

POLITECHNIKA KOSZALIŃSKA
ZAKŁAD SYSTEMÓW MULTIMEDIALNYCH I SZTUCZNEJ
INTELIGENCJI

Analiza drzew niezdatności z zależnościami czasowymi

dr inż. Paweł Skrobanek
(pawel.skrobanek@tu.koszalin.pl)

Koszalin 2018

Plan

- Wprowadzenie
- Drzewa niezdatności - DN (ang. fault trees)
- Drzewa niezdatności z zależnościami czasowymi
- DNZC (ang. fault trees with time dependencies)
- Analiza DNZC
- Podsumowanie

Wprowadzenie

SZKODA (źródło: PN-EN 61508)

ang. harm

- obrażenia fizyczne lub uszczerbek dla życia ludzkiego spowodowany bezpośrednio lub pośrednio poprzez zniszczenia w mieniu lub środowisku

HAZARD /niebezpieczeństwo, zagrożenie/

ang. hazard

- potencjalne źródło powstania szkody

Wprowadzenie

SYSTEM ZWIĄZANY Z BEZPIECZEŃSTWEM (ang. safety - related system)

- taki, który bezpośrednio lub poprzez zainicjowanie zdarzeń pośredniczących może doprowadzić do szkody

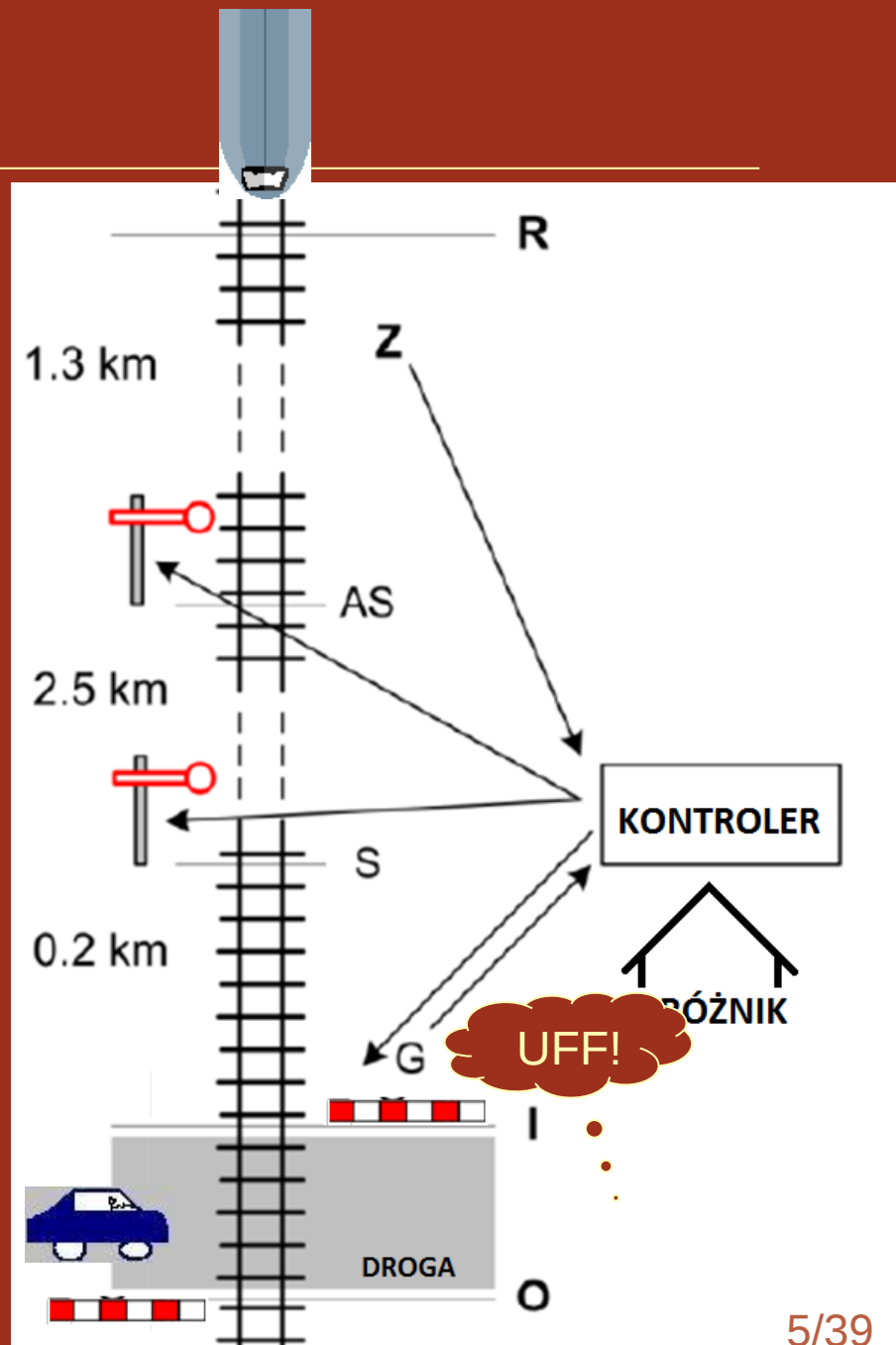
ANALIZA BEZPIECZEŃSTWA (ang. safety analysis)

- proces identyfikacji mechanizmów powstawania szkód oraz ocena poziomu ryzyka

Wprowadzenie

Główne założenia:

- tylko jeden pociąg w sekcji,
- „Kontroller” zamyka rogatki (tryb normalny lub tryb „ALARM”),
- jeśli kontroler nie zadziała, to rogatki zamyka Dróżnik,
- parametry konfiguracji T_m (odczyt), T_{ch_m} (test)



Wprowadzenie

Formalne metody analizy systemów związanych z bezpieczeństwem



Wprowadzenie

OBSZARY STOSOWALNOŚCI analizy DN

- elektroenergetyka,
- energetyka nuklearna,
- aeronautyka,
- inżynieria procesowa,
- transport,
- budownictwo,
- medycyna,
- inżynieria sanitarna.

