# DCS
# Rozproszone Systemy Automatyki
# Wykład 11

Adam Ratajczak

Pracownia Automatyki, Modelowania i Mechatroniki
Katedra Automatyki, Mechatroniki i Systemów Sterowania
Wydział Elektroniki
Politechnika Wrocławska



[1] Niniejszy dokument zawiera materiały do wykładu z przedmiotu Rozproszone Systemy Automatyki. Jest on udostępniony pod warunkiem wykorzystania wyłącznie do własnych, prywatnych potrzeb i może być kopiowany wyłącznie w całości, razem ze stroną tytułową.

# Definicje

## Ryzyko

Kombinacja prawdopodobieństwa wystąpienia szkody/wypadku oraz stopnia nasilenia tej szkody.

## Wypadek

Wypadkiem jest nieoczekiwane zdarzenie przytrafiające się nieprzygotowanym.

# Definicje

## Bezpieczeństwo

Stan, w którym ryzyko ograniczono do akceptowalnego poziomu.

## Bezpieczeństwo funkcjonalne

Część bezpieczeństwa całkowitego odnosząca się do procesu i BPCS, która zależy od prawidłowego działania SIS i innych warstw zabezpieczeń.
Zdolność systemu do podejmowania niezbędnych działań w celu osiągnięcia i utrzymania zdefiniowanego uprzednio stanu bezpiecznego.

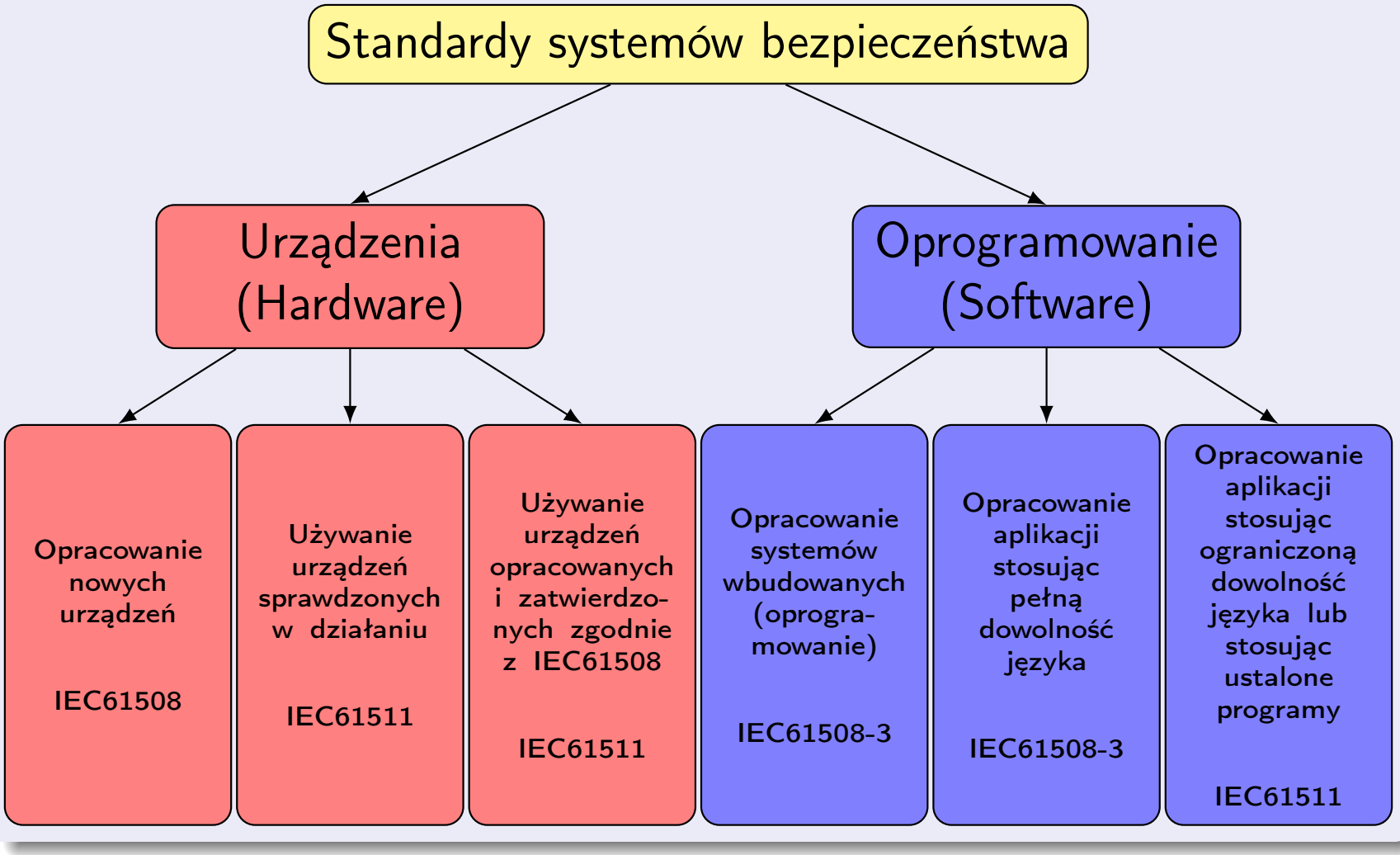
# Wstęp

## Normy

| | |
|---|---|
| IEC 61508 | Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ elektronicznych programowalnych systemów związanych z bezpieczeństwem |
| IEC 61511 | Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa dla sektora inżynierii przemysłowej |

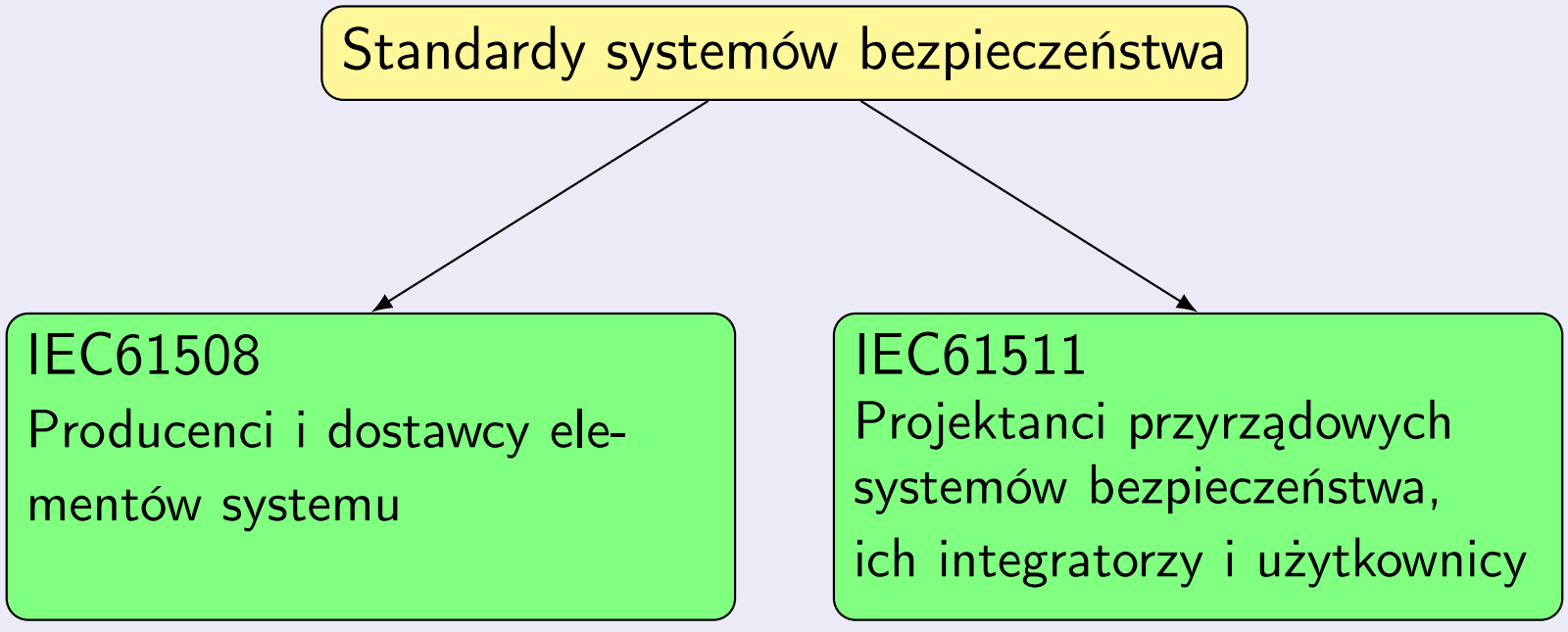
# Wstęp

## Normy


Standardy systemów bezpieczeństwa
Urządzenia (Hardware)
Oprogramowanie (Software)
Opracowanie nowych urządzeń
IEC61508
Używanie urządzeń sprawdzonych w działaniu
IEC61511
Używanie urządzeń opracowanych i zatwierdzonych zgodnie z IEC61508
IEC61511
Opracowanie systemów wbudowanych (oprogramowanie)
IEC61508-3
Opracowanie aplikacji stosując pełną dowolność języka
IEC61508-3
Opracowanie aplikacji stosując ograniczoną dowolność języka lub stosując ustalone programy
IEC61511

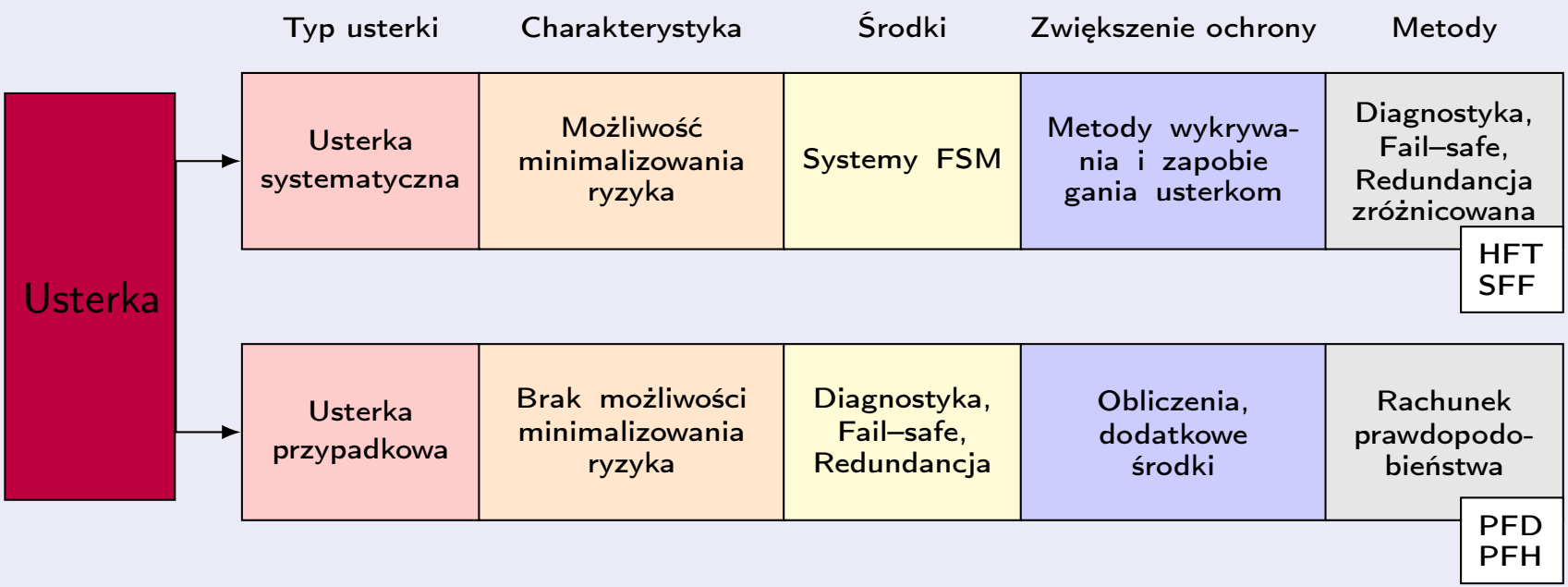
# Wstęp

## Normy


Standardy systemów bezpieczeństwa
IEC61508
Producenci i dostawcy elementów systemu
IEC61511
Projektanci przyrządowych systemów bezpieczeństwa, ich integratorzy i użytkownicy
Rozwój nowych elementów systemu
Systemy sprawdzone w działaniu

