



Řízení rizik při vývoji SW

Barry Boehm, USC

“Pokud aktivně nenapadnete rizika, ...



..., rizika napadnou aktivně vás.”



Tom Gilb



Význam rizikového řízení



- Týká se složitých SW systémů.
- Soustředí pozornost projektu na kritické rizikové položky.
- Poskytuje techniky pro zvládnutí rizikových položek.
- Redukuje ceny SW tím, že snižuje cenu přepracování, obvykle 40-50% ceny SW.

Když je řízení rizik důležité, proč to lidé nedělají ?



Neochota připustit existenci rizik.

- Zanechává dojem, že nevíte přesně, co děláte.
- Zanechává dojem, že vaši pánové - zákazníci neví přesně, co dělají.
- Orientace na úspěch.

Tendence odložit obtížné části.

- Možná, že zmizí.
- Možná se budou řešit snáze, až vyřešíme lehké části.

Prevence stojí peníze a čas.

Kdy použijí lidé řízení rizik?



Poté, co se spálili v podobné situaci.

- Vyhýbání se bolesti.
- Přesvědčivá evidence následků.

Když je každý zúčastněný přesvědčen, že rizika existují, ale že má stále cenu pokračovat.

- Každý je vítězem, realistická očekávání.

Když se to konečně naučili dělat správně.

- Techniky nejsou všeobecně známé, ale lze se je naučit.

Definice rizika



Riziko = Možnost ztráty nebo zranění (Webster)

$$E = P \cdot Z$$

E = Expozice rizika

P = Pravděpodobnost nežádoucího výsledku

Z = Ztráta při nežádoucím výsledku

Složky uspokojivého výsledku



Zákazník:	Cena, termín dodání ...
Vývojář:	Rozpočet, plán ...
Uživatel:	Funkcionalita, výkon, spolehlivost, použitelnost ...
Údržbář:	Modifikovatelnost, přenositelnost ...
Manažer výroby:	Další použitelnost ...

Příklad rizikové SW situace



Software řídí vesmírný experiment

PROB (pravděpodobnost kritické chyby) = 0.4

Ztráta po výskytu kritické chyby = \$20M

Pokud se provede nezávislá V&V:

- PROB (kritická chyba zůstane) = 0.05

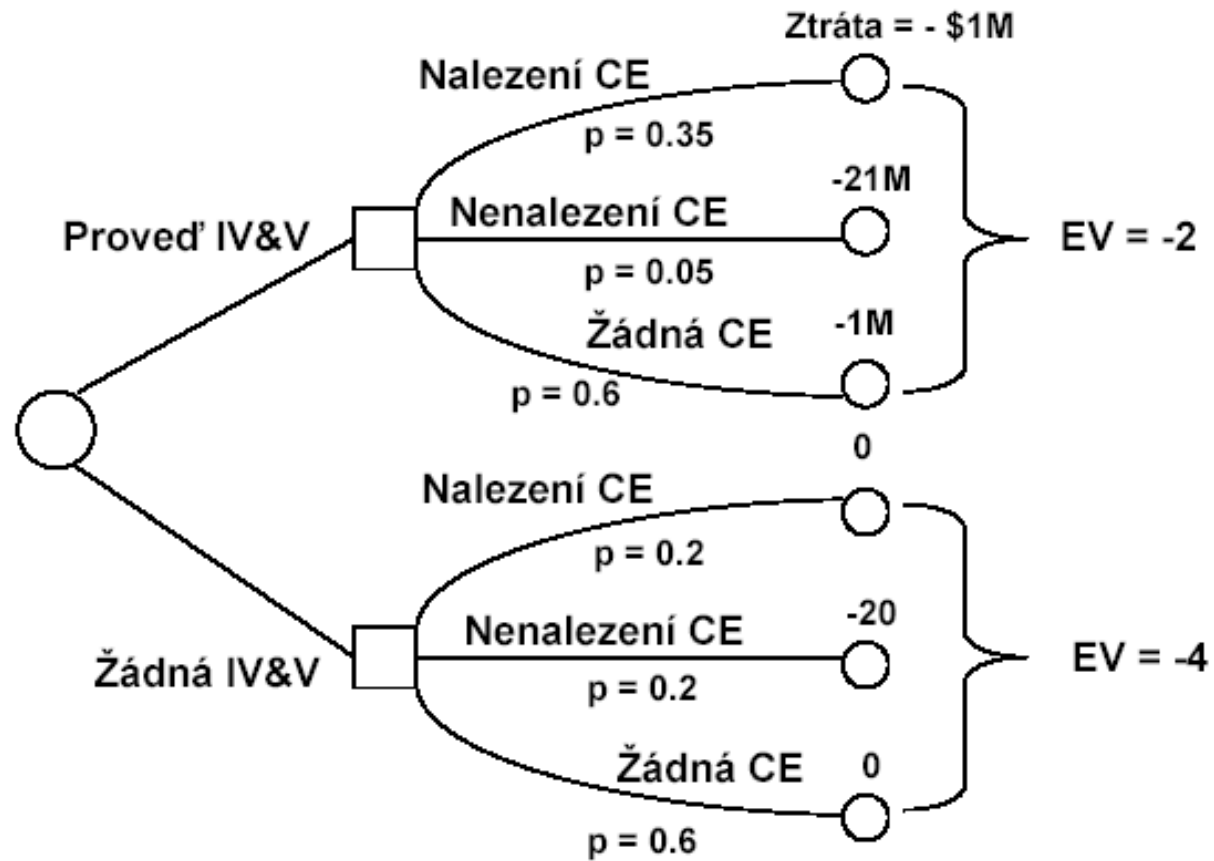
- Přidaná cena k SW projektu = \$1M

Pokud se neprovede nezávislá V&V:

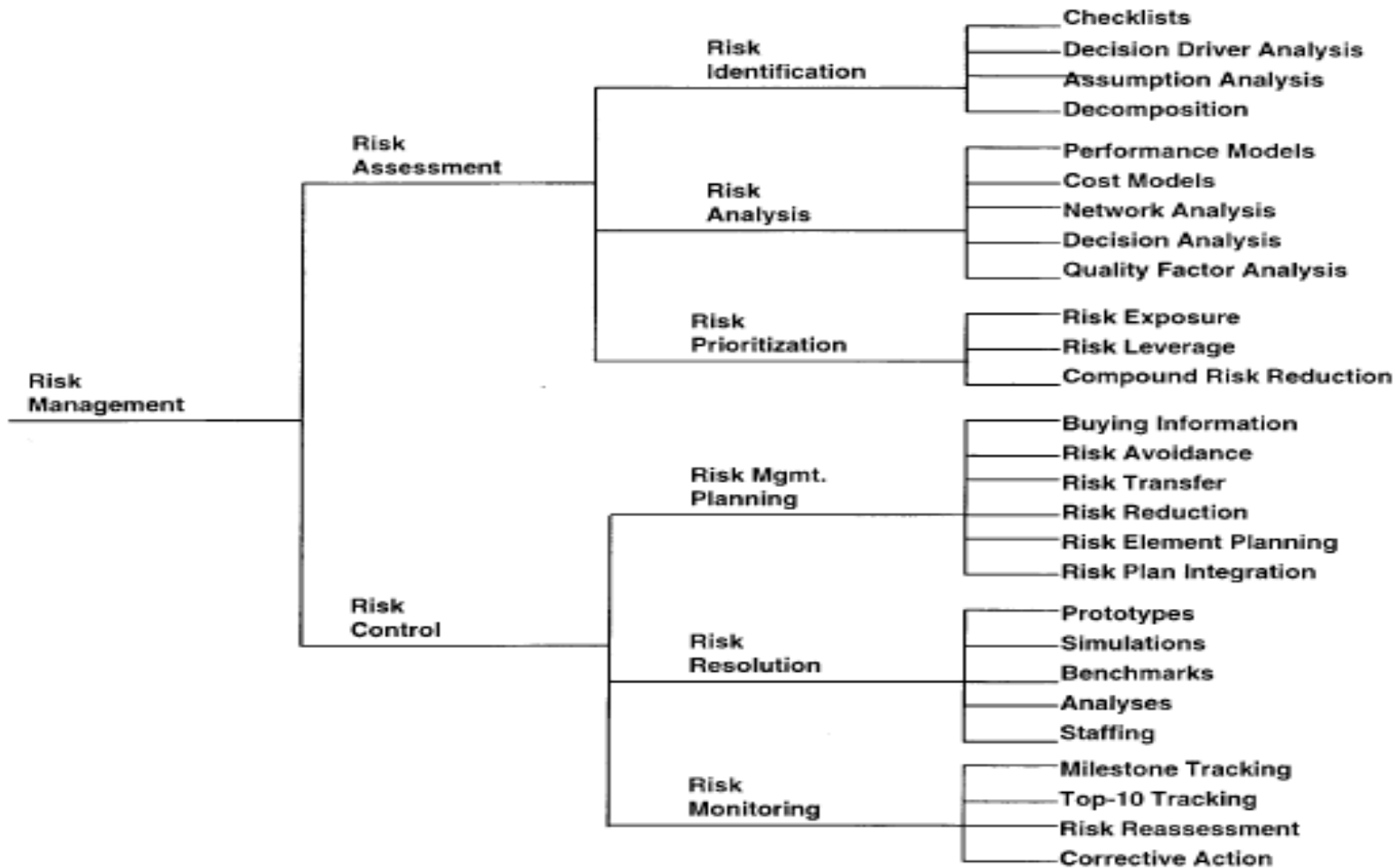
- PROB (kritická chyba zůstane) = 0.2

- Přidaná cena k SW projektu = \$0

Příklad rizikové SW situace – základní paradigma



Řízení rizik při vývoji SW



„Top 10“ rizikové položky



1. Nedostatek pracovníků
2. Plány, rozpočty, proces
3. COTS, externí komponenty
4. Neshody v požadavcích
5. Neshody v uživatelském rozhraní
6. Architektura, výkon, kvalita
7. Změny v požadavcích
8. Zděděný software
9. Externě řešené úlohy
10. Přecenění možností informatiky

„Top 10“ Rizika vývoje SW



1. Personnel Shortfalls

Staffing with top talent; key personnel agreements; incentives; team-building; training; tailoring process to skill mix; peer reviews.

2. Unrealistic schedules and budgets

Business case analysis; design to cost; incremental development; software reuse; requirements descoping; adding more budget and schedule.

3. COTS; external components

Qualification testing; benchmarking; prototyping; reference checking; compatibility analysis; vendor analysis; evolution support analysis.

„Top 10“ Rizika vývoje SW



4. Requirements mismatch; gold plating

Stakeholder win-win negotiation; business case analysis; mission analysis; ops-concept formulation; user surveys; prototyping; early users' manual; design/develop to cost.

5. User interface mismatch

Prototyping; scenarios; user characterization (functionality, style, workload).

