S&K GLOBAL SOLUTIONS

A Salish & Kootenai Tribally Owned Business • SBA 8(a) Certified

Integrating Fault Management Planning Tools with System Engineering: Fault Management Viewer (FMV)

AIAA-HSI ATS 2017

Carroll Thronesbery, Pamela Fournier, Timothy Olson, Eugene McMahon, Mike Monahan

Agenda

- Project Description
- Fault Management (FM) Evaluation Questions
- Displays to Address Those Questions
- Innovations
- Next Steps

Fault Management Viewer (FMV): Human Centered View

- A tool to help system engineers plan fault management for new systems
- People tasks:
  - Build a model of fault management (FM) concepts
  - Refine the model
  - Address a number of analysis questions important to effective fault management planning and design

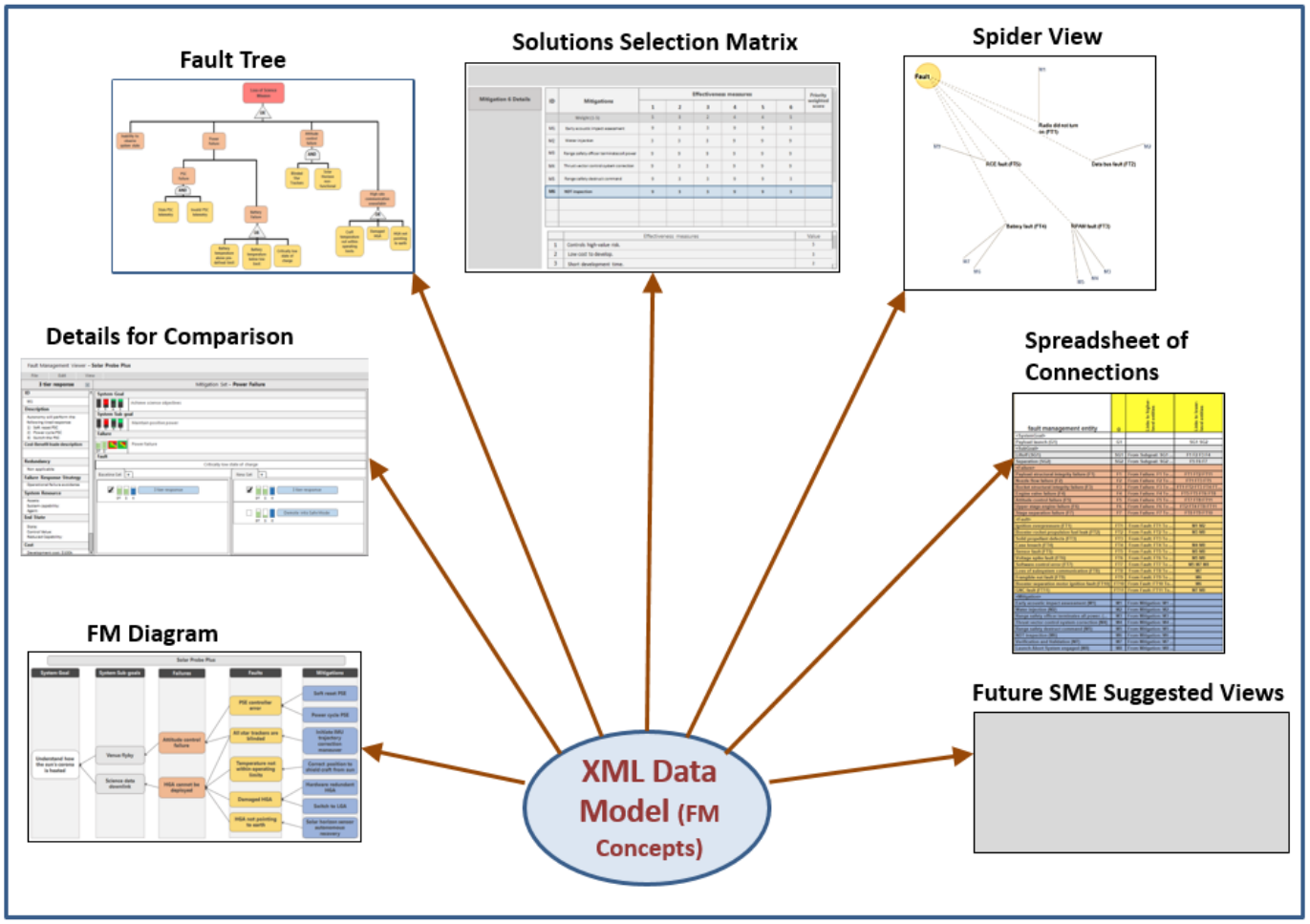
Fault Management Viewer (FMV) project: System View

- Identify a design reference mission
- Design an XML schema
- Design information displays
- Explore effectiveness measures and automation options
- Develop a concept of operations
- Build a feasibility prototype
- Write the final report

Project Description

- SBIR Phase I project – June-December 2016
- Fault Management Concepts
- NASA FM Handbook (2012) – concepts & processes
- Fault Management Viewer
  - Makes FM Handbook easier to follow and implement
  - One data model, multiple views
  - Edit any view, see changes to all views
  - Each view supports unique set of evaluation questions
- Design Reference Mission
  - Based on launch vehicles (SLS) and deep space (Solar Probe Plus)
  - Evaluation questions to guide the development of views