① Identyfikacja niezdatności / zdarzeń
niebezpiecznych



② Budowa drzew niezdatności (dla każdej
zidentyfikowanej niezdatności w systemie)



③ Analiza drzew niezdatności



④ Analiza wyników + dodatkowe działania
(np. w celu minimalizacji prawdopodobieństwa
niezdatności, wprowadzenia zabezpieczeń)

NIEZDATNOŚĆ (źródło: PN-EN 60812)

(ang. fault)

- „stan obiektu charakteryzujący się niezdolnością do wypełniania wymaganych funkcji (...)”

ZDARZENIE WIERZCHOŁKOWE (źródło: PN-EN 61025)

(ang. top event)

- wynik „kombinacji” wszystkich zdarzeń wejściowych (inaczej: *final event*, *top outcom*)

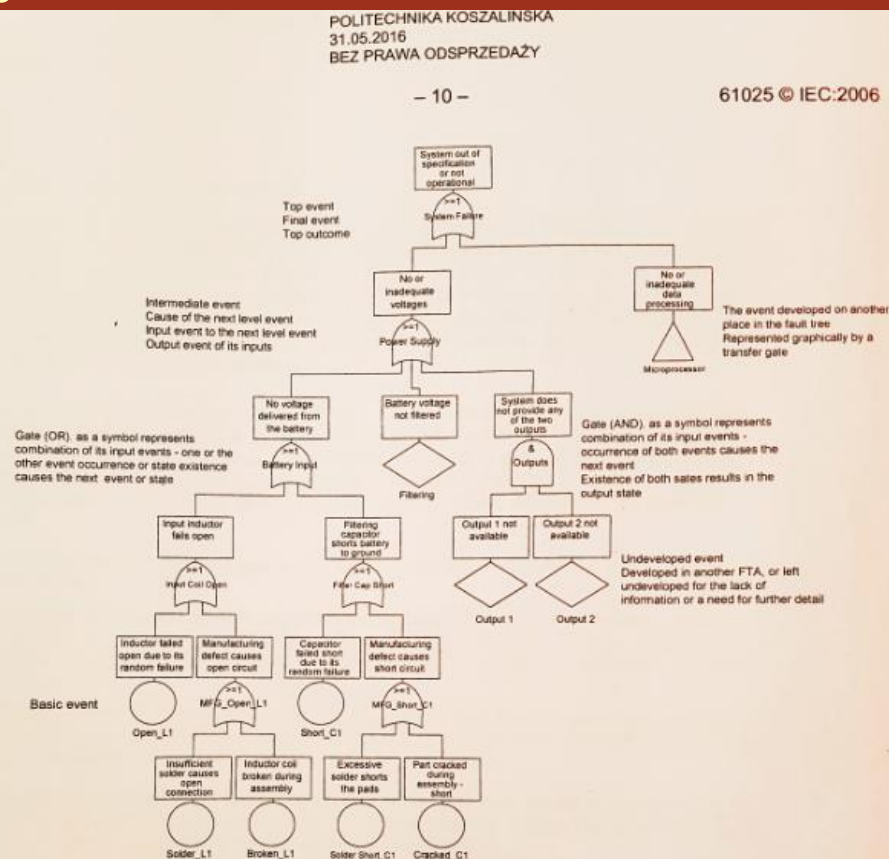
Budowa drzewa

- „top event”
 - umieszczenie niezdatności jako „top outcom/top event”,
 - ustalenie bezpośrednich zdarzeń prowadzących do zdarzenia wynikowego,
 - opisanie relacji między nimi i zdarzeniem wynikowym,
- wykonywanie podobnej analizy dla nowo zidentyfikowanych zdarzeń /dopóki jest to możliwe lub do określonego poziomu szczegółowości/



DRZEWO NIEZDATNOŚCI

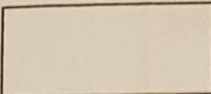
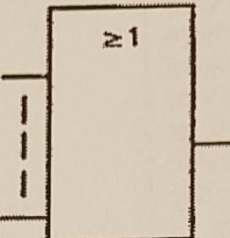
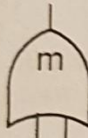
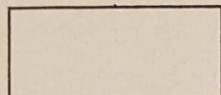
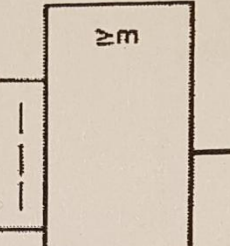
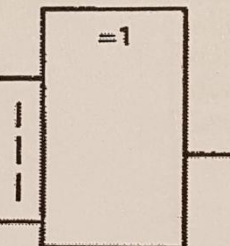
- graficzna reprezentacja kombinacji przypadków prowadzących do zdarzenia finalnego (top event)



(źródło: PN-EN 61025)

Figure 1 – Explanation of terms used in fault tree analyses

Podstawowe typy bram (źródło: PN-EN 61025)