6. Architecture, performance, quality

Architecture tradeoff analysis and review boards; simulation; benchmarking; modeling; prototyping; instrumentation; tuning.

„Top 10“ Rizika vývoje SW



7. Requirements changes

High change threshold; information hiding; incremental development (defer changes to later increments).

8. Legacy software

Design recovery; phaseout options analysis; wrappers/mediators; restructuring.

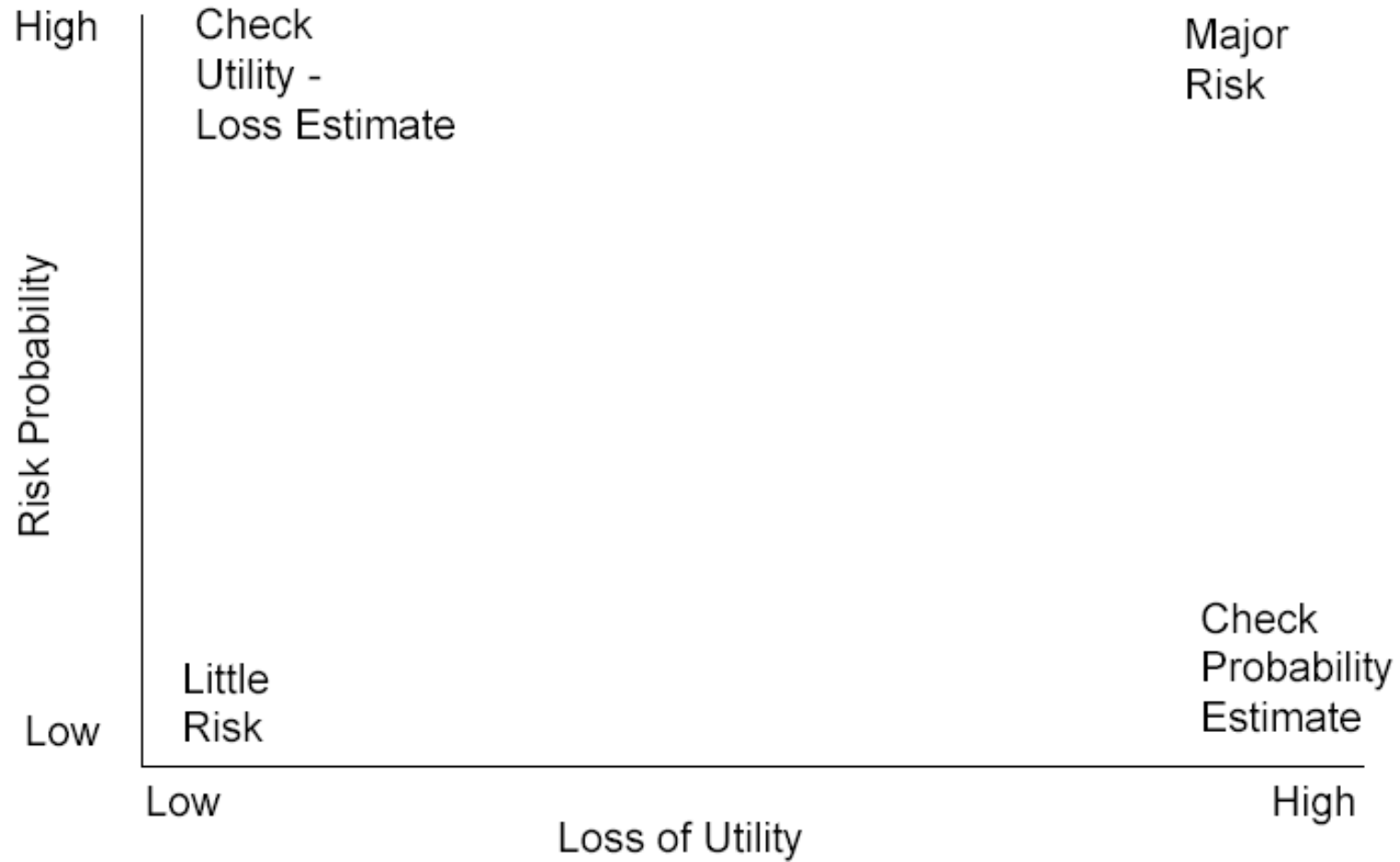
9. Externally-performed tasks

Reference checking; pre-award audits; award-fee contracts; competitive design or prototyping; team-building.

10. Straining computer science capabilities

Technical analysis; cost-benefit analysis; prototyping; reference checking.

Stanovení priority rizik



Risk Reduction Leverage (RRL)



$$\text{RRL} = \frac{\text{RE}_{\text{BEFORE}} - \text{RE}_{\text{AFTER}}}{\text{RISK REDUCTION COST}}$$

· Spacecraft Example

	LONG DURATION TEST	FAILURE MODE TESTS
LOSS (UO)	\$20M	\$20M
PROB (UO) _B	0.2	0.2
RE _B	\$4M	\$4M
PROB (UO) _A	0.05	0.07
RE _A	\$1M	\$1.4M
COST	\$2M	\$0.26M
RRL	$\frac{4-1}{2} = 1.5$	$\frac{4-1.4}{0.26} = 10$

Plány řízení rizik



Otázky pro každou rizikovou položku:

1. Proč?

Význam rizikové položky, vztah k cílům projektu.

2. Co, kdy?

Výstupy pro rozhodnutí rizik, milníky, sítě aktivit.

3. Kdo, kde?

Zodpovědnosti, organizace.

4. Jak?

Přístup (Prototypy, Přehledy, Modely, ...).

