SE463
Software Requirements Specification & Analysis

Risk Management

Risk

A risk is an uncertain factor whose occurrence may result in some loss of satisfaction of some corresponding objective.

[van Lamsveerde, p. 3.6]

- has a likelihood to occur
- has consequences
- product-related risks
- process-related risks

Project Risk Manager

No Risk, No Reward

Trying to completely eliminate risk from your software project is unrealistic and can be prohibitively expensive.

"Gain is commensurate with risk."

M.K. Soni

"He who doesn't risk never gets to drink champagne."

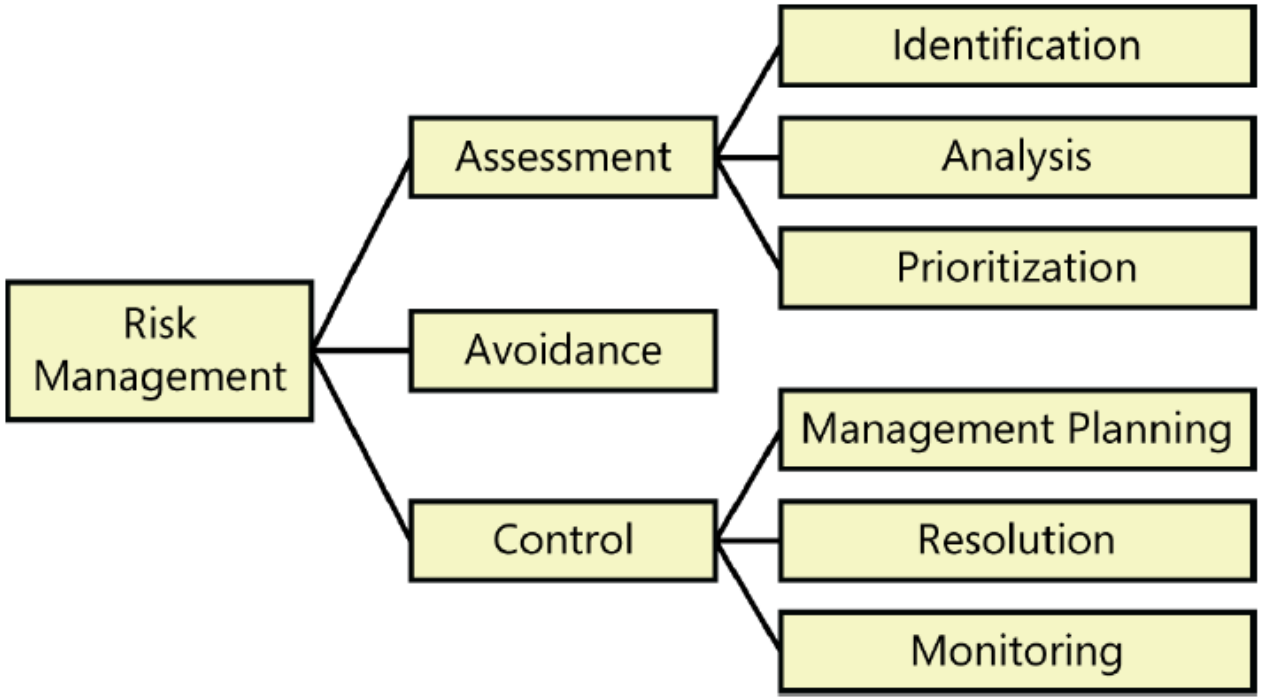
Russian Proverb

"Don't be afraid to take a big step when one is indicated. You can't cross a chasm in two small steps."

David Lloyd George

Risk Management

Risk Management attempts to manage the degree to which a project is exposed to risks of quality, delay, or failure.



K. Wiegers and J. Beatty, Software Requirements 3ed, Microsoft Press, 2013.

Risk Management

"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."

Theodore Roosevelt

Defect Detection and Prevention (DDP)

DDP is a process developed by NASA for systematic risk assessment and mitigation.

