TAGES-2SD Risk Management Process

Prepared by: Mark Kelsch

Date: 7/23/02

Scope

- This document captures the procedures and techniques which will be used to identify project risks for TAGES-2SD. It outlines the procedures which will be used to identify, track and communicate risks. It discusses tools for quantifying and prioritizing risks. It details the acceptance criteria for a risks throughout the life of the project. It presents normal risk correction and mitigation procedures.

Introduction

- Risk is an unavoidable part of any new science or engineering project. The goal of risk management is to avoid unnecessary risks, communicate unavoidable risks, and aid in project planning by prioritizing activities which will reduce risk. Good risk management is used to develop procedures and plans to control the engineering process and to aid in engineering decisions. Project failure or large changes late in the project can be avoided by careful planning at the start of the project.
- Risk management is a project planning and tracking tool.

Mission Statement

- **The PGF-SP hardware is being developed to support the TAGES and RASTA experiments. The hardware will be used to grow plants in a monitored and controlled environment. The plants will be supplied with light and conditioned air. The PGF-SP will operate in a safe and effective manner with minimal impact to crew activities. The PGF-SP will be designed to interface the SST as a standard Middeck locker or as an ISS express rack device. The PGF-SP will be designed to maximize manifest opportunities and maximize flexibility for use on other missions.**

Continuous Risk Management

- Risk management will be conducted throughout all phases of the project
- Focus between planning and analysis will shift as the project matures
- New risks become evident throughout the project life cycle
- Risks will be identified and tracked throughout the project
- Risk management will be an integral part of project management

Project Unique Risks

- This plan primarily addresses project unique risks.
  - Technical challenges specific to the project goals
  - Project risks associated with special schedule, budget, and resource limitations
- Risks may be identified which are deemed common, recurring or normal.

Common Project Risks

- Risks which are common to most projects will be addressed by creating or correcting cross project plans and procedures as well as training
  - Project management procedures/check lists
  - Technical best practices/check lists
  - Standard operating procedures
  - Project templates
- Risks which are controlled adequately by plans, procedures and systems already in place will not be tracked specifically by this process
- Common risks are controlled by normal project management procedures

Risk Life Cycle

- Identify Project Risk
- Evaluate Risk for potential to impact the project and prioritize efforts
- Develop corrective action plans to reduce project risk
- Incorporate corrective actions into normal program plans schedules, procedures, requirements etc.
- Track progress of corrective actions for effectiveness
- Retire risks as requirements, designs, analysis, test, inspection etc. indicate risks are no longer significant
- Record Lessons Learned and modify SOP's to avoid recurrence

Risk Identification

- Risks will be identified at all points in the project.
  - Identified through structured procedures such as brainstorming, Fault Tree analysis or Failure Mode and Effects analysis.
  - Identified through normal managerial, quality and engineering processes where a potential problem becomes evident.
- New Risks will be added to the Risk Data Base and reviewed at the next team meeting.
- Risks will follow the NASA preferred form of :
  - Undesirable Condition; Possible negative effect on project goals including worst case outcomes

Number of Risks Identified

- The number of risks documented and tracked does not necessarily reflect the amount of project risk
- Risks are not only issues but also place holders for important efforts which should be executed to improve the overall project performance
- Some risks may define potential problem areas which require simple solutions such as:
  - Creating contingency plans for mission changes
  - Adding additional informal testing to insure formal test success

Risk Evaluation

- Risks will be evaluated based on the current documented project plan, standard procedures and technical baselines.
- Risks will be evaluated for three critical characteristics based on applicable historical data (whenever available) or cumulative team experience.
  - Magnitude of Impact: Impact to project success.
  - Probability of Occurrence/Failure: Statistical probability that the negative condition or event will occur.

Risk Evaluation

- **Risk Characteristics Continued**
  - **Probability of detection: Probability that the negative condition will be detected by systems or procedures currently in place and that procedures or systems currently in place will correct the problem before it impacts project goals. If there is no contingency plan in case of detection then the probability of detection is considered zero.**

Magnitude of Failure Definition

	Safety Impacts
10	Loss of life
9	Serious injury, serious damage to vehicle
8	Moderate crew injury or damage to vehicle, condition of probable serious injury or damage to vehicle (narrowly averted incident)
7	Moderate Injury to ground personnel, minor crew injury, minor vehicle damage, condition of probable minor crew injury or vehicle damage
6	Nuisance condition on orbit (condition effecting or interfering with other crew or vehicle operations)
5	Minor injury to ground personnel
4	Condition of possible minor injury to ground personnel
3	Condition requiring significant increase in on orbit crew time
2	Condition requiring unpracticed/unreviewed crew activities
1	N/A

Magnitude of Failure Definition

	Science Impacts
10	N/A
9	N/A
8	N/A
7	N/A
6	Complete loss of mission scientific value, no data available to draw any conclusion of scientific value
5	Failure to meet all primary scientific objectives, unable to draw defendable scientific conclusions
4	Significant reduction in primary scientific objectives
3	Small reduction in primary scientific objectives
2	Failure to meet all secondary scientific objectives
1	Reduction in secondary scientific objectives