5. Kolik?

Zdroje (Rozpočet, plán, klíčoví pracovníci).



Identifikované riziko

- poškození auta a zranění pasažérů při autonehodě cestou do práce

- vyhnutí se

- bydlet blízko práce a chodit pěšky/ používat MHD

- předpokládání

- jet do práce a doufat, že to dobře dopadne

- řízení

- snížení maximální povolené rychlosti, bezpečnostní pásy, zesílení oddělovacích panelů, cesta se zkušeným, bezpečným řidičem

- přenesení

- pojištění auta, záchranný systém, žaloba druhého řidiče

- získání znalosti

- určení nejbezpečnějších aut pomocí nárazových testů, nalezení nejbezpečnější cesty do práce



Identifikované riziko

- být někým zastřelen
- vyhnutí se
 - zákaz ručních palných zbraní
- předpokládání
 - stane se to někomu jinému
- řízení
 - držet se mimo nebezpečné oblasti, být stále ve střehu, koupit neprůstřelnou vestu
- přenesení
 - pojistit se, provozovat záchranný systém, žalovat střelce
- získání znalosti
 - zjistit nebezpečná místa, zjistit varovné příznaky nebezpečí

Techniky řízení rizik

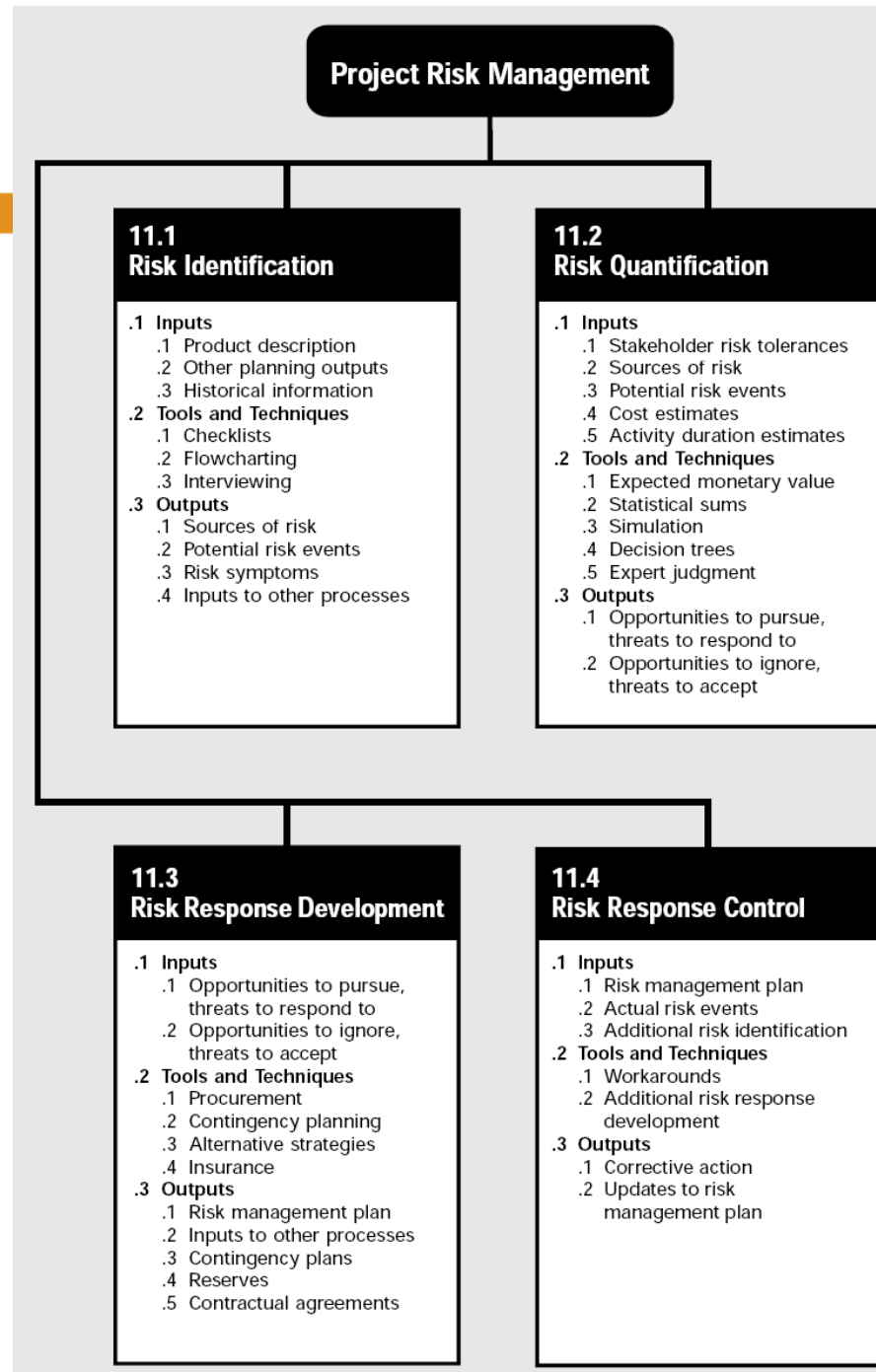


Identifikované riziko

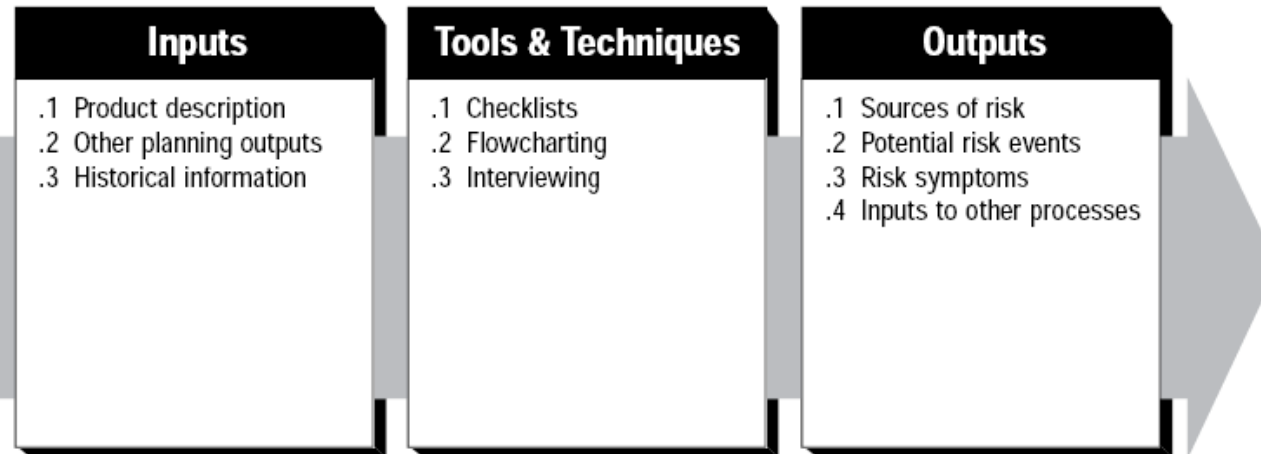
- selhání disku
- vyhnutí se
 - nepoužívat disk
- předpokládání
 - používat disk a slíbit si, že zítra udělám zálohu
- řízení
 - pravidelně zálohovat disk