DDP Process:

1. Identify most critical requirements
2. Identify potential risks
3. Estimate the impact of each risk on each requirement
4. Identify possible countermeasures
5. Identify the most effective countermeasures

Result of DDP: Optimized collection of mitigating actions that may be applied to project

Risk Consequence Table

DDP Process:

1. Identify most critical requirements, and their relative importance
2. Identify potential risks, and their likelihood
3. Estimate the impact of each risk on each requirement
4. Identify possible countermeasures
5. Identify the most effective countermeasures

Goal:

- To develop a prioritized set of risks to be addressed
- Perhaps to identify which requirements are the most “risk driving”

Risk Consequence Table

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Likelihood (risk)		**0.5**	**0.8**	**0.7**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.7**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**1.96**
Risk Criticality		**0.715**	**0.968**	**1.071**	**0.13**	

Impact(risk, req) = estimate of loss of requirement

0 = no loss

1 = total loss

Loss of Objectives

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Likelihood (risk)		**0.5**	**0.8**	**0.7**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.7**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**1.96**
Risk Criticality		**0.715**	**0.968**	**1.071**	**0.13**	

$$\text{Loss(req)} = \text{Weight(req)} \times \sum_{\text{risk}} \left(\text{Impact(req,risk)} * \text{Likelihood(risk)}\right)$$

Risk-Driving Requirements

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Likelihood (risk)		**0.5**	**0.8**	**0.7**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.7**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**1.96**
Risk Criticality		**0.715**	**0.968**	**1.071**	**0.13**	

Risk-driving requirement

Risk-driving requirements are the requirements that are most at risk of being achieved.

Risk Criticalities

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Likelihood (risk)		**0.5**	**0.8**	**0.7**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.7**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**1.96**
Risk Criticality		**0.715**	**0.968**	**1.071**	**0.13**	

$$\text{Criticality(risk)} = \text{Likelihood(risk)} \times \sum_{\text{req}} \left(\text{Impact(req,risk)} * \text{Weight(req)}\right)$$

