Risk Management During Design

Leila Meshkat

Jet Propulsion Laboratory

California Institute of Technology

Outline

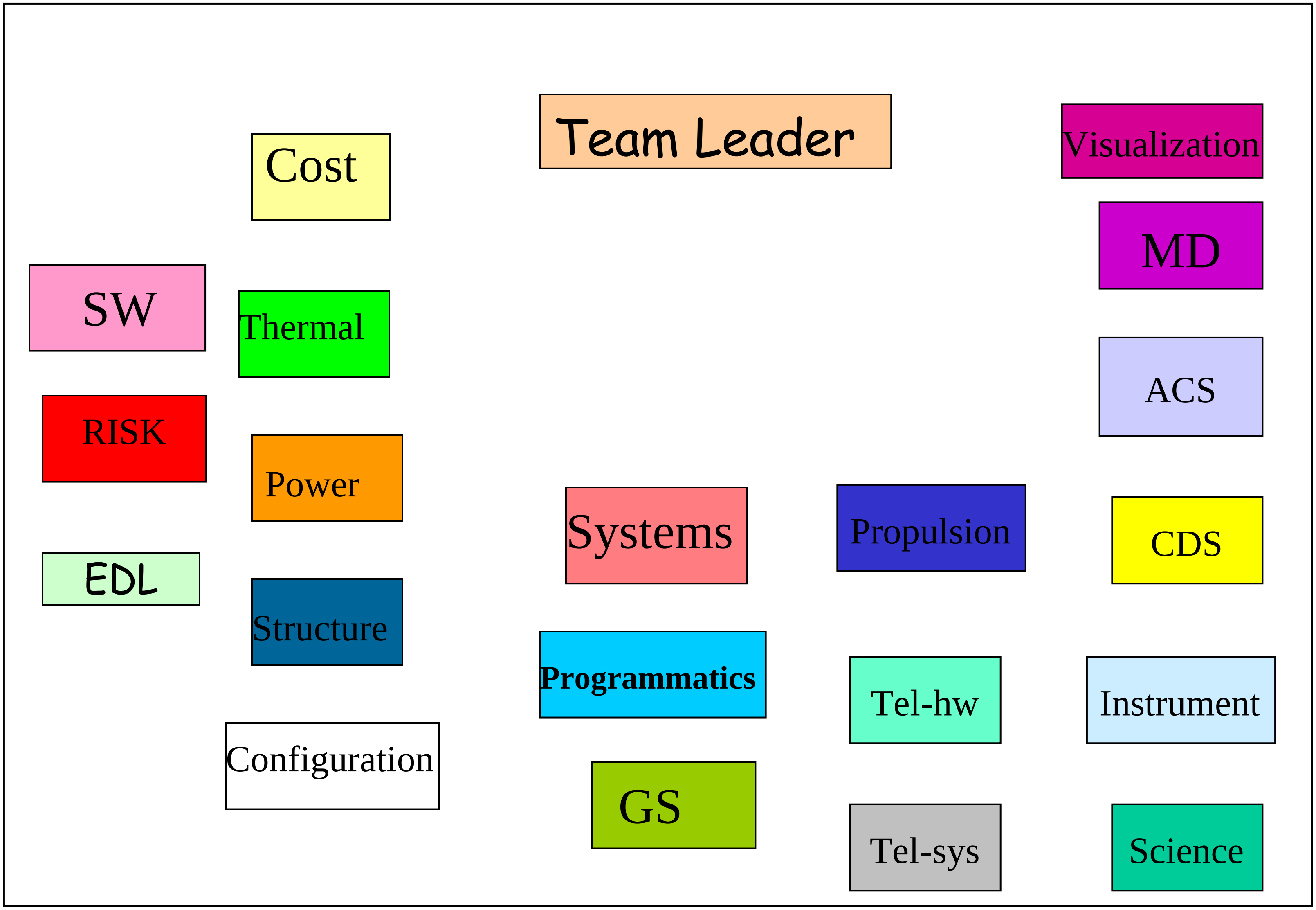
- Background
  - TeamX
  - Risk Assessment in TeamX
  - PRA in TeamX
    - Motivation
    - Risk Assessment Process
    - Experiments with PRA
      - Refinement/Customization of existing models.
      - Data collection for PRA modeling.
  - Lessons Learned
- Risk Patterns during design
- Generalized approach
- Summary & Conclusions

Background

- TeamX
  - Produces Conceptual Space Mission Designs.
  - Mainly for the purpose of Feasibility Studies.
  - Duration of study is typically one to two weeks.
  - Final report includes equipment lists, mass and power budgets, system and subsystem description, and projected mission cost estimate.

