

Softvérové riziká - včera a dnes

ANDREJ ANTAL

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

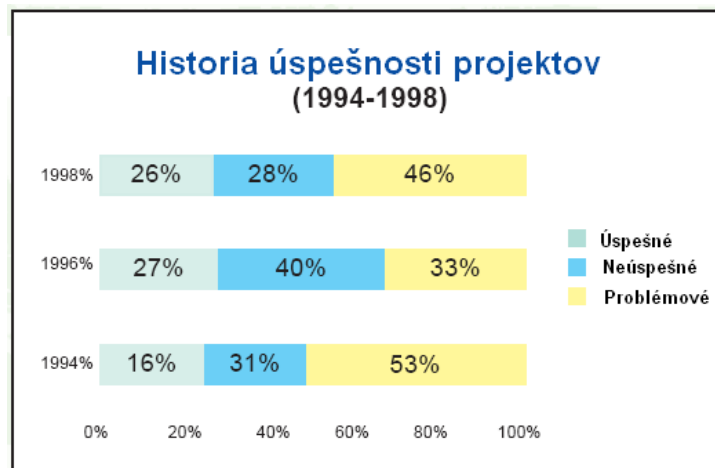
Abstrakt. Manažment rizík v softvérovom systéme vznikol už v minulom tisícročí. Ľudia pri vývoji softvéru si rýchlo uvedomili, že treba podrobne analyzovať problémy, ktoré môžu vzniknúť. Tak isto ako iné odbory aj tento prechádza určitým vývojom. Pribudli nové metódy a spôsoby na analýzu a plánovanie rizík. Dnes už nikto nespochybňuje dôležitosť tejto činnosti a len málo projektov existuje bez rizikových analýz a plánov na ich riešenie. Ich určovanie a plánovanie nieje proces krátkodobý. Vykonáva sa vo viacerých etapách počas celého cyklu projektu.

Mojou esejou sa budem snažiť odpovedať na tri základné otázky: Prečo sú dôležité identifikácia, klasifikácia a plánovanie problémov v softvérovom systéme? Ako robiť manažment rizík, aby sa v projekte ušetrilo čo najviac peňazí, prostriedkov a ľudskej práce. Kde všade môžeme využiť manažment rizík pri vytváraní tímového projektu.

Úvod

S postupným zväčšovaním softvérových projektov a so zvyšujúcimi sa stratami na týchto projektoch vystala potreba týmto stratám predchádzať. Ako v iných oblastiach, tak aj pri vytváraní softvéru vznikla disciplína, ktorá sa zaoberá analýzou a plánovaním rizík počas celého cyklu tvorby projektu. Jej dôležitosť stále dokazujú štúdie, ktoré sa prevádzajú. V roku 2000 bolo iba 28% projektov[4] dokončených bez problémov, zvýšeného rozpočtu a v danom časovom období. Napriek tomu, že úspešnosť projektov má zvyšujúcu tendenciu[Obr. 1], je pohoršujúce, že v období, kedy sa informatika dostáva do všetkých oblastí ľudskej spoločnosti, toľko projektov končí neúspechom alebo s problémami. Príkladom sú škody niekoľko miliónov dolárov u firiem ako Microsoft alebo Oracle, pokiaľ sa posunie doba vydania, alebo produkt neodpovedá očakávaným požiadavkám. Podobne aj aukčná spoločnosť eBay stratí milióny dolárov, pokiaľ sa ich systém pokazí na niekoľko hodín.

Manažment projektov softvérových a informačných systémov, október 2008, s. 1-8.

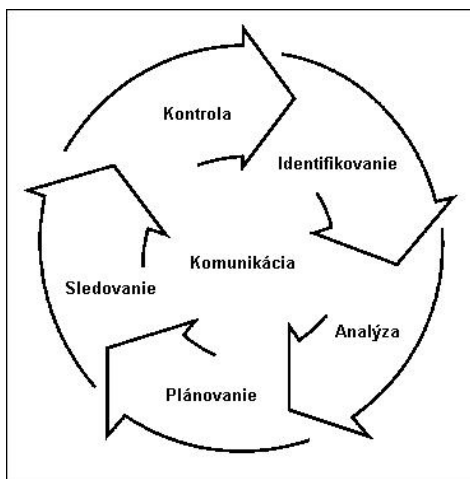


Obr. 1. Úspešnosť ukončenia projektov v Amerike počas rokov 1994-8[7]

Mnoho spoločností kvôli všetkým týmto hrozbám používa množstvo metód v snahe redukovať časové straty a počet chýb. Nanešťastie, tieto metódy mnohokrát majú skôr opačný charakter a celý projekt tak ešte viac spomalia. Vrchný manažéri si problém mnohokrát všimnú až keď je neskoro, alebo im ho nahlásia zákazníci.

