Risk analysis

DDP - Defect Detection and Prevention

CS 645

Grad Tutorial

[redacted]

University of Waterloo, 2007

Outline

- Risk Analysis
  - Definition of a risk
  - Risk Management Process
    - Risk identification
    - Risk assessment
    - Risk control
  - Definition of Risk Analysis
  - Why? When? Who?

- A tool for Risk Analysis
  - DDP - Defect Detection and Prevention
    - The Three-Step process
    - Applied Example – Meeting Scheduling System
    - Summary and Advantages

Definition of a risk

- Definition: A factor whose occurrence may result in some loss of satisfaction of some corresponding objective
- A risk has a likelihood to occur and one or more consequences on the project that will experience undesirable events
- Two main types of risks
  - Product-related risks
    - Negative impact on functional or non-functional objectives on the product
    - Examples: failing to meet the product's specified requirements
  - Process-related risks
    - Negative impact on objectives of the development process
    - Examples: schedule delay, cost overruns, outright cancellation

Risk Management – In General

- Risk Management is a process that includes:
  - Identifying risks
    - Checklists, component inspection, risk trees
  - Assessing risks
    - Qualitative assessment
      - Quality scales “very unlikely” to “very likely”
    - Quantitative assessment
      - Numerical scales
  - Control risks
    - Take actions to reduce high risks in a cost effective way
- The process of RE Risk Management focuses on risks related to requirements and requirements processes which might lead to a delay, over-cost or even failure of the project

Definition of Risk Analysis

- Risk analysis is the process of examining each identified risk issue to estimate the likelihood of a risk and predict the impact on the project

- Some typical risk analysis techniques
  - Network analysis
  - Decision trees
  - Cost models
  - Performance models
  - DDT (software tool)

Risk analysis – Why? When? Who?

- **Why?**
  - All projects have risks
  - Important to identify risks to avoid undesirable events to occur
  - Save a lot of money - unidentified risks can be very expensive surprises
  - Avoid overrun of time
  - **But…**
    - No guarantee to succeed with a project
    - Only useful if the risk management process continues and actions are defined and executed to mitigate the identified risks
- **When?**
  - Most important in the requirement phase
  - Best result if risk analysis is used as a continuous process, because of:
    - Changes made late in the life cycle can cause associated risks and high costs
    - New risks can appear
- **Who?**
  - One person or a group of people
  - Involves every stakeholder
  - Experts
  - **Note:** The quality of the result highly depends on the competence and the experiences of participants

DDP – Defect Detection and Prevention

- **Description of DDP**
  - Software tool developed by NASA
  - Process for achieving life-cycle risk management
- **Goal:** To find mitigations that cost-effective reduce risks and give aid in the achievement of continuous risk management
- **Use DDP to:**
  - Plan how to reduce risk in a cost-effective manner
  - Plan how to accept more risk in exchange for reduced cost and schedule, more functionality, etc.
  - Maintain a desired risk profile through the lifetime of the project.
  - Assess risk status

DDP cont.

- **DDP process:**
  - Makes the user think about:
    - Requirements (Objectives)
    - Potential risks (Failure modes)
    - Countermeasures (PACTS; Preventative measures, Analyses, process Controls and Tests or Mitigations)
  - Analyzes the consequences of the potential risks if they should occur by scoring their impact on the requirements
  - Scoring the effect which is the (mitigation times the risk) proportion by which risk reduced if mitigation is applied
  - Implemented over the entire project life cycle
- **Result of DDP:** Optimized collection of mitigation activities performed on a project

Using DDP on Example Meeting Scheduling Software

(Case study 3 in course package)