# Wstęp

## Anatomia usterki




HFT Hardware Fault Tolerance

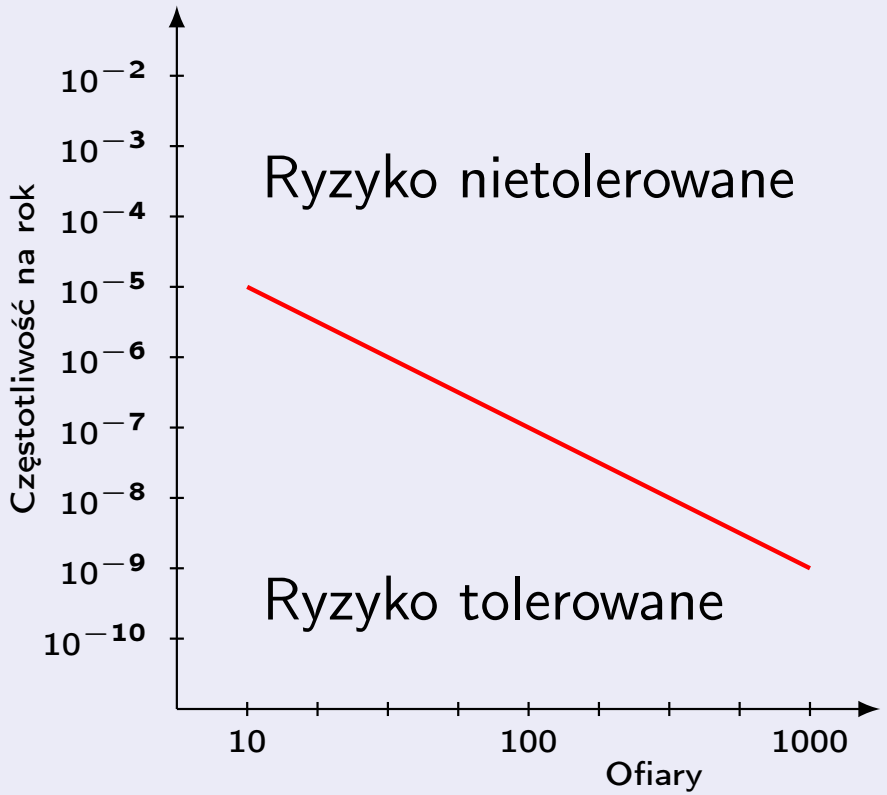
SFF Safe Failure Fraction

PFD Probability of Failure on Demand

PFH Probability of Failureper Hour

# Ryzyko tolerowane

## Przykład




Dopuszczalny poziom tolerancji ryzyka zależy od

- Kraju/regionu
- Względów społecznych
- Uwarunkowań prawnych
- Skutków/konsekwencji

# Metody oceny zagrożeń i ryzyka

## Środki oceny zagrożeń i ryzyka

- Burza mózgów nad strukturą i kluczowymi elementami obiektu
- Opinie i wypowiedzi ekspertów
- Wywiady i kwestionariusze
- Listy kontrolne
- Dostępne dane z podobnych aplikacji
- Doświadczenie personelu
- Doświadczenia i modelowanie

# Metody oceny zagrożeń i ryzyka

## Metody oceny zagrożeń

| | |
|---|---|
| HAZOP | **HAZ**ard and **OP**erability study |
| FME(C)A | **F**ailure **M**ode and **E**ffect (and **C**riticality) **A**nalysis |
| ETA | **E**vent **T**ree **A**nalysis |
| FTA | **F**ault **T**ree **A**nalysis |

# Metody oceny zagrożeń

## HAZOP

Identyfikacja korelacji w procesie i w zmiennych procesowych oraz kategoryzacja ich w odpowiednio zgranulowanej skali. Następnie określenie, jak te korelacje mogą wpłynąć na wywyłanie usterki. HAZOP bazuje na pewnych hasłach wiodących (guide words) takich jak

- no/not
- more/less
- both/as well as
- in part
- early/late
- before/after
- other than
- contrary to

Metoda określona normą IEC61882

# Metody oceny zagrożeń

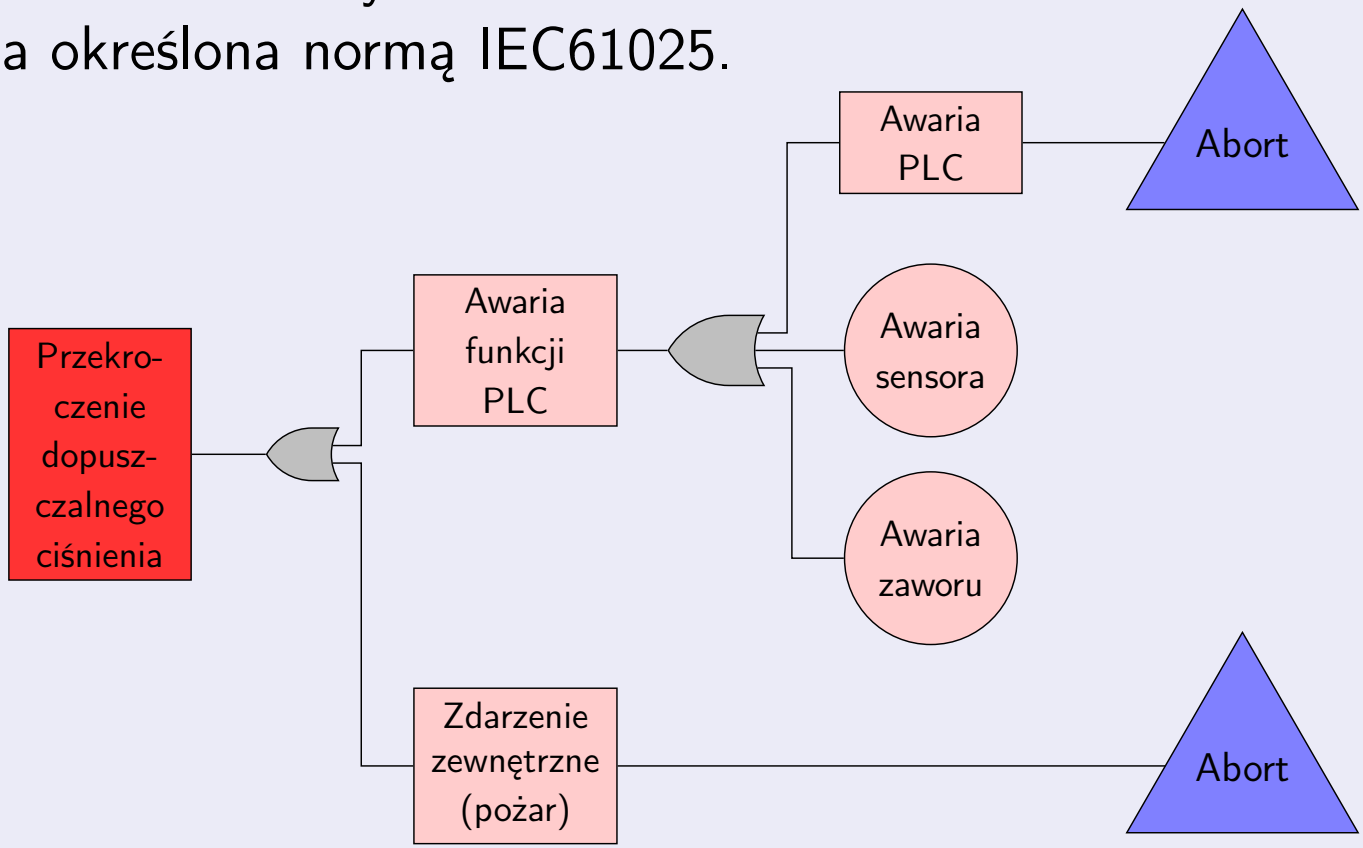
## FME(C)A

FMEA to systematyczne przeglądanie wszystkich części wszystkich urządzeń obiektowych pod względem uszkodzeń i ich konsekwencji. Następnie przydzielane jest prawdopodobieństwo ich wystąpienia.
FMECA uwzględnia również urządzenia E/E/PE.
Metoda określona normą IEC 60812.

