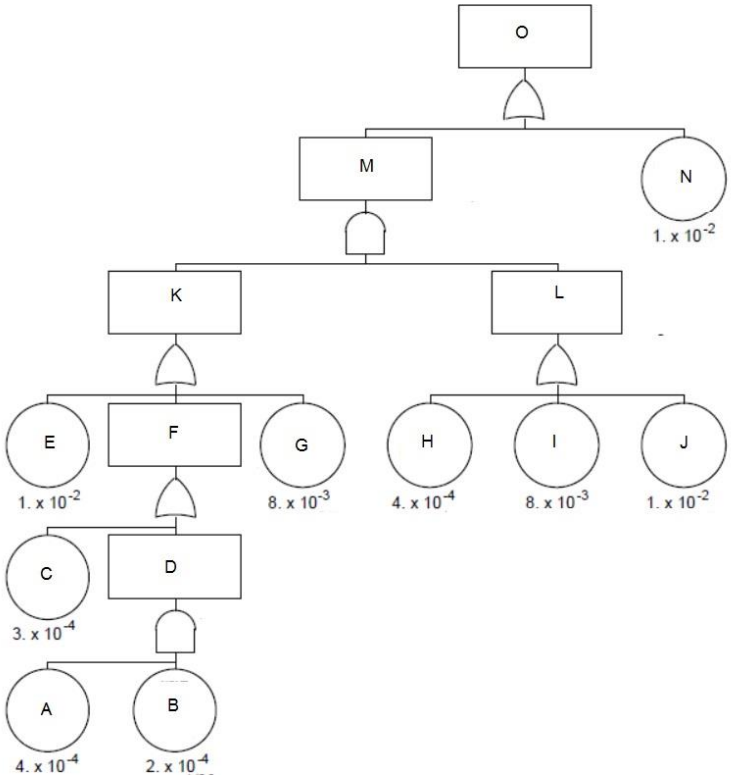
Relacje pomiędzy zdarzeniami na wejściach bramki są takie, że **zdarzenie A albo zdarzenie B** spowoduje awarie, natomiast zaistnienie dwóch zdarzeń w jednej chwili nie spowoduje awarii. Dla trzech zdarzeń wchodzących do bramki EX-OR słuszny będzie wzór:

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - [P(A \cap B) + P(A \cap C) + P(B \cap C)].$$

Idea zastosowania tej bramki w drzewie usterek jest taka, że tylko **jedno zdarzenie** może spowodować awarię.

5. Przykład zastosowania drzewa usterek w praktyce

Niech dane będzie drzewo usterek dla pewnego systemu informatycznego (rysunek 2):



Rysunek 2: Przykładowe drzewo usterek z wartościami prawdopodobieństwa awarii podstawowych komponentów [opracowanie własne]

Duże litery to nazwy zdarzeń, a pod symbolami dane są wartości prawdopodobieństwa awarii związanej z konkretnym zdarzeniem. Niech zdarzenia opisane dużymi literami będą parami niezależnymi oraz wykluczającymi się, P będzie funkcją prawdopodobieństwa oraz wszystkie zdarzenia są elementami pewnego Б-ciała (wystarczy wziąć rodzinę wszystkich podzbiorów zbioru, z którego wydzielone są zdarzenia). Zdarzenie O to zdarzenie inicjujące i dla tego zdarzenia należy wyznaczyć wartość $P(O)$. Wobec tego:

$$P(O) = P(M) + P(N) \ (1)$$

$$P(O) = P(K)P(L) + P(N) \ (2)$$

$$P(O) = [P(E) + P(F) + P(G)] \cdot [P(H) + P(I) + P(J)] + P(N) \ (3)$$

$$P(O) = [P(E) + P(C) + P(D) + P(G)] \cdot [P(H) + P(I) + P(J)] + P(N) \ (4)$$

$$P(O) = [P(E) + P(C) + P(A)P(B) + P(G)] \cdot [P(H) + P(I) + P(J)] + P(N) \ (5)$$

Po podstawieniu wartości do wzoru (5) otrzymujemy w przybliżeniu prawdopodobieństwo wystąpienia awarii:

$$P(O) = 0{,}0103 = 1{,}03\ \%.$$

Należy zaznaczyć, że awaria systemu nie musi automatycznie wiązać się z negatywnymi konsekwencja dla klienta czy użytkownika – przykładowo: analizując ryzyko w przemyśle lotniczym najpierw bierze się pod uwagę prawdopodobieństwo wystąpienia zdarzenia np. awarii silników, a następnie liczy się prawdopodobieństwo, że ta awaria doprowadzi do tragiczne zdarzenia, jakim jest katastrofa.

