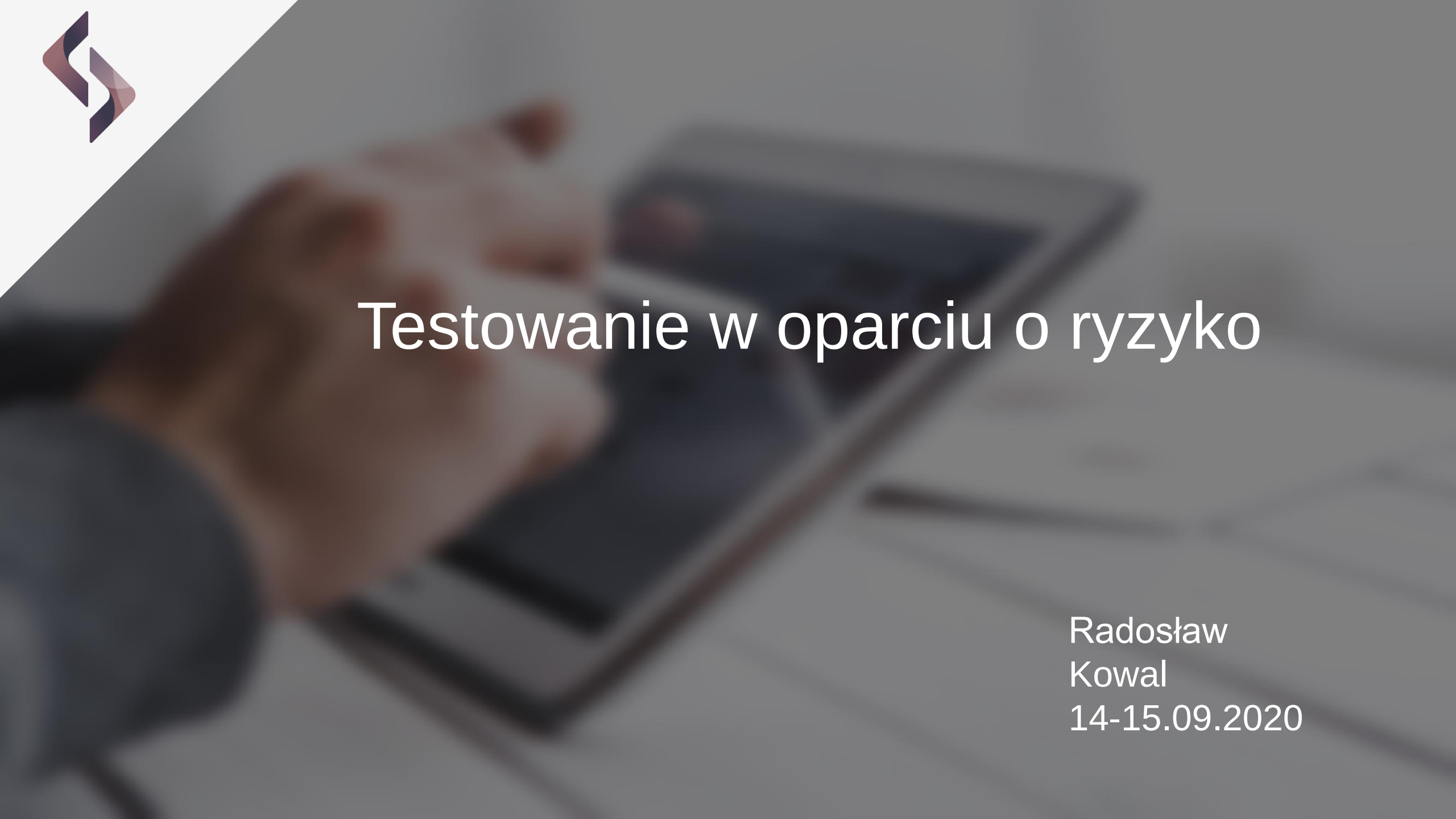


Testowanie w oparciu o ryzyko

Radosław
Kowal
14-15.09.2020

Co to takiego?

Ryzyko wg Was…

Ryzyko

Termin ryzyko (*ang.risk*) wywodzi się z języka włoskiego (*wł. Risico*), w którym oznacza przede wszystkim przedsięwzięcie, którego wynik jest nieznany albo niepewny, lub możliwość, że coś się uda albo nie uda.

Ryzyko wg ISTQB

Ryzyko jest możliwością wystąpienia w przyszłości zdarzenia o niepożądanych konsekwencjach. O poziomie ryzyka decyduje prawdopodobieństwo wystąpienia niekorzystnego zdarzenia oraz jego wpływ (tj. wynikające z niego szkody).

Ryzyko wg PMBoK

Ryzyko to prawdopodobieństwo wystąpienia sytuacji, która może oddziaływać na dalszy przebieg projektu — jego jakość, zakres, koszty i/lub harmonogram. Istotne jest, że wpływ ten może być zarówno pozytywny, jak i negatywny, ponadto może wpływać pozytywnie na jeden a negatywnie na inny obszar tego samego projektu. Charakterystycznym dla ryzyka jest możliwość oszacowania prawdopodobieństwa jego wystąpienia oraz siły oddziaływania na projekt.

Ryzyko wg PRINCE2

Ryzyko jest zdarzeniem lub ich zbiorem, które w sytuacji wystąpienia mogą mieć wpływ na osiągnięcie celów projektu. Oznacza ono wprost niepewność wyniku. Metodyka PRINCE2 rozróżnia dwa typy ryzyka:

Zagrożenie — prawdopodobne zdarzenie mające negatywny wpływ na realizację celów.

Szansa/okazja — prawdopodobne zdarzenie, mające pozytywny wpływ na realizację założonych celów

Ryzyko w projekcie

Ryzyko można definiować jako przypadek, niebezpieczeństwo, możliwość lub sytuację występującą w projekcie z niepożądanymi konsekwencjami — potencjalny problem.
Poziom ryzyka będzie określony prawdopodobieństwem wystąpienia zdarzenia i jego wpływem.

Najważniejsze cechy ryzyka

Ryzyko istnieje, kiedy istnieje prawdopodobieństwo wystąpienia problemu, który może pogorszyć zdanie klienta, użytkownika, uczestnika lub interesariusza o jakości produktu, lub sukcesie projektu.

Ryzyko może, ale nie musi wystąpić – niepewność.

Zazwyczaj prawdopodobieństwo wystąpienia ryzyka jest trudne do oszacowania, a tym bardziej do przedstawienia go w miarach ilościowych.

Zazwyczaj używa się miar jakościowych, a nie ilościowych (znikome, duże itp.).

Najważniejsze cechy ryzyka

Przy wystąpieniu ryzyka mogą być odczuwalne jego konsekwencje.

