

Riziká softvérových projektov

PETER ŠIMNO

*Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
stalker0@centrum.sk*

Abstrakt. Softvérový priemysel je pomerne mladé, ale dynamicky sa rozvíjajúce odvetvie. Podobne, ako manažment riadiaci ostatné odbory ľudskej činnosti, aj manažment v softvérovom inžinierstve sa musí potýkať s rizikami počas celého procesu vývoja produktu. Každý manažér by ich mal vedieť v rámci svojho projektu identifikovať, predchádzať im a pokiaľ predsa len nastanú, vedieť minimalizovať škody. V opačnom prípade hrozia firme straty, či už peňažné alebo morálne v očiach zákazníkov. Táto esej si kladie za cieľ poukázať, čo to vlastne riziko je, aké druhy rizík v procese tvorby softvéru nastávajú a aké majú dopady na projekt. Ďalej je spomenutý prehľad najčastejších príčin vzniku rizík a ich kategorizácia.

Úvod

Pravdepodobne najznámejší Murphyho zákon znie: „čo sa môže pokaziť, to sa aj pokazí“. Je natoľko univerzálny, že sa mu nevyhýba ani oblasť softvérového inžinierstva. V praxi má za následok omeškanie, v horšom prípade neodovzdanie finálneho produktu zákazníkovi.

Doba, kedy sa softvér vyrábal „v garáži“ a predával za nevelké finančné obnosy je dávno preč. Dnešné výdavky na informačné systémy sa šplhajú do astronomických výšok. Nemenej ohromujúce sú potom aj vynaložené prostriedky na neúspešné projekty. Napríklad [2] uvádza, že v roku 1998 bolo zbytočne investovaných 1,5 miliardy dolárov na neúspešný projekt automatického systému pre americké ministerstvo dopravy. Podobných príkladov možno nájsť viacero. Štatistiky z roku 2001 udávajú, že až 70% projektov je odovzdaných zadávateľovi neskoro, za väčšie náklady, s menšou funkcionalitou alebo neodovzdaných vôbec.

Čo všetko sa môže pokaziť v procese tvorby softvérového produktu? Povedzme si úprimne, skoro všetko. Neznamená to ale, že je to úplne neriešiteľný problém. Práve naopak. Analýza rizík napomáha odhaľovať hlavné príčiny vzniku problémov a ich dopady. Manažment rizík vychádza z týchto znalostí a snaží sa im predchádzať, poprípade minimalizovať straty. Nad tým, aké problémy môžu vzniknúť, čo to vlastne analýza rizík a vôbec riziko je, by som sa rád zamyslel ďalej.

Manažment v softvérovom inžinierstve, október 2006, s. 1-9.

Čo to je riziko

Riziko môžeme definovať ako *možnosť výskytu nepriaznivej udalosti alebo udalostí, ktoré by mali za následok ohrozenie našich cieľov*. Hodnota rizika (V) je podľa [3] určená nasledovným vzťahom

$$V(A) = P(A) * C(A) \quad (1)$$

v ktorom $P(A)$ predstavuje pravdepodobnosť, že udalosť A nastane a $C(A)$ znamená cenu nákladov (dopadu). Hodnota rizika vlastne ukazuje priemerné očakávané straty, ktoré nastanú.

Vzťah (1) je pomerne jednoduchý a intuitívny pre malý počet možných udalostí. Pri komplexnejších problémoch ale nemusí stačiť, pretože problematické udalosti môžu na seba nadväzovať a vzájomne sa ovplyvňovať, čo vyžaduje poznať mieru ich podmienených pravdepodobností. Hodnota rizika sa potom vyjadruje zložitejšími vzťahmi.

Aké riziká ale môžu nastať? Podľa [2] existujú nasledovné druhy rizík týkajúce sa softvéru:

1. zlyhanie softvérového projektu, ktoré má za následok finančné alebo časové straty spoločnosti, a teda zle využitú (nevyužitú) obchodnú príležitosť
2. zlyhanie softvérového systému, ktoré môže viesť k ohrozeniu bezpečnosti a zdravia ľudí alebo okolitého prostredia
3. zlyhanie softvérového systému, ktoré má za následok únik informácií alebo poškodenie integrity systému útočníkom

Posledné dva body predstavujú bezpečnostné riziká a spadajú pod manažment bezpečnosti v IT. Rád by som sa teda zamerlal na bod prvý a popísal bližšie procesy z oblasti manažmentu rizík v softvérovom projekte.