# Metody oceny zagrożeń

## FTA

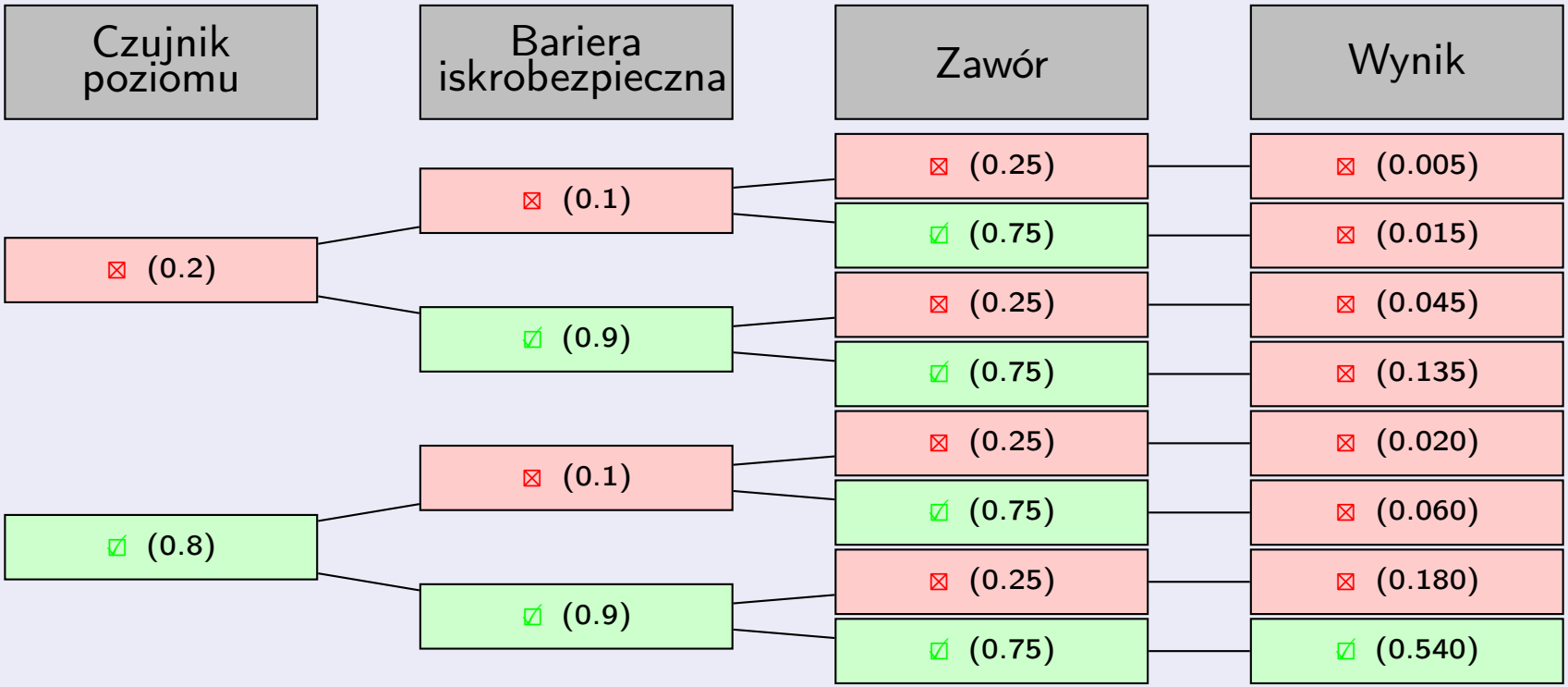
Diagram opisujący przyczyny wystąpienia konkretnej usterki.
Dodatkowym zadaniem jest określenie prawdopodobieństwa wystąpienia konkretnych zdarzeń.
Metoda określona normą IEC61025.



# Metody oceny zagrożeń

## ETA

Rozpoczynając od początkowego zdarzenia ETA przedstawia potencjalne zdarzenia podczas pracy. W wyniku otrzymuje się graf z konsekwencjami wynikającymi ze zdarzenia oraz prawdopodobieństwem ich wystąpienia. Metoda określona normą IEC62502.



# Metody oceny zagrożeń i ryzyka

## Metody oceny ryzyka

Norma IEC61508 definiuje cztery metody analizy ryzyka. Mające na celu określenie poziomu ryzyka oraz wymaganego stopnia jego redukcji

ALARP **A**s **L**ow **A**s **R**easonably **P**racticable
- Risk Graph
- Risk Matrix

LOPA **L**ayer **O**f **P**rotection **A**nalysis

# Metody analizy ryzyka

## ALARP

Pozwala określić czy bieżąca redukcja ryzyka jest wystarczająca czy potrzebne są dodatkowe środki w celu dalszej redukcji. Ponadto pozwala zestawić poziom redukcji z kwestiami ekonomicznymi. Ryzyko jest sklasyfikowane na cztery klasy: od I (nie do przyjęcia) do IV (ogólnie tolerowane). Ryzyko resztkowe jest segregowane ze względu na częstotliwość oraz skutki.

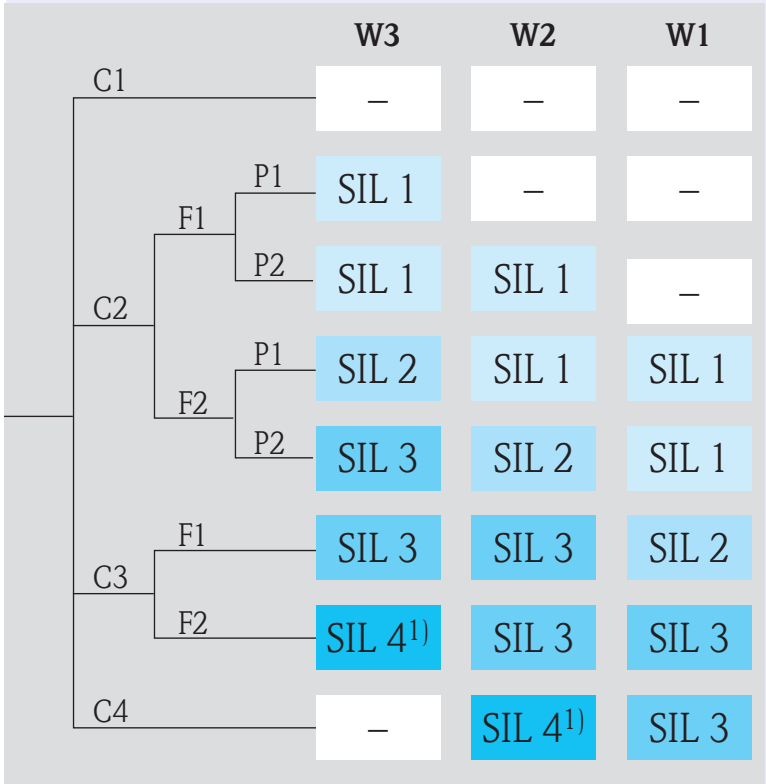
Przykład

| Częstotliwość | Konsekwencje | | | |
|---|---|---|---|---|
| | Katastrofalne | Krytyczne | Poboczne | Pomijalne |
| Częste | I | I | I | II |
| Prawdopodobne | I | I | II | III |
| Okazjonalne | I | II | III | III |
| Mało prawdopodobne | II | III | III | IV |
| Nieprawdopodobne | III | III | IV | IV |
| Prawie niemożliwe | IV | IV | IV | IV |

# Metody analizy ryzyka

## Risk Graph

Graf ryzyka określa współczynniki ryzyka w odniesieniu do obiektu bez SIS. Bierze pod uwagę konsekwencje (C), częstotliwość (F), p–stwo uniknięcia (P) oraz p–stwo wystąpienia zdarzenia (W).




Konsekwencje awarii
**C1** niewielkie obrażenia ludzi
**C2** poważne obrażenia jednej lub kilku osób; możliwy zgon jednej osoby
**C3** zgony kilku osób
**C4** duża liczba ofiar śmiertelnych
Narażanie na skutki awarii
**F1** rzadkie lub okresowe
**F2** częste lub ciągłe
Ograniczanie ryzyka awarii
**P1** możliwe pod określonymi warunkami
**P2** prawie niemożliwe
Prawdopodobieństwo zajśca zdarzenia
**W1** bardzo małe
**W2** niewielkie
**W3** względnie duże

# Metody analizy ryzyka

## Risk Matrix

Macierz ryzyka zestawia ze sobą kwestie częstotliwości wystąpienia zdarzenia z jego potencjalnymi konsekwencjami. Stopień granulacji, zarówno w pionie jak i poziomie może być stosownie dopasowywany

Przykład

| (Potencjalne) konsekwencje | Częstotliwość wystąpienia | | |
|---|---|---|---|
| | Rzadko | Czasem | Często |
| Ofiary, poważne konsekwencje dla środowiska, poważne uszkodzenia mienia | 🟥 | 🟥 | 🟥 |
| Poważne obrażenia, ograniczone konsekwencje dla środowiska, uszkodzenia mienia | 🟨 | 🟨 | 🟥 |
| Lekkie obrażenia, brak konsekwencji dla środowiska, znikome uszkodzenia mienia | 🟩 | 🟨 | 🟥 |
| Pomijalny wpływ na osoby, środowisko lub mienie | 🟩 | 🟩 | 🟨 |

🟥 poziom ryzyka nie tolerowany
🟨 poziom ryzyka wymaga dalszej analizy, brak pełnej informacji
🟩 poziom ryzyka tolerowany

# Metody analizy ryzyka

## LOPA

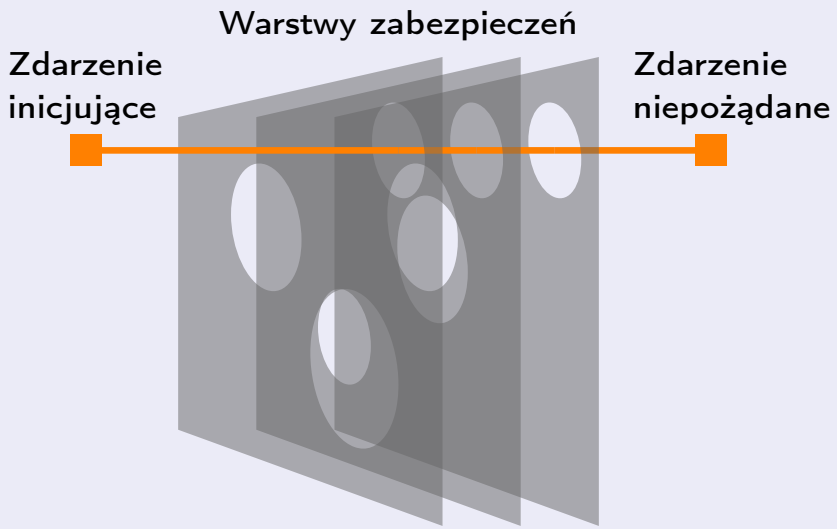
Analiza warstw zabezpieczeń. Odnosi się do funkcji bezpieczeństwa traktowanych jako warstwy. Po pierwsze, identyfikowane są potencjalne zagrożenia, do których przystawia się związane z nimi uszkodzenia i prawdopodobieństwo wystąpienia co pozwala określić poziom ryzyka. Następnie określa się jak użyć dostępne środki zabezpieczeń w celu maksymalizacji efektu. Warstwy zabezpieczeń dzieli się na