	Symbols		Name	Description
	 		OR gate	The output event occurs if any of the input events occur
	 		MAJORITY VOTE GATE	The output occurs if m or more inputs out of a total of n inputs occur
			EXCLUSIVE OR gate	The output event occurs if one, but not the other inputs occur

Z1: Obecność pociągu na
niezabezpieczonym
przejeździe



AND

z2: Pociąg w sekcji IO

z3: Nie zamknięte
rogatki

Standardowa analiza stosowana jest typowo w celu znalezienia:

- **minimalnych zbiorów przyczyn** (ang. minimal cut sets) - minimalnych zbiorów zdarzeń prowadzących do zdarzenia finalnego,
- **prawdopodobieństwa wystąpienia niezdatności,**
- **średniego czasu do wystąpienia niezdatności lub pomiędzy wystąpieniami niezdatności.**

Przykłady istotnych parametrów czasowych wymagających innych metod lub rozszerzenia DN:

- czas opóźnienia pomiędzy przyczyną, a skutkiem (zależności w łańcuchu zdarzeń prowadzących do hazardu),
- czas wykrywania niezdatności,
- czas występowania niezdatności,
- czas tolerowania niezdatności,
- czas działania zabezpieczeń.

DNZC

Zdarzenia są reprezentowane:

- nazwę, np. x , y , z ,
- czas trwania $\langle \alpha^S, \beta^S \rangle$

α^S , β^S – minimalny i maksymalny czas trwania zdarzenia

$\langle 1, \infty \rangle$

z2: Pociąg w sekcji IO

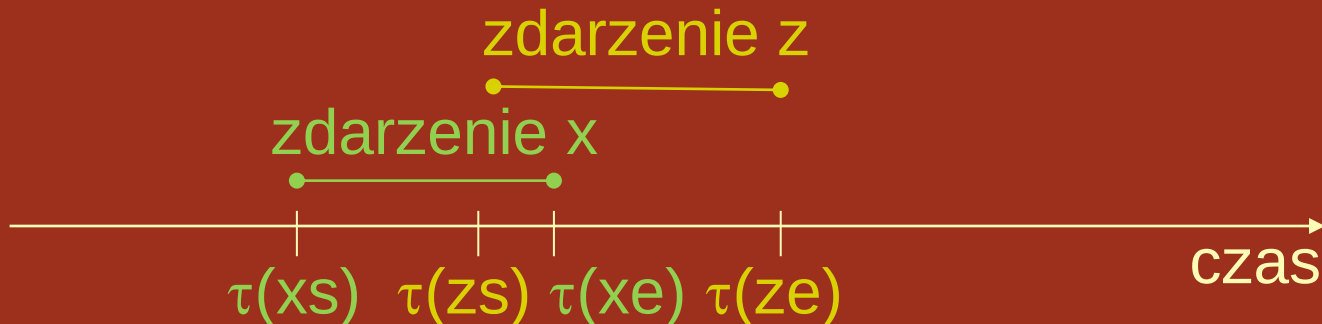
Wyjątki:

- zdarzenia wyjściowe bram uogólniających nie mają podanego czasu trwania.

DNZC

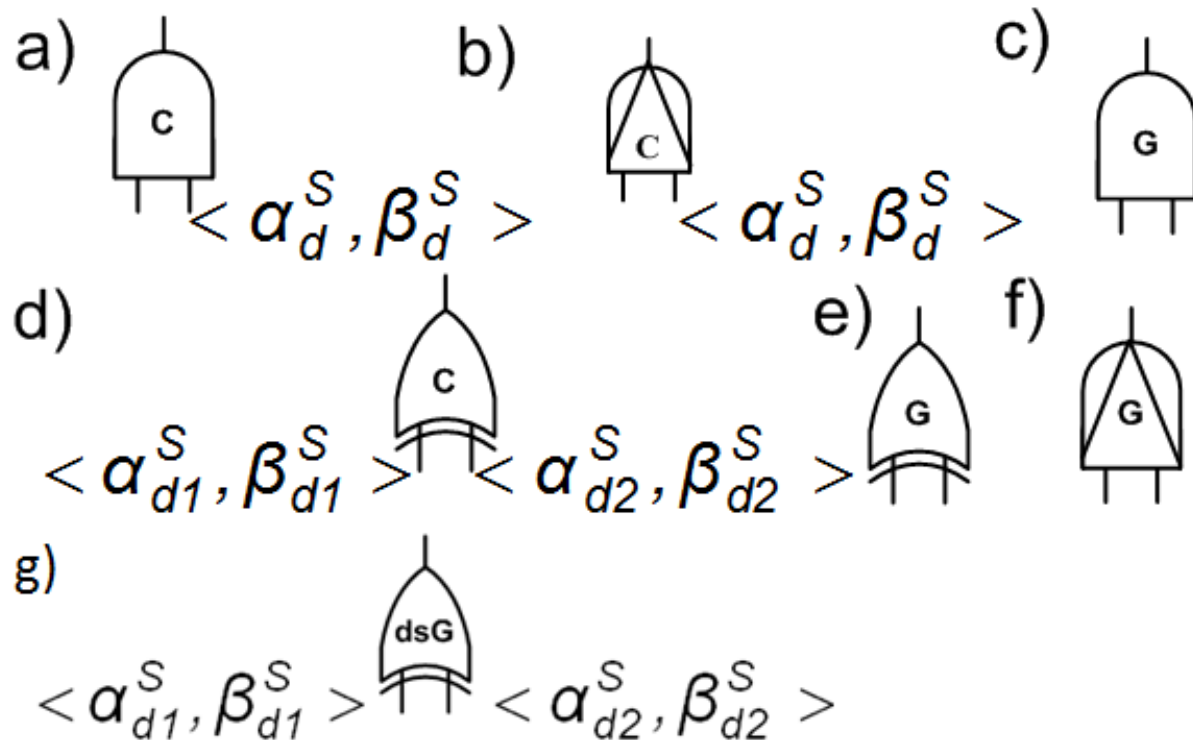
Wystąpienie zdarzenia charakteryzowane jest:

- nazwą,
- moment startu i moment zakończenia, odpowiednio:
 $\tau(xs)$, $\tau(xe)$, gdzie $\alpha^S \leq \tau(xe) - \tau(xs) \leq \beta^S$,



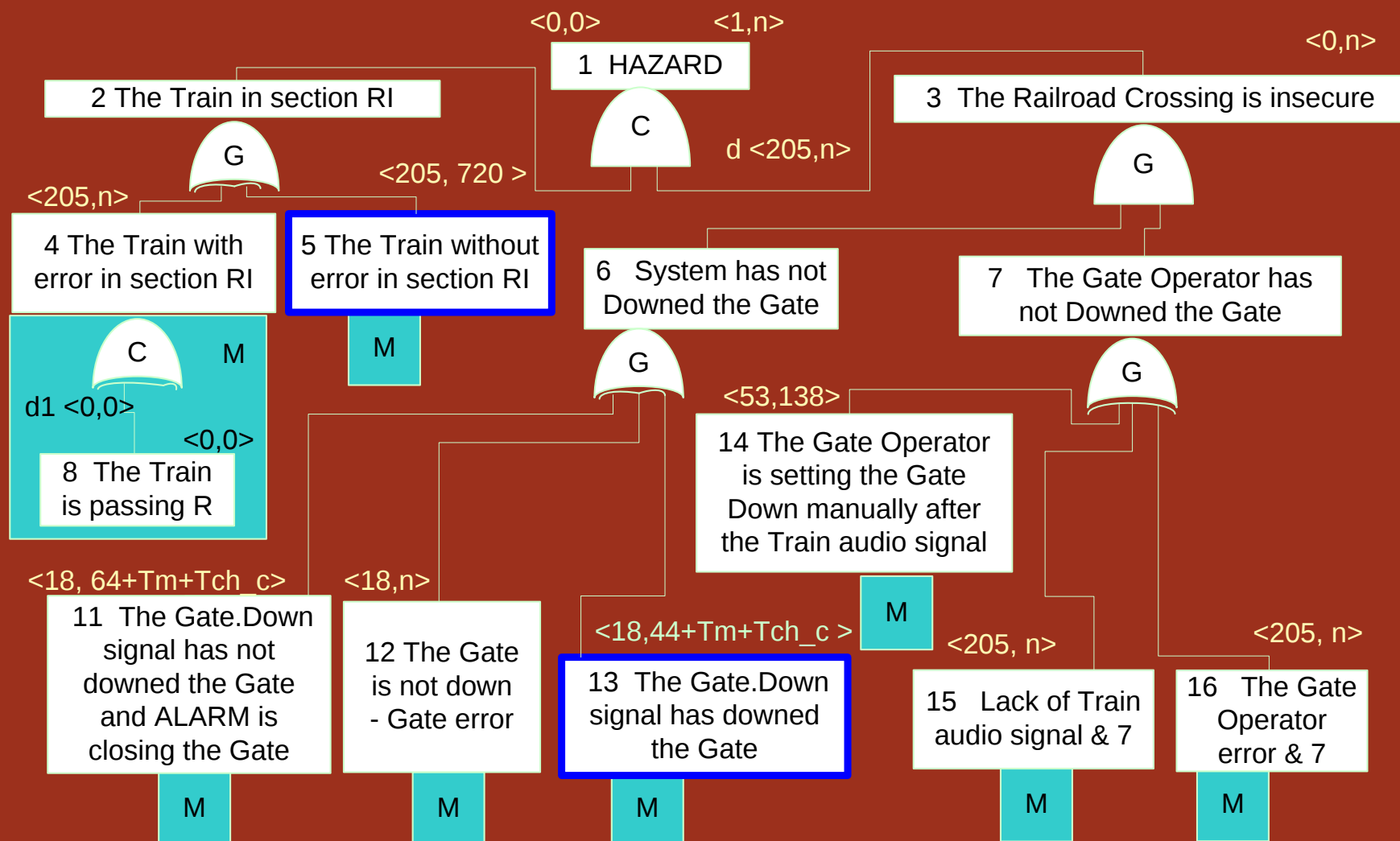
DNZC

NOTACJA BRAMEK



- a) przyczynowa AND; b) przyczynowa priorytetowa AND;
c) uogólniająca AND; d) przyczynowa XOR;
e) uogólniająca XOR; f) uogólniająca priorytetowa AND;
g) uogólniająca z opóźnieniem

DNZC



System = Controller and G, Z sensors
Assumption: S, AS, System correctly working

- the events
 - the events for correctly working system

(źródło: [4])

Analiza „od skutku do przyczyn”

Znajdź przedziały czasu dla startu i końca zdarzenia „top event”:

$$\langle \alpha_{te_start}, \beta_{te_start} \rangle, \langle \alpha_{te_end}, \beta_{te_end} \rangle$$

względem umownego momentu 0 (start top event)