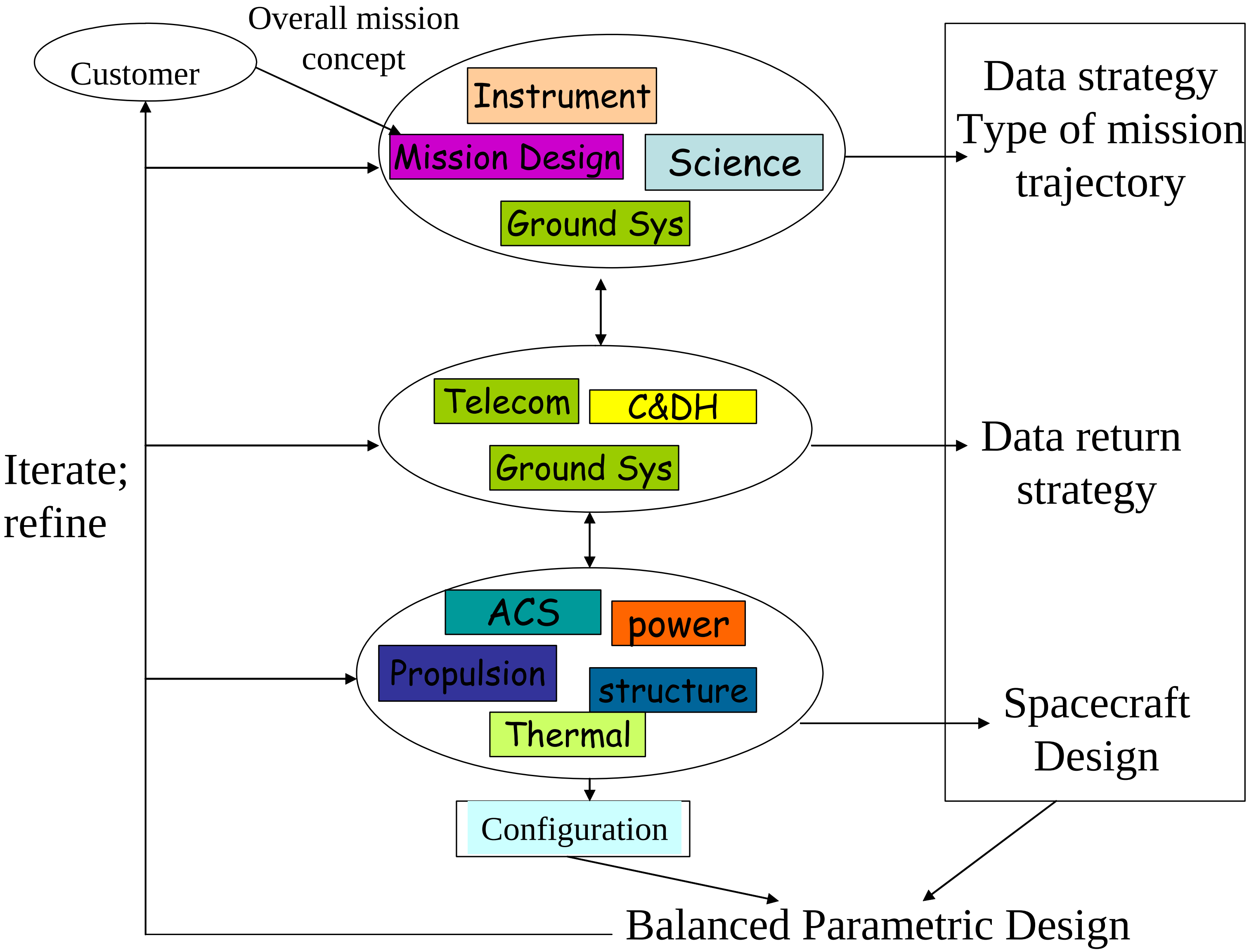

JPL-29656 ec

Team X
(at the Project Design Center)