- architektura procesu
- system sterowania
- alarmy
- ograniczanie dostępu

# Metody analizy ryzyka

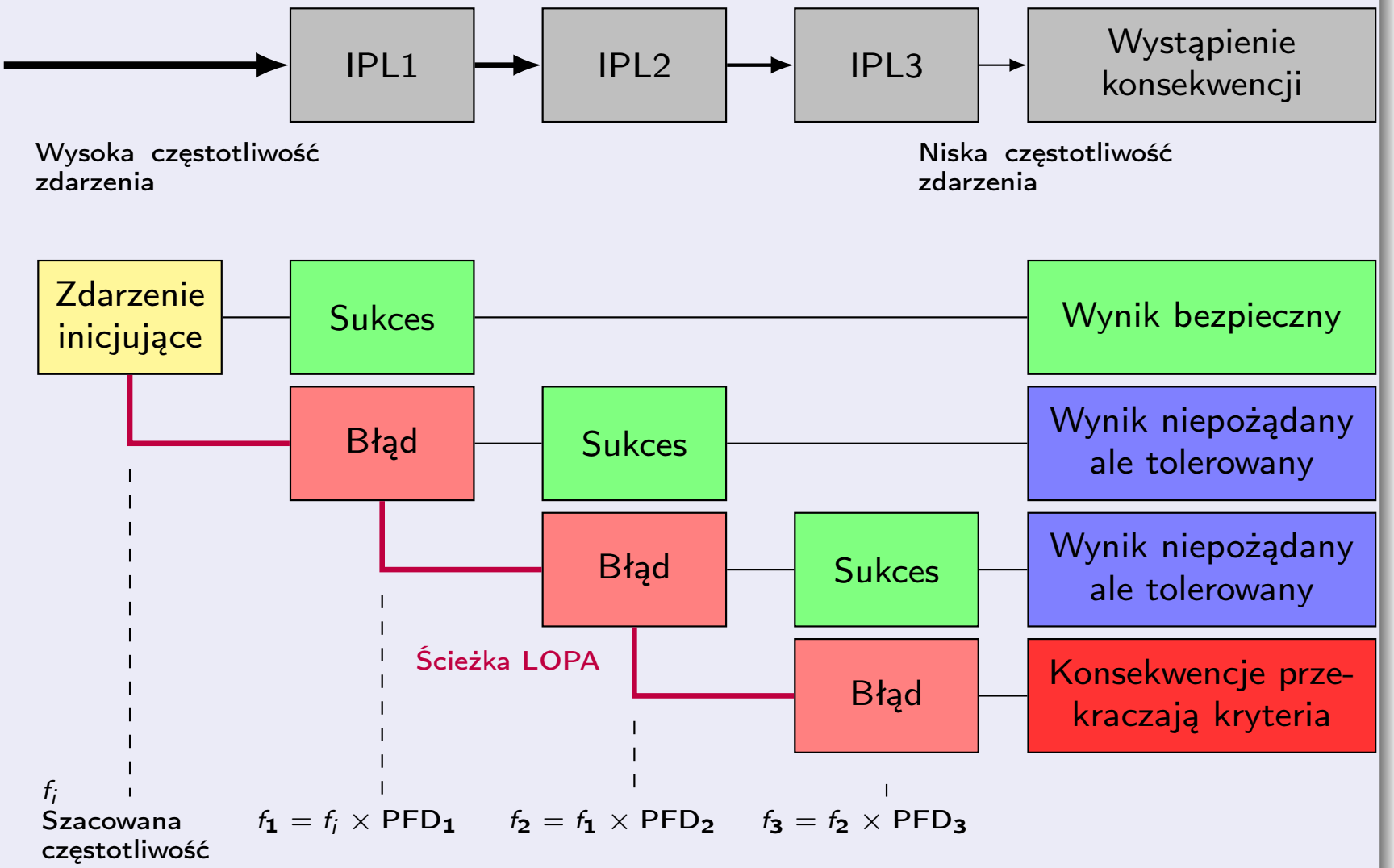
## LOPA c.d.

Kwestie ryzyka resztkowego pozostałego po zastosowaniu wszystkich dostępnych warstw zabezpieczeń modeluje się modelem „sera szwajcarskiego”.



