

Analýza ako odrazový mostík k efektívnemu plánovaniu rizík v softvérovom projekte

LUBOŠ UKROP

*Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
lukrop[zavináč]gmail[.]com*

Abstrakt. Vývoj softvérového projektu je komplikovaný proces, ktorý je ovplyvňovaný množstvom interných, ako aj externých rizikových faktorov. Tieto spolu s meniacim sa prostredím prinášajú do procesu prvok neistoty, spôsobujúci, že úspešné ukončenie projektu a spokojnosť zákazníka nie je nikdy vopred zaručená. Odhliadnuc od ekonomických dopadov, aj neúspešný projekt môže priniesť vývojovému tímu cenné skúsenosti. V očiach zákazníkov však rozhodne nie je dobrou vizitkou. Preto je v záujme manažmentu pokúsiť sa vopred identifikovať riziká, analyzovať ich a naplánovať postup vedúci k ich minimalizácii. Cieľom tejto eseje je poskytnúť prehľad vybraných kvantitatívnych a kvalitatívnych techník analýzy rizík v softvérovom projekte a zamyslieť sa nad vhodnosťou ich použitia v tíme menšieho rozsahu.

Úvod do problematiky

V každom odvetví ľudskej činnosti sa stretáme s nebezpečenstvom možného neúspechu, zlyhania. Vývoj softvéru nie je výnimkou. Naopak, štatistiky ukazujú, že v tomto smere patrí medzi obzvlášť rizikové. Podľa staršej štúdie vykonanej Standish Group [9] bolo zo softvérových projektov realizovaných v rokoch 1994-2004 iba 29 percent dokončených načas, bez prekročenia rozpočtu a vo vyhovujúcej kvalite. 53 percent takýmto požiadavkám nevyhovelo a 18 percent bolo zrušených alebo nedokončených. Aj keď oproti prieskumu tej istej skupiny spracúvajúceho údaje spreď roku 1994 sa počet úspešných projektov takmer zdvojnásobil, pôsobí uvedená štatistika značne alarmujúco.

Aké sú najčastejšie príčiny zlyhania? Nepochopenie používateľových požiadaviek, implementácia zlých softvérových funkcií, nerealistické plány a finančné zdroje a iné. Chyby ako na strane vývojového tímu, tak projektového manažmentu. Mnohé z nich by nemuseli mať také fatálne dôsledky, keby manažment venoval dostatočnú pozornosť aktívnemu vyhľadávaniu a eliminácii rizík, ktoré môžu prerásť do vážnych problémov. V nasledujúcom texte vysvetlím najskôr niektoré základné

pojmy a postupy vo vzťahu k disciplíne manažmentu rizík, následne sa pokúsim zamyslieť, ktoré zo známych techník analýzy rizík by sa dali využiť pri tvorbe nekomerčného softvérového projektu v menšom, začínajúcom tíme.

Čo je to riziko?

Pojem „riziko“ je definovaný v Krátkom slovníku slovenského jazyka [4] stručne ako „možnosť, nebezpečenstvo straty, neúspechu, škody“. Ďalšie používané definície tohto pojmu uvádza vo svojom článku Misra a kolektív [6]:

- „Možná budúca udalosť, ktorá ak nastane, bude mať nežiadúce následky.“
- „Riziko odkazuje na možnosť straty, stratu samotnú, alebo každú charakteristiku, objekt prípadne činnosť súvisiacu s touto možnosťou.“

To, akú stratu alebo ujmu máme na mysli, závisí od kontextu, v ktorom je pojem použitý. V ekonomickom sektore sa jedná spravidla o finančnú stratu, v oblasti medicíny o fyzickú ujmu.

V oblasti vývoja softvéru táto strata vyjadruje vplyv na projekt, ktorý môže mať formu zníženej kvality výsledného produktu, zvýšených nákladov, neskorého dokončenia alebo aj jeho úplného zrušenia [6].

