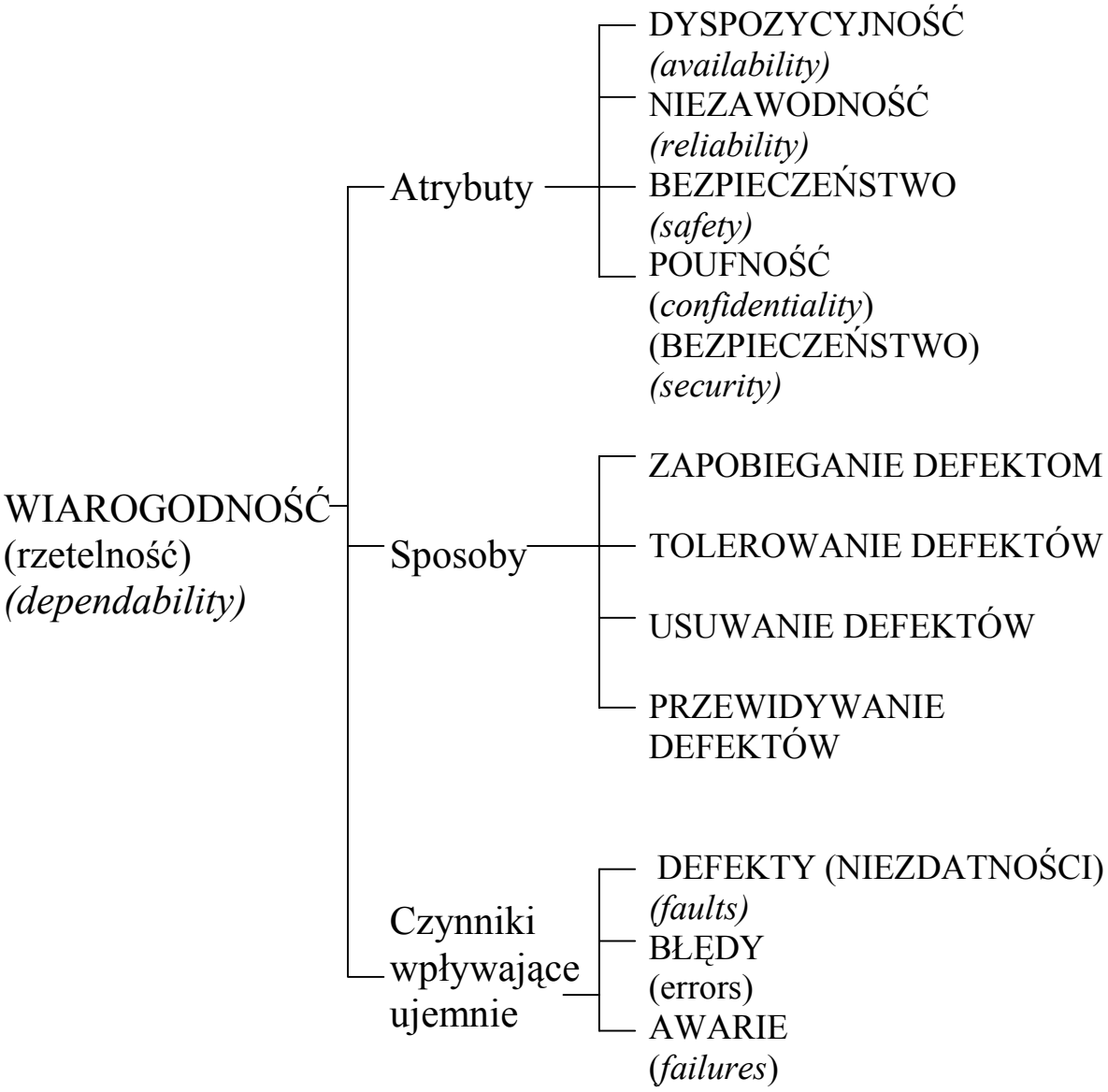
METODY ANALIZY BEZPIECZEŃSTWA SYSTEMÓW KOMPUTEROWYCH

Zagadnienia:

1) Wyjaśnienie pojęć związanych z bezpieczeństwem.
2) Norma IEC 1508.
3) Metody analizy bezpieczeństwa:
   a) analiza drzew niezdatności (FTA),
   b) analiza rodzajów i skutków uszkodzeń (FMEA),
   c) analiza hazardu i gotowości systemu (HAZOP),
   d) obiektowe podejście do analizy bezpieczeństwa.
4) Podsumowanie.

DRZEWO ZALEŻNOŚCI POMIĘDZY POJĘCIAMI DOTYCZĄCYMI WIARYGODNOŚCI



ANALIZA BEZPIECZEŃSTWA

Analiza bezpieczeństwa jest procesem, w ramach którego oceniany jest poziom ryzyka związanego z systemem i identyfikowane są mechanizmy występowania wypadków. Zdarzenia prowadzące w sposób bezpośredni do wypadku nazywane są stanami hazardowymi lub hazardami.