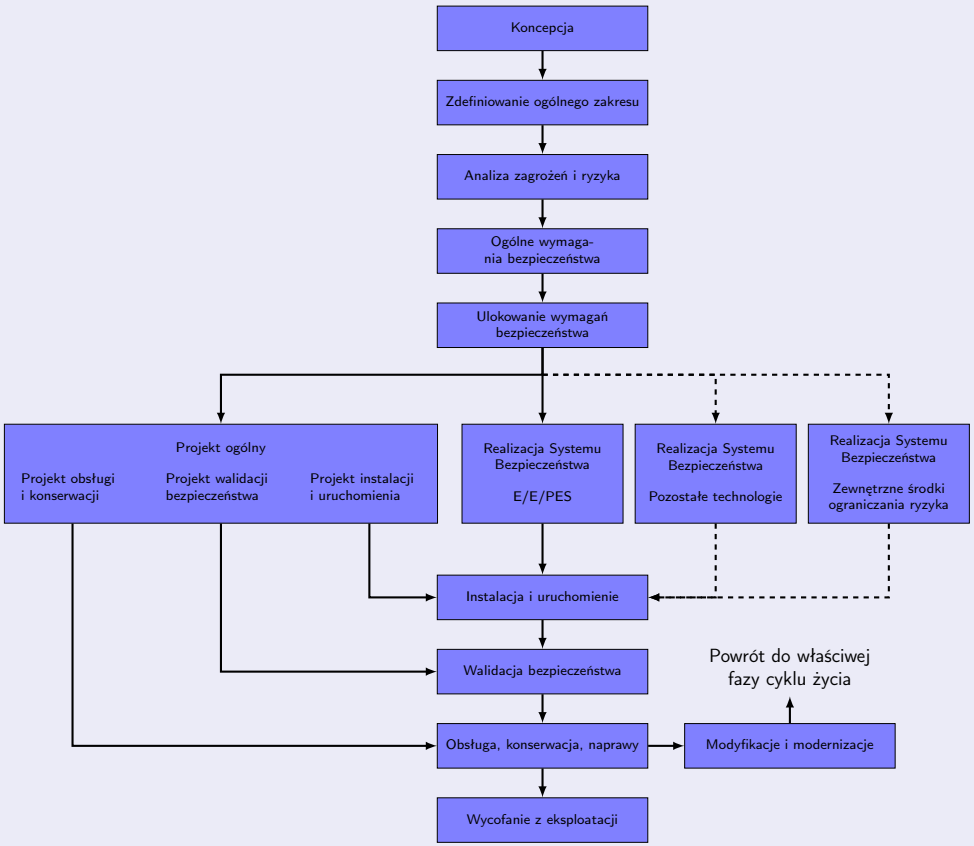
# Metody analizy ryzyka

## LOPA c.d.



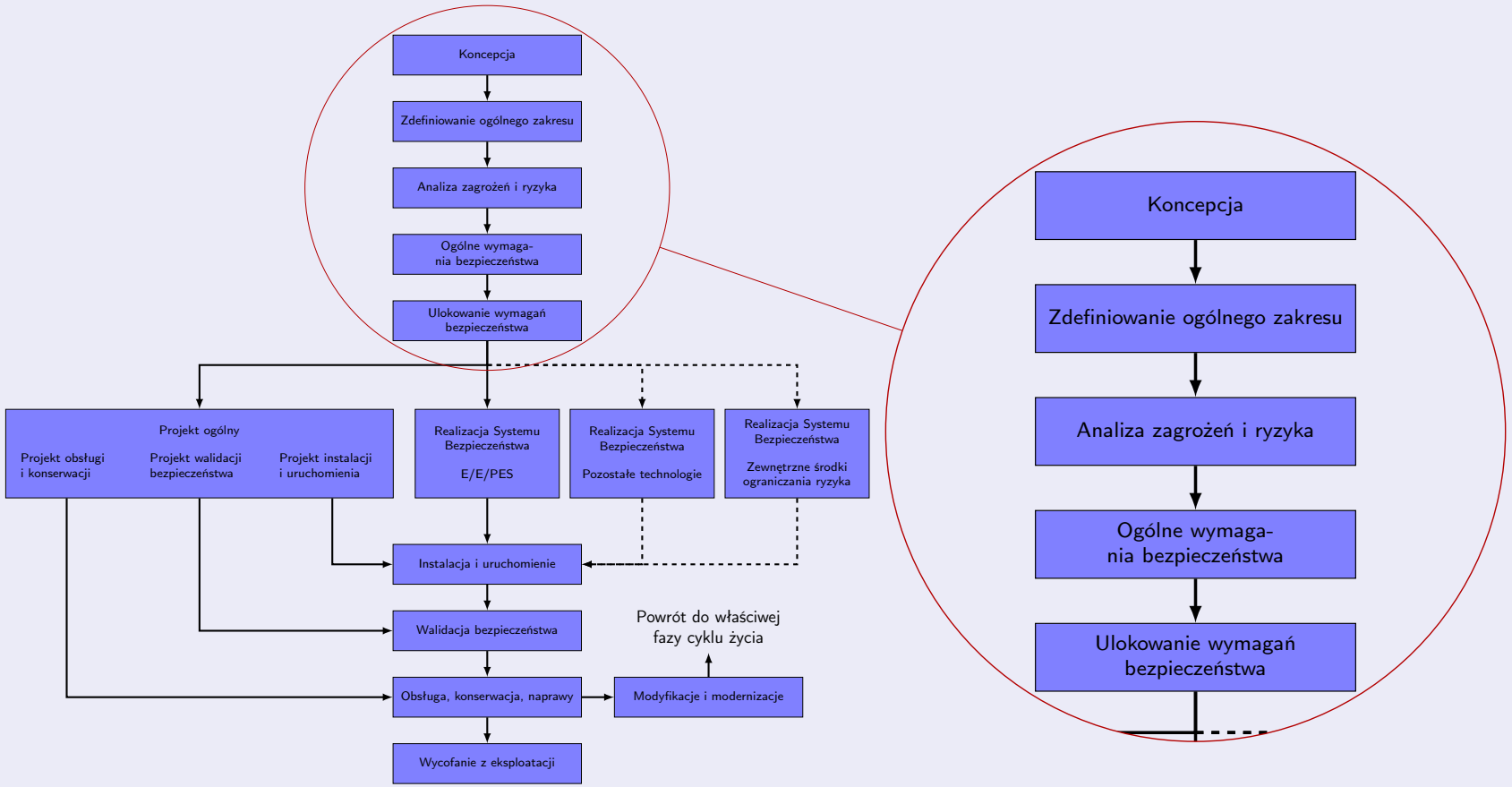
# Cykl życia systemu bezpieczeństwa

## Cykl życia



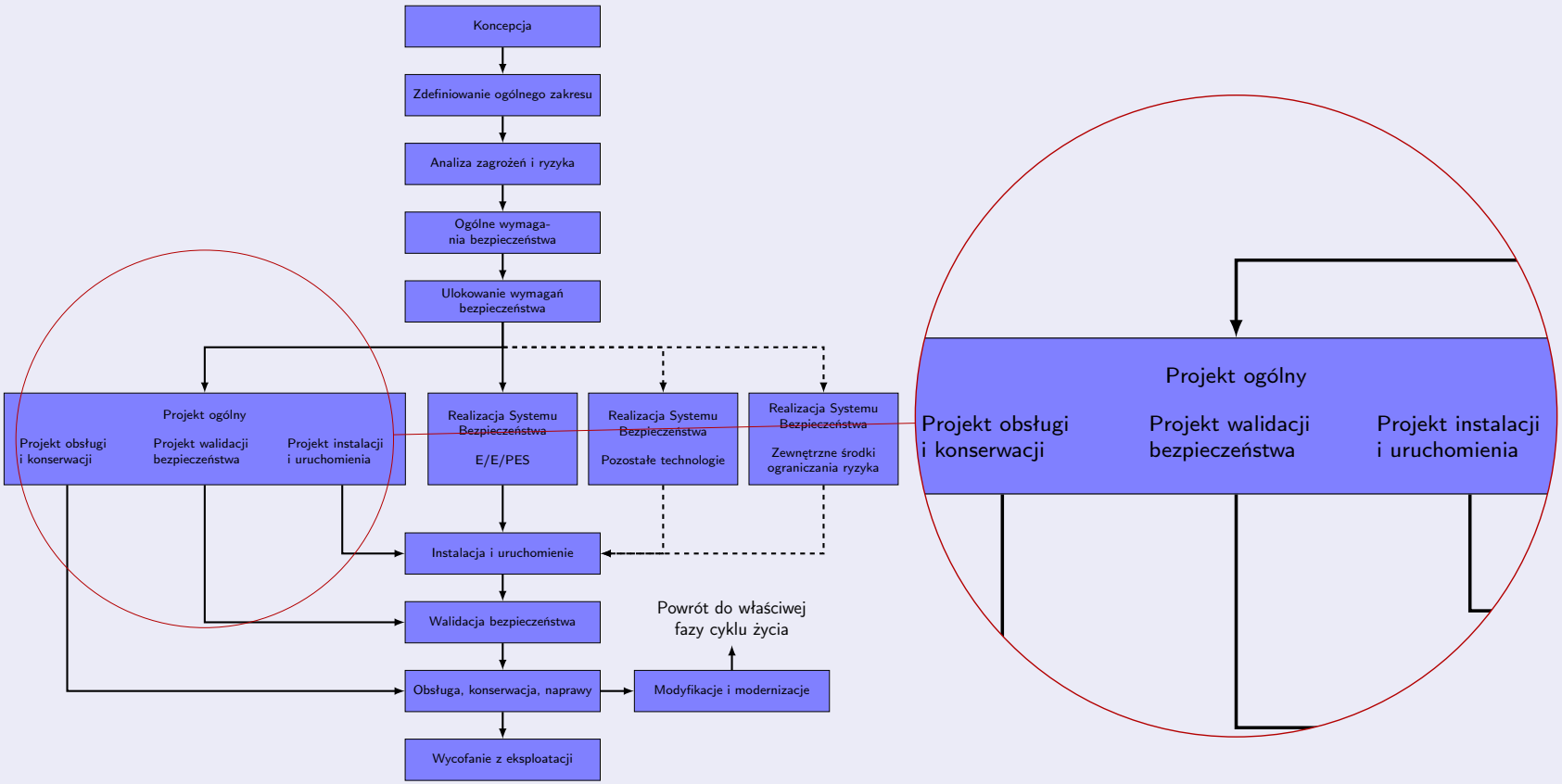
# Cykl życia systemu bezpieczeństwa

## Cykl życia



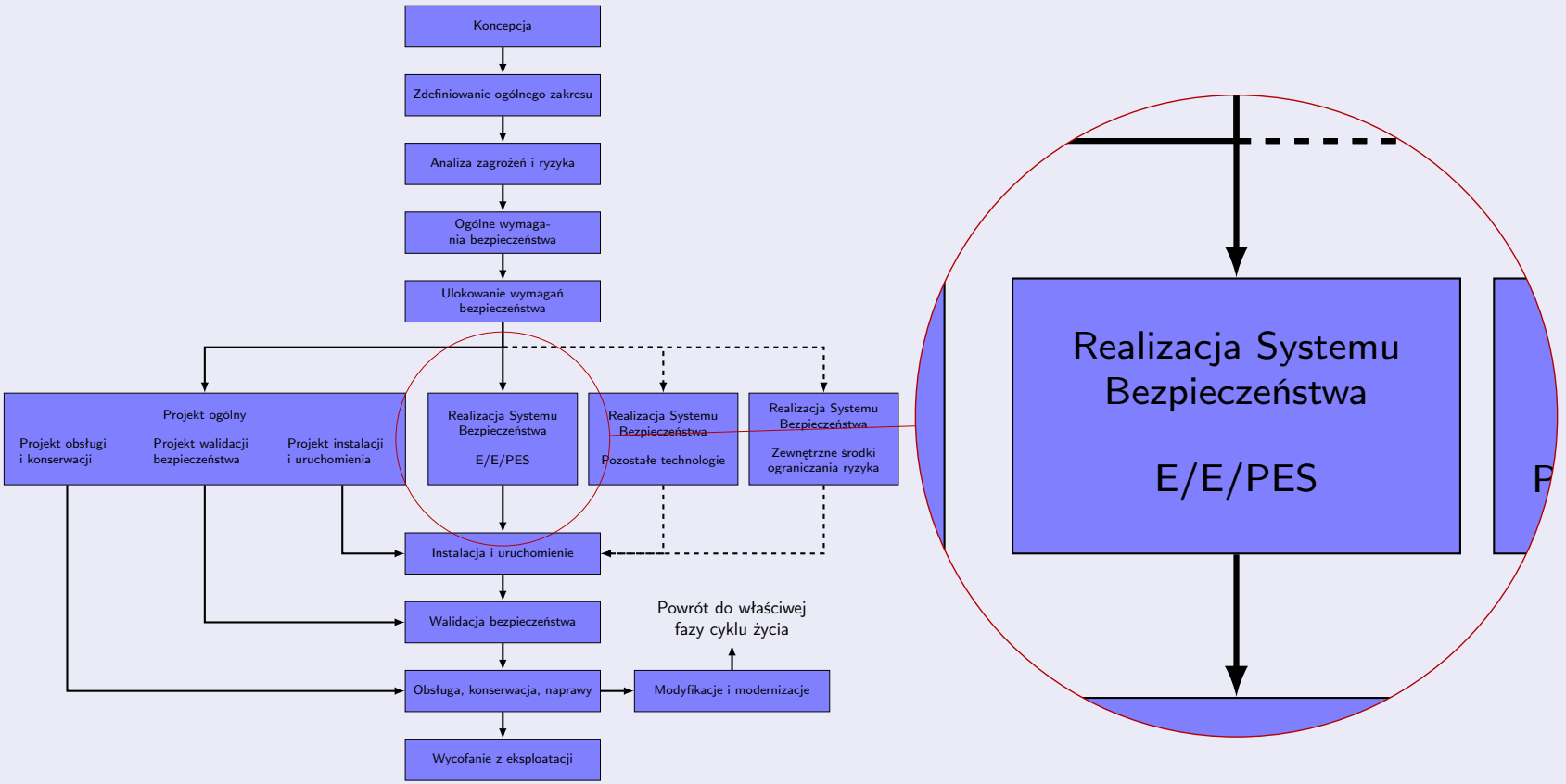
# Cykl życia systemu bezpieczeństwa

## Cykl życia



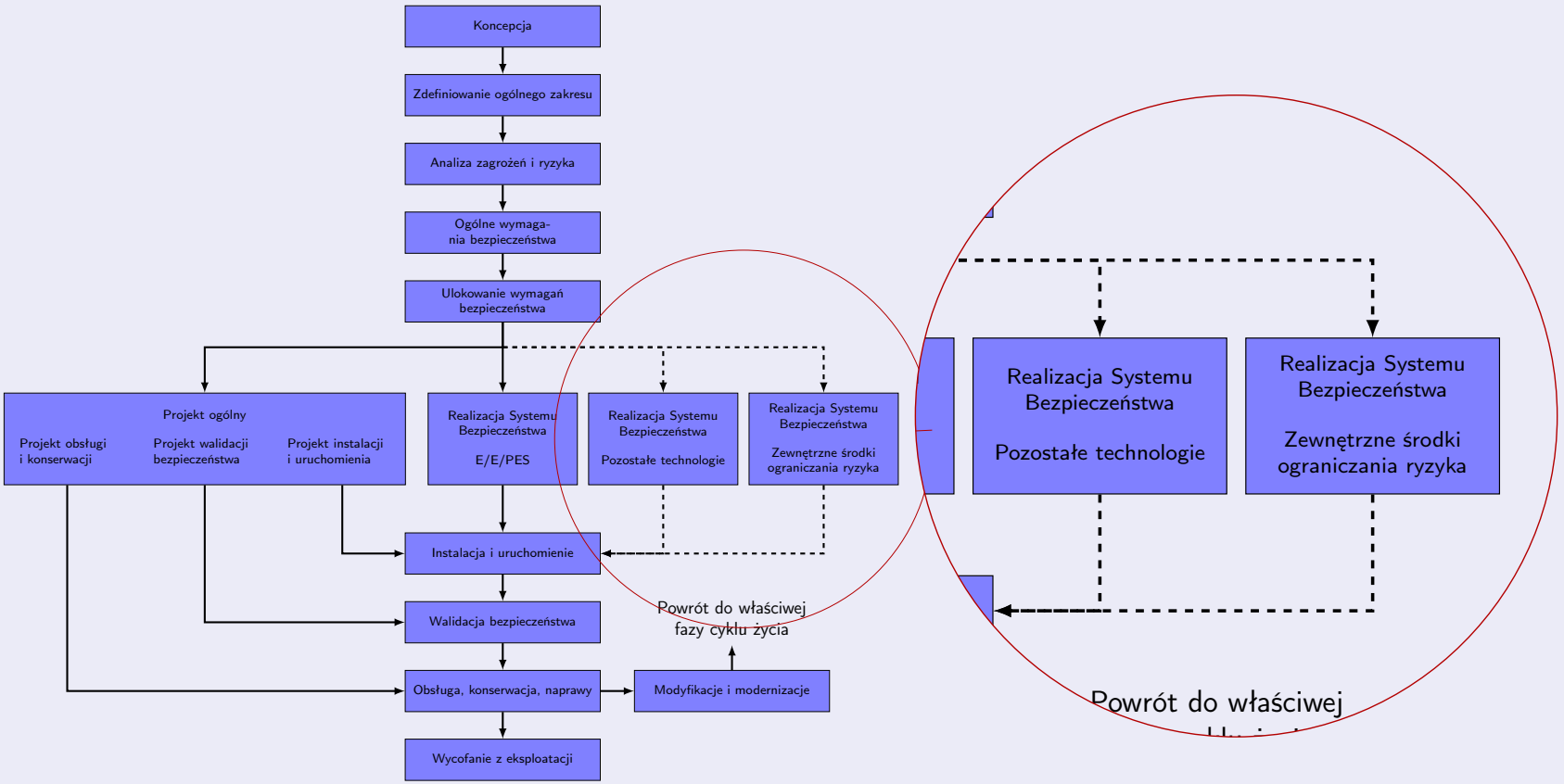
# Cykl życia systemu bezpieczeństwa

## Cykl życia



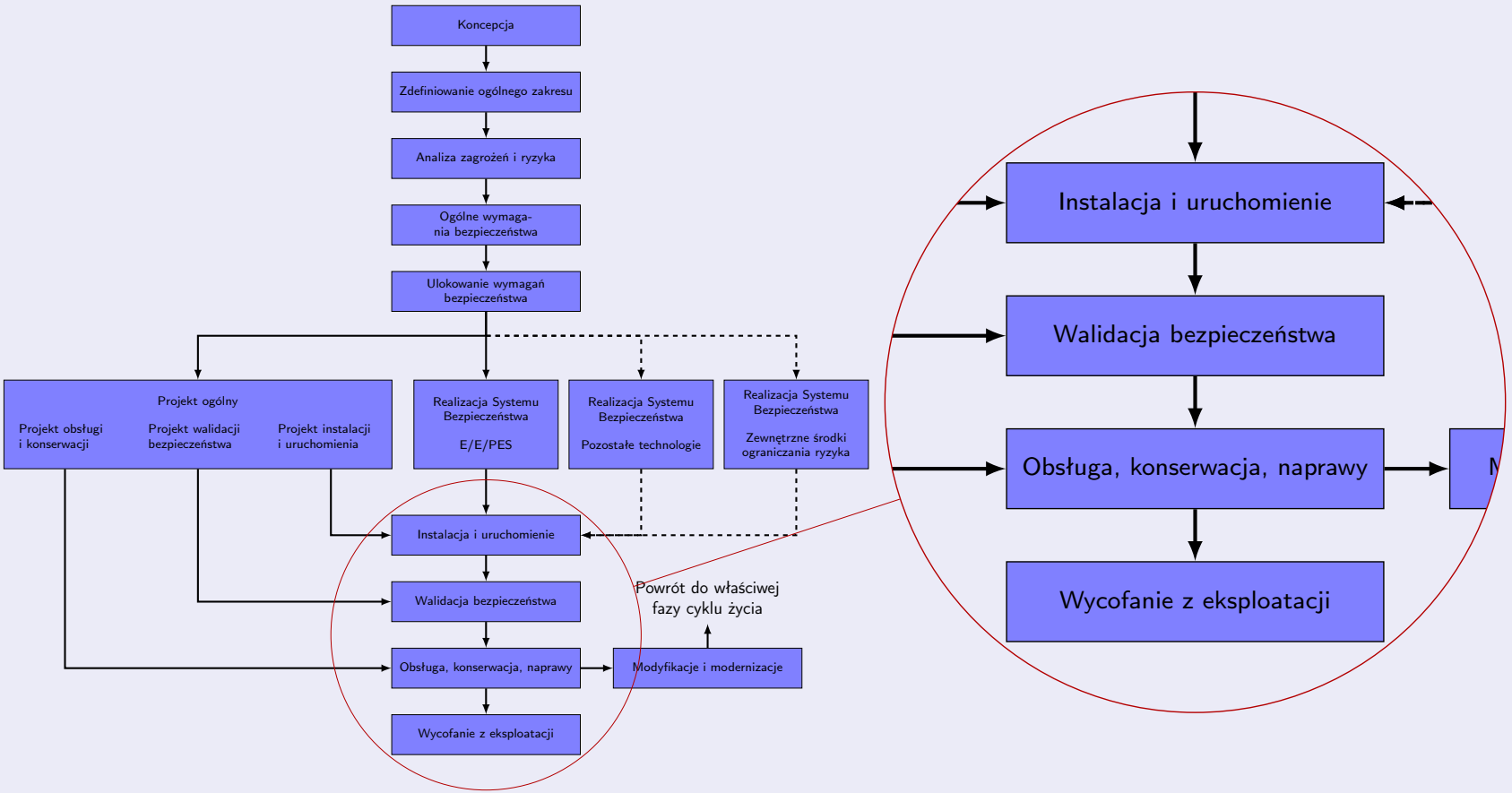
# Cykl życia systemu bezpieczeństwa

## Cykl życia



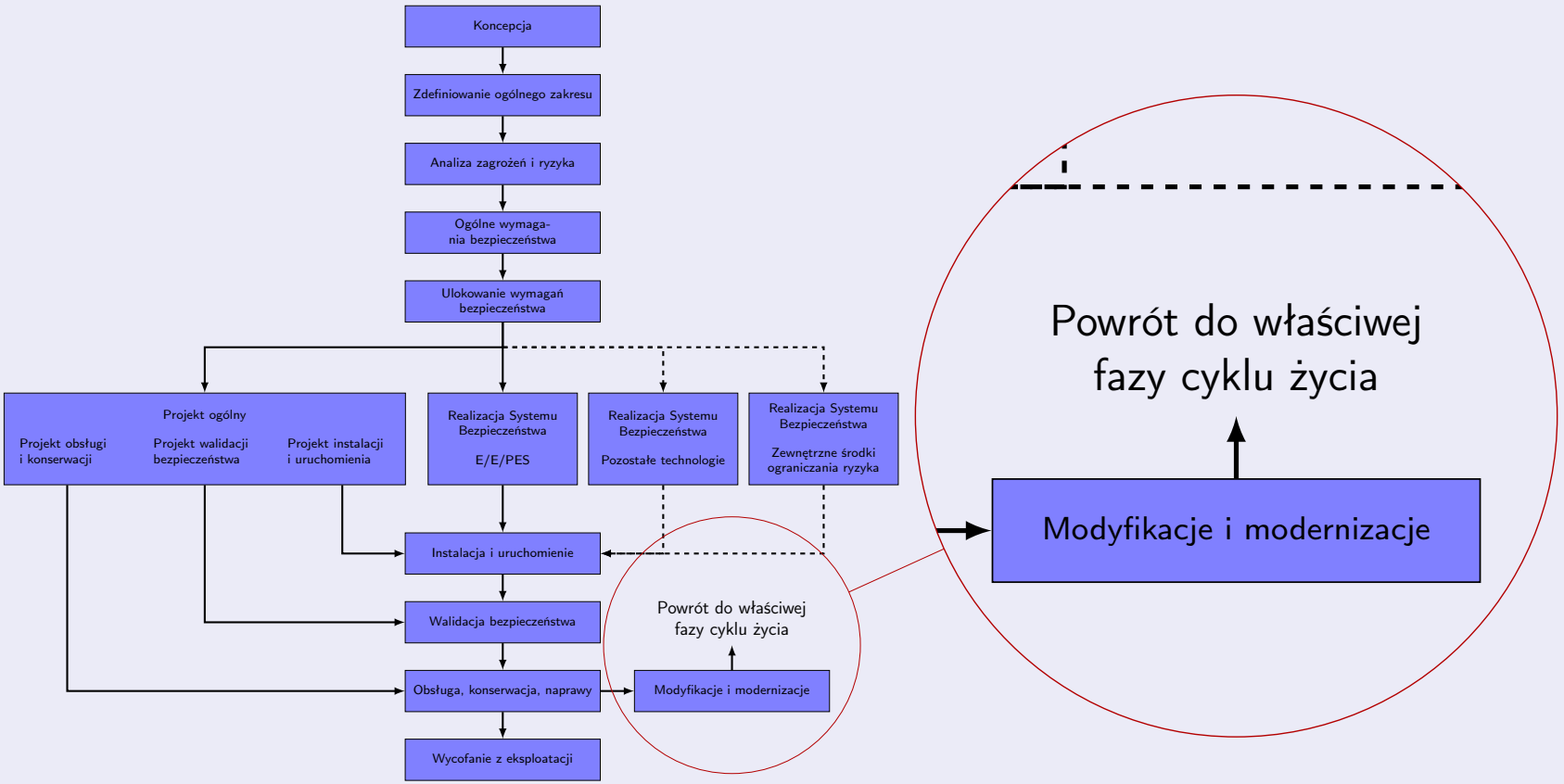
# Cykl życia systemu bezpieczeństwa

## Cykl życia



# Cykl życia systemu bezpieczeństwa

## Cykl życia



# Definicje

## Przyrządowa funkcja bezpieczeństwa (SIF)

Funkcja realizowana przez przyrządowy system bezpieczeństwa SIS, inny (niż BCPS) techniczny system bezpieczeństwa lub zewnętrzne ośrodki ograniczania ryzyka. Jej zadaniem jest doprowadzenie do osiągnięcia stanu bezpiecznego (osiągnięcie poziomu ryzyka tolerowanego) przez instalację zautomatyzowaną. W szczególności, zadziałanie funkcji bezpieczeństwa ma kluczowe znaczenie, gdy zachodzi realne ryzyko utraty kontroli nad instalacją zautomatyzowaną oraz narażenia zdrowia lub życia ludzi, czystości środowiska lub zniszczenia majątku trwałego.

# Definicje

## Przyrządowy system bezpieczeństwa (SIS)

System stosowany do zaimplementowania co najmniej jednej przyrządowej funkcji bezpieczeństwa (SIF), składający się z dowolnej kombinacji czujników, jednostek logicznych oraz elementów wykonawczych.