Magnitude of Failure Definition

	Performance Impacts
10	N/A
9	N/A
8	N/A
7	N/A
6	Hardware does not perform in a controlled and predictable manner on orbit
5	Hardware continually does not perform within defined limits of operation for multiple variables on orbit
4	Hardware fails to keep one variable within limits continuously or multiple variables exceed their limits occasionally (<10% of time)
3	Hardware is very difficult to manifest, hardware is not capable of a second mission
2	Hardware is difficult to manifest
1	Hardware requires significant effort to refurbish or upgrade for a second mission

Magnitude of Failure Definition

	Cost Impacts	Schedule Impacts
10	N/A	N/A
9	N/A	N/A
8	N/A	N/A
7	Cancellation in project	Cancellation of project
6	>100% increase in cost	Missing a scheduled/manifested flight, > 100% schedule slip
5	>80%	> 80% schedule slip
4	>60%	> 60% schedule slip
3	>40% Increase in cost	> 40% schedule slip
2	>20%	> 20% schedule slip, missing a possible flight opportunity
1	>10%	> 10% schedule slip

Risk Priority Number

- The risk priority number (RPN) is a method for quantifying and prioritizing risks. Using historical data we estimate:
  - Probability of occurrence of a specific failure (PO)
  - Probability of Detection of the failure before full impact to the project (PD). This assumes there is a planned corrective action or mitigation which will reduce the impact to the project
  - Magnitude of Failure which is the impact to overall project success.
  - RPN = PO x (1- PD) x MF x 100
  - RPN reflects the level of effort which would be required to prevent project failure caused by the specific risk.

Criticality Index

- **Severity Category and Failure Probability Index (typically used in FMEA-CIL) will be derived from the Impact and Probability of Detection.**
- **The relationship between Severity Category and Magnitude of Impact is:**

Magnitude of Impact	Severity Category	Severity Category Definition
10 - 7	I	Catastrophic - Failure of severe dimensions, Failure is a given
6 - 4	II	Critical - Serious failure which can cause major impact on project deliverables
3 - 2	III	Marginal - moderate failure which can lead to project difficulties if not resolved quickly
1	IV	Minor - Normal project management and planning required

Failure Probability Index

- **The relationship between Relative Probability of Failure and Probability of Occurrence is:**

Probability of Occurrence	Failure Probability Index	Failure Probability Index
25% - 100%	A	Frequent - High probability of occurrence during project
5% - 24.9%	B	Moderate
1% - 4.9%	C	Occasional
.1% - .99%	D	Remote
0 - .099%	E	Extremely Unlikely

Initial Risk Priority Number

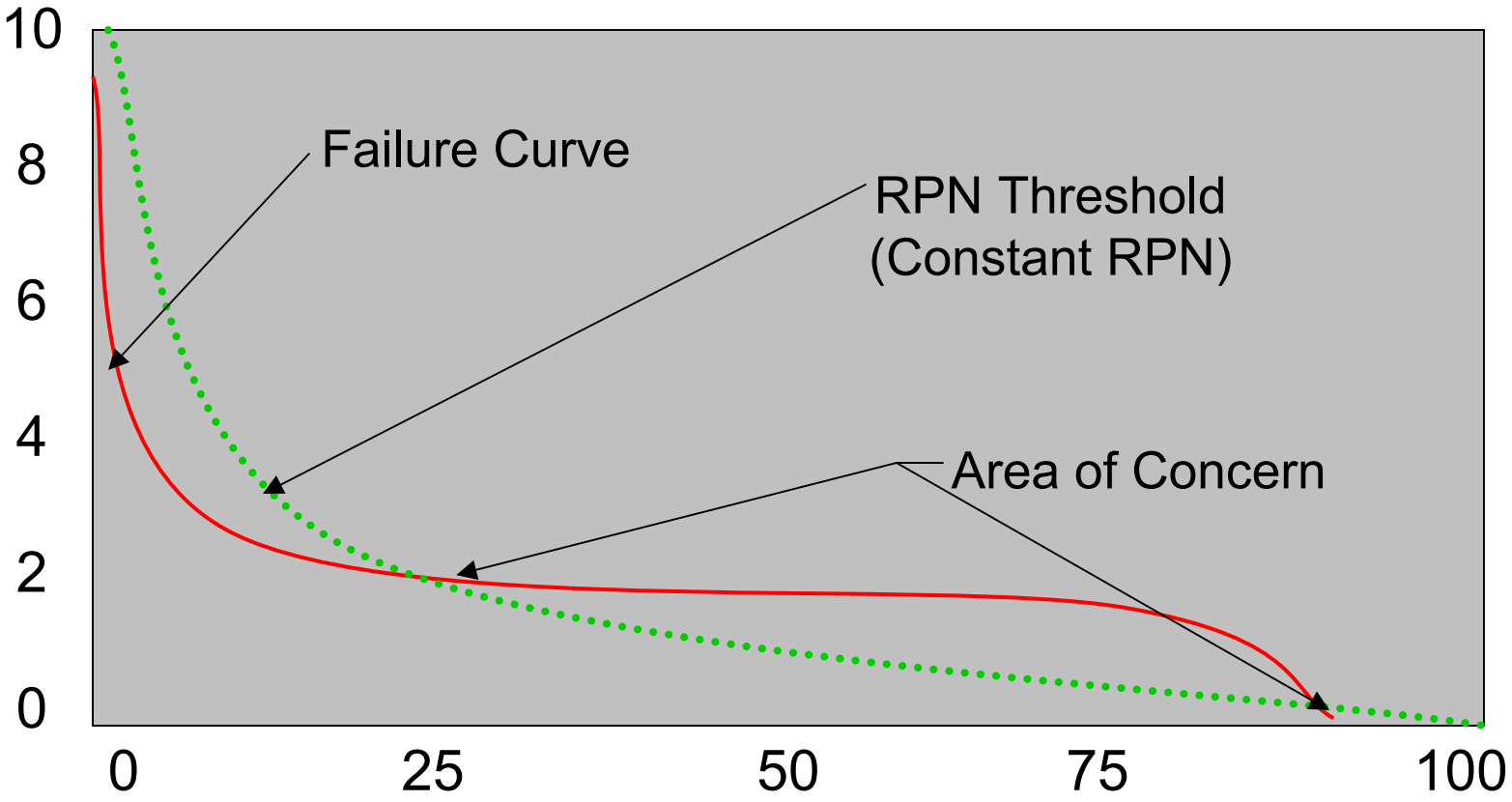
- Initial RPN's are calculated assuming no special technology must be developed, no additional resources will be required, no special procedures or tests will be performed.
- This means only projects which are essentially a repeat of a successful project will start with very low RPN.
- The Initial RPN will be used to prioritize activities, develop project schedules and plans, identify resource requirements, special testing or inspections, and generate technology development efforts.
- These project changes which address high risk items are the corrective action plans
- Corrective action plans include efforts to improve reliability, detect failures early and reliably, and develop contingency plans for reducing the impact of the failure to the project

