Lecture 5, Part 1: Eliciting Requirements

- Basics of elicitation
  - Why info collection is hard
  - Dealing with Bias
- A large collection of elicitation techniques:
  - Background Reading
  - Hard data collection
  - Interviews
  - Questionnaires
  - Group Techniques
  - Participant Observation
  - Ethnomethodology
  - Knowledge Elicitation Techniques

Difficulties of Elicitation

- **Thin spread of domain knowledge**
  - The knowledge might be distributed across many sources
    - It is rarely available in an explicit form (I.e. not written down)
  - There will be conflicts between knowledge from different sources
    - Remember the principle of complementarity!
- **Tacit knowledge (The "say-do" problem)**
  - People find it hard to describe knowledge they regularly use
- **Limited Observability**
  - The problem owners might be too busy coping with the current system
  - Presence of an observer may change the problem
    - E.g. Probe Effect; Hawthorne Effect
- **Bias**
  - People may not be free to tell you what you need to know
  - People may not want to tell you what you need to know
    - The outcome will affect them, so they may try to influence you (hidden agendas)

Example

- **Loan approval department in a large bank**
  - The analyst is trying to elicit the rules and procedures for approving a loan
- **Why this might be difficult:**
  - Implicit knowledge:
    - There is no document in which the rules for approving loans are written down
  - Conflicting information:
    - Different bank staff have different ideas about what the rules are
  - Say-do problem:
    - The loan approval process described to you by the loan approval officers is quite different from your observations of what they actually do
  - Probe effect:
    - The loan approval process used by the officers while you are observing is different from the one they normally use
  - Bias:
    - The loan approval officers fear that your job is to computerize their jobs out of existence, so they are deliberately emphasizing the need for case-by-case discretion (to convince you it has to be done by a human!)

Bias

- What is bias?
  - Bias only exists in relation to some reference point
    - can there ever be "no bias"?
  - All views of reality are filtered
  - All decision making is based partly on personal values.
- Types of bias:
  - Motivational bias
    - expert makes accommodations to please the interviewer or some other audience
  - Observational bias
    - Limitations on our ability to accurately observe the world
  - Cognitive bias
    - Mistakes in use of statistics, estimation, memory, etc.
  - Notational bias
    - Terms used to describe a problem may affect our understanding of it

Examples of Bias

- Social pressure
  response to verbal and non-verbal cues from interviewer
- Group think
  response to reactions of other experts
- Impression management
  response to imagined reactions of managers, clients,...
- Wishful thinking
  response to hopes or possible gains.
- Appropriation
  Selective interpretation to support current beliefs.
- Misrepresentation
  expert cannot accurately fit a response into the requested response mode
- Anchoring
  contradictory data ignored once initial solution is available
- Inconsistency
  assumptions made earlier are forgotten
- Availability
  some data are easier to recall than others
- Underestimation of uncertainty
  tendency to underestimate by a factor of 2 or 3.

Elicitation Techniques

- Traditional techniques
  - Introspection
  - Reading existing documents
  - Analyzing hard data
  - Interviews
    - Open-ended
    - Structured
  - Surveys / Questionnaires
  - Meetings
- Collaborative techniques
  - Focus Groups
    - Brainstorming
    - JAD/RAD workshops
  - Prototyping
  - Participatory Design
- Contextual (social) approaches
  - Ethnographic techniques
    - Participant Observation
    - Enthnomethodology
  - Discourse Analysis
    - Conversation Analysis
    - Speech Act Analysis
  - Sociotechnical Methods
    - Soft Systems Analysis
- Cognitive techniques
  - Task analysis
  - Protocol analysis
  - Knowledge Acquisition Techniques
    - Card Sorting
    - Laddering
    - Repertory Grids
    - Proximity Scaling Techniques

Background Reading

- **Sources of information:**
  - company reports, organization charts, policy manuals, job descriptions, reports, documentation of existing systems, etc.
- **Advantages:**
  - Helps the analyst to get an understanding of the organization before meeting the people who work there.
  - Helps to prepare for other types of fact finding
    - e.g. by being aware of the business objectives of the organization.
  - may provide detailed requirements for the current system.
- **Disadvantages:**
  - written documents often do not match up to reality.
  - Can be long-winded with much irrelevant detail
- **Appropriate for**
  - Whenever you not familiar with the organization being investigated.