Analiza bezpieczeństwa jest częścią **cyklu życia bezpieczeństwa** – według standardu IEC 1508, wykonywana jest w ramach kolejnych etapów cyklu życia systemu:

- Podczas budowy systemu – w celu identyfikacji zagrożeń i dobrania właściwych środków projektowania i realizacji;
- Podczas eksploatacji systemu – w celu sprawdzenia i/lub poprawienia stanu bezpieczeństwa systemu;
- Podczas oceny systemu przez niezależną instytucję certyfikującą, dla sprawdzenia stopnia bezpieczeństwa i zaakceptowania (lub odrzucenia) systemu do użytkowania.

Norma IEC 1508

Norma IEC 1508:

- wprowadza pewną terminologię opisu problemu,
- precyzuje miary bezpieczeństwa systemu,
- definiuje strategię postępowania
- rekomenduje metody, odpowiednie do zastosowania w różnych fazach projektu.

Hazard (*hazard*)– definiuje jako sytuację mogącą spowodować śmierć lub obrażenia ludzi.
Ryzyko (*risk*) – jest miarą stopnia zagrożenia, wyrażającą zarówno stopień szkodliwości hazardu, jak i p-stwo jego wystąpienia.

Prawdopodobieństwo, że elementy zabezpieczające prawidłowo wykonają wymagane funkcje jest nazywane **integralnością zabezpieczeń** (*safety integrity*). Norma wyróżnia cztery poziomy integralności zabezpieczeń, określone przez prawdopodobieństwa awarii.

Poziom integralności (*SIL*)	**Praca start-stopowa: p-stwo błędu**	**Praca ciągła: p-stwo błędu w ciągu godziny**
4	10^{-5} do. 10^{-4}	10^{-9} do 10^{-8}
3	10^{-4} do 10^{-3}	10^{-8} do 10^{-7}
2	10^{-3} do 10^{-2}	10^{-7} do 10^{-6}
1	10^{-2} do 10^{-1}	10^{-6} do 10^{-5}

Zalecenia dotyczące metod oceny bezpieczeństwa

	Metoda lub technika	SIL 1	SIL 2	SIL 3	SIL 4
1	Kwestionariusze ocen	R	R	R	R
2	Tablice decyzyjne i tablice prawdy	R	R	R	R
3	Miary złożoności programów	R	R	R	R
4	Diagramy przyczynowo-skutkowe (CCD)	R	R	R	R
4a	Analiza drzewa zdarzeń (ETA)	R	R	R	R
5	Analiza drzewa niezdatności (FTA)	R	R	HR	HR
6	Analiza rodzajów i skutków uszkodzeń (FMEA)	R	R	HR	HR
7	Analiza hazardu i gotowości systemu (HAZOP)	R	R	HR	HR
8	Modele Markowa	R	R	R	HR
9	Schematy blokowe niezawodności	R	R	R	R
10	Symulacja (Monte-Carlo)	R	R	R	R

Metoda analizy drzew niezdatności (FTA)
(fault tree analysis)

Dwa rodzaje analizy:
- Jakościowa:
  - oparta o wnioskowanie matematyczne – pozwala wypowiadać się o zależnościach przyczynowo-skutkowych;
- Ilościowa:
  - pozwala określić prawdopodobieństwo awarii oraz jej przyczyn

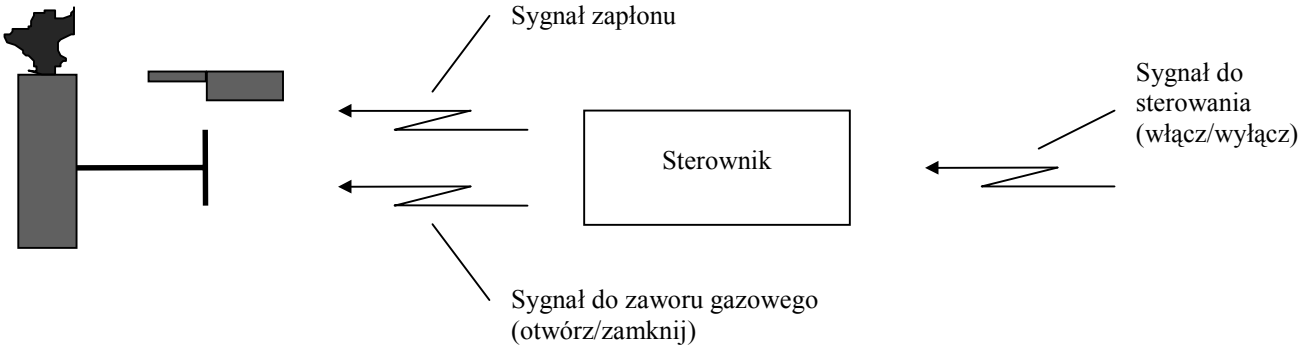
Główne cele metody:
- identyfikację przyczyn powodujących wystąpienie stanów niebezpiecznych,
- określenie częstości wystąpień stanów niebezpiecznych,
- Identyfikacja krytycznych elementów systemu.