Caution On Worst Case Impact Evaluation

- It is possible that certain risks may seem acceptable because the worst case outcome has a very low probability of occurrence. However, this does not take into account non-linearity in the Probability vs. Impact curve.
- Example
  - Condition: Software bit error caused by EMI/Cosmic Radiation
  - Consequences: System lock up with no reboot, system lock up with reboot, lost data, slowed network speed resulting in poor control and partial loss of science

Caution On Worst Case Impact Evaluation

- **The Probability of Occurrence Vs. Magnitude of impact curve might look like:**



Using Consistent Cases

- A consistent failure scenario should be used to calculate all values used in the RPN.
- This will ensure that the Probability of failure is for the specific magnitude of impact and probability of detection.
- Inconsistencies will produce erroneous RPN values which may result in more or less effort being focused on a risk than is appropriate.
- If necessary a second risk may be identified which incorporates a slightly different failure scenario and a different corrective action plan

Predicted RPN

- **Predicted RPN's are calculated assuming that corrective actions are successfully implemented.**
- **Predicted RPN's are used to determine if the corrective actions are sufficient to make the risk of failure acceptable.**
- **If a predicted RPN is still high then additional corrective actions must be added to the project plan.**
- **Since corrective actions are not always successfully implemented the initial RPN is tracked until the corrective action is completed.**

Project Risk Acceptance and Tracking

- All risks must have a feasible detection, mitigation, and correction plan as soon as they are identified or tasks required to determine the proper corrective action must be developed.
- Risks which are detected and corrected by established engineering procedures such as quality inspections and hardware testing will be accepted if there RPN (risk priority number) is one (1) or less. These risks will not be tracked throughout the project but may be reviewed at critical design reviews
- Risks which are not detected by normal engineering procedures will be accepted when the required corrective action is added to the project plan and the resulting predicted RPN is one (1) or less. These risks will be discussed by the project team on a monthly basis.
- Risks which have been retired will no longer be tracked.

Risk Acceptance Schedule

Maximum Initial RPN

Maximum RPN	Any 1 Risk>	Any 5 Risks>
• Project definition phase	500	400
• Project Planning phase	400	300
• Conceptual design review	200	100
• Preliminary design review	100	50
• Critical Design Review	10	5
• Pre-flight testing	5	3
• Pre-mission	1.0	1.0

Unavoidable Risk Acceptance

- **Risks which require excessive resources or time to mitigate or which are simply a defined part of the project (i.e. successfully proving a theory through an experiment) may be accepted by the project management team with the concurrence of the NASA management team. The specific technical rational for the acceptance and an estimate of the cost, time or resources to mitigate the risk will be presented to the NASA management team to justify the decision and document the current state of the project.**
- **The risk will be tracked throughout the course of the project and will be reconsidered if the predicted RPN increases by more than 25%.**
- **If the risk is overcome by events and is determined to be a non-risk the justification will be presented at the next quarterly review. The risk will then be retired.**

Risk Retirement

- Risks will be considered retired (closed) when the correction and mitigation plans have been fully implemented. At this time the initial RPN will drop to the predicted RPN.
- This means that redesign, analysis, testing, and inspections which are critical to reducing the probability of occurrence, probability of non-detection, or magnitude of impact, must be completed at specific points in the schedule in order to meet the Risk Acceptance Schedule.
- Some risks will be replaced as correction and mitigation plans are implemented.
- Example
  - Original Risk: PGF-SP EMI disrupts shuttle system - RPN = 45
  - Corrective action: Add filters to design, Add EMI test to schedule - new RPN = 0.9
  - Original risk is retired when EMI testing is included in schedule and test plan.
  - New Risk: PGF-SP fails EMI test, rework required - RPN = 25
  - Corrective action: Add one cycle of pre-test and modification - New RPN = 0.9
  - New Risk will be retired after passing EMI test

Rationale for Risk Acceptance Schedule

- Project Definition should identify key risks for the overall project. If significant risks exist at this point, the project should be redefined to bring these into some acceptable range or deferred. An RPN of 500 represents a 50% chance that if **no special corrective action** was taken throughout the project that an undetected failure would occur causing a magnitude 10 project failure. This criteria will be used to prevent impractical or improbable projects from beginning. Re-planning may include changes in scope, increase in resources, multi-step development with a critical “decision to proceed review”, or separate technology research development efforts. If other significant risks are present (more than five between 400 and 500) then the project will include significant efforts to reduce these risks also. This would result in an unmanageable project.

