Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Inżynierii Mechanicznej i Mechatroniki

Zarządzanie bezpieczeństwem

Wykład 3 – analiza ryzyka

dr inż. Agnieszka Terelak-Tymczyna

Wybór podejścia do zarządzania ryzykiem

Przed rozpoczęciem czynności związanych z analizą ryzyka instytucja powinna mieć przygotowaną strategię dla tej analizy.

Wybór podejścia do zarządzania ryzykiem

Do analizy ryzyka można wybrać jedną z następujących strategii:

- **strategia podstawowego poziomu zabezpieczenia**
- **nieformalna analiza ryzyka**
- **szczegółowa analiza ryzyka**
- **strategia mieszana**

Wybór podejścia do zarządzania ryzykiem

Strategia podstawowego poziomu zabezpieczenia – w praktyce strategia ta polega na zastosowaniu standardowych zabezpieczeń we wszystkich systemach informatycznych bez względu na zagrożenia i znaczenie poszczególnych systemów dla podmiotu.

Wybór podejścia do zarządzania ryzykiem

Nieformalna analiza ryzyka – strategia ta opiera się na metodach strukturalnych, ale wykorzystuje wiedzę i doświadczenie ekspertów – podejście to może być skuteczne tylko w małych instytucjach.

Wybór podejścia do zarządzania ryzykiem

Szczegółowa analiza ryzyka – strategia ta wymaga dogłębnej identyfikacji i wyceny zasobów, analizy zagrożeń oraz podatności; wyniki tych działań stanowią podstawę do oszacowania ryzyka i wyboru zabezpieczeń.

Wybór podejścia do zarządzania ryzykiem

Strategia mieszana – strategia ta polega na przeprowadzeniu wstępnej analizy ryzyka w celu stwierdzenia, które systemy wymagają dalszej szczegółowej analizy ryzyka, a w których wystarczy podejście podstawowego poziomu. Stanowi kombinację podejścia podstawowego poziomu i szczegółowej analizy ryzyka.

Wybór podejścia do zarządzania ryzykiem

Warianty strategii stanowią cztery różne sposoby podejścia do analizy ryzyka. Jak z powyższej charakterystyki wynika, podstawową różnicę pomiędzy strategiami stanowi **stopień szczegółowości analizy ryzyka**.

Analiza ryzyka

Analiza ryzyka – czynności identyfikacji (środowiska, zagrożeń, podatności, potencjalnych strat) oraz oszacowania i oceny ryzyka

Ogólna procedura analizy ryzyka

Bezpieczeństwo a analiza ryzyka

Bezpieczeństwo wiąże się z ograniczeniem ryzyka, czyli wyeliminowaniem nieakceptowalnego ryzyka utraty życia lub zdrowia ludzkiego, bezpośrednio lub pośrednio, na wskutek wystąpienia zniszczeń w obiekcie lub w jego otoczeniu.

Bezpieczeństwo funkcjonalne – część bezpieczeństwa zależna od samego systemu lub poprawnego działania urządzenia i jest związane z właściwą odpowiedzią na pobudzenie jego wejść.

Bezpieczeństwo funkcjonalne

Przykład :

Czujnik w uzwojenie silnika, który wykrywa stan przegrzania i umożliwia wyłączenie silnika, zanim ulegnie on uszkodzeniu,

Bezpieczeństwo a analiza ryzyka

Bezpieczeństwo funkcjonalne powinno spełniać dwa rodzaje wymagań:

1. Na funkcje bezpieczeństwa, opracowane na podstawie wyników analizy hazardów o określające, co funkcje powinny realizować i w jaki sposób.
2. Na integralność, wypracowane na podstawie wyników szacowania ryzyka, a określających prawdopodobieństwo, że funkcja bezpieczeństwa zadziała niepoprawnie.

Identyfikacja i wycena wartości chronionych

Pierwszym etapem analizy ryzyka jest identyfikacja i wycena wartości chronionych. Warunkiem koniecznym, aby zbudować efektywny system zarządzania ryzykiem, jest **zidentyfikowanie aktywów narażonych na ryzyko** oraz ustalenie, jakiego rodzaju wartości mogą zostać utracone.

Aktywa organizacji są to wszelkie wartości materialne i niematerialne mające znaczenie dla osiągnięcia wyznaczonych celów organizacji.

Dla każdego rodzaju aktywów należy rozważyć, na czym polega ich wartość dla organizacji i które cechy aktywów powinny być chronione w warunkach ryzyka.