Ďaleko lepší spôsob je súbor preventívnych postupov k zmenšovaniu rizík založený na skúsenostiach z praxe. Hlavnou myšlienkou je identifikovať oblasti, kde môže dôjsť k zdržaniu alebo k zlyhaniu projektu. Následne vymyslieť stratégie, ktoré dané riziká zmenšia alebo úplne eliminujú.

Manažment rizík je proces prebiehajúci neustále, počas všetkých fáz projektu. Tento proces môžeme rozčleniť do šiestich fáz[Obr. 2].



Obr. 2. Spojité vykonávanie činností pri manažmente rizík[5]

Sú to: identifikovanie rizík, ich analýza, plánovanie, sledovanie kontrola a komunikácia. To že je to opakujúci sa proces dokazuje skutočnosť, že v jednom okamihu sa identifikuje a analyzuje jedno riziko, zatiaľ čo ostatné sú sledované.

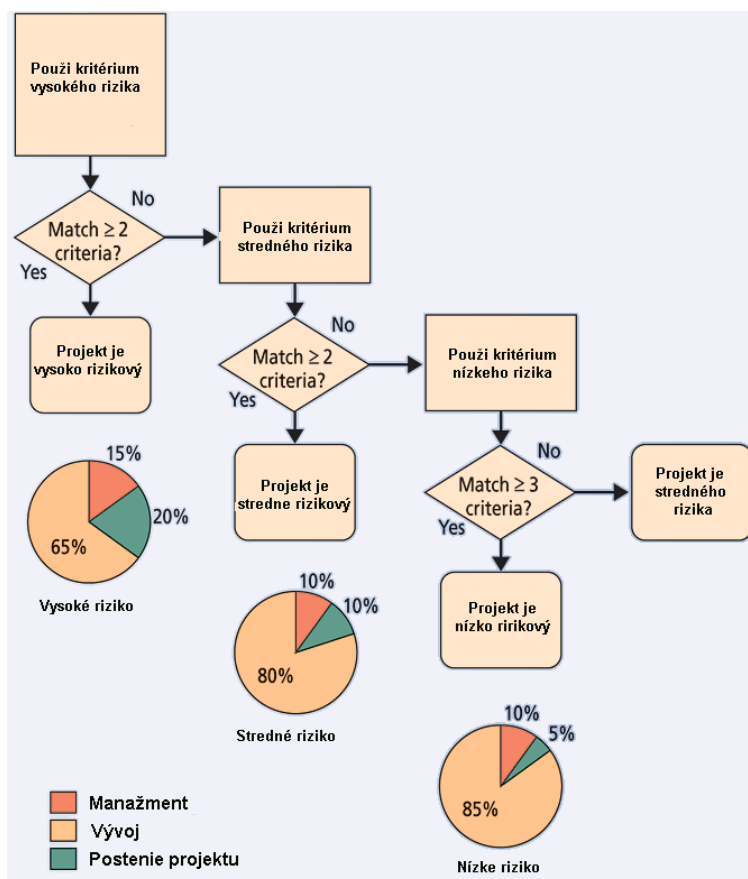
Manažment rizík môžeme robiť pomocou viacerých metód. Záleží hlavne na tom, či do procesu identifikácie rizík zaradíme len členov rizikového manažmentu alebo aj ostatných.

