Wzorce identyfikacji ryzyka w projektach informatycznych

Jakub Miler, Janusz Górski
Katedra Zastosowań Informatyki, Politechnika Gdańska
{jakubm, jango}@eti.pg.gda.pl

Streszczenie

Rozdział prezentuje systematyczne podejście do identyfikacji ryzyka w projektach informatycznych, oparte na wzorcach ryzyka. Podejście zakłada jawne modelowanie rozważanego obszaru biznesowego, co pozwala na kontrolę zakresu identyfikacji i zapewnia kompletność analiz. Zastosowano to podejście wykorzystując RUP jako model odniesienia dla procesów wytwarzania oprogramowania. Następnie omówiono eksperyment, w którym zastosowano omawiane podejście do weryfikacji kompletności znanej listy zagrożeń dla harmonogramu. W podsumowaniu skomentowano wyniki eksperymentu oraz podano dalsze plany badawcze.

1. Wprowadzenie

Sukces projektu informatycznego nie jest przesądzony. Celem projektu jest dostarczenie udziałowcom przedsięwzięcia zadowalającego ich rozwiązania w ramach ograniczeń budżetu i harmonogramu. Ryzyko niskiej jakości produktu oraz przekroczenia budżetu lub harmonogramu jest wysokie, co potwierdza liczba projektów wstrzymanych, opóźnionych lub przepłaconych. Skuteczne zarządzanie tymi zagrożeniami jest obecnie postrzegane jako jeden z najistotniejszych obszarów w zarządzaniu przedsięwzięciami [PMB2000]. Dotychczasowa praktyka zarządzania ryzykiem jest przeważnie oparta na intuicji i osobistym doświadczeniu kierowników projektów. Prowadzone w tym zakresie badania mają na celu dostarczenie efektywnego wsparcia dla czynności zarządzania ryzykiem, a w szczególności umożliwienie ponownego wykorzystania informacji o ryzyku z wcześniejszych projektów.

Rozdział przedstawia wyniki badań autorów w zakresie identyfikacji ryzyka. Skuteczna identyfikacja ryzyka jest niezbędnym warunkiem innych kroków zarządzania ryzykiem, zatem wsparcie tej właśnie fazy jest szczególnie istotne.

Proponowane podejście do identyfikacji ryzyka, omówione w kolejnych rozdziałach, charakteryzuje się następującymi cechami:

- jawne modelowanie *procesu wytwórczego* dla kontroli zakresu identyfikacji,
- użycie *wzorców ryzyka* do identyfikacji potencjalnych czynników ryzyka.

W rozdziale opisano proponowane podejście oraz podano przykłady jego zastosowania. Przedstawiono również zastosowanie tego podejścia w eksperymencie, którego celem była walidacja szeroko znanej listy kontrolnej zagrożeń w projektach informatycznych [MCC1996]. W szczególności pokazano jak omawiane podejście pomaga w znalezieniu, w systematyczny sposób, wielu (istotnych) zagrożeń, których zabrakło w [MCC1996], pokrywając jednocześnie większość zagrożeń opisanych w [JON1994].

Wyniki przeprowadzonego eksperymentu pokazują, że proponowane podejście jest skutecznym mechanizmem wspierania kompletnej identyfikacji ryzyka na różnych poziomach abstrakcji struktury procesu.

Dotychczasowe techniki identyfikacji ryzyka można podzielić na dwie grupy:

- identyfikacja ryzyka za pomocą list kontrolnych (zarówno kwestionariusze jak i listy zagrożeń),
- identyfikacja ryzyka oparta na pracy grupowej (np. sesje typu „burza mózgów").

Praca z predefiniowanymi listami kontrolnymi oznacza łatwe lecz męczące odpowiadanie na liczne pytania, nie zawsze przystające do potrzebnego poziomu szczegółowości. Zaletą list kontrolnych jest to, iż pomagają one kontrolować zakres i (jeśli są kompletne) zapobiegają przeoczeniu ważnych zagrożeń. Praca grupowa, taka jak burze mózgów, akcentuje znaczenie zaangażowania człowieka w identyfikację ryzyka, jednak w znacznie mniejszym stopniu pozwala kontrolować zakres identyfikacji.

Opracowano wiele różnych list kontrolnych o zróżnicowanej strukturze. Niektóre z tych list są dostępne w literaturze (np. „Taxonomy-Based Questionnaire" SEI [SIS1994], 60 czynników ryzyka Capersa Jonesa [JON1994], „Complete List of Schedule Risks" Steve'a McConnella [MCC1996]), podczas gdy inne pozostają własnością ich prawnych właścicieli (np. firmy wytwarzające oprogramowanie, firmy konsultingowe). Software Engineering Institute (SEI) [SEI1991] proponuje własną taksonomię dla projektów informatycznych wraz ze szczegółowym kwestionariuszem (194 pytania). Jednakże kwestionariusz ten nie jest stowarzyszony z żadną zaawansowaną metodą identyfikacji ryzyka, a także brak jest listy zagrożeń, które sygnalizowane byłyby poprzez udzielone odpowiedzi. Inni badacze proponujący własne listy zagrożeń opisują ryzyko albo poprzez pojedyncze zdanie w języku naturalnym [MCC1996], albo poprzez ustrukturalizowany zbiór takich zdań [JON1994].

W obszarze grupowego podejścia do identyfikacji ryzyka szczególnie wyróżnia się podejście proponowane przez J. Kontio. Studiował on skuteczność burz mózgów w identyfikacji ryzyka i w rezultacie swoich badań opracował specjalne szablony dla uczestników sesji burzy mózgów pomagające lepiej specyfikować wykryte ryzyko. Nadal jednak, dla zachowania łatwości użycia metody, używał on do wyrażania ryzyka sformułowań w języku naturalnym [KON2001].

Metoda proponowana w niniejszym rozdziale może być użyta w obu podejściach do identyfikacji ryzyka. W podejściu bazującym na listach kontrolnych, można ją zastosować do przekonstruowania istniejących list dla zapewnienia lepszej kontroli zakresu oraz kompletności. W podejściu bazującym na pracy grupowej, może ona wspierać sesje burzy mózgów poprzez kontrolę zakresu analiz oraz dostarczenie technik precyzyj-

nego opisu ryzyka na różnych poziomach szczegółowości.

Wyniki przedstawione w niniejszym rozdziale mieszczą się w szerszym kontekście badań autorów w kierunku zintegrowanego środowiska wspierającego zarządzanie ryzykiem w przedsięwzięciach informatycznych [MIL2002]. Została już opracowana pilotowa wersja narzędzia programowego [MIL2003], a także przeprowadzono serię eksperymentów walidacyjnych. Podsumowanie prowadzonych badań dostępne jest na stronach internetowych autorów [RISK2002].