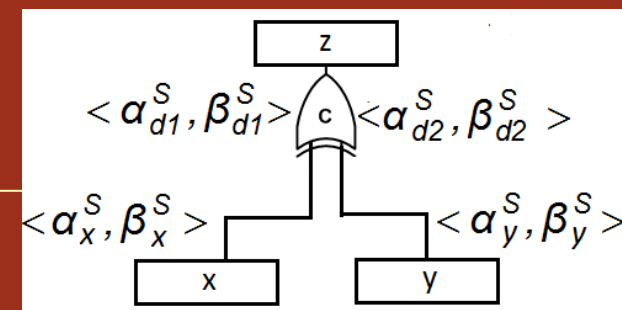
Znajdź przedziały czasu dla startu i końca zdarzeń:

$$\langle \alpha_{event_i_start}, \beta_{event_i_start} \rangle, \langle \alpha_{event_i_end}, \beta_{event_i_end} \rangle$$

dla pozostałych zdarzeń

DNZC

PRZYCZYNOWA XOR



jeśli z wystąpiło to:

x wystąpiło

y wystąpiło

(y nie wystąpiło)

(x nie wystąpiło)

CAUSAL XOR

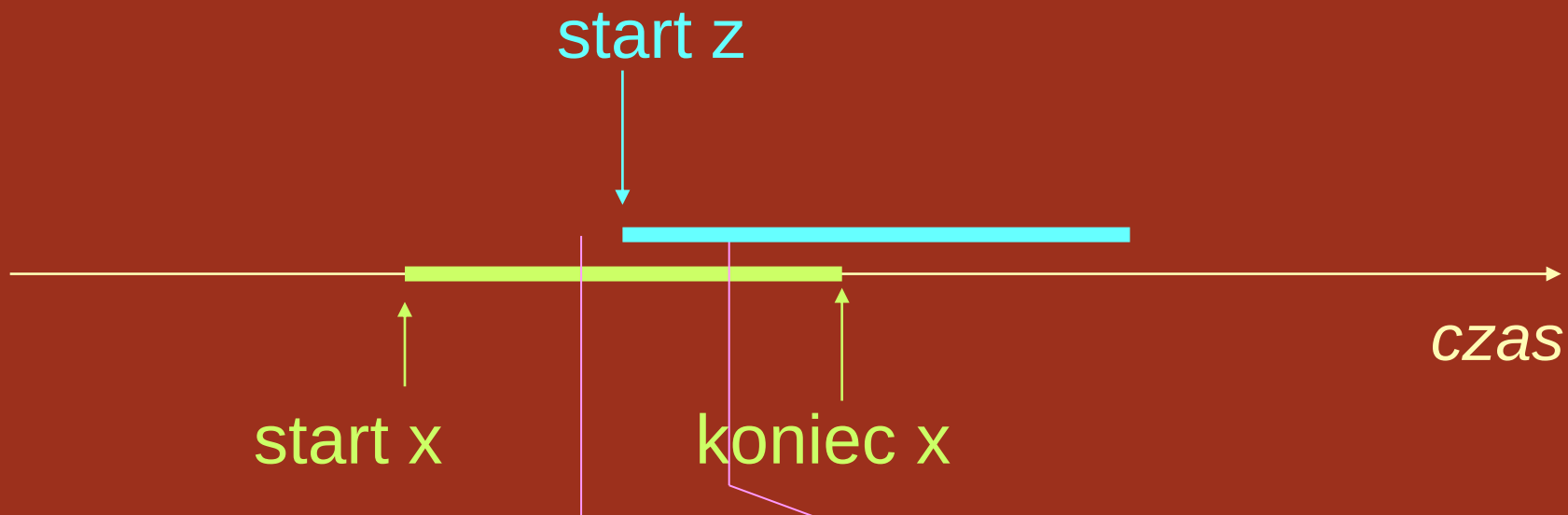
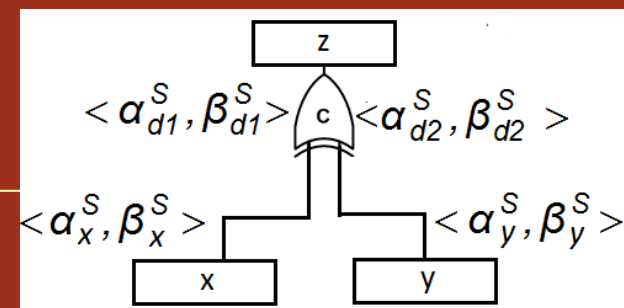
$\text{occur}(z) \Rightarrow (\exists x \bullet (\text{duration}(x) \geq \alpha_{d1}^S \wedge \tau(xs) + \alpha_{d1}^S \leq \tau(zs) \leq \tau(xs) + \beta_{d1}^S))$

$\oplus (\exists y \bullet (\text{duration}(y) \geq \alpha_{d2}^S \wedge \tau(ys) + \alpha_{d2}^S \leq \tau(zs) \leq \tau(ys) + \beta_{d2}^S))$

