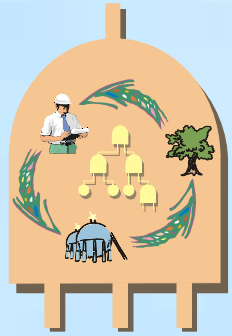
Politechnika Gdańska

Wydział Elektrotechniki i Automatyki

Katedra Automatyki



Kazimierz Kosmowski

k.kosmowski@ely.pg.gda.pl

Opracowanie metod analizy i narzędzi do komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym w ramach systemu warstw zabezpieczeniowo-ochronnych obiektów przemysłowych podwyższonego ryzyka

Seminarium PPT BPP

Priorytety i formy badań naukowych i prac rozwojowych w ramach Polskiej Platformy Technologicznej Bezpieczeństwo Pracy w Przemyśle

CIOP PIB, Warszawa, 17 maja 2007

Zakres prezentacji

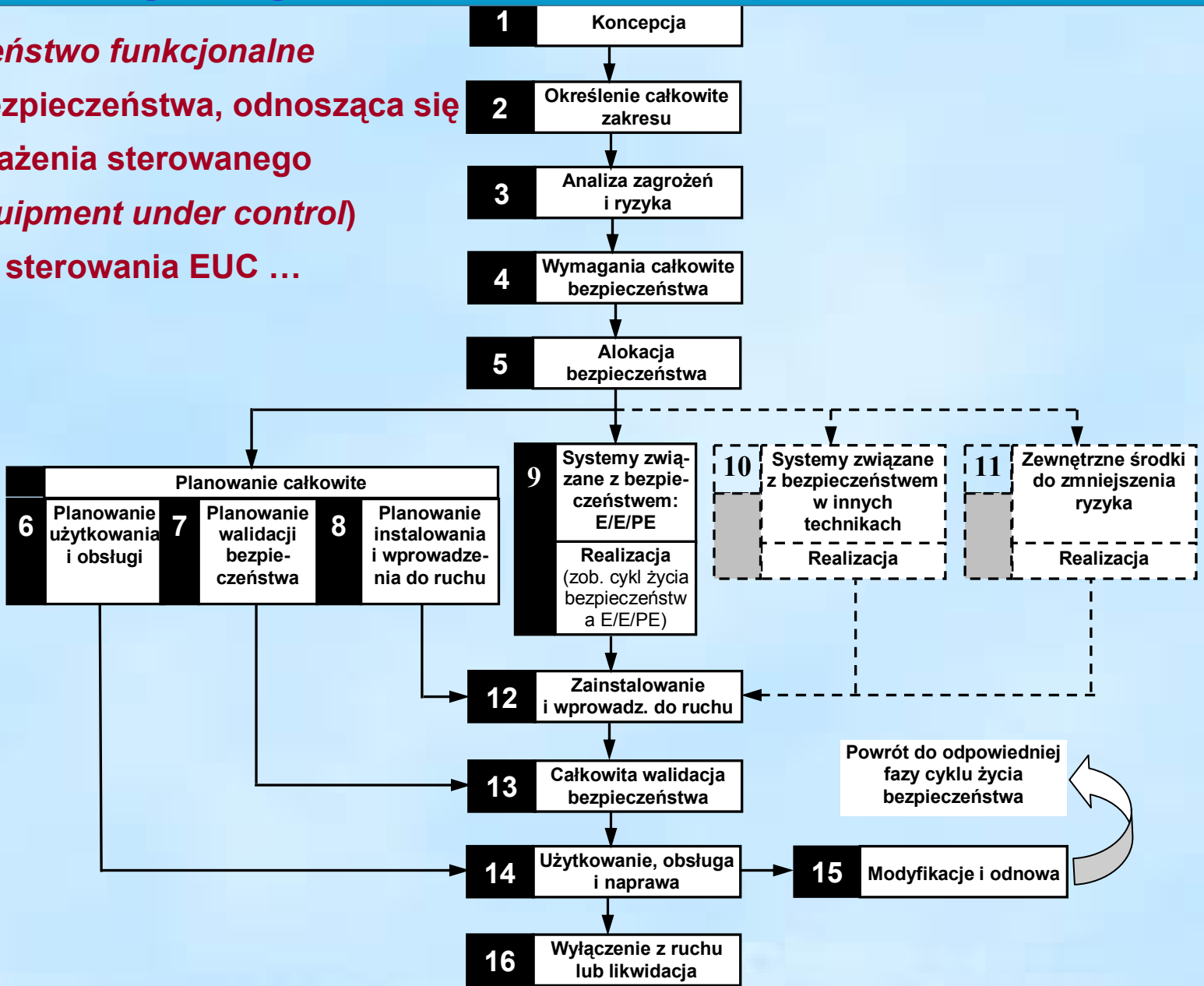
- Koncepcja bezpieczeństwa funkcjonalnego (IEC 61508)
- Określanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL (safety integrity level) na podstawie analizy ryzyka
- Weryfikacja poziomu nienaruszalności bezpieczeństwa systemów E/E/PE i SIS
- Metoda LOPA (Layer of Protection Analysis) w praktyce w nawiązaniu do IEC 61511
- Kategorie częstości, skutków zdarzeń awaryjnych i ryzyka oraz określanie SIL
- Projekt w programie wieloletnim koordynacja CIOP PIB