1. Technika softvérového hodnotenia rizika(SRE) je dobrý príklad súboru metodických postupov k obmedzeniu rizika. Identifikácia rizík a ich analýza je vedená jedným človekom prípadne jedným tímom. Investori, zákazníci ani ostatní pracovníci sa nepodieľajú na identifikácii rizík.
2. Technika tímového rizikového manažmentu(TME). Naopak pri tomto type analýzy sa podieľajú všetci jednotlivci pri tvorbe softvéru, čo umožňuje manažérovi identifikovať čo najviac rizík.
3. Softrisk prístup sa sústreďuje na dokumentáciu. Tento model môže byť použitý v akomkoľvek type projektu. Dôležitý rys tohto nástroja je, že môže meniť veľkosť a pravdepodobnosť výskytu rizík. Pri tomto prístupe dochádza k zvýrazneniu dôležitého rizika.
4. ARMOR je systematický prístup, ktorý nielen identifikuje riziko ale tiež identifikuje zdroj rizika a snaží sa ho zlepšiť.
5. Riskit manažérsky model je populárny v množstve priemyselných odvetví. Používa obrazec, aby definoval rôzne aspekty rizík. Taktiež obsahuje rysy TRM, pretože umožňuje účasť investorov.

Okrem metód existuje aj množstvo postupov, ako v jednotlivých metódach postupovať. Ja som sa rozhodol predstaviť päťstupňový odhad rizík.[6]

1. Najprv si vyberiem počet rizikových úrovní.(Ja som si vybral tri kategórie – vysoké, stredné a malé riziko)
2. Pre každé riziko definujem rizikové kritéria(Napr. vysoký risk – unikátna aplikácia, stredný risk – aplikačná doména nie je dobre známa, nízky risk – aplikačná doména je dobre známa).
3. Pre každú úroveň určiť potrebný počet zhôd, pri koľkých projekt zaradím do danej kategórie.(vysoký risk – dve, stredný risk – dve, nízky risk – tri)[Obr.3.]. Pokiaľ si z vysokého rizika vyberiem pre daný projekt viac ako dve kritéria je daný projekt vysokorizikový a uplatní sa podiel manažmentu(15%), vývoja(65%) a poistenia projektu(20%). Pokiaľ nie, postupujem na obrázku ďalej a porovnávam môj projekt so stredne rizikovým projektom. Pokiaľ mi nevyhovuje ani jeden typ, tak prechádzam do základnej úrovne, ktorú si vždy určím na začiatku.
4. Určiť základnú úroveň.(Ja som si určil postupovať podľa stredného rizika).
5. Pre každú úroveň určiť zastúpenie manažmentu, vývoja a poistenia.

Pokiaľ svoj projekt dokážem začleniť do jednej s kategórií, viem z jednoduchosťou určiť pomer zastúpenia manažmentu, vývoja a poistenia. Z tohto postupu pekne vidno ako na základe rizík dokážeme zaradiť projekt a následne určiť, čo je pre neho najlepšie.



Obr. 3. Aplikácia rizikových kritérií

Identifikácia rizika

Identifikácia rizík spočíva v systematickej analýze, identifikácie, kategorizácie a dokumentácii rizík, ktoré môžu ovplyvniť projekt.

V praxi sa stretáva z dvoma druhmi rizík. Externé, ktoré nemožno priamo riadiť (činnosť vlády, správanie zákazníka,...) a interné. Tento zoznam odráža rizikové kategórie, s ktorými sa určite väčšie projekty stretnú.[5]. Flexibilný vývojový proces môže zmierniť riziká v prvých troch kategóriách.