Manažment rizík

Manažment rizík zahŕňa všetky aktivity, ktoré sú vykonávané s cieľom redukovať neurčitost' spojenú s vykonávanými úlohami a budúcimi udalosťami. V kontexte projektov sa snaží zmierniť dopad neželaných udalostí na projekt. Jeho korene vychádzajú z teórie pravdepodobnosti a teórie rozhodovania sa v menlivých podmienkach.

Vysoký dôraz na manažment rizík je tradične kladený napríklad v oblastiach finančníctva a poisťovníctva. V softvérovom inžinierstve bol dlhý čas opomínaný, až v poslednej dekáde si aj ľudia z tejto oblasti začali uvedomovať jeho dôležitosť [6].

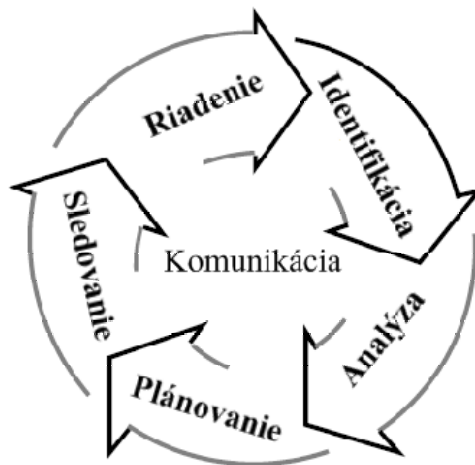
Niektorí by mohli namietat', že prečo sa máme zaoberat' predchádzaním problémom spôsobených rizikami, u ktorých si nie sme istý, či sa vôbec niekedy stanú aktuálnymi. Nie je to len zbytočné plytvanie kapacitami? Iste, niektoré riziká nepredstavujú zásadné ohrozenie projektu. Ak nás ale zastihnú vážne problémy nepripravených, môže to mať katastrofálne následky. Aj Boehm [1] potvrdzuje, že post-mortem analýzy neúspešných softvérových projektov ukázali, ako ich zlyhaniu bolo možné zabrániť, ak by bola venovaná explicitná pozornosť identifikácii vysoko rizikových elementov a následnému prijatiu ochranných opatrení. Manažment rizík v softvérových projektoch má teda preventívnu funkciu vo vzťahu k identifikovaným rizikám.

Podľa [8] riziká pre softvérový projekt spadajú do troch kategórií:

- riziká teoreticky známe projektovému tímu a zároveň identifikované ako hrozby pre projekt
- riziká teoreticky známe, no nepredstavujúce hrozbu pre projekt

- neznáme riziká

Je na manažmente aby riziká správne zaradil. Prirodzene, najnebezpečnejšie riziká sú tie, o ktorých existencii vôbec nevieme.



Obr. 1. Paradigma manažmentu rizík podľa SEI [3].

Základné fázy manažmentu rizík

Základná, dodnes uznávaná paradigma manažmentu rizík v softvérovom projekte bola stanovená Inštitútom softvérového inžinierstva (Software Engineering Institute) v roku 1990. Ako naznačuje schéma (viď Obr. 1.), manažment rizík sa tu chápe ako cyklický proces opierajúci sa o komunikáciu. Rozdelený je na niekoľko základných fáz, ktoré Higuera a kolektív [3] popisujú takto:

Identifikácia

Cieľom identifikácie je odhaliť hroziace riziká skôr ako prerastú do reálnych problémov. Typické techniky identifikácie rizík zahŕňajú kontrolný zoznam, dekompozíciu, porovnanie so skúsenosťami, prípadne preskúmanie rozhodovacích konceptov [1].

Analýza

Vo fáze analýzy sú údaje o rizikách transformované na informácie užitočné pre ďalšie rozhodovanie. Čo by mala dobrá analýza zahŕňať? Určite by sme sa z nej mali dozvedieť, v ktorej fáze vývoja softvéru nám dané riziko hrozí, za akých podmienok sa ho máme obávať a aké dôsledky (napr. finančné) by malo jeho naplnenie. Analýza je

tiež vhodné miesto pre priradenie priority rizikám, čím zabezpečíme, že sa manažment bude zaoberať naozaj tými najkritickejšími rizikami.