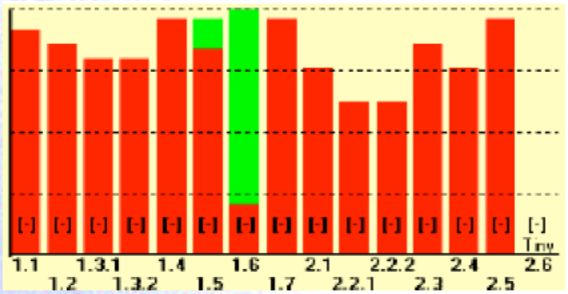
- A meeting initiator informs potential participants about the need for a meeting and specifies a date range within which the meeting should take place, asking them to return their constraints within the time interval.
- Constraints are expressed as two sets;
  - one **exclusion** set (dates in date range where at participants **can not attend**)
  - one **optional** set (**can attend**)
- To know the participant's constraints we have to obtain them with email requests.
- Initiator also ask for specific requirements on meeting room.
- The scheduled meeting date should belong to the stated date range and to none of the exclusion sets. The date should also belong to as many preference sets as possible and for the preferences of "important" participants. A new scheduling cycle is required in case of date or room conflict.
- Conflicts can be resolved in several ways: the initiator may extend the date range, some participants may remove dates from their exclusion set or some participants may decline the invitation to attend the meeting.
- The software should provide major improvements in several aspects like participant attendance should be increased, meetings should be scheduled as quickly as possible and notifications should be sent to participants.

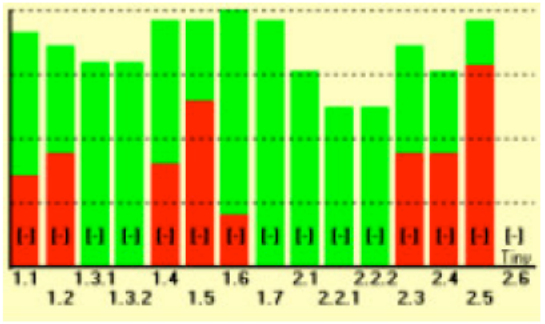
The DDT process

Step 1 - Developing the Requirements Matrix (RM)

Step 2 - Developing the Effectiveness Matrix (EM)

Step 3 - Optimizing the Residual Risk





Step 1 - Developing the Requirements Matrix (RM)

- **Goal**:
  - To develop a prioritized set of failure modes
  - This goal may also identify which requirements that are most “risk-driving” and the most irrelevant requirements
- List the requirements
  - Requirements may be individually weighted, relative to their importance
- List the failure modes
  - Failure modes may be weighted by their probability of occurrence (i.e. with no mitigation activities) - in most cases this weight factor is chosen to be 1.0.
- Build a RM that for each pair of objective associated risk specifies an **estimated loss if the risk occurs** (**impact**)
- You need domain experts, estimates, or models and simulations to get good impact values

Step 1 cont.

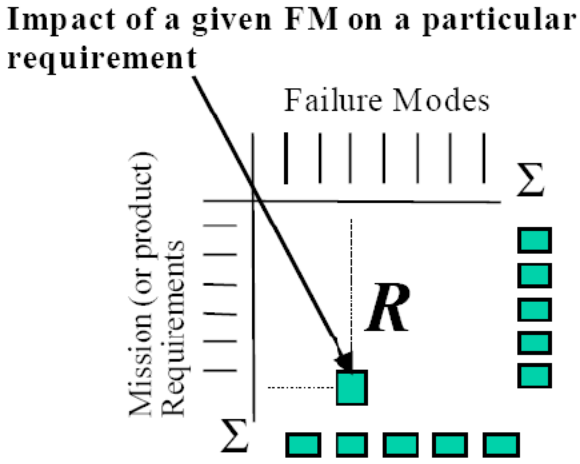
- Calculate the risk criticality of each failure mode:

$$Criticality(FM) = Likelihood(FM) * \sum_{req} (\mathrm{Im}\, pact(FM, req) * Weight(req))$$

- Sort by the criticality and find the “tall pole” failure modes
- Calculate the loss of objective for each requirement:

$$Loss(req) = Weight(req) * \sum_{FM} (\mathrm{Im}\, pact(FM, req) * Likelihood(FM))$$

- Identify the most “risk-driving” and also the most irrelevant requirements.
- **Result**: A RM and DDT will also provide a bar chart visualizing the critical impact, by decreasing order, of the various risks on all requirements