2. Modelowanie zakresu identyfikacji ryzyka

Wczesna świadomość możliwych zagrożeń stanowi podstawę skutecznego obniżania ryzyka. Identyfikacja ryzyka jest zatem zawsze pierwszym krokiem w procesie zarządzania ryzykiem. Zidentyfikowane ryzyko powinno być właściwie udokumentowane. Informacja o ryzyku składa się z dwóch głównych elementów:

- *opis ryzyka* – opis danego wydarzenia, które, gdy zaistnieje, negatywnie wpływa na projekt,
- *kontekst ryzyka* – opis usytuowania wydarzenia w ramach zadań, personelu i produktów w projekcie.

W szczególności, opis ryzyka dostarcza właściwego objaśnienia niechcianego zdarzenia lub stanu, podczas gdy kontekst ryzyka odnosi to zdarzenie bądź stan do konkretnych aktywności w strukturze zadaniowej projektu. Kontekst ten wskazuje również personel odpowiedzialny za zadania oraz materiały źródłowe i produkty tych zadań.

W celu ustanowienia kontekstu zagrożeń w projekcie informatycznym potrzebny jest model tego projektu definiujący aktywności, role i artefakty procesu wytwórczego, jak również ich wzajemne powiązania.

Procesy projektowe różnią się w swojej strukturze. Można jednak wyróżnić kilka elementów, które zachowują ważność dla każdego procesu wytwórczego (lub, bardziej ogólnie, dla każdego procesu biznesowego):

- *Aktywność* – akcja wykonywana przez człowieka (ludzi) w konkretnej roli (rolach) przetwarzająca artefakty wejściowe w wyjściowe,
- *Rola* – funkcja, odpowiedzialność osoby realizującej aktywność (jedna osoba może występować w wielu rolach),
- *Artefakt* – przedmiot przetwarzany przez aktywności (np. materiały źródłowe, dokumenty, narzędzia oraz produkty końcowe).

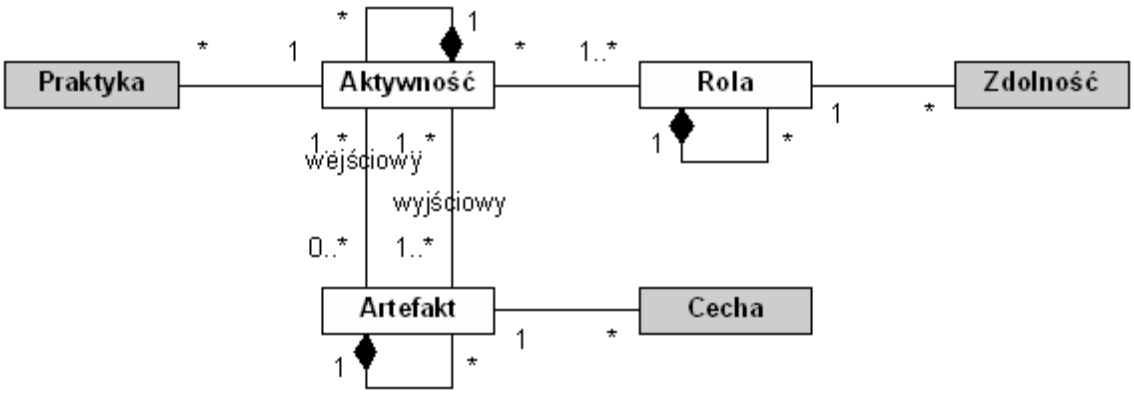
Mówienie o ryzyku wymaga jawnego rozdzielenia korzystnych i szkodliwych aktywności, artefaktów i ról, a bardziej precyzyjnie ich własności. W tym celu rozszerzono podstawowy model aktywności, artefaktów i ról o obiekty wartościujące:

- *Praktyka* – praktyka stosowana w celu ukończenia aktywności,
- *Zdolność* – doświadczenie, biegłość, umiejętność człowieka w danej roli,
- *Cecha* – aspekt jakościowy danego artefaktu.

Zakłada się, że aktywności, artefakty i role mogą być rekursywnie dekomponowane.

Pozwala to na specyfikowanie procesu wytwórczego do takiego stopnia szczegółowości, jaki odpowiada aktualnej perspektywie identyfikacji ryzyka.

Powstały w ten sposób meta-model procesu projektowego pokazano na rysunku 1. w postaci diagramu klas w języku UML.



Rysunek 1. Meta-model procesu projektowego

Opracowany meta-model może być użyty do reprezentacji różnych modeli procesów projektowych. Każdy taki model dostarcza kontekst do opisu potencjalnych zagrożeń. Ocena tych zagrożeń może być następnie dokonana poprzez odwołanie się do rzeczywistego projektu (wcielenia modelu). Należy w tym miejscu zaznaczyć, że model procesu projektowego jest z definicji uproszczeniem rzeczywistego projektu i jako taki pozwala na opis zagrożeń tylko z dokładnością do ustalonych elementów modelu. Możliwa jest jednak dalsza rozbudowa stosowanego modelu procesu projektowego, tak by jak najlepiej odpowiadał on rzeczywistości.

W przeprowadzonych badaniach wybrano Rational Unified Process (RUP) [RUP2001] jako model odniesienia dla projektów informatycznych. Model RUP może być łatwo reprezentowany w terminach zaproponowanego meta-modelu. Definiuje on bezpośrednio aktywności, artefakty oraz role. Przepływy zadań (ang. *workflows*), szczegóły przepływów (ang. *workflow details*), zbiory artefaktów (ang. *artifact sets*) oraz zbiory ról (ang. *role sets*) można zaadaptować jako aktywności, artefakty i role wyższych (bardziej ogólnych) poziomów abstrakcji modelu. Praktyki, cechy i zdolności wydobywane są z opisów odpowiednich elementów modelu RUP, gdzie często podawane są w formie niewymagającej dodatkowej adaptacji. Dla celów opisu ryzyka przebudowano role w modelu RUP w zakresie Zbioru Ról Dodatkowych (ang. *Additional Role Set*) oraz poszerzono rolę Udziałowiec (ang. *Stakeholder*), którą uznano za zbyt ogólną przy modelowaniu kontekstu ryzyka.

