BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 24, 2007

Zarys metodyki sterowanego ryzykiem testowania systemów wbudowanych

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. Kaliskiego 2, 00–908 Warszawa

Zbigniew ZIELIŃSKI

Zakład Teleinformatyki, Instytut Teleinformatyki i Automatyki WAT,
ul. Kaliskiego 2, 00–908 Warszawa

STRESZCZENIE: Artykuł zawiera propozycję metodyki wykonania planu testów dla systemu wbudowanego, bazującej na wynikach analizy ryzyka i wyborze określonego zestawu kryteriów jakościowych. Jest on rozwinięciem tematyki zawartej w [3].

SŁOWA KLUCZOWE: ryzyko, plan testów, systemy wbudowane

1. Wstęp

Specyfika wytwarzania systemów wbudowanych polega głównie na konieczności uwzględniania dość ograniczonych zasobów systemu docelowego, jak również obowiązujących rygorystycznych standardów jakościowych i certyfikacyjnych. Ze względu na bardzo wysokie koszty testowania systemów wbudowanych, sięgające nawet do 70% ogólnych nakładów na wytwarzanie systemu [1], niezbędne jest zastosowanie racjonalnej strategii testowania. Testowanie powinno z jednej strony dawać możliwości jak najwcześniejszego potwierdzenia poprawności rozwiązań, z drugiej – powinno koncentrować się na najważniejszych cechach jakościowych systemu. Dalej przedstawiono propozycję metodyki konstruowania planu testów dla systemu wbudowanego na

podstawie wyników analizy ryzyka i przyjęcia określonego zestawu kryteriów jakościowych. Niniejszy artykuł jest rozwinięciem koncepcji zaprezentowanej w [3].

Do przedstawienia procesów i przepływu dokumentów niezbędnych do opracowywania planu testów, zostały wykorzystane elementy metody strukturalnej projektowania systemów informatycznych. Elementy te, to przede wszystkim tabele IPO (ang. *Input–Process–Output*), diagramy przepływu danych (DFD – ang. *Data Flow Diagram*) oraz stosowane na nich oznaczenia procesów, przepływów i magazynów. Wybrane procedury realizacji procesów zostały zapisane w postaci pseudokodu (pkt. 4).

2. Komentarze do procesów wytwarzania planu testów

W dalszej części tego punktu podano komentarze do wybranych procesów wytwarzania planu testów. Uszczegółowienie niniejszego opisu stanowią procedury realizacji procesów, których specyfikację i przykłady zamieszczono w pkt. 4.

2.1. Wybór zbioru kryteriów jakościowych i ustalenie wagi poszczególnych kryteriów

To, czego oczekuje się od systemu nie tylko klasy sterowania, to jego „dobre" działanie: system ma działać w zakresie wykonywanych funkcji tak jak się tego oczekuje (spełniać wymagania funkcjonalne), być łatwym w obsłudze (spełniać wymagania niefunkcjonalne) oraz działać bezawaryjnie (spełniać wymagania niezawodnościowe). Zwykle w tym kontekście używa się terminu „jakość" – wymaga się, aby system był systemem o dobrej jakości. Według potocznego rozumienia jakość: *„...to wszystko, co jest związane z konkretnym produktem (systemem) i uszczęśliwia jego nabywcę"*. Żeby bardziej sprecyzować to nieprecyzyjne określenie, zostało sformułowanych wiele różnych zbiorów kryteriów jakości. Do najczęściej używanych należą:

1. Kryteria jakości według normy **ISO 9126**:
   - funkcjonalność;
   - łatwość użytkowania;
   - pielęgnowalność;
   - niezawodność;
   - efektywność;
   - przenośność.

2. Kryteria według firmy Hewlett-Packard (**FURPS**):
   - **F**unctionality – dostarczane funkcje i ich cechy,

- **U**sability – użyteczność: estetyka, spójność, dokumentacja itp.,
- **R**eliability – niezawodność,
- **P**erformance – wydajność,
- **S**upportability – pielęgnowalność, testowalność, zgodność itp.

