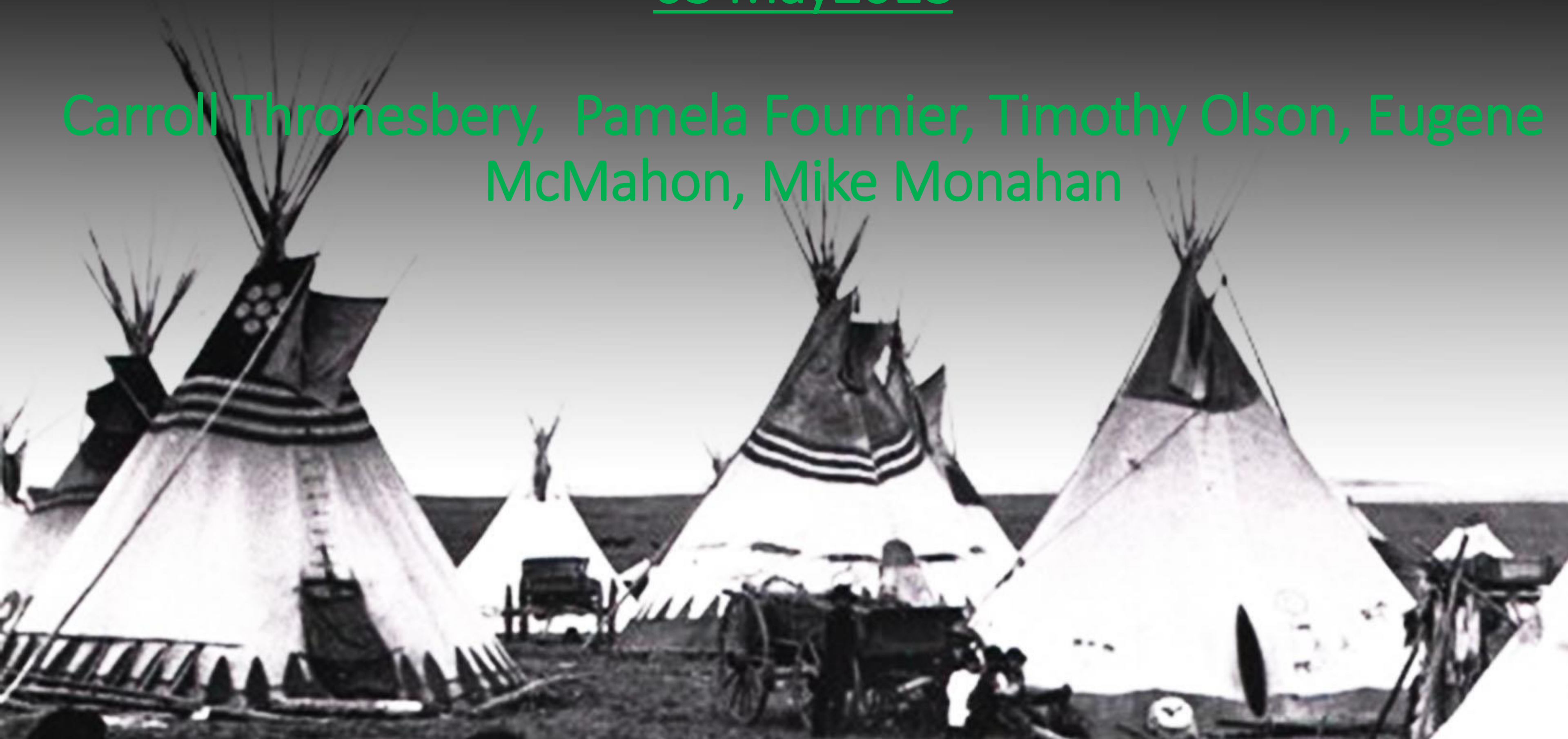
S&K GLOBAL SOLUTIONS

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

Visualizations to Support the Design of Fault Management

INCOSE Gulf Coast Chapter 2018
03 May2018

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



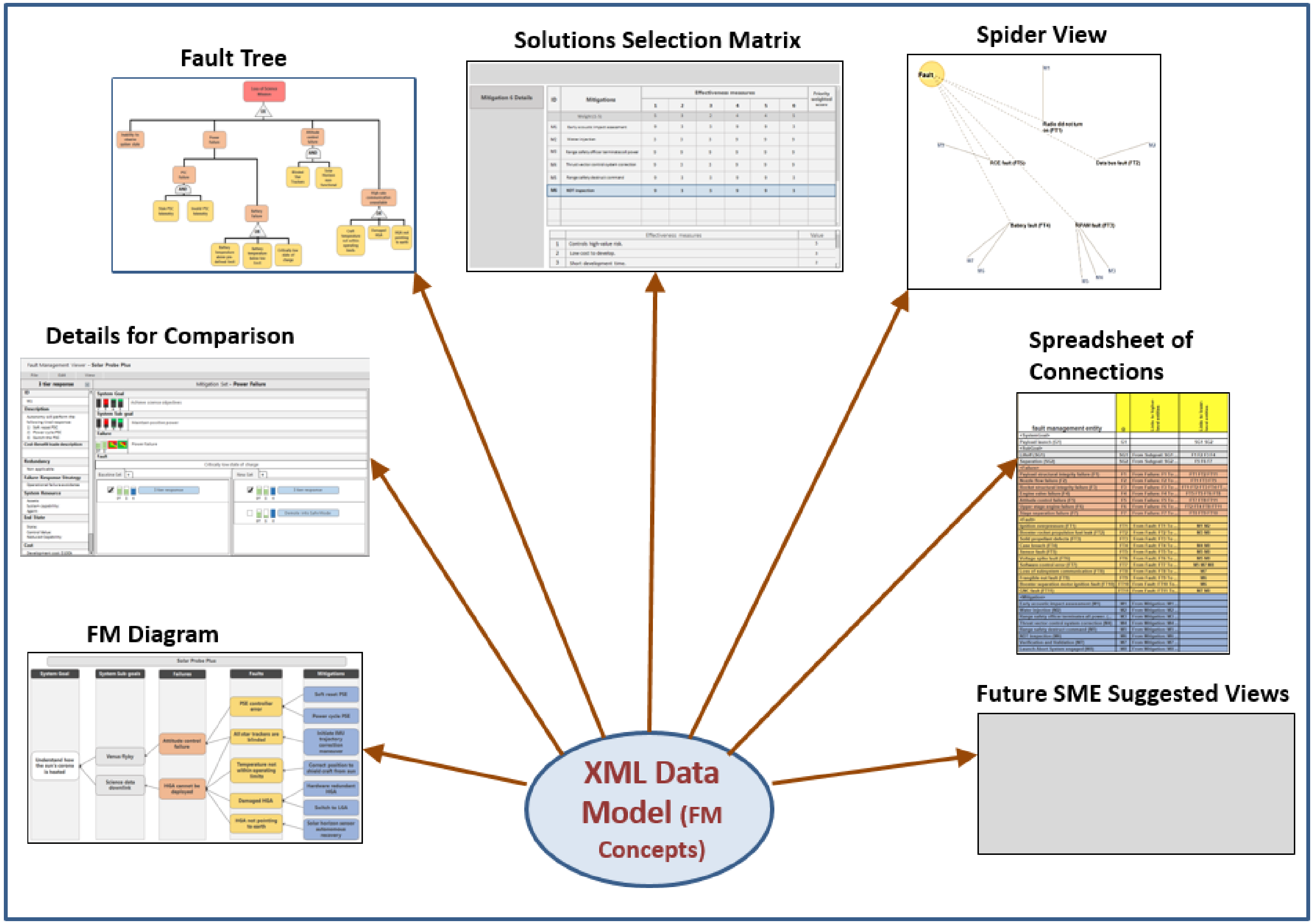
Fault Management Viewer (FMV)

- Project Description
- Fault Management (FM) Evaluation Questions
- Displays to Address Those Questions
- Extensions (Funding from State of Montana)
- Next Steps
- Suggestions? (opportunities, partnerships, references, places to expand, something overlooked)

Fault Management Viewer (FMV)

- A tool to help system engineers plan fault management for new systems
- People tasks supported:
  - 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