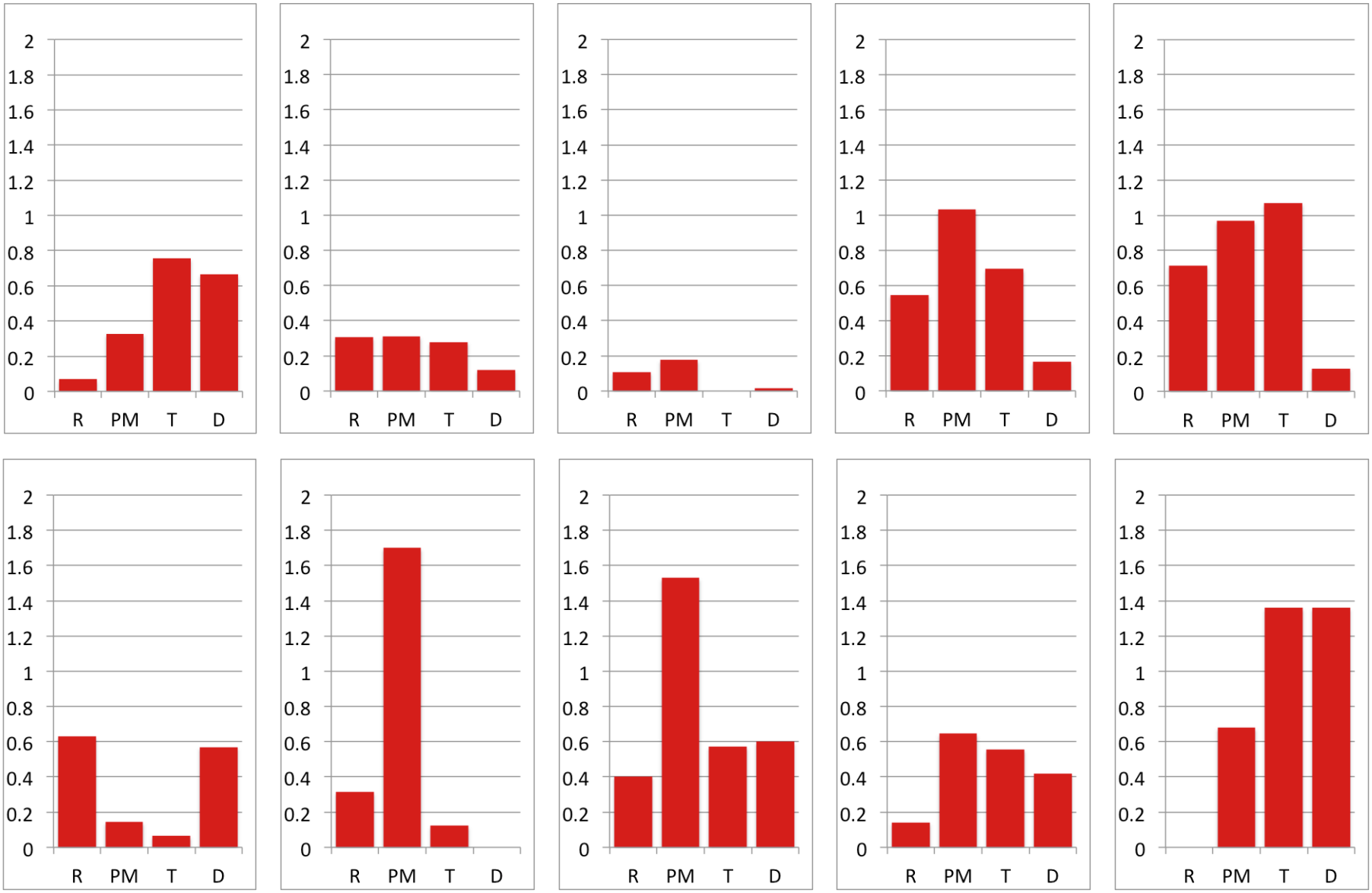
Tall Poles

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Likelihood (risk)		**0.5**	**0.8**	**0.7**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.7**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**1.96**
Risk Criticality		**0.715**	**0.968**	**1.071**	**0.13**	

Tall Poles

Tall Poles are the most critical risks, having the most severe consequences

Teams' Assessments of Risks



Risk Management

"One thing that makes is possible to be an optimist is if you have a contingency plan for when all hell breaks loose."

Randy Pausch

Risk Countermeasures Table

DDP Process:

1. Identify most critical requirements
2. Identify potential risks, and their likelihood
3. Estimate the impact of each risk on each requirement
4. Identify possible countermeasures, and their effectiveness in reducing risk
5. Identify the most effective countermeasures

Goal:

- Identify options for preventing or detecting failure modes
  - Preventative measures, Analyses, Process controls, Tests, Mitigations
- Perhaps to identify the most effective countermeasures

Risk Countermeasures Table

	Risks (Failure Modes)				
Countermeasures	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Overall single effect of countermeasure**
Criticality (risk)	**0.715**	**0.968**	**1.071**	**0.13**	
Collaborative elicitation process with extensive user involvement; modelling; mock-ups	0.5	0.3	0	0.1	**0.6479**
Continually estimate costs; use shorter development iterations	0.25	0.7	0.2	0	**1.09655**
Prototype novel or risky requirements; plan time for learning and experimentation	0.25	0.25	0.5	0	**1.02125**
Investigate suppliers; monitor their progress; develop backup plans	0	0	0.1	0.5	**0.1201**
Combined Risk Reduction	**0.71875**	**0.8425**	**0.64**	**0.55**	

Effect(cm, risk) = estimate of reduction of risk

0 = no reduction

1 = risk eliminated

Overall Effect of Countermeasures

	Risks (Failure Modes)				
Countermeasures	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Overall single effect of countermeasure**
Criticality (risk)	**0.715**	**0.968**	**1.071**	**0.13**	
Collaborative elicitation process with extensive user involvement; modelling; mock-ups	0.5	0.3	0	0.1	**0.6479**
Continually estimate costs; use shorter development iterations	0.25	0.7	0.2	0	**1.09655**
Prototype novel or risky requirements; plan time for learning and experimentation	0.25	0.25	0.5	0	**1.02125**
Investigate suppliers; monitor their progress; develop backup plans	0	0	0.1	0.5	**0.1201**
Combined Risk Reduction	**0.71875**	**0.8425**	**0.64**	**0.55**	

$$\text{OverallEffect}(cm) = \sum_{risk} \left(\text{Reduction}(cm, risk) * \text{Criticality}(risk)\right)$$