Bezpieczeństwo funkcjonalne (IEC 61508)

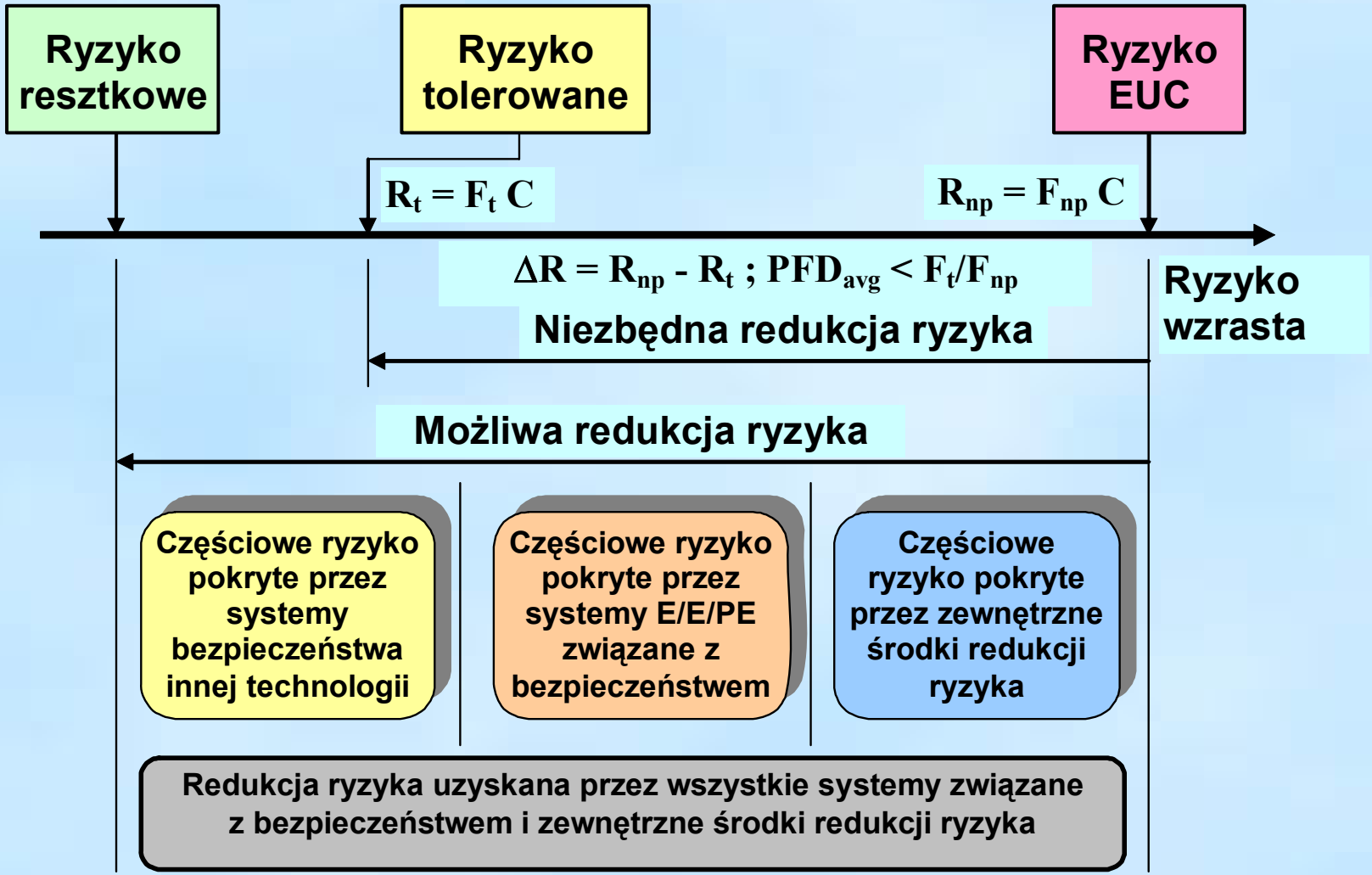
Cykl życia / trwania bezpieczeństwa

Bezpieczeństwo funkcjonalne

- część bezpieczeństwa, odnosząca się do wyposażenia sterowanego (*EUC - equipment under control*) i systemu sterowania EUC …



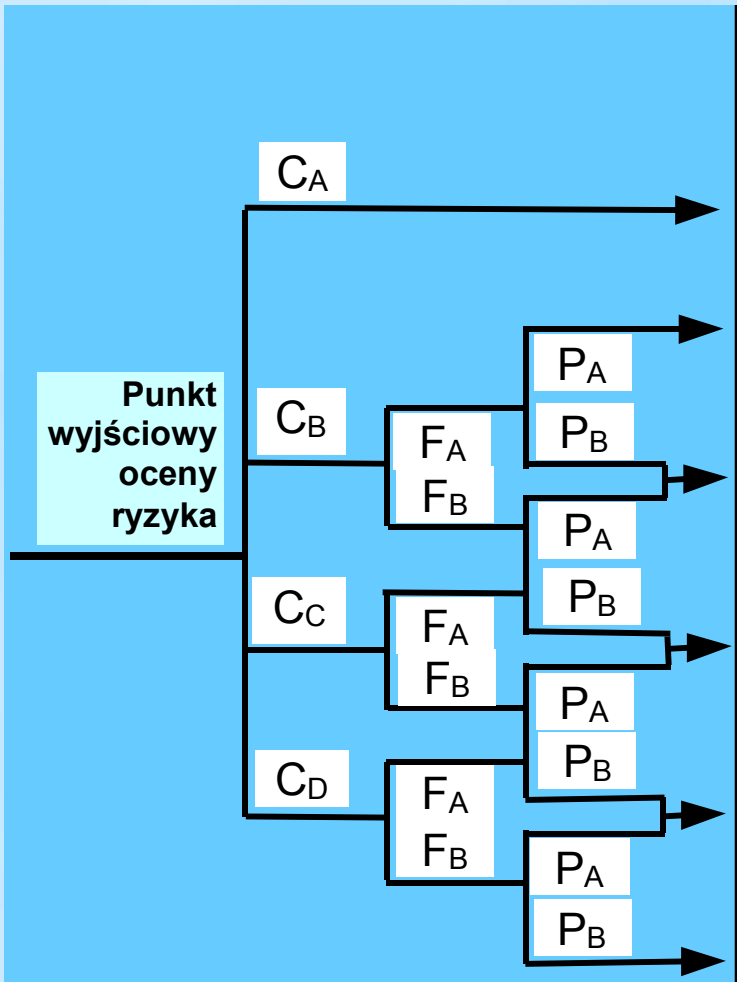
Redukowanie ryzyka za pomocą E/E/PE lub SIS



Kryteria probabilistyczne dla systemów E/E/PE i SIS pełniących funkcje bezpieczeństwa

SIL (poziom nienaruszal-ności bezpie-czeństwa)	Prawdopodobieństwo niewypełnienia funkcji na przywołanie - rodzaj pracy rzadkiego przywołanie (LDM)	Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę - rodzaj pracy częstego przywołania lub ciągły (HDM)
4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
1	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

Graf ryzyka do określania SIL według IEC 61508



W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

C - skutki - parametr ryzyka
F - częstość i czas ekspozycji
P - możliwość uniknięcia zagrożenia
W - prawdopodobieństwo zdarzenia