"Hard Data" and Sampling

- **Hard data includes facts and figures…**
  - Forms, Invoices, financial information,…
  - Reports used for decision making,…
  - Survey results, marketing data,…
- **Sampling**
  - Sampling used to select representative set from a population
    - Purposive Sampling - choose the parts you think are relevant without worrying about statistical issues
    - Simple Random Sampling - choose every kth element
    - Stratified Random Sampling - identify strata and sample each
    - Clustered Random Sampling - choose a representative subpopulation and sample it
  - Sample Size is important
    - balance between cost of data collection/analysis and required significance
  - Process:
    - Decide what data should be collected - e.g. banking transactions
    - Determine the population - e.g. all transactions at 5 branches over one week
    - Choose type of sample - e.g. simple random sampling
    - Choose sample size - e.g. every 20th transaction

Example of hard data

- Questions:
  - What does this data tell you?
  - What would you do with this data?

Agate

Campaign Summary

Date 23rd February 1999

Client Yellow Partridge
Park Road Workshops
Park Road
Jewellery Quarter
Birmingham B2 3DT
U.K.

Campaign Spring Collection 1999

Billing Currency GB £

Item	Curr	Amount	Rate	Billing amount
Advert preparation: photography, artwork, layout etc.	GB £	15,000.00	1	15,000.00
Placement French Vogue	FFr.	47 000,00	11.35	4,140.97
Placement UK Vogue	GB £	5,000.00	1	5,000.00
Placement US Vogue	US $	15,000.00	2.47	6.072.87
Total				30,213.84

This is not a VAT Invoice. A detailed VAT Invoice will be provided separately.

210-212 Carstairs Street, Birmingham B1 5TG
Tel.0121-111-1234 Fax.0121-111-1245
Email.agate@agateltd.co.uk

Interviews

- Types:
  - Structured - agenda of fairly open questions
  - Open-ended - no pre-set agenda
- Advantages
  - Rich collection of information
  - Good for uncovering opinions, feelings, goals, as well as hard facts
  - Can probe in depth, & adapt followup questions to what the person tells you
- Disadvantages
  - Large amount of qualitative data can be hard to analyze
  - Hard to compare different respondents
  - Interviewing is a difficult skill to master
- Watch for
  - Unanswerable questions ("how do you tie your shoelaces?")
  - Tacit knowledge (and post-hoc rationalization)
  - Removal from context
  - Interviewer's attitude may cause bias (e.g. variable attentiveness)

Source: *Adapted from Goguen and Linde, 1993, p154.*

Interviewing Tips

- **Starting off…**
  - Begin the interview with an innocuous topic to set people at ease
    - e.g. the weather, the score in last night's hockey game
    - e.g. comment on an object on the person's desk: "My,… what a beautiful photograph! Did you take that?"
- **Ask if you can record the interview**
  - Make sure the tape recorder is visible
  - Say that they can turn it off at any time.
- **Ask easy questions first**
  - perhaps personal information
    - e.g. "How long have you worked in your present position?"
- **Follow up interesting leads**
  - E.g. if you hear something that indicates your plan of action may be wrong,
    - e.g.,"Could we pursue what you just said a little further?"
- **Ask open-ended questions towards the end**
    - e.g. "Is there anything else you would like to add?"

Questionnaires

- **Advantages**
  - Can quickly collect info from large numbers of people
  - Can be administered remotely
  - Can collect attitudes, beliefs, characteristics
- **Disadvantages**
  - Simplistic (presupposed) categories provide very little context
    - No room for users to convey their real needs
- **Watch for:**
  - Bias in sample selection
  - Bias in self-selecting respondents
  - Small sample size (lack of statistical significance)
  - Open ended questions (very hard to analyze!)
  - Leading questions (*"have you stopped beating your wife?"*)
  - Appropriation (*"What is this a picture of?"*)
  - Ambiguous questions (I.e. not everyone is answering the same question)

Note: Questionnaires MUST be prototyped and tested!

