



Zintegrowany proces podejmowania decyzji w zakresie bezpieczeństwa instalacji procesowych

M. Borysiewicz, K. Kowal, S. Potemski

Narodowe Centrum Badań Jądrowych, Otwock-Świerk

XI Konferencja Naukowo-Techniczna
Bezpieczeństwo Techniczne w Przemysle
Łódź, 19.09.2012



Plan prezentacji

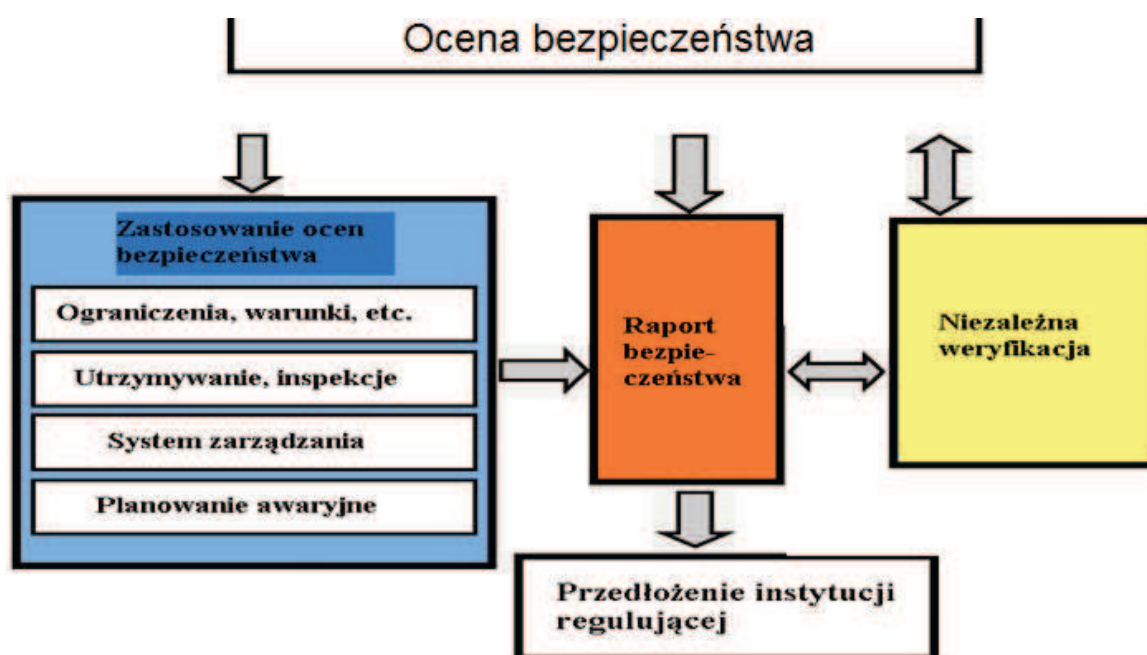
- ✓ Elementy oceny bezpieczeństwa
- ✓ Zintegrowana ocena ryzyka (IRIDM)
- ✓ Analizy deterministyczne (DSA)
- ✓ Analizy probabilistyczne (PSA)
- ✓ Integracja podejścia DSA i PSA
- ✓ Problemy niepewności

Elementy oceny bezpieczeństwa



źródło: IAEA: Safety Guards

Elementy oceny bezpieczeństwa



źródło: IAEA: Safety Guards



IRIDM – Integrated Risk Informed Decision Making

- Zwiększone zainteresowanie w stworzeniu strukturalnej platformy wspomagającej podejmowania optymalnych decyzji
- Narzędzia PSA/QRA są coraz bardziej dojrzałe i częściej używane. Jest to więc dobry moment do ustanowienia dobrych praktyk opartych na spójnym wykorzystaniu podejścia deterministycznego oraz probabilistycznego
- Cel: zintegrowanie procesu podejmowania decyzji dla instalacji technologicznych
- Przykład: MAEA zachęca do stosowania takiego podejścia w dziedzinie bezpieczeństwa reaktorów
- Podejście zintegrowane może być zastosowane do podejmowania decyzji dotyczących bezpieczeństwa instalacji technologicznych w fazie projektowej oraz eksploatacyjnej



Analizy deterministyczne (DSA)

✓ Cechy podejścia DSA

- Projektowanie z tolerancją błędów
- Marginesy bezpieczeństwa
- Oparte na filozofii „głębokiej obrony”
- Nacisk na prewencję
- Łagodzenie skutków awarii
- Analizy projektowe

✓ Cel podejścia DSA

Określenie i zastosowanie konserwatywnych założeń i wymogów do projektu a także funkcjonowania instalacji oraz planowanych i wykonywanych działań.