Plánovanie

Plánovanie spočíva v navrhnutí akcii v reakcii na dané konkrétne riziká, v priradení priority týmto akciám a vo vytvorení integrovaného plánu manažmentu rizík. Kvôli obmedzeným zdrojom býva často nevyhnutné riziká s menšou prioritou jednoducho akceptovať. Kľúčové je dôkladne zvážiť následky prijatých rozhodnutí.

Sledovanie

Sledovaním zistíme aktuálny status identifikovaných rizík a účinnosť prijatých opatrení.

Riadenie

Fáza riadenia spočíva v náprave odchýliek vykonávaných akcií od tých naplánovaných, úprave plánu a všeobecnom zdokonaľovaní procesu manažmentu rizík.

Žiadny prístup k manažmentu rizík by nebol životaschopný bez efektívnej komunikácie. Komunikácia je jednak nevyhnutná na nižšej úrovni, kedy sa musia synchronizovať kroky vykonávané v jednotlivých fázach manažmentu. Okrem toho je vhodné riziká komunikovať na príslušných organizačných úrovniach a vo vzťahu k zákazníkovi, prípadne používateľovi [3].

V ďalšej časti eseje sa zameriam na analýzu rizík, ktorú považujem za kľúčovú pre produktívne fungovanie manažmentu rizík. Prečo? Ak nemá projektový manažment o riziku dostatok korektných informácií, hrozí, že v ďalšej fáze naplánuje postup, ktorý nebude mať na minimalizáciu rizika žiadny vplyv. Nesprávne určenie priority rizík, prípadne úplná absencia takýchto informácií, zase môže spôsobiť, že vplyv zdroje na prevenciu veľmi nepravdepodobných rizík, pričom tie skutočne nebezpečné ostanú nepovšimnuté. Pri analýze máme možnosť oprieť sa o existujúce, overené techniky.

Techniky analýzy rizík

Techniky analýzy rizík môžeme v zásade rozdeliť na kvantitatívne a kvalitatívne.

Pri *kvantitatívnych* technikách využívame nejakú formu metriky pre priradenie numerickej hodnoty vopred identifikovanému riziku. V oblasti softvérového inžinierstva sa metriky používajú jednak na ohodnotenie aktuálneho stavu (takzvané hodnotiace metriky), alebo na odhadnutie budúcich charakteristík projektu (prediktívne metriky). V manažmente rizík nájdeme uplatnenie obidvo druhov. Hodnotiace metriky môžeme použiť vo fáze monitorovania rizika, kedy si chceme overiť účinnosť naplánovaných a prijatých opatrení. Prediktívne metriky použijeme práve pri analýze pre určenie pravdepodobnosti naplnenia daného rizika a závažnosti následkov, ktoré na projekte zanechá [7].

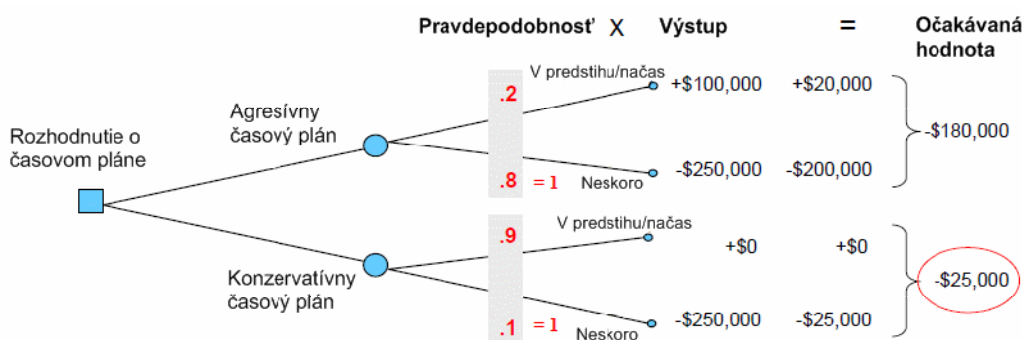
Miera dopadu rizika a stromy rozhodovania