Source: *Adapted from Goguen and Linde, 1993, p154.*

Meetings

- Used for summarization and feedback
  - E.g. meet with stakeholders towards the end of each stage:
    - to discuss the results of the information gathering stage
    - to conclude on a set of requirements
    - to agree on a design etc.
  - Use the meeting to confirm what has been learned, talk about findings
- Meetings are an important managerial tool
  - Used to move a project forward.
  - Every meeting should have a clear objective:
    - E.g. presentation, problem solving, conflict resolution, progress analysis, gathering and merging of facts, training, planning,...
  - Plan the meeting carefully:
    - Schedule the meeting and arrange for facilities
    - Prepare an agenda and distribute it well in advance
    - Keep track of time and agenda during the meeting
    - Follow up with a written summary to be distributed to meeting participants
    - Special rules apply for formal presentations, walkthroughs, brainstorming, etc.

Group Elicitation Techniques

- Types:
  - Focus Groups
  - Brainstorming
- Advantages
  - More natural interaction between people than formal interview
  - Can gauge reaction to stimulus materials (e.g. mock-ups, storyboards, etc)
- Disadvantages
  - May create unnatural groups (uncomfortable for participants)
  - Danger of Groupthink
  - May only provide superficial responses to technical questions
  - Requires a highly trained facilitator
- Watch for
  - sample bias
  - dominance and submission

Joint/Rapid Application Development

- **JAD & RAD Principles:**
  - Group Dynamics - use workshops instead of interviews
  - Visual Aids
    - Lots of visualization media, e.g. wall charts, large monitors, graphical interfaces
  - Organized, Rational Process
    - Techniques such as brainstorming and top-down analysis
  - WYSIWYG Documentation Approach
    - each JAD session results in a document which is easy to understand and is created and agreed upon during the session
- **Notes:**
  - Choose workshop participants carefully
    - they should be the best people possible representing various stakeholder groups
  - Workshop should last 3-5 days.
    - Must turn a group of participants into a team - this takes 1-2 days.
    - Session leader makes sure each step has been completed thoroughly.
    - Session leader steps in when there are differences of opinion - "open issues".
    - Meeting room should be well-equipped for presentations, recording etc.

Participant Observation

- **Approach**
  - Observer spends time with the subjects
    - Joining in long enough to become a member of the group
    - Hence appropriate for longitudinal studies
- **Advantages**
  - Contextualized;
  - Reveals details that other methods cannot
- **Disadvantages**
  - Extremely time consuming!
  - Resulting 'rich picture' is hard to analyze
  - Cannot say much about the results of proposed changes
- **Watch for**
  - going native!

Ethnomethodology

- **Basis**
  - Social world is ordered
    - The social order may not be obvious, nor describable from common sense
  - The social order cannot be assumed to have an a priori structure
    - Social order is established on a moment-to-moment basis through participants' collective actions (no pre-existing structures)
    - i.e. social order only observable when an observer immerses herself in it.
  - Observation should be done in a natural setting
  - Need to consider how meanings develop and evolve within context
- **"Use the members' own Categories"**
  - Most conventional approaches assume preexisting categories
    - This may mislead the observer (e.g. appropriation)
  - Ethnography attempts to use the subjects' own categories
    - What categories (concepts) do they use themselves to order the social world?
  - What methods do people use to make sense of the world around them?
    - Use the same methods members use during observation
    - E.g by developing a legitimate role within the community under observation.