Na najbardziej ogólnym poziomie (poziom 0), który nie jest jawnie wyrażony w modelu RUP, określono następujące elementy:

Rola:

- Personel (Dowolna Rola z RUP – ang. *Any Role*)

Aktywność:

- Projekt informatyczny

Artefakt:

- Produkt (wytworzone oprogramowanie)

Na ramowym poziomie dostosowanego modelu RUP (poziom 1) *zbiory ról* z modelu RUP przyjęto jako role, *przepływy zadań* (ang. *workflows*) jako aktywności, przemianowane i poprawione *zbiory artefaktów* jako artefakty i otrzymano następujące elementy:

Role (Zbiory Ról z RUP – ang. *Role Set*):

- Analityk (ang. *Analyst*)
- Wytwórca (ang. *Developer*)
- Tester
- Kierownik (ang. *Manager*)
- Personel Pomocniczy (Zbiór Ról Dodatkowych z RUP – ang. *Additional Role Set*)
- Zewnętrzny udziałowiec (Udziałowiec z RUP – ang. *Stakeholder*)

Aktywności (Przepływy Zadań z RUP – ang. *Workflow*):

- Modelowanie biznesowe (ang. *Business Modeling*)
- Wymagania (ang. *Requirements*)
- Analiza i Projekt (ang. *Analysis & Design*)
- Implementacja (ang. *Implementation*)
- Testowanie (ang. *Testing*)
- Wdrożenie (ang. *Deployment*)
- Zarządzanie Konfiguracją i Zmianami (ang. *Configuration & Change Management*)
- Zarządzanie Projektem (ang. *Project Management*)
- Środowisko (ang. *Environment*)

Artefakty (spoza RUP):

- Dokumentacja Modelowania Biznesowego
- Dokumentacja Wymagań
- Dokumentacja Analizy Systemowej
- Dokumentacja Projektowa
- Dokumentacja Implementacyjna
- System
- Dokumentacja Testowania
- Dokumentacja Wdrożenia
- Wdrożony Produkt
- Środowisko Zarządzania Konfiguracją
- Dokumentacja Zarządzania Konfiguracją
- Plany
- Dokumentacja Zarządzania
- Infrastruktura
- Wytyczne

Na pośrednim poziomie dostosowanego modelu RUP (poziom 2) umieszczono wpro-

st *role* z modelu RUP, przyjęto *szczegóły przepływów* (ang. *workflow details*) jako aktywności oraz wyróżniono nowe artefakty. W ten sposób na poziomie 2 otrzymano następujące elementy:

Role (Role z RUP):

- 8 ról Analityka
- 10 ról Wytwórcy
- 1 rola Testera
- 7 ról Kierownika
- 5 ról Personelu Pomocniczego (pomniejszony Zbiór Ról Dodatkowych z RUP)
  - Twórca Materiałów Szkoleniowych (ang. *Course Developer*)
  - Grafik (ang. *Graphic Artist*)
  - Administrator (ang. *System Administrator*)
  - Twórca Materiałów dla Użytkownika (ang. *Technical Writer*)
  - Specjalista ds. Narzędzi (ang. *Tool Specialist*)
- 6 ról Zewnętrznego Udziałowca (rozszerzona rola Udziałowiec z RUP)
  - Zamawiający
  - Klient
  - Użytkownik
  - Dostawca
  - Konsultant
- Polityka

Aktywności (Szczegóły Przepływów z RUP – ang. *Workflow Details*):

- 56 szczegółów przepływów / średnio 6,2 na przepływ zadań

Artefakty (spoza RUP):

- produkty szczegółów przepływów / około 1-2 na szczegół przepływu

Na najbardziej szczegółowym poziomie dostosowanego modelu RUP (poziom 3) umieszczono *aktywności* i *artefakty* z modelu RUP i zdefiniowano następujące elementy:

Aktywności (wprost z RUP):

- 150 aktywności / średnio 2,7 na szczegół przepływu

Artefakty (wprost z RUP):

- 119 artefaktów, w tym:
  - 6 modeli UML
  - 6 artefaktów złożonych

Przedstawiony powyżej adaptowany model RUP może być dalej rozbudowany w ramach potrzeb konkretnego projektu informatycznego. Dodanie do modelu nowych elementów (np. aktywności) wymaga ustalenia ich miejsca w hierarchii elementów (tychże aktywności), a także powiązań z już istniejącymi elementami innych typów

(w przykładzie: artefaktami i rolami). Ponadto należałoby ustalić zbiór pożądanych własności nowego elementu (tj. praktyk dla aktywności, zdolności dla ról oraz cech dla artefaktów). Pomocne może tu być sięgnięcie do własności elementów istniejących już w modelu. Doświadczenia z dostosowaniem modelu RUP do potrzeb badań wskazują, że dalsza adaptacja modelu nie będzie wymagała znacznych nakładów. W szczególności, w miarę uszczegóławiania modelu, nakład pracy przypadający na jeden nowy element powinien maleć ze względu na tendencję do lokalizowania się zmian.

3. Wzorce identyfikacji ryzyka

Negatywne zdarzenie, odniesione do modelu procesu projektowego, może być reprezentowane jako naruszenie (pożądanego) związku w modelu np. *dana aktywność nie przestrzega zalecanej praktyki*. Poprzez przejrzenie wszystkich elementów i związków w meta-modelu pokazanym na rysunku 1. możliwe jest zdefiniowanie kompletnego zbioru klas zdarzeń stanowiących ryzyko. Wypisano je poniżej stosując konwencję, że nazwa obiektu jest pogrubiona i uzupełniona o jego meta-klasę (kursywą w nawiasach ostrych).

Klasy zdarzeń dla Artefaktów:

Ar<*artefakt*> nie został wytworzony

Ar<*artefakt*> traci **C**<*cecha*>

Klasy zdarzeń dla Aktywności:

A<*aktywność*> nie została wykonana

A<*aktywność*> zabiera więcej czasu niż przewidziano

A<*aktywność*> kosztuje więcej niż przewidziano

A<*aktywność*> traci **R**<*rola*>

A<*aktywność*> traci **Ar**<*artefakt*>

A<*aktywność*> traci **P**<*praktyka*>

Klasy zdarzeń dla Ról:

R<*rola*> nie jest przydzielona

R<*rola*> traci **Z**<*zdolność*>

Zdarzenia oznaczające brak materializacji pewnych elementów modelu (artefaktu, aktywności, roli) zostały dodane w celu uwzględnienia możliwych odstępstw w realizacji modelu. Podobnie, zdarzenia związane z czasem i kosztem zostały wprowadzone dla pokrycia wpływu ryzyka na harmonogram i budżet.