Identyfikacja zagrożeń

Aspekt ryzyka	Źródło ryzyka	
Techniczny	Własności fizyczne Własności materiałowe Własności radiacyjne Testowanie i modelowanie Integracja i interfejs Architektura oprogramowania Bezpieczeństwo	Zmiany wymogów Wykrywanie bledów Środowisko operacyjne Sprawdzone/niesprawdzone technologie Złożoność systemu Rzadkie lub specjalne zasoby
Programowy	Dostępność materiałów Dostępność personelu Umiejętność personelu Bezpieczeństwo Zabezpieczenia Wpływ środowiskowy Problemy komunikacyjne	Przerwy w pracy Zmiany wymogów Wsparcie polityczne Stabilność kontrahentów Struktura finansowania Zmiany regulacyjne

Identyfikacja zagrożeń

Aspekt ryzyka	Źródło ryzyka	
Obsługowy	Niezawodność i utrzymywalność Szkolenie i wsparcie szkolenia Sprzęt Kwestie dotyczące zasobów ludzkich Bezpieczeństwo systemu Dane techniczne	Udogodnienia Zgodność operacyjna Łatwość transportu Wsparcie zasobów informatycznych Pakowanie, przeładunek, przechowywanie
Kosztowy	Wrażliwość na ryzyko - Techniczne - Programowe - Obsługowe	Wrażliwość na ryzyko harmonogramowe Wielkość kosztów ogólnych i kosztów ogólnego zarządu Błąd szacowania
Harmonogramowy	Wrażliwość na ryzyko - Techniczne - Programowe - Obsługowe	Wrażliwość na ryzyko kosztowe Stopień równoczesności Liczba elementów tworzących ścieżkę krytyczną Błąd szacowania

Przykład

Pewna maszyna ma niebezpieczne wirujące ostrze, osłonięte pokrywą umocowaną na zawiasach, która musi być odchylana podczas konserwacji urządzenia. Podniesienie pokrywy powinno wyleczyć napęd, zanim dojdzie do zranienia operatora.

Podczas analizy hazardu zidentyfikowano hazard towarzyszący czyszczeniu ostrza. Należy zapewnić by uniesienie pokrywy o wyżej niż 5 mm doprowadzało do wyłączenia napędu i zadziałania hamulca. Ponadto wyznaczono czas hamowania - 1 s. W ten sposób powstała specyfikacja funkcji bezpieczeństwa, czyli pewnego elementu automatyki wbudowanego do systemu, który w ciągu 1 s od uniesienia pokrywy na wysokość 5 mm ma zatrzymać maszynę.

Oszacowanie ryzyka sprowadza sic do oceny skuteczności funkcji bezpieczeństwa. Jego celem jest uzyskanie przekonania, ze zachowanie integralności funk j i bezpieczeństwa jest wystarczające, by nikt nie był narażany na nieakceptowalne ryzyko podczas konserwacji maszyny, wynikające z istnienia hazardu.

Szkodą może tu być zranienie ręki operatora, a nawet jej utrata. W tym wypadku wielkość ryzyka zależy takie od częstości prowadzenia prac konserwacyjnych. Wymagany w tym przypadku poziom integralności SIL zależy od rodzaju uszkodzenia i częstości, z jaką operator jest w ten sposób narażany.

Czynniki zagrożeń

1. Zależne od konstruktora:
   - Błędy w specyfikacjach systemu, sprzętu , oprogramowania;
   - Niekompletne specyfikacje bezpieczeństwa, np. nie uwzględnienie pewnych trybów pracy.

2. Sprawcze:
   - Błąd ludzki
   - Przypadkowe uszkodzenie sprzętowe
   - Błąd oprogramowania
   - Wahania zasilania
   - Zjawiska zachodzące w środowisku (zakłącenia elektromagnetyczne, przegrzanie itp.)

Ocena ryzyka

Metody oceny ryzyka:

1. **ilościowa**, gdzie oszacowanie wartości ryzyka wiąże się z wykorzystaniem miar liczbowych – wartość zasobów informacyjnych jest określana kwotowo, częstotliwość wystąpienia zagrożenia liczbą przypadków, a podatność wartością prawdopodobieństwa ich utraty,