Source: *Adapted from Goguen and Linde, 1993, p158.*

Ethnomethodological approach

- **Ethnomethodology is a subarea of Anthropology**
  - Looks for behaviours that are culture-specific
    - E.g. Frenchmen brag about sexual conquests to gain status;
    - E.g. Americans brag about money to gain status.
    - Each of these topics is taboo in the other culture
- **Uses a very tightly controlled set of methods:**
    - Conversational analysis
    - Measurement of body system functions - e.g. heartbeat
    - Non-verbal behaviour studies
    - Detailed video analysis
  - These techniques are useful in capturing information about a social setting.
- **Other observation techniques can be applied:**
  - Time-motion study
    - who is where, when?
  - Communication audit
    - who talks to whom about what?
  - Use of tools - status symbols plus sharing rules

Knowledge Elicitation Techniques

Protocol Analysis

- based on vocalising behaviour
  - Think aloud vs. retrospective protocols
- Advantages
  - Direct verbalisation of cognitive activities
  - Embedded in the work context
  - Good at revealing interaction problems with existing systems
- Disadvantages
  - Essentially based on introspection, hence unreliable
  - No social dimension

Proximity Scaling Techniques

- Given some domain objects, derive a set of dimensions for classifying them:
  - step 1: pairwise proximity assessment among domain elements
  - step 2: automated analysis to build multi-dimensional space to classify the objects
- Advantages
  - help to elicit mental models, where complex multivariate data is concerned
  - good for eliciting tacit knowledge
- Disadvantages
  - Requires an agreed on set of objects
  - Only models classification knowledge (no performance knowledge)

Source: *Adapted from Hudlicka, 1996.*

more KE techniques

Card Sorting

- For a given set of domain objects, written on cards:
  - Expert sorts the cards into groups...
  - ...then says what the criterion was for sorting, and what the groups were.
- Advantages
  - simple, amenable to automation
  - elicits classification knowledge
- Problems
  - suitable entities need to be identified with suitable semantic spread across domain.
  - No performance knowledge

Laddering

- Uses a set of probes to acquire stakeholders' knowledge.
  - Interview the expert.
  - Use questions to move up and down a conceptual hierarchy
  - E.g. developing goal hierarchies
- Advantages
  - deals with hierarchical knowledge, including poly-hierarchies (e.g., goal trees, "is-a" taxonomies).
  - knowledge is represented in standardised format
  - can elicit structural knowledge
  - suitable for automation.
- Disadvantages
  - assumes hierarchically arranged knowledge.

Lecture 5, Part 2: Risk

- General ideas about Risk
- Risk Management
  - Identifying Risks
  - Assessing Risks
- Case Study:
  - Mars Polar Lander

Risk Management

- About Risk
  - Risk is "the possibility of suffering loss"
  - Risk itself is not bad, it is essential to progress
  - The challenge is to manage the amount of risk
- Two Parts:
  - Risk Assessment
  - Risk Control
- Useful concepts:
  - For each risk: Risk Exposure
    - RE = p(unsat. outcome) X loss(unsat. outcome)
  - For each mitigation action: Risk Reduction Leverage
    - RRL = (RE_{before} - RE_{after}) / cost of intervention

Principles of Risk Management

- **Global Perspective**
  - View software in context of a larger system
  - For any opportunity, identify both:
    - Potential value
    - Potential impact of adverse results
- **Forward Looking View**
  - Anticipate possible outcomes
  - Identify uncertainty
  - Manage resources accordingly
- **Open Communications**
  - Free-flowing information at all project levels
  - Value the individual voice
    - Unique knowledge and insights
- **Integrated Management**
  - Project management is risk management!
- **Continuous Process**
  - Continually identify and manage risks
  - Maintain constant vigilance
- **Shared Product Vision**
  - Everybody understands the mission
    - Common purpose
    - Collective responsibility
    - Shared ownership
  - Focus on results
- **Teamwork**
  - Work cooperatively to achieve the common goal
  - Pool talent, skills and knowledge

