Introduction to Risk Management for Software Projects

Peter Kolb

Purpose of Presentation

- To provide an Overview of the Risk Management Process
- To describe Specific Risks with Distributed and Outsourced Software Engineering
- To explain Software Product Risk Management

Objectives of Project Risk Management

Improve the predictability of a project!

By:

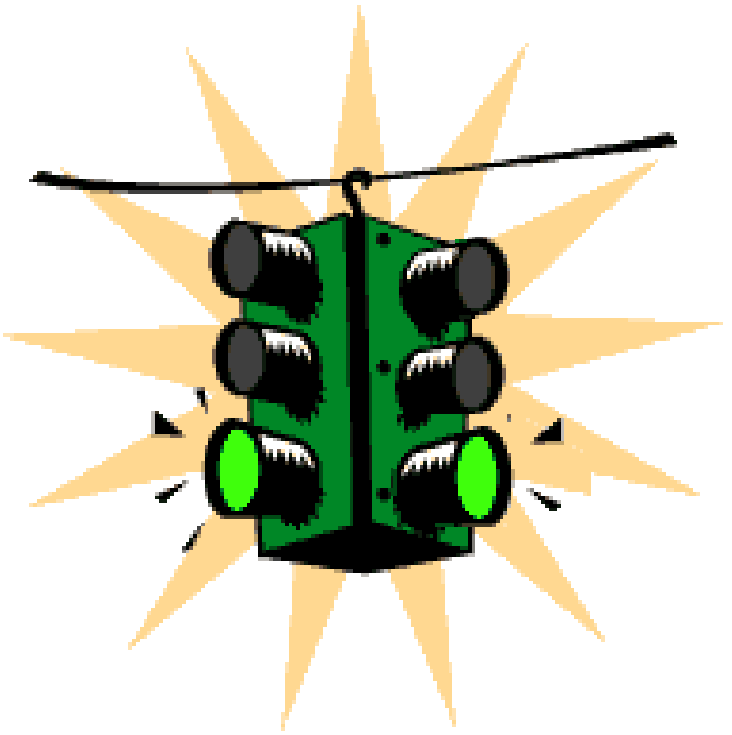
- Raising awareness and visibility of risks
- Managing risks by mitigation actions to prevent major disasters
- Preparing for contingency

What Is A Risk?

- A Risk is a Potential Event with Negative Consequences that Has Not Happened Yet.
  - However a Risk could also be defined as the event with unforeseen positive consequences.
- A Possibility of Loss — Not the Loss Itself!
  - A *source* of problem during a project
  - Avoid labeling the cost of a risk as a risk (e.g. schedule slippage). Find the causes!
  - Strike at the root of the problem, not the leaves!
- Something that Makes the Project Special
  - In the widest sense everything is a risk
  - There are better ways of handling recurrent problems!