Miera dopadu rizika (angl. „*Risk exposure*“) je jednou z najklasickjších metrík používanou v rámci analýzy rizík. Je definovaná vzťahom (1), kde $Pr ob(uo)$ je pravdepodobnosť neuspokojivého výstupu uo a $Loss(uo)$ predstavuje stratu, ktorú má uo za následok [1].

$$RE = Pr ob(uo) \times Loss(uo) \quad (1)$$

Miera dopadu rizika je často používaná v spojení s technikou *rozhodovacích stromov* pri analyzovaní a plánovaní opatrení na zmiernenie dopadu rizika.

Príklad rozhodovacieho stromu je zobrazený na Obr. 1. V tomto prípade je strom použitý pre analýzu rizika finančného penalizovania v prípade neskorého dokončenia projektu. Ak bude zvolený agresívny časový plán a skorý termín odovzdania, môžeme pri jeho splnení počítať s bonusom 100000 \$. Dostatočne včasné odovzdanie je však veľmi nepravdepodobné, a teda sa vystavujeme veľkému riziku pokuty. Preto je bezpečnejšie zvoliť konzervatívny časový plán.



Obr. 2. Príklad použitia rozhodovacieho stromu pri analýze rizík [8].

Modulárne riziko

Táto metrika sa používa na určenie rizika zlyhania jednotlivých modulov. Odhaduje ho ako súčin očakávaného počtu zlyhaní v dôsledku chýb v danom module a veľkosti očakávanej straty plynúcej zo zlyhania [7].

Na základe kvantitatívnych techník analýzy je vďaka exaktnej povahe výstupu určenie priority rizík pomerne jednoznačné. Otázne však je, či bude skutočne správne, a teda či naplánujeme kroky na elimináciu naozaj tých najnebezpečnejších hrozieb. Kameňom úrazu je podľa môjho názoru určenie pravdepodobnosti, či sa riziko naplní a teda dôjde k neuspokojivému výstupu. Aby táto mohla byť odhadnutá presne, musel by sa manažér opierať buď o bohaté skúsenosti, alebo o presné štatistiky podobných prípadov. Riziká interného charakteru, akým je napríklad riziko neadekvátnych znalostí vývojového tímu sa dajú, v prípade že dobre poznáte svoj tím, ohodnotiť

pomerne spoľahlivo. Riziká externé, povedzme zvýšenie cien zdrojov alebo ich nedostatok na trhu sa budú predvídať len ťažko.

V prípade začínajúceho tímu malého rozsahu vidím kvantitatívnu analýzu rizík veľmi pesimisticky. Numerická povaha ohodnotení môže byť zdrojom nepresností. Absencia skúseností v tejto oblasti by mohla ľahko zapríčiniť, že sa určovanie pravdepodobností zmení na hádanie z kávovej usadeniny. Nehovoria o tom, že zďaleka nie všetky projekty majú komerčnú povahu, a teda ťažko pri nich vyčísl'ovať finančné straty plynúce z naplnenia rizika. Netreba zabúdať, že chybná analýza vplýva zásadným spôsobom na celý manažment rizík, ktorý sa vďaka nej ľahko zmení na plytvanie časom a ľudskými zdrojmi.

Pri *kvalitatívnej* analýze, na rozdiel od tej kvantitatívnej, popisujeme pravdepodobnosť rizika a jeho dopad slovné, teda pre človeka intuitívnejšou formou. Známymi technikami kvalitatívnej analýzy sú:

Delfská technika

Delfská technika (angl. „Delphi technique“) je technika hľadania názorovej zhody zahŕňajúca nezávislú analýzu a hlasovanie expertov, poskytujúc im spätnú väzbu, ako sa ich posudok zhoduje s názormi zvyšku skupiny [7].