RM for Meeting Scheduling System

Risks (Failure Modes)							
Objectives (Requirements)	**Weight (obj)**	Participant does not read emails	Participant does not reply on requests	Room with required equipment is not avaliable	System response is too close to meeting	Important participant has last-minute change	**Loss of objective**
Likelihood(r)		0,4	0,3	0,1	0,3	0,5	
Time taken to schedule meetings reduced	0,5	0,6	0,8	0,2	0,7	0,2	0,405
Send out notification asap when time and place are found	0,4	0	0,8	0	1	0,2	0,552
Participant avarage attendance increased	0,3	0,8	0,8	0	0,8	0,5	0,462
Schedule conflicts reduced	0,6	0,2	1	0	0	0,7	0,786
Risk criticallity		0,264	0,396	0,016	0,042	0,37	

Step 2 - Developing the Effectiveness Matrix (EM)

- **Goal:** Develop a set of options (PACTs) for preventing or detecting the failure modes
- List the countermeasures (PACTs)
- List the same failure modes as in the RM
- The PACT options for detecting and preventing failure modes range from design rules to system level tests and they have varying effectiveness against different failure modes
- The determination of the effectiveness of a given PACT on a given failure mode can be accomplished a number of ways:
  - Experts
  - Historical data
  - Results of experiments or measurements
  - Data from the literature

Step 2 cont.

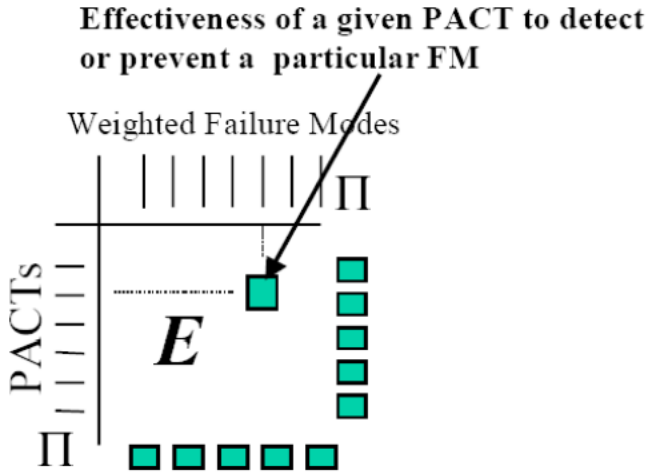
- Build an Effectiveness matrix (EM) that captures the effectiveness of each PACT against each (weighted) failure mode and is scored as the fractional reduction in the likelihood of occurrence of the failure mode
- Calculate the combined risk reduction

$$combined\,\mathrm{Re}duction(FM) = 1 - \prod_{PACT}(1 - \mathrm{Re}duction(PACT, FM))$$

- Calculate the overall single effect of each PACT, to identify the most globally effective one

$$overallEffect(PACT) = \sum_{FM}(\mathrm{Re}duction(PACT, FM) * Criticality(FM))$$

- **Note**: DDP calculates a more refined option for overall effect of a PACT based on failure modes with their likelihoods as already reduced by whichever of the other PACTs have already been selected
- **Result:** A risk balance chart shows the residual impact of each risk on all objectives if the corresponding countermeasure is selected. The DDP prepares the team with a collection of possible PACTs and the costs associated with them