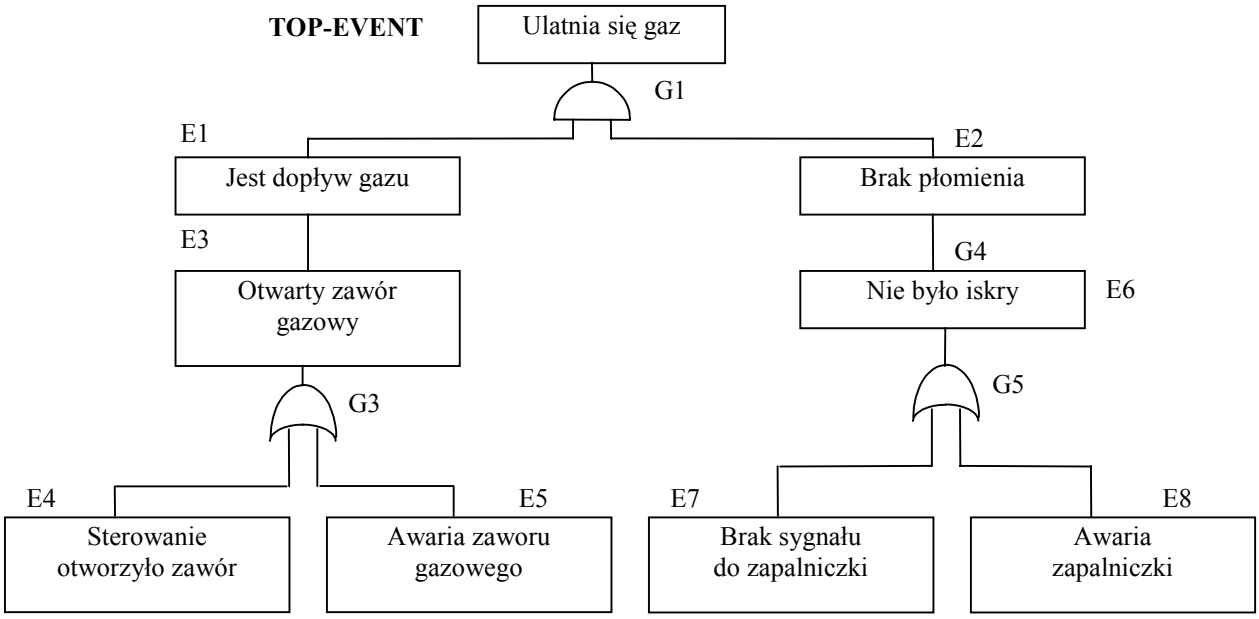
Metoda drzew niezdatności składa się z kilku kroków:
- Przygotowanie analizy:
  - definicja zakresu analizy,
  - zapoznanie się z systemem, jego funkcjami, zasadami działania,
  - identyfikacja stanu niebezpiecznego;
- Konstrukcja drzewa;
- Analiza drzewa i opracowanie wyników.

Konstrukcja drzewa:

- Każdy znany stan niebezpieczny stanowi punkt wyjścia dla oddzielnego drzewa niezdatności;
- Podstawowe elementy drzewa to zdarzenia (*events*) oraz bramy (*gates*);
- Drzewo jest budowane poprzez cykliczne powtarzanie jednego kroku – jakim jest dodanie bezpośrednich przyczyn zdarzenia będącego liściem drzewa.

Przykład. System palnika gazowego





Analiza minimalnych zbiorów przyczyn

Minimalnym zbiorem przyczyn (MZP) nazywany jest taki najmniejszy zbiór zdarzeń, dla którego wystąpienie wszystkich jego elementów powoduje stan niebezpieczny.

Analiza probabilistyczna obejmuje wyznaczenie**:**

- Niedostępności systemu *Q(t)* (*system unavailability*) – czyli prawdopodobieństwa zdarzenia szczytowego;
- Udziału MZP w niedostępności systemu, wyznaczanego procentowo;
- Współczynnika zwiększenia ryzyka RIF dla zdarzenia *i;*
- Współczynnika obniżenia ryzyka RDF dla zdarzenia *i;*
- Udziału w niedostępności systemu FC dla zdarzenia *i.*