Combined Risk Reduction

	Risks (Failure Modes)				
Countermeasures	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Overall single effect of countermeasure**
Criticality (risk)	**0.715**	**0.968**	**1.071**	**0.13**	
Collaborative elicitation process with extensive user involvement; modelling; mock-ups	0.5	0.3	0	0.1	**0.6479**
Continually estimate costs; use shorter development iterations	0.25	0.7	0.2	0	**1.09655**
Prototype novel or risky requirements; plan time for learning and experimentation	0.25	0.25	0.5	0	**1.02125**
Investigate suppliers; monitor their progress; develop backup plans	0	0	0.1	0.5	**0.1201**
Combined Risk Reduction	**0.71875**	**0.8425**	**0.64**	**0.55**	

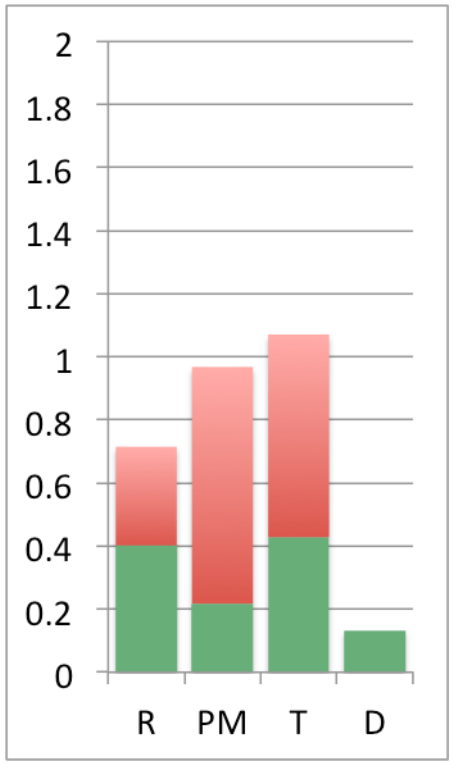
$$\text{CombinedReduction}(risk) = 1 - \prod_{cm} \left(1 - \text{Reduction}(cm, risk)\right)$$

Apply Optimal Countermeasures

		Risks (Failure Modes)				
Requirements	**Weight (req)**	**Requirements** (incomplete, incorrect, ambiguous, changing)	**Project Management** (estimations, project, team management)	**Technical** (complex problem, lack of experience with technology)	**Dependencies** (on adjacent systems, components, other people)	**Loss of Objective**
Mitigated Likelihood (risk)		**0.28125**	**0.18**	**0.28**	**0.2**	
Creating a product that users would like	**0.7**	0.9	0.3	0.9	0.5	**0.3437875**
Completing the product on time	**1.0**	0.8	1	0.9	0.3	**0.745**
Mitigated Risk Criticality		**0.4021875**	**0.2178**	**0.4284**	**0.13**	

$$\text{MitigatedLikelihood(risk)} = \text{Likelihood(risk)} * \prod (1 - \text{Reduction(cm,risk)})$$

Apply Optimal Countermeasures



Red bars show the risk levels before mitigation.

Green bars show the risk levels after mitigation.

Example: Meeting Scheduler

- 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 scheduling constraints
- Constraints are expressed as two sets:
  - one **exclusion set (dates when a participant cannot attend)**
  - one **preference set (dates when a participant prefers to attend)**
- Initiator also asks for specific requirements of meeting room
- All correspondence with participants is via email
- The meeting should be scheduled within the stated date range and not be in any exclusion sets. The date should also belong to as many preference sets as possible, especially of the “important” participants.
- A new schedule 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.