Multiple Views, One Data Model



Fault Tree

Solutions Selection Matrix

Spider View

Details for Comparison

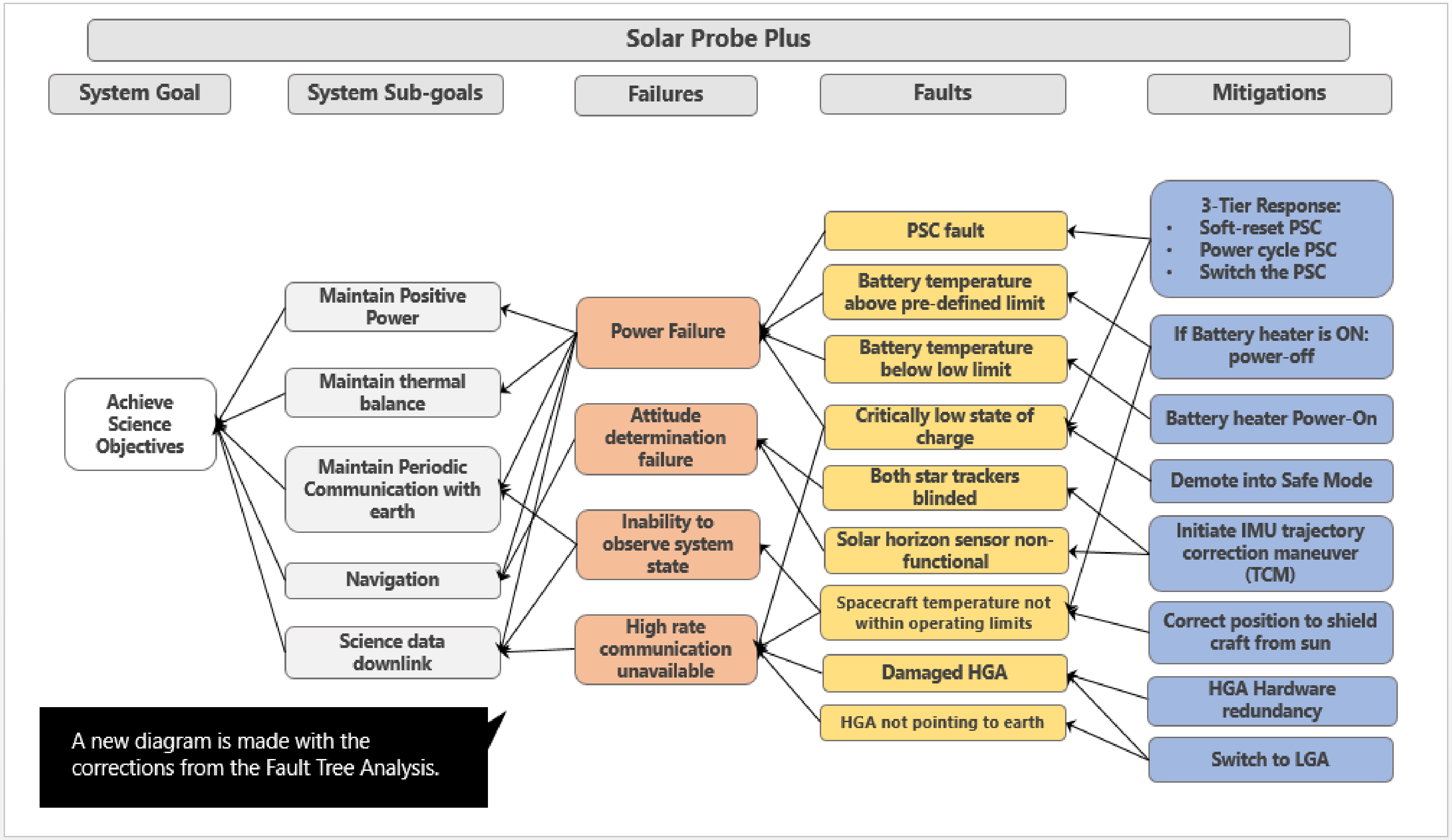
Spreadsheet of Connections

FM Diagram

Future SME Suggested Views

XML Data Model (FM Concepts)

Fault Management Diagram



Solar Probe Plus

System Goal

System Sub-goals

Failures

Faults

Mitigations

Achieve Science Objectives

Maintain Positive Power

Maintain thermal balance

Maintain Periodic Communication with earth

Navigation

Science data downlink

Power Failure

Attitude determination failure

Inability to observe system state

High rate communication unavailable

PSC fault

Battery temperature above pre-defined limit

Battery temperature below low limit

Critically low state of charge

Both star trackers blinded

Solar horizon sensor non-functional

Spacecraft temperature not within operating limits

Damaged HGA

HGA not pointing to earth

3-Tier Response:
- Soft-reset PSC
- Power cycle PSC
- Switch the PSC

If Battery heater is ON: power-off

Battery heater Power-On

Demote into Safe Mode

Initiate IMU trajectory correction maneuver (TCM)