V prípade analýzy rizík pozostáva z týchto základných krokov [8]:

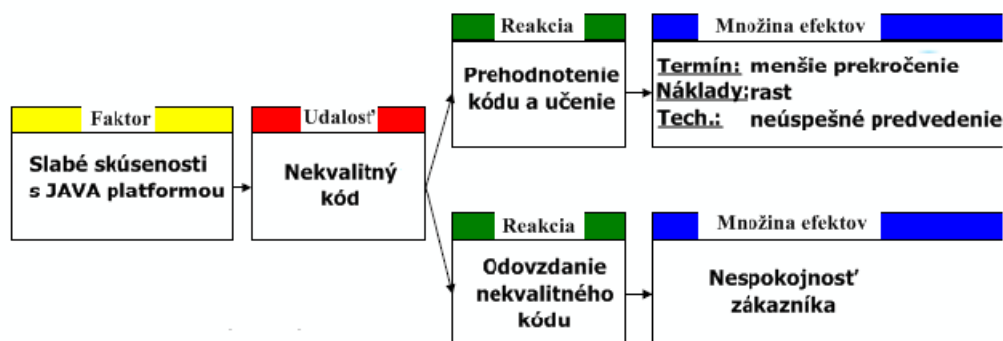
1. Výber skupiny expertov. Títo budú pracovať v anonymite, nezávisle od seba, pričom sa nemusia navzájom vôbec poznať.
2. Príprava a rozoslanie otázok, ktoré sa vzťahujú sa na identifikované riziká.
3. Zozbieranie odpovedí, ich analýza za účelom identifikácie hlavnej názorovej tendencie a vymykajúcich sa názorov.
4. Zdieľanie odpovedí a vytvorenej štatistiky medzi účastníkmi.
5. Ak nebola dosiahnutá priateľná zhoda, alebo ak nebol prekročený zvolený počet iterácií, pokračuje sa krokom dva. Účastníci s extrémnymi názormi ich po konfrontácii so všeobecným názorovým prúdom v skupine môžu potvrdiť, alebo korigovať.

Hlavné pozitíva tejto techniky vidím v zachovaní anonymity účastníkov. Ak sa účastníci navzájom nepoznajú, nebudú ovplyvňovaní osobnostnou zaujatosťou. Môže im to umožniť voľnejšie vyjadrovať vlastné názory, prípadne priznať chyby v ich predchádzajúcich úsudkoch. Vhodnosť použitia tejto techniky menším tímom je však diskutabilná. Princíp anonymity je pri výbere expertov z malého okruhu ľudí ohrozený. Podľa [5] sa pri Delfskej technike pracuje väčšinou so skupinou 15-20 ľudí v trvaní niekoľkých týždňov. Malé tímy častokrát ani nemajú taký rozsah, a aj keby áno, každý člen určite nie je fundovaný pre vyjadrenie sa k daným rizikám. Výhodou takýchto tímov je často aj schopnosť veľmi dynamicky prijímať rozhodnutia. Obávam sa, že v tomto prípade by bola Delfská technika zbytočne zdĺhavá.

Analyza scenárov

Analyza rizík za použitia scenárov je zahrnutá napríklad v Riskit metóde [2] manažmentu rizík. Pomocou scenárov môžeme reprezentovať alternatívne postupnosti budúcich udalostí na základe prijatia nejakého rozhodnutia.

Príklad dvoch scenárov možných udalostí pri naplnení rizika nedostatočných skúseností s Java platformou zobrazuje Obr. 3. Zo scenárov možno vyčítať efekty, plynúce z rozdielnych reakcií na dané riziko, potom ako sa stalo reálnym problémom. Samozrejme, najlepším riešením v uvedenom príklade bolo takémuto riziku vopred predísť. Toto však nemusí byť vždy možné, napríklad kvôli nepresnostiam vo fáze identifikácie rizík.



Obr. 3. Scenáre v Riskit metóde manažmentu rizík [2].