Risk Consequence Table

		Risks (Failure Modes)					
Requirements	**Weight (req)**	Participant does not read emails	Participant does not reply to requests	Room with required equipment is not available	System response is too close to meeting	Important participant has last minute change	**Loss of objective**
Likelihood (risk)		**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	**0.256**
Participant average attendance increased	**0.3**	0.8	0.8	0	0.8	0.5	**0.315**
Schedule conflicts reduced	**0.6**	0.2	1	0	0	0.7	**0.438**
Risk criticality		**0.264**	**0.468**	**0.01**	**0.297**	**0.375**	

Impact(risk, req) = estimate of loss of requirement

0 = no loss

1 = total loss

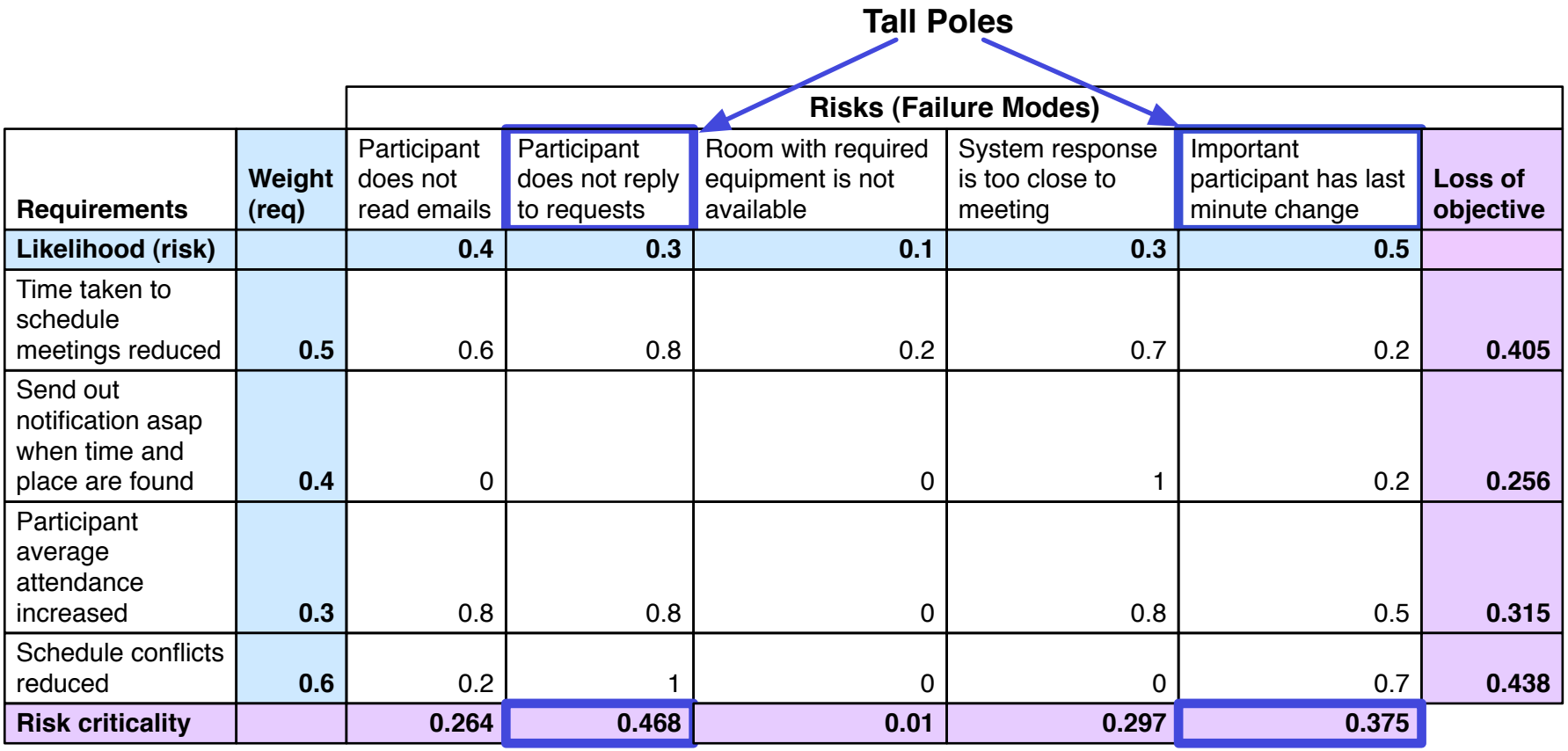
Risk-Driving Requirements

			Risks (Failure Modes)				
Requirements	**Weight (req)**	Participant does not read emails	Participant does not reply to requests	Room with required equipment is not available	System response is too close to meeting	Important participant has last minute change	**Loss of objective**
Likelihood (risk)		**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	1	0.2	**0.256**
Participant average attendance increased	**0.3**	0.8	0.8	0	0.8	0.5	**0.315**
Schedule conflicts reduced	**0.6**	0.2	1	0	0	0.7	**0.438**
Risk criticality		**0.264**	**0.468**	**0.01**	**0.297**	**0.375**	

Risk driving

Risk-driving requirements are the requirements that are most at risk of not being achieved

Tall Poles



Requirements	Weight (req)	Participant does not read emails	Participant does not reply to requests	Room with required equipment is not available	System response is too close to meeting	Important participant has last minute change	Loss of objective
Likelihood (risk)		**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	1	0.2	**0.256**
Participant average attendance increased	**0.3**	0.8	0.8	0	0.8	0.5	**0.315**