- přenesení
 - použití utility pro obnovení disku
- získání znalosti
 - určit frekvenci selhání pro různé značky disků



Schéma řízení rizik dle PMI:

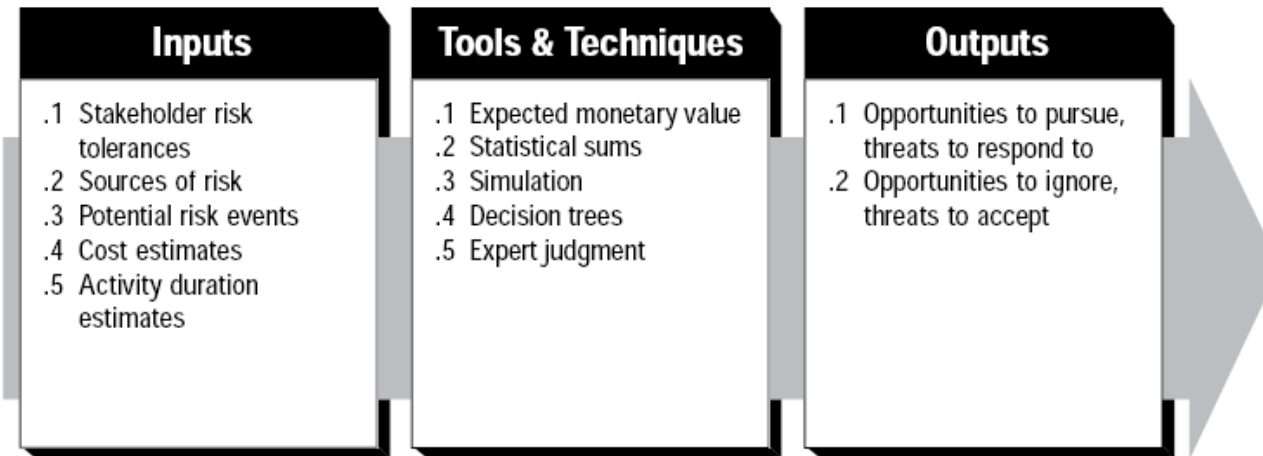


Risk identification



Zdroj: PMI

Risk quantification



Zdroj: PMI

Pravděpodobnostní odhady (příklad)

Nástroj pro ohodnocení rizik

Zdroj: PMI

Activity Name	Low a	Most Likely m	High b	Mean \bar{x}	Sigma σ	Variance σ^2
---------------	----------	------------------	-----------	-------------------	-------------------	------------------------

Triangular Distribution

Initial draft

Gather information	40	45	80	55.0	8.9	79.2
Write sections	35	50	100	61.7	13.9	193.1
Review informally	10	15	30	18.3	4.2	18.1

Inspection

Inspectors inspect	18	25	50	31.0	6.9	47.2
Prepare defects/issues list	10	20	40	23.3	6.2	38.9
Resolve defects/issues	10	25	60	31.7	10.5	109.7
Make necessary changes	15	<u>20</u>	40	<u>25.0</u>	5.4	<u>29.2</u>

Estimated Project Totals: 200 246.0 22.7 ← 515.2

$$\text{Mean} = (a + m + b) / 3 \quad \text{Variance} = [(b - a)^2 + (m - a)(m - b)] / 18$$

Beta Distribution (using PERT approximations)

Initial draft

Gather information	40	45	80	50.0	6.7	44.4
Write sections	35	50	100	55.8	10.8	117.4
Review informally	10	15	30	16.7	3.3	11.1