Team X Mission Design Process

- Customer presents an overall concept during pre-session.
  - Guidelines are defined.
    - Tentative schedule & cost cap
  - Feasible options are identified.
  - Key mission drivers are identified.
  - Initial Set of Requirements are identified.
- Science and Instruments, Mission Design and Ground Systems define science data strategy, type of mission and trajectory.
- Telecom, Ground Systems, CDH develop data return strategy
- ACS, Power, Propulsion, Thermal, Structure iterate spacecraft design.
- Requirements are further granulated and refined.
- Configuration prepares initial concept
- Subsystem designs are refined
- Balanced parametric design is achieved.
- Configuration is refined to accommodate final requirements and constraints.


Overall mission concept
Customer
Instrument
Mission Design
Science
Ground Sys
Data strategy
Type of mission
trajectory
Telecom
C&DH
Ground Sys
Data return strategy
Iterate; refine
ACS
power
Propulsion
structure
Thermal
Spacecraft Design
Configuration
Balanced Parametric Design

Risk Assessment in TeamX

- Provide a framework to enable consideration of risk throughout the design process.
- Produce better risk profiles for the mission to document in the report.
- Facilitate better communication between the various subsystem experts.
- Capture the information communicated between subsystem experts for future reference and decision traceability purposes.

Approach

STEP ONE:	STEP TWO	STEP THREE	FUTURE STEPS
•Define Risk Terminology; •Define software requirements	•Design Architecture for Software tool •Initiate Process of “risk training” within team	•Develop prototype tool. •Train team members to use tool and refine tool using team feedback. •Determine role of risk chair/ approach for risk communication within team.	•Use tool concurrently during design. •Build standard risk item libraries to make consistent assessments across missions. •Refine tool •Add additional features; •Towards Probabilistic Risk Assessment in Conceptual Design

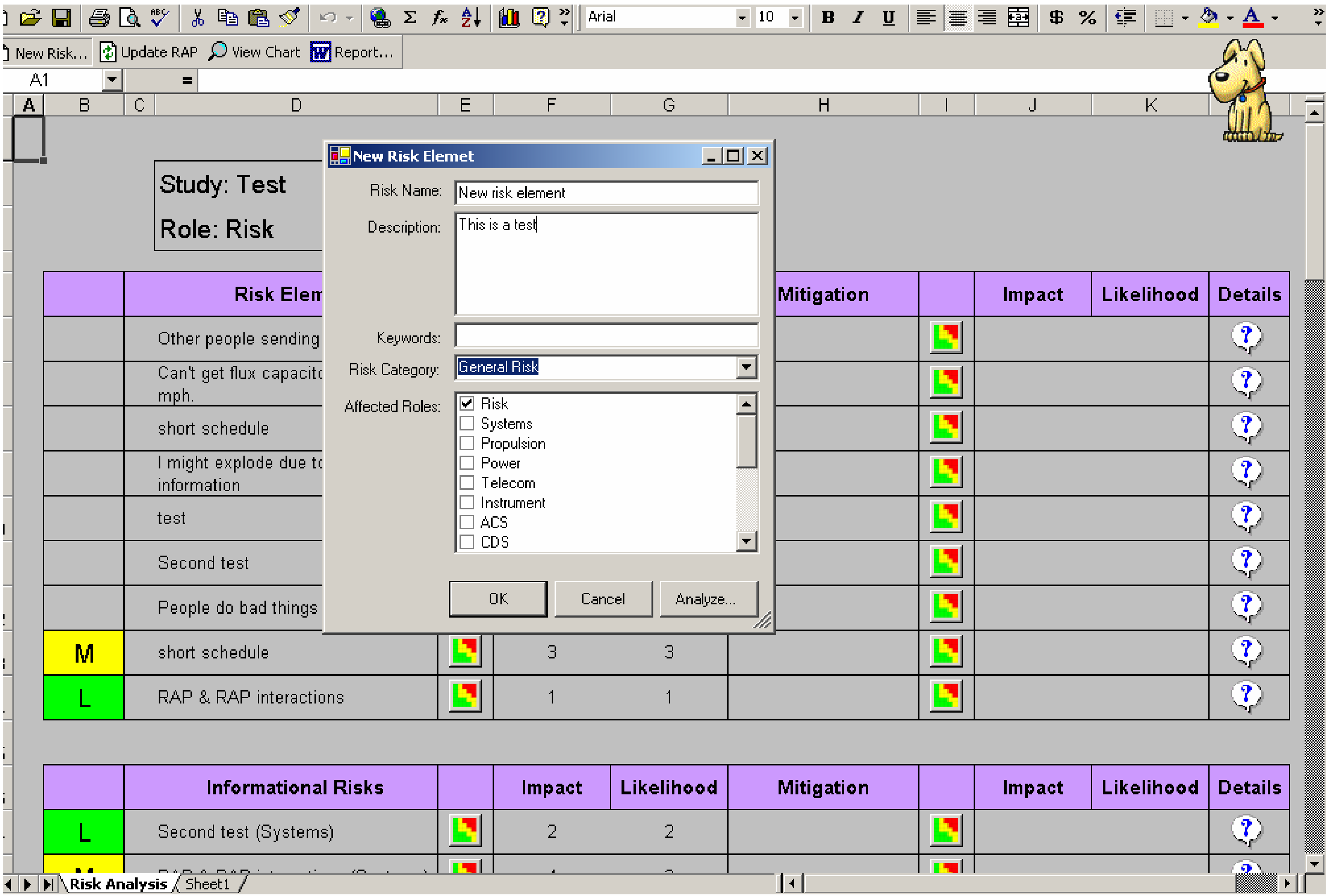
Risk & Rationale Assessment Program (RAP)