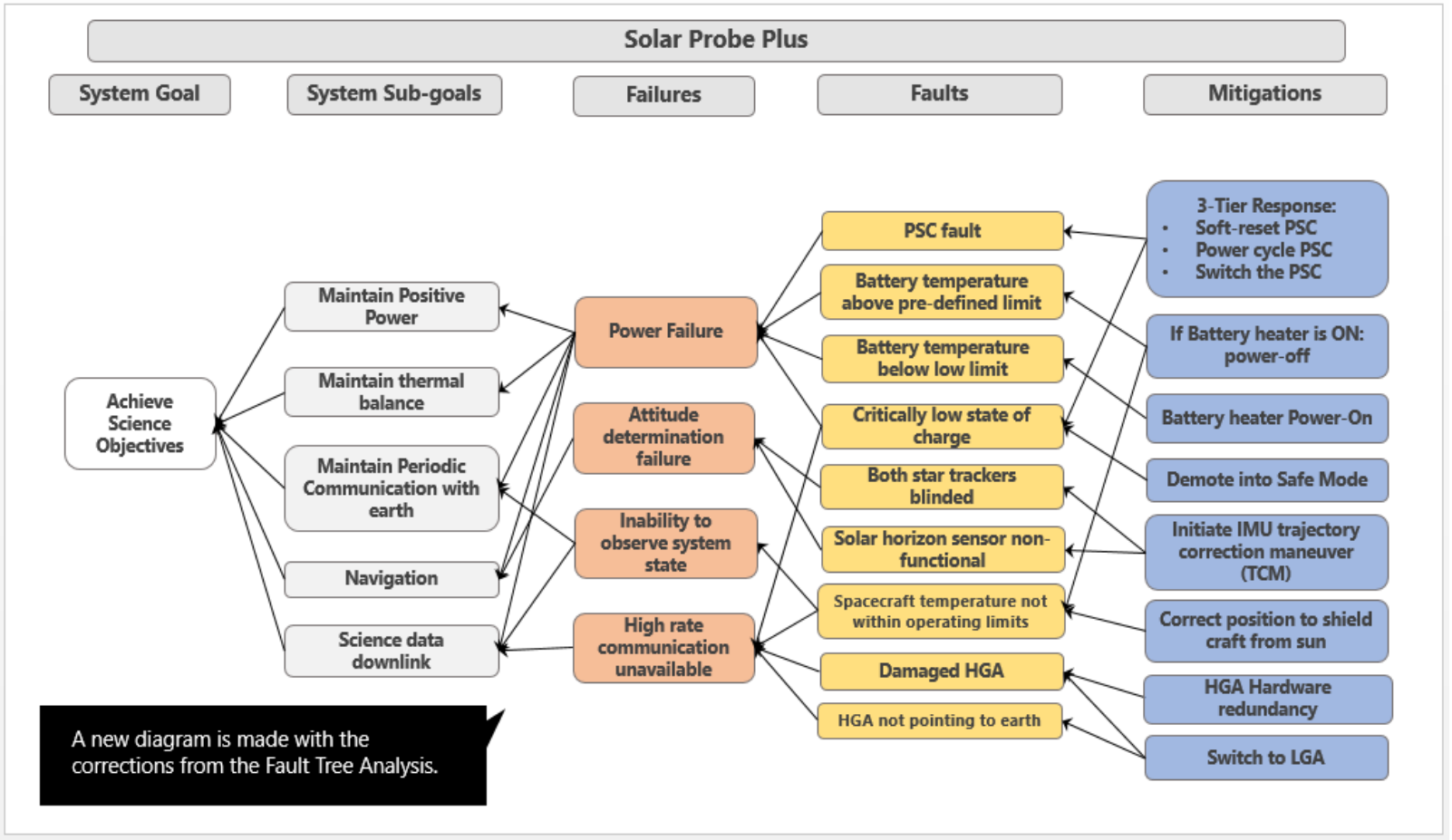
Multiple Views, One Data Model



Supported Fault Management Tasks

- Build a model of FM concepts
- Refine FM concepts to support better decisions
- Address Fault Management analysis questions
  - What are primary system goals?
  - How well am I protecting the system against this failure?
  - Which of these mitigation sets is most effective?
  - Where can I spend my FM development resources most effectively?
  - How much resource would be required to bolster the protection?
  - How much would my risk profile be improved if we add this set of FM mitigations?
  - How much would my system function improve in dependability if we add this FM measure?

Fault Management Diagram



Build a Model of FM Concepts

System Goal | System Sub-goals | Failures

Building a Fault Management diagram begins with identifying the main purpose of the system to be analyzed.

Understand how the sun's corona is heated

That is, if it is a launch vehicle meant to deliver cargo, a crew or manned vehicle, or a probe meant for gathering science data. Said purpose is going to guide what is entered as a System Goal in the diagram.

In this example, the system to be analyzed is the Solar Probe Plus. Consequently, the System Goal is going to be the completion of its Science Objectives.