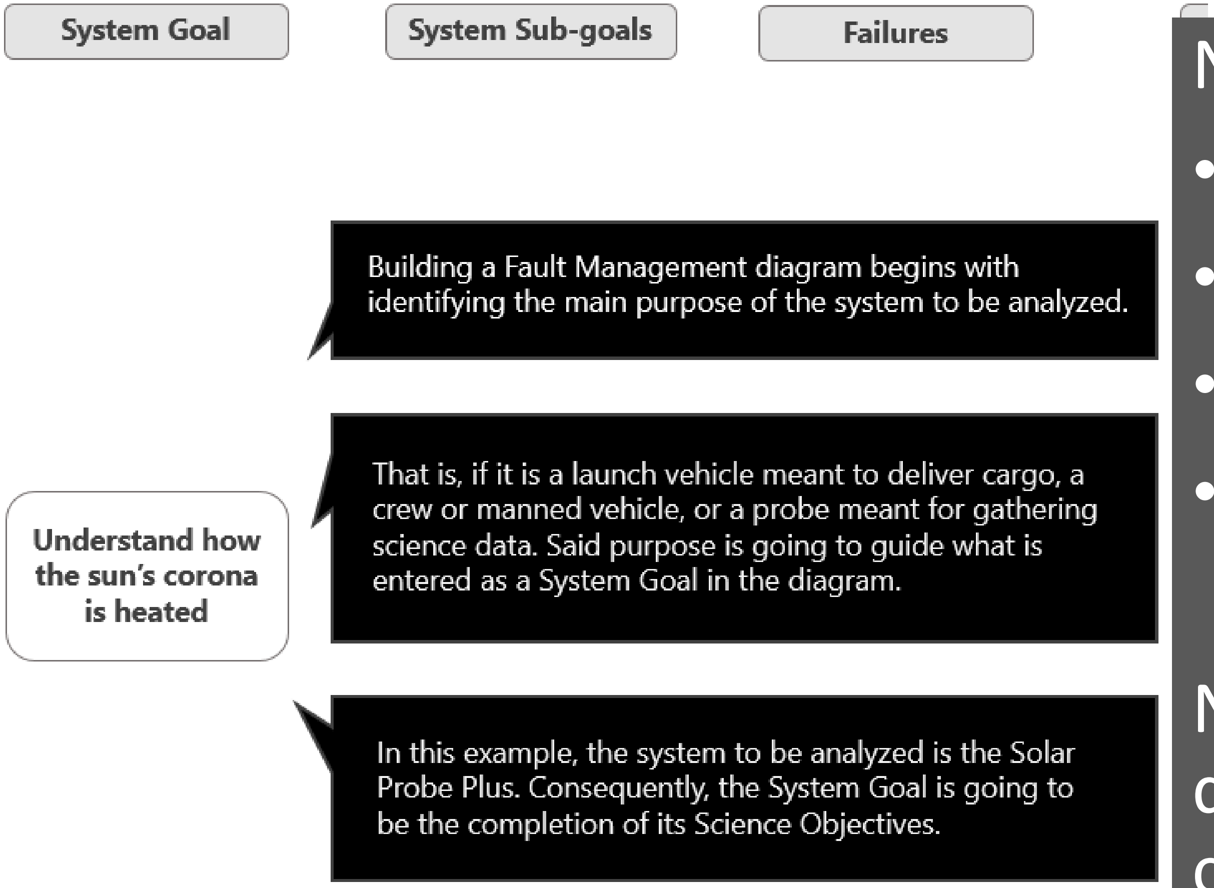
Correct position to shield craft from sun

HGA Hardware redundancy

Switch to LGA

A new diagram is made with the corrections from the Fault Tree Analysis.

Build a Model of FM Concepts



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

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.