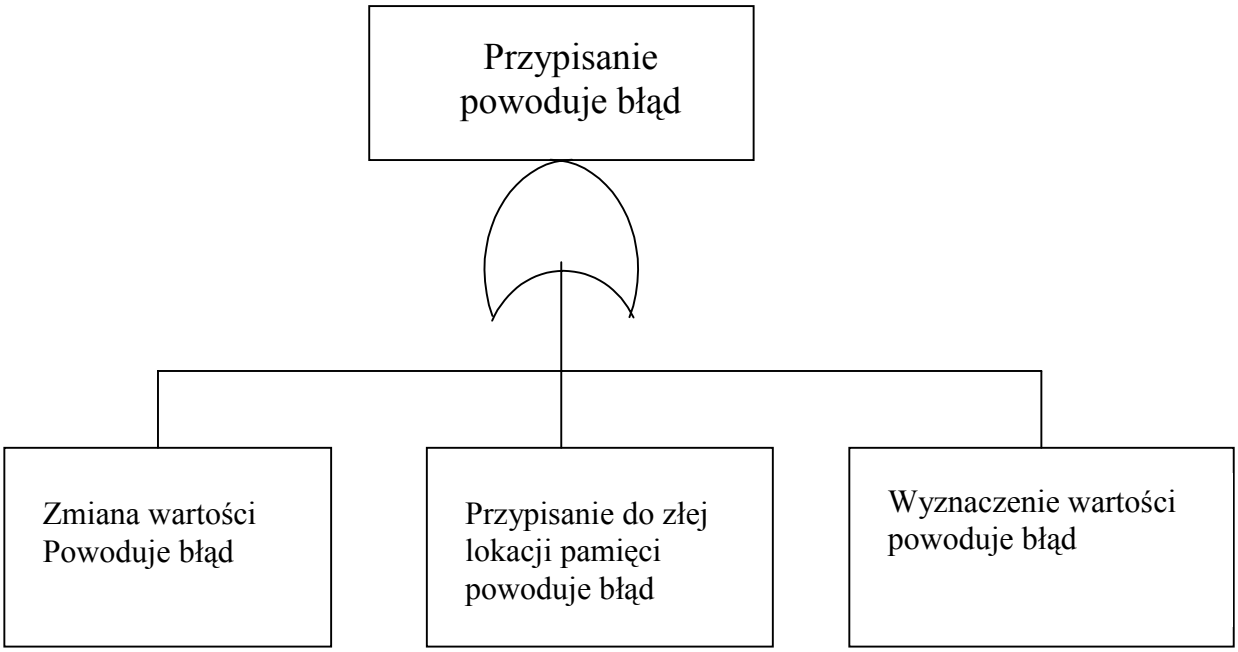
Analiza drzew błędów oprogramowania (SFTA)

Analiza oprogramowania wymaga innego podejścia.

Podczas konstrukcji drzewa określane są możliwe ścieżki dojścia do niebezpiecznego stanu oprogramowania. Dla każdej ścieżki prowadzącej do stanu niebezpiecznego ocenia się, czy jej wystąpienie jest możliwe. Analiza drzewa błędów daje wynik pozytywny, czyli stwierdza, że program nie powoduje stanu niebezpiecznego, jeżeli zostanie wykazane, że wszystkie ścieżki prowadzące do takiego stanu są niemożliwe.

Dla każdej konstrukcji programowej : przypisanie, instrukcja warunkowa IF oraz CASE, pętle WHILE, FOR posługujemy się szablonem dla określenia błędu danej instrukcji.

Szablon dla instrukcji przypisania



Szablony zawierają wszystkie możliwe przyczyny błędu danej konstrukcji języka programowania. Podczas analizy konkretnego programu należy stosować je w całości jako fragmenty drzewa błędów, a następnie odrzucać zdarzenia niemożliwe.

Przykładowo dla instrukcji przypisania:

x:=7;

gdzie x jest zmienną typu INTEGER, zdarzenie „wyznaczenie wartości powoduje błąd" jest niemożliwe.

Integracja analizy oprogramowania oraz systemu

Standardowa procedura postępowania:

- Utworzenie systemowego drzewa w tradycyjny sposób;
- Niektóre zdarzenia podstawowe tego drzewa dotyczą błędów oprogramowania;
- Dla tych zdarzeń tworzone są osobne poddrzewa metodą SFTA.

Drzewa niezdatności z zależnościami czasowymi

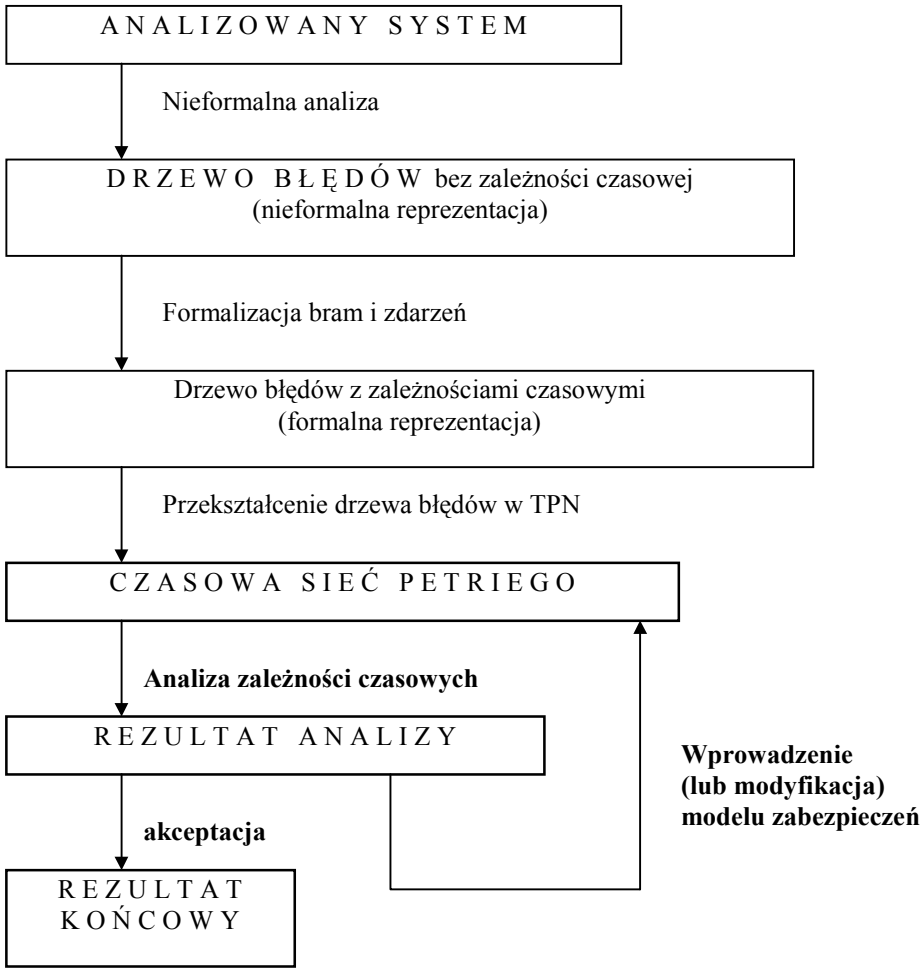
W podanym przykładzie systemu palnika gazowego hazard wystąpi dopiero, kiedy zdarzenia E1 i E2 będą występowały razem odpowiednio długo.
Aby uniknąć niejednoznaczności, przeprowadza się formalizację drzewa błędów. W rezultacie otrzymamy opisy bram:

- G1:

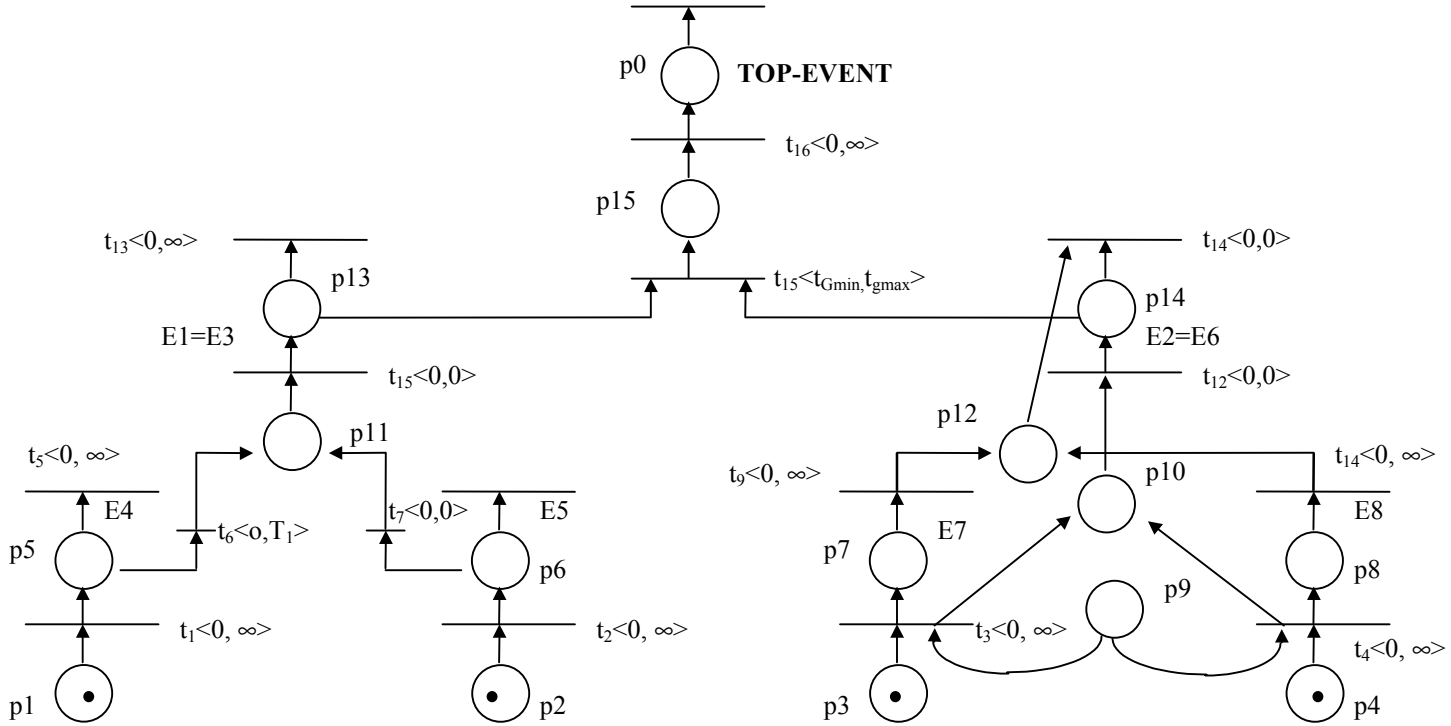
$$occur(top\_event) \Rightarrow occur(e1) \wedge occur(e2) \wedge duration(e1 \wedge e2) > t_{Gmin}$$

$$\wedge max(start(e1), start(e2)) + t_{Gmin} \leq start(top\_event) \leq max(start(e1), start(e2)) + t_{Gmax}$$

- G2, G4: . . .