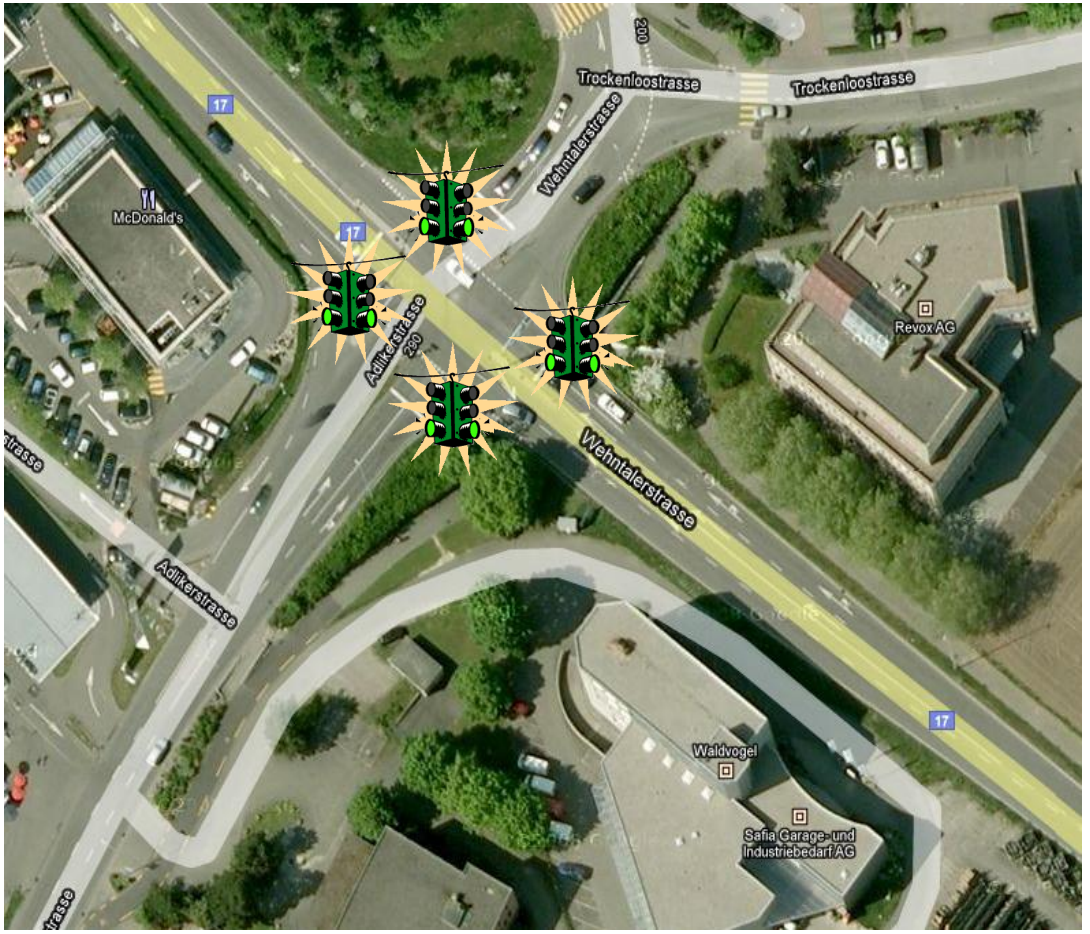
Sequence of Events

- 1. Failure, cause of hazard



Sequence of Events

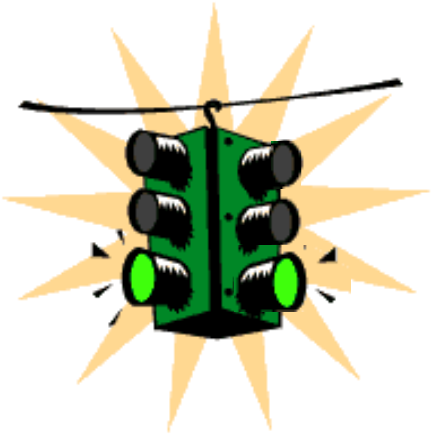
2. Hazard [Gefährdung] = potential source of harm