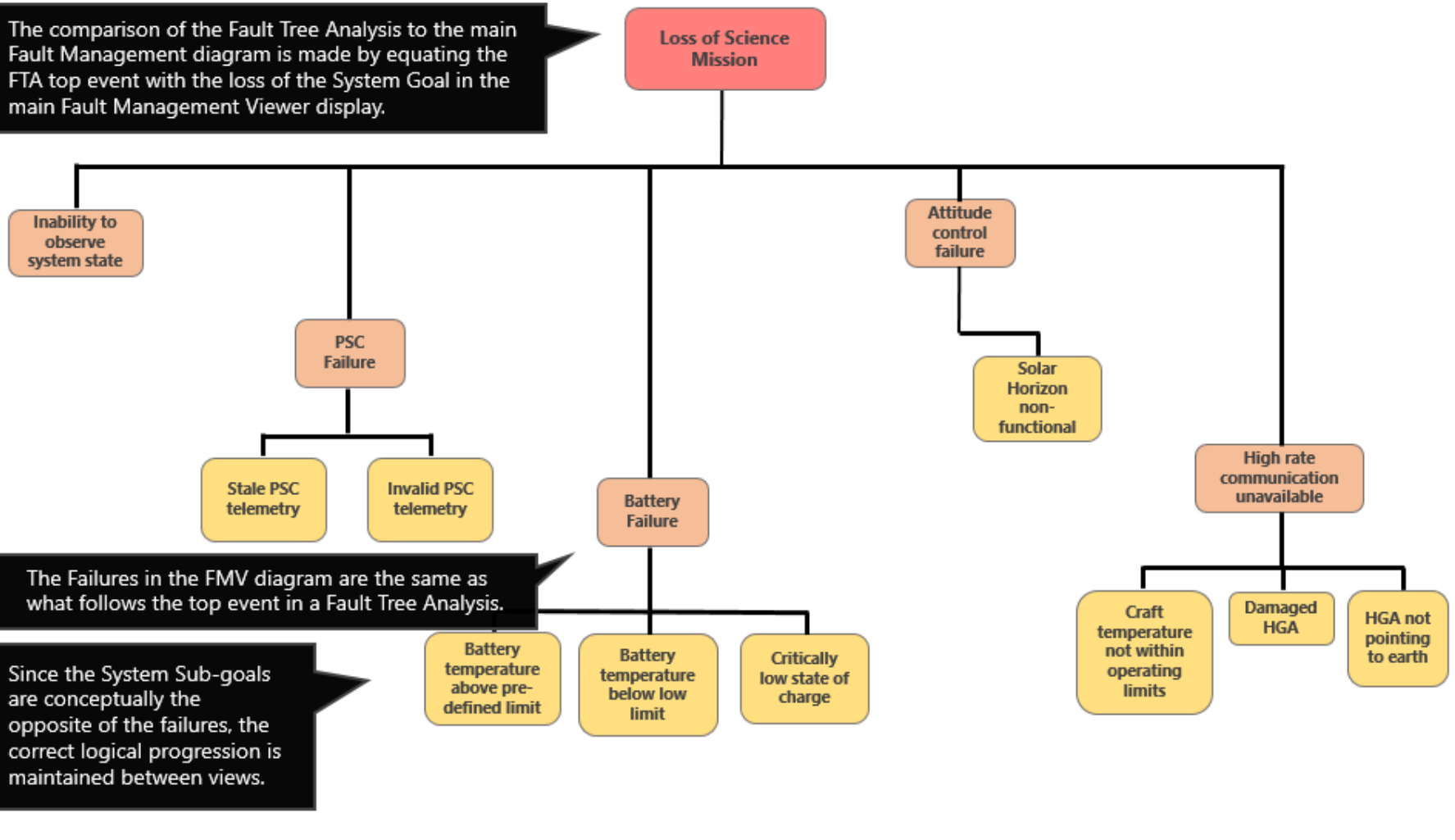
Next, add :

- Sub-goals
- Failures
- Faults
- Mitigations

Next, add details of each concept

Refine Concepts w/ SMEs, More Views

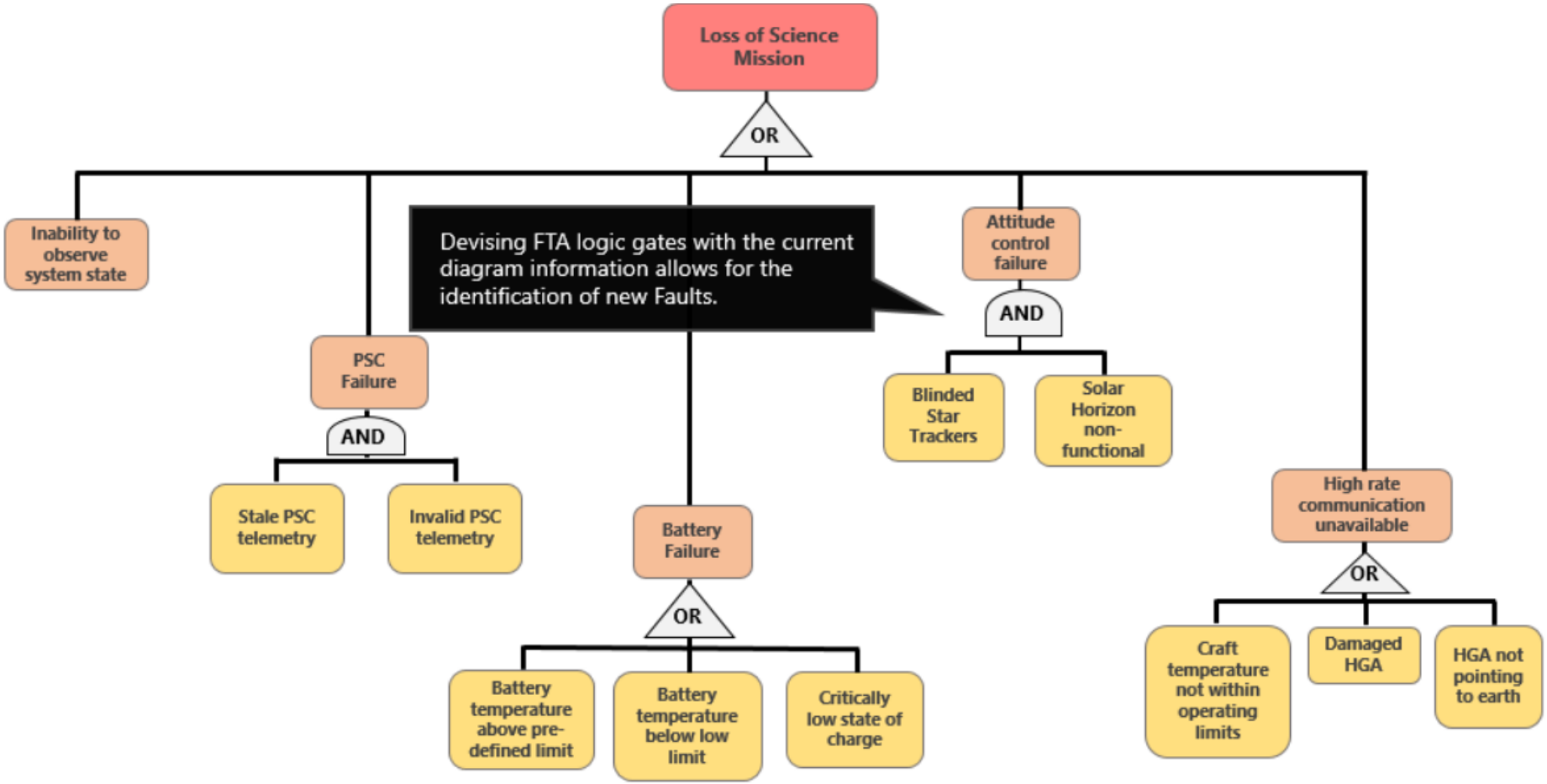
The comparison of the Fault Tree Analysis to the main Fault Management diagram is made by equating the FTA top event with the loss of the System Goal in the main Fault Management Viewer display.