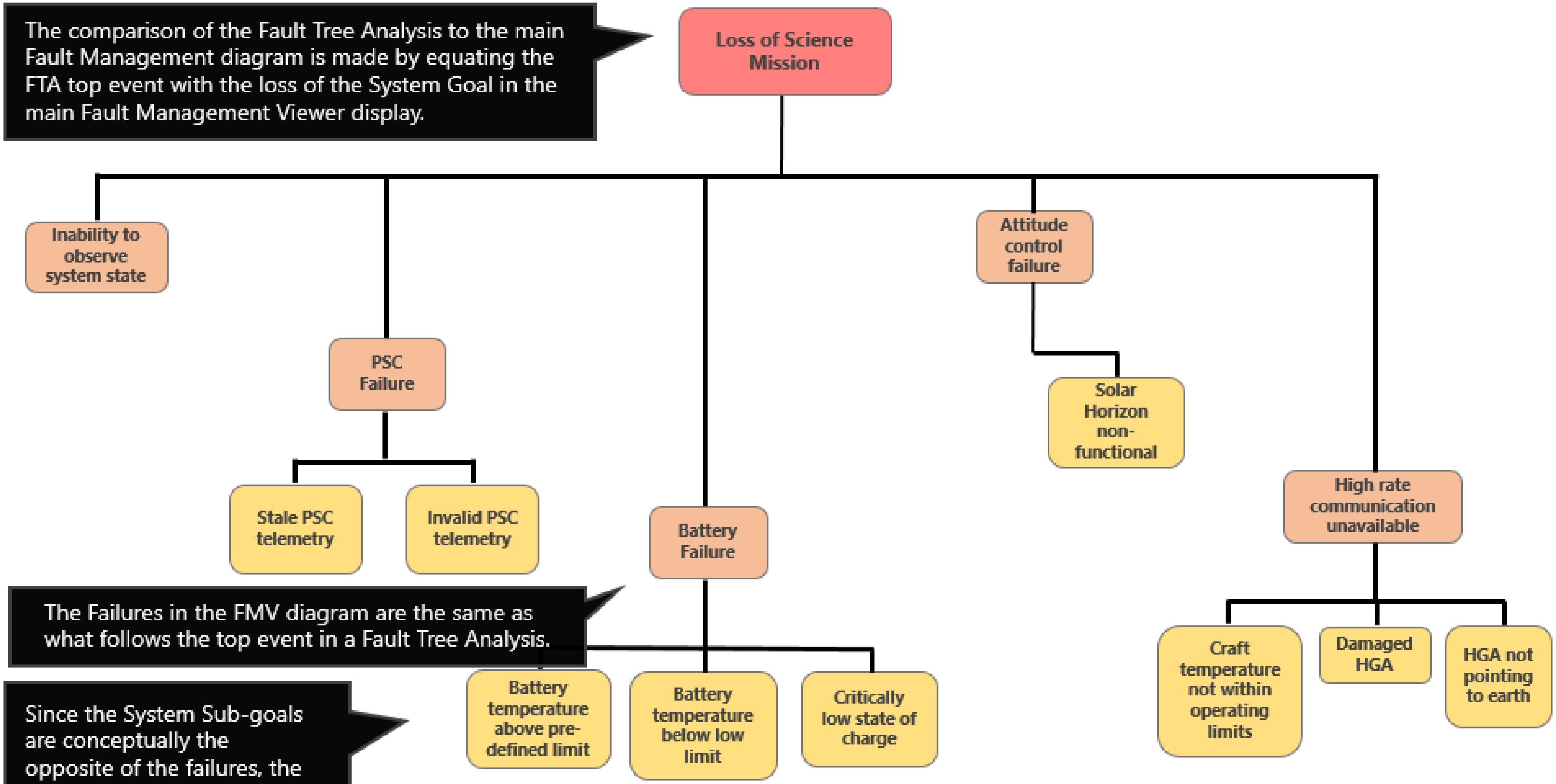
Next, add :

- 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.