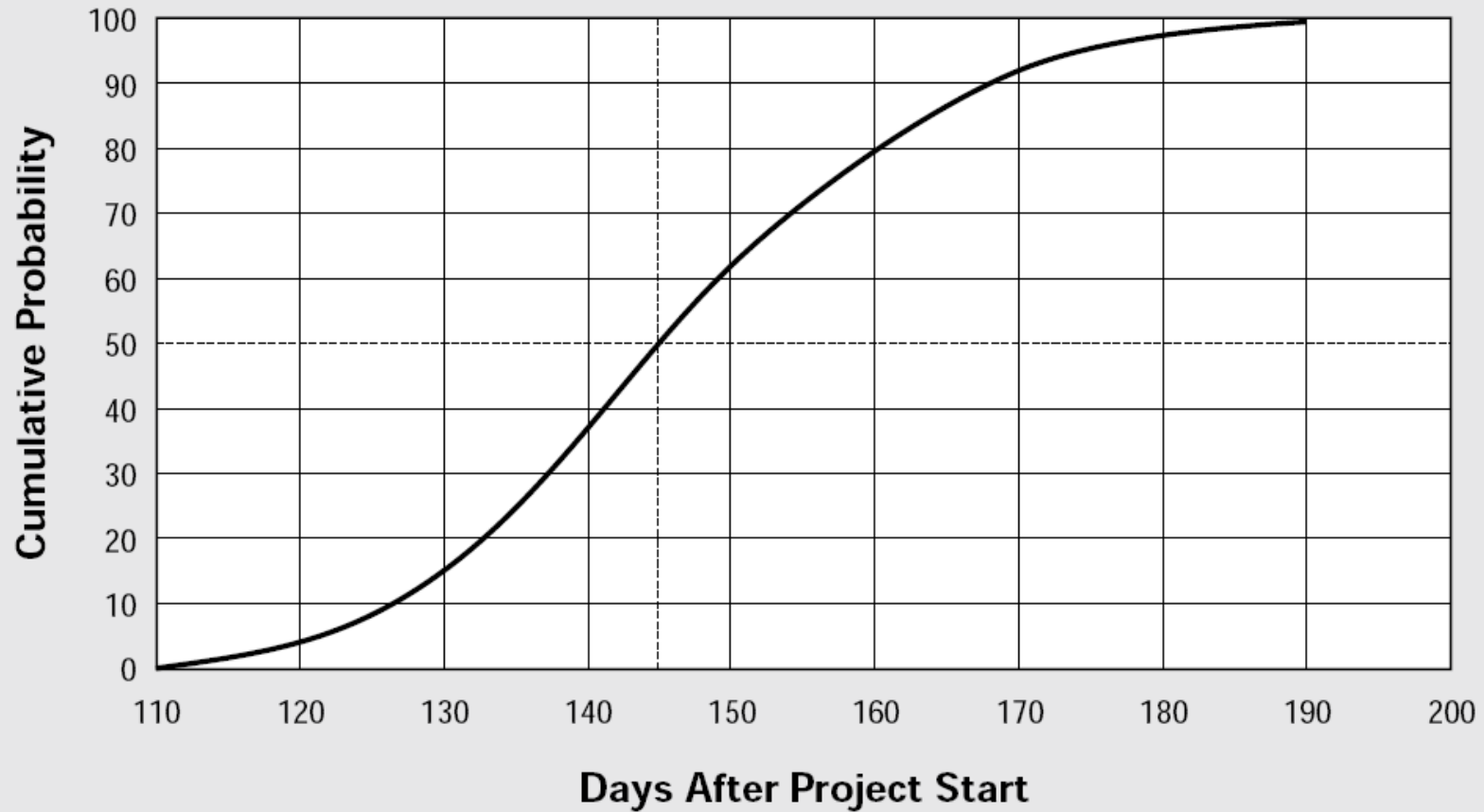
Inspection

Inspectors inspect	18	25	50	28.0	5.3	28.4
Prepare defects/issues list	10	20	40	21.7	5.0	25.0
Resolve defects/issues	10	25	60	28.3	8.3	69.4
Make necessary changes	15	<u>20</u>	40	<u>22.5</u>	4.2	<u>17.4</u>

Estimated Project Totals: 200 223.0 17.7 ← 313.2

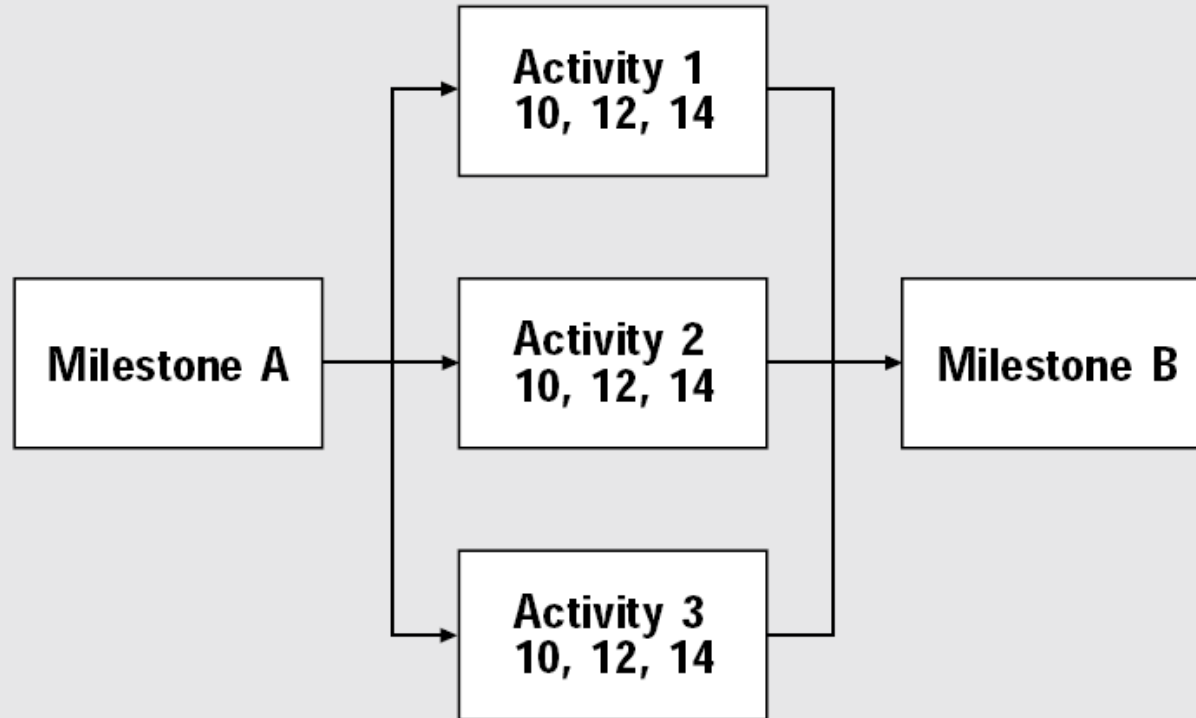
$$\text{Mean} = (a + 4m + b) / 6 \quad \text{Variance} = [(b - a) / 6]^2$$