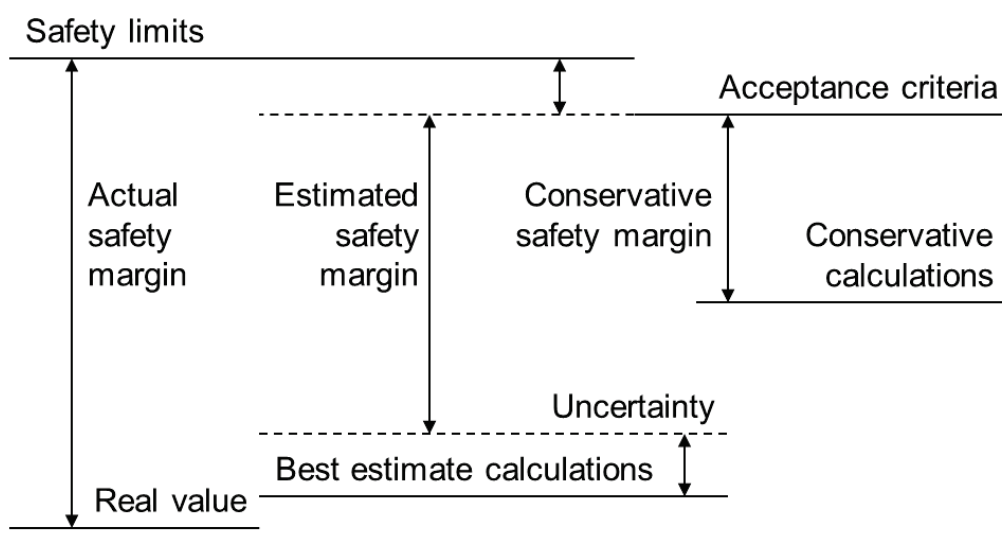
✓ Metodologia DSA

- Oczekuje się, że poziom ryzyka dla pracowników i populacji, związany z daną instalacją będzie akceptowalnie mały.
- Jest to osiągane poprzez wprowadzenie dużego marginesu bezpieczeństwa co kompensuje niepewności związane ze sprzętem i zachowaniem się personelu.
- Analizy deterministyczne stosują przyjęte założenia inżynierskie odnośnie rozwiązań technicznych i organizacyjnych dla przewidywania przebiegu zdarzeń i ich skutków.



Analizy deterministyczne (DSA)

- Minimalne marginesy do kryteriów akceptacji określone są dla każdej grupy postulowanych zdarzeń inicjujących i sekwencji