Znaczenie straty jest zdefiniowane następująco:

A<*aktywność*> traci **P**<*praktyka*> oznacza, że **P** nie jest realizowana w ramach **A**,

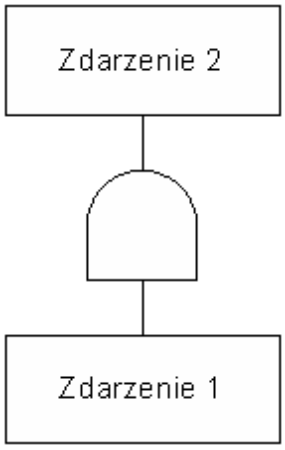
A<*aktywność*> traci **R**<*rola*> oznacza, że **R** nie uczestniczy (nawet jeśli jest komuś przypisana) w realizacji **A**,

A<*aktywność*> traci **Ar**<*artefakt*> oznacza, że **Ar** nie jest używany (nawet jeśli został wytworzony) w kontekście **A**,

Ar<*artefakt*> traci **C**<*cecha*> oznacza, że **Ar** posiada **C** w mniejszym stopniu niż oczekiwano,

R<*rola*> traci **Z**<*zdolność*> oznacza, że **R** posiada **Z** w mniejszym stopniu niż oczekiwano.

Analizując związki przyczynowo-skutkowe pomiędzy zdarzeniami powyższych klas można łatwo określić potencjalne *wzorce identyfikacji ryzyka*. Schemat takiego wzorca został przedstawiony na rysunku 2. Oznacza on: *jeśli* Zdarzenie 1 *występuje w stanie bieżącym, to należy rozważyć wystąpienie* Zdarzenia 2 *w przyszłym stanie*. Innymi słowy, materializacja przyczyny nie powoduje automatycznie wystąpienia skutku, a raczej zwiększa szansę tego wystąpienia.



Rysunek 2. Drzewo zdarzeń dla scenariusza typu przyczyna-skutek

Aby wygenerować wszystkie możliwe wzorce ryzyka połączono wzajemnie wszystkie klasy zdarzeń w ramach schematu przyczyna-skutek pokazanego na rysunku 2. Następnie zastosowano filtr składniowy aby usunąć te kombinacje, które nie miały sensu niezależnie od rzeczywistych elementów modelu procesu projektowego. W ten sposób obniżono liczbę wzorców ze 100 do 82.

Wzorce te zostały także przeanalizowane z uwzględnieniem znaczenia różnych kombinacji rzeczywistych elementów modelu. Kiedy podstawi się autentyczne aktywności, role i artefakty do wzorca, tylko niektóre z kombinacji będą reprezentowały rzeczywiste scenariusze ryzyka. Ponadto niektóre z nich mogą nawet oznaczać zdarzenia pozytywne w procesie. Podstawiając rzeczywiste elementy procesu do wzorców można ograniczyć otrzymaną listę tylko do zagrożeń istotnych w kontekście danego modelu procesu.

Przykłady wzorców identyfikacji ryzyka podano poniżej (w pierwszym wzorcu A1 i A2 oznaczają różne aktywności):

Jeżeli **A1**<*aktywność*> nie jest wykonana to **A2**<*aktywność*> zabiera więcej czasu niż przewidziano.

Jeżeli **A**<*aktywność*> zabiera więcej czasu niż przewidziano to **R**<*rola*> traci

<*zdolność*>.

Jeżeli **A**<*aktywność*> kosztuje więcej niż przewidziano to **A**<*aktywność*> traci **P**<*praktyka*>.

Jeżeli **A**<*aktywność*> traci **R**<*rola*> to **A**<*aktywność*> zabiera więcej czasu niż przewidziano.

Jeżeli **A**<*aktywność*> traci **Ar1**<*artefakt*> to **Ar2**<*artefakt*> traci **C**<*cecha*>.

Jeżeli **A**<*aktywność*> traci **P**<*praktyka*> to **A**<*aktywność*> zabiera więcej czasu niż przewidziano.

Jeżeli **A**<*aktywność*> traci **P**<*praktyka*> to **Ar**<*artefakt*> traci **C**<*cecha*>.

Jeżeli **Ar**<*artefakt*> nie jest wytworzony to **A**<*aktywność*> traci **Ar**<*artefakt*>.

Jeżeli **Ar**<*artefakt*> traci **C**<*cecha*> to **A**<*aktywność*> traci **P**<*praktyka*>.

Jeżeli **R**<*rola*> nie jest przydzielona to **A**<*aktywność*> nie jest wykonana.

Jeżeli **R**<*rola*> traci **Z**<*zdolność*> to **A**<*aktywność*> traci **P**<*praktyka*>.

Jeżeli **R**<*rola*> traci **Z**<*zdolność*> to **R**<*rola*> traci **Z**<*zdolność*>.

Przed przypisaniem właściwych aktywności, ról, artefaktów, praktyk, zdolności i cech do zmiennych występujących we wzorcach nie można stwierdzić, czy wzorce te reprezentują sensowne scenariusze ryzyka. Niektóre potencjalne wzorce mogą być jednak odrzucone na bazie kryteriów czysto składniowych, tak jak w poniższym przykładzie:

Jeżeli **Ar**<artefakt> traci **C**<cecha> to **A**<aktywność> traci **R**<rola>.

Niezależnie od konkretnych obiektów podstawionych pod Ar, C, A i R ten wzorzec łączy dwa wysoce niezależne zdarzenia, które nie stanowią scenariusza ryzyka.

Wzorce identyfikacji ryzyka mogą być systematycznie zastosowane do danego modelu procesu w celu identyfikacji możliwych scenariuszy ryzyka. Poniżej podano przykłady zdarzeń i scenariuszy ryzyka wygenerowanych poprzez zastosowanie wybranych wzorców do modelu odniesienia RUP przestawionego w poprzednim rozdziale. Przykłady podzielono zgodnie z poziomem szczegółowości modelu. W nawiasach klamrowych podano opis bardziej złożonych scenariuszy w języku naturalnym.