Wykorzystanie czasowych sieci Petriego (TPN)



Metoda analizy rodzajów i skutków uszkodzeń (FMEA) oraz jej rozszerzenie o ocenę stanów krytycznych FMCEA (*Failure Modes, Effects and Criticality Analysis***)**

Przedmiotem FMEA może być zarówno **architektura**, jak i **proces realizacji systemu.**

W odniesieniu do architektury systemu, FMEA polega na identyfikacji i analizie możliwych **stanów uszkodzeń elementów** systemu, wyznaczaniu wpływu, jakie te stany mogą mieć na działanie innych elementów i całego systemu oraz na ocenie możliwych konsekwencji tego wpływu na środowisko zewnętrzne.

Stany uszkodzeń systemu są definiowane przez powiązanie ich z klasami możliwych usterek/wad/defektów (trwałych lub przemijających).

W metodzie FMEA zakłada się, że **struktura systemu** i **dane o jego elementach są znane**.
W szczególności, zidentyfikowane zostały czynniki podstawowe – najniższy poziom elementów struktury, o którym mamy dostateczną wiedzę, dotyczącą możliwych stanów uszkodzeń każdego elementu, ich funkcjonowania i zależności między nimi.
Poziom ten zależy od **celu i zakresu** analizy i stanowi punkt wyjścia do analizy FMEA.

Analizę FMEA stosujemy wtedy, gdy:

- Liczba stanów wyjściowych systemu jest duża i potrzebujemy techniki wspierającej identyfikację możliwych stanów systemu;
- Podejrzewamy, że system może „produkować" nieakceptowalne stany wyjściowe, których nie znamy;
- Istnieje potrzeba poprawy konstrukcji, rozpoznawania problemów diagnostyki, przygotowania specyfikacji i planu testów.

Analizy **FMEA** oraz **FTA** uzupełniają się. Analiza FMEA może być wykorzystana do uzasadnienia poprawności wyborów w trakcie analizy FTA, dotyczących zdarzeń elementarnych.

Kolejne kroki FMEA:

Określenie celu i zakresu analizy:
Przygotowanie funkcjonalnego diagramu blokowego systemu + (opisy, diagramy, modele i dane o strukturze);
Wybór wyjściowego poziomu struktury i elementów do analizy.

Definicja potencjalnych typów uszkodzeń:
Ustalenie czynników i prawdopodobnego mechanizmu uszkodzeń dla każdego elementu z poziomu wyjściowego analizowanej struktury;
Ustalenie działań personelu autoryzowanego i nieautoryzowanego

Identyfikacja wpływu wyróżnionych typów uszkodzeń na działanie innych elementów i całego systemu:
Identyfikacja prawdopodobnego wpływu tych uszkodzeń na inne elementy, podsystemy w wyższej warstwie struktury i w konsekwencji na cały system;
Identyfikacja metod wykrywania błędów lub uszkodzeń.

Ocena ryzyka związanego z wyróżnionymi typami uszkodzeń:
Oszacowanie skutków uszkodzeń;
Wyznaczenie prawdopodobieństwa (lub innych charakterystyk liczbowych) wystąpienia danych typów uszkodzeń (np., *intensywność uszkodzeń*);
Klasyfikacja uszkodzeń, ustalenie priorytetów dla działan korekcyjnych.

Przygotowanie dokumentacji błędów i uszkodzeń.

Nr	Element/ Proces	Funkcja/ Cel	Typ uszkodzenia	Efekt uszkodz.	Przyczyna	Planowana metoda testowania	Dział. napra -wcze

Analiza hazardu i gotowości systemu wg metody HAZOP
(Hazard and Operability Studies)

Metoda ma charakter półformalnej procedury inspekcji dokumentacji systemu, mającej na celu identyfikacje odstępstw od założonego działania i oceny ich wpływu na bezpieczeństwo.

Założenie:
Wypadki są powodowane odstępstwami od przyjętych założeń projektowych.

- Aby zmniejszyć ryzyko pominięcia jakiejś sytuacji niebezpiecznej, HAZOP jest wykonywany w sposób systematyczny, obejmując swym zasięgiem każdy fragment badanej reprezentacji systemu.
- HAZOP wykrywa odstępstwa, które występują w przepływie pomiędzy komponentami. Przyjmuje się, że usterki zlokalizowane w komponentach prowadzą do zakłóceń w przepływie.

Wykorzystywane pojęcia:

Połączenie – (*interconnection*) fizyczne lub logiczne powiązania pomiędzy dwoma komponentami, definiujące interakcje lub relacje pomiędzy nimi;
Przepływ – (*flow*) logicznie wyodrębniona, składowa część połączenia;
Parametr - (*attribute*) fizyczna bądź logiczna właściwość przepływu;
Odstępstwo – (*deviation*) odchylenie wartości parametru od założonych;
Słowo przewodnie – (*guideword*) słowo lub fraza, która określa typ odstępstwa.

Reprezentacja systemu

Jednym z problemów związanych ze skutecznością metody HAZOP jest wybór odpowiedniej reprezentacji systemu, w oparciu o którą będzie przeprowadzana analiza.