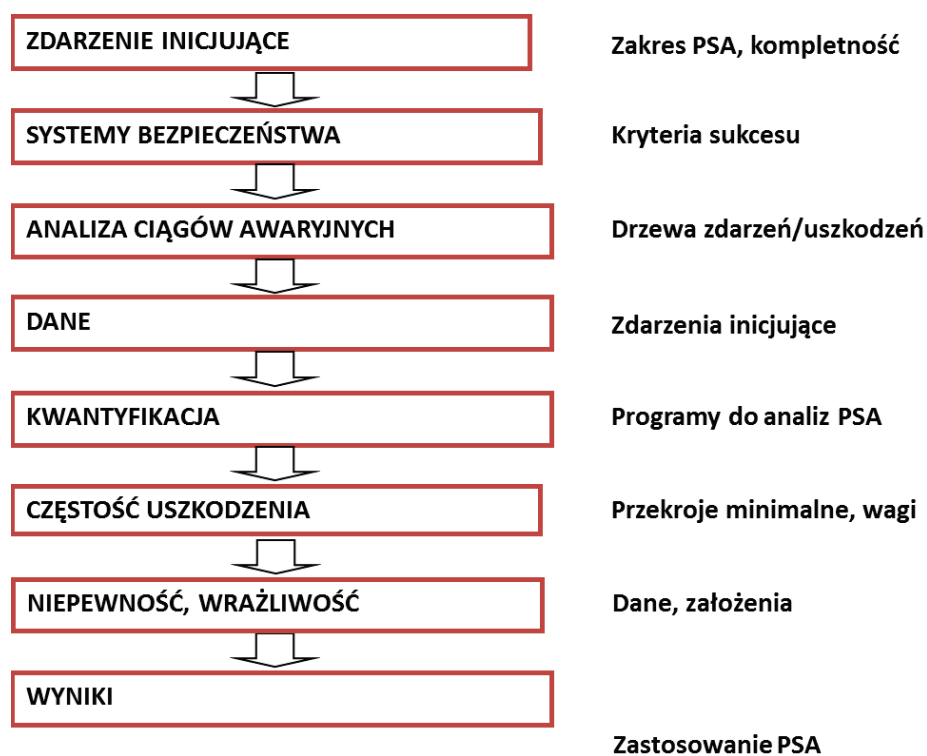


Analizy probabilistyczne (PSA/QRA)

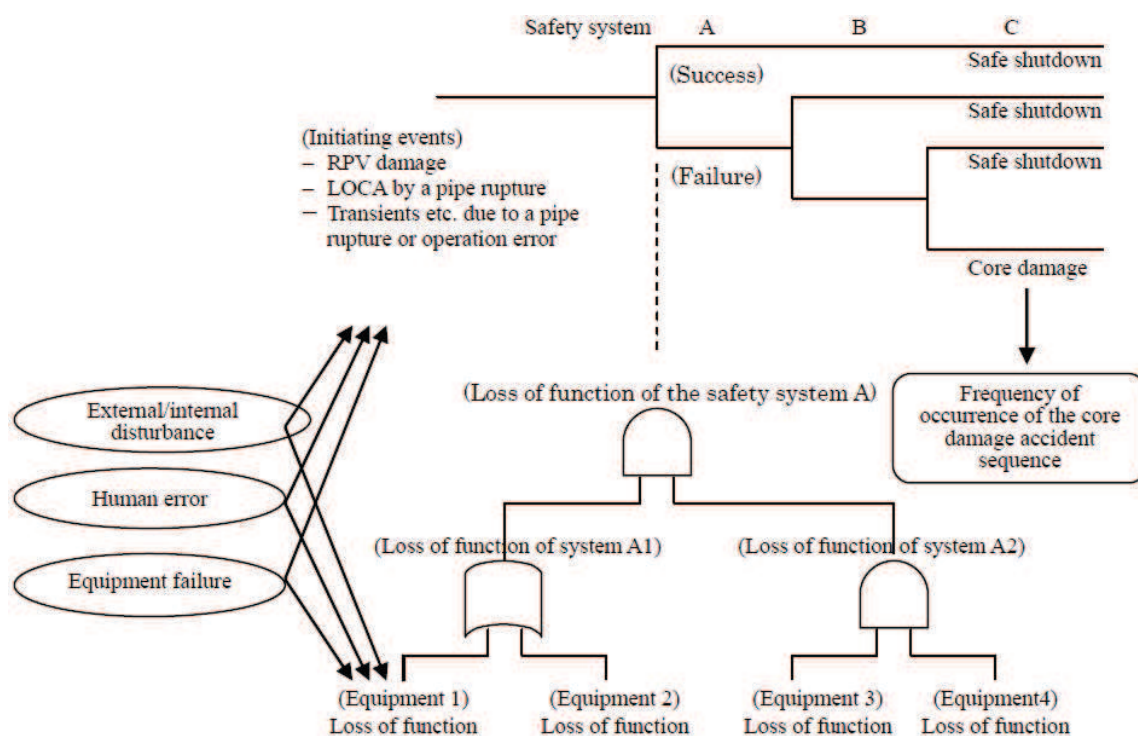
- Informacje z diagramów logicznych mogą pokazać słabości i brak zrównoważonego podejścia w danym projekcie lub operacji technologicznej, lub zbyt silna zależność od szczególnej funkcji, urządzeń czy działań operatora
- Używane są do identyfikacji wagi możliwych słabych punktów rozwiązań inżynierskich i procedur eksploatacji instalacji
- Mogą być używane do analizowania zdarzeń wymagających szczegółowych analiz deterministycznych
- Pozwalają na określenie marginesów bezpieczeństwa i wskazania sposobów redukcji ryzyka poważnych awarii