1. Požiadavky. Nejasné, alebo nepresné požiadavky sú veľkým rizikom. Je to najbežnejší typ rizika a sú pravdepodobne najviac zodpovedné za neúspešné alebo omeškané projekty. Je to spôsobené tým, že je ťažké si predstaviť používateľovi software, pokiaľ ho sám nevyskúša. Na elimináciu tohto rizika je dôležité, aby objednávatel' projektu mal k nemu čo najväčší prístup a dokázal prípadné nezrovnalosti opraviť už počas návrhu softvéru.
2. Technologické. V niektorom bode vývoja príde tím k záveru, že daná technológia nie je schopná uspokojiť všetky systémové požiadavky. V tom prípade sa musí technológia buď nahradiť, alebo upraviť požiadavky projektu.
3. Obchod. Obchodné riziká predstavujú množstvo rizík. Môže dôjsť ku konfliktu medzi partnermi. Jeden z partnerov rozviaže zmluvu.
4. Politické. Tieto problémy je najťažšie prekonať. Niektoré veľké firmy sa správajú ako rodiny. Členovia týchto firiem sú úzko poprepájaný. Pokiaľ dôjde k rozporom medzi tímami znamená to omeškanie, prípadne neúspech projektu. Tieto riziká sa veľmi ťažko určujú. Dôležitá je komunikácia medzi členmi.
5. Zdroje. Nastáva pokiaľ projekt nedostane požadovaný počet členov, dostatok peňazí, zariadenia. Nedostatok zdrojov znamená zníženie morálky členov v tíme. Pomôcť môže dodanie alternatívneho zdroja.(napr. niektorý iný tím môže zdieľať niektorý zo svojich serverov).
6. Schopnosti. Tieto riziká nastávajú vtedy, keď tím neovláda potrebnú technológiu. Tento problém sa dá riešiť usporiadaním odborných tréningov na danú tému, prípadne pridaním skúsenej osoby do tímu.
7. Rozmiestnenie a podpora. Tím nemôže nainštalovať software, pretože nie je dodaný potrebný hardware na jeho chod. Niekedy tento problém vzniká kvôli tomu, že jednotlivé tímy nevedia čo robí ten druhý. Riešením tejto situácie je zlepšenie vzájomnej komunikácie.
8. Integrácia. Pri väčších aplikáciách je nutné aby jej jednotlivé časti dokázali spolu komunikovať. Nakoľko každú časť programu robí iný tím, je dôležité, aby rozhrania dokázali pracovať spoločne ako sa očakávalo. Komunikácia medzi tímami redukuje toto riziko. Integráciu častí je treba robiť počas ich vývoja a skoro tak odhaliť prípadné problémy.
9. Rozvrh. Pokiaľ niektorá časť systému nie je ešte dostupná znamená to problém pre celý projekt. Dochádza k omeškaniu. Dôležitá je opäť dobrá komunikácia medzi oddeleniami . Taktiež je potrebné, aby každý tím vedel ako je na tom ten druhý, prípadne koľko mu chýba do dokončenia daného modulu.
10. Údržba a rozšírenia. Firma nemôže udržiavať alebo rozšíriť software, pretože je nedostatočná dokumentácia, platforma na ktorej systém pracuje je zastaraná, nie je dostatok ľudí ovládajúcich daný systém. Východiskom je

venovať väčšie financie a viac času školeniu kvalifikovaných pracovníkov, písaniu podrobnej dokumentácie.

11. Návrh. Zle spracovaný návrh systému znamená zlú použiteľnosť. Etapu návrhu nemožno podceňovať. Dôležité sú hlavne názory používateľov a prepracovanosť systému do najmenších detailov.
12. Ostatné. Toto je kategória rizík, ktoré ide veľmi ťažko predvídať. Napríklad oheň, alebo hurikán, ktorý zničí vašu kanceláriu, havária serveru a tak ďalej. Väčšina týchto rizík znamená stratu dajakého zdroja. Stratégiou jeho riešenia je zmenšenie jeho vplyvu (Použitie náhradného serveru, ľudia budú pracovať z domu).

Podľa môjho názoru sa s väčšinou rizík môžeme stretnúť aj pri riešení nášho tímového projektu. Identifikáciu rizík by sme nemali podceňovať, pretože sa často stáva aj v školskom prostredí, že sa pre danú úlohu vyberie zlá platforma. Problém môže nastať aj v komunikácii, či medziľudských vzťahoch v tíme, nedodržaním harmonogramu, alebo nedostatočnými skúsenosťami. Kvôli týmto všetkým rizikám by sme ich identifikáciu a analýzu mali urobiť čo najskôr a predísť tak prípadným komplikáciám.

Analýza rizika

Pri analýze rizík dochádza k vyhodnoteniu a určeniu, ktoré riziká si vyžadujú dajakú akciu. Významnou časťou identifikácie a analýzy je generovanie rizík a ich následné hodnotenie. Výstupom analýzy rizík je zoznam udalostí, ktorými sa treba zaoberať a ktorými nie. Taktiež sa riziká usporadúvajú podľa priorít.