- Distributed software that enables communication between designers.
- User can initiate a “New Risk” or assess a risk already on their screen.
- Features include:
  - Risk statement- likelihood, impact, type of risk.
  - Mitigation- residual likelihood & impact.
  - Details – any additional explanation.
  - Objective that the risk effects.
  - Affected Roles
- System allows user to enter as little or as much information as they want.
- It can automatically generate reports for any combination of roles.
  - Report includes fever chart, overview table, and all details

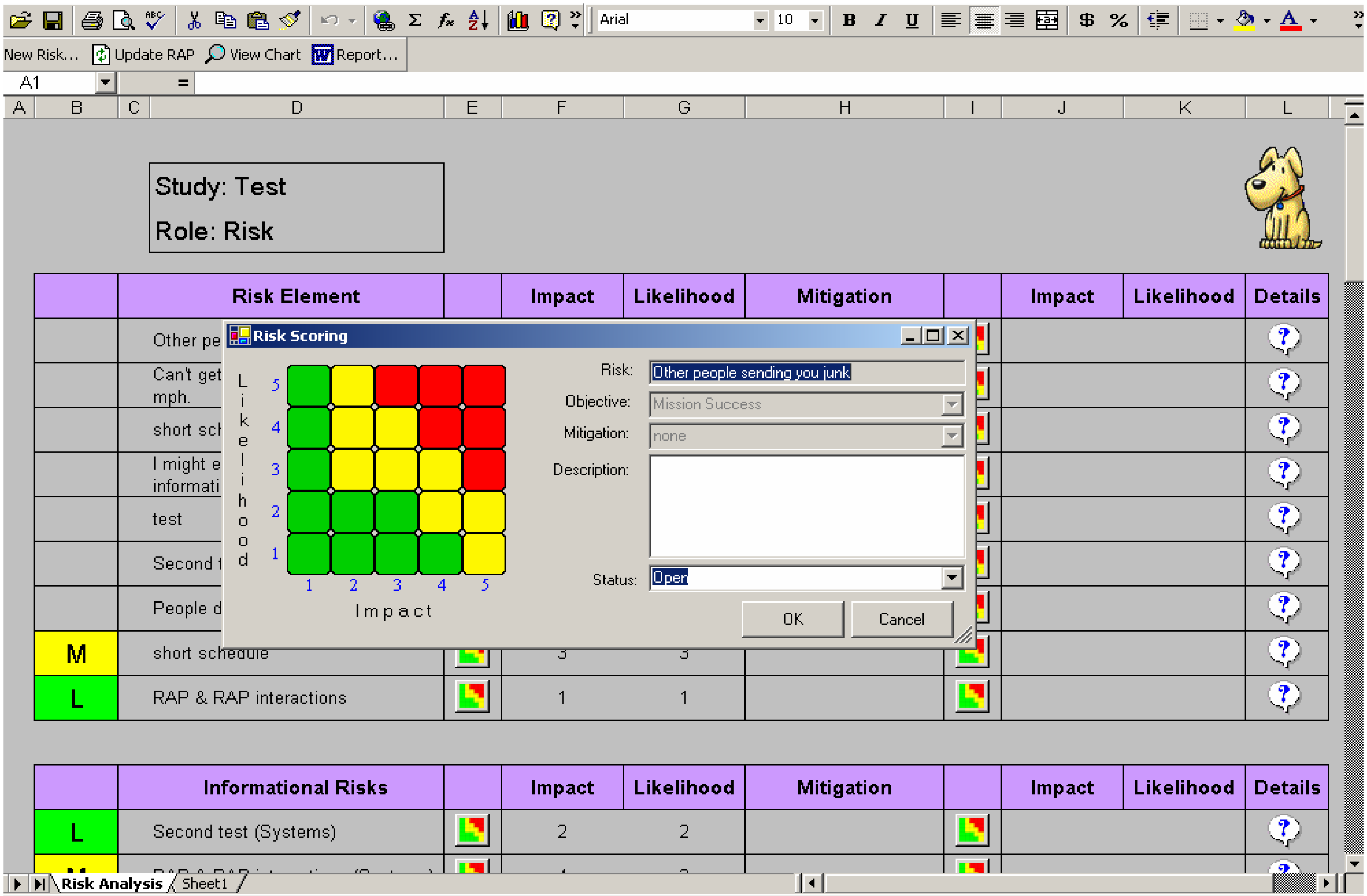
Risk Assessment Process

- Identification
  - Risk elements are identified and sent to the designers.
  - Risks are generated from scratch for each study.
  - Major Assumptions & Events are also identified.
- Assessment
  - Risks are assessed;
  - Mitigations suggested or applied to design are captured.
  - Descriptions are often included.
  - Events can be correlated with risk to give insight into failure scenarios.
  - Designers often open their tool and assess their risks towards the end of the session when the design has been *already* determined.
- Synthesis
  - Often there are inconsistencies between various expert opinions about elements.
  - This leads to conversations and clarifications.
  - Reports are generated from final risk profile.