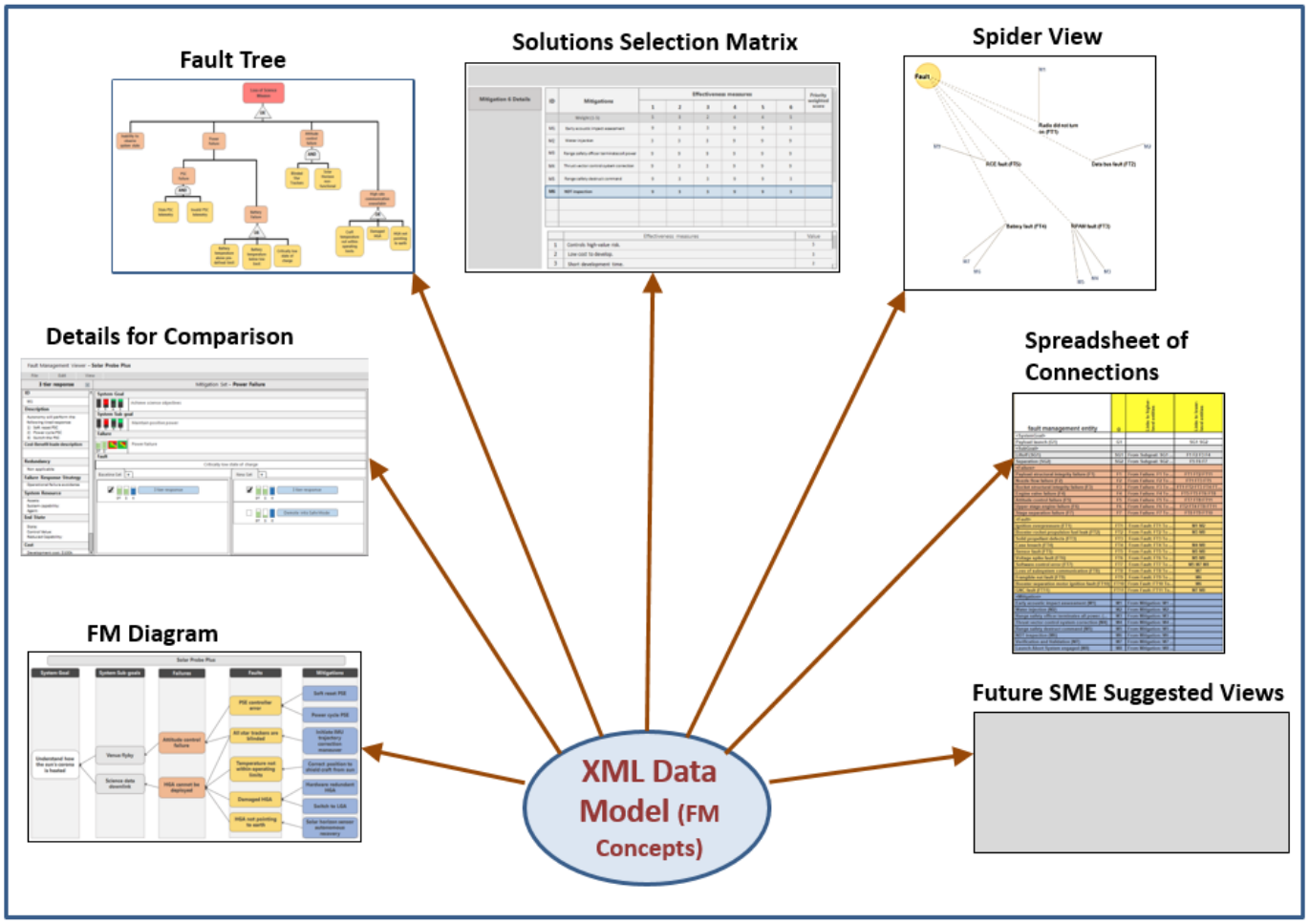
The Failures in the FMV diagram are the same as what follows the top event in a Fault Tree Analysis.

Since the System Sub-goals are conceptually the opposite of the failures, the correct logical progression is maintained between views.