3. Kryteria jakości **McCalla [4]**:

Kryterium	**Składowe kryterium**
Zgodność	kompletność, spójność, sprawdzalność
Niezawodność	precyzja, złożoność, spójność, odporność, modularność,
Efektywność	zwięzłość w liniach kodu źródłowego, szybkość działania, łatwość obsługi
Integralność	sprawdzalność, samodiagnozowanie, stopień ochrony danych i kodu
Pielęgnowalność	zwięzłość, spójność, samodiagnozowanie, samodokumentacja
Elastyczność	złożoność, zwięzłość, spójność, rozszerzalność, prostota,
Testowalność	sprawdzalność, złożoność, modularność, samodokumentacja
Przenośność	ogólność, niezależność od sprzętu i środowiska, samodokumentacja
Możliwość wielokrotnego użycia	ogólność, niezależność od sprzętu i środowiska, samodokumentacja
Współoperatywność	ogólność, jednorodność komunikacji i danych, modularność
Łatwość użytkowania	łatwość obsługi systemu, pomoc kontekstowa i samouczki

Wymienione kryteria jakości stosowane są najczęściej do oprogramowania. W przypadku wbudowanych systemów sterowania należy wziąć pod uwagę również część sprzętową systemu i ww. kryteria odpowiednio zinterpretować w tym kontekście. Przykładem może tutaj być np. *wydajność obliczeniowa* (jako wariant „efektywności" według ISO 9126 lub „wydajności" według HP), zależna nie tylko od składników programowych, ale przede wszystkim od elementów sprzętowych i architektury systemu. Określa ona potencjalne możliwości obliczeniowe systemu komputerowego znajdującego się w stanie zdatności użytkowej. Podstawowe miary wydajności obliczeniowej to:

- przepustowość (ang. *throughput*) – służy do przedstawiania szybkości przetwarzania lub przesyłania informacji w systemie komputerowym,

- czas odpowiedzi systemu (ang. *response time*),
- szybkość realizacji rozkazów (z listy rozkazów danego procesora – można ją traktować jako przepustowość ograniczoną do procesora, tzn. określa wydajność obliczeniową procesora, a nie całego systemu komputerowego).

Po wybraniu do praktycznego zastosowania któregoś z prezentowanych wcześniej zbiorów kryteriów[1], należy rozważyć:

1. Które z podanego zestawu kryteriów, zastosowane do konkretnego systemu, mają istotny wpływ na związane z tym systemem procesy biznesowe i środowisko.
2. Jaka jest względna „ważność" zidentyfikowanych kryteriów.

Wyniki mogą być przedstawione do dalszych działań np. tak jak w tabeli 1.

Tab. 1. Kryteria jakości i ich względne wagi (przykład)

Lp.	Kryterium jakości	Względna waga [%]
1	funkcjonalność	25
2	łatwość użytkowania	-
3	niezawodność	40
4	efektywność	25
5	przenośność	-
6	pielęgnowalność	10
	RAZEM:	100

Interpretacja zawartości tabeli 1 może być następująca: podczas sesji „burzy mózgów" z udziałowcami przedsięwzięcia typu „projekt nowego systemu wbudowanego X" stwierdzono że:

- dla procesów biznesowych oraz środowiska eksploatacji, związnych z wykorzystaniem systemu X, łatwość użytkowania i przenośność tego systemu są nieistotne,
- pozostałe kryteria mają względną ważność jak w tabeli 1.

2.2. Przypisanie ryzyka do komponentów systemu

Podczas realizacji zadań w ramach analizy bezpieczeństwa stosuje się

[1] W przykładzie opisywanym w [3] zostal wybrany zestaw kryteriów jakościowych podanych w ISO 9126.

zwykle klasyfikację zaproponowaną w standardzie RTCA DO-178B odnoszącą się do szkód ponoszonych na zdrowiu przez ludzi. Klasyfikacja ta obejmuje:

- klasyfikację ryzyk (używana m.in. w FMEA, por. tabela 2);
- klasyfikację częstości zdarzeń (por. tabela 3);
- klasyfikację szkód (por. tabela 4).