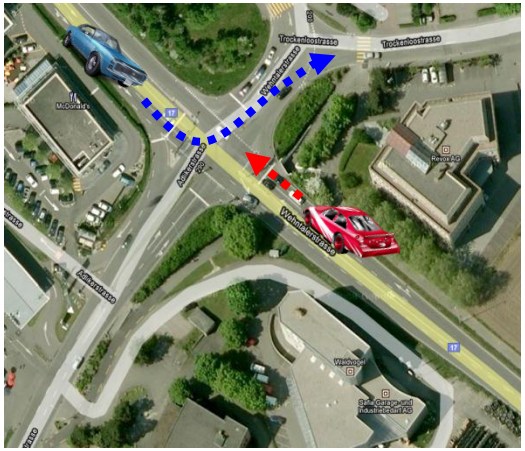
Sequence of Events

3. Hazardous event

… which has a certain likelihood



+



+

+

=

Sequence of Events

4. Harm [Schaden, Unheil]

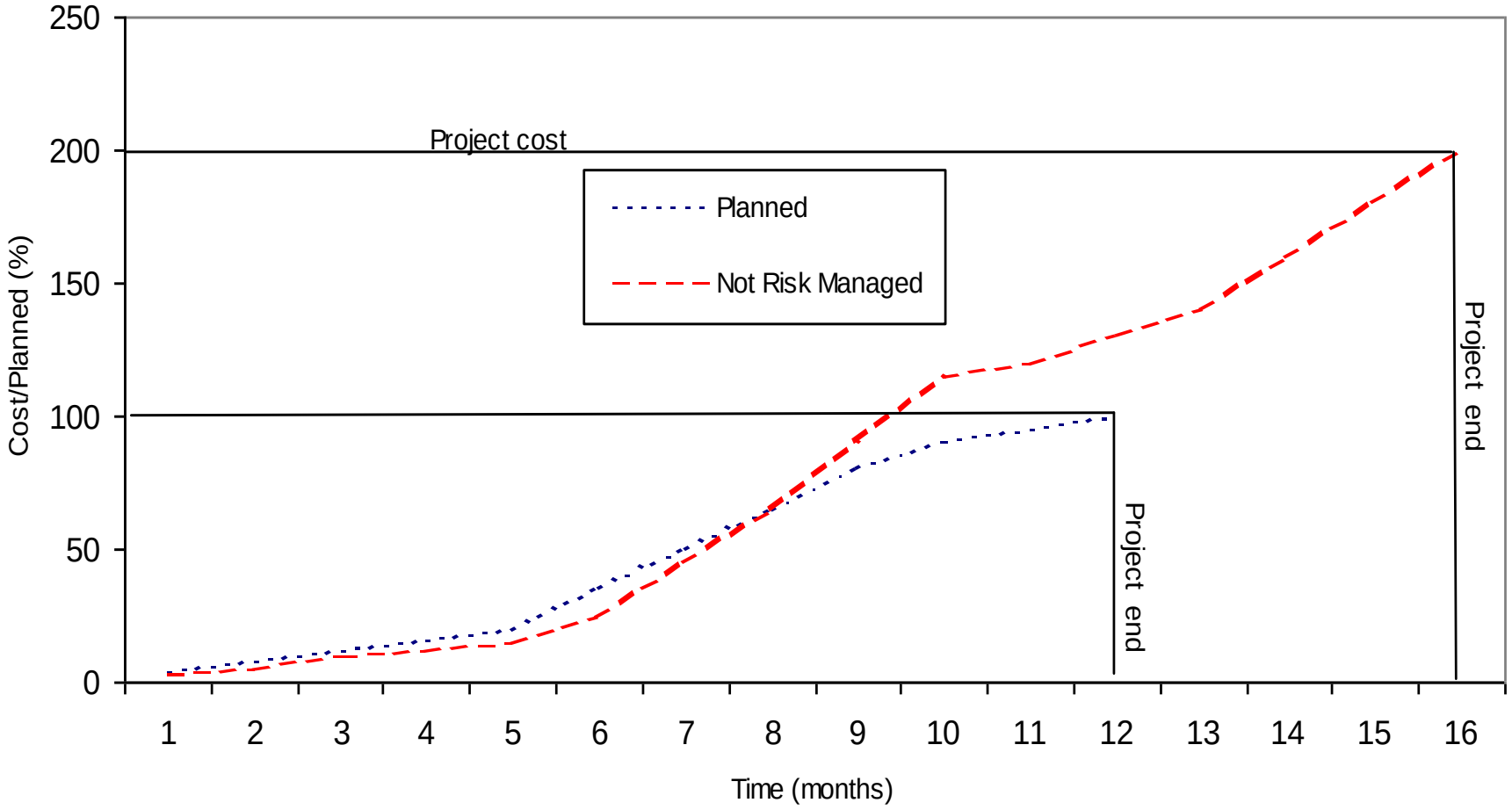
…which has a certain severity

Definition of Risk

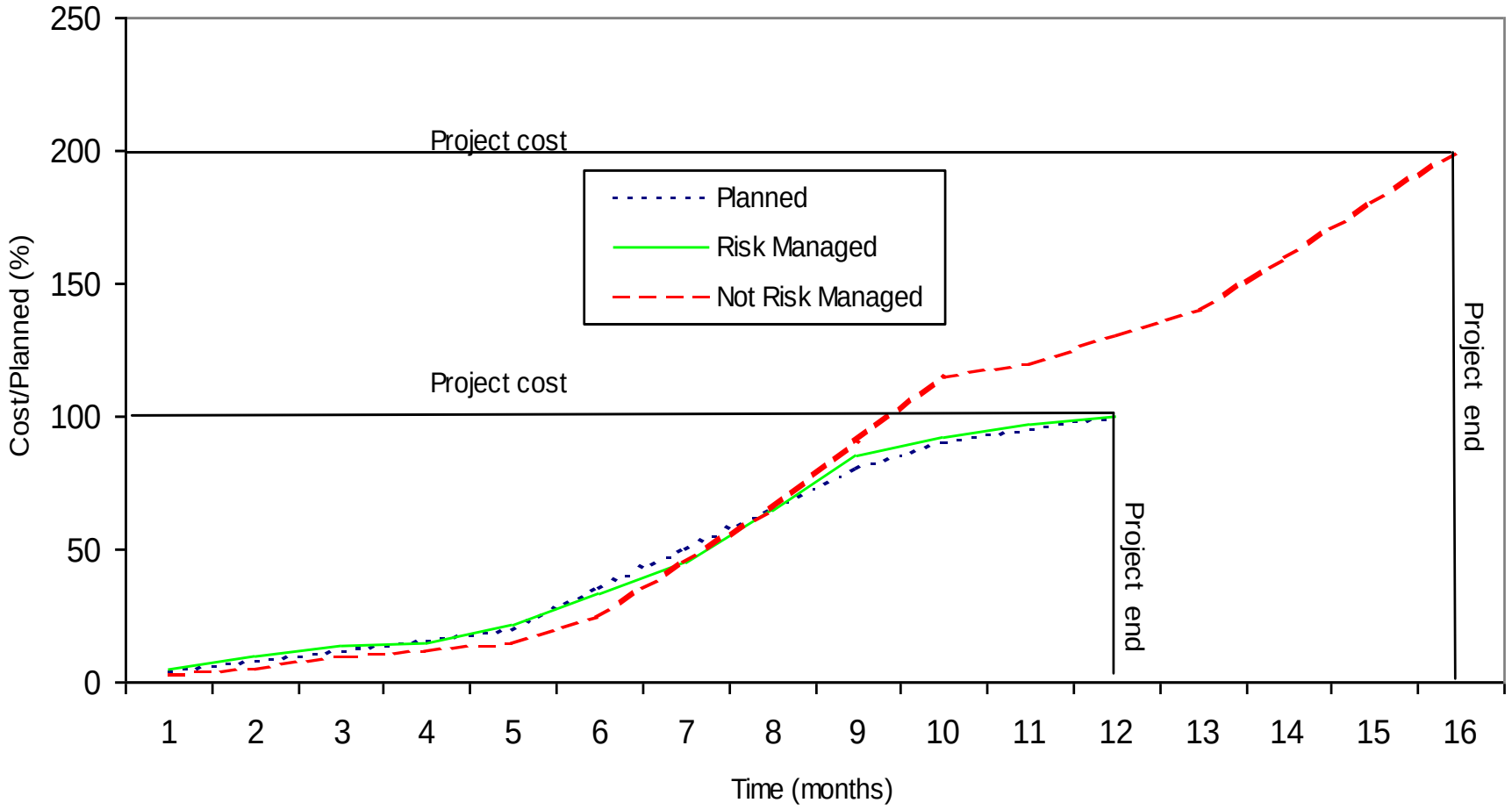
Risks are defined by their

- Likelihood of Occurrence of Harm and
- Severity of Harm

Project Predictability



Project Predictability

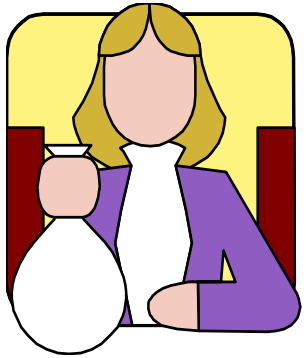


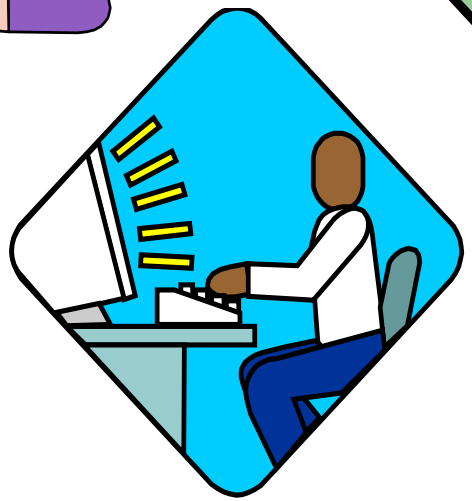
Is this Risk Management?

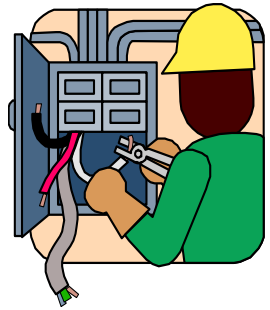
Risk	Description