Rationale for Risk Acceptance Schedule

- Project planning should define specific system requirements and a project plan and schedule. Some risks will have been reduced by the creation of verifiable requirements which will reduce the risk of failures. Risks will also be reduced by incorporating specific design, analysis and testing activities in the plan. Due to lack of real design, analysis and testing large risks will still exist. The decision to proceed or re-plan will be based on the current level and quantity of risk.

Rationale for Risk Acceptance Schedule

- At the Conceptual Design Review, conceptual designs, research and preliminary analysis should lower risks noticeably. Concepts may already include failsafe designs, backup systems or detection systems for key risks. Analysis indicating significant margin in technical performance also reduces the risk of certain failures. However, without specific hardware testing some risks may still be high. An RPN of 200 represents a 20% chance that if **no special corrective action** was taken throughout the project that an undetected failure would occur causing a magnitude 10 project failure. As stated earlier, any risk with an RPN greater than 1 must have a corrective action or mitigation plan which would bring the RPN to 1 or less. Part of the success criteria for the conceptual design review will be clearly indicating the level of risk is acceptable according to the Risk Acceptance Schedule. If meeting the risk acceptance schedule is not expected at the scheduled conceptual design review it will be postponed while additional risk reduction occurs.

Rationale for Risk Acceptance Schedule

- At the Preliminary Design Review, prototype designs, testing and analysis should lower risks significantly. Hardware will be developed to test critical failure modes associated with key risks. The requirements and system definition should be mature enough to develop a reliable schedule. Again without a fully integrated system which meets all requirements some risks may still be high. An RPN of 100 represents a 10% chance that if **no special corrective action** was taken throughout the remainder of the project that an undetected failure would occur causing a magnitude 10 project failure. This is reasonable due to the fact that no flight hardware design has actually occurred. Part of the success criteria for the PDR will be clearly indicating the level of risk is acceptable according to the acceptance schedule. If meeting the risk acceptance schedule is not expected at the scheduled PDR it will be postponed while additional risk reduction occurs.

Rationale for Risk Acceptance Schedule

- At the Critical Design Review, completed flight hardware designs, significant prototype testing and extensive analysis should lower risks to nearly acceptable levels. Hardware will be developed to test critical failure modes associated with key risks. Requirements, hardware capabilities and project team capabilities should be well understood. A clear project schedule including fabrication, integration, testing and flight preparation should be developed. However, without testing of flight hardware project success is not guaranteed. An RPN of 100 represents a 1% chance that if **no special corrective action** was taken throughout the remainder of the project that an undetected failure would occur causing a magnitude 10 project failure. As stated earlier, any risk with an RPN greater than 1 must have a corrective action or mitigation plan which would bring the RPN to 1 or less. The decision to proceed with CDR will be based in part on the estimated risks without corrective actions or mitigations.

Rationale for Risk Acceptance Schedule

- Before pre-flight testing most risks should have been retired or reduced significantly. All flight hardware should already be evaluated for most of the technical requirements during integration and testing. Any expected modifications should already be made. Some risks may still need to be retired due to the cost of testing some requirements prior to pre-flight testing. An RPN of 5 represents a 0.6% chance that if **no special corrective action** was taken throughout the project that an undetected failure would occur causing a magnitude 8 project failure. It is assumed that at this point proper design and safety analysis along with planned testing will prevent any failure with a magnitude 10 impact from occurring. All plausible risks with a potential magnitude of 10 should have been corrected or mitigated by this time or they will be detected during pre-flight testing.

Rationale for Risk Acceptance Schedule

- After pre-flight testing all risks should be retired. All technical requirements have been verified. All functional testing has been completed. A thorough safety review has been completed. The probability of any significant failure should be extremely low. Any plausible failure mode which could result in a large project impact should have built in detection systems and a corrective action procedure developed for the crew (with these procedures in place the RPN should be 1 or less).

Corrective Action Categories

- **Relax Requirement/Success Criteria**
  - Seek waivers, exceptions or permanent changes to requirements in order to reduce the risk to the program.
- **Research**
  - Reviewing related data to accurately determine the probability of occurrence and impact as well as evaluating various corrective action plans and there impacts to the project.
- **Monitor**
  - Choosing indicators of potential failures and tracking their changes throughout the project to determine if failure will occur. Adding methods of failure detection which will provide feedback to initiate a contingency plan.

Corrective Action Categories

- **Improve Reliability**
  - Change design or procedures to reduce probability of failure.
- **Mitigate**
  - Add redundancy or other features which reduce impact when failure occurs.
- **Contingency Plan**
  - Create an action plan and associated procedures or design changes to recover from a failure and allow for repair, replacement or redirection to reduce the impact of the failure to the project.
- **Accept**
  - Accept the risk with little or no corrective actions. Track risks for changes which may increase or decrease the level of risk.