Source: Adapted from SEI Continuous Risk Management Guidebook

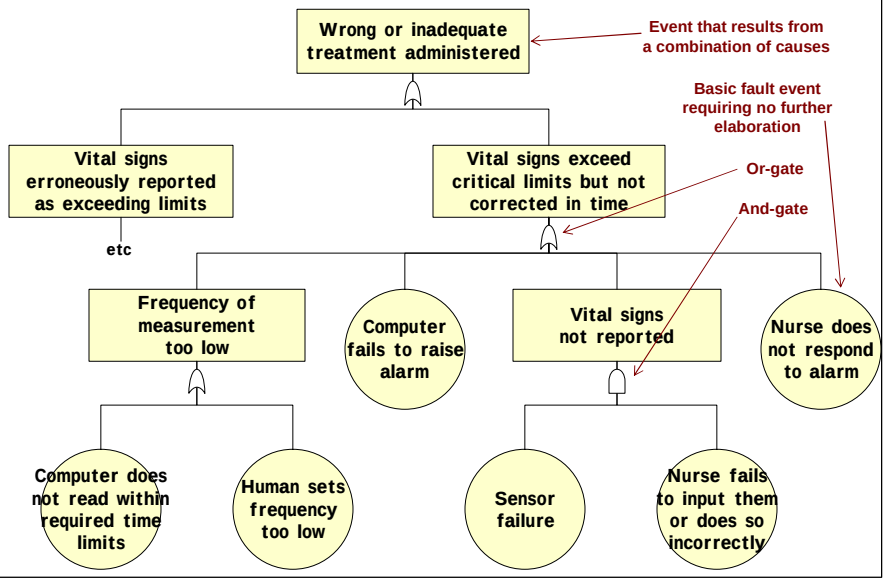
Continuous Risk Management

- **Identify:**
  - Search for and locate risks before they become problems
    - Systematic techniques to discover risks
- **Analyse:**
  - Transform risk data into decision-making information
  - For each risk, evaluate:
    - Impact
    - Probability
    - Timeframe
  - Classify and Prioritise Risks
- **Plan**
  - Choose risk mitigation actions
- **Track**
  - Monitor risk indicators
  - Reassess risks
- **Control**
  - Correct for deviations from the risk mitigation plans
- **Communicate**
  - Share information on current and emerging risks

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Source: Adapted from SEI Continuous Risk Management Guidebook

Fault Tree Analysis



Source: *Adapted from Leveson, "Safeware", p321*

Risk Assessment

- **Quantitative:**
  - Measure risk exposure using standard cost & probability measures
  - Note: probabilities are rarely independent
- **Qualitative:**
  - Develop a risk classification matrix:

		Likelihood of Occurrence		
		Very likely	**Possible**	**Unlikely**
Undesirable outcome	**(5) Loss of Life**	Catastrophic	Catastrophic	Severe
	(4) Loss of Spacecraft	Catastrophic	Severe	Severe
	(3) Loss of Mission	Severe	Severe	High
	(2) Degraded Mission	High	Moderate	Low

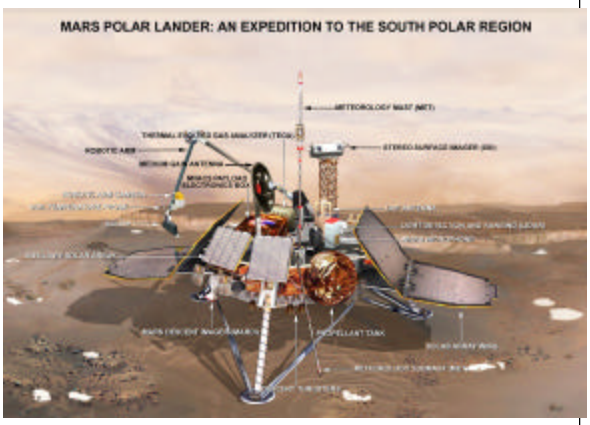
Top 10 Development Risks (+ Countermeasures)