# Definicje

## Nienaruszalność bezpieczeństwa

Średnie prawdopodobieństwo, że przyrządowy system bezpieczeństwa wykona w sposób zadowalający wymagane przyrządowe funkcje bezpieczeństwa, we wszystkich określonych warunkach i w określonym przedziale czasu.

# Definicje

## Poziom nienaruszalności bezpieczeństwa (SIL)

Poziom dyskretny (od 1 do 4) określający wymagania nienaruszalności bezpieczeństwa przyrządowych funkcji bezpieczeństwa, które powinny być przypisane przyrządowym systemom bezpieczeństwa (SIS).

# Cykl życia systemu bezpieczeństwa

## Zdefiniowanie zakresu

Cykl życia bezpieczeństwa wdrażający wymagania bezpieczeństwa funkcjonalnego powinien być zdefiniowany podczas planowania bezpieczeństwa systemu technicznego.
Muszą istnieć procedury zapewniające szybkie i poprawne wdrażanie zaleceń z oceny bezpieczeństwa funkcjonalnego w cyklu życia.

# Cykl życia systemu bezpieczeństwa

## Ocena zagrożeń

Ocena zagrożeń i ryzyka ma na celu wykrycie zdarzeń awaryjnych związanych z działaniem systemu technicznego.
Każde zidentyfikowane zagrożenie powinno zostać poddane dalszej analizie ryzyka. Na tej podstawie wyznaczyć należy wymaganą redukcję ryzyka związaną z pracą systemu technicznego.

# Cykl życia systemu bezpieczeństwa

## Funkcje bezpieczeństwa

Należy zidentyfikować warstwy zabezpieczeń występujące w systemie technicznym, a następnie przypisać funkcje bezpieczeństwa konkretnym warstwom zabezpieczeń.
Każda funkcja bezpieczeństwa musi mieć przypisaną wartość wymaganej redukcji ryzyka wyrażoną za pomocą wymaganego poziomu SIL.