Simulace „Monte Carlo“ (příklad)



This S-curve shows the cumulative probability of project completion by a particular date. For example, the intersection of the dashed lines shows that there is a 50 percent probability that the project will be finished within 145 days of its start. Project completion dates toward the left have higher risk while those toward the right have lower risk.

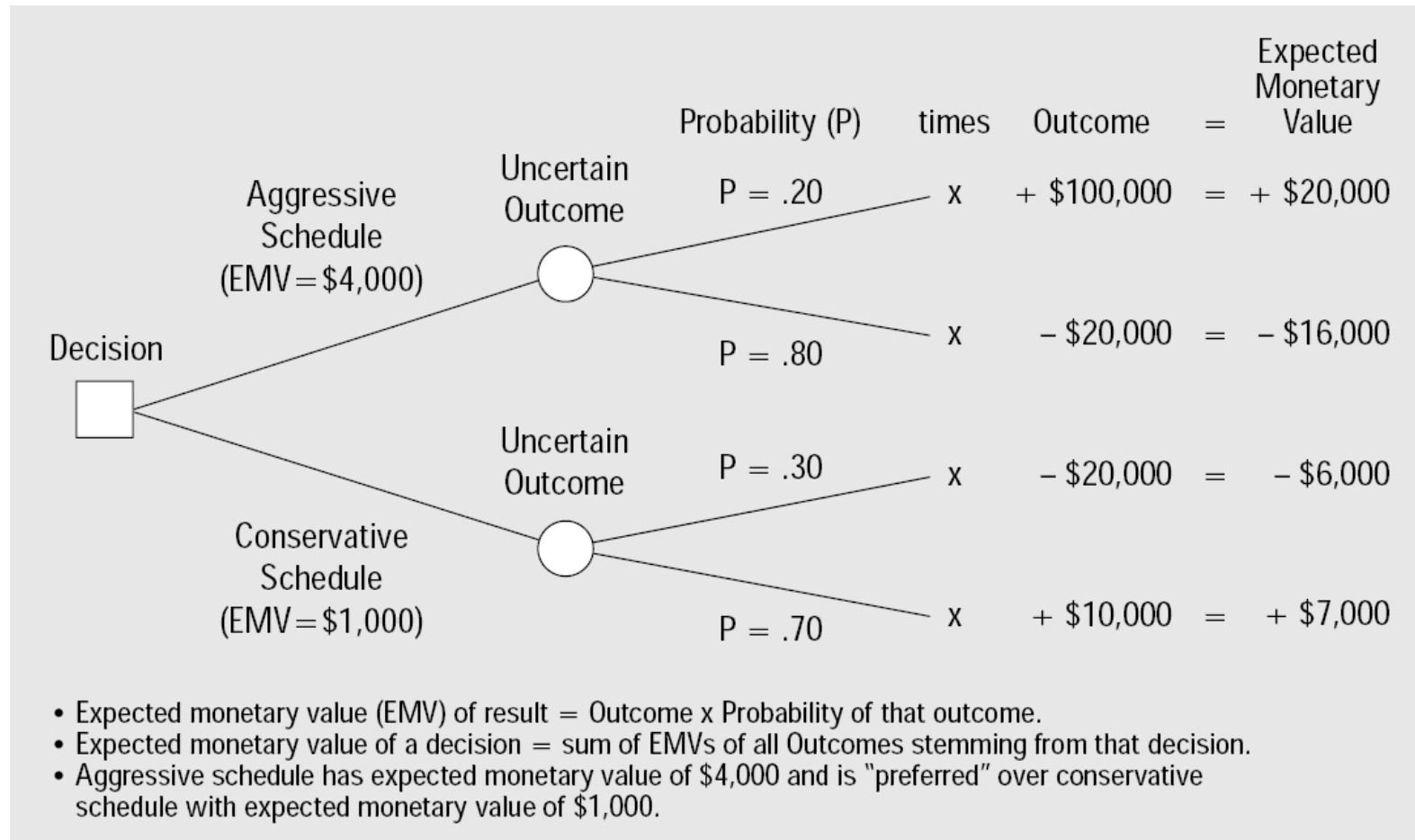
Rizika plynoucí z konvergence cest (příklad)



Activities 1, 2, and 3 all have an expected duration of 12 days, ± 2 days. The CPM calculated duration of Milestone A to Milestone B is, therefore, 12 days. However, the actual duration will be greater than 12 days if any one of the activities is delayed. This is true even if the other activities finish in less than 12 days.