Wystąpienie ryzyka generuje dodatkowe koszty.

Aby uniknąć niekorzystnych skutków oraz dodatkowych kosztów, należy zapobiegać ryzykom.

Prawdopodobieństwo wystąpienia awarii

Można wyróżnić kilka czynników, które mają wpływ na wystąpienie awarii w czasie eksploatacji oprogramowania:

- Złożone funkcjonalności składające się z dużej ilości modułów.
- Częste zmiany kodu w różnych obszarach systemu.
- Niska jakość analizy w czasie projektowania systemu.
- Niska jakość wymagań, dostarczonych do zespołu deweloperskiego.

Prawdopodobieństwo wystąpienia awarii

- Duża ilość osób zaangażowanych w projekt.
- Presja czasu.
- Ograniczone zasoby ludzkie oraz sprzętowe.

Prawdopodobieństwo wystąpienia awarii w oprogramowaniu jest czynnikiem indywidualnym, zależy od konkretnej implementacji. Stąd lista może być krótsza bądź dłuższa.

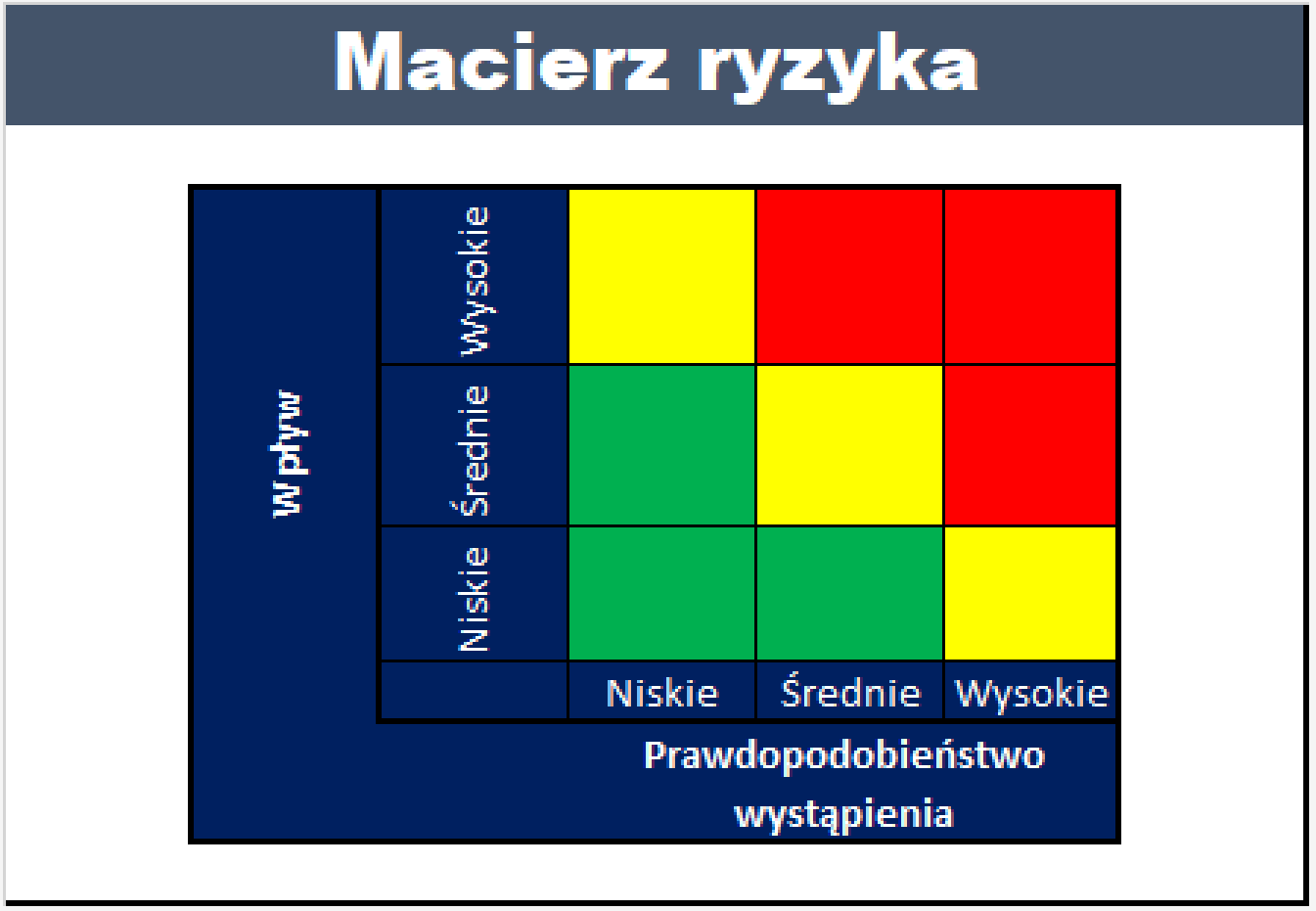
Poziom ryzyka

Prawdopodobieństwo wystąpienia awarii można spróbować oszacować przy pomocy poziomu ryzyka. Wykorzystuje się do tego trzy czynniki:
Poziom ryzyka (*ang. risk level*)
Wpływ ryzyka (*ang. risk impact*)
Prawdopodobieństwo ryzyka (*ang. risk likelihood*)

Poziom ryzyka

poziom ryzyka = prawdopodobieństwo zdarzenia * wpływ zdarzenia

Poziom ryzyka



Prawdopodobieństwo oraz wpływ

Prawdopodobieństwa wystąpienia ryzyka oraz jego wpływ:

A – niskie prawdopodobieństwo, niski wpływ

B – mało prawdopodobne, duży wpływ

C – średnie prawdopodobieństwo, średni wpływ

D – wysokie prawdopodobieństwo wystąpienia, duży wpływ

E – wysokie prawdopodobieństwo wystąpienia, niski wpływ

F – najwyższe prawdopodobieństwo wystapienia, najwyższy wpływ

Priorytety od najwyższego do najniższego:

F > D > B > C > E > A

Zalety testowania opartego na ryzyku

- Wszystkie czynności procesu testowego (**planowanie, analiza, monitorowanie**) są odnoszone do poziomu ryzyka.
- Koncentruje się na pytaniu, co może pójść źle, jeśli nastąpi awaria.
- Konieczne jest ustalenie możliwych ryzyk – rodzajów awarii oraz przeanalizowania wpływu ich pojawienia się.

Zalety testowania opartego na ryzyku

- Testowanie weryfikuje, czy poszczególne ryzyka naprawdę istnieją w systemie, czy też nie. Gdy test wykonał się z wynikiem pozytywnym — oznacza to, że ryzyko związane z tym testem nie istnieje lub jego wystapienie jest bardzo mało prawdopodobne.
- Im więcej testów pokrywa dany obszar ryzyka, tym wzrasta przekonanie o tym, że ryzyko nie stanowi już takiego zagrożenia.
- Priorytetyzacja testów – ryzyka — optymalizujemy naszą pracę pod kątem dostępnych zasobów oraz czasu.