COTS dependency	Windows XP SP xy, ERP system version yz.
Human resources	The availability of human resources from xxx is hard to control since many of the people still have work to do in older projects. Unfortunately, that work has usually a higher priority
Supplier delivery time dependency	The outsourced application components may be delayed due to plan execution slippery.
…	

Who is involved in Risk Management?

- Customer
- End-user
- Project Team
- Management
- Product Management
- Related Projects
- Subcontractors and Suppliers







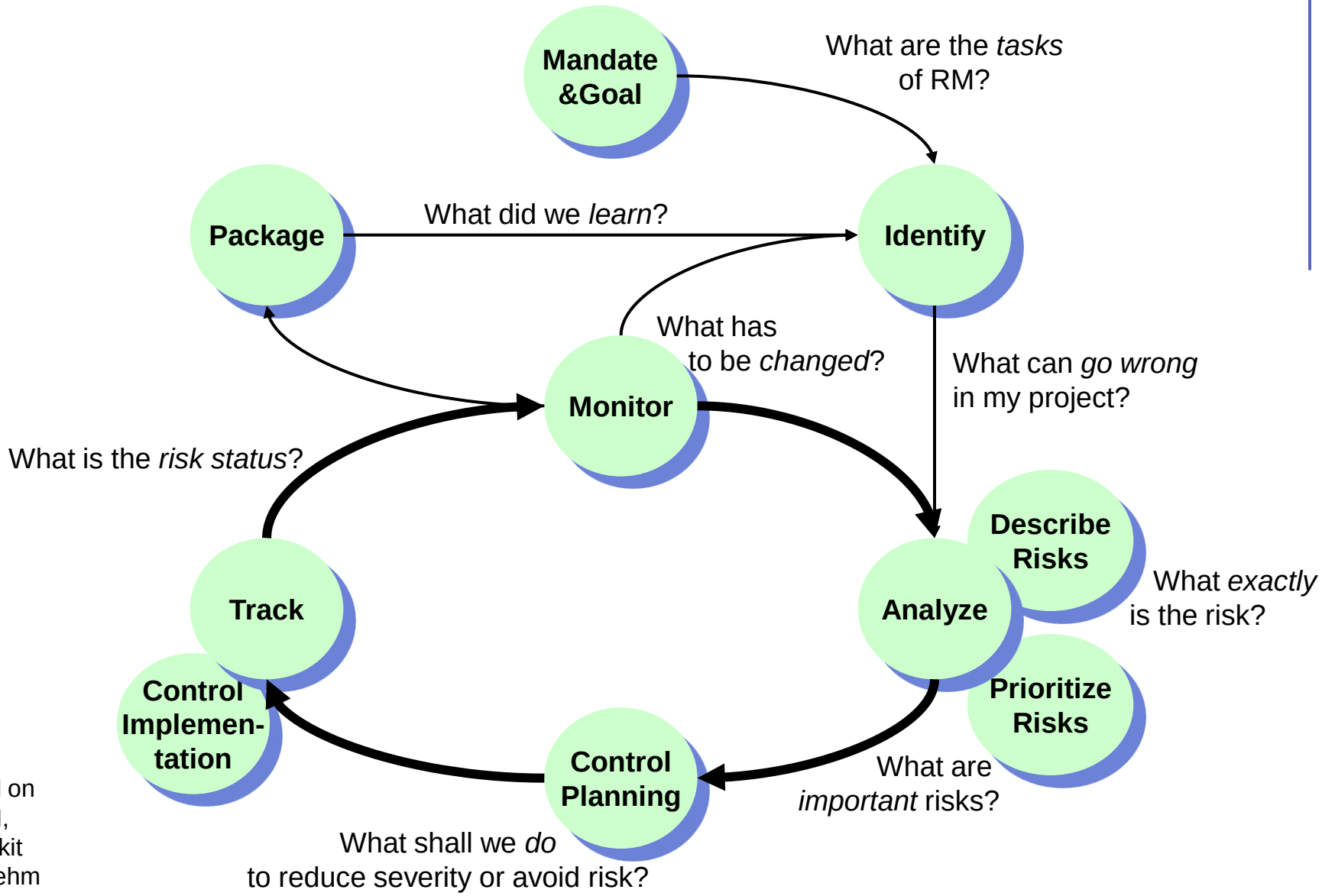
Risk Management is Communication!