- Personnel Shortfalls
  - use top talent
  - team building
  - training
- Unrealistic schedules/budgets
  - multisource estimation
  - designing to cost
  - requirements scrubbing
- Developing the wrong Software functions
  - better requirements analysis
  - organizational/operational analysis
- Developing the wrong User Interface
  - prototypes, scenarios, task analysis
- Gold Plating
  - requirements scrubbing
  - cost benefit analysis
  - designing to cost
- Continuing stream of reqts changes
  - high change threshold
  - information hiding
  - incremental development
- Shortfalls in externally furnished components
  - early benchmarking
  - inspections, compatibility analysis
- Shortfalls in externally performed tasks
  - pre-award audits
  - competitive designs
- Real-time performance shortfalls
  - targeted analysis
  - simulations, benchmarks, models
- Straining computer science capabilities
  - technical analysis
  - checking scientific literature

Source: *Adapted from Boehm, 1989*

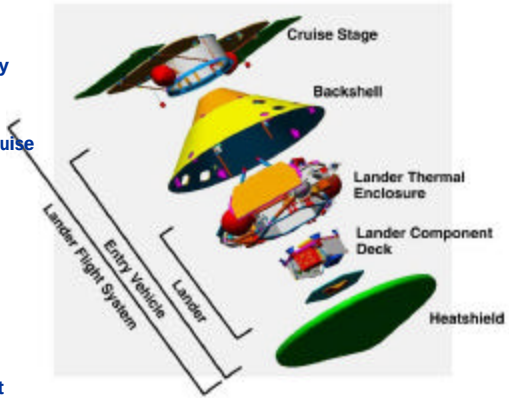
Case Study: Mars Polar Lander

- Launched
  - 3 Jan 1999
- Mission
  - Land near South Pole
  - Dig for water ice with a robotic arm
- Fate:
  - Arrived 3 Dec 1999
  - No signal received after initial phase of descent
- Cause:
  - Several candidate causes
  - Most likely is premature engine shutdown due to noise on leg sensors



What happened?

- Investigation hampered by lack of data
  - spacecraft not designed to send telemetry during descent
  - This decision severely criticized by review boards
- Possible causes:
  - Lander failed to separate from cruise stage (plausible but unlikely)
  - Landing site too steep (plausible)
  - Heatshield failed (plausible)
  - Loss of control due to dynamic effects (plausible)
  - Loss of control due to center-of-mass shift (plausible)
  - Premature Shutdown of Descent Engines (most likely!)
  - Parachute drapes over lander (plausible)
  - Backshell hits lander (plausible but unlikely)



Premature Shutdown Scenario

- Cause of error
  - Magnetic sensor on each leg senses touchdown
  - Legs unfold at 1500m above surface
    - transient signals on touchdown sensors during unfolding
    - software accepts touchdown signals if they persist for 2 timeframes
    - transient signals likely to be long enough on at least one leg
- Factors
  - *System* requirement to ignore the transient signals
    - But the *software* requirements did not describe the effect
    - s/w designers didn't understand the effect, so didn't implement the requirement
  - Engineers present at code inspection didn't understand the effect
  - Not caught in testing because:
    - Unit testing didn't include the transients
    - Sensors improperly wired during integration tests (no touchdown detected!)
    - Full test not repeated after re-wiring
- Result of error
  - Engines shut down before spacecraft has landed
    - When engine shutdown s/w enabled, flags indicated touchdown already occurred
    - estimated at 40m above surface, travelling at 13 m/s
    - estimated impact velocity 22m/s (spacecraft would not survive this)
    - nominal touchdown velocity 2.4m/s

SYSTEM REQUIREMENTS		FLIGHT SOFTWARE REQUIREMENTS
	3.7.2.2.4.2	Processing
1) The touchdown sensors shall be sampled at 100-Hz rate. The sampling process shall be initiated prior to lander entry to keep processor demand constant. However, the use of the touchdown sensor data shall not begin until 12 meters above the surface.	a.	The lander flight software shall cyclically check the state of each of the three touchdown sensors (one per leg) at 100 Hz during EDL.
	b.	The lander flight software shall be able to cyclically check the touchdown event state with or without touchdown event generation enabled.
2) Each of the 3 touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic. The test shall consist of two (2) sequential sensor readings showing the expected sensor status. If a sensor appears failed, it shall not be considered in the descent engine termination decision.	c.	Upon enabling touchdown event generation, the lander flight software shall attempt to detect failed sensors by marking the sensor as bad when the sensor indicates "touchdown state" on two consecutive reads.
3) Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.	d.	The lander flight software shall generate the landing event based on two consecutive reads indicating touchdown from any one of the "good" touchdown sensors.