Wynikiem interpretacji danych zebranych w tabelach 2-4 może być przykładowa, zbiorcza tabela 5. Konkretna zawartość (tzn. rozstawienie klas ryzyk w takiej tabeli) w praktyce zależy od rodzaju projektu, sposobu użycia produktu, organizacji eksploatującej produkt itp.

Tab. 2. Klasyfikacja ryzyk

Lp.	Klasa ryzyka	Opis
1	**A**	Nietolerowane
2	**B**	Niepożądane, akceptowane tylko w przypadku gdy redukcja jest niepraktyczna
3	**C**	Tolerowane, w przypadku zgody komitetu przeglądu bezpieczeństwa projektu
4	**D**	Tolerowane, w przypadku zatwierdzenia podczas normalnego przeglądu projektu
5	**E**	Tolerowane w każdych warunkach

Tab. 3. Klasyfikacja częstości zdarzeń

Lp.	Opis częstości	Liczba wystąpień w czasie cyklu eksploatacyjnego
1	częste	10000×10^{-6}, możliwość występowania w sposób ciągły
2	prawdopodobne	100×10^{-6}, możliwość częstego występowania
3	okazjonalne	1×10^{-6}, możliwość okazjonalnego występowania
4	rzadkie	$0{,}01\times10^{-6}$ możliwość rzadkiego występowania
5	nieprawdopodobne	$0{,}0001\times10^{-6}$ niemożliwe, ale mogące się zdarzyć wyjątkowo
6	niewiarygodne	$0{,}000001\times10^{-6}$ wystąpienie zdarzenia wysoce niemożliwe

Tab. 4. Klasyfikacja szkód

Lp.	Kategoria	Opis
1	Katastrofalne	Wiele ofiar śmiertelnych

2	Krytyczne	Pojedyncze przypadki śmiertelne i/lub liczne przypadki zranień lub liczne przypadki chorób zawodowych
3	Duże	Pojedyncze przypadki zranień lub chorób zawodowych i/lub liczne przypadki niewielkich zranień lub niegroźnych chorób zawodowych
4	Małe	Pojedyncze przypadki niewielkich zranień lub niegroźnych chorób zawodowych
5	Nieznaczne	Brak szkód

Tab. 5. Związki ryzyka ze szkodami i częstością zdarzeń

Szkody → **Częstość ↓**	Katastrofalne	Krytyczne	Duże	Małe	Nieznaczne
częste	A	A	B	D	E
prawdopodobne	A	A	B	E	E
okazjonalne	A	B	C	E	E
rzadkie	A	B	C	E	E
nieprawdopodobne	B	C	D	E	E
niewiarygodne	C	D	D	E	E

3. Specyfikacja dokumentów związanych z procesem przygotowywania planu testów

W tym punkcie metodą IPO (ang. *Input-Process-Output*) wyspecyfikowano dokumenty związane z procesem przygotowywania planu testów. Na końcu punktu, w tabeli 6, są zebrane dokumenty wytwarzane podczas przygotowywania planu testów (robocze oraz dokument wynikowy - plan testów) oraz niezbędne dokumenty wejściowe.

3.1. Tabele IPO

Objaśnienia do tabel IPO:

1. Symbol (*) przy numerze procesu oznacza, że proces ten jest dekomponowany na podprocesy.
2. Czcionką pogrubioną są zaznaczone podstawowe dokumenty wynikowe procesu przygotowania planu testów.