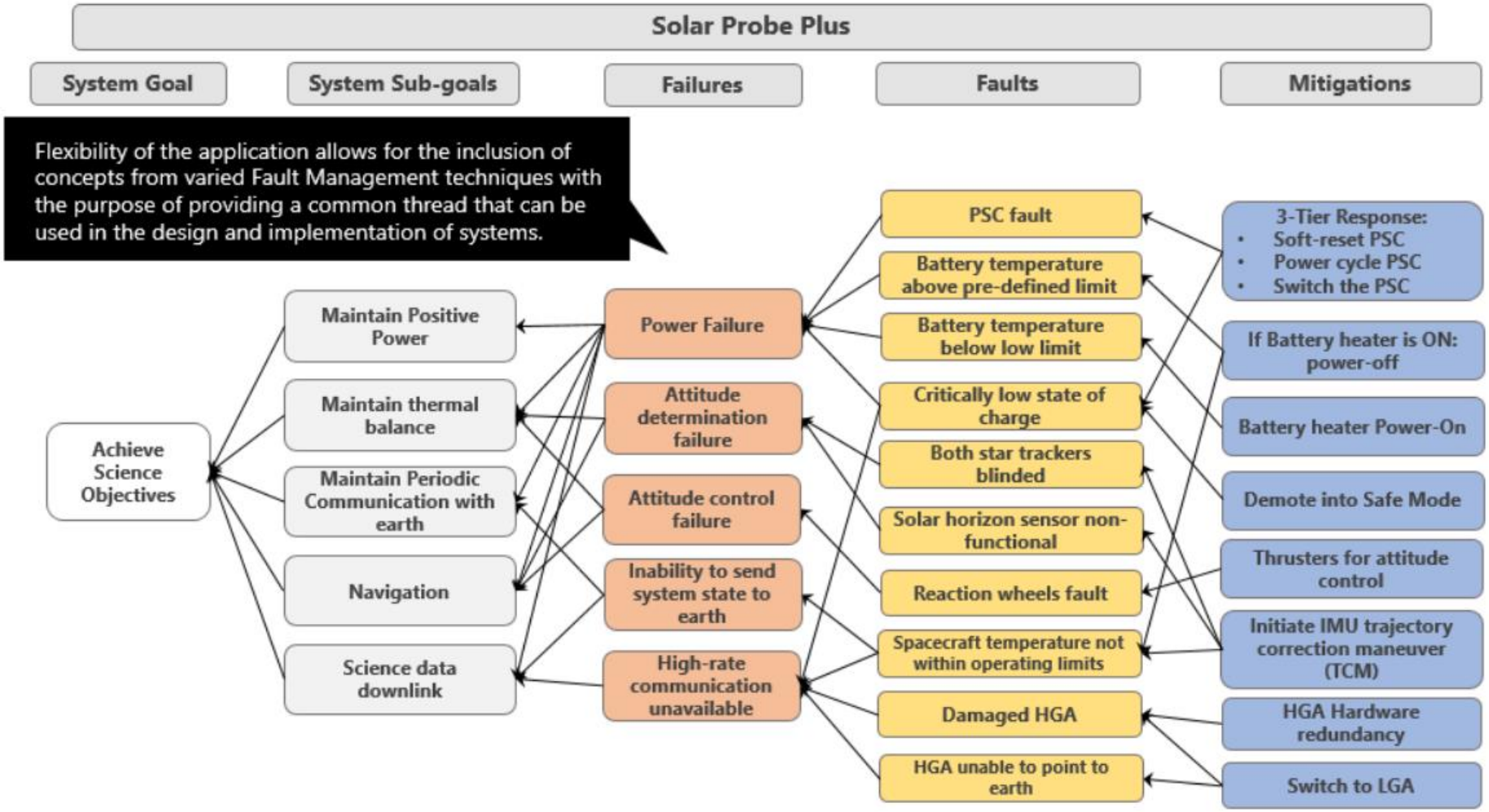
Add Info expected by fault tree



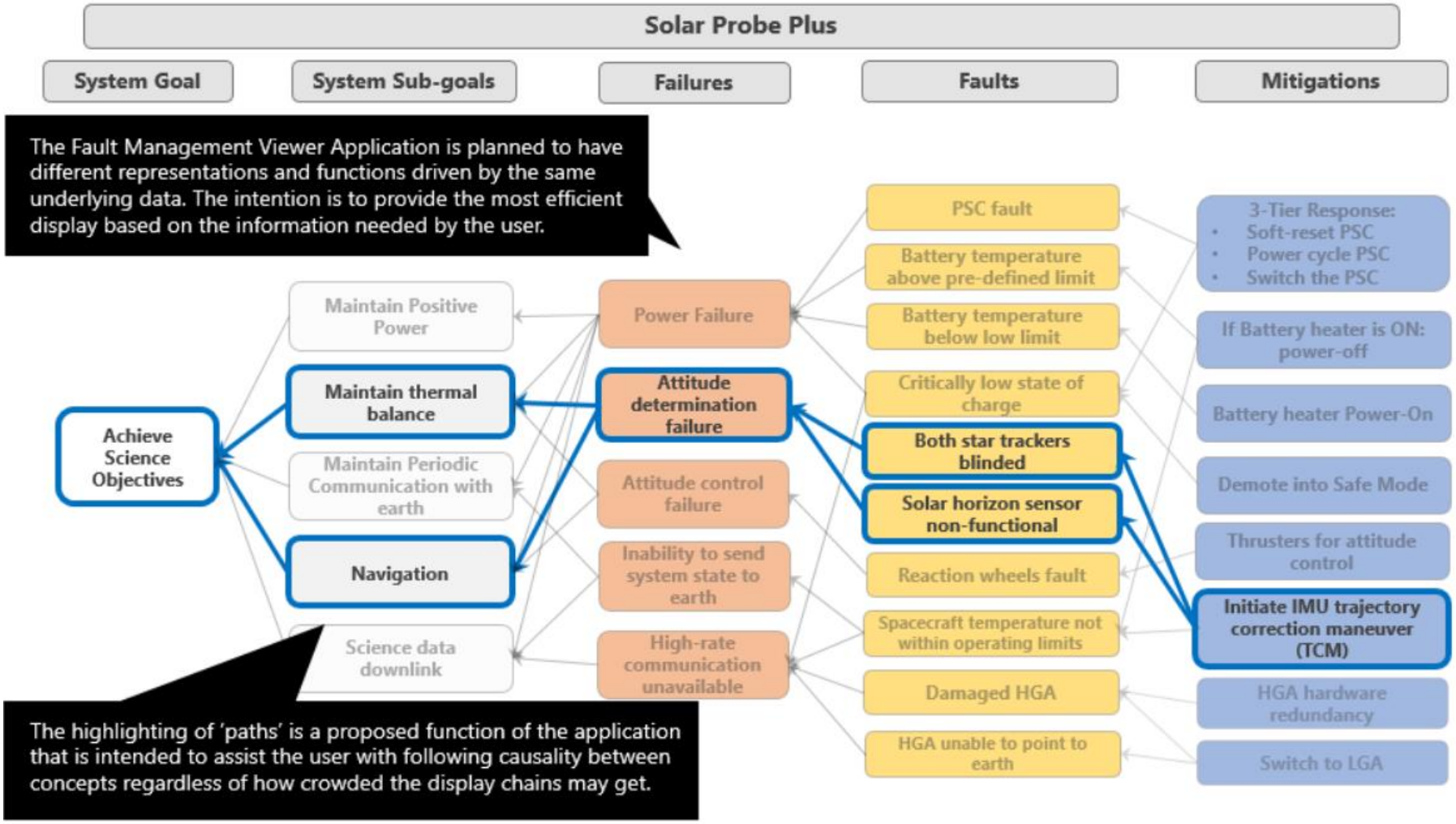