Corrective Action Plans

- May be a combination of any or even all of the previous options
- Should reduce the predicted RPN to 1 or less when properly executed
- Incorporated into the appropriate project documents to ensure that they are carried out
- Monitored and updated for proper implementation, effectiveness and to ensure that no new risks are being created

Contingency Triggers

- Risks which use contingency plans to reduce risk will identify a trigger which will indicate the need to begin contingency operations.
  - Triggers are measurable conditions which indicate the health of the project or equipment related to a specific failure mode or risk.
  - Project triggers are monitored and updated at least once a month or more frequently when required.
  - Technical triggers are sensors or devices which detect some performance deficiency during mission operations.

Trigger Limits

- **Trigger limits will indicate that the system is near failure and that contingency operations must be carried out.**
- **Trigger limits should be established and documented as soon as possible after the trigger is identified.**
- **Trigger limits should indicate imminent failure but give enough time for contingency plans to take effect and prevent serious project impacts.**

Risk Tracking

- Risks will be tracked until they are retired.
- Risk status will be updated monthly, and reviewed quarterly.
- Status for risk related tasks will be given during normal staff and team meetings and do not require any special format or presentation.
- If trigger values have been exceeded then corrective action plans should be put into place.
  - Corrective action plans will be integrated in to normal project documentation
  - Status for active corrective actions plans will be given following the guidelines given for mentioned earlier.

Risk Assignee

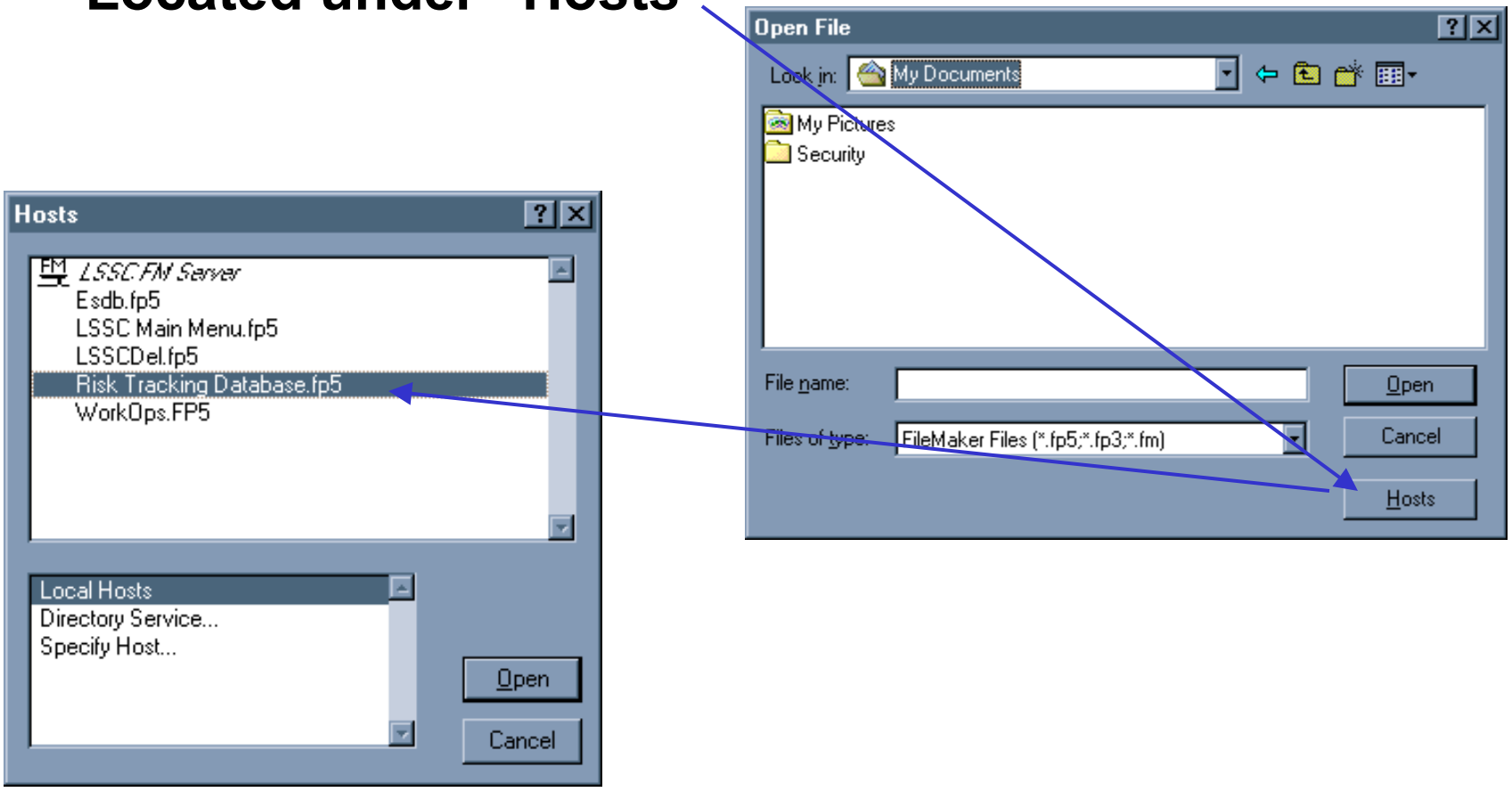
- The responsibility for entering and updating data for a given risk is given to the assignee.
- This is a cognizant team member with good knowledge of the risk area.
- He/She is responsible for entering the data as well as updating the risk status for quarterly reviews and design reviews.
- The entire team is required to assist in developing any information needed as well as creating corrective action plans.