Wejście	• Opis systemu
Nr procesu	**1**
Proces	**Identyfikacja komponentów systemu**
Wyjście	• Lista komponentów

Wejście	• Opis systemu • Zbiór kryteriów jakości
Nr procesu	**2**
Proces	**Ustalenie wagi kryteriów jakości**
Wyjście	• Lista kryteriów jakości z wagami

Wejście	• Lista komponentów
Nr procesu	**3***
Proces	**Przypisanie ryzyk do komponentów**
Wyjście	• Lista ryzyk dla komponentów

Wejście	• Lista komponentów • Lista kryteriów jakości z wagami
Nr procesu	**4**
Proces	**Ustalenie związków komponentów z kryteriami jakości**
Wyjście	• Lista kryteriów jakości dla komponentów

Wejście	• Lista komponentów
Nr procesu	**5**
Proces	**Ustalenie istotności komponentów**
Wyjście	• Lista istotności komponentów

Wejście	• Lista kryteriów jakości dla komponentów • Lista istotności komponentów • Lista ryzyk dla komponentów • Lista kryteriów jakości z wagami

Nr procesu	**6**
Proces	**Ocena wpływu komponentu na kryterium jakości**
Wyjście	• Lista wartości wpływu komponentu na określone kryterium jakości

Wejście	• Lista wartości wpływu komponentu na określone kryterium jakości
Nr procesu	**7**
Proces	**Opracowanie planu testów**
Wyjście	• **Plan testów**

Tab. 6. Wykaz dokumentów przedsięwzięcia wytwarzania planu testów

Lp.	**Nazwa dokumentu**	**Status dokumentu**
1	Opis systemu	wejściowy
2	Zbiór kryteriów jakości	wejściowy
3	Lista komponentów	*roboczy*
4	Lista kryteriów jakościowych z wagami	*roboczy*
5	Lista kryteriów jakości dla komponentów	*roboczy*
6	Lista ryzyk dla komponentów	*roboczy*
7	Lista istotności komponentów	*roboczy*
8	Lista wartości wpływu komponentu na określone kryterium jakości	*roboczy*
9	**Plan testów**	**wyjściowy**

UWAGA
Nazwy dokumentów wypisane pogrubioną czcionką oznaczają dokumenty końcowe przedsięwzięcia.

3.2. Diagramy przepływu danych

Ze względu na ograniczone ramy artykułu, w dalszej części jest

przedstawiony tylko diagram DFD poziomu 1 (nie są pokazane rozwinięcia procesów złożonych). Na podstawie tego diagramu można:

1) ocenić złożoność procesów składających się na przygotowanie planu testów,
2) prześledzić zależności pomiędzy dokumentami wytwarzanymi w tych procesach,
3) ocenić na podstawie zależności pomiędzy procesami możliwości równoległej realizacji zadań.

Interpretacja symboli używanych na diagramie DFD jest przedstawiona w załączniku.