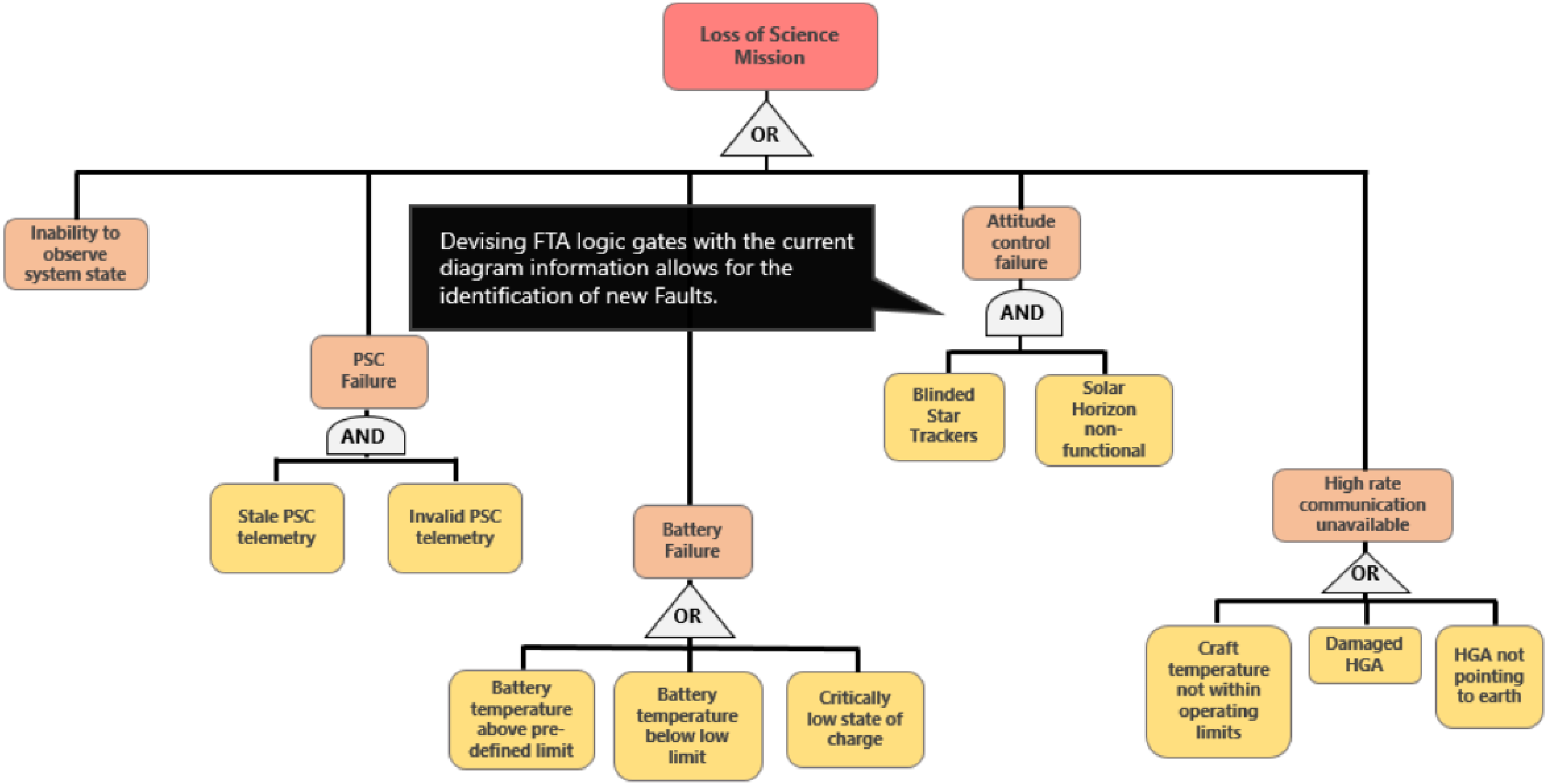


- Loss of Science Mission
  - Inability to observe system state
  - PSC Failure
    - Stale PSC telemetry
    - Invalid PSC telemetry
  - Battery Failure
    - Battery temperature above pre-defined limit
    - Battery temperature below low limit
    - Critically low state of charge
  - Attitude control failure
    - Solar Horizon non-functional
  - High rate communication unavailable
    - Craft temperature not within operating limits
    - Damaged HGA
    - HGA not pointing to earth