Schedule conflicts reduced	**0.6**	0.2	1	0	0	0.7	**0.438**
Risk criticality		**0.264**	**0.468**	**0.01**	**0.297**	**0.375**	

Tall Poles are the most critical risks, having the most severe consequences

Risk Countermeasures Table

	Risks (Failure Modes)					
Countermeasures	Participant does not read emails	Participant does not reply to requests	Room with required equipment is not available	System response is too close to meeting	Important participant has last minute change	**Overall single effect of countermeasure**
Criticality (risk)	**0.264**	**0.468**	**0.01**	**0.297**	**0.375**	
Email reminder sent	0.7	0.7	0	0.1	0	**0.542**
Change the meeting, increase time range	0.2	0.2	0	0.1	0	**0.176**
System has access to personal e-agendas	0.3	0.2	0.1	0.2	0.3	**0.346**
Change the meeting, fewer constraints (equipment)	0	0	0.9	0	0	**.009**
Cancel a meeting and send email confirmation	0.8	0.8	1	0.7	0.9	**1.141**
Combined risk reduction	**0.966**	**0.962**	**1**	**0.806**	**0.93**	

Effect(cm, risk) = estimate of reduction of risk

0 = no reduction

1 = risk eliminated

Combined Risk Reduction

	Risks (Failure Modes)					
Countermeasures	Participant does not read emails	Participant does not reply to requests	Room with required equipment is not available	System response is too close to meeting	Important participant has last minute change	**Overall single effect of countermeasure**
Criticality (risk)	**0.264**	**0.468**	**0.01**	**0.297**	**0.375**	
Email reminder sent	0.7	0.7	0	0.1	0	**0.542**
Change the meeting, increase time range	0.2	0.2	0	0.1	0	**0.176**
System has access to personal e-agendas	0.3	0.2	0.1	0.2	0.3	**0.346**
Change the meeting, fewer constraints (equipment)	0	0	0.9	0	0	**.009**
Cancel a meeting and send email confirmation	0.8	0.8	1	0.7	0.9	**1.141**
Combined risk reduction	**0.966**	**0.962**	**1**	**0.806**	**0.93**	