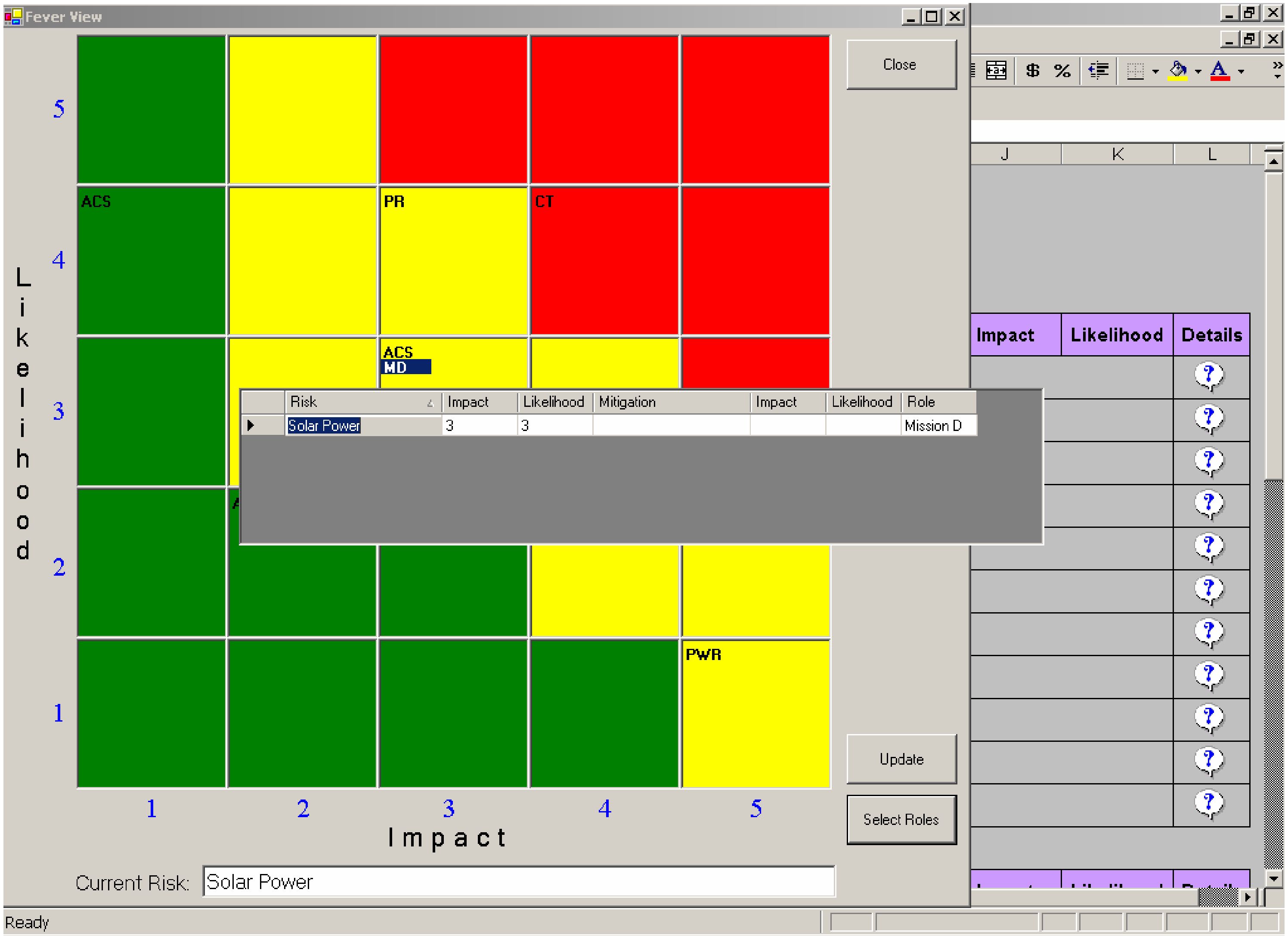
Risk & Rationale Assessment Program (RAP)



Risk & Rationale Assessment Program (RAP)