Kierunek analizy: od efektu do przyczyny

DNZC

PRZYCZYNOWA XOR przykład 1/3

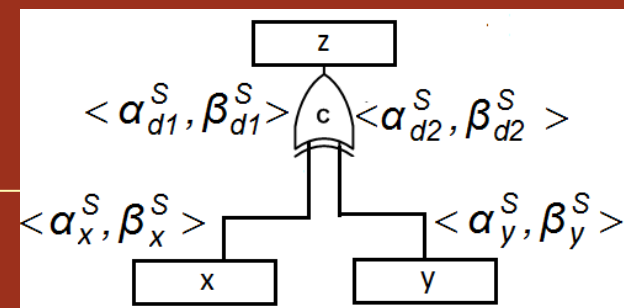


minimal opóźnienie pomiędzy
startem x i startem z
(licząc od startu x)

maksymalne
opóźnienie

DNZC

PRZYCZYNOWA XOR przykład 2/3



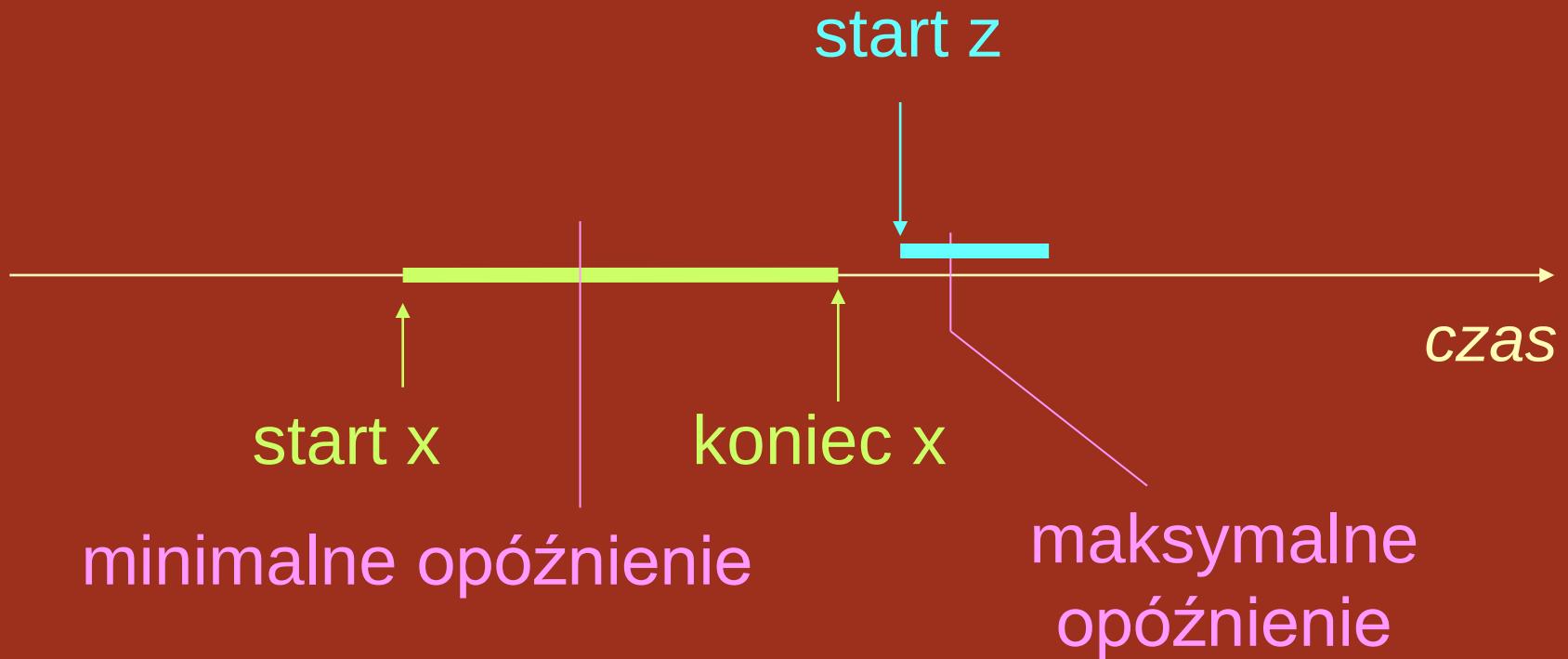
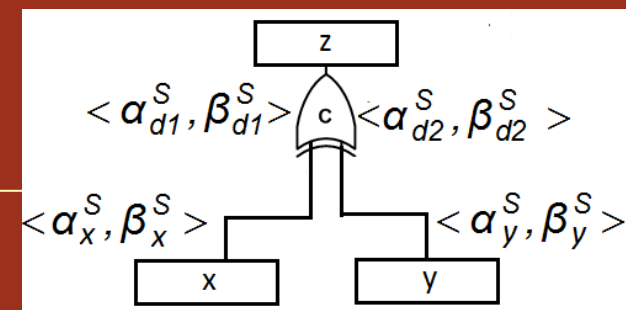
~~start z~~

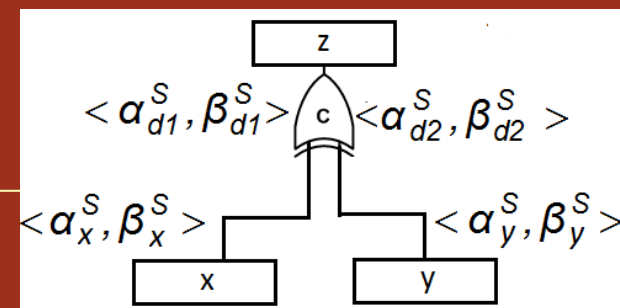
zbyt krótki
czas trwania x



DNZC

PRZYCZYNOWA XOR przykład 3/3





BRAMA PRZYCZYNOWA XOR

- WYZNACZANIE PRZEDZIAŁÓW CZASU DLA PRZYCZYN

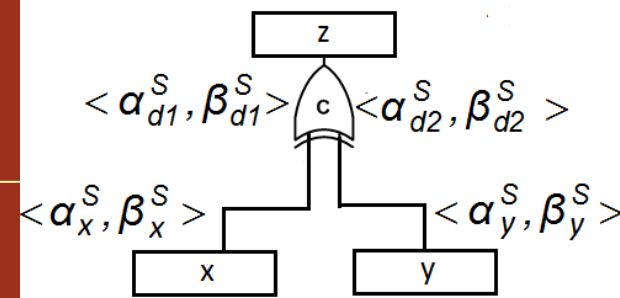
Założenie: dane są $\alpha_{zs} \beta_{zs} \alpha_{ze} \beta_{ze}$

$\alpha_{zs} (\beta_{zs})$ – najwcześniejszy (najpóźniejszy) moment startu zdarzenia z ,

$\alpha_{ze} (\beta_{ze})$ – najwcześniejszy (najpóźniejszy) moment zakończenia zdarzenia z .