Ryzyko projektowe

Czynniki dostawcy:

- niemożność dostarczenia produktu/podzespołu przez zewnętrzną grupę;
- czynniki kontraktowe

Ryzyko projektowe

Czynniki organizacyjne:

- brak umiejętności i ludzi
- czynniki osobiste i treningi
- czynniki polityczne
- niepoprawny odbiór lub oczekiwania względem testowania

Ryzyko projektowe

Czynniki techniczne:

- problem ze zdefiniowaniem właściwych wymagań
- zakres wymagań
- jakość projektów, kodu i testów

Ryzyko produktowe

Potencjalne obszary występowania awarii (powodujące przyszłe niebezpieczeństwa) w oprogramowaniu lub systemie nazywane są ryzykiem produktu, gdyż są ryzykiem w odniesieniu do jakości produktu.

Ryzyko produktowe

Wyróżniamy następujące ryzyko produktu:

- oprogramowanie dostarczone na rynek zawierające defekty powodujące awarie
- potencjalne zagrożenia zranienia osoby lub wprowadzenie niebezpieczeństwa uszkodzeń wewnątrz organizacji
- słabe parametry oprogramowania (np. funkcjonalność, bezpieczeństwo, niezawodność, użyteczność i wydajność)
- oprogramowanie, które nie zachowuje się tak jak powinno

Ryzyko produktowe

Wyróżniamy następujące ryzyko produktu:

- oprogramowanie dostarczone na rynek zawierające defekty powodujące awarie
- potencjalne zagrożenia zranienia osoby lub wprowadzenie niebezpieczeństwa uszkodzeń wewnątrz organizacji
- słabe parametry oprogramowania (np. funkcjonalność, bezpieczeństwo, niezawodność, użyteczność i wydajność)
- oprogramowanie, które nie zachowuje się tak jak powinno

Testowanie a ryzyko

Testowanie uwzględnia ryzyko na trzy następujące sposoby:
Testowanie ukierunkowane (*ang. targeted testing*)
Priorytetyzacja (*ang. prioriterized testing*)
Raportowanie (*ang. reporting*)
Powyższe zdarzenia powinny występować podczas całego cyklu wytwarzania oprogramowania.

Tester a ryzyko

- Właścicielem ryzyka zawsze jest biznes, a nie zespół deweloperski.
- Biznes decyduje o akceptacji aktualnego poziomu ryzyka i jest zainteresowany, aby był na jak najniższym poziomie.
- Testerzy zapewniają obiektywne informacje interesariuszom biznesowym, właścicielowi produktu na temat poziomu ryzyka.
- Tester nie jest osobą decyzyjną, ale jego zadania powinny uwzględniać poziom dopuszczalnego ryzyka.

Ryzyko w testowaniu

Pojęcia ryzyka używa się dla zdecydowania gdzie zacząć testowanie i gdzie przetestować bardziej dogłębnie

Etapy rozpoznania ryzyka:

➔Identyfikacja ryzyk

➔Szacowanie wpływu ryzyk na projekt – ocena ryzyka

➔Plany redukujące ryzyka – łagodzenie ryzyka

➔Plany „B” – zarządzanie ryzykiem

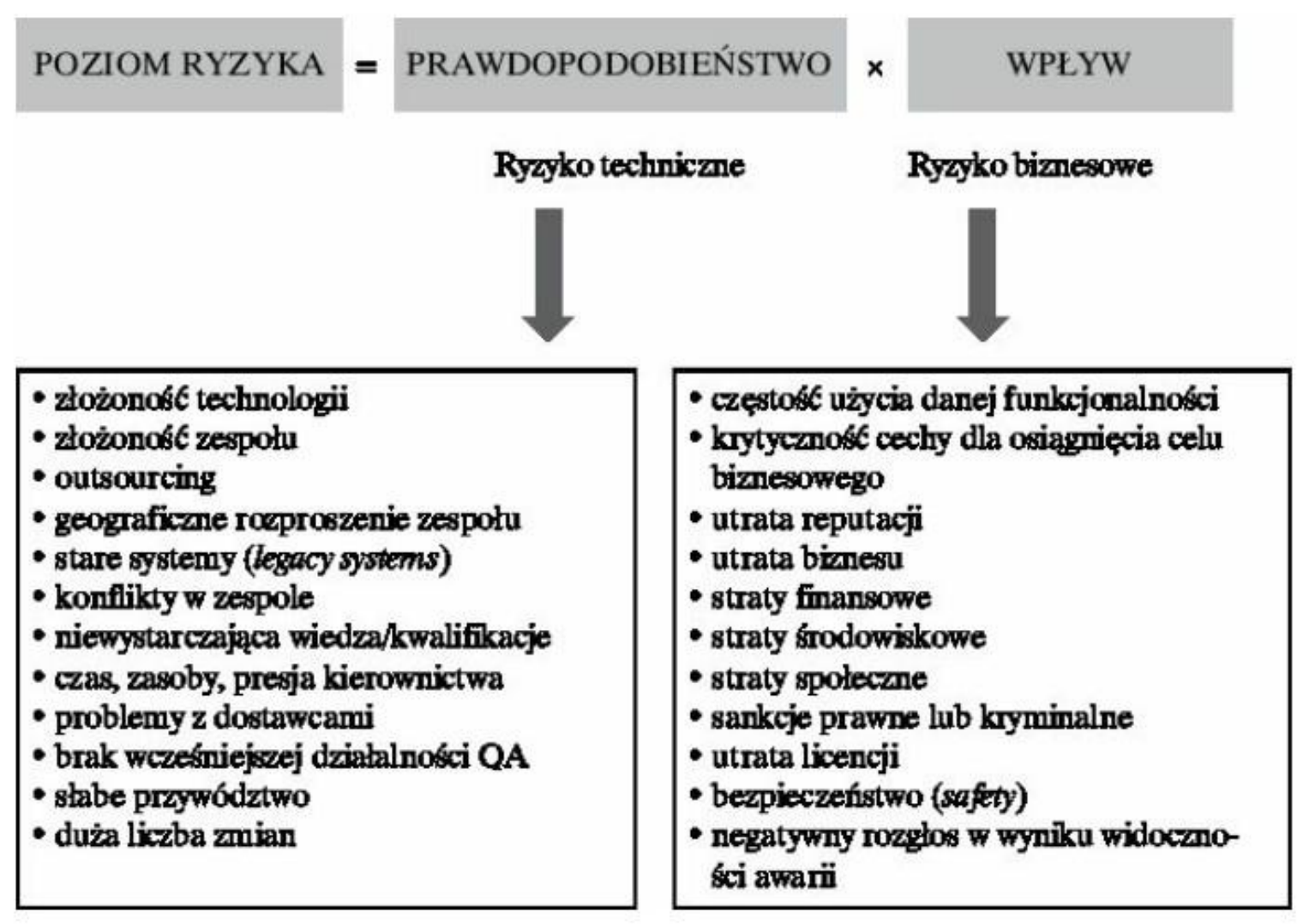
➔Wszystkie czynności testowe odnosimy do poziomu ryzyka