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

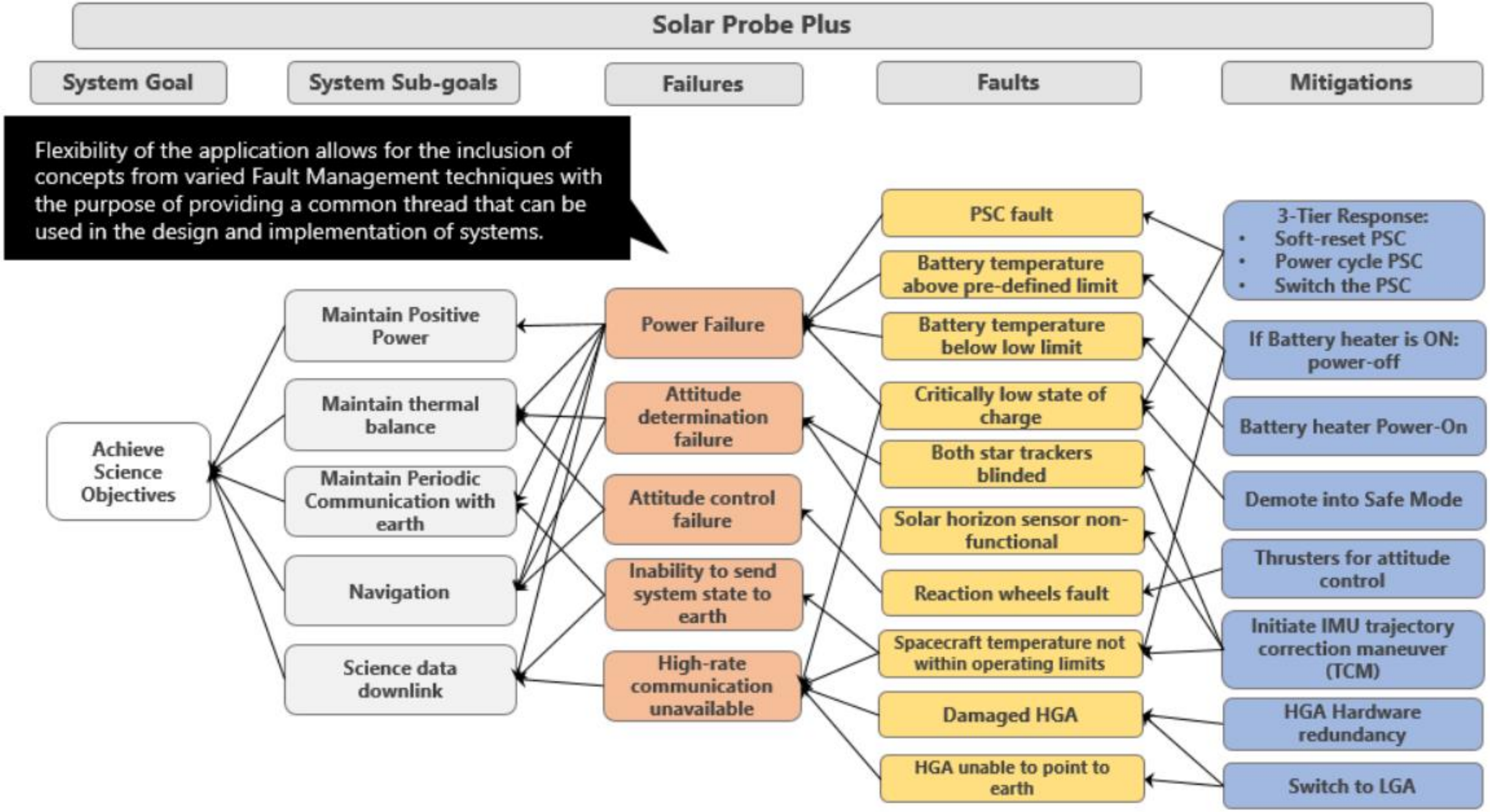

Loss of Science Mission
OR
Inability to observe system state
PSC Failure
AND
Stale PSC telemetry
Invalid PSC telemetry
Battery Failure
OR
Battery temperature above pre-defined limit
Battery temperature below low limit
Critically low state of charge
Attitude control failure
AND
Blinded Star Trackers
Solar Horizon non-functional
High rate communication unavailable
OR
Craft temperature not within operating limits
Damaged HGA
HGA not pointing to earth

Devising FTA logic gates with the current diagram information allows for the identification of new Faults.

FM Evaluation 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?

What are primary system goals?



Solar Probe Plus

System Goal

System Sub-goals

Failures

Faults

Mitigations

Flexibility of the application allows for the inclusion of concepts from varied Fault Management techniques with the purpose of providing a common thread that can be used in the design and implementation of systems.