--- Bez wymagań bezpieczeństwa
a - Bez specjalnych wymagań
b - Pojedynczy E/E/PE nie wystarcza
1, 2, 3, 4 - SIL

Wyznaczanie PFD systemu w weryfikowaniu SIL

$$PED_{avg}^{SYS} \cong PFD_{avg}^{A} + PFD_{avg}^{B} + PFD_{avg}^{C}$$

A. Podsystem wejściowy (czujniki i przetworniki).
B. Podsystem przetwarzania informacji (sterowniki programowalne).
C. Podsystem wyjściowy (człony wykonawcze i elementy końcowe).

Przykładowa struktura szeregowa:

$PFD_{avg}^{A} = 2.2 \cdot 10^{-2}$ — SIL1

$PFD_{avg}^{B} = 1.5 \cdot 10^{-3}$ — SIL2

$PFD_{avg}^{C} = 1.4 \cdot 10^{-2}$ — SIL1

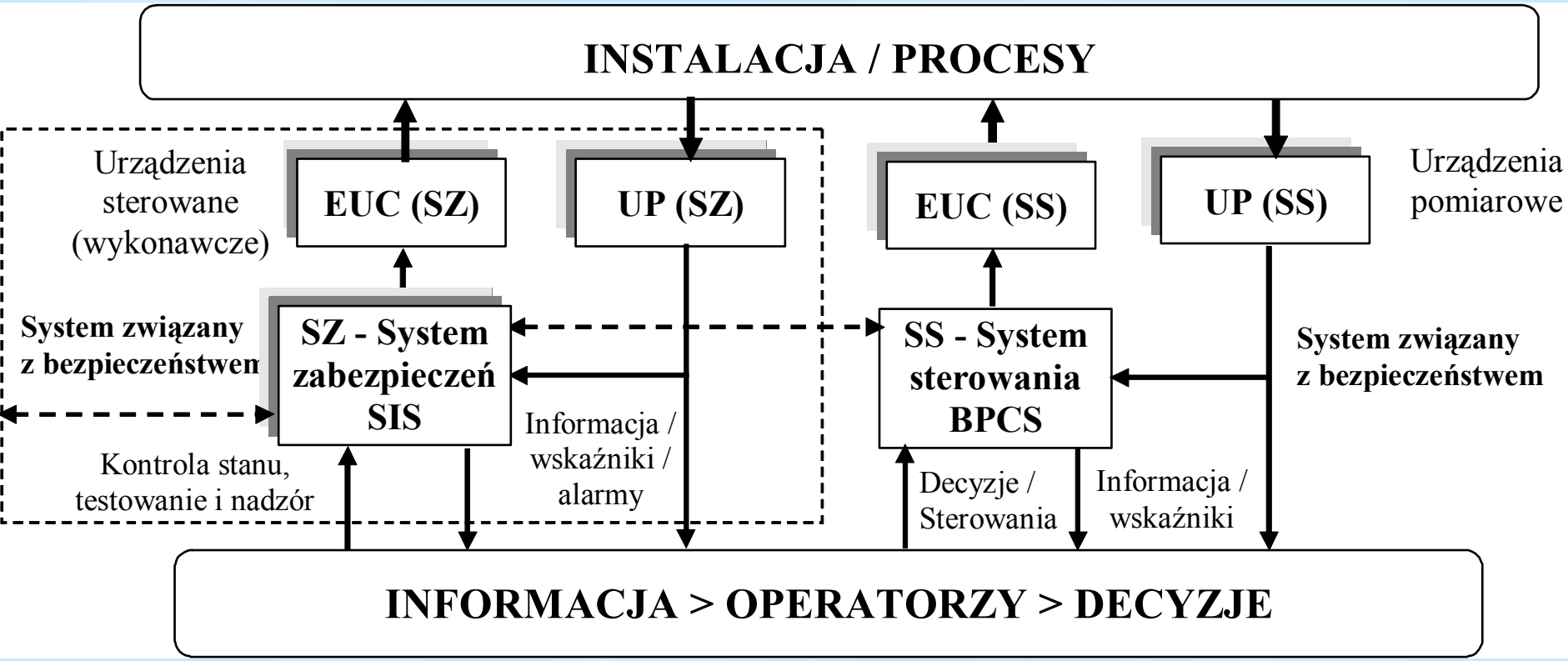
$$PFD_{avg}^{S} \cong 3.75 \cdot 10^{-2}$$