Analizy PSA – Poziom 1

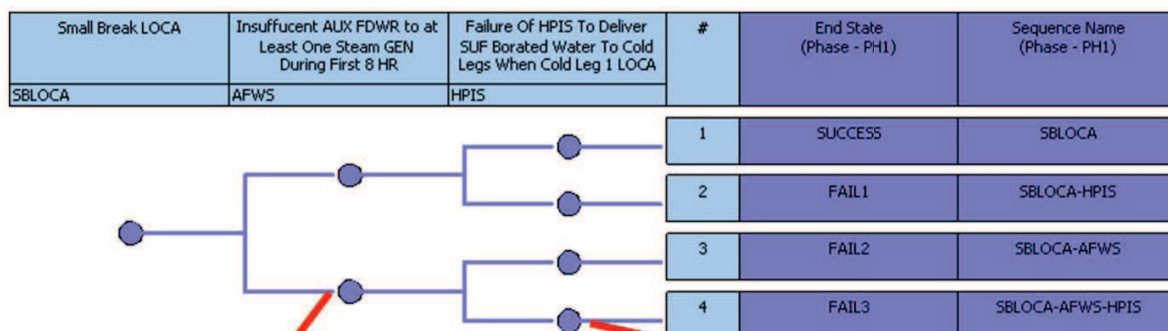


Analizy PSA – Drzewa zdarzeń/uszkodzeń

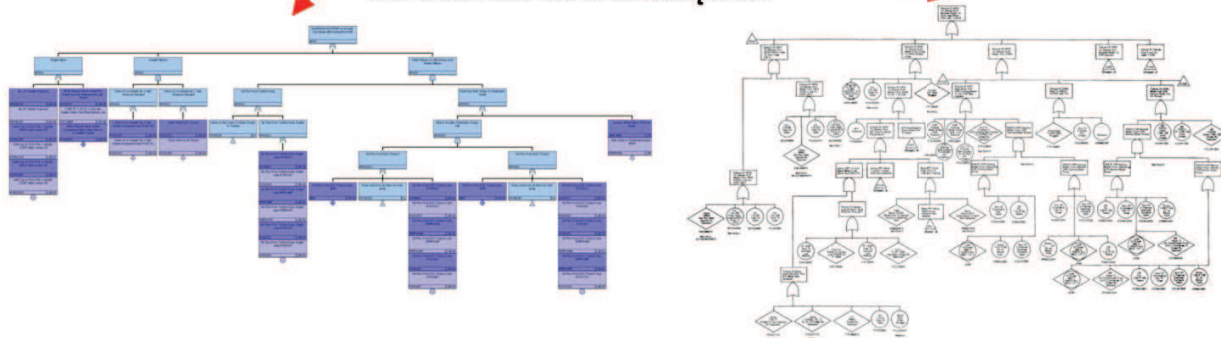


Analizy PSA – Drzewa zdarzeń oraz uszkodzeń

Drzewo zdarzeń

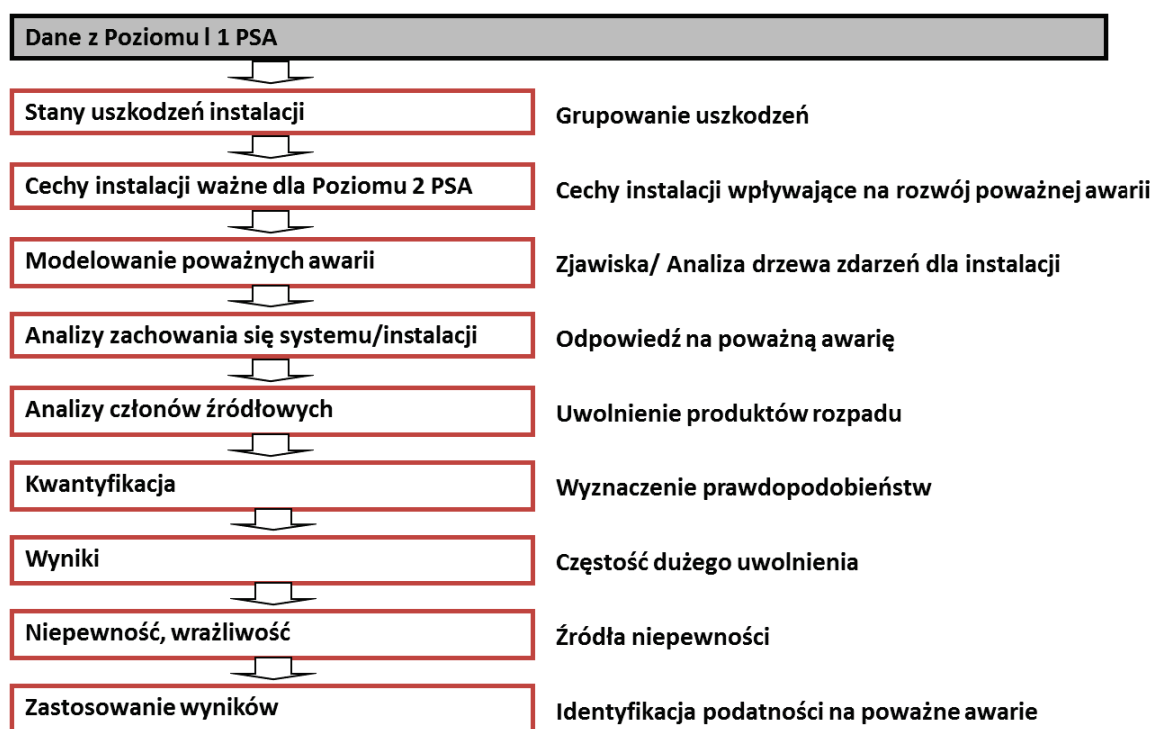


Drzewa uszkodzeń/błędów





Analizy PSA – Poziom 2



Analizy PSA – Poziom 3

Dane z poziomu 2 PSA