Achieve Science Objectives

Maintain Positive Power

Maintain thermal balance

Maintain Periodic Communication with earth

Navigation

Science data downlink

Power Failure

Attitude determination failure

Attitude control failure

Inability to send system state to earth

High-rate communication unavailable

PSC fault

Battery temperature above pre-defined limit

Battery temperature below low limit

Critically low state of charge

Both star trackers blinded

Solar horizon sensor non-functional

Reaction wheels fault

Spacecraft temperature not within operating limits

Damaged HGA

HGA unable to point to earth

3-Tier Response:

- Soft-reset PSC
- Power cycle PSC
- Switch the PSC

If Battery heater is ON: power-off

Battery heater Power-On

Demote into Safe Mode

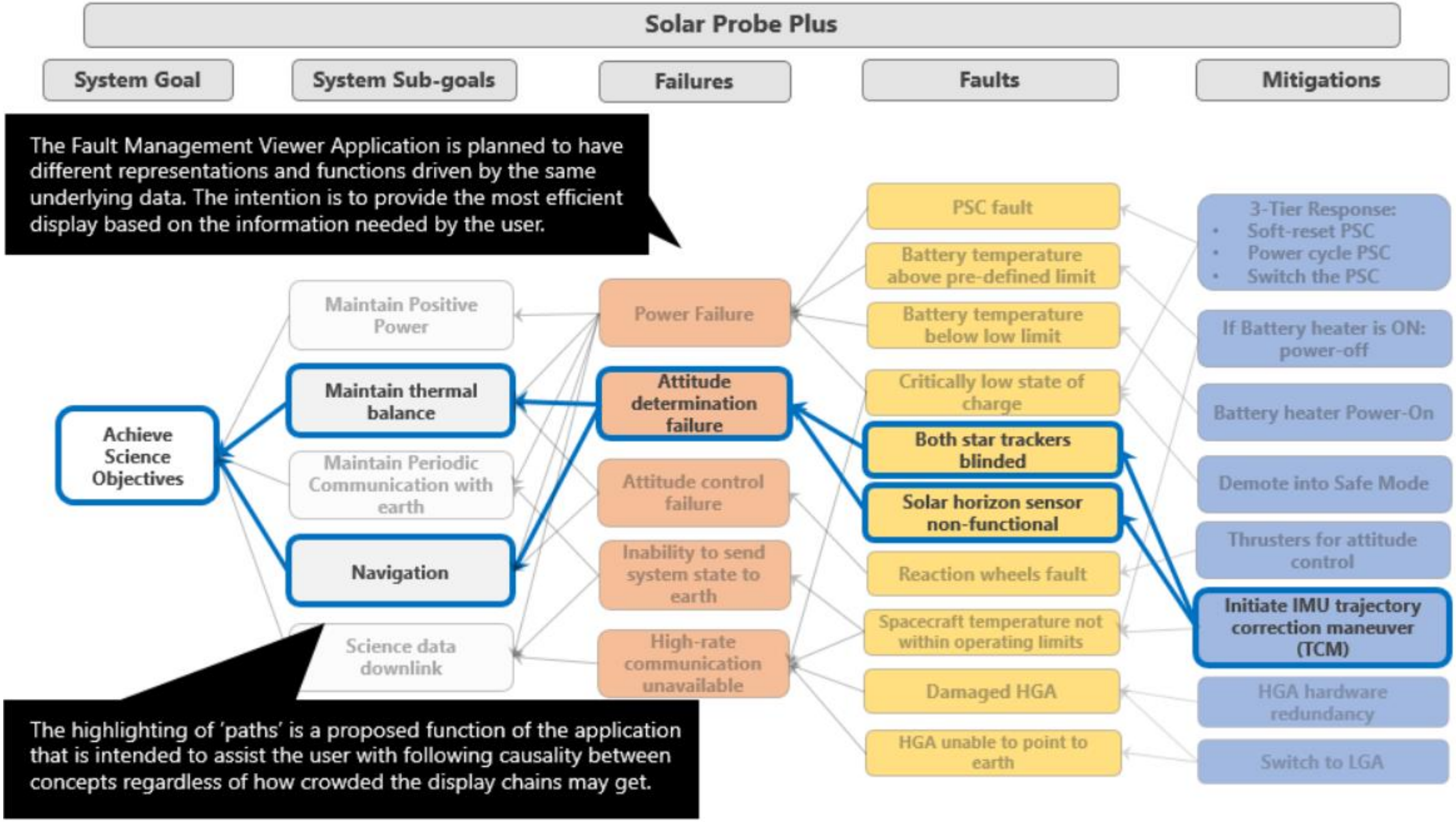
Thrusters for attitude control