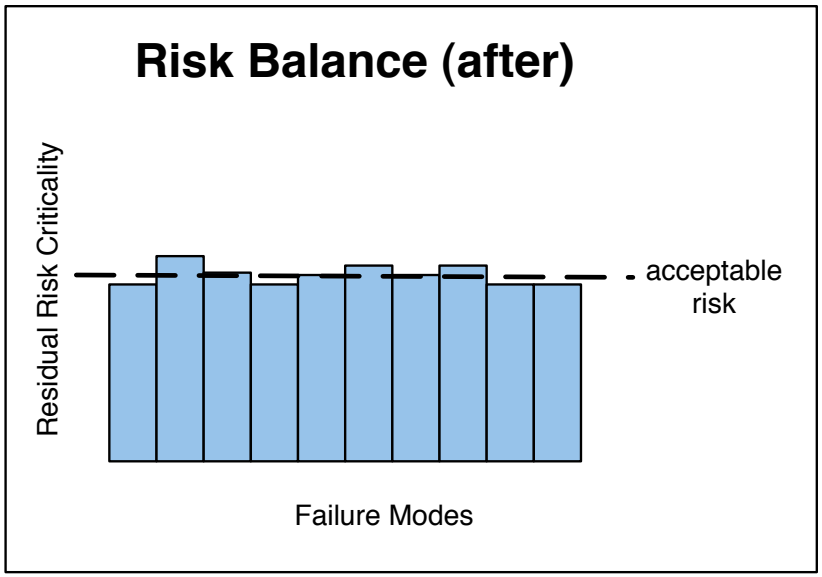
$$\text{CombinedReduction(risk)} = 1 - \prod_{cm} (1 - \text{Reduction(cm, risk)})$$

Optimizing the Residual Risk

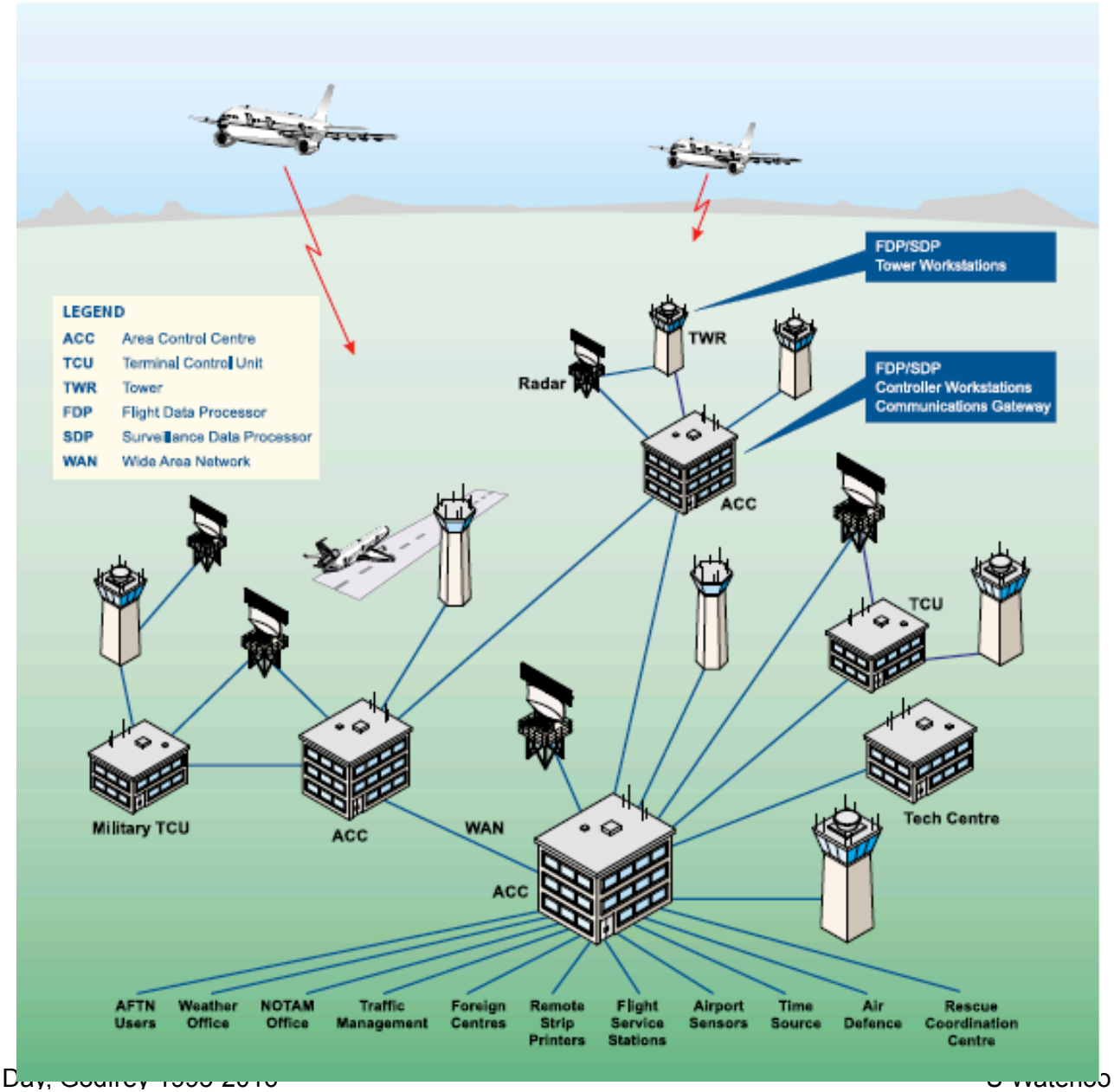
Goal: Select the optimal combinations of countermeasures

