Metoda FMEA v softwarovém inženýrství

Branislav Lacko

VUT Fakulta strojní, Ústav automatizace a informatiky, Technická 2, 616 69 Brno, Česká Republika

Motto: "Máš smrtelný hřích ty blůmo!"
"Proč?", otázal se Čeněk Jirsák.
Pravil jsem: " Protože když se skáče
se stráně na traf, tak je to opovážlivé spoléhání na milost Boží."
(K.Poláček: Bylo nás pět)

Abstrakt
Příspěvek vysvětluje principy a účel metody FMEA pro oblast softwarového inženýrství. Poukazuje na nutnost využít této metody pro zvýšení jakosti programových produktů a pro zvýšení jakosti procesu, při kterém jsou programové moduly vytvářeny.

1. VŠEOBECNĚ O FMEA

Metoda FMEA - Failure Mode and Effect Analysis představuje základní metodu pro řízení jakosti v procesech návrhu k preventivnímu ošetření potenciálních vad výrobů a poruch procesů. Jak napovídá doslovně přeložený název jedná se o analýzu projevů, důsledků a závažnosti poruch. Metoda byla původně vyvinuta pro kosmický výzkum, ale její úspěšnost způsobila následné rozšíření do jiných odvětví průmyslu (letectví, automobilový průmysl, elektrotechnický průmysl, zbrojní průmysl atd.). Např. v automobilce firmy FORD byla rozpracována pro konkrétní potřeby firmy a je standardně používána při návrhu všech modelů automobilů této firmy. Metoda má dvě modifikace:

FMEA-D modifikace pro potřeby procesu návrhu výrobku, kdy se uplatňuje v rámci fáze hodnocení procesu návrhu tzv. DESIGN REVIEW.
FMEA-P modifikace pro potřeby vyhodnocení konkrétního produktu.

Všeobecně se prokázala metoda své následující výhody:

1. Pomáhá v počáteční fázi projektu s vysokou spolehlivostí a vysokou bezpečností při výběru různých možností návrhu.
2. Zajišťuje, že budou vzaty v úvahu všechny případné chyby a jejich vliv na správnou funkci vyvýjeného produktu.
3. Uvádí všechny možné chyby a identifikuje relativní velikost jejich účinku.
4. Je základem pro testování během vývoje a konečného hodnocení produktu.
5. Vytváří prvotní kritéria pro všechny fáze (návrh, implementace, testování, přejímání, provoz, údržba, servis.
6. Poskytuje dokumentaci pro analýzu chyb v praxi a bere v úvahu možné změny v průběhu projektu
7. Vytváří podklady pro organizaci změnového řízení
8. Způsobuje, že se uvažuje o prevenci selhání návrhového procesu a produktu již v počátečních fázích projektu.

Hledáme-li metody, podporující zajištění vysoké jakosti software, je metoda FMEA jednou z možných technik, které můžeme použít. Následující text je rámcovým návrhem aplikace metody FMEA pro potřeby softwarového inženýrství. Proto je příspěvek koncipován tak, že popisuje dále jednotlivé části metody FMEA tak, že obecné zásady přizpůsobuje potřebám softwarového inenýrství.

2.TÁMOVÁ PRÁCE

Metoda FMEA využívá důsledně přednosti týmové práce. Pro zajištění činností, které vyžaduje musí být sestaven tým odborníků z různých specialistů, aby se zajistil komplexní systémový přístup k řešeným problémům.

Pro modifikaci FMEA-D jsou to pracovníci, kteří se podílejí na jednotlivých fázích projektu:
- zástupce marketigu firmy,
- zástupce analytiků,
- zástupce systémových programátůrů,
- zástupce aplikačních programátonů,
- zástupci dodavatelů technických komponent,
- zástuupce testovací skupiny,
- zástupce instalačního servisu,
- další specialisté podle potřeby.

Pro modifikaci FMEA-P jsou to pracovníci, kteří rozumí jednotlivým komponentám programového produktu:
- zástupci, reprezentující požadavky zákazníka,
- zástupci marketingu,
- zástupci jednotlivých aplikačních modulů,
- zástupci jednotlivých systémových komponent (operační systém, databázový systém, síťový systém, sandardní a servisní programy, vývojové prostředí včetně použitého kompilátoru programovacího jazyka),
- zástupci dodavatelů technických komponent,
- další specialisté podle potřeby.

Týmy by měly pracovat podle zásad a metod týmové práce. Zde je nutno upozornit, že v Čechách tyto zásady a metody nejsou příliš známy což způsobuje, že týmy jsou sestaveny nevhodně, nemají vytvořeny příznivé podmínky pro svoji práci a nepoužívají metod, které by jim umožnily ve skupinách efektivně nalézat optimální řešení zadaných problémů [4,5].

3. PŘEDMĚT POZORNOSTI FMEA

Jak již bylo řečeno v modifikaci FMEA-D analyzujeme možnosti poruchy programového produktu, které mohou být zaviněny použitým procesem návrhu, implementace a dodávky. Proto předmětem pozornosti jsou:
- použité vývojové prostředí,
- použité ladící a testovací prostředky,
- použitá metoda návrhu software,
- jednotliví pracovníci, podílející se na vývoji,

- použité technické prostředky,
- atd.

V případě modifikace FMEA-P jsou to jednotlivé moduly navrženého produktu včetně použitých jiných komponent (standardní programy, nakoupené programy, základní operační software atd.).

V obou případech můžeme seznam potřebných komponent získat např. aplikací kauzálních diagramů (tzv. Ishikawových diagramů) [1].