When?

- Business-Case Analysis for Outsourcing
- Preparation for Outsourcing (Partner Selection, Frame Contracts)
- Status and Briefing of Requirements,
- Detailed Contracts and Project Planning
- Milestones in Project Execution
- Transfer and Maintenance

Risk Management is a Continuous Process!

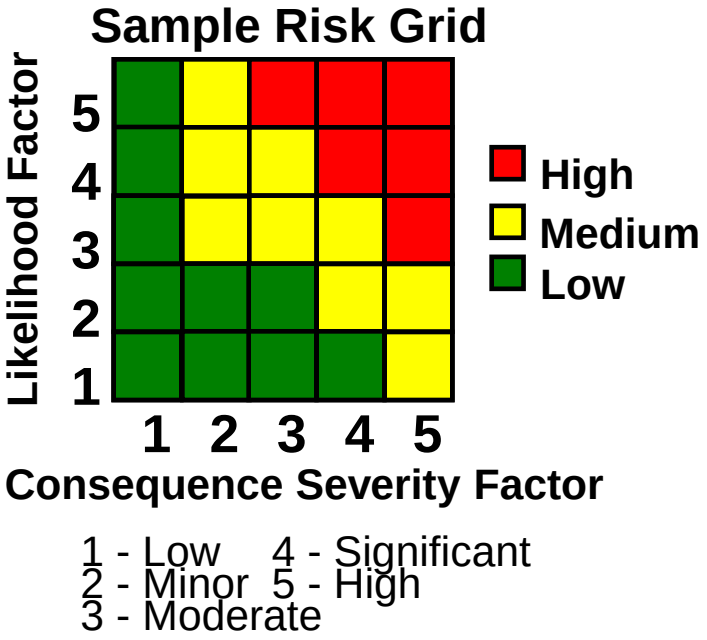
Generic Risk Management Process



- Based on SEI, Riskit Boehm

Risk Analysis Method

- Describe the Risks
  - Brainstorming potential risks
  - Walkthrough of the risk identification checklist
- Analyze and Prioritize Risks
  - Walkthrough risk sheet and estimate the probability and cost of each risk
  - Calculate risk rating of each risk (e.g. likelihood * consequence)
  - Prioritize in risk classes concentrate on class “High”



Likelihood

What Is the Likelihood the Risk Will Happen?		
Level		**Your Approach and Processes...**
1	Not Likely:	...Will effectively avoid or mitigate this risk based on standard practices
2	Low Likelihood:	...Have usually mitigated this type of risk with minimal oversight in similar cases
3	Likely:	...May mitigate this risk, but workarounds will be required
4	Highly Likely:	...Cannot mitigate this risk, but a different approach might
5	Near Certainty:	...Cannot mitigate this type of risk; no known processes or workarounds are available