Słowa przewodnie

Badanie odstępstwa opiera się na analizie wybranego parametru przepływu, korzystając z interpretacji słowa przewodniego. Standard HAZOP proponuje następującą listę słów przewodnich (dla systemów programowalnych):

NO	nie
MORE	więcej
LESS	mniej
AS WELL AS	jak również
PART OF	część z
REVERSE	odwrotnie, w przeciwnym kierunku
OTHER THAN	inaczej niż

Dla zależności czasowych:

EARLY	(za) wcześnie, wcześniej
LATE	(za) późno
BEFORE	przed
AFTER	po

Uczestnicy analizy i ich role:

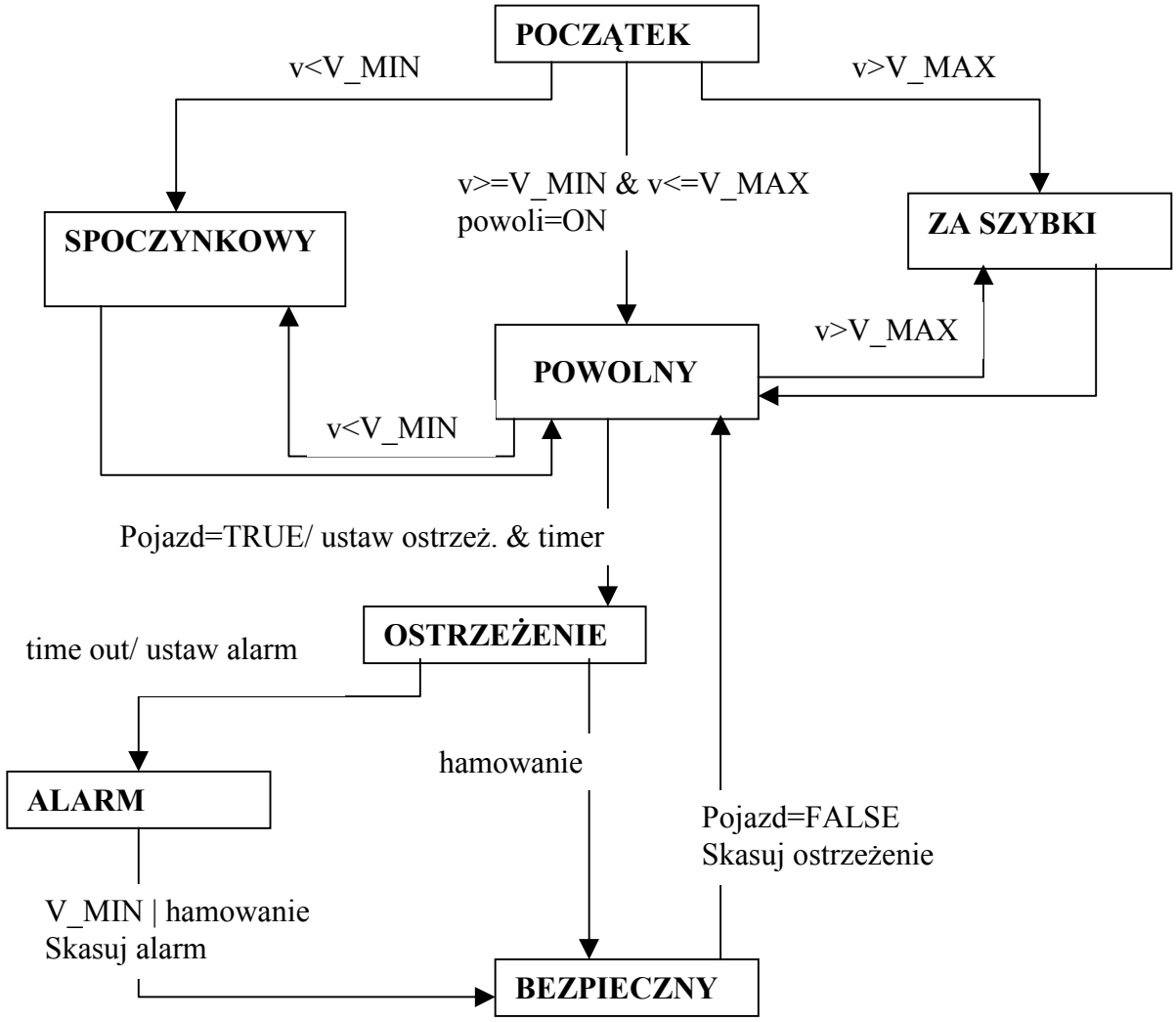
- lider,
- ekspert,
- projektant,
- użytkownik,
- sekretarz.

Przykład . Samochodowy system unikania kolizji.
Celem systemu jest wykrycie obecności pojazdu znajdującego się przed samochodem i uniknięcie uderzenia w jego tył.

System składa się z :

- czujnika radarowego,
- czujnika hamulca,
- systemu ostrzegającego.