SIL1

Warstwy zabezpieczeń w obiekcie podwyższonego ryzyka (IEC 61511)

Filozofia „obrony w głąb” – warstwy powinny spełniać warunek niezależności funkcjonalnej i strukturalnej

Systemy E/E/PE – sterowania i automatyki zabezpieczeniowej



System sterowania i system automatyki zabezpieczeniowej

- wymaganie niezależności funkcjonalnej

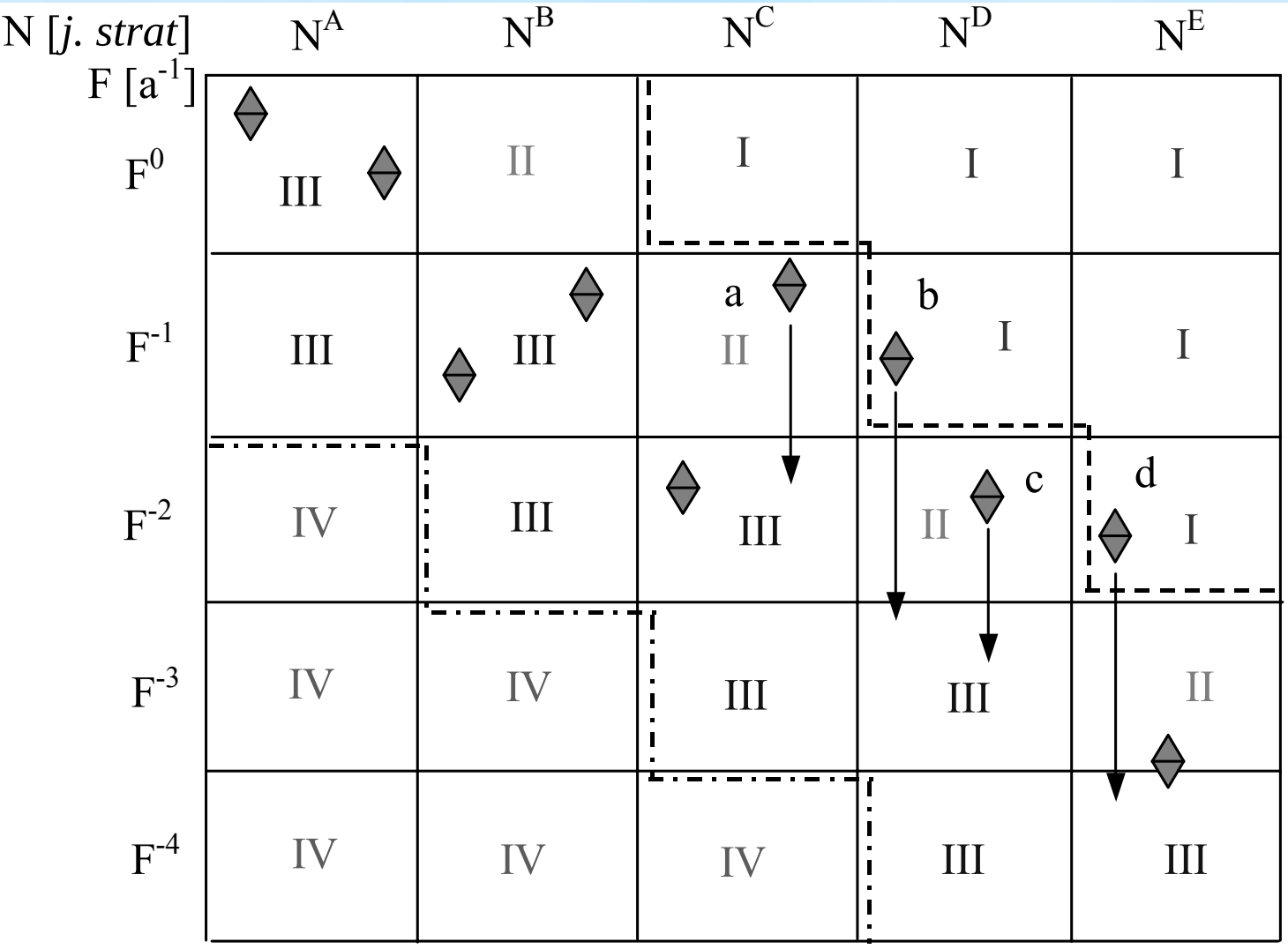
Analiza warstw zabezpieczeń LOPA (*Layer of Protection Analysis*)