Poziom 0:

Projekt Informatyczny<*aktywność*> kosztuje więcej niż przewidziano

Produkt<*artefakt*> traci **Jakość**<*cecha*>

Personel<*rola*> traci **Motywacja**<*zdolność*>

Poziom 1:

Jeżeli **Modelowanie biznesowe**<*aktywność*> traci Uzyskaj **wspólne zrozumienie dziedziny biznesowej i modeluj docelowy proces**<*praktyka*> to **Dokumentacja Modelowania Biznesowego**<*artefakt*> traci **Zgodność z dziedziną biznesową**<*cecha*>

{Dokumentacja modelowania biznesowego nie reprezentuje dobrze dziedziny biznesowej z powodu słabego jej zrozumienia i braku modelowania}

Jeżeli **Dokumentacja Modelowania Biznesowego**<*artefakt*> traci **Zgodność z**

dziedziną biznesową<*cecha*> to **Produkt**<*artefakt*> traci **Jakość**<*cecha*>

{Złe zrozumienie dziedziny biznesowej skutkuje niską jakością produktu}

Poziom 2:

Jeżeli **Identyfikuj Procesy Biznesowe**<*aktywność*> traci **Przeprowadź spotkanie w celu ustalenia terminologii i naszkicowania przypadków użycia i aktorów**<*praktyka*> to **Lista Procesów Biznesowych**<*artefakt*> traci **Kompletność**<*cecha*>

{Brak spotkania definiującego dziedzinę biznesową skutkuje niekompletną identyfikacją procesów biznesowych}

Kierownik Projektu<*rola*> nie jest przydzielona

{Kierownik projektu opuszcza projekt}

Poziom 3:

Śledź Stan Projektu<*aktywność*> traci **Używaj odpowiednich pomiarów**<*praktyka*>

{Nieodpowiednie pomiary}

Można zauważyć, że to ryzyko jest podawane także przez Capersa Jonesa [JON1994] jako ryzyko nr 28.

Jeżeli **Glosariusz Biznesowy**<*artefakt*> traci **Jednoznaczność**<*cecha*> to **Model Biznesowych Przypadków Użycia**<*artefakt*> traci **Spójność terminologii**<*cecha*>

{Niejednoznaczny glosariusz pojęć dziedziny biznesowej skutkuje niespójnym modelem biznesowym}

Jeżeli **Lista Technik Testowania**<*artefakt*> traci **Reprezentacja wszystkich zagrożeń dla jakości**<*cecha*> to **Przypadek Testowy**<*artefakt*> nie jest wytworzony.

{Zły zakres testowania pod kątem docelowej jakości wyklucza pewne pożądane testy}

Mając zbiór potencjalnych scenariuszy ryzyka możliwe jest wykrycie, które z nich faktycznie mają miejsce w projekcie. Można to osiągnąć, ogólnie, na dwa sposoby: stosując kwestionariusze lub sesje burzy mózgów. Obie techniki mogą skorzystać na użyciu proponowanej metody wzorców identyfikacji ryzyka. Kwestionariusze mogą być uproszczone i ustandaryzowane, a pytania przybiorą formę, na przykład:

Czy **A**<*aktywność*> stosuje **P**<*praktyka*>?

Czy **R**<*rola*> posiada **Z**<*zdolność*>?

Czy **Ar**<*artefakt*> posiada **C**<*cecha*>?

W sesji burzy mózgów uczestnicy mogą rozpocząć pracę z bardzo ogólną definicją procesu projektowego (np. poziom 1 modelu RUP), a następnie zgłębiać obszary, gdzie identyfikowane jest największe ryzyko. W trakcie całej sesji ryzyko jest dokumentowane poprzez zastosowanie wzorców ryzyka do danych elementów modelu procesu.

Ryzyko zidentyfikowane obiema technikami musi być następnie ocenione, tak by

wybrać to przeznaczone do obniżania (np. najbardziej zagrażające projektowi, najtańsze do obniżenia). Zagadnienie szacowania prawdopodobieństwa wystąpienia danego scenariusza opisanego wzorcem oraz wagi konsekwencji tego wystąpienia wychodzi poza ramy niniejszego rozdziału i stanowi obszar dalszych badań autorów.

4. Eksperyment walidacyjny

4.1. Projekt eksperymentu

W celu empirycznej walidacji proponowanego podejścia przeprowadzono kontrolowany eksperyment. W eksperymencie wykorzystano jedną z publicznie dostępnych list kontrolnych identyfikacji ryzyka, a mianowicie „Complete List of Schedule Risks" Steve'a McConnella [MCC1996]. Ta lista spisuje 109 czynników ryzyka w 12. obszarach projektu informatycznego takich jak: harmonogram, produkt, personel czy klient. Czynniki wyrażone są w postaci zdań w języku naturalnym.

Zdefiniowano dwa odrębne cele eksperymentu:

- Pierwszy skupiał się na walidacji kompletności listy McConnella przy użyciu proponowanej metody wzorców ryzyka,
- Drugi skupiał się na systematycznym zastosowaniu metody do rozbudowanego na bazie RUP procesu implikowanego listą McConnella.

Plan eksperymentu obejmował 5 kroków:

1. Odtworzenie modelu procesu (tj. aktywności, artefaktów, ról, praktyk, cech i zdolności), który kryje się w liście McConnella,
2. Wyrażenie wszystkich zagrożeń na liście kontrolnej w terminach tego modelu z użyciem wzorców ryzyka,
3. Systematyczne zastosowanie wzorców identyfikacji ryzyka do odtworzonego modelu procesu w celu sprawdzenia, czy możliwe jest odnalezienie ważnych zagrożenie, które nie znalazły się na liście McConnella,
4. Rozszerzenie modelu procesu McConnella o wybrane reprezentatywne elementy modelu odniesienia RUP,
5. Ponowne zastosowanie wzorców identyfikacji ryzyka do rozbudowanego modelu procesu i identyfikacja brakujących czynników ryzyka w nowych obszarach.

Ponieważ nie istnieje jawny model procesu leżącego u podstaw listy kontrolnej Steve'a McConnella (a przynajmniej nie jest on znany autorom artykułu), taki model (implikowany przez listę) został zbudowany w kroku 1. Następnie do tego modelu zastosowano opracowane wzorce identyfikacji ryzyka, najpierw w celu wyrażenia zagrożeń już istniejących na liście McConnella (krok 2), a później do wyprowadzenia nowych zagrożeń z modelu (krok 3). Te dwie fazy zrealizowały pierwszy cel eksperymentu – możliwe było sprawdzenie, czy wzorce identyfikacji ryzyka mogą uzupełnić badaną listę o ważne zagrożenia. Dla realizacji drugiego celu rozbudowano oryginalny model procesu (krok 4) o elementy sugerowane przez model RUP (a jeszcze nieobecne) i jesz-

cze raz zastosowano wzorce identyfikacji ryzyka do tak otrzymanego modelu procesu (krok 5).

4.2. Szczegółowe wyniki eksperymentu

Główne wyniki eksperymentu otrzymano w krokach 3. i 5., jednak każdy krok eksperymentu przyniósł pewne interesujące wyniki, które warto opisać odrębnie. Kolejne podrozdziały opisują rezultaty poszczególnych kroków.