More Refinements w/ Each Data View



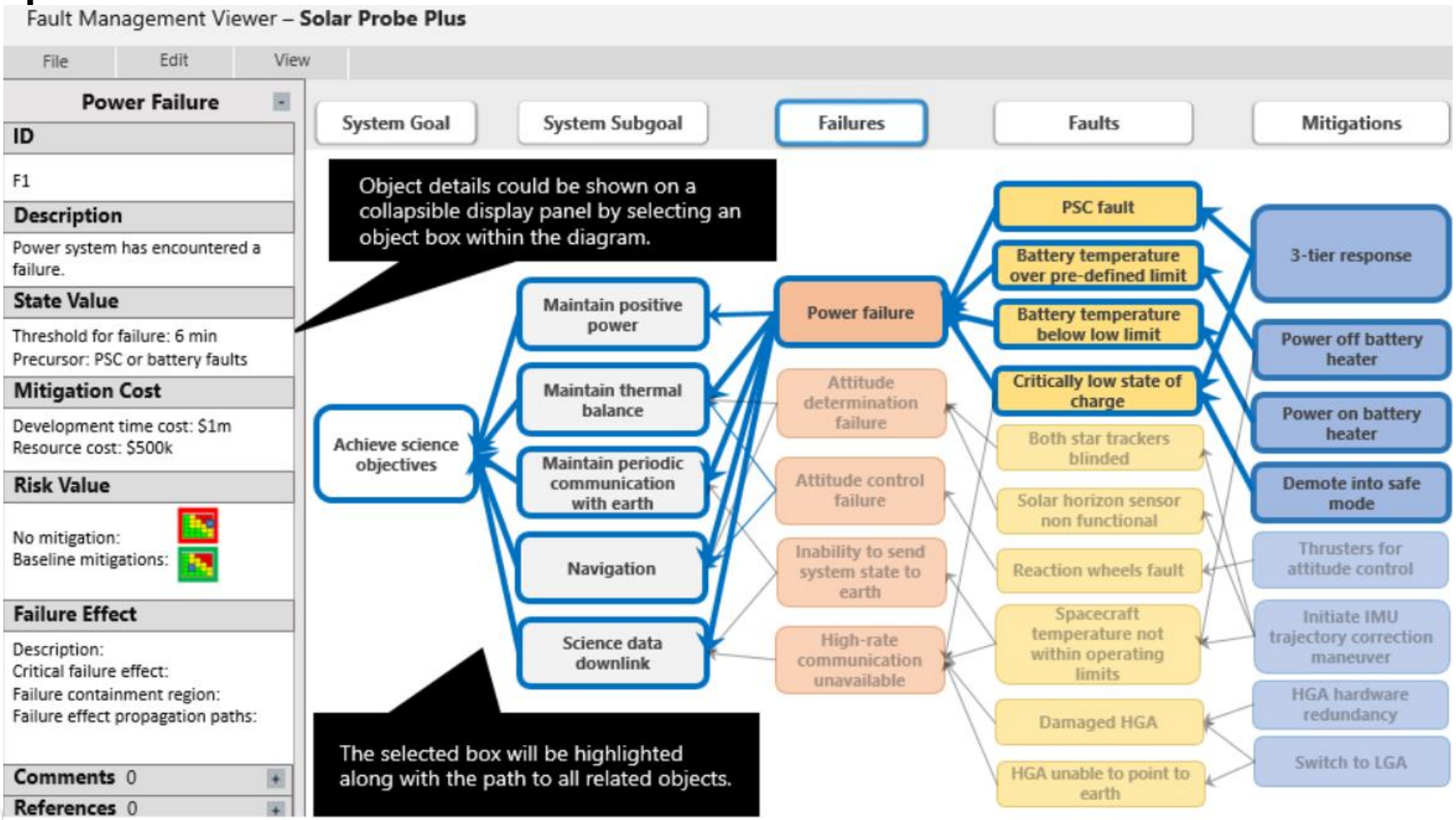
What are primary system goals?