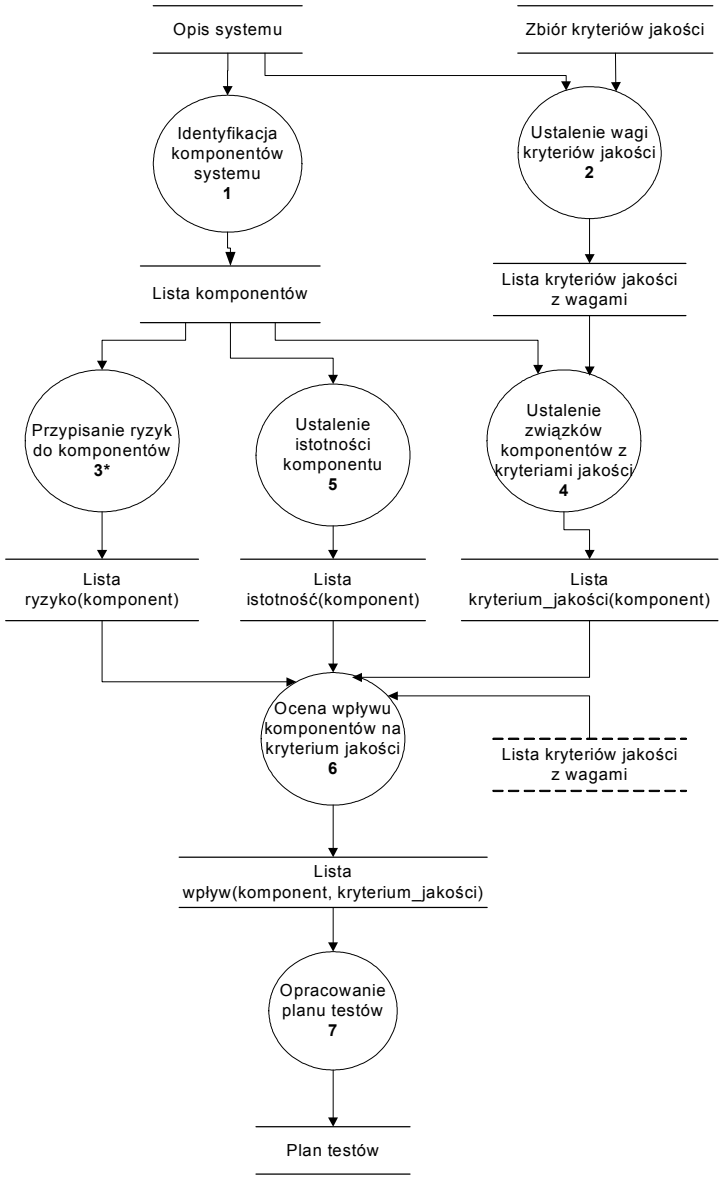
Przedstawiony diagram jest pomocny przy ustalaniu harmonogramu opracowania planu testów oraz pozwala ocenić stopień złożoności przedsięwzięcia oraz niezbędne zaangażowanie w tym przedsięwzięciu zasobów (głównie w postaci ekspertów dziedzinowych). Diagramy (i metodyka jako całość) znacznie wspomagają wycenę prac związanych z testowaniem.

4. Procedury realizacji procesów przedsięwzięcia opracowania planu testów

Z realizacją każdego z procesów wyspecyfikowanych w punkcie 3.1 związane są określone procedury:

1. **Proc(komp_)** – procedura określenia struktury istotnych komponentów systemu wbudowanego, dla którego jest opracowywany plan testów (proces 1).
2. **Proc(waga_kj)** – procedura ustalania wagi kryteriów jakościowych odnoszonych do systemu wbudowanego, dla którego jest opracowywany plan testów (proces 2).
3. **Proc(ryzyko)** – procedura określania ryzyka związanego z konkretnym komponentem systemu wbudowanego (proces 3).
4. **Proc(związki)** – procedura ustalania związku komponentów systemu wbudowanego z kryteriami jakości (proces 4).
5. **Proc(istotność_komp_)** – procedura ustalania istotności komponentów systemu wbudowanego w realizacji zadań tego systemu (proces 5).
6. **Proc(ocena_wpływu)** – procedura określania wpływu komponentu na konkretne, wybrane kryterium jakości (proces 6).
7. **Proc(plan_testów)** – procedura ustalania planu testów (proces 7).

Dalej, jako przykład sposobu realizacji i proponowanej notacji, zostaną przedstawione dwie procedury: Proc(ryzyko) i Proc(plan_testów).



Rys. 1. Diagram DFD_1 przedsięwzięcia sterowanego ryzykiem opracowania planu testów

4.1. Proc(ryzyko)

Dane wejściowe procedury:

- lista komponentów K $(K = \{k_i \mid i \in 1,...,l\})$,
- lista przyjętych kryteriów jakości Ξ $(\Xi = \{\xi_i \mid i \in 1,..., p\})$ oraz lista odpowiadających im wartości w_i $(0 < w_i \leq 1, i \in 1,..., p)$, określających względny wpływ na jakość.