- based on their joint effectiveness in reducing risk
- based on their associated cost of implementation

Result: Optimal (or near optimal) balance of risk exposure



Canadian Automated Air Traffic Control System



Case Study: CAATS

- Goals of project were to provide
  - Paperless, integrated flight data to controllers
  - Automatic conflict detection and prediction
  - Automatic proposals for conflict resolution
- Project completed
  - 64 months later than originally planned
  - With a cost >$123 million more than originally planned
  - With reduced functionality
    - excluded hardware and some commercial software
    - no automatic proposal of conflict resolution
    - to be installed at 23 control towers instead of 60
    - no automatic management of military altitude reservation
    - reduced traffic flow management features
    - transition to CAATS to be gradual rather than synchronized

CAATS Timeline

Nov. 1989	Treasury Board approves CAATS. Primary contractor awarded fixed-price contract with ceiling of $465.6 million.
1990	Transport Canada rejects first major milestone (contractor's description of proposed new system)
Dec. 1994	Agreement on requirements still not reached. Progress payments stopped ($230 million already paid out)
Sept. 1995	Treasury Board approves substantially amended project and contract
Sept. 1996	CAATS project office and contractor renegotiated contract again, to bring status of project into good standing
Dec. 2000	CAATS delivered to NAV Canada

Auditor General Office, *Systems Under Development: Getting Results*, 1996.
http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_24_e_5055.html

Requirements Problems

- Hughes had no local workforce in Vancouver (moved people from their LA base)
- Hughes had little experience with air traffic control
- Expertise of traffic controllers who worked on site became dated
- Scope of project from 1990 - 1995 grew 82%, with over 5300 requirements change requests

Ineffective Risk Management

A report by the Auditor General of Canada found that project risks were not being managed effectively:

- Government project leaders were part-time, inexperienced
  - lacked knowledge of project management
  - lacked knowledge of system/software development processes
  - failed to track status of project
- Project leaders did not take a central role in decision-making.
  - contractor would propose system specifications
  - Transport Canada would reject then due to nonconformance to its understanding of the requirements

Auditor General Office, *Systems Under Development: Getting Results*, 1996.
http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_24_e_5055.html

Ineffective Risk Management

A report by the Auditor General of Canada found that project risks were not being managed effectively (cont.):

- Government entered into long-term, fixed-price contracts before a clear understanding of what will be built was reached by all parties.
- Because contracts were fixed-price, only the contractor's performance with respect to the planned schedule was tracked.
  - Project costs increased dramatically even though contract costs remained fixed
  - Led to compromises in final schedule and final functionality

Auditor General Office, *Systems Under Development: Getting Results*, 1996.
http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_24_e_5055.html

Summary

Risk Management

- Risk - What could go wrong?
- Risk Analysis
- Risk Mitigation
- CAATS Case Study