4.2.1.Krok 1

W tym kroku odtworzono model procesu projektowego przywoływany przez czynniki ryzyka wyszczególnione na liście McConnella. Opisano ten model w terminach proponowanego meta-modelu (rysunek 1). Ze względu na ograniczenia artykułu nie jest możliwe pełne zaprezentowanie tego modelu. Zamiast tego, w tabeli 1. podano podsumowanie jego złożoności. Poszczególne elementy tego modelu będą użyte w dalszej części artykułu w przykładowych opisach zagrożeń.

Tabela 1. Statystyki modelu procesu wydobytego z listy kontrolnej McConnella

Element modelu	Liczba	Uwagi
Rola	11	2 poziomy szczegółowości
Aktywność	26	4 poziomy szczegółowości
Artefakt	20	2 poziomy szczegółowości
Zdolność	37	dla 9 ról
Praktyka	31	dla 11 aktywności
Cecha	53	dla 20 artefaktów

4.2.2.Krok 2

W kroku 2, stosując wzorce ryzyka, przedefiniowano zagrożenia już istniejące na liście kontrolnej McConnella. Krok ten może wydawać się niepotrzebny, gdyż wykorzystuje on informacje wydobyte z listy kontrolnej do rekonstrukcji jej samej. W ten sposób jednak można było zweryfikować, czy proponowany język wzorców ma wystarczającą siłę wyrazu, aby wypowiedzieć zagrożenia opisane przez McConnella.

Ostatecznie wszystkie 109 zagrożeń zostało przetłumaczone zgodnie ze wzorcami ryzyka, ale ze względu na oczywiste ograniczenia artykułu, podać można tylko przykłady. Kolejne akapity podają przykłady czynników ryzyka McConnella wyrażonych przy użyciu wzorców identyfikacji ryzyka (najpierw podano kursywą oryginalną definicję zagrożenia wraz z jego pozycją na liście McConnella z nawiasach kwadratowych, a następnie wypowiedziano to samo zagrożenie w języku wzorców ryzyka):

[9] Nadmierna presja ze strony terminów zmniejsza produktywność

Jeżeli **Projekt**<*aktywność*> traci **Unikaj nadmiernej presji harmonogramu**<*praktyka*> to **Personel**<*rola*> traci **Produktywność**<*zdolność*>.

[24] Kierownictwo preferuje "herosów" ponad rzetelną informacje o stanie projektu, co zmniejsza zdolność do wykrywania i korygowania problemów

Jeżeli **Kierownictwo**<*rola*> traci **Zdolność do promowania rzetelnego raportowania**<*zdolność*> to **Kierownictwo**<*rola*> traci **Zdolność do wykrycia i korygowania problemów**<*zdolność*>.

[29] Narzędzia wspomagające wytwarzanie nie funkcjonują zgodnie z oczekiwaniami - inżynierowie zużywają czas na ich dopasowanie do potrzeb lub na zaznajamianie się z nowymi narzędziami

Jeżeli **Narzędzia Wytwórcze**<*artefakt*> traci **Niezawodność**<*cecha*> to **Wytwarzanie**<*aktywność*> zabiera więcej czasu niż przewidziano.

[33] Użytkownicy nie włączają się do projektu i w konsekwencji nie dają niezbędnego wsparcia

Jeżeli **Użytkownik**<*rola*> traci **Zaangażowanie**<*zdolność*> to **Projekt**<*aktywność*> traci **Uzyskaj wsparcie końcowych użytkowników**<*praktyka*>.

[48] Zleceniobiorca nie włącza się w projekt i w konsekwencji nie realizuje swoich zadań na wymaganym poziomie wydajności

Jeżeli **Zleceniobiorca**<*rola*> traci **Zaangażowanie**<*zdolność*> to **Zleceniobiorca**<*rola*> traci **Produktywność**<*zdolność*>.

[52] Zgrubnie zdefiniowane wymagania dotyczące produktu wymagają więcej pracy niż oczekiwano

Jeżeli **Wymagania**<*artefakt*> traci **Precyzja**<*cecha*> to **Wytwarzanie**<*aktywność*> zabiera więcej czasu niż przewidziano.

[53] Moduły zawierające błędy wymagają więcej nakładów na testowanie, projektowanie i implementację niż oczekiwano

Jeżeli **Moduł**<*artefakt*> traci **Niezawodność**<*cecha*> to **Testowanie**<*aktywność*> zabiera więcej czasu niż przewidziano i **Projektowanie**<*aktywność*> zabiera więcej czasu niż przewidziano i **Implementacja**<*aktywność*> zabiera więcej czasu niż przewidziano.

[56] Wytworzono niewłaściwy interfejs użytkownika, który wymaga przeprojektowania i ponownej implementacji

Jeżeli **Produkt**<*artefakt*> traci **Właściwy interfejs użytkownika**<*cecha*> to **Projektowanie**<*aktywność*> zabiera więcej czasu niż przewidziano i **Implementacja**<*aktywność*> zabiera więcej czasu niż przewidziano.

[82] Konflikty w ramach zespołu powodują słabą komunikację, wadliwe rozwiązania

projektowe, błędy interfejsów i w efekcie dodatkową pracę

Jeżeli **Projekt**<*aktywność*> traci **Rozwiązuj konflikty między członkami zespołu**<*praktyka*> to **Komunikacja**<*aktywność*> zabiera więcej czasu niż przewidziano i **Projekt**<*artefakt*> traci **Jakość**<*cecha*> i **Moduł**<*artefakt*> traci **Jakość interfejsu**<*cecha*>.

[91] Sabotaż ze strony kierownictwa skutkuje nieefektywnym harmonogramowaniem i planowaniem

Jeżeli **Kierownictwo**<*rola*> traci **Dobra wola**<*zdolność*> to **Harmonogram**<*artefakt*> traci **Wydajność**<*cecha*> i **Plan Wytwarzania**<*artefakt*> traci **Efektywność**<*cecha*>.

[97] Niezbędnej funkcjonalności nie da się zaimplementować na bazie wybranych bibliotek; wytwórcy muszą zacząć stosować inne biblioteki lub zrealizować niezbędne funkcje "od zera"

Jeżeli **Ponownie Użyty Kod**<*artefakt*> traci **Odpowiednia funkcjonalność**<*cecha*> to **Implementacja**<*aktywność*> zabiera więcej czasu niż przewidziano.

[108] Zdawkowe zarządzanie ryzykiem powoduje, że nie dostrzeżono poważnych zagrożeń

Jeżeli **Zarządzanie Ryzykiem**<*aktywność*> traci **Uzyskaj zaangażowanie personelu w zarządzanie ryzykiem**<*praktyka*> to **Lista Zagrożeń**<*artefakt*> traci **Pokrycie głównych zagrożeń**<*cecha*>.