Poważne awarie/ Drzewa zdarzeń dla instalacji





Zintegrowane podejście oparte na ryzyku (IRIDM)

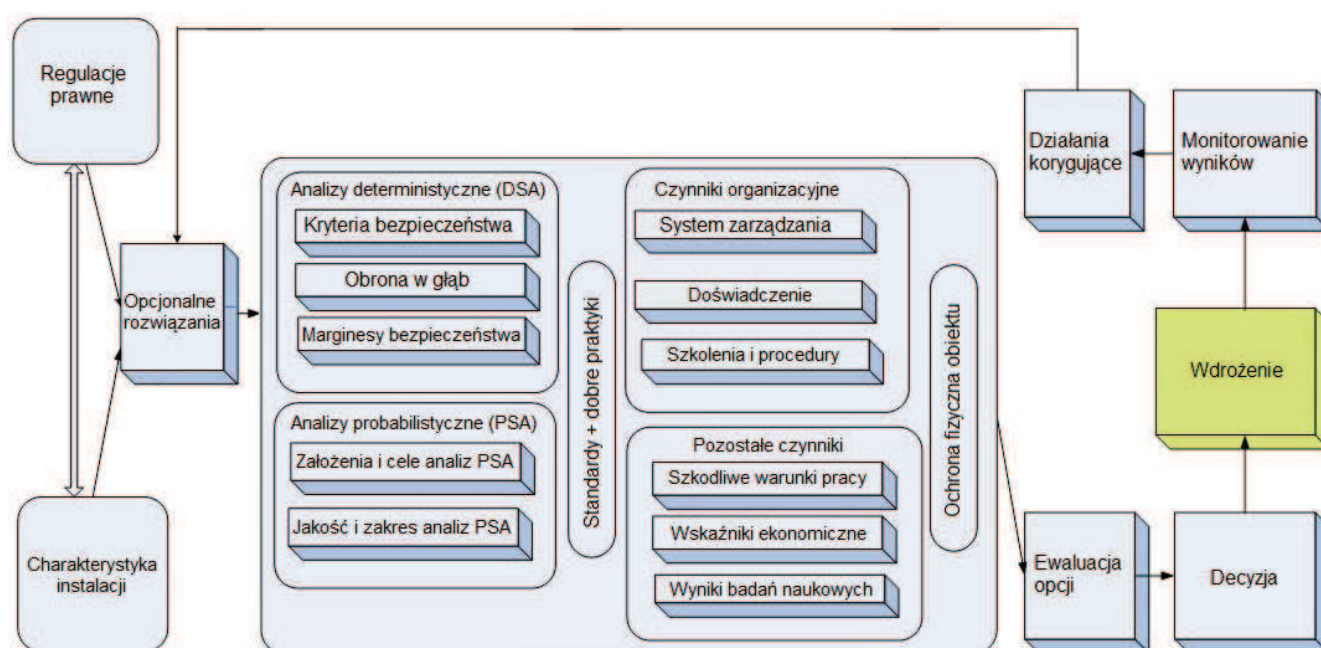
✓ Typowe elementy IRIDM

- Urządzenia instalacji i spec. techniczna
- Ograniczenia i warunki eksploatacji
- Okresowe kontrole jakości, audyty etc.
- Dopuszczalne stany instalacji
- Operacyjne procedury awaryjne
- Środki zarządzania stanami awaryjnymi