Ryzyko w testowaniu

Techniki identyfikacji:

- Rozmowy z ekspertami
- Niezależne oceny
- Wykorzystanie szablonów ryzyka
- Retrospektywy projektu
- Warsztaty dotyczące ryzyka
- Burza mózgów
- Listy kontrolne
- Odwołanie się do przeszłego doświadczenia

Ryzyko w testowaniu – ocena ryzyka



Ryzyko w testowaniu - łagodzenie

Łagodzenie ryzyka to proces, w którym podejmuje się decyzje i implementuje metryki w celu redukcji ryzyka lub utrzymania go na określonym poziomie.
Istnieją cztery główne sposoby łagodzenia ryzyka:
łagodzenie ryzyka (ang. risk mitigation) przez przedsięwzięcie czynności prewencyjnych, zapobiegających pojawieniu się ryzyka lub zmniejszających ich ewentualną dotkliwość;
plany awaryjne (ang. contingency plans) mające na celu zredukować siłę oddziaływania ryzyka, które rzeczywiście nastąpi;
transfer ryzyka (ang. risk transfer), czyli przeniesienie ryzyka na stronę trzecią (np. ubezpieczyciela), który będzie ponosił skutki ewentualnego wystąpienia ryzyka;
zignorowanie i zaakceptowanie ryzyka, które polega po prostu na tym, że nie podejmuje się żadnych akcji do momentu wystąpienia tego ryzyka.

Ryzyko w testowaniu – łagodzenie przez testowanie

Wykrywanie awarii pozwala na usunięcie defektu (potencjalnego źródła ryzyka)
Wykonanie testów daje nam informację o prawdopodobieństwie wystąpienia ryzyka
Poziom ryzyka wyznacza zakres i dokładność testowania

Jak testerzy mogą łagodzić ryzyko?

- priorytetyzacja testów według poziomu ryzyka; wykorzystywanie umiejętności najbardziej doświadczonych osób;
- wybór odpowiednich technik projektowania testów; przeprowadzanie szkoleń z testowania czy tworzenia testowalnego kodu o wysokiej jakości;
- przeprowadzanie przeglądów i inspekcji;
- przeprowadzanie przeglądów projektów testów;
- zdefiniowanie zakresu i intensywności testów regresji;
- stosowanie wczesnego prototypowania;
- automatyzowanie projektowania i wykonywania testów;
- uzyskanie określonego poziomu niezależności;

Ryzyko w testowaniu – łagodzenie przez testowanie

- Zarządzamy przez cały cykl życia projektu
- Sprawdzamy czy proces redukcji ryzyka przebiega prawidłowo
- Raportujemy, zgłaszamy do kierownictwa – podstawa decyzji o kolejnej fazie projektu oraz archiwizujemy dane

W związku z postępem projektu, lista ryzyk powinna być okresowo przeglądana i kierownik testów powinien dla każdego ryzyka produktowego przedyskutować następujące kwestie:

- czy dane ryzyko zostało prawidłowo oszacowane?
- czy czynności łagodzenia ryzyka (np. wykonanie testów) zostały
- przeprowadzone?
- jakie są efekty czynności łagodzących ryzyko (np. wyniki testów)?
- czy w stosunku do danego ryzyka należy przeprowadzić dodatkowe
- czynności, np. więcej testów?
- czy można dane ryzyko usunąć z listy ryzyk?
- Dodanie nowych ryzyk do listy

Identyfikacja ryzyka

Techniki testowania opartego na ryzyku

Techniki Lekkie

Minimalizacja kosztów
Szybkość reakcji
Elastyczność
Np: PRAM, SST, PrisMa

Techniki formalne i ciężkie

Wykorzystują więcej czynników
Bardziej złożone oceny jakościowe i skale
Np: FMEA, SQF, FTA

Techniki testowania opartego na ryzyku – wybór technik

Podczas wyboru odpowiedniej techniki powinniśmy wziąć pod uwagę:

- dostępność zasobów oraz kwalifikacje personelu – niektóre metody wymagają doświadczenia w ich stosowaniu;
- czas poświęcony na wdrożenie oraz stosowanie metody;
- koszt (np. dodatkowe szkolenia czy koszt wynikający z czasu, jaki
- członkowie zespołu poświęcają na wykonywanie czynności
- wymaganych przez metodę);
- dostępność wymaganych przez metodę danych

Techniki testowania opartego na ryzyku – Analiza SWOT

Analiza SWOT to jedna z metod analitycznych przedsiębiorstwa. Cechuje ją prostota i szybkość zastosowania.
SWOT to w rzeczywistości akronim angielskich słów:
- **S** jak strengths – mocne strony
- **W** jak weaknesses – słabe strony
- **O** jak opportunities – szanse
- **T** jak threats – zagrożenia

Analiza SWOT to analiza mocnych i słabych stron oraz szans i zagrożeń przedsiębiorstwa.

Techniki testowania opartego na ryzyku – Analiza SWOT

Mocne strony to pozytywne czynniki wewnętrzne. Stanowią o wewnętrznej sile firmy. Należy o nie dbać, aby utrzymać je również w przyszłości. Mogą zostać wykorzystane do działań związanych z ekspansją firmy. Przykłady mocnych stron to:

•Wysokie kwalifikacje zatrudnionych pracowników
•Ponadprzeciętnie dobrze zorganizowana praca firmy (np. poprawnie wdrożone metodologie zarządzania)
•Duże zasoby finansowe zgromadzone w przeszłości

Słabe strony to negatywne czynniki wewnętrzne. Należy skupić się na ich eliminacji, aby nie osłabiły mocnych stron. Ograniczają one bowiem sprawność przedsiębiorstwa i hamują jego rozwój. Przykłady słabych stron to:

•Ograniczony proces produkcyjny, wpływający na niską jakość produktu
•Przestarzałe, awaryjne maszyny, które doprowadzają do przestoju w produkcji
•Duża rotacja pracowników

Techniki testowania opartego na ryzyku – Analiza SWOT

Techniki testowania opartego na ryzyku – FMEA

Failure Mode and Effect Analysis

Analiza przyczyn i skutków awarii
Rozpoznanie i ocena potencjalnych awarii systemu oraz ich wpływu
Analiza od najniższego poziomu (detali) – metoda typu bottom-up

Pozwala odpowiedzieć na pytanie

Co może ulec awarii?
W jaki sposób może to ulec awarii?
Jak często będzie ulegało awarii?
Jakie są konsekwencje awarii?
Jak awaria wpływa na niezawodność/bezpieczeństwo systemu?