Nedostatkem tejto techniky môže byť fakt, že pri zostavovaní scenárov sa postupuje na základe vlastných skúseností, ktoré nemusia byť vždy dostatočné. Ľahko môže dôjsť aj k prehliadnutiu dôležitej alternatívy reakcie. Ak sa potom v procese plánovania bez výhrady spoľahneme na vytvorené scenáre, môže to priniesť závažné problémy.

Aké sú možnosti použitia techniky scenárov malým tímom? Podľa môjho názoru veľmi dobré. Na základe prepracovaných scenárov je možné bez ďalšej zdĺhavej analýzy prijímať rozhodnutia, ktoré majú pre projekt a tím najpriaznivejší efekt.

Rozmazaná metrika

Rozmazaná metrika (angl. „Fuzzy metrics“) využíva druh uvažovania známy ako škálové monotónne zret'azenie, ktoré mapuje riziká špecifikované v jednotlivých pravidlách na pokročilú fuzzy množinu pre meranie rizík. Pre svoju zložitosť, ktorá je zrejme už z definície, však táto metrika nie je v praxi často využívaná [8].

Záver

Manažment rizík je dnes etablovaný ako štandardná súčasť manažmentu softvérového projektu. Pomáha nám minimalizovať hroziace riziká, alebo zmierniť ich dopad. Pre jeho efektívne fungovanie je obzvlášť dôležité vykonať dôkladnú analýzu, ktorá bude slúžiť ako podklad pre ďalšie rozhodovanie. V tejto eseji som sa zaoberal niekoľkými známymi technikami analýzy rizík, s cieľom zhodnotiť možnosť ich využitia začínajúcim malým tímom. Ako najvhodnejšia sa mi, po zvážení týchto kritérií, javí kvalitatívna technika *analýzy scenárov*. Pre exaktnejší výstup by ju mohlo byť, obzvlášť v prípade problematického rozhodovania medzi alternatívami, vhodné skombinovať s niektorou kvantitatívnou technikou.

Použitá literatúra

1. Boehm, B. W.: Software Risk Management: Principles and Practices. *IEEE Software*, Vol. 8, No. 1 (1991) 32-41.
2. Freimut, B. et al.: An industrial case study of implementing software risk management. In: *Proceedings of the 8th European software engineering conference*, 163-166, 2001.
3. Higuera, R.P., Haimes, Y.Y.: Software Risk Management. *Technical Report CMU/SEI-96-TR-012*, 1996.
4. Kačala, J., Pisárčiková, M., Považajm M.: Krátky slovník slovenského jazyka. *Veda*, 4. vyd., Bratislava 2003.
5. Ludwig, B.: Predicting the future: Have you considered using the Delphi methodology? *Journal of Extension*, Vol. 35 No. 5 (1997), 1-4.
6. Misra, C., Kumar, V., Kumar, U.: Different Techniques for Risk Management in Software Engineering: A Review. In: *Proceedings of Technology and Innovation Management Division*, Administrative Sciences Association of Canada, Banff, 2006.
7. Pedayachee, K.: Techniques used in Risk Analysis of Software Development. In *University of South Africa - Postgraduate Research Symposium*, Pretoria, 2001.
8. Shafer, D. F.: Software Risk: Why must we keep learning from experience? In *Dynamic Positioning Conference*, Marine Technology Society, 2004.
9. Standish Group International: The Chaos Report. *West Yarmouth*, Massachusetts, 2004.

Annotation

Analysis as a jumping board toward effective risk planning in software project

Software project development is a complicated process, which is influenced by a large number of internal and external risk factors. These, together with the changing environment, can bring an element of uncertainty into the process, causing that successful completion of the project and customer satisfaction is never guaranteed in advance. Apart from significant economic impact, an unsuccessful project can bring valuable experiences. Unfortunately, it sends also negative signals to potential customers. Therefore, it is on the behalf of management to identify the risks in advance, to analyze them and to schedule the procedure for their reduction. Main aim of this essay is to give an overview of selected quantitative and qualitative techniques of risk analysis in the software project and to consider the appropriateness of their use by a small team.