Princípy manažmentu rizík

Nedá sa dobre manažovať niečo, o čom vieme málo alebo nič. Takisto platí, že teoretické znalosti sú dobré, ale je žiaduce ich uplatniť aj v praxi. Preto idú analýza a manažment rizík spolu ruka v ruke nadväzujúc na seba.

Vychádzajúc z princípov uvedených v [2] zistíme, že určenie rizík prebieha v nasledovnej sekvencii:

- *identifikácia rizík* – jednoznačné určenie aké riziká sú pre úspech projektu významné (určenie rizikových scenárov)
- *analýza rizík* – vyhodnotenie informácií získaných v predošlom bode za účelom posúdenia závažnosti identifikovaných rizík a ich zoradenia podľa váhy

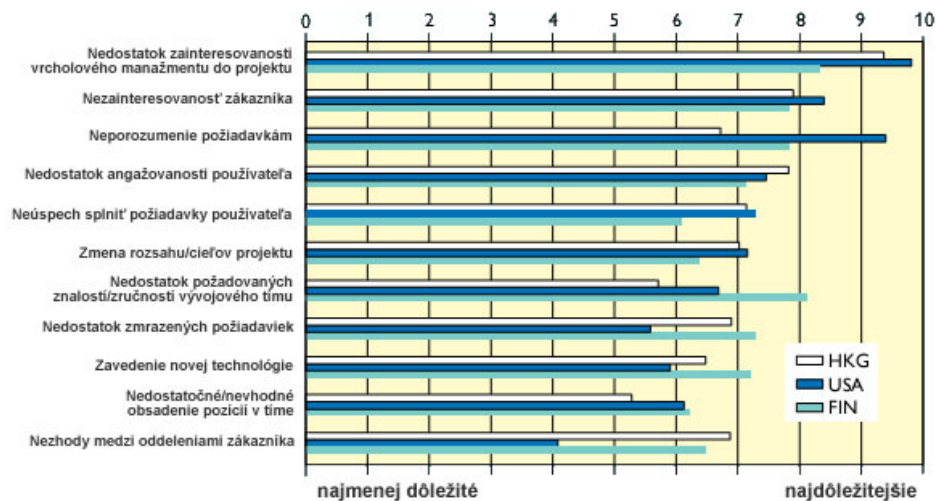
- *vyhodnotenie rizík* – posúdenie váh rizík podľa zvolených kritérií a určenie zostatkových rizík (t.j. takých, ktoré sme schopný akceptovať a nezaoberať sa nimi)

Zmiernenie rizík zahŕňa nasledovné aktivity:

- *plánovanie kontrolných opatrení* – plánovanie prostriedkov za účelom predchádzaniam rizikám a taktiež opatrení na navrátenie do normálneho stavu procesu
- *implementácia kontrolných opatrení* – vykonanie preventívnych úloh naplánovaných v predošlom bode
- *monitorovanie* – kontrola efektívnosti vykonávaných úloh, kontrola plnenia plánu a posudzovanie súčasného stavu rizík
- *regulovanie* – riadenie rizík spočívajúce v nasadzovaní prostriedkov, ktoré by im mali predchádzať
- *poučenie z rizík* – zaznamenávanie skúseností z procesu riadenia rizík ako aj z účinnosti nasadených prostriedkov do akejsi bázy znalostí, z ktorej budeme v budúcnosti znovu vychádzať

Najčastejšie príčiny neúspechu

Stále sme si však neukázali, aké konkrétne rizikové faktory sa v procese tvorby softvéru vyskytujú. Ktoré z nich vnímajú projektoví manažéri ako riziká a ktoré považujú za najdôležitejšie? Na tieto otázky sa zamerala štúdia [1]. Zachytáva skúsenosti softvérových manažérov z Fínska, Hong Kongu a Spojených štátoch amerických, pričom bola využitá metóda Delphi. Výsledky sú uvedené na Obr. 1.