Severity of Consequence / Harm

Given the risk is realized, what would be the magnitude of the impact?			
Level	**Technical**	**Schedule**	**Cost**
1	Minimal or no impact	Minimal or no impact	Minimal or no impact
2	Minor perf shortfall, same approach retained	Additional activities required; able to meet key dates	Budget increase of less than 1%
3	Mod perf shortfall, but workarounds available	Minor schedule slip; will miss need date	Budget increase of less than 5%
4	Unacceptable, but workarounds available	Program critical path affected	Budget increase of less than 10%
5	Unacceptable; no alternatives exist	Cannot achieve key program milestone	Budget increase of more than 10%

Risk Mitigation and Contingency Planning

- List Mitigation Actions
  - Start with most severe risks
  - List possible actions to reduce probability and/or cost
  - Some risks can be avoided (e.g. avoid a specific requirement)
- Contingency Planning
  - Only for the most severe risks that *cannot* be mitigated
  - List actions to take should the risk materialize

Monitor

- Risks identified as “High” are tracked at the Program Level. The status of each step in the risk reduction plan is updated and reported at the regularly scheduled reviews by the Project Manager.
  - Actions are initiated as required where risk reduction plan activities are not being accomplished.
  - Special briefings of program risks to program management will also be scheduled as needed.
- “Medium” Risks are monitored on Project Management level.
- Re-Assess Risks regularly:
  - Where the taken risk control measures successful?
    i.e. Likelihood and damage of controlled risks reduced?
  - Did the risk control measures introduce new risks?
  - Additional other risks identified?
    E.g. through early evaluation with customers. Analyze them.

Supplier Selection Risk Factors

- Supplier selection process / criteria
- Supplier capability evaluation
- Executive (or customer) influence on selection
- Number of supplier candidates
- Selection process documentation

	Risk Factors	*Low Risk Cues*	*Medium Risk Cues*	*High Risk Cues*
	Supplier Selection Risk Factors			
1	Supplier selection criteria	organization weighs technical, process and cost implications when selecting supplier	organization advocates mitigating technical and process related risks while selecting low cost	organization expects low cost supplier will be selected
2	Supplier evaluation	potential suppliers' technical and process capabilities were reviewed by technical	supplier alternatives were reviewed based on questionnaires or other high level materials	supplier capabilities reviewed by a small team of technical experts, who recommended selection without looking at alternatives
3	End user involvement in supplier eval.	end users were directly involved in evaluation of the supplier	end users reviewed the results of the evaluation	end users were not involved in the supplier evaluation
4	Executive (or customer) influence	executives have expressed no written or verbal support for any particular supplier	executives have made written or verbal comments favoring a particular supplier	executives have made a written or verbal mandate of a particular supplier or customer has selected the supplier
5	Number of supplier candidates	several qualified suppliers from which to choose	just a few qualified suppliers	this candidate is the sole potential supplier, thus evaluation is almost irrelevant; or all supplier candidates have poor prior
6	Selection process documentation	the evaluation and selection process follows an approved, documented organization	the evaluation and selection process were based on external recommendations	no documented evaluation and selection process was used
7	Evaluation criteria	supplier evaluation criteria consider defined requirements	supplier evaluated using pre-defined evaluation criteria	no evaluation criteria used in supplier selection process