✓ Korzyści ze stosowania IRIDM

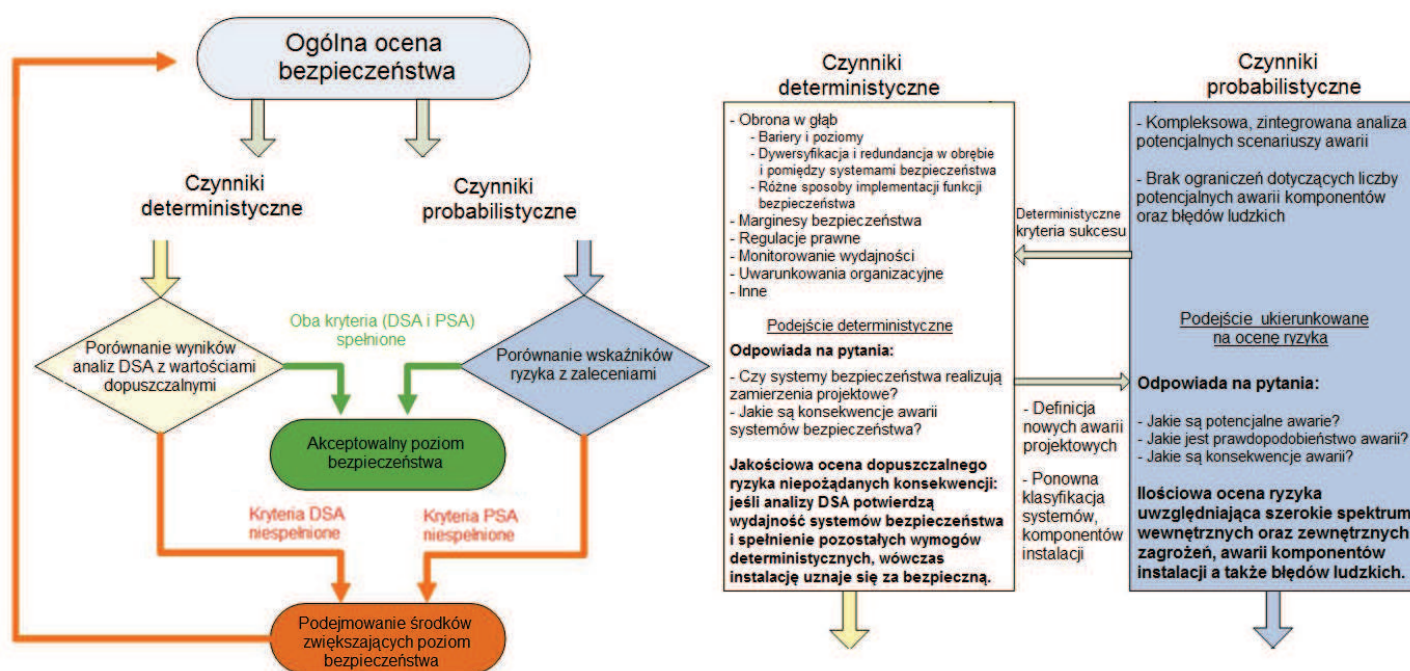
- **Transparentność** poprzez ustalenie wag elementów oraz poziomu szczegółowości
- **Zrównoważoność** gdy wagi elementów są określone właściwie
- **Logika** poprzez działanie strukturalne
- **Konsystentność** jeśli metodyka określania wag jest odpowiednio opracowana
- **Weryfikowalność** jeśli proces jest dobrze udokumentowany i może być zrekonstruowany

Podstawy i kluczowe elementy IRIDM



źródło: IAEA: A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, Vienna (2011)

Integracja podejścia deterministycznego i PSA



źródło: IAEA: A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, Vienna (2011)



Integracja podejścia DSA i PSA a problemy niepewności

✓ Podejście zintegrowane

- Ma jasną strukturę logiczną i uwzględnia doświadczenie ekspertów
- Uwzględnia negatywne efekty również poza rozważanym systemem
- Posiada przejrzyste zasady przypisywania wag poszczególnym elementom
- Jest weryfikowalne na podst. dokument.
- Możliwość łączenia różnych form danych wejściowych dla różnych elementów