Techniki testowania opartego na ryzyku – kroki FMEA

Failure Mode and Effect Analysis

- Zdefiniowanie analizowanego systemu
- Zdefiniowanie możliwych typów awarii oraz oszacowanie ich częstotliwości
- Analiza systemu (identyfikacja potencjalnych przyczyn awarii oraz działań korekcyjnych)
- Identyfikacja metod detekcji awarii oraz działań korekcyjnych, naprawczych lub prewencyjnych
- Określenie przyczyn awarii, ich konsekwencji, lista zagrożeń i ryzyk

Techniki testowania opartego na ryzyku – tabela FMEA

FMEA przeprowadzana jest zwykle przy użyciu arkusza kalkulacyjnego, w którym uzupełnia się tabelę FMEA. Istnieje wiele różnych wersji takiej tabeli, które różnią się poziomem szczegółowości niektórych informacji. Przykładowa tabela może zawierać następujące informacje:

- nazwa funkcji, w której może wystąpić awaria;
- możliwa awaria (ryzyko produktowe);
- możliwa przyczyna awarii;
- konsekwencje awarii;
- Pr. – prawdopodobieństwo wystąpienia awarii (ang. likelihood);
- W. – wpływ;
- Dotkl. – dotkliwość (ang. severity); w niektórych wersjach FMEA ten parametr się pomija;
- RPN – priorytet ryzyka (ang. Risk Priority Number), definiowany jako
- iloczyn: RPN = Pr · W · Dotkl;
- metoda wykrywania i zalecane czynności.

Techniki testowania opartego na ryzyku – PRISMA

Product Risk Managment

- Lekka

- Prosta

- Macierz ryzyka produktowego – jasna informacja dla interesariuszy

- Ryzyko jest charakteryzowane prawdopodobieństwem i wpływem (nie połączone ze sobą)

Techniki testowania opartego na ryzyku – PRISMA

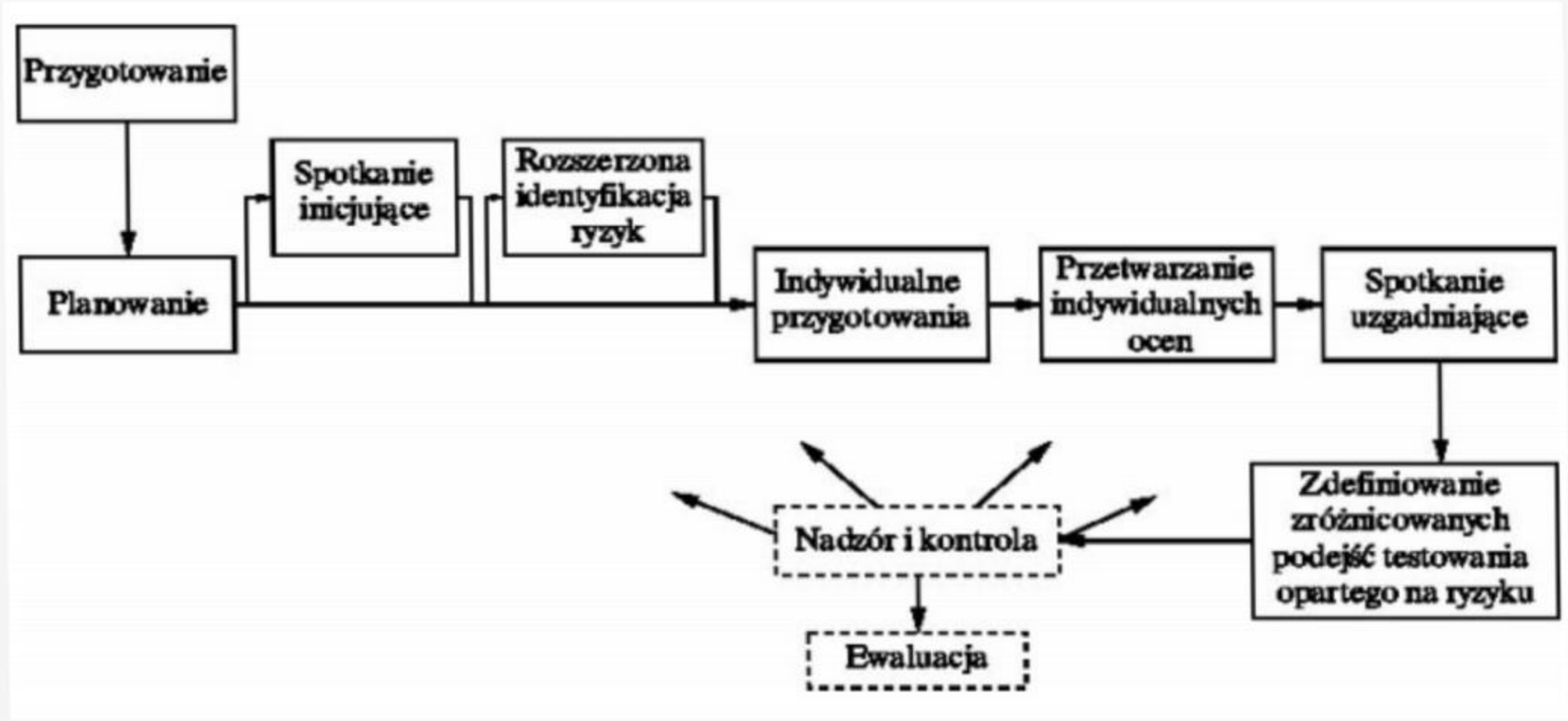
Czynniki dla wpływu:

- obszary krytyczne (identyfikowane na podstawie analizy użycia systemu oraz tego, w jaki sposób system może ulec awarii);
- obszary widoczne (czyli takie, w których użytkownicy mogą bezpośrednio odczuć awarię, jeśli coś pójdzie nie tak, jak trzeba);
- najczęściej używane obszary (podział funkcji na te, których użytkownicy używają zawsze, często, okazjonalnie lub rzadko i oszacowanie wpływu na podstawie tej klasyfikacji);
- istotność z biznesowego punktu widzenia (tzn. jaka jest ważność poszczególnych cech systemuunktu widzenia biznesowego celu jego działania);
- koszt zmian (zwykle wykorzystywany w tzw. systemach systemów).