Model dynamiki systemu



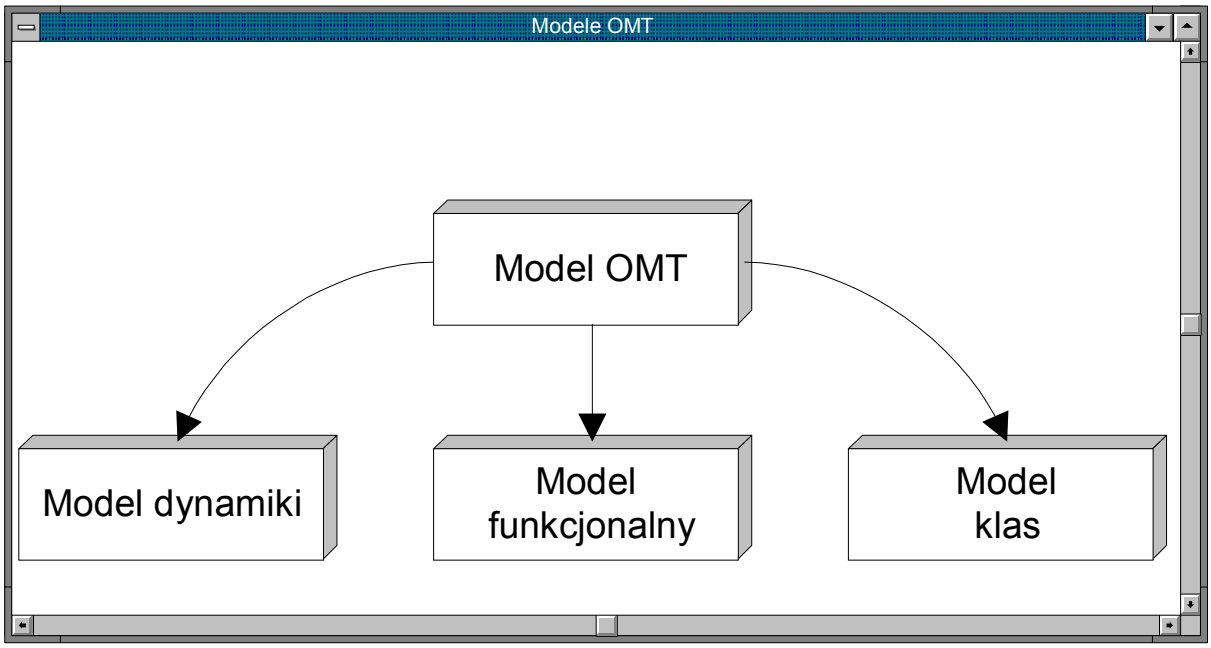
Fragment tabeli HAZOP dla systemu unikania kolizji

	Połączenie	Para-metr	Słowo przewod-nie	Przyczyna	Skutki	Zaleceni e/ komenta rz
1	POCZĄTEK - SPOCZYNKOWY	Zdarz.	NO	Uszkodzenie czujnika prędkości	Brak	
2	POCZĄTEK - SPOCZYNKOWY	Zdarz.	LESS	Brak	Brak	
3	POCZĄTEK - SPOCZYNKOWY	Zdarz.	AS WELL AS	Pojazd znajdujący się z przodu może się cofnąć	Brak ostrzeżenia ze strony systemu	
. . .	...					
	POCZĄTEK - POWOLNY	Zdarz.	OTHER THEN	Koło napędzające w poślizgu/ czujnik prędkości będzie sygnalizował prędkość znacznie przewyższającą rzeczywistą	**System nie zostanie uaktywniony**	

Obiektowe podejście do analizy bezpieczeństwa

Charakterystyka OMT

- Metodyka OMT wprowadza notację graficzną dla reprezentacji obiektów i ich związków;
- Proponuje zestaw procedur postępowania prowadzących od wymagań na system, przez coraz bardziej szczegółowe modele obiektowe, aż do odpowiedniego oprogramowania;
- Model składa się z 3 części pokrywających różne aspekty systemu.



Fazy realizacji systemu:

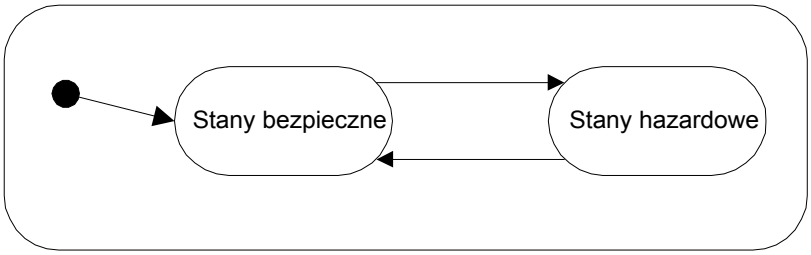
- Analiza
- Projekt systemu
- Projekt klas
- Implementacja

Metoda obiektowej analizy bezpieczeństwa systemów komputerowych

Modelowanie misji systemu
(zapożyczono rozwiązanie proponowane przez OMT dla fazy analizy)

Analiza bezpieczeństwa misji
Celem jest wykrycie niebezpiecznych błędów projektowych systemu sterowania (np., dotyczących zależności czasowych, współbieżności, itp.) .
Model ukierunkowany na misję nie pokrywa aspektu bezpieczeństwa.

Wprowadzany jest model hazardu, który jawnie rozróżnia stany bezpieczne i niebezpieczne:



Analiza wpływu błędów na bezpieczeństwo systemu
Celem tego kroku jest systematyczna identyfikacja możliwych błędów instalacji oraz środowiska.

Monitorowanie bezpieczeństwa
Wprowadzany jest monitor bezpieczeństwa, którego jedynym celem jest nadzór bezpieczeństwa systemu.