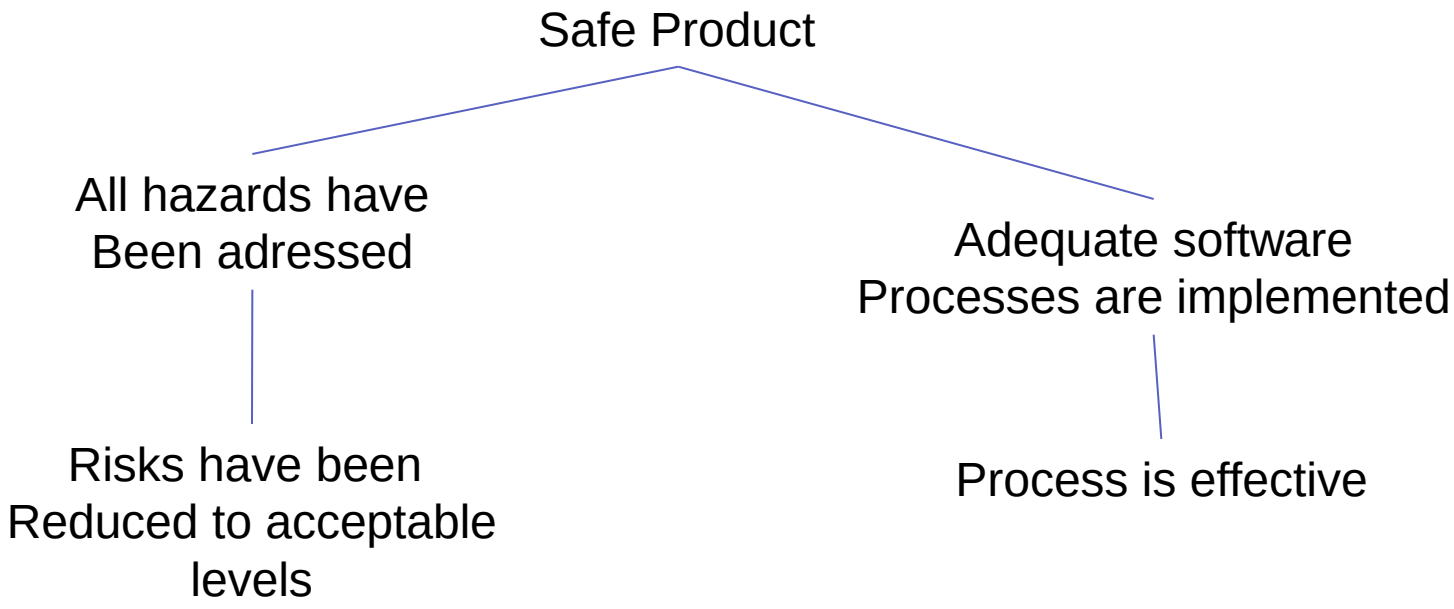
Management of Product Risks

Risk Areas

- IT Security Risks
- Product Safety Risks

Product Safety Risks

- What are possible hazards?
  - Major: May lead to death or serious injury
  - Moderate: Non-serious injury is possible
  - Minor: No injury or damage to health is possible
- Software Risk Management Approach



Hazard identification

- Software and Product IT-Security hazards cover Confidentiality, Integrity and Availability aspects, e.g.
  - A medical Instrument can be run with expired maintenance or reagents.
  - Data storage exhausted e.g. harddisk is filled with logfiles
  - Wrong or unclear patient result presentation
  - Timing-, multitasking-, jittering-problems or deadlocks occur
  - Access to patient/personal data for unauthorized people
  - Instruments or databases are accessed by unauthorized persons via the intra- or internet
  - Service passwords are static and become widely known
  - Audit trails and logfiles can be edited

Product Risk Management

- Same process as for Business or Project Risk Management
- Product Manufacturer is held responsible for
  - Whole product
  - All integrated parts

	Formal Product Risk Management Process
Inhouse developed software	X
Outsourced development for the purpose of the product	X
Software already available (OTSS, legacy code)	Not possible, OTSS already exists

Software Risk Management According to IEC 62304

IEC 62304 Medical Device Software

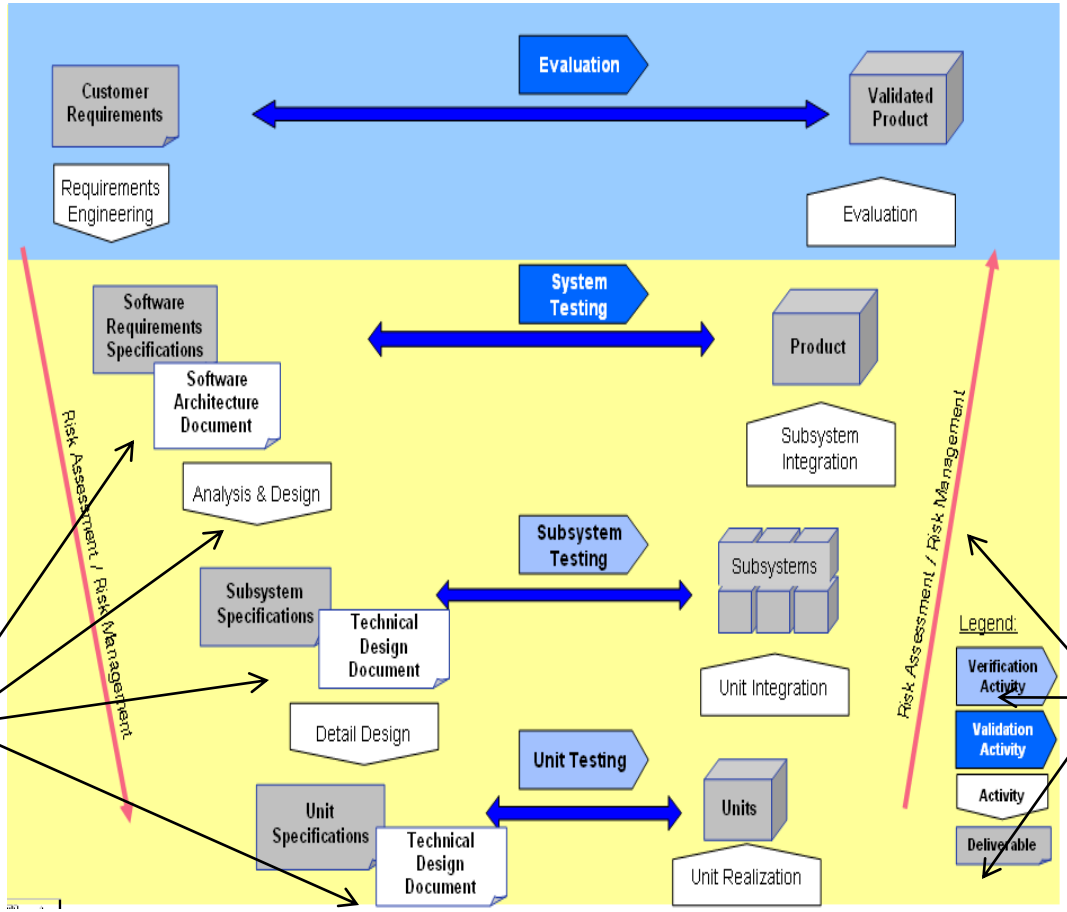
Risk Assessment

Critical Harm

Sequence of critical software events / Causes for harm

Critical Software Items in Architecture

Risk Control Measures
-New Requirement (SRQ)
-Improved Design
-SW Item Specification