Dane wyjściowe procedury:

- lista par ⟨ komponent k_i $(k_i \in K)$, ryzyko $r(k_i)$ ⟩.

Oznaczenia:

- $Z = \{z_i \mid i \in 1,..., m\}$ – zbiór niekorzystnych zdarzeń tzn. takich, które mogą wpływać na niepoprawne działanie systemu lub obniżać jakość systemu względem przyjętych kryteriów jakości,
- $G =< V, U >$ – graf zwykły (dwudzielny), w którym $V = Z \cup K$ stanowi zbiór węzłów $(Z \cap K = \varnothing)$, a U jest zbiorem krawędzi ($(z_i, k_j) \in U \Leftrightarrow$ gdy zdarzenie z_i może dotyczyć komponentu k_j),
- G^* – graf opisany: $G^* = \langle G(V,U); \{r(u) : u \in U\}\rangle$ taki, że $\forall u = (z_i, k_j) \in U : r(u) = r(z_i)$ oraz $r(z_i) \in \{A, B, C, D, E\}$ (wg tab. 5).

POCZĄTEK Proc(ryzyko)

POWTARZAJ dla wszystkich $\xi_i \in \Xi$:

1. Określ zbiór zdarzeń niekorzystnych $Z(\xi_i)$, dotyczących kryterium ξ_i.
2. Ustal podzbiór komponentów systemu $K(\xi_i)$, powiązanych ze zdarzeniami ze zbioru $Z(\xi_i)$.
3. Dla każdego zdarzenia $z_i \in Z(\xi_i)$:

   3.1. Oceń realną możliwość zajścia każdego zdarzenia z_i *(„częstość" wg tab. 3),*

   3.2. Zidentyfikuj skutki (*straty wg tab. 4*) dla związanych procesów biznesowych i środowiska (w tym ludzi), jakie może przynieść

niepoprawne działanie systemu związane ze zdarzeniem z_i, 3.3. Określ *na podstawie tab. 2 i tab. 5 oraz wyników pkt. 3.2.* klasę ryzyka $r(z_i)$ ($r(z_i) \in \{A, B, C, D, E\}$) zdarzenia z_i.

4. Zbuduj graf G^*, w którym $V = Z(\xi_i) \cup K(\xi_i)$ i $\forall u \in U, (u = (z_i, k_j)) : r(u) = r(z_i)$.
5. Określ ryzyko komponentów $k_j (k_j \in K)$ w następujący sposób: $\forall k_j \in K(\xi_i) : r(k_j) = \max_{z_i:(z_i,k_j)\in U} (r(z_i, k_j))$.

KONIEC Proc(ryzyko).

4.2. Proc(plan_testów)

Dane wejściowe procedury:

- lista (⟨ kryterium_jakości ξ_i ($\xi_i \in \Xi$), wpływ $w_i (0 < w_i \leq 1)$ ⟩),
- lista (⟨ kryterium_jakości ξ_i, komponent k_j $(k_j \in K)$, istotność $\mu(k_j)$ ⟩).

Należy zaznaczyć, że istotność komponentu $\mu(k_j)$ ($\mu(k_j) \in \{5, 4, 3, 2, 1\}$) wyznaczana jest na podstawie uzyskanej oceny ryzyka $r(k_j)$, przykładowo, $\mu(k_j) = 5 \Leftrightarrow r(k_j) = A$.

Dane wyjściowe procedury: plan testów.

Oznaczenia:

- $\vec{\Xi} = \langle \xi_i : i \in 1, ..., p \rangle$ – uporządkowany zbiór kryteriów jakości według ich wag tj. $(\forall i, j \in 1, .., p : i < j) \Rightarrow w_i \geq w_j$,
- obszar testowania o istotności s: $O^s(\xi_i) = \{k_j : k_j \in K(\xi_i) \wedge \mu(k_j) = s\}$ - podzbiór takich komponentów związanych z kryterium jakości ξ_i, dla których wyznaczona istotność ma wartość s.