Retired Risks

- A short justification for retiring risks will be generated before the risk is formally closed.
- Whenever practical a “lesson learned” will be generated in order to prevent recurrence in future projects.
- When risks are ready for formal closure they will be reviewed by the flight experiments manager and the NASA project manager.
- The flight experiments manager has final authority to close project risks whose RPN is 1 or less.

Risk Tracking Database

- **Filemaker Pro Database for capturing risk data**
- **Located under “Hosts”**



Risk Tracking Database

- **Risk Information Sheet**

Serial Number Automatic

Serial Number Automatic

Project Data

Priority

Risk Short Title

Risk Statement

LSSC Risk Management

RISK INFORMATION SHEET

ID # 1			**Date Identified:** 03/11/2002
Project EXAMPLE	**Project Segment** Hardware Subsystem Dev	**Segment Title** Thermal Control	
Priority 3	**Risk Title** TEC Failure		

Initial Risk Values

Probability of Occurance	.01
Magnitude of Impact	6
Probability of Detection	0
Initial Risk Priority Num	6
Timeframe	Near Term

Risk Statement: Condition ; Consequences

TEC failes in open circuit condition; loss of cooling for one PGC, possible loss of science. total failure of people to get the point of all of the important things in life

Originator **Assigned To** Roberteen McCray

Classification ☐ **Safety** ☐ **Cost** ☐ **Schedule** ☒ **Science** ☒ **Performance** ☐ **Other**

Context TEC's are used to provide cooling and humidity control for the plant growth chambers. The actual failure rate has not been determined but it is believed to be low.

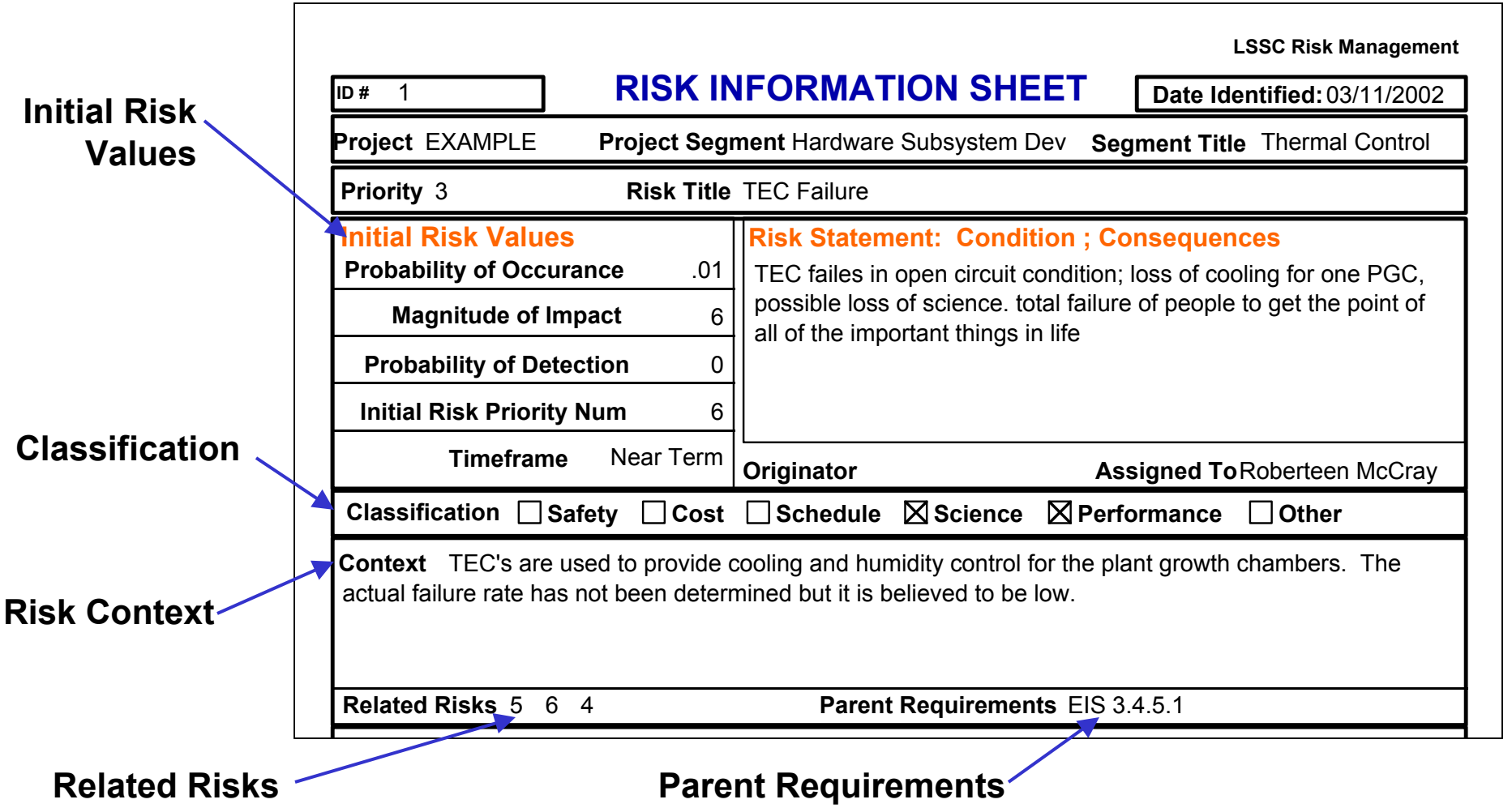
Related Risks 5 6 4 **Parent Requirements** EIS 3.4.5.1