X

Adapted from the "Report of the Loss of the Mars Polar Lander and Deep Space 2 Missions -- JPL Special Review Board (Casani Report) - March 2000". See http://www.nasa.gov/newsinfo/marsreports.html

Learning the Right Lessons

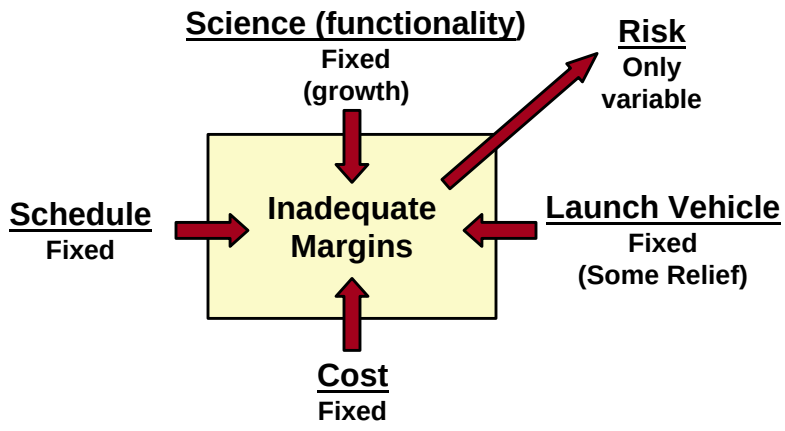
- **Understand the Causality**
  - Never a single cause; usually many complex interactions
  - Seek the set of conditions that are both necessary and sufficient…
    - …to cause the failure
- **Causal reasoning about failure is very subjective**
  - Data collection methods may introduce bias
    - e.g. failure to ask the right people
    - e.g. failure to ask the right questions (or provide appropriate response modes)
  - Human tendency to over-simplify
    - e.g. blame the human operator
    - e.g. blame only the technical factors

"In most of the major accidents of the past 25 years, technical information on how to prevent the accident was known, and often even implemented. But in each case… [this was] negated by organisational or managerial flaws." (Leveson, Safeware)

Is there an existing "Safety Culture"?

- Are overconfidence and complacency common?
  - the Titanic effect - "it can't happen to us!"
  - Do managers assume it's safe unless someone can prove otherwise?
- Are warning signs routinely ignored?
  - What happens to diagnostic data during operations?
  - Does the organisation regularly collect data on anomalies?
  - Are *all* anomalies routinely investigated?
- Is there an assumption that risk decreases?
  - E.g. Are successful missions used as an argument to cut safety margins?
- Are the risk factors calculated correctly?
  - E.g. What assumptions are made about independence between risk factors?
- Is there a culture of silence?
  - What is the experience of whistleblowers? (Can you even find any?)

Failure to manage risk



Adapted from MPIAT - Mars Program Independent Assessment Team Summary Report, NASA JPL, March 14, 2000.
See http://www.nasa.gov/newsinfo/marsreports.html

Summary

- Risk Management is a systematic activity
  - Requires both technical and management attention
  - Requires system-level view
  - Should continue throughout a project
- Techniques exist to identify and assess risks
  - E.g. fault tree analysis
  - E.g. Risk assessment matrix
- Risk and Requirements Engineering
  - Risk analysis can uncover new requirements
    - Especially for safety-critical or security-critical applications
  - Risk analysis can uncover feasibility concerns
  - Risk analysis will assist in appropriate management action