Obr. 1 – výsledky štúdie rizík a ich dôležitosti [1]

Zo štúdie vyplývajú zaujímavé dôsledky. Je tu badať istá univerzálnosť. Pri identifikovaní a ohodnotení rizikových faktorov projektoví manažéri z troch rozdielnych oblastí sveta identifikovali tie isté faktory a to v približne rovnakom poradí. Toto zistenie dáva možnosť zamyslieť sa, či je možné vytvárať akési globálne kategórie jednotlivých rizík.

Ďalej by som rád priblížil niekoľko najkritickejších faktorov vyplývajúcich zo štúdie.

Nezainteresovanosť zákazníka

Patrí sem najmä riziko nezainteresovanosti zákazníka v procese analýzy a špecifikácie požiadaviek. Pokiaľ zákazník len zadá úlohu a nenájde v svojich ľudských zdrojoch kompetentnú osobu, ktorá bude aktívne komunikovať pri procese tvorby špecifikácie, hrozí, že špecifikácia bude neúplná alebo dokonca úplne nevhodná. Na jej základe sa potom vybuduje systém, ktorý si zákazník – jeho používateľ – predstavoval ináč. Nasleduje prerábanie, a teda ďalšie časové zdržanie a nespokojnosť zákazníka.

Neporozumenie požiadavkám

Neporozumenie požiadavkám čiastočne súvisí aj s predošlým bodom. Bez stopercentnej analýzy a špecifikácie požiadaviek nemôže vzniknúť dobrý produkt. Bez požiadaviek by nevzniklo zadanie a ak sú požiadavky nesprávne pochopené, vzniká produkt, ktorý síce môže fungovať správne, ale len ak za správne považujeme chovanie, aké zákazník vlastne nechcel.

Nedostatok angažovanosti používateľa

Znova je tu istý súvis s prechádzajúcim. Projekt síce zadáva zákazník, ale málokedy je to konkrétna osoba. Zvyčajne je to právnická osoba – firma, ktorej zamestnanci vystupujú v rolích konkrétnych používateľov. Avšak tí môžu byť z tohto procesu vynechaní a postavení až pred hotový produkt. Takto vznikajú problémy s použiteľnosťou, neprehľadnosťou systému, ale aj so zavádzaním dodatočnej funkcionality. Nepatrná dodatočná zmena v programe z pohľadu používateľa totiž môže znamenať veľkú zmenu v systéme, nečakanú nutnú optimalizáciu a podobne.

Neúspech splniť požiadavky používateľa

Toto riziko je tiež pomerne časté. Používateľ má na vytváraný systém určité nároky a požiadavky. Tie sa môžu častokrát javiť ako prehnané, alebo zbytočné. Pokiaľ ich však nedostane, nemusí byť spokojný.

Druhá strana mince ale je, že mnohokrát ani používateľ sám nevie, čo chce. Prípadne požaduje veci, ktoré by príliš komplikovali projekt a zvyšovali náklady. Vtedy je na mieste ponúknuť prijateľné alternatívy. Platí veta: „robme to, čo používateľ chce, nie to, čo hovorí, že chce“. Vedieť správne zobrať do úvahy obe strany tejto mince ale nie je zvyčajne jednoduché.

Zavedenie novej technológie

Je zaujímavé, že je to jediný rizikový faktor vyplývajúci zo štúdie, ktorý pojednáva o použitej technológii. Inými slovami vyjadruje vetu Dana Stearnsa: „Don't use new tools on new projects!“ (nepoužívajte nové nástroje na nové projekty).

Pri ich použití je tu totiž vždy určité riziko, že spôsobia spočiatku istú eufóriu z novej technológie, ktorú neskôr určite vystrieda odhalenie limít a obmedzení nového nástroja. Preto by mali byť pred zavedením akejkoľvek novej technológie s ňou všetci úplne oboznámení a to hlavne vrátane jej nevýhod.