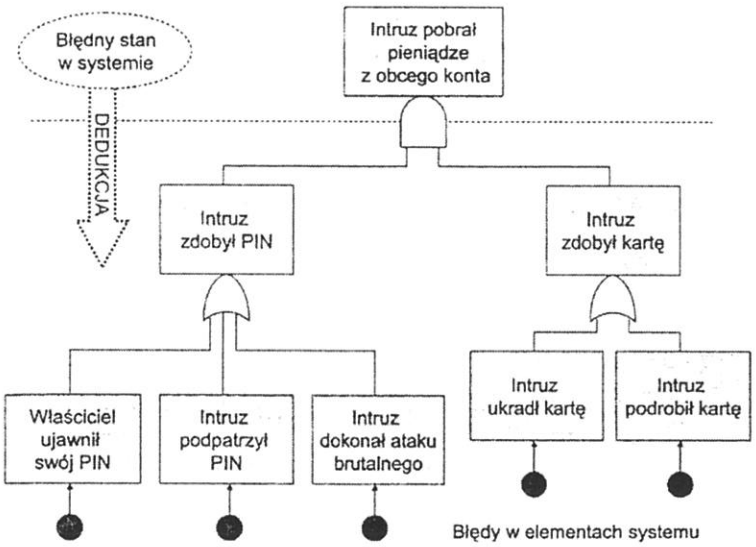
2. **jakościowa**, gdzie oszacowanie wartości ryzyka wiąże się z:
   - opisem jakościowym wartości aktywów, określeniem skal jakościowych dla częstotliwości wystąpienia zagrożeń i podatności na dane zagrożenie, albo
   - opisem tzw. scenariuszy zagrożeń[1] poprzez przewidywanie głównych czynników ryzyka, które powodują i wskazują, w jaki sposób system kontroli wewnętrznej może zostać ominięty przez oszustwo lub nieszczęśliwy wypadek.

Ocena ryzyka

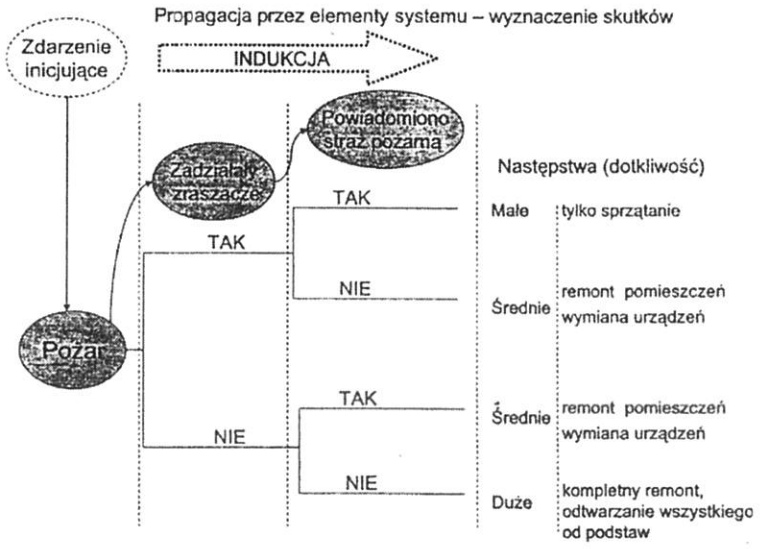
Metody jakościowe oceny ryzyka:

1. Metoda wstępnej analizy ryzyka i hazardu
2. Metoda FMEA
3. Metoda drzewa błędów FTA
4. Metoda drzewa zdarzeń ETA
5. Analiza przyczynowo-skutkowa

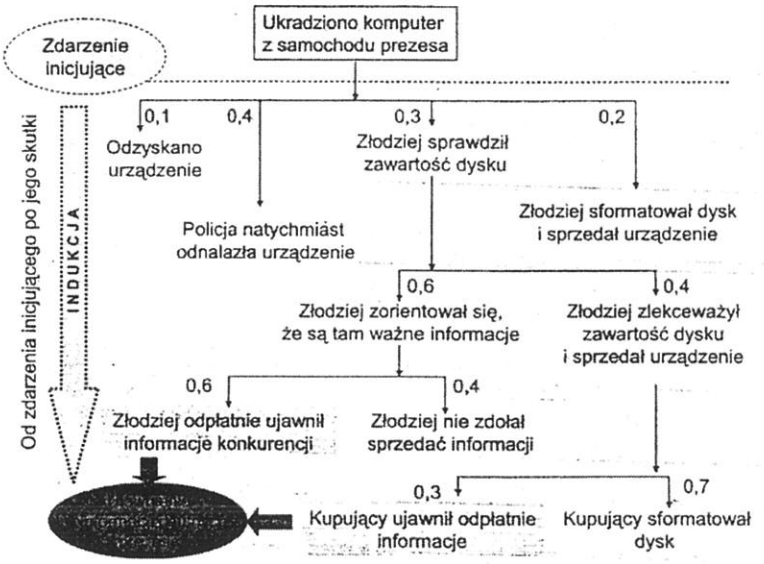
Przykład FTA



Przykład ETA



Przykład ETA



Przykład analizy przyczynowo-skutkowej