POCZĄTEK Proc(plan_testów)

POWTARZAJ kolejno dla wszystkich $\xi_i \in \vec{\Xi}$ ($i = 1, 2, ..., p$):

1. Opracuj testy dla kryterium jakości ξ_i:

   POWTARZAJ dopóki $K(\xi_i) \neq \varnothing$:

   1.1. Wyznacz obszar testowania $O^s(\xi_i)$ o największej istotności (wartości *s*),

   1.2. Przygotuj testy dla komponentów $k_j \in O^s(\xi_i)$,

   1.3. Podstaw $K(\xi_i) \leftarrow K(\xi_i) \setminus O^s(\xi_i)$.

KONIEC Proc(plan_testów).

5. Podsumowanie

W artykule przedstawiono zarys sterowanej ryzykiem metodyki testowania systemów wbudowanych. Podstawową zaletą prezentowanej metody jest jej prostota. Wystarczy identyfikacja zagrożeń i oszacowanie związanego z nimi ryzyka oraz ustalenie wagi kryteriów jakościowych oraz istotności i wpływu komponentów, aby opracować plan testów. Alternatywą jest wykonanie pełnej analizy ryzyka, czyli (używając np. drzewa błędów) znalezienie przyczyn każdego możliwego niekorzystnego zdarzenia i na tej podstawie dopiero projektowanie testów.

Obecnie prowadzone są prace nad uszczegółowieniem metodyki. Przewiduje się także opracowanie oprogramowania wspierającego zaprezentowaną metodykę.

Literatura

[1] Broekman B., Noteboom E.: *Testing Embedded Software*, Addison-Wesley, 2003.

[2] Liderman K.: *Zarządzanie ryzykiem jako element zapewniania odpowiedniego poziomu bezpieczeństwa teleinformatycznego*, Biuletyn ITA. Nr 23. Warszawa, 2006.

[3] Liderman K., Zieliński Z.*: Sterowana ryzykiem strategia testowania systemów wbudowanych*, W: materiałach konferencji „Systemy Czasu Rzeczywistego". Karpacz, 2007.

[4] Pressman R.S.: *Praktyczne podejście do inżynierii oprogramowania*, WNT. Warszawa, 2004.

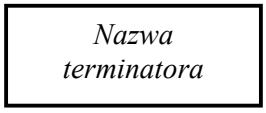
[5] PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania*.

[6] IEC 61508:1995: *Functional Safety: Safety-Related Systems*.

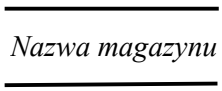
ZAŁĄCZNIK

SYMBOLE GRAFICZNE NA DIAGRAMIE DFD

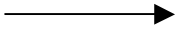
symbol **procesu** na DFD



symbol **terminatora**, tj. elementu zewnętrznego w stosunku do procesów opisywanych za pomocą DFD.



symbol **magazynu**, tj. elementu mogącego gromadzić dane (dokumenty lub inne, zależne od modelowanego kontekstu, elementy)



symbol **przepływu** danych (dokumentów, informacji itd.) pomiędzy elementami DFD

UWAGA!

Symbole graficzne procesów i magazynów rysowane na diagramach DFD linią przerywaną oznaczają procesy i magazyny powielone, tzn. są to te same procesy i magazyny co narysowane linią ciągłą, tylko umieszczone jeszcze raz na diagramie w celu uzyskania lepszej przejrzystości (unika się niepotrzebnego, zaciemniającego diagram, rysowania przepływów).

Methodology of developing a risk-based test strategy for embedded systems

ABSTRACT: In the paper the methodology of developing a risk-based test strategy for embedded systems is proposed. The methodology is based on risk analysis results and quality criteria of the system being tested. The outline of basic procedures is depicted.

KEYWORDS: risk, test plan, embedded systems

Recenzent: dr hab. inż. Antoni Donigiewicz

Praca wpłynęła do redakcji: 15.10.2007 r.