Risk Tracking Database

- Serial Number - Automatically entered with each new risk. Method for tracking each risk.
- Identification date - date risk was initially documented, Can use right click menu, insert, today's date
- Project Data - Project title, level or segment to which risk applies, segment title (if applicable)
- Priority - Not RPN, assigned manually, determined by either RPN or Multi-voting procedure
- Risk Title - Short Unique descriptive phrase related to failure/condition, used in most summary tables.
- Risk Statement- Full risk statement including single condition ";" possible consequences

Risk Tracking Database

- **Risk Information Sheet**



Risk Tracking Database

- Initial Risk Values - Values at the time of identification assuming current project conditions
  - Probability of Occurance - 0 - 1 probability of negative condition/event
  - Magnitude of Impact - 1 - 10 value of
- Identification date - date risk was initially documented, Can use right click menu, insert, today's date
- Project Data - Project title, level or segment to which risk applies, segment title (if applicable)
- Priority - Not RPN, assigned manually, determined by either RPN or Multi-voting procedure
- Risk Title - Short Unique descriptive phrase related to failure/condition, used in most summary tables.
- Risk Statement- Full risk statement including single

Standard Risk Tools

- Fault Tree Analysis
  - Used to predict probable failure modes for the project or identify probable causes of failure after occurrence.
- Risk Brainstorming
  - Method for using all team resources to determine risk
- Risk Identification Sheet
  - Used to define a given risk, and critical data used in later analysis as well as historical background
- Preliminary Failure Analysis
  - Used to compare and summarize risks

Standard Risk Tools

- Risk Tracking Table
  - Used to summarize key risks and status of correction plans
- Failure Mode and Effects Analysis
  - Used to accurately predict reliability of system and impact of various failures
- Reliability Budget
  - Used in complex systems to allocate Reliability requirements to subsystems or components.
- Materials List
  - For Safety review, Flammability, Odor, Off gassing risks