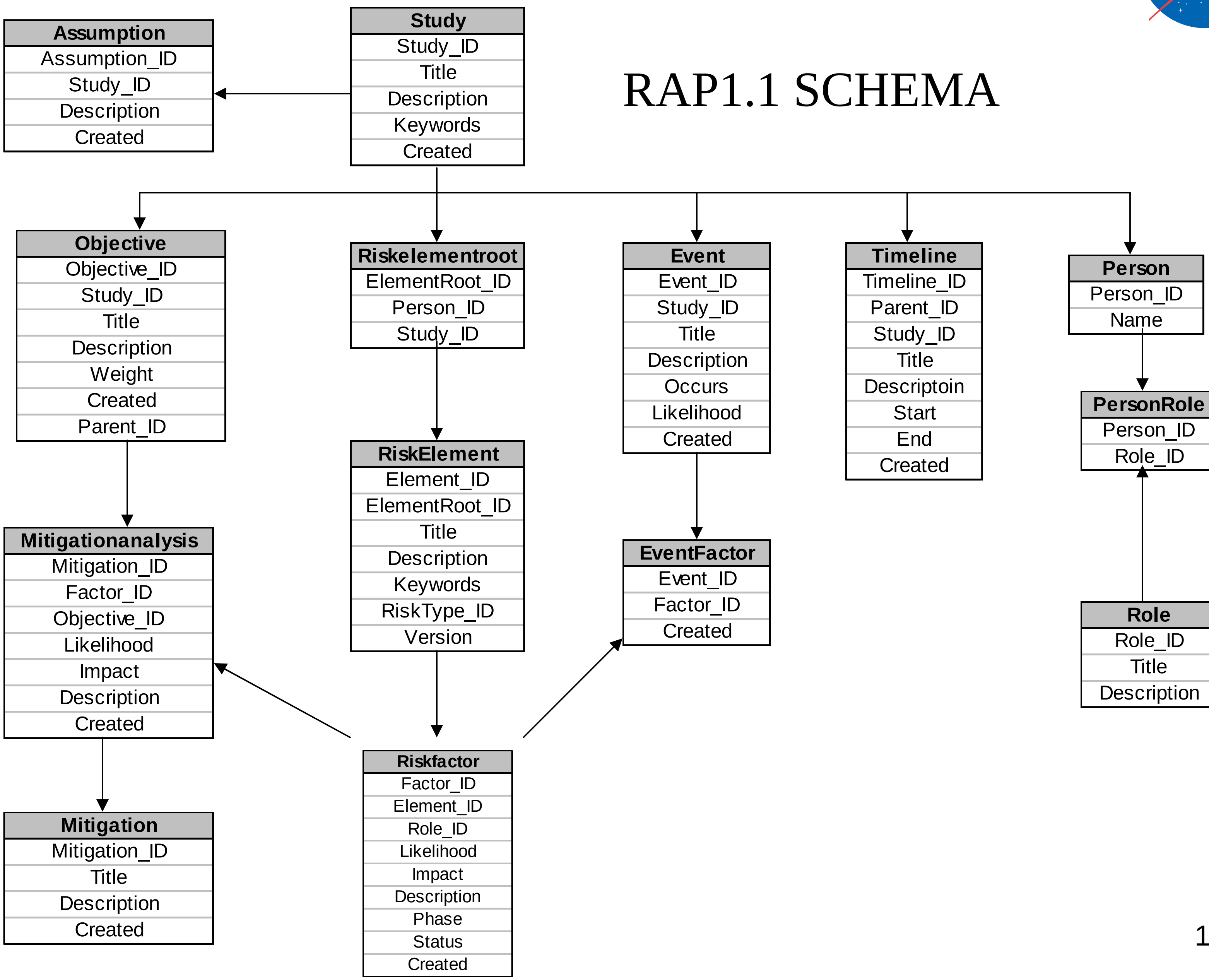
Risk & Rationale Assessment Program (RAP)



Motivation for PRA during Design

- PRA during Conceptual design
  - Drives the refinement of the design by identifying optimal areas for investments.
  - It is more viable and less expensive to refine a design at the time that it is being conceived – hence PRA during conceptual design.
- Concurrent Engineering Teams
  - Greatly reduce the design time and costs
  - Capability to produce a consistent and valid risk metric associated with such designs would greatly enhance the value of such design teams.

RAP1.1 SCHEMA



Experiments with PRA

- Case study for Mars Aero-capture Mission Design:
  - Used the TeamX sessions to generate data needed for conducting PRA
    - Data related to expert opinions about events, risk items, and mitigations was collected through RAP.
    - Design information, and system schematics was included in the subsystem write-ups.
    - Used information for building PRA models with several different tools.
      - These tools include DDP, QRAS and Galileo ASSAP
      - Each tool served a different purpose
    - Developed algorithm for combining different PRA tools and approaches.