4.2.3.Krok 3

W tym kroku zidentyfikowano dodatkowe zagrożenia dla harmonogramu nieobecne na liście McConnella. W ramach tego kroku skupiono się wyłącznie na modelu procesu wyodrębnionym w kroku 1., bez rozszerzania go o jakiekolwiek nowe obszary, które implikowałyby nowe klasy zagrożeń. Wszystkie zagrożenia zidentyfikowane w tym kroku były już obecne w modelu procesu użytym niejawnie przez McConnella, lecz zostały pominięte w jego liście kontrolnej.

Ze względu na ograniczone zasoby nie było możliwe zastosowanie wszystkich wzorców do całego modelu. Taka całościowa analiza mogłaby być najlepiej wykonana za pomocą narzędzia. Niemniej jednak, w trakcie dwóch godzin analiz udało się odnaleźć 14 nowych scenariuszy, które wyrażają znaczące czynniki ryzyka dla harmonogramu w projekcie informatycznym. Niektóre z nich podano poniżej.

Projekt<*aktywność*> traci **Regulacje prawne**<*artefakt*>.

{Projekt pomija obowiązujące regulacje prawne}

Jeżeli **Komunikacja**<*aktywność*> zabiera więcej czasu niż przewidziano to **Projekt**<*aktywność*> traci **Rozwiązuj konflikty między członkami zespołu**<*praktyka*>.

{Nieefektywny kanał komunikacyjny skutkuje słabym wykrywaniem i rozwiązywaniem konfliktów}

Jeżeli **Projekt**<*aktywność*> traci **Uzyskaj wsparcie końcowych użytkowników**<*praktyka*> to **Produkt**<*artefakt*> traci **Właściwy interfejs użytkownika**<*cecha*>.

{Brak wsparcia końcowych użytkowników powoduje wytworzenie niewłaściwego interfejsu użytkownika}

Projekt<*aktywność*> traci **Zleceniobiorca**<*rola*>.

{Praca w projekcie, tam gdzie mogłaby i powinna, nie jest podzlecana}

Jeżeli **Wymagania**<*artefakt*> traci **Stabilność**<*cecha*> to **Zleceniobiorca**<*rola*> traci **Zaangażowanie**<*zdolność*>.

{Zleceniobiorca wycofuje się z projektu z powodu bardzo niestabilnych wymagań zmieniających warunki kontraktu}

Nawet pobieżna analiza tych czynników wskazuje, że są one ważne, a ich zignorowanie może mieć opłakane skutki dla projektu.

4.2.4.Krok 4

W tym kroku dodano nowe elementy do modelu procesu wynikającego z listy McConnella. Rozszerzenia te zostały wywiedzione z modelu RUP. Dodano nowe praktyki, cechy oraz zdolności do już istniejących aktywności, artefaktów i ról jak również do nowo wprowadzonych elementów modelu. Powstały w ten sposób model procesu jest bardziej zgodny z RUP niż oryginalny model implikowany przez listę.

Tabela 2. podsumowuje rozszerzenia modelu.

Tabela 2. Statystyki rozszerzeń oryginalnego modelu procesu

Element modelu	Liczba	Uwagi
Rola	2	
Aktywność	2	
Artefakt	3	
Zdolność	4	dla 3 oryginalnych i 1 nowej roli
Praktyka	4	dla 2 oryginalnych aktywności
Cecha	5	dla 3 oryg. i 1 nowego artefaktu

4.2.5.Krok 5

W tym kroku zidentyfikowano czynniki ryzyka dla harmonogramu dotyczące nowych obszarów projektu, dodanych w kroku 4. Nie były one oczywiście obecne na liście kontrolnej McConnella, gdyż zostały wywiedzione z nowych elementów modelu procesu zapożyczonych z modelu RUP. Warto zauważyć, że nowe czynniki ryzyka nie różnią się poziomem szczegółowości od tych wcześniej podanych przez Steve'a McConnella (są wyrażone na podobnym poziomie abstrakcji).

Podobnie jak w kroku 3., ograniczone zasoby zmusiły autorów do poszukiwania jedynie znaczących przykładów. Zatem, po kolejnych dwóch godzinach analiz zidentyfikowano 14 dodatkowych scenariuszy. Poniżej podano jedynie kilka przykładów odnalezionych nowych czynników ryzyka dla harmonogramu.

Jeżeli **Materiały Szkoleniowe**<*artefakt*> nie jest wytworzony to **Użytkownik**<*rola*> traci **Zdolność do akceptacji produktu**<*zdolność*>.

{Końcowy użytkownik nie akceptuje produktu z powodu braku materiałów szkoleniowych}

Jeżeli **Zarządzanie Konfiguracją i Zmianami**<*aktywność*> nie jest wykonana to **Wymagania**<*artefakt*> traci **Kompletność**<*cecha*> i wtedy **Produkt**<*artefakt*> traci **Zgodność z oczekiwaniami użytkownika**<*cecha*>.

{Bez zarządzania zmianami nowe wymagania nie mogą być skutecznie włączone skutkując niezadowalającym produktem}

Jeżeli **Wytyczne dla Programistów**<*artefakt*> nie jest wytworzony to **Moduł**<*artefakt*> traci **Czytelność**<*cecha*> i wtedy **Testowanie**<*aktywność*> zabiera więcej czasu niż przewidziano.

{Brak wytycznych dla programistów skutkuje nieczytelnym kodem, który wymaga dodatkowych nakładów na testowanie}

Jeżeli **Projekt**<*aktywność*> traci **Modeluj wizualnie (UML)**<*praktyka*> to **Wymagania**<*artefakt*> traci **Zrozumiałość**<*cecha*>.

{Wymagania niespecyfikowane wizualnie są mniej zrozumiałe dla zespołu projektowego}

Jeżeli **Kierownictwo**<*rola*> traci **Zdolności prezentacyjne, komunikacyjne i negocjacyjne**<*zdolność*> to **Klient**<*rola*> traci **Zaangażowanie**<*zdolność*>.

{Słabe zdolności interpersonalne kierownictwa zniechęcają klienta}

4.3. Podsumowanie eksperymentu

W poszczególnych etapach eksperymentu zebrano pewne metryki dla uzyskania lepszej świadomości co do pracochłonności prac analitycznych. Tabela 3. podaje zmierzone czasy trwania faz eksperymentu.

Tabela 3. Czas trwania faz eksperymentu

Faza	Czas trwania [godz.]

Kroki 1 i 2	10
Krok 3	2
Krok 4	1
Krok 5	2
Całość eksperymentu	15

W eksperymencie całość pracy wykonana została bez wsparcia narzędziowego (dedykowanego dla metody). Całościowa analiza modelu procesu McConnella, taka jak wykonana w kroku 3., z pewnością będzie wymagała takiego wsparcia, zatem trudno jest w obecnej fazie badań podać wiarygodną estymację jej pracochłonności.