DNZC

PRZYCZYNOWA XOR



Kalkulacja dla zdarzenia x:

start x: $\langle \alpha_{xs}, \beta_{xs} \rangle$, koniec x : $\langle \alpha_{xe}, \beta_{xe} \rangle$

$$\begin{cases} \alpha_{d1}^S \leq \beta_{xe}^S \\ \alpha_{xs} = \alpha_{zs} - \min\{\beta_{d1}^S, \beta_{xe}^S\}, & \beta_{xs} = \beta_{zs} - \alpha_{d1}^S \\ \alpha_{xe} = \alpha_{zs}, \beta_{xe} = \beta_{xs} + \beta_{xe}^S \end{cases}$$

⊕ Kalkulacja dla zdarzenia y.

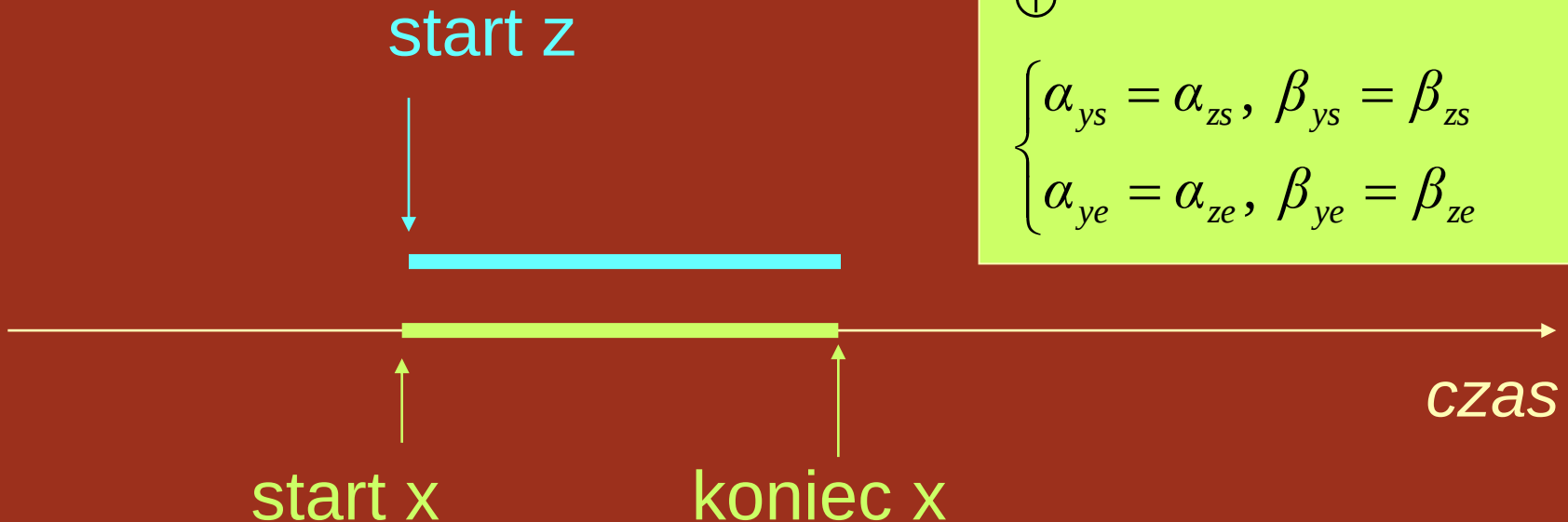
$$\begin{cases} \alpha_{d2}^S \leq \beta_{ye}^S \\ \alpha_{ys} = \alpha_{zs} - \min\{\beta_{d2}^S, \beta_{ye}^S\}, & \beta_{ys} = \beta_{zs} - \alpha_{d2}^S \\ \alpha_{ye} = \alpha_{zs}, \beta_{ye} = \beta_{ys} + \beta_{ye}^S \end{cases}$$

DNZC

GENERALIZATION XOR

$$\text{occur}(z) \Rightarrow (\text{occur}(x) \wedge x = z) \oplus (\text{occur}(y) \wedge y = z)$$

UOGÓLNIAJĄCA XOR przykład



$$\begin{cases} \alpha_{xs} = \alpha_{zs}, \beta_{xs} = \beta_{zs} \\ \alpha_{xe} = \alpha_{ze}, \beta_{xe} = \beta_{ze} \end{cases}$$

$\oplus$

$$\begin{cases} \alpha_{ys} = \alpha_{zs}, \beta_{ys} = \beta_{zs} \\ \alpha_{ye} = \alpha_{ze}, \beta_{ye} = \beta_{ze} \end{cases}$$

DNZC

1. Przykład minimalnych zbiorów przyczyn (MZP) z przedziałami czasu:

MZP 1

$\{E4 <-\infty, -205> <0, \infty>, \\ E12 <-\infty, -205> <0, \infty>, \\ E15 <-\infty, -205> <0, \infty>\}$