Czynniki dla prawdopodobieństwa:

- złożoność (np. w sensie złożoności cyklomatycznej, skomplikowanej logiki);
- liczba zmian (jest ona ważnym czynnikiem defektotwórczym);
- nowe technologie i metody;
- presja czasu;
- brak doświadczenia;
- rozproszenie geograficzne zespołu;
- kod nowy vs. re-używalny;
- interfejsy
- rozmiar
- historia defektów
- jakość wymagań

Techniki testowania opartego na ryzyku – PRISMA



Techniki testowania opartego na ryzyku – PRISMA

Faza planowania:

- Określenie interesariuszy i przypisanie czynników:
- Kierownik projektu: widoczne obszary, istotność biznesowa, złożoność, nowe technologie
- Analityk biznesowy: widoczne obszary, istotność biznesowa
- Analityk systemu: złożoność, nowe technologie

Zidentyfikowano ryzyka:

- brak komunikacji systemu z ekranem
- niepoprawność wyświetlanych wyników na ekranie;
- niewygodny interfejs użytkownika;
- błędy w logice biznesowej systemu (zarządzanie liniami i kursami);
- wolne działanie systemu.

Techniki testowania opartego na ryzyku – PRISMA

Faza indywidualnego przygotowania
Analiza ryzyk przez członków zespołu, przykład dla kierownika projektu:

Kierownik projektu	Wpływ		Prawdopodobieństwo	
Czynniki	**WidOb**	**IstBiz**	**Złoż**	**NTech**
Wagi	**1,0**	**2,0**	**1,0**	**2,0**
R1: brak komunikacji z ekranem	4	5	1	5
R2: niepoprawna informacja na ekranie	5	5	3	1
R3: niewygodny interfejs	2	1	1	2
R4: błędy w logice biznesowej	1	3	5	4
R5: wolne działanie systemu	2	4	4	4

Techniki testowania opartego na ryzyku – PRISMA

Faza przetwarzania indywidualnych ocen Kierownik testów uśrednia oceny:

Uśrednione oceny	Wpływ		Prawdopodobieństwo	
Czynniki	**WidOb**	**IstBiz**	**Złoż**	**NTech**
Wagi	**1,0**	**2,0**	**1,0**	**2,0**
R1: brak komunikacji z ekranem	4,5	4,0	2,0	5,0
R2: niepoprawna informacja na ekranie	5,0	5,0	4,0	1,0
R3: niewygodny interfejs	1,5	1,0	1,0	1,5
R4: błędy w logice biznesowej	2,0	2,5	4,5	4,0
R5: wolne działanie systemu	3,0	3,5	2,5	3,5

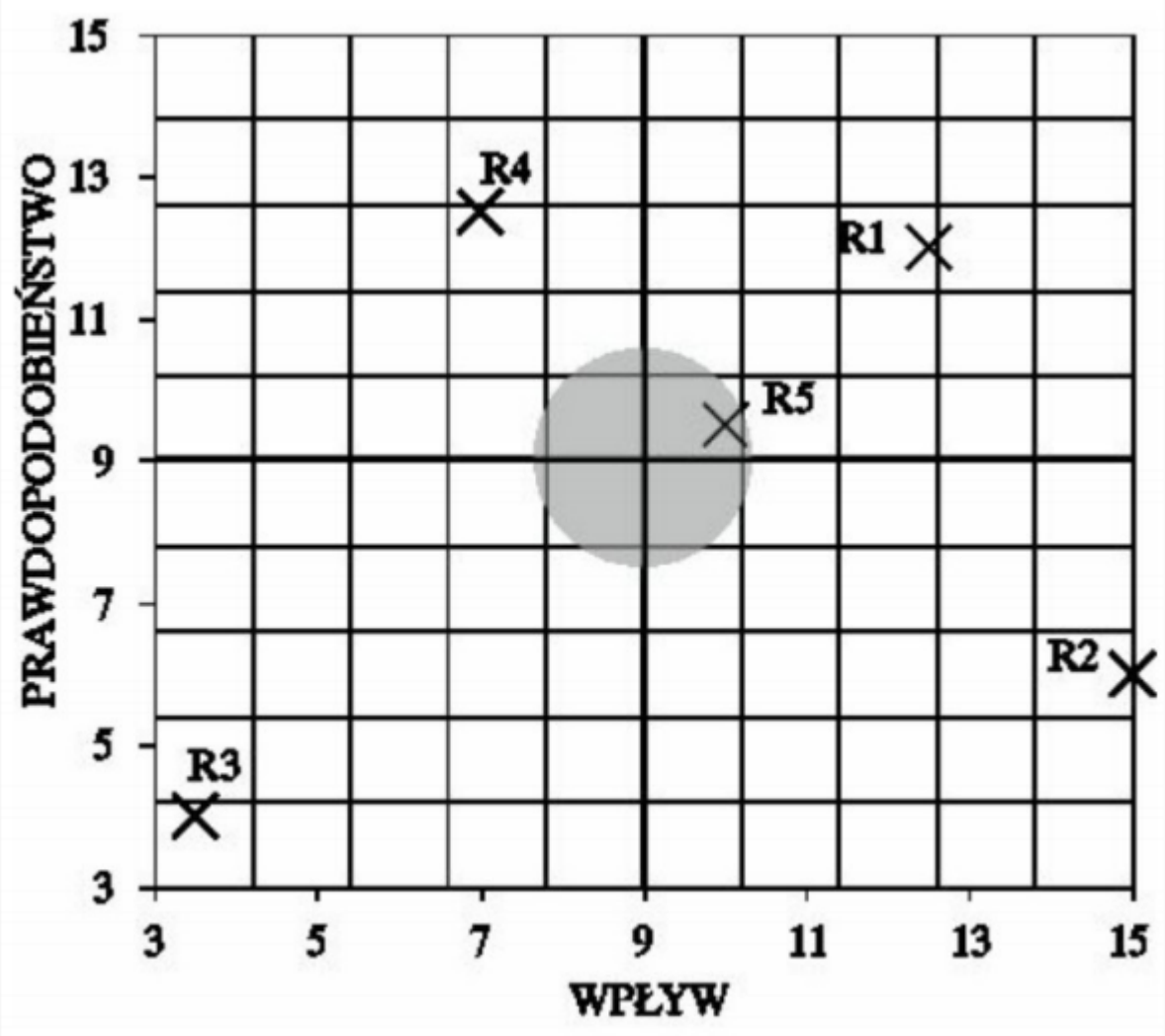
Techniki testowania opartego na ryzyku – PRISMA

Faza przetwarzania indywidualnych ocen Liczymy ważoną ocenę:

Ryzyko	Wpływ	Prawdopodobieństwo
R1: brak komunikacji z ekranem	4,5+8,0=12,5	2,0+10,0=12,0
R2: niepoprawna informacja na ekranie	5,0+10,0=15,0	4,0+2,0=6,0
R3: niewygodny interfejs	1,5+2,0=3,5	1,0+3,0=4,0
R4: Błędy w logice biznesowej	2,0+5,0=7,0	4,5+8,0=12,5
R5: Wolne działanie systemu	3,0+7,0=10,0	2,5+7,0=9,5