Kategorizácia rizík

V predchádzajúcej časti bola načrtnutá otázka, či riziká možno zaradiť do určitých kategórií. Vystavenie sa riziku je možné odhadnúť z dvoch aspektov:

- pravdepodobnosť výskytu
- spôsobené škody (alebo dopad)

Nepoužíva sa číselná škála kategorizácie, ale slovná a zakresľuje sa v tzv. matici rizík (matica pravdepodobnosti a dopadu). Dá sa popísať rôzne (napr. invertovaná matica), ale výsledný zmysel zostáva rovnaký. Príklad matice je znázornená na Obr. 2.

Riziko		Škody			
		Katastrofické	Vysoké	Mierne	Nízke
Pravdep.	Veľmi pravdepodobné	Katastrofické	Vysoké	Mierne	Nízke
	Pravdepodobné	Vysoké	Mierne	Nízke	Okrajové
	Nepravdepodobné	Mierne	Nízke	Okrajové	Okrajové

Obr. 2 – príklad matice rizík [2]

Vidíme, že okrajové riziká predstavujú hrozby s malou pravdepodobnosťou a dopadom, zatiaľ čo kritické až katastrofické riziká majú vysokú pravdepodobnosť a dopad.

Takéto delenie má ale aj svoje nevýhody. Jednou z nich je aj zvolená škála, ktorá je dosť voľná a zaradenie do kategórií môže byť subjektívne vzhľadom na posudzovanie oboch „osí“ naraz.

Problémom môže byť aj odhad rizík v rámci samotnej škály. Je často jednoduchšie posúdiť, ktoré riziko je väčšie ako druhé, ako určiť presný odhad rizika. Toto si už zväčša vyžaduje značné skúsenosti manažérov.

Je tu ale ešte jeden nezanedbateľný faktor. Manažéri môžu ohodnotiť riziká, ktoré nemajú priamo pod kontrolou, vyšším stupňom ohrozenia. Tento fakt viedol k vytvoreniu inej kategorizácie, ako vidíme z Obr. 3.



Obr. 3 – kategorizácia rizík z pohľadu úrovne ich kontroly [1]

Rôzne druhy rizík sú znázornené rôznym kvadrantom v jednoduchej mriežke rozmeroch 2×2 . Jeden rozmer charakterizuje relatívnu dôležitosť rizikových faktorov. Je to vlastne kombinácia pravdepodobnosti rizika (ako často nastane udalosť) a dopadu rizika (čo spôsobí). Je zrejmé, že pre zaradenie rizika v rámci tejto osi sa dá použiť predchádzajúca spomenutá kategorizácia.

Druhý rozmer udáva mieru kontroly. Práve táto určuje, ako veľmi môže manažér svojimi právomocami ovplyvniť rizikovú situáciu. Pridaním tohto pohľadu sme teda zaviedli rozšírený pohľad na riziká ako pri jednoduchej matici.

Do prvého kvadrantu spadajú predovšetkým riziká nedostatočnej zaangažovanosti zákazníka (a používateľa) a nedostatok zainteresovanosti vrcholového manažmentu. Na ich potlačenie je nutné vytvoriť dobré väzby so zákazníkom a získať jeho dôveru.

Druhý kvadrant predstavuje hrozby týkajúce sa požiadaviek na systém. Jedná sa o ich nepochopenie, časté zmeny funkcionality alebo jednoducho súbor základných a doplnkových vlastností. Ak projektový manažér zadá programátorovi bez nejakej kontroly plnenia dve úlohy – jednu kriticky dôležitú, ale pre jeho intelekt „nudnú“, druhú okrajovú, ale s možnosťou zaujímavej realizácie – s veľkou pravdepodobnosťou splní najskôr druhú, pretože môže ukázať svoj dôvtip. Bohužiaľ pritom vyminie väčšie časové prostriedky, ako keby sa najskôr venoval tej prioritnejšej.