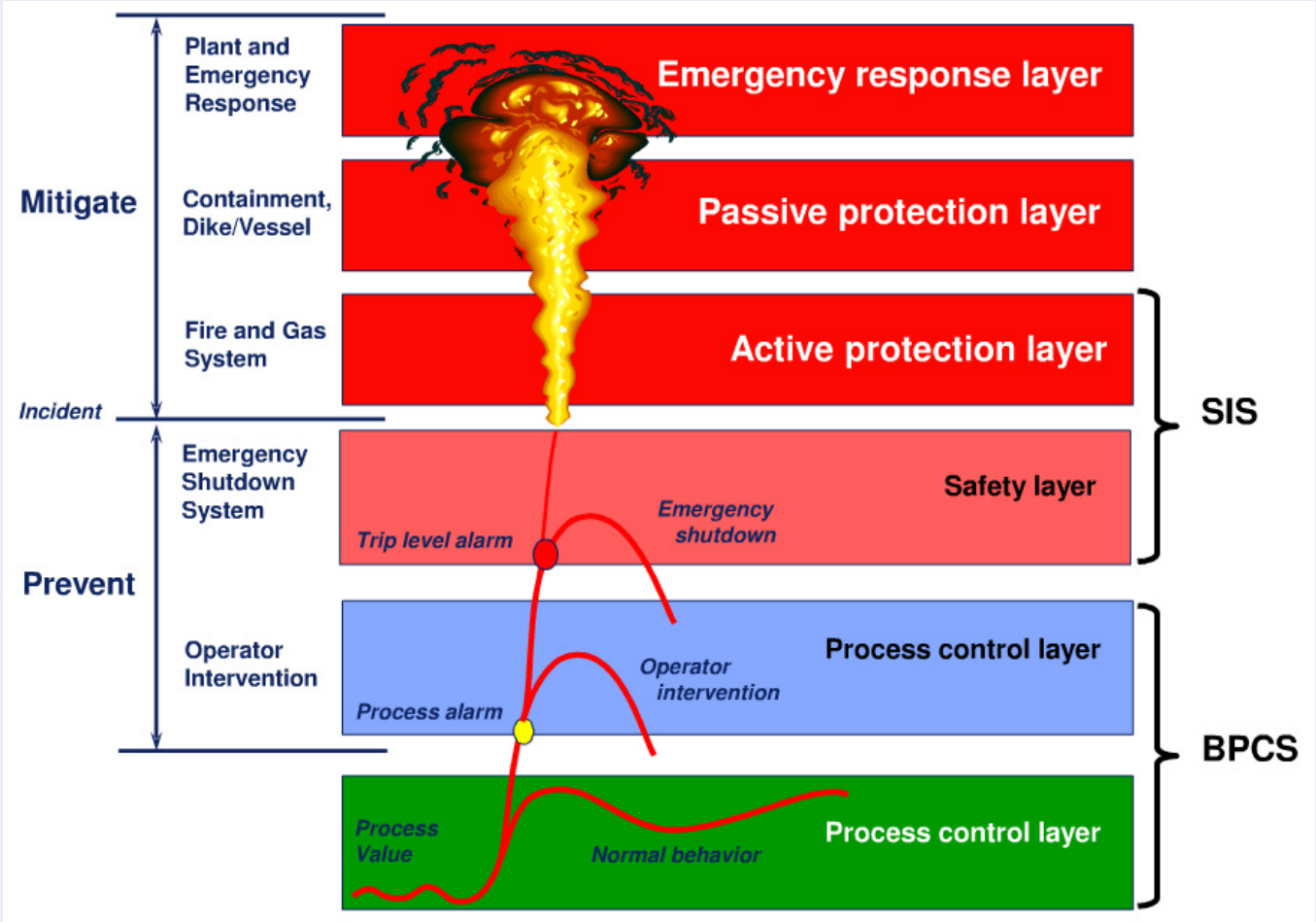
# Cykl życia systemu bezpieczeństwa

## Warstwy zabezpieczeń

1. Instalacja procesowa
2. Automatyka procesowa (BPCS)
3. Alarmy/interwencje operatorów
4. Automatyka zabezpieczeniowa (SIS)
5. Ograniczanie skutków awarii
6. Wewnętrzne przeciwdziałanie skutkom
7. Zewnętrzne przeciwdziałanie skutkom

# Cykl życia systemu bezpieczeństwa

## Warstwy zabezpieczeń



# Cykl życia systemu bezpieczeństwa

## Specyfikacja wymagań – wymagania funkcjonalne

Jakie zadania w systemie bezpieczeństwa przypisane są poszczególnym funkcjom bezpieczeństwa oraz jakie wymagania funkcjonalne muszą one spełniać.

## Wymagania SIL

Wymagana redukcja ryzyka (RRF) przypisana do warstwy realizującej funkcję bezpieczeństwa.
SIL przypisany jest do przedziału prawdopodobieństwa lub częstości niezadziałania funkcji.

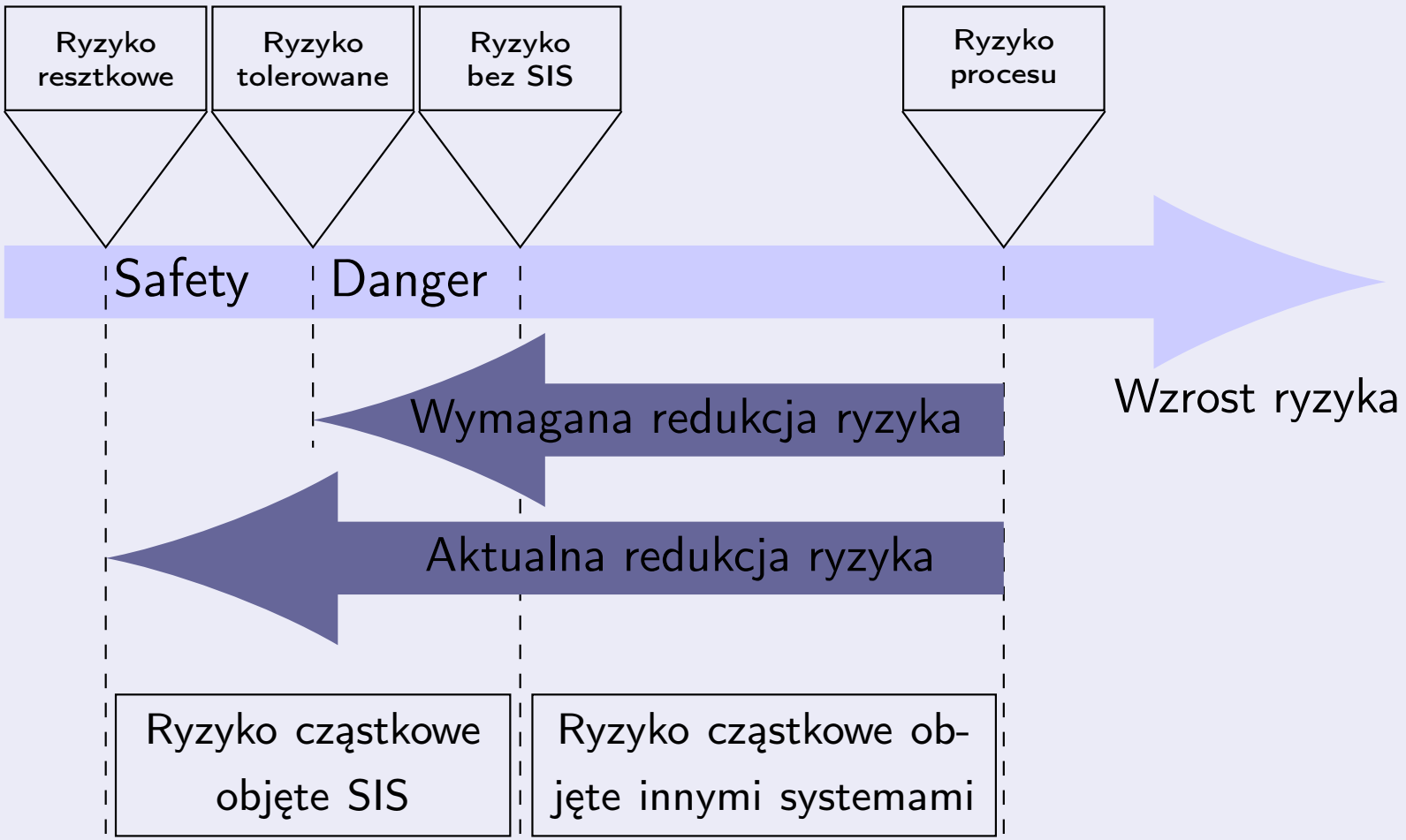
# Cykl życia systemu bezpieczeństwa

## SIL

| SIL | Docelowe zmniejszenie ryzyka RRF |
|---|---|
| SIL 4 | od >10000 do < 100000 |
| SIL 3 | od >1000 do < 10000 |
| SIL 2 | od >100 do < 1000 |
| SIL 1 | od >10 do < 100 |

# Cykl życia systemu bezpieczeństwa

## Redukcja ryzyka



# Cykl życia systemu bezpieczeństwa

## Projekt systemu SIS i jego weryfikacja

Funkcje bezpieczeństwa muszą być realizowane przez przyrządowy system bezpieczeństwa (SIS).
Projekt SIS powinien być zgodny z wymaganiami funkcjonalnymi oraz spełniać warunek na nienaruszalność bezpieczeństwa. Wynikają one ze specyfikacji wymagań bezpieczeństwa określonej w poprzednim etapie cyklu życia bezpieczeństwa.

# Cykl życia systemu bezpieczeństwa

## Projekt systemu SIS i jego weryfikacja

Prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa powinno być równe lub mniejsze docelowej mierze uszkodzeń wyszczególnionej w specyfikacji wymagań bezpieczeństwa.
W zależności od trybu pracy funkcji bezpieczeństwa osiągnięty poziom SIL wyraża się za pomocą parametru $\mathrm{PFD}_{\mathrm{avg}}$ lub $\mathrm{PFH}$.