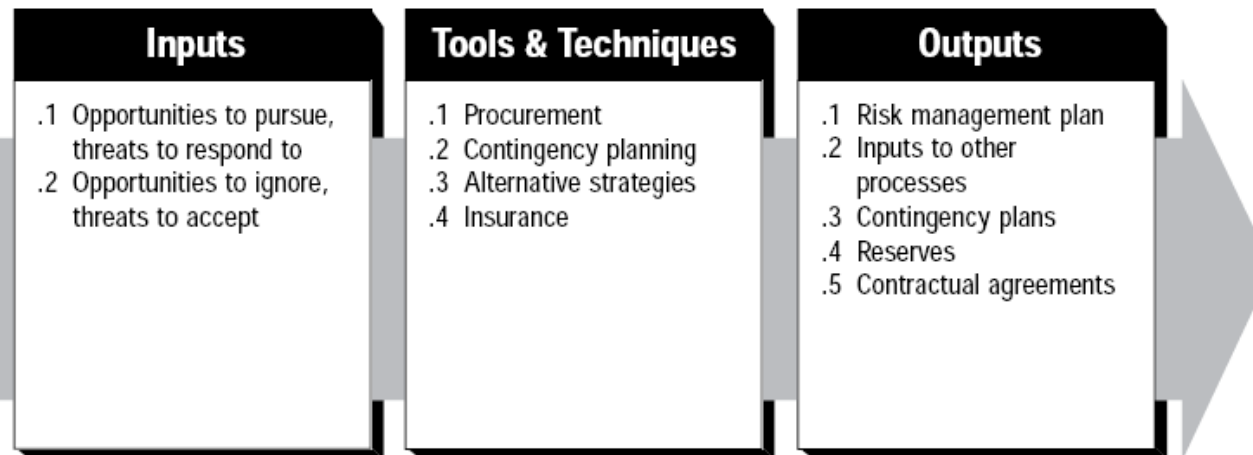
Zdroj: PMI

Rozhodovací strom (příklad)



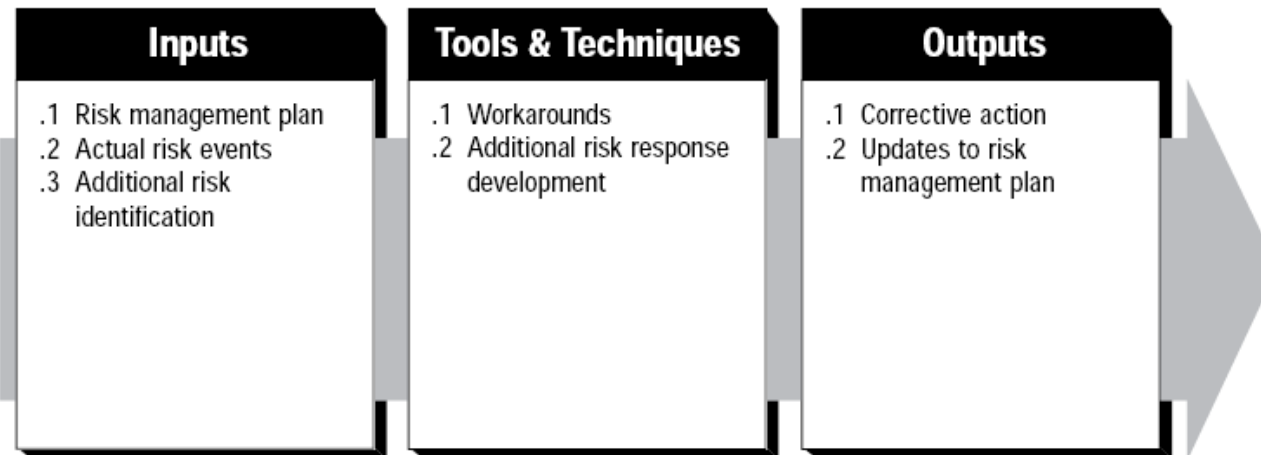
Zdroj: PMI

Risk response development



Zdroj: PMI

Risk response control



Zdroj: PMI



- Rizikové řízení je vhodné u komplexních SW projektů, kde umožňuje:
 - vyhnout se překvapením,
 - redukce nákladů.
- Ověřené techniky řízení rizik jsou k dispozici.
- Rizikové řízení nelze dělat podle kuchařky.

Úkoly



- Revidujte přiřazení pracovníků podle jejich dovedností.
- Prověřte potřebné dovednosti a naplánujte zvýšení kvalifikace.
- Identifikujte hlavní rizika a odhadněte jejich expozice (předpokládejte znalost nákladů).
- Přiřaďte rizika k jednotlivým fázím projektu.

„Nečekaný“ úkol



Po té, co jste vše naplánovali a zahájili jste projekt, postihla Vaši firmu morová epidemie. Ze dne na den jste přišli o dvě třetiny programátorů. Ve Vašem týmu dále nezůstal nikdo, kdo má zkušenosti s tvorbou uživatelského rozhraní podobných aplikací, jaké vyvíjíte.

- Navrhněte seznam opatření, kterými budete danou situaci řešit.
- Jak se tato opatření projeví na časovém plánu?