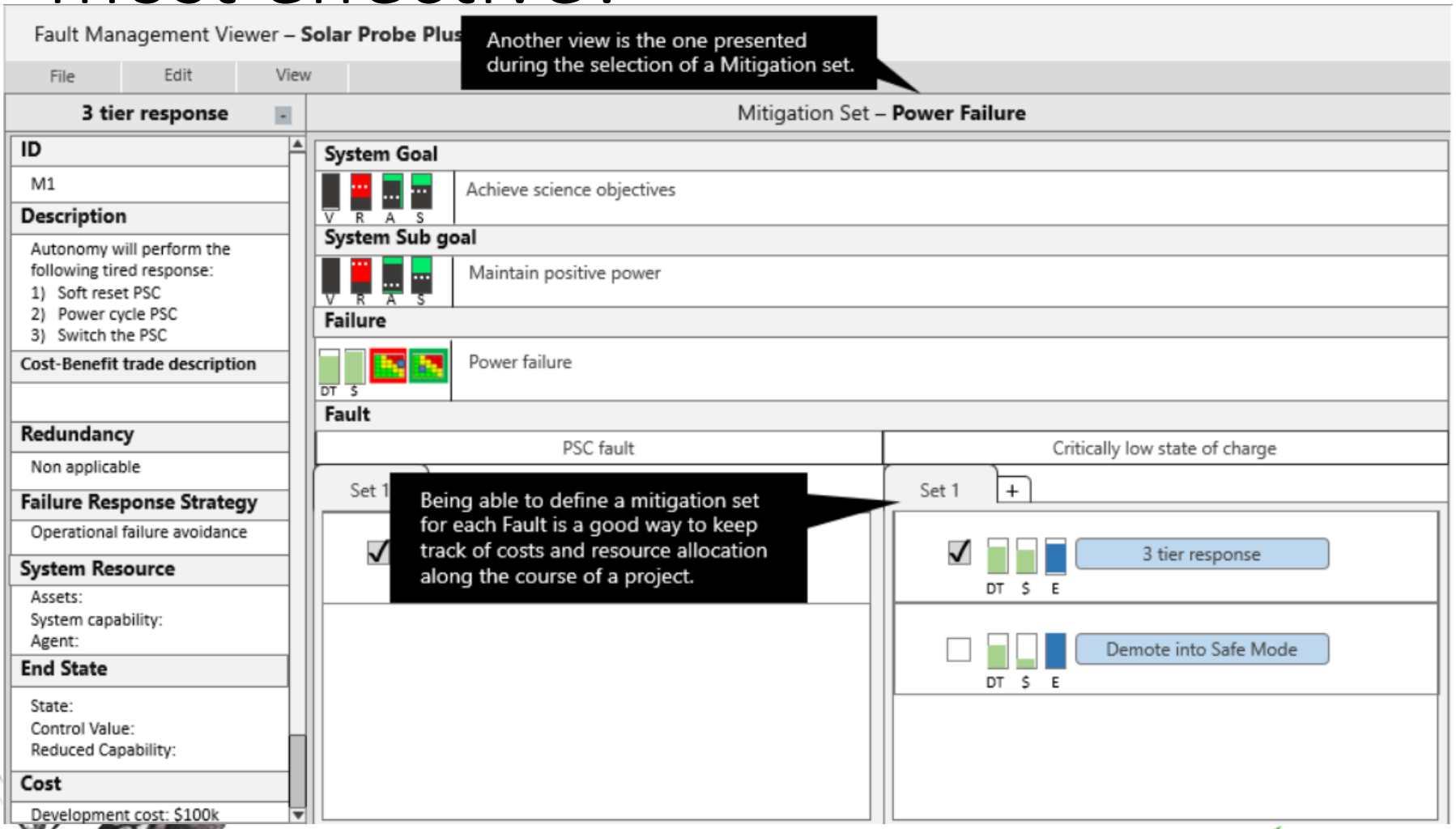
What goals are affected by attitude determination failure?



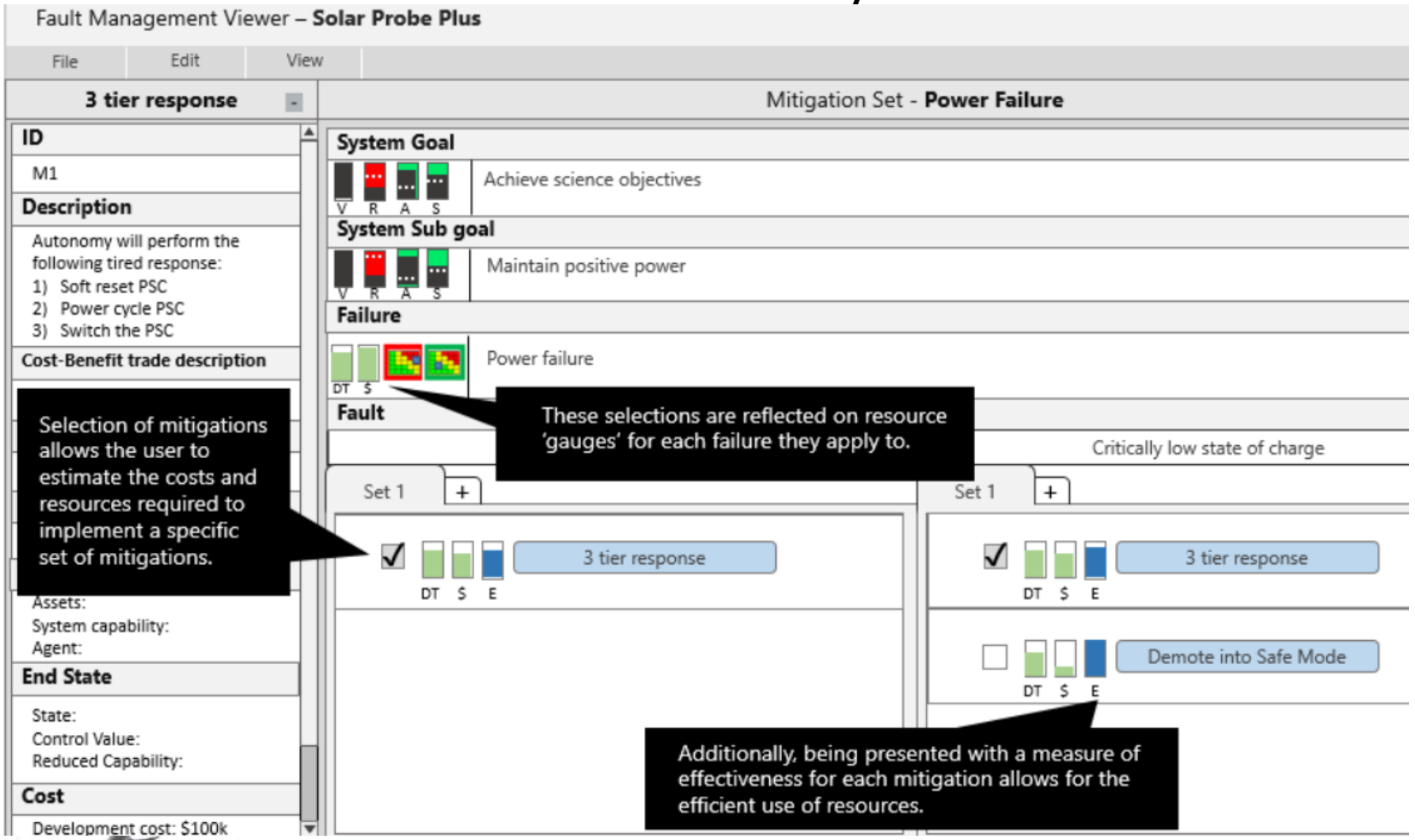
How well have I protected against power failure?