MZP 2

$\{E4 <-\infty, -205> <0, \infty>, \\ E12 <-\infty, -205> <0, \infty>, \\ E16 <-\infty, -205> <0, \infty>\}$

E4 - pociąg z awarią w sekcji RI

E12 - rogatek nie zamknięte – awaria rogatek

E15 - brak sygnału dźwiękowego z pociągu i dróżnik nie zamknął rogatek

E16 - dróżnik nie zamknął rogatek – błąd dróżnika

DNZC

Diagram przedziałów czasu dla MZP1:



E4 - pociąg z awarią w sekcji RI

E12 - Rogatki nie zamknięte – awaria rogatek

E15 - brak sygnału dżw. i dróżnik nie zamknął rogatek

Zdarzenia z MZP1 muszą współwystępować:
 $\{<-\infty, -205> <0, \infty>\}.$

Zatem, sytuacja niebezpieczna może wystąpić.

2. Jeśli Dróżnik zamyka Rogatki ręcznie
($205 \leq 138$) sytuacja niebezpieczna nie wystąpi.

DNZC

3. W przypadku poprawnej pracy systemu:

$$205 \leq 44 + T_m + T_{ch_h}$$

✓ sytuacja niebezpieczna nie wystąpi jeśli

$$T_{ch_c} + T_m < 161$$

4. Jeśli ALARM zamyka Rogatki otrzymamy:

$$205 \leq 64 + T_m + T_{ch_h}$$

✓ sytuacja niebezpieczna nie wystąpi jeśli

$$T_{ch_c} + T_m < 141$$

Zły dobór parametrów może prowadzić do sytuacji niebezpiecznej!

Podsumowanie

Oprogramowanie

Analizy DNZC (wersja prototypowa)

Wspomaganie wyznaczania parametrów czasowych DNZC (w planach, w oparciu o czasowe diagramy stanów).

Podsumowanie

Obszar zastosowań (1)

Uzupełnienie klasycznej analizy

analiza DN:

top event może wystąpić dla danego MZP,

analiza DNZC:

top event nie wystąpi dla danego MZP
przy określonych parametrach czasowych.

Podsumowanie

Obszar zastosowań (2)

Specyfikacja wymagań czasowych dla systemu i/lub zabezpieczeń (np. monitoring, detekcja, reakcja) w celu zapobieżenia wystąpienia niezdatności.

Podsumowanie

Potencjalne obszary badań:

- analiza skomplikowanych rzeczywistych przykładów (empiryczna walidacja),
- rozbudowa (opracowanie) oprogramowania pozwalającego na analizę klasyczną i czasową,
- integracja z innymi metodami formalnymi.

Przegląd bibliograficzny DNZC

Opis metody Drzewa niezdatności z zależnościami Metoda czasowymi (DNZC) analizy

[1]		J. Górski, J. Magott, A. Wardziński, <i>Modelling Fault Trees Using Petri Nets</i> , in: Proc. SAFECOMP'95, Belgirate, Italy, LNCS, Springer-Verlag, 1995
[2]	 	J. Magott, P. Skrobanek, <i>A Method of Analysis of Fault Tree with Time Dependencies</i> , Proc. SAFECOMP 2000, Rotterdam, The Netherlands, LNCS, Vol. 1943, Springer-Verlag, 2000, pp. 176-186.
[3]	 	J. Magott, P. Skrobanek, <i>Method of time Petri net analysis for analysis of fault trees with time dependencies</i> , IEE Proc.-Comput. Digit. Tech., Vol.149, No.6, November, 2002

Przegląd bibliograficzny DNZC

Opis metody

DNZC

Metoda analizy

[4]	J.Magott, P. Skrobanek, <i>The safety analysis using the fault trees with time dependencies</i> , W: Tagungsband zur Informationstagung Mikroelektronik 06, [Wien, 12 October 2006] / Hrsg. W. Pribyl, E. Schoitsch. Wien : Osterreichischer Verband fur Elektrotechnik, cop. 2006. s. 176-182.
[5]	P.Skrobanek, <i>A method of analysis of fault tree with time dependencies for safety-related systems</i> (in Polish), Technical University of Wroclaw, Poland, report: PRE. 24/2005
[6]	J. Magott, P. Skrobanek, <i>Partially automatic generation of fault-trees with time dependencies</i> , in: Proc. Dependability of Computer Systems", DepCoS '06, Szklarska Poręba, Poland, IEEE Computer Society Press, 2006, 8 pages

Przegląd bibliograficzny DNZC

Opis metody

DNZC

Metoda
analizy

[7]	<i>M. Jureczko M., P. Skrobanek, Tool for analysis of the fault tree with time dependencies, Przegląd Elektrotechniczny. 2010, R. 86, nr 9, s. 179-183</i>
[8]	<i>J. Magott, P. Skrobanek, Timing analysis of safety properties using fault trees with time dependencies and timed state-charts, Reliability Engineering & Systems Safety. 2012, vol. 97, nr 1, s. 14-26</i>

POLITECHNIKA KOSZALIŃSKA
ZAKŁAD SYSTEMÓW MULTIMEDIALNYCH I SZTUCZNEJ
INTELIGENCJI

Analiza drzew niezdatności z zależnościami czasowymi

Dziękuję za uwagę...

dr inż. Paweł Skrobanek
(pawel.skrobanek@tu.koszalin.pl)

Koszalin 2018