# Cykl życia systemu bezpieczeństwa

## Poziomy nienaruszalności bezpieczeństwa

| SIL | Rzadkie przywołanie do działania $\mathrm{PFD}_{\mathrm{avg}}$ | Częste przywołanie lub praca ciągła PFH |
|---|---|---|
| SIL 4 | od $\geqslant 10^{-5}$ do $< 10^{-4}$ | od $\geqslant 10^{-9}$ do $< 10^{-8}$ |
| SIL 3 | od $\geqslant 10^{-4}$ do $< 10^{-3}$ | od $\geqslant 10^{-8}$ do $< 10^{-7}$ |
| SIL 2 | od $\geqslant 10^{-3}$ do $< 10^{-2}$ | od $\geqslant 10^{-7}$ do $< 10^{-6}$ |
| SIL 1 | od $\geqslant 10^{-2}$ do $< 10^{-1}$ | od $\geqslant 10^{-6}$ do $< 10^{-5}$ |

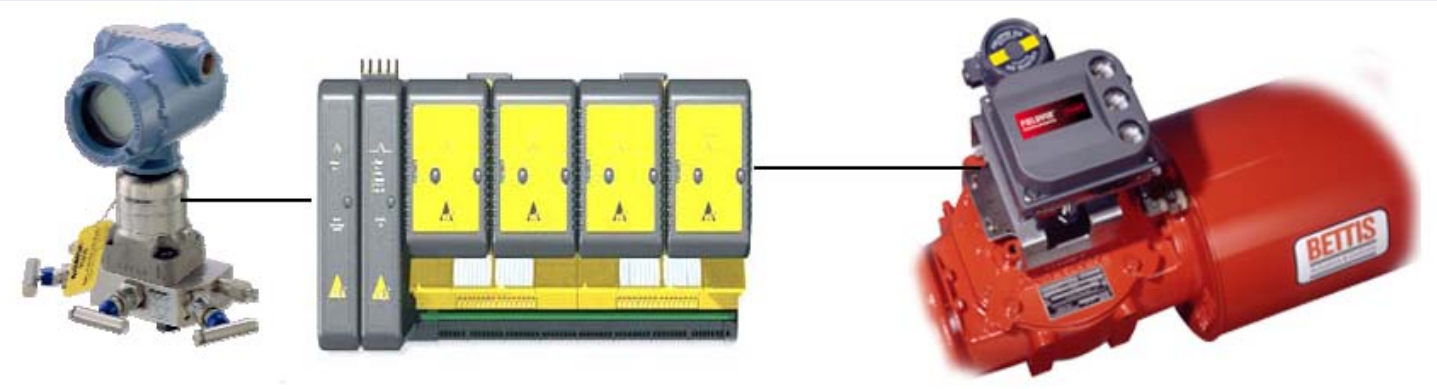
## $\mathrm{PFD}_{\mathrm{AVG}}$ i PFH

$\mathrm{PFD}_{\mathrm{AVG}}$ Średnie prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie

PFH Średnia częstość uszkodzenia niebezpiecznego funkcji bezpieczeństwa na godzinę

# Cykl życia systemu bezpieczeństwa

## Przyrządowy system bezpieczeństwa (SIS)




## Ograniczenia architektury

Czujniki, jednostki logiczne oraz elementy wykonawcze zastosowane w realizacji funkcji bezpieczeństwa powinny mieć określoną minimalną tolerancję defektów sprzętu (HFT).
HFT wyraża zdolność wypełnienia wymaganej funkcji bezpieczeństwa przy wystąpieniu przynajmniej jednego defektu sprzętu (związane jest to z tzw. redundancją sprzętową).

# Cykl życia systemu bezpieczeństwa

## Minimalna tolerancja defektów sprzętu typu A

| SFF | Tolerancja defektów sprzętu (HFT) | | |
|---|---|---|---|
| Udział uszkodzeń bezpiecznych | 0 | 1 | 2 |
| $< 60\%$ | SIL 1 | SIL 2 | SIL 3 |
| od 60% do 90% | SIL 2 | SIL 3 | SIL 4 |
| od 90% do 99% | SIL 3 | SIL 4 | SIL 4 |
| $> 99\%$ | SIL 3 | SIL 4 | SIL 4 |

## Urządzenie typu A

Urządzenia „proste“ (wszelkie usterki znane i opisane)

# Cykl życia systemu bezpieczeństwa

## Minimalna tolerancja defektów sprzętu typu B

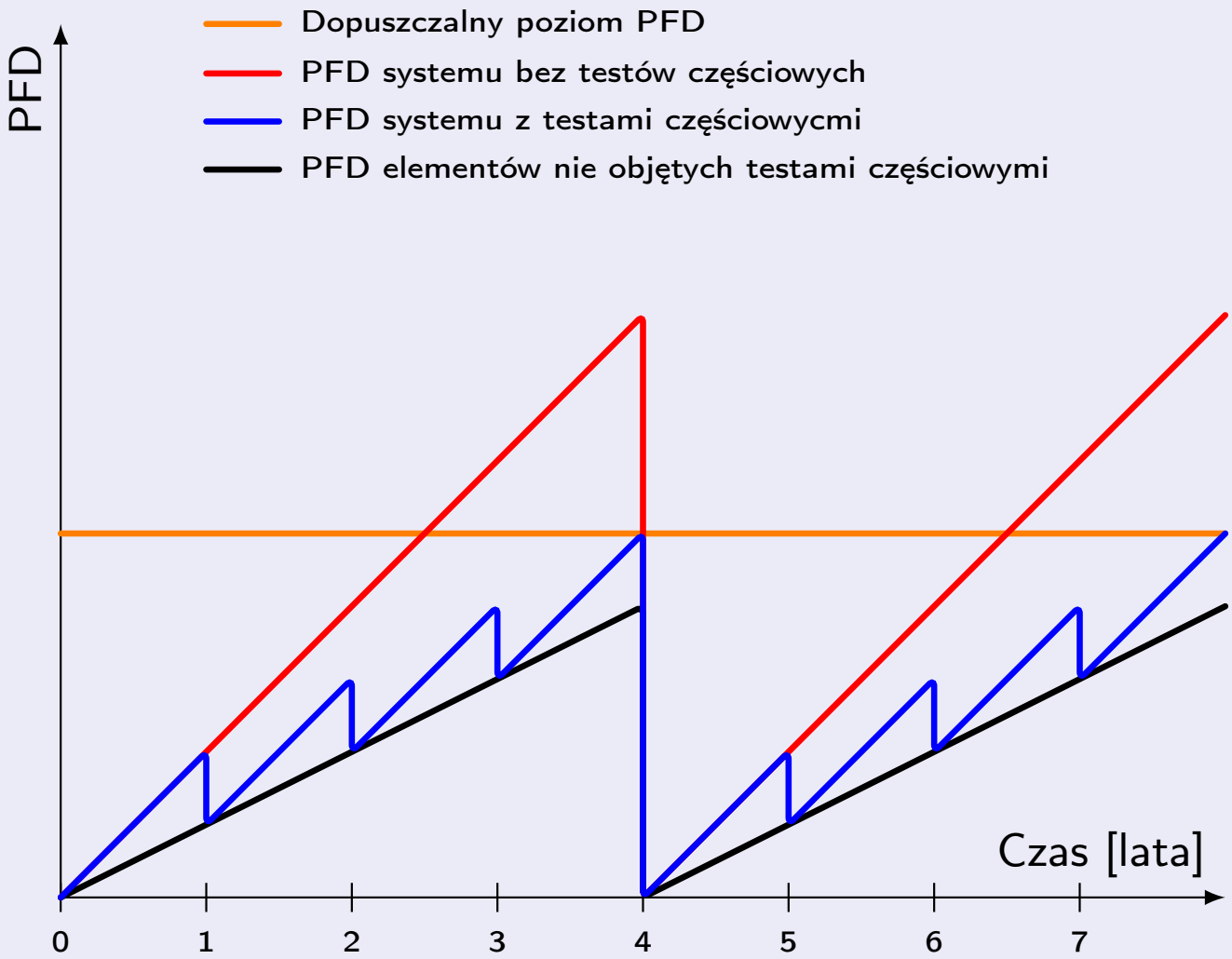
| SFF | Tolerancja defektów sprzętu (HFT) | | |
|---|---|---|---|
| Udział uszkodzeń bezpiecznych | 0 | 1 | 2 |
| $< 60\%$ | niedozwolone | SIL 1 | SIL 2 |
| od 60% do 90% | SIL 1 | SIL 2 | SIL 3 |
| od 90% do 99% | SIL 2 | SIL 3 | SIL 4 |
| $> 99\%$ | SIL 3 | SIL 4 | SIL 4 |

## Urządzenie typu B

Urządzenia „złożone“ (nie wszystkie usterki znane i opisane)

# Cykl życia systemu bezpieczeństwa

## Testy częściowe i okresowe a wartość $PFD_{AVG}$



# Cykl życia systemu bezpieczeństwa

## Testy sprawdzające

Okresowe testy sprawdzające należy przeprowadzać w oparciu o procedurę pisemną, w celu wykrycia błędów nieujawnionych, które uniemożliwiają pracę systemu SIS zgodną ze specyfikacją bezpieczeństwa.
Częstość testów sprawdzających powinna być taka jaką użyto w procesie weryfikacji SIL.

# Cykl życia systemu bezpieczeństwa

## Eksploatacja i wdrożenie

Należy pracować i obsługiwać system realizujący funkcje bezpieczeństwa tak, aby było utrzymane zaprojektowanie bezpieczeństwo funkcjonalne.
Należy zapewnić, że wymagany poziom nienaruszalności bezpieczeństwa SIL każdej funkcji bezpieczeństwa jest utrzymywany podczas pracy i obsługi.

# Cykl życia systemu bezpieczeństwa

## Eksploatacja i wdrożenie

Należy przeprowadzić planowanie pracy i obsługi systemów realizujących funkcje bezpieczeństwa.
Wg planu przeprowadza się m.in. walidację systemu bezpieczeństwa, dokumentowanie stanów normalnej pracy i awaryjnych, dokumentowanie wyników testów okresowych, weryfikację przestrzegania planu.

# Cykl życia systemu bezpieczeństwa

## Zarządzanie modyfikacjami

Przed wykonaniem jakiejkolwiek modyfikacji systemu realizującego funkcje bezpieczeństwa powinny zaistnieć procedury autoryzacji i kontrolowania zmian.
Procedury te powinny zawierać jasne metody identyfikacji i żądania prac do wykonania oraz zagrożeń, na jakie mają mieć wpływ.

# Cykl życia systemu bezpieczeństwa

## Zarządzanie modyfikacjami

Należy określić wpływ wprowadzanych modyfikacji na bezpieczeństwo funkcjonalne. Jeżeli analiza wykaże taki wpływ, należy powrócić do pierwszej z faz cyklu życia systemu bezpieczeństwa, zakłóconej przez tę modyfikację.
Każda zmiana wprowadzona do systemu realizującego funkcje bezpieczeństwa musi być udokumentowana, a personel ją wykonujący powinen być odpowiednio przeszkolony.

# Cykl życia systemu bezpieczeństwa

## Wyłączenie z eksploatacji

W ramach wyłączenia z eksploatacji systemu związanego z bezpieczeństwem należy wykonać ocenę oddziaływania czynności tego etapu an bezpieczeństwo funkcjonalne.
Ocena ta powinna zawierać uaktualnione oceny zagrożeń i ryzyka wynikające z przeprowadzonych czynności związanych z wyłączeniem systemu z eksploatacji.

# Słowniczek

| | |
|---|---|
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SIF | Safety Instrumented Function |
| BPCS | Basic Process Control System |
| IPL | Independent Protection Layer |
| FSM | Functional Safety Management |

# Słowniczek

| | |
|---|---|
| MTTF | Mean Time To Failure |
| HFT | Hardware Fault Tolerance |
| SFF | Safe Failure Fraction |
| PFD | Probability of Failure on Demand |
| PFH | Probability of Failure per Hour |
| RRF | Risk Reduction Factor |

# Literatura


- Functional Safety Compendium
  Pepperl+Fuchs
- Manual Safety Integrity Level
  Pepperl+Fuchs
- Basic Fundamentals Of Safety Istrumented Systems
  Emerson
- HIMA's Next Generation Safety Controller Maximizes Availability for Demanding Process Applications
  ARC Advisory Group