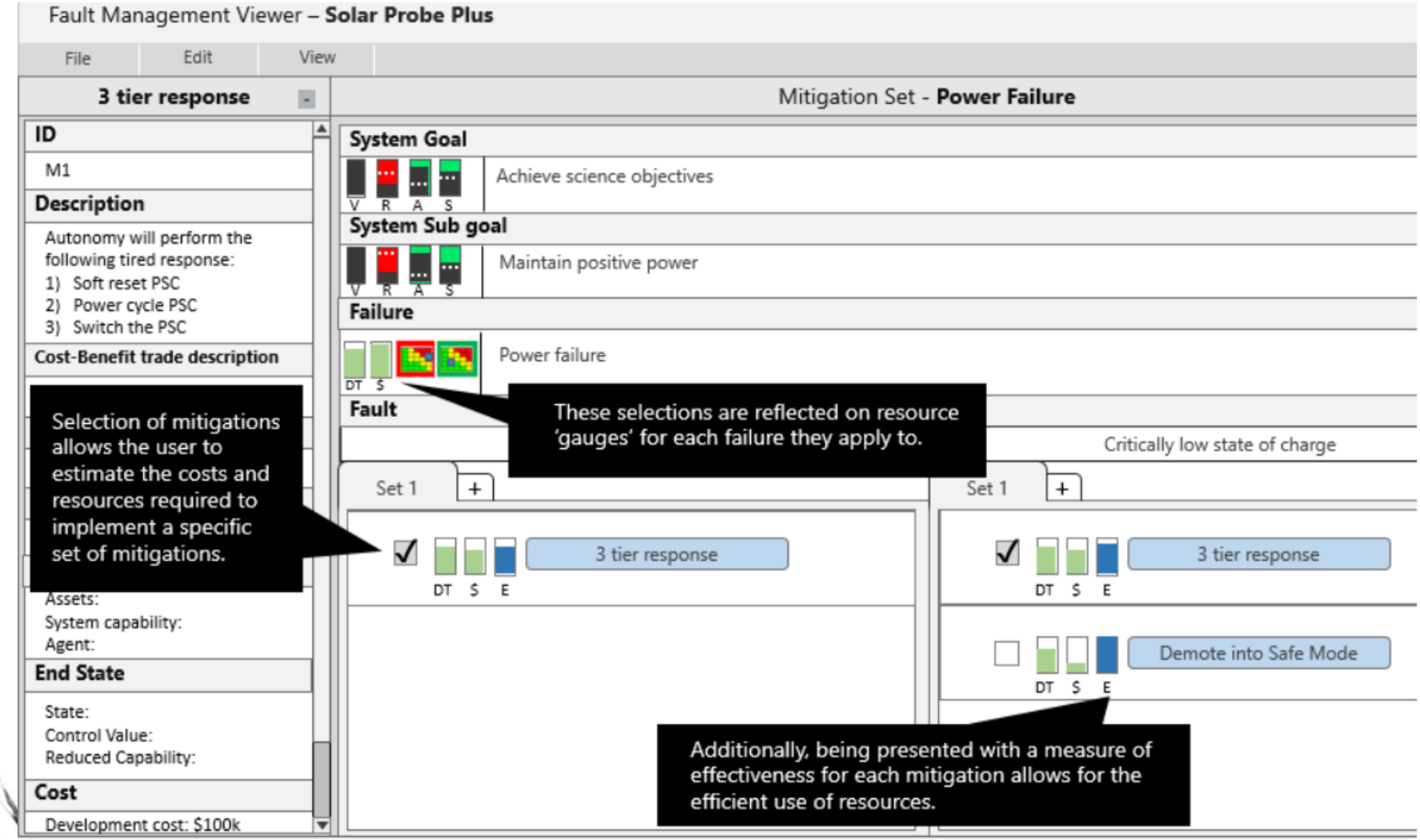
Which of these mitigation sets is most effective?



Where can I spend my FM development resources most effectively?



- How much resource would be required to bolster protection of this function?
- How much would my risk profile improve if we add this set of mitigations?
- How much would my system function improve in dependability if we added this FM measure?



Innovations

- A public XML data model of FM concepts based in
  - common diagram formats
  - NASA FM Handbook
  - One data model – multiple views
  - Edit one, see changes in all views
  - Each view is optimized for unique analysis of FM concepts
  - Better refinements, better support of analysis
- Key concepts for evaluating the inclusion of prospective fault management measures

Next Steps

- Agile approach – iterative development
- Phase I
  - Designed FMV
  - Developed ConOps
  - Created a feasibility prototype
- Next
  - Full-function, proof-of-principle prototype
  - Include SME improvements and expansions
  - Evaluate for refinement and commercial readiness