Techniki testowania opartego na ryzyku – PRISMA

Macierz ryzyka produktowego:



Techniki testowania opartego na ryzyku – PRISMA

Metody łagodzenia ryzyka:

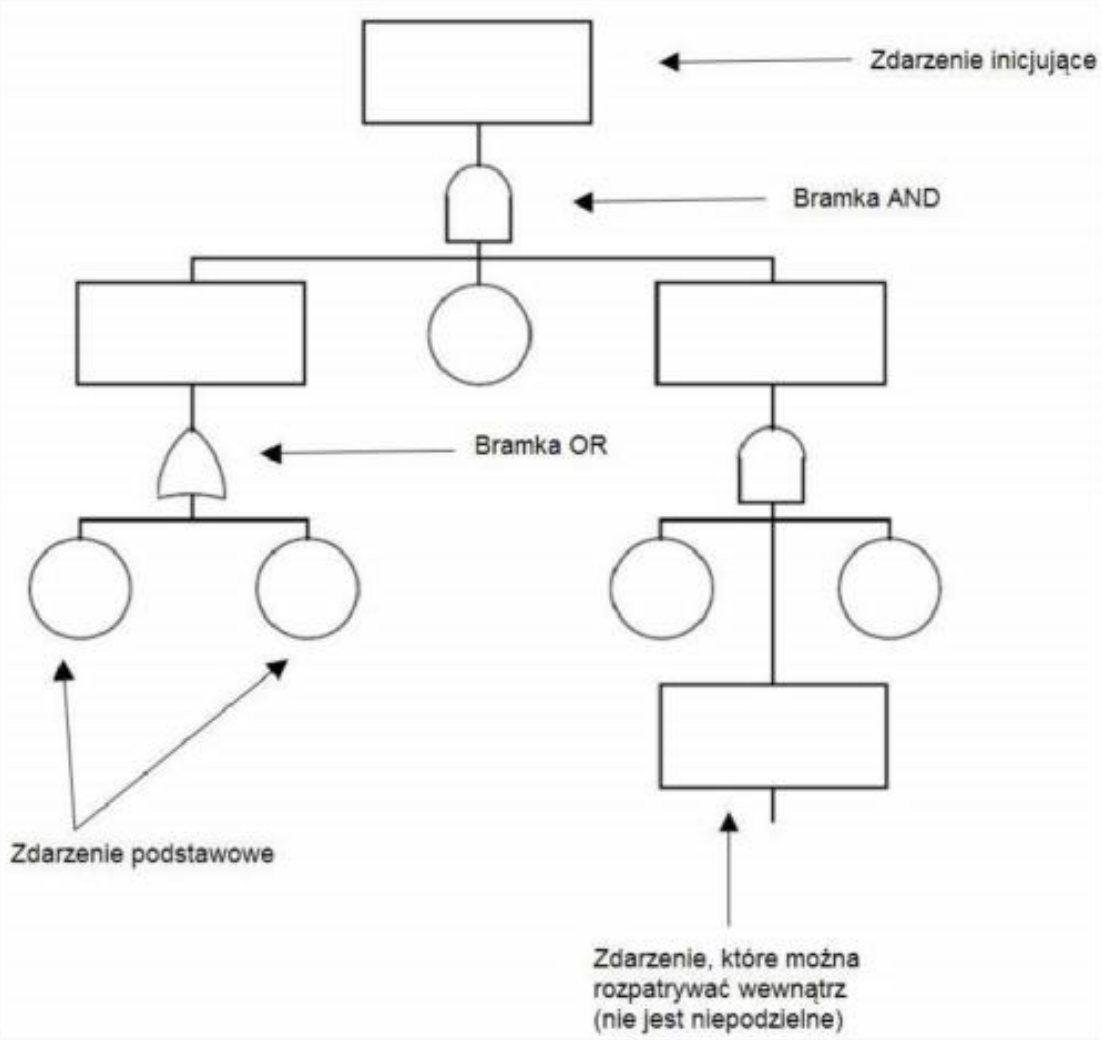
Ryzyko	Kwadrant	Wpływ	Prawdopodobieństwo	Metody łagodzenia
R1	II	wysoki	wysokie	wczesny prototyp systemu sprawdzający połączenie z ekranem
R2	IV	wysoki	niskie	testowanie białoskrzynkowe (kryterium MC/DC) oraz inspekcje kodu
R5	IV	wysoki	niskie	testy wydajnościowe, inspekcja projektu bazy danych
R4	I	niski	wysokie	testowanie eksploracyjne oraz testowanie oparte na przypadkach użycia
R3	III	niski	niskie	brak (poziom znikomy, nie ma potrzeby alokacji zasobów na testowanie tego ryzyka)

Techniki testowania opartego na ryzyku – FTA

- Analiza drzewa awarii
- Określa przyczyny źródłowe (root cause) awarii
- Określa prawdopodobieństwo niepożądanych zdarzeń
- Dobrze sprawdza się w przypadku dużych i skomplikowanych systemów, a także systemów o znaczeniu krytycznym
- W sposób graficzny prezentuje zależności pomiędzy kombinacjami zdarzeń
- Metoda dedukcyjna – top-down