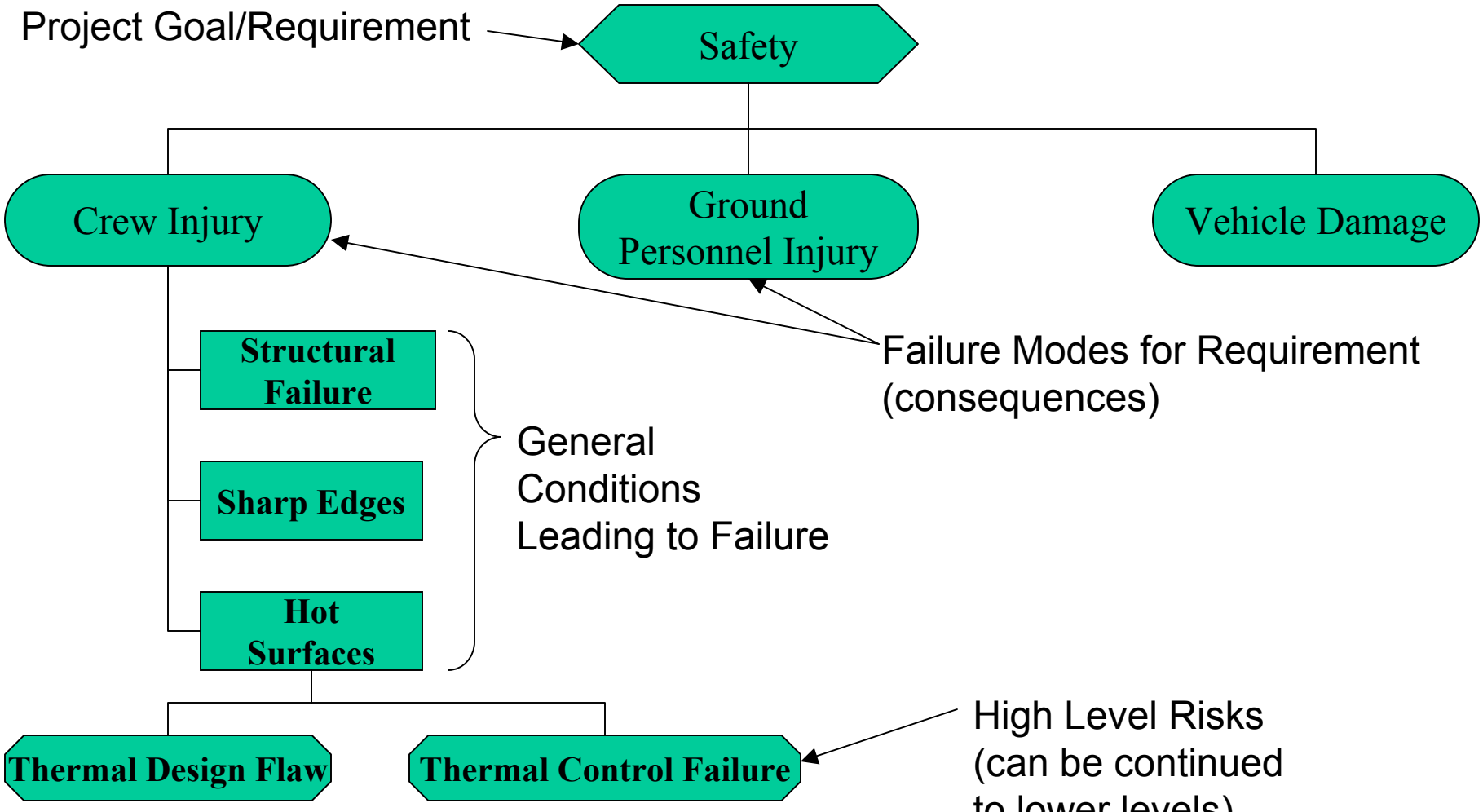
Standard Risk Tools

- **Critical Components List/Single Point Failure List**
  - **Identifies components whose failure would result in a significant impact to project**
  - **Identifies special handling, screening and testing used to detect flaws and prevent additional defects**

Initial Fault Tree Analysis

- Used to predict root causes of critical project failures and generate a list of risks to be addressed
- Takes key requirements based on mission statement and identifies probable failure modes which impact each requirement
- Taken to the appropriate level where PO, PD, MF can be properly estimated and where corrective actions can be generated which address failure modes.

Initial Fault Tree Analysis Example



Risk Brainstorming

- **Simple brainstorming process used throughout project to identify likely failure modes**

Risk Identification Sheet

- Provides detailed data on each risk to justify RPN's and for future reference
- Captures context and historical data
- Captures top level details of corrective action plan

LSSC Risk Management

RISK INFORMATION SHEET

ID # 2 | **Date Identified:** 03/11/2002

Project TAGES-2SD | **Project Segment** Project Management | **Segment Title** Schedule

Priority 1 | **Risk Title** Project Staffing

Initial Risk Values

Probability of Occurance	.2
Magnitude of Impact	5
Probability of Detection	.60
Initial Risk Priority Num	40
Timeframe	Near Term

Risk Statement: Condition ; Consequences

Limmited staffing for hardware development; may result in slippage of schedule or reduced qualitysdalasjd

Originator Mark Kelsch | **Assigned To** Mark Kelsch

Classification ☐ Safety ☐ Cost ☒ Schedule ☐ Science ☒ Performance ☐ Other

Context The thermal control system redesign for the PGF-SP will take significantly more resources than previously expected. Staff is extremely lean and other project demands are threatening to reduce the available resources even more

Related Risks 1 | **Parent Requirements** N/A

Mitigation Approach **Careful planning, Hiring additional personnel, deffer efforts**

Money is currently budgeted for two new engineers. Careful project planning will identify the critical need areas and justify additional expense. Some engineering efforts associated with ISS compliance will be postponed until additional resources become available.

Contingency Plan

Detection Trigger Greater than 5 days of schedule slip per month | **Trigger Status** 2

Predicted Level of Risk After Mitigation

Probability of Occurance .02	Probability of Detection .9
Magnitude of Impact 4	Predicted RPN .8

Risk Retired After Project Completion

Status Currently replanning schedule | **Status Date** 03/12/2002

Creating new project baseline for planning and tracking purposes.

Closing Rationale

Lesson Learned

Approval | **Closing Date**

Preliminary Failure Analysis

- **Used to summarize, communicate and prioritize Risks.**
- **Used at key design reviews and during project planning**
- **May be used in subsystem analysis**

Project Title								Project Segment:											
Project Engineer												Date							
	Consequences						Risk (uncorrected/unmitigated)							Risk (After Mitigation)					
Potential System Failures	Budget	Schedule	Deliverables	HW Performance	Safety	Others	Prob. Of Failure	Prob. Of Detection	Magnitude	RPN	Failure Prob. Index	Severity Category	Corrective Action/ Mitigation	Prob. Of Failure	Prob. Of Detection	Magnitude	RPN	Failure Prob. Index	Severity Category
Thing breaks	X	X		X			0.1%	10.0%	10	0.9	E	I	Increase Margins	0.1%	10.0%	10	0.9	E	IV

Risk Tracking Table

- **Tool for status of risks during quarterly reviews**

Project Segment:	Fluids Subsystem		Date:	10/05/2001
Risk	RPN	Corrective Action	Status	Scheduled Retirement
Cooling Pump Fails	70	Add redundant pump	Models generated	11/01/01 Drawings completed

Failure Mode and Effects Analysis

- Analysis tool used to accurately predict system reliability and failure impacts
- Can be used at a system or subsystem level
- May be started after PDR to aid in design development
- Used at critical design review and for safety package development

Project Requirements

- Risk identification and evaluation will follow the guidelines and procedures laid out in this document.
- New risks will be reviewed at each regular project team meeting.
- Risks will be updated at least once a month and will be summarized for quarterly reviews.
- All risks will be reviewed once a quarter to verify that corrective action plans are in place.

Summary

- Risk management is a planning and tracking tool.
- Risk management will be carried out early and often.
- Corrective action plans will be incorporated into normal project documents to insure that it is properly executed.
- Corrective action plans will be tracked for effectiveness.
- A risk database is available to capture and track risks.
- Standard risk tools may be used to identify and evaluate risks.