4. OBECNÉ K POSTUPU FMEA

Metoda má stanovený doporučený postup, který vychází z určitých zásad. Zásady a postup jsou specifikovány pro každou modifikaci tj. FMEA-D a FMEA-P zvlášť. Se zásadami a postupem jsou svázány určité základní pojmy, které jsou předem definovány. S těmi je potřeba se důkladně seznámit, protože některé odborné termíny neodpovídají zcela přesně termínům, jak jsme zvyklí z ČSN (např. porucha, typ poruchy apod.) Podrobný popis všeho by přesáhl rozsah příspěvku. Proto budou uvedeny jen hlavní zásady a stručně komentován doporučený postup.

4.1 Zásady postupu FMEA-P

Protože se FMEA-P provádí v době, kdy konkrétní programový produkt je teprve ve stádiu stanovení cílů a specifikace plánovaných funkcí, nemůžeme se opírat o výsledky sledování provozní spolehlivosti produktu. Proto se snažíme stanovit poruchy, které mohou nastat vynecháním nebo špatným fungováním plánovaných funkcí. Navíc se snažíme využít informací o poruchách jiných, podobných produktů, které máme k dispozici z minulých záznamů o spolehlivosti. K tomu je potřeba si uvědomit:

a) Každý produkt resp. jeho dílčí část musíme uvažovat jako součást nějakého vyššího systému, přičemž se často nemůžeme omezit jen na jediný vyšší systém, protože porucha v jednom z nich může mít v druhém nepříznivý důsledek.
b) K analýze jednotlivých subsystémů a nižších komponent přistupujeme v tom pořadí, v jakém jsou významné pro daný programový produkt.

4.2 Zásady postupu FMEA-D

Zásady jsou orientovány na analýzu možných poruch v procesu návrhu, které následně mohou znamenat, že výsledný produkt vývojového procesu bude obsahovat chyby:

a) Analyzujeme vždy jeden souvislý řetězec činností, jehož výsledkem je určitá část programového produktu. Protože každý takový postup je součástí nějakého jiného, nadřazeného postupu, uvádíme tyto souvislosti s cílem, podrobit analýze i tento proces.
b) Postupujeme od nejsložitějších postupů k nejjednoduš-
c) ším, přičemž zvažujeme i důležitost a cenu částí produktu, které proces produkuje
d) Využíváme poznatků z minulosti o problémech, které používaný postup přinášel a ohledem na dopady na špatné funkce minulých programových produktů.

4.3 Konkretizace postupů FMEA-D a FMEA-P

Vlastní postup je dán jednak podrobnými popisy činností, které je potřeba vykonat, jednak jsou doporučeny určité techniky, které se mají používat. Celý postup se opírá o formuláře, do kterých se zapisuje celý průběh metody FMEA (v podmínkách počítačové éry se může jednat o soustavu předdefinovaných obrazovek, které je nutno na počítači vyplnit).

Formuláře obsahují:
- souhrnné identifikační údaje o konkrétním produktu (části, komponentě) nebo o procesu návrhu (jednotlivém řetězci návrhových činností),
- charakteristiku současného stavu,
- charakteristiku cílového stavu,
- činnosti zajišťující dosažení cílového stavu,
- zodpovědnost za provední potřebných činností,
- další organizační a pomocné údaje.

Právě zde je nutno přizpůsobit metodu konkrétní firmě, konkrétní oblasti kterou představuje produkt nebo proces, který ho produkuje. Každá firma zde používá vlastní firemní formláře, pro které jsou sestaveny podrobné pokyny, jak se mají vyplňovat.

5. ZÁVĚR

Na závěr si položme otázku, inspirovanou mottem na začátku příspěvku:
"Na co resp. na koho spoléhají naše softwarové firmy, když žádné exaktní metody pro podporu zvýšení spolehlivosti svých programových produktů nepoužívají?"

Požadavky na zvýšenou jakost programových produktů nutně zamenají pro naše softwarové firmy potřebu hledat metody, které jim umožní jakostní software dodávat na softwarový trh.

Metoda FMEA je jednou z nabízených možností. Je zajímavé, že se zatím nepodařilo zjistit softwarovou firmu u nás, která by tuto metodu používala. Podstatná většina softwarových firem ani o ní neslyšela. Na druhé straně je v ČR řada firem v jiných průmyslových oborech, které metodu s úspěchem používají (MESIT Uh. Hradiště, ČZ Strakonice aj.).

Na druhé straně je potřeba konkretizovat metodu FMEA v obou jejích modifikacích pro potřeby softwarového inženýrství tak, aby ji softwarové firmy mohly rychle a bez obtíží zavést.

Na VUT v Brně Fakultě strojní byla dohodnuta spolupráce dvou ústavů - Ústavu automatizace a informatiky a Ústavu jakosti procesů - na konkretizaci této metody pro oblast softwarového inženýrství. Cíle spolupráce je zpracovat metodický materiál podporující kurs, který by obsahoval:
- Všeobecné údaje o metodě FMEA,
- Konkretizaci obou modifikací (FMEA-D, FMEA-P) do oblasti softwarového inženýrství,
- Postup, jak zavést metodu v softwarové firmě,

- Podpůrné materiály (číselníky, třídníky, apod).
- Návrh na počítačovou podporu metody.

Obě pracoviště jsou přesvědčena, že metoda FMEA může dobře podpořit zvýšení jakosti programových produktů produkované českými firmami.

LITERATURA:

[1] Ishikawa,K.: Guide to Quality Control. New York 1985
[2] Olexa,J.: Metoda FMEA. Praha 1990
[3] Čech,J.: Statistické řízené jakosti. Skriptum VUT Fakulty strojní, Brno 1990
[4] Adair,J.: Vytváření efektivních týmů. Management Press, Praha 1994
[5] Robson,M.: Skupinové řešení problémů. Victoria Publishing, Praha 1995