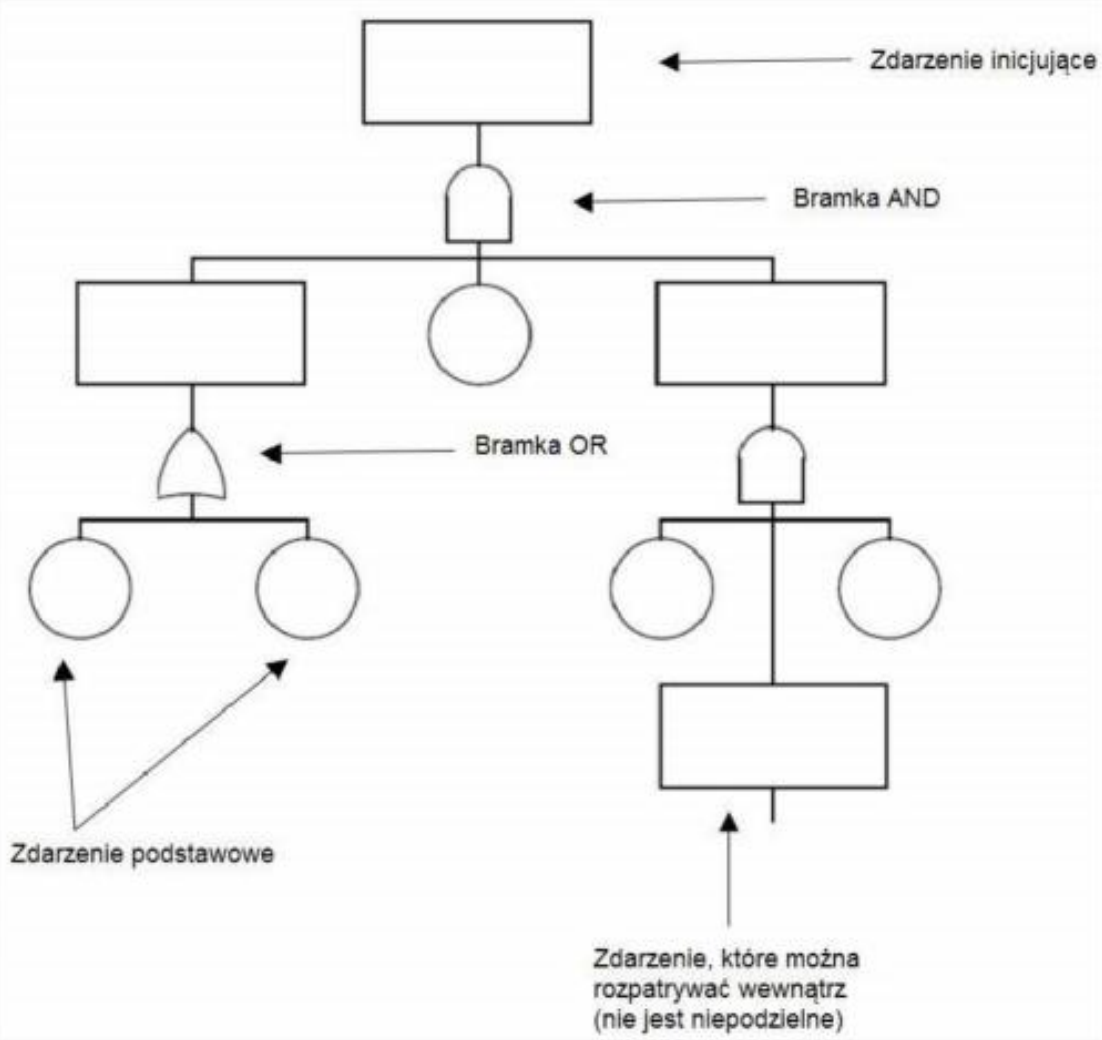
Techniki testowania opartego na ryzyku – FTA

Przykładowe drzewo awarii:



Techniki testowania opartego na ryzyku – FTA

Przykładowe drzewo awarii:



5 x dlaczego?

Jest jedną z metod pozwalających na wykrywanie przyczyn problemów (lub defektów). Jest to zasada, którą stosujemy w celu ustalenia podstawowej przyczyny problemu. Zadawanie kilku pytań „Dlaczego?” pozwala dojść do źródła zakłóceń, gruntownie zbadać ich przyczynę i skupić się na ich skutecznym rozwiązywaniu. Dzięki zadawaniu pytań „Dlaczego?” problem staje się bardziej zrozumiały, przez co podstawowa przyczyna jego powstania jest łatwiejsza do zidentyfikowania i wyeliminowania. Analiza **5 Whys** pozwala odpowiedzieć na pytania:

5 x dlaczego? - zasady

Reguły i wskazówki pomocne do prawidłowego wykonania analizy[2]:
1.Konieczne jest prawidłowe sformułowanie i zapisanie problemu, a także jego zrozumienie przez uczestników.
2.Należy dbać o logikę ciągu przyczynowo-skutkowego oraz odróżnienie przyczyn od objawów. Aby upewnić się, że przyczyny źródłowe na pewno prowadzą do błędu, można odwrócić powstałe w analizie zdania za pomocą zwrotu „i dlatego”.
3.Analizę należy wykonywać krok po kroku, nie skakać do konkluzji. Przyczyn należy szukać w procesach, nie w ludziach. Błędem jest określać przyczynę źródłową jako „błąd ludzki”, „nieuwaga pracownika” itp..
4.Należy pytać „dlaczego”, aż do określenia przyczyny źródłowej, a zatem takiej, której eliminacja sprawi, że błąd już nie wystąpi.
5.Poleca się wykonywać analizę na papierze czy tablicy, zamiast na komputerze.
6.Niezbędne jest zaangażowanie kierownictwa, moderatora oraz prawidłowo dobranej grupy.
7.Ważna jest atmosfera szczerości i zaufania.

5 x dlaczego? - przykład

Problem – Nie wysłaliśmy biuletynu informującego o najnowszych aktualizacjach oprogramowania na czas.
1.Dlaczego nie wysłaliśmy biuletynu na czas? Aktualizacje nie zostały wdrożone do ostatecznego terminu.
2.Dlaczego aktualizacje nie zostały wdrożone na czas? Ponieważ programiści wciąż pracowali nad nowymi funkcjami.
3.Dlaczego programiści wciąż pracowali nad nowymi funkcjami? Jeden z nowych programistów nie znał procedur.
4.Dlaczego nowy programista nie znał wszystkich procedur? Nie był odpowiednio przeszkolony.
5.Dlaczego nie został odpowiednio przeszkolony? Ponieważ dyrektor ds. technicznych jest przekonany, że nowi pracownicy nie potrzebują dokładnych szkoleń i powinni się uczyć podczas pracy

Pytania, jakie warto zadań przed podjęciem decyzji co testujemy

- które elementy aplikacji mogą zostać przetestowane we wczesnej fazie?
- które części kodu/moduły są najbardziej skomplikowane i dlatego najbardziej narażone na wystąpienie błędów?
- która funkcjonalność jest najważniejsza z punktu widzenia zastosowania projektu? która funkcjonalność jest najbardziej widoczna dla klienta?
- które z wymagań zostały zmienione lub ogólnie zdefiniowane?
- która funkcjonalność ma największy wpływ na bezpieczeństwo aplikacji?
- która funkcjonalność ma największy wpływ na finanse?

Pytania, jakie warto zadań przed podjęciem decyzji co testujemy

- które elementy testowanej aplikacji mają największe znaczenie dla klienta?
- które aspekty podobnych, ukończonych poprzednio projektów powodowały problemy?
- które elementy podobnych, ukończonych projektów powodowały największe problemy w fazie utrzymania (maintenance)?
- co programiści uznają na najbardziej narażony na ryzyko element aplikacji?
- która część systemu była tworzona pod presją czasu?
- jaki rodzaj problemów może spowodować negatywną reakcję klienta?
- jaki rodzaj testów może pokryć możliwie najwięcej funkcjonalności?
- które z poprzednio wykonanych przypadków testowych powodowały wykrycie błędów? (test case value)

PYTANIA?

kowal.radek@gmail.com