6. Ekspotencjalny model prawdopodobieństwa awarii

Model ekspotencjalny wiąże się z obliczaniem współczynnika $\boldsymbol{MTBF}$, znanego nie tylko z informatyki. $\boldsymbol{MTBF}$ (*Mean Time Between Failures*) – to średni czas wyrażony w godzinach, w którym urządzenie może działać bez przerwy (awarii). $MTBF$ jest stosowany m.in. w informatyce oraz zarządzaniu ryzykiem. Dla produktów, współczynnik $MTBF$ oparty jest na badaniach lub też przewidywaniach. Dla wielu osób jest dowodem wysokiej jakości produktu. Mając podany współczynnik $MTBF$, oblicza się kolejny współczynnik λ nazywany współczynnikiem awarii (*ang. Fault rate*) wg następującego wzoru:

$$\lambda = \frac{1}{MTBF}.$$

Sporo systemów ma stały współczynnik λ, a przy takim założeniu prawdopodobieństwo awarii danego zdarzenie jest równe:

$$\boldsymbol{e}^{-\lambda T},$$

gdzie T jest pewnym interwałem czasowym szacowanym wg relacji $T \leq 0{,}2 \cdot MTBF$. Nie zawsze jednak ten model jest dobry. Oszacowanie prawdopodobieństwa może wymagać innych metod zależnych od wielu czynników wewnętrznych oraz zewnętrznych związanych z danym systemem.

Podsumowanie

Głównym celem artykułu było zebranie najważniejszych informacji dotyczących metody analizy drzewa usterek, uświadomienie czytelnikowi na czym ta metoda polega, kiedy ją można zastosować oraz pokazanie przykładu jej zastosowania. Metoda ta nie jest znana osobom związanym z testowaniem oprogramowania, być może dlatego, że nie jest zbyt często opisywana w polskiej literaturze przedmiotu oraz nie zawsze jest ujęta w programie nauczania na kierunkach informatycznych.

Referencje

[1] Coppit D., Sullivan K. J., *Formal specification in collaborative design of critical software tools,* In Proceedings Third IEEE International High-Assurance Systems Engineering Symposium, p. 13-20, IEEE, Washington D.C., 13-14 November 1998.

[2] Helmer G., Wong J., Slagell M., Honavar V., Miller L., Lutz R., *A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System,* Springer-Verlag London Limited, 2002.

[3] Henley E. J., Kumamoto H., *Probabilistic Risk Assessment,* IEEE Press, 1992.

[4] http://relia-sol.pl/informacje/failure-analysis/what-are-failure-analysis-methods/

[5] http://blogoryzyku.blogspot.com

[6]http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjRpPvCjazJAhXppXIKHRlxDrcQFggfMAA&url=http%3A%2F%2Futk.gov.pl%2Fdownload%2F1%2F10301%2FPrzewodnikCSMM.pdf&usg=AFQjCNEglz1RuInplJzPnCjqcFPYoCQg2A&sig2=AuQ3UfgD8oePwor6CVWe9w&bvm=bv.108538919,bs.2,d.bGQ&cad=rja

[7] Krysicki W., Bartos J., Dyczka W., Królikowska K., Wasilewski., *Rachunek prawdopodobieństwa i Statystyka matematyczna w zadaniach,* PWN, Warszawa, 2005.

Autor

Marek Żukowicz jest absolwentem matematyki na Uniwersytecie Rzeszowskim. Obecnie pracuje jako tester. Jego zainteresowania skupiają się wokół testowania, matematyki, zastosowania algorytmów ewolucyjnych oraz zastosowania matematyki w procesie testowania. Interesuje się również muzyką, grą na akordeonach oraz na perkusji.

Recenzenci

Radosław Smilgin, Grzegorz Libor

Analiza drzewka usterek omawiana jest na szkoleniu ISTQB Poziom Zaawansowany - Kierownik Testów.