Risk Control Verification

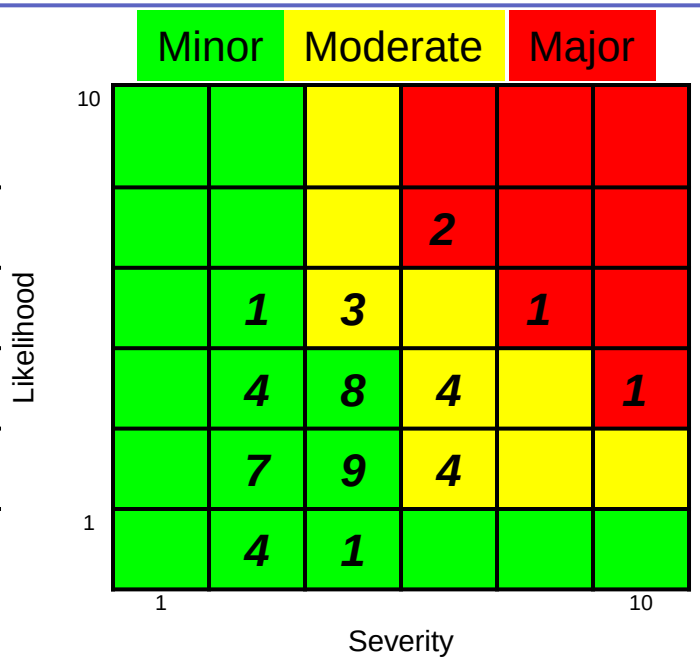
Declaration of residual risks

Test Plans, Unit, Integration, System Testing

Verification of risk control measurements (effective, Residual risks)

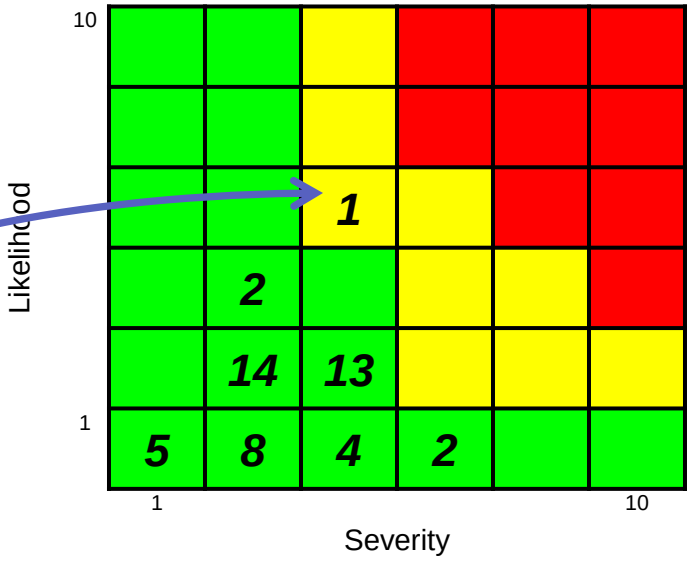
Risk Mitigation Documentation

Project stage	Product … **Before measures**
Date	24-Jan-09
Risks assessed	49
Green area:	34
Yellow area:	11
Red area:	4



Product Risk Reduction to Acceptable Level

Project stage	Product … **After measures**
Date	30-Nov-09
Risks assessed	49
Green area:	48
Yellow area:	1
Red area:	0



Documentation Of Residual Risks

Off-the-Shelf Software (OTSS)

- Analysis and Documentation during Design:
  - Make vs. Buy Analysis
  - Software Package Selection and Purchasing Control

- Steps
  - Analyze Level of Concern:
    Worst case hazard severity if software malfunctions:
    - Minor: document hazard mitigation actions
    - Moderate: Describe and justify residual risks (Basic documentation)
    - Major: Special documentation demonstrates risk reduction

OTSS Risk Documentation

- Basic Documentation
  - Why the OTSS is appropriate for use in the product
  - Used versions, patches, drivers, …
  - OTSS requirements for the product
  - Testing appropriate for hazards
  - Configuration Management for OTSS deliverables
- Special Documentation (major hazards)
  - Provide assurance regarding the OTSS development process by the vendor
  - Demonstrate that vendor‘s Verification & Validation are adequate
  - Demonstrate maintenance and support of the OTSS will be adequate