Tretí kvadrant zahŕňa riziká samotnej realizácie. Manažér by mal teda poznať odpovede na otázky, či je v jeho silách uradiť projekt s prideleným počtom ľudí, ich kvalifikáciou a skúsenosťami. Toto je oblasť, ktorú má manažér skoro plne pod kontrolou.

Posledný kvadrant ukazuje vnútorné aj vonkajšie hrozby prostredia organizácie, v ktorej sa projekt realizuje. Dajú sa sem zaradiť napr. nezhody medzi oddeleniami zákazníka, ale z dôsledného pohľadu napr. aj spoločenské a prírodné katastrofy.

Techniky odhadu rizík

Ako ale môžeme prakticky vykonať odhad rizík okrem spomínanej kategorizácie? V súčasnosti existujú dve zaujímavé techniky. Pokúsme sa ich v krátkosti popísať.

Kontrolné zoznamy

Kontrolný zoznam (checklist) je vzorový zoznam typických rizikových faktorov získaných napr. z predchádzajúcich projektov. V praxi majú formu dotazníkov alebo jednoduchého zoznamu. Dotazník predstavuje zbierku otázok ku konkrétnej fáze projektu. Až samotnými odpoveďami bývajú potom naznačené možné rizikové faktory. Naproti tomu zoznam je zložený z typických rizikových faktorov popisujúcich stav projektu, ktorých prítomnosť v súčasnej etape sa následne overuje.

Tieto techniky sú pomerne jednoduché na použitie, avšak treba dať pozor na ich prílišnú rozsiahlosť alebo naopak všeobecnosť a na fakt, že nepokrývajú faktory mimo ich zamerania.

Skupinová práca

Skupinová práca (group work) je kolaboratívna technika, ktorá spolieha na prirodzenú ľudskú vynaliezavosť a synergický efekt. Inými slovami „viac hláv, viac rozumu“. Prakticky sa dá realizovať napr. známou technikou brainstormingu, keď viacero ľudí diskutuje o možných rizikách.

Záver

V úvode tejto práce bol spomenutý jeden z Murphyho zákonov. V podobnom duchu sa bude niesť aj jej záver. Je na mieste uviesť jeho dodatok: „čo sa nemôže pokaziť, pokazí sa aj tak“. Ani dôsledné dodržanie analýzy a manažmentu rizík nemusí ochrániť projekt úplne a zabezpečiť stopercentné dodržanie stanoveného plánu. Vždy budú existovať zostatkové riziká, ktoré sa môžu prejaviť. Ani raketoplány NASA nie sú bezchybné, ako sme sa žiaľ mali možnosť presvedčiť.

Napriek tomu je podľa mňa analýza a zvládnutie pravdepodobných a známych rizík jednou z kľúčových vecí pre dokončenie projektu. Manažéri by mali mať o tejto problematike dostatočné odborné znalosti, ale aj praktické skúsenosti. Spoločnosť, ktorá bude tento fakt prehliadať, bude určite rýchlo nahradená na trhu konkurenciou.

Použitá literatúra

1. Keil, M., Cule, P., Lyytinen, K., Schmidt, R.: A framework for identifying software project risks. In: *Communications of the ACM*, Vol. 41, No. 11 (November 1998), 76-83.
2. Miler, J.: A Method of Software Risk Identification and Analysis. Gdańsk: Gdańsk University of Technology – Faculty of Electronics, Telecommunications and Informatics, 2005 PhD Thesis
3. Roy Geoffrey G., A Risk Management Framework for Software Engineering Practice, In: *aswec*, p. 60, 2004 *Australian Software Engineering Conference (ASWEC'2004)*
4. Tiwana A., Keil M.: The One-Minute Risk Assessment Tool. In: *Communications of the ACM*, Vol. 47, No. 11 (November 2004), 73-77.

Annotation

Software project risks

Software industry is quite young, but dynamically expanding segment. Software managers have to handle with risks in whole process of software development. Each of them should know, how to identify them, prevent them and if they happen, try to minimalise loss. Otherwise has company not only financial or time loss but also might loose its customers. This essay tries to refer, what exactly the risk in software project is, what kind of risks could happend and how

they could affected the project. Next are mentioned most often kind of risks and their basic categorization.