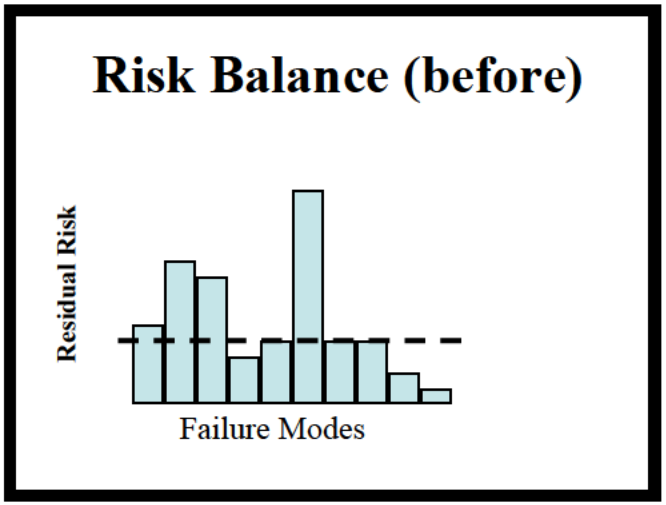


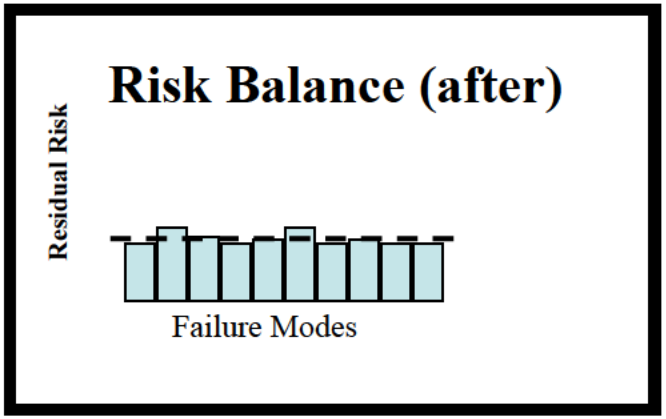
EM for Meeting Scheduling System

	Risks (Failure Modes)					
Countermeasures (PACTs)	Participant does not read emails	Participant does not reply on requests	Room with required equipment is not avaliable	System response is too close to meeting	Important participant has last-minute change	**Overall single effect of countermeasure**
Likelihood(r)	0,4	0,3	0,1	0,3	0,5	
Email reminder sent	0,7	0,7	0	0,1	0	0,4662
Change the meeting, greater time range	0,2	0,2	0	0,1	0	0,1362
System has access to personal e-agenda	0,3	0,2	0,1	0,2	0,3	0,2794
Change the meeting, less constraints (equipment)	0	0	0,9	0	0	0,0144
Cancel a meeting and send email confirmation	0,8	0,8	1	0,7	0,9	0,9064
Combined risk reduction	0,9664	0,9616	1	0,8056	0,93	

Step 3- Optimizing the Residual Risk

- **Goal:** Select the optimal combinations of PACTs which minimize the risks, subject to various resource constraints (time, money, etc.) for the project
- Each PACT has resource costs associated with it. This cost needs to be estimated by experts.
- Since each PACT has varying effectiveness against different failure modes, one can and must "mix and match" different PACT combinations each of which has associated resource costs
- DDT provides a risk balance chart displays
  - Status of each of the failure modes
  - Degree to which it is currently impacting
  - requirements, taking into account the
  - mitigating effects of selected PACTs.
- Identify the under-covered risks ('tall poles') and the over-covered risk
- **Result:** Optimal (or near optimal) selections of countermeasurements (PACTs) that the DDT has found by using a method of simulated annealing





DDP – in the Project Life Cycle

- **During the project life cycle:**
  - Requirements and hardware maturity evolve
  - Their refinement to lower levels may result in modification of various levels of requirements
  - Evolution of the design results in evolved failure modes
- **DDP process allows to**:
  - Capture these changes
  - Evaluate their impact on the “tall pole” failure modes
  - Identify risk-driving requirements
  - Update the Effectiveness matrix
  - Re-evaluate the Residual Risk

Summary and some Advantages of DDP

- **DDP approach:**
  - Provides a good illustration of the kind of technology supporting the risk analysis process during both
    - Requirements evaluation
    - Entire project life cycle
  - Links explicitly to objectives and requirements
  - Shows typical quantitative reasoning schemes that are available for requirements evaluation
  - Has tool support for carrying out such reasoning and for vitalizing the results

- **Some advantages of DDP**
  - Reduces development and operating costs
  - Reduces risk and increases safety and reliability
  - Designs better software architecture and more maintainable systems
  - Enable companies to handle more complex systems in the future

Resources

- Risk Management in a Software Development Life Cycle
  http://www.cis.um.edu.mt/~abut/
- DDP Tutorial on the Web
  http://ddptool.jpl.nasa.gov/
- DDP – A tool for life-cycle risk management
  http://ddptool.jpl.nasa.gov/docs/f344d-slc.pdf
- Course Package - Software Requirements Specification & analysis