✓ Problemy niepewności

- Wszystkie testy oparte na obliczeniach numerycznych mają szereg ograniczeń związanych z różnymi czynnikami
- Analizy niepewności zwiększają trafność oraz słuszność decyzji
- Wyniki numerycznych obliczeń powinny być rozważane nie jak wartości punktowe, lecz jako rozkłady prawdopodobieństw
- Z elementami jakościowymi również związane są niepewności



Typy niepewności w PSA (wymagające oddzielnej oceny)

✓ Stochastyczne (przypadkowość)

- Nie mogą być wyeliminowane ze względu na losowy charakter zdarzeń inicjujących oraz uszkodzeń komponentów instalacji
- Redukowane ze wzrostem doświadczenia eksploatacyjnego instalacji
- PSA jest bezpośrednim modelem procesów losowych, a więc modelem niepewności związanych ze statystyką
- Ocena na podstawie klasycznej analizy danych przy wyznaczaniu prawdopodobieństwa awarii

✓ Epistemologiczne (brak wiedzy)

- Powstają gdy stosuje się wnioskowanie statystyczne na podstawie danych lub wskutek niekompletnego opisu stanów instalacji technologicznych w modelu PSA
- Redukowane z postępem badań nauk.
- Określają stopień reprezentatywności oraz zasadność modelu PSA tzn.: jak dobrze model PSA odzwierciedla projekt i funkcje instalacji oraz jak dobrze prognozuje on odpowiedź instalacji lub systemu na awarie
- Wymagają wiedzy i oceny eksperckiej



Niepewności epistemologiczne w PSA (fundament IRIDM)

✓ Trzy typy epistemologiczne

- Niepewność wartości szacowanych parametrów
- Niepewność modelu szacowania prawdopodobieństwa zdarzeń
- Niepewność kompletności modelu

Identyfikacja, zrozumienie oraz uwzględnienie niepewności epistemologicznych stanowi fundament IRIDM

✓ Niepewność parametrów

- Niepewność parametrów jest związana z niepewnością ich wartości przy założeniu, że opis matematyczny modelu został uznany za prawidłowy
- Obecnie praktyką jest charakteryzowanie niepewności parametrów za pomocą rozkładów prawdopodobieństwa ich wartości
- Większość praktycznych projektów PSA jest ukierunkowana na oszacowanie niepewności parametrów



Niepewność modelu

✓ Przyczyny

- Brak konsensusu co do wyboru podejścia dla danej kwestii technologicznej
- Braku wiedzy jak zachowa się system w różnych warunkach awaryjnych
- Proces nie dostatecznie poznany
- Dane zbierane i stos. w innych warunkach
- Natura uszkodzeń jest niezrozumiała lub nieznana np. cyfrowy sprzęt kontrolny

✓ Uwagi

- Kiedy nie ma jasności który model powinien być użyty należy traktować to jako niepewność modelu
- Niepewność modelu nie dotyczy założeń, przybliżeń oraz aproksymacji. ponieważ zawsze można rozszerzyć model PSA w tym kierunku
- Brak zupełności modelu nie jest sam w sobie niepewnością, ale określeniem ograniczeń jego stosowania. Jednakże ma to wpływ na niepewność wyników, dlatego może być traktowane jako niepewność modelu



Niepewność kompletności

- Niepewność kompletności reprezentuje typ niepewności, który nie może być ujęty ilościowo, oraz te aspekty, które nie są uwzględnione w modelu, odzwierciedla te elementy niepewności, które są trudne lub niemożliwe do oszacowania
- ✓ **Niekompletność modelu powstaje w dwóch sytuacjach:**
 - Pewne efekty nie zostały świadomie wzięte pod uwagę z różnych powodów jak choćby fakt, że metody analizy dla tych efektów nie zostały opracowane (np. wpływ efektywności organizacyjnej na bezpieczeństwo instalacji nie może być wyznaczony explicite) lub też zasoby potrzebne do opracowania modelu kompletnego są niewystarczające, co prowadzi do pominięcia niektórych elementów
 - Pewne procesy/zjawiska lub mechanizmy uszkodzeń mogą być pominięte gdyż ich potencjalne istnienie nie zostało w ogóle zidentyfikowane



Dziękuję za uwagę