Trzy przykładowe warstwy PL (mają zapobiec wstąpieniu zdarzeń awaryjnych o poważnych konsekwencjach):

- **PL1 – System sterowania BPCS (*Basic Proces Control System*)**
- **PL2 – Człowiek-operator (nadzoruje proces i interweniuje w razie wystąpienia sytuacji nienormalnej lub awaryjnej,**
- **PL3 – System zabezpieczeń SIS (*Safety Instrumented System*).**

$$F_i^{PLs} = F_i^{I} \cdot PFD_i^{PL1} PFD_i^{PL2} PFD_i^{PL3} = d \cdot F_i^{IPLs}$$

Wyniki analizy scenariuszy awaryjnych - przykładowa matryca ryzyka



Kategorie ryzyka:

I – niedopuszczalne

II - niepożądane

III - tolerowane

IV - akceptowane

Przykładowe kategorie częstości i skutków zdarzeń do definiowania matrycy ryzyka

Kategorie częstości zdarzenia	F^{-4}	F^{-3}	F^{-2}	F^{-1}	F^{0}
Określenie słowne kategorii częstości	Rzadkie	Mało prawdopo-dobne	Sporadyczne	Prawdopo-dobne	Częste
Przedziały wartości [a^{-1}]	$(10^{-5}, 10^{-4}]$	$(10^{-4}, 10^{-3}]$	$(10^{-3}, 10^{-2}]$	$(10^{-2}, 10^{-1}]$	$(10^{-1}, 10^{0}]$
Kategorie skutku zdarzenia	N^{A}	N^{B}	N^{C}	N^{D}	N^{E}
Określenie słowne kategorii skutku	Marginalne	Małe	Duże	Krytyczne	Katastro-ficzne
Orientacyjna liczba poszko-dowanych	Pojedyn-cze obrażenia	Liczne obrażenia	Pojedyncze zejścia	Kilka zejść	Więcej niż kilka zejść

PPT BPP – projekt w programie wieloletnim – koordynacja CIOP PIB

Opracowanie metod analizy i narzędzi do komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym w ramach systemu warstw zabezpieczeniowo-ochronnych obiektów przemysłowych podwyższonego ryzyka

Zadania projektu obejmują:

1. Opracowanie metodyki analizy bezpieczeństwa funkcjonalnego w projektowaniu i użytkowania systemów SIS (safety instrumented systems) zgodnie wymaganiami z EN 61508 i EN 61511;
2. Opracowanie metody kalibrowanego grafu ryzyka do określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL (safety integrity level) dla zdefiniowanych funkcji bezpieczeństwa;
3. Opracowanie metod weryfikacji SIL systemów SIS i BPCS (basic process control system);
4. Opracowanie metody analizy warstw zabezpieczeń LOPA (layer of protection analysis) uwzględniającej analizę niezawodności człowieka i uszkodzeń zależnych;

PPT BPP – projekt w programie wieloletnim – koordynacja CIOP PIB (c.d.)

Opracowanie metod analizy i narzędzi do komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym w ramach systemu warstw zabezpieczeniowo-ochronnych obiektów przemysłowych podwyższonego ryzyka

5. Opracowanie koncepcji funkcjonalnej i strukturalnej oprogramowania komputerowego wspomagającego zarządzanie bezpieczeństwem funkcjonalnym w cyklu życia systemu;
6. Projekt i oprogramowanie modułu wspomagającego wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL;
7. Projekt i oprogramowanie modułu wspomagającego weryfikację SIL systemów SIS;
8. Projekt i oprogramowanie modułów graficznych oraz baza danych niezawodnościowych do wspomaganej komputerowo analizy bezpieczeństwa funkcjonalnego;
9. Testowanie prototypowego oprogramowania dla przykładowych rozwiązań BPCS i SIS.