Jako dodatkowy rezultat eksperymentu warto wspomnieć listę 17-tu zalecanych praktyk dla aktywności „Projekt informatyczny" wydobytych z listy kontrolnej Steve'a McConnella. Lista obejmuje praktyki takie jak, na przykład:

- Unikaj nadmiernej presji harmonogramu,
- Uzyskaj wsparcie końcowych użytkowników,
- Utrzymuj dobre stosunki między wytwórcami i kierownictwem,
- Rozwiązuj konflikty między członkami zespołu,
- Stosuj się do zaleceń i standardów,
- Unikaj biurokratycznego stosowania zaleceń i standardów.

5. Wnioski

W rozdziale zaprezentowano nową metodę systematycznej identyfikacji ryzyka opartą na wzorcach identyfikacji ryzyka. Istotą tego podejścia jest to, że jawnie modelowany jest kontekst, w ramach którego poszukuje się ryzyka. W ten sposób kontrolowany jest zakres i zapewniana jest kompletność analiz. Model kontekstu ryzyka reprezentuje objęty zainteresowaniem proces biznesowy. Zaproponowano meta-model, który pozwala zbudować model dowolnego procesu biznesowego. Na obecnym etapie badań skoncentrowano się jednak wyłącznie na procesach reprezentujących przedsięwzięcia informatyczne. Odwołanie się do modelu RUP gwarantuje, że nie pominięto żadnych istotnych obszarów dotyczących wytwarzania oprogramowania.

W ramach badań zdefiniowano kompletny zestaw wzorców identyfikacji ryzyka, które odnoszą się do odstępstw od zaleceń zawartych w opisie modelu RUP. Wzorce te mogą być następnie zastosowane do konkretnego modelu procesu projektowego, który został wyrażony w terminach modelu RUP, w celu identyfikacji potencjalnych zagrożeń właściwych temu modelowi. Zależnie od rozmiaru modelu, liczba otrzymanych zagrożeń może być dość duża, lecz praca związana z zastosowaniem wzorców jest wydatkowana tylko raz dla danego modelu (może być wielokrotnie wykorzystana w projektach realizowanych według tego samego modelu procesu). Pracochłonność stworzenia listy możliwych scenariuszy ryzyka dla modelu rzeczywistego procesu oraz dalszych analiz ryzyka w rzeczywistych projektach jest trudna do oszacowania na obecnym etapie ba-

dań. Będzie to wymagało przeprowadzenia dodatkowych eksperymentów, również z wykorzystaniem wsparcia narzędziowego.

W celu walidacji proponowanego podejścia zastosowano je do znanej listy kontrolnej opublikowanej w [MCC1996]. Eksperymentu przyniósł następujące wyniki:

1. Możliwa była identyfikacja szeregu brakujących zagrożeń, które nie znalazły się na badanej liście kontrolnej, mimo że nie wydają się być mniej istotne od tych już obecnych na liście,
2. Możliwe było uzupełnienie modelu procesu implikowanego przez badaną listę kontrolną o istotne elementy (do których nie odwoływała się oryginalna lista), co następnie umożliwiło identyfikację kolejnych zagrożeń brakujących na liście.

Cechą wyróżniającą proponowane podejście jest to, że tworzy ono ramę dla systematycznej identyfikacji ryzyka oraz że może być użyte na różnych poziomach abstrakcji procesu. W odróżnieniu od kwestionariuszy, często zawierających przemieszane pytania o zróżnicowanej ogólności, użycie wzorców jest sterowane dobrze zdefiniowanymi poziomami ogólności modelu procesu. Daje to analitykowi ryzyka możliwość dostosowania podejścia do wymaganego poziomu szczegółowości oraz utrzymanie kontroli nad zakresem i kompletnością analiz. Ponadto scenariusze wykryte na bazie wzorców, dzięki ścisłemu powiązaniu z modelem procesu, odnoszą się bardziej precyzyjnie do szczegółów analizowanego przedsięwzięcia niż uniwersalne pytania kwestionariuszy.

W opinii autorów, proponowane podejście stanowi uzupełnienie w stosunku do już stosowanych metod identyfikacji ryzyka: użycia predefiniowanych list kontrolnych lub identyfikowania ryzyka w ramach różnych form pracy grupowej.

Plany dalszych prac badawczych autorów obejmują:

- eksperymenty identyfikacji ryzyka prowadzone wraz z partnerami przemysłowymi,
- studia nad konstrukcją bardziej złożonych wzorców identyfikacji ryzyka wykorzystujących logikę zdarzeń i logikę temporalną,
- badanie możliwości użycia wzorców ryzyka dla wsparcia fazy analizy ryzyka,
- wbudowanie proponowanego podejścia w rozwijane narzędzie do zarządzania ryzykiem [MIL2003].

Autorzy planują również zastosowanie zaprezentowanego podejścia do innych procesów biznesowych, np. procesy medyczne lub procesy e-biznesu.

Bibliografia

[JON1994] C Jones, *Assessment and Control of Software Risks*, Yourdon Press, New Jersey, 1994.

[KON2001] J Kontio, *Software Engineering Risk Management: A Method, Improvement Framework, and Empirical Evaluation*, rozprawa doktorska, Politechnika Helsińska, Finlandia, 2001.

[MCC1996] S McConnell, *Rapid Development*, Microsoft Press, 1996.

[MIL2002] J Miler i J Górski, *Supporting team risk management in software procurement and development projects*, mat. konf. 4. Krajowej Konferencji Inżynierii Oprogramowania, Poznań - Tarnowo Podgórne, październik 2002, wyd. NAKOM, Poznań, 2002.

[MIL2003] J Miler i J Górski, *Środowisko wspomagające zarządzanie ryzykiem w przedsięwzięciach informatycznych*, mat. konf. I Krajowej Konferencji Technologie Informacyjne, Gdańsk, maj 2003, wyd. PG, Gdańsk, 2003.

[PMB2000] *PMBOK Guide, 2000 Edition*, Project Management Institute, 2000.

[RUP2001] *Rational Unified Process*, http://www.rational.com/rup.

[RISK2002] *Strona projektu RiskGuide*, http://mkzlway.eti.pg.gda.pl/RiskGuide.

[SIS1994] F Sisti i F Joseph, *Software Risk Evaluation Method*, Tech. Rep. CMU/SEI-94-TR-19, Carnegie Mellon University, Pittsburgh PA, 1994.

[SEI1991] *Software Engineering Institute*, http://www.sei.cmu.edu.