Plánovanie rizika

Po odhalení a analyzovaní rizík ich treba dostať pod kontrolu. Prvým krokom ako dostať riziká pod kontrolu je zostaviť si plán najúspešnejších techník. Medzi takéto techniky patrí napríklad simulovanie, modelovanie, prototypovanie. Ďalším krokom je zostavenie si takéhoto plánu pre každé riziko. Posledným krokom je integrovanie rizikových plánov každého rizika z inými rizikami a nakoniec s celkovým projektovým plánom.

Sledovanie a kontrola rizík

Sledovanie a kontrola rizík obsahuje:

1. sledovanie stavu a javov, ktoré môžu vznik budúceho rizikového stavu indikovať
2. kontrolné meranie procesov, ktoré súvisí s potencionálnymi rizikami

3. sledovanie kritických javov a procesov mimo projektu, hodnotenie zmien, ktoré môžu mať vplyv na predtým stanovené indikátory a úrovne prijateľnosti rizík
4. hodnotenie všetkých odchýlok medzi plánom projektu a skutočným stavom v priebehu projektu z pohľadu ich vzťahov k definovaným rizikám, alebo pri vzniku potencionálneho konfliktu v plánovaných bežných zdrojoch podniku
5. porovnanie aktuálne vzniknutého rizika s veľkosťou rezervných zdrojov pridelených pre elimináciu, alebo zníženie dopadu rizika, vyvolanie eskalačného procesu v prípade konfliktu
6. iniciáciu obranných stratégií a zavedenie vhodných opatrení podľa plánu riadenia rizík
7. kontrola účinnosti kontrolných opatrení
8. zachytenie vzniku ďalšieho, predtým neidentifikovaného rizika
9. koordináciu riadenia rizík projektu s obdobnými aktivitami na úrovni spoločnosti

Záver

Podľa môjho názoru je rizikový manažment je dôležitá súčasť každého projektu a v dnešnej dobe ho už ani nikto nepodceňuje. Investície do rizikových odhadov sa každej firme niekoľkonásobne vrátia v neskorších etapách vývoja, či už v podobe ušetreného času alebo financií. Manažment rizík v softvérových systémoch existuje už niekoľko desaťročí, vďaka čomu existuje množstvo prístupov a metód na identifikáciu, analýzu, či plánovanie. Popísanie všetkých metód by vyžadovalo ďaleko väčší čas a väčší priestor.

Napriek tomu, že náš tímový projekt je relatívne malého rozsahu, nebude určenie základných rizík plytvaním času. Minimálne pri niektoré rizikové oblasti, akými sú skúsenosti, rozvrh, alebo návrh.

Použitá literatúra.

1. Bieliková, M.: Manažment v softvérovom inžinierstve, Bratislava, 1999.
2. Boehm, B.W.: Software Risk Management: Principles and Practices, *IEEE Software*, January (1991) 32-41
3. McGraw, G.: Risk Analysis in Software Design. *IEEE Security & Privacy*, July/August (2004) 79-84
4. Murthi, S.: Preventive Risk Management for Software Projects, *IEEE* (2002)
5. Rabbi, F., Mannan, K.O.B.: A Review of Software Risk Management for Selection of best Tools and Techniques, *IEEE Computer Society* (2008) 773-778

6. Scott, E.D., Stanley, G.S.: Enriching Your Project Planning: Tying Risk Assessment to Resource Estimation. *IT Pro*. September | October (2007) 20-27
7. Standish Group International: *Chaos: A Recipe for Success*, 1999

Annotation

Software Risks – Yesterday and Now

Management of risk in software's system originate in last century. People got know by software development, that it is necessary to analyze troubles which can begin. This branch goes through development as another branch. A new methods and a ways are added up on analyze and planning of risk. Today nobody has doubts about important of this work and a few projects exist without analyses of risk and without plans of solution. Planning and identification are not shot-time processes. It is executing in many of stages during whole cycle of project. I will try to give answers on three basic questions by my essay: Why are important identification, classification and planning problems in software's system. How to do management of risk for saving money in the project, for saving resources and for saving the work of people. Where we can use management of risk in creating of team project.