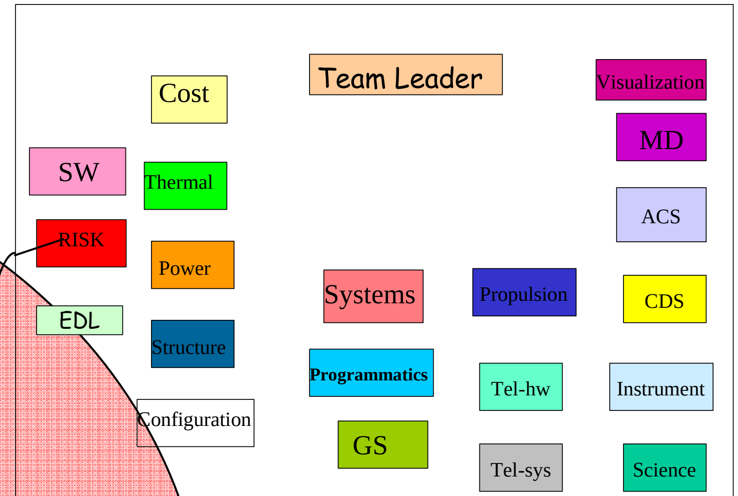
Experiments with PRA

- Mars Odyssey (ODY) Risk Models
  - Developed risk models for the Mars Odyssey Orbiter using project information before the TeamX session.
  - The goal of the TeamX sessions was for the team to adopt the existing design within the TeamX templates.
  - Utilized the TeamX session to collect additional risk information from the designers.
  - Updated the risk models accordingly.
- Mars Telecommunications Orbiter (MTO)
  - Used existing TeamX design for MTO, as well as the ODY models to generate MTO risk models.

Problem Statement

- How do you manage risks during the design process?
  - Risk Identification
    - How can you tell where the risks are?
    - What are the indicators?
    - How do you know that the system is out of balance?
  - Risk Assessment
    - How do you assess these risks?
  - Risk Mitigation
    - How to you mitigate them?
  - Continuous Risk Management
    - How do you iterate and continue with this process?

Risk Identification



Who do I speak with NOW?

Patterns during design: Risk Identification

- Mission Risk Drivers
  - New Technology
  - Environmental factors
  - Design Challenges
  - Reliability Issues
    - Mechanisms, Electronics, Software, etc.
  - Major Events
    - EDL, Orbit Insertion, rendezvous, etc.

These risks are often predictable from early in the design process

Patterns during design: Risk Identification

- Surprises during the design process
  - Significant deviation from expected mass, cost or performance for any element of the spacecraft.
  - Significant deviation from the expected challenge associated with any subsystem design.
    - Too much or too little interaction between a designer and the rest of the team.
      - Too much interaction – is it a complex issue, or is the designer missing an important piece of information?
      - Too little interaction – is the subsystem in question keeping up to date with the rest of the design?
    - Too much or too little management (team lead and systems engineer).
      - Too much – Is there some disagreement between domain expert and management? Why?
      - Too little - Is there a critical issue that management is unwilling to address? Why?
        - » Is something going unnoticed?
    - Too much or too little effort (man/hours) needed
      - Too much – Are we over-designing?
      - Too little - Are we doing our best?

Something must be out of balance!!!

Patterns during design: But how do I measure surprises?

- Expected mass, cost, performance for each subsystem of each type of mission.
  - Obtained from historical data.
  - Adjusted to current project.
- Expected challenge associated with a subsystem design.
  - Indices for subsystem complexity.
- Expected interactions between designers, and management.
  - Communications (time, # of times, # of issues brought up in MMR's, etc.)

Risk Assessment

- Now I know something's wrong, how do I assess the risks?
  - Zoom in to the risky area.
  - Ask as many questions as it takes to identify the exact cause of the problem.
  - Use probabilistic analysis techniques and any available data for risk assessment purposes.

Risk Mitigation

- Brainstorm with the associated designers.
- Make sure all affected subsystem engineers are aware of the new mitigation strategy.
- Measure the effect this has on the system balance.

Continuous Risk Management

- Define "System Balance" to be a Vector as follow:
- [E(mass), E(cost), E(performance), E(interaction between all 2x2 combinations of key project personnel),..]
- Determine the System Balance vector at time intervals during the project and measure against the actual values of this vector.
- Keep an eye on the fluctuations.

Lessons Learned

- Lessons Learned:
  - TeamX is very valuable for validating/updating risk models that have been built before the sessions.
    - Conduct a “red team review” of the risk models with the participation of all discipline experts.
  - Many Design decisions made “on-the-fly” in the TeamX setting. The process would need to change in order to accommodate a PRA-based-design.
  - Designs have considerable heritage from previous designs, and therefore having a library of PRA models is extremely useful.
  - Need consistent data for input to the risk models.

Summary & Conclusions

- There are recurring risk patterns during design that enable us to formalize the Risk Management Process.
- This formalization helps us identify, assess, and mitigate risk.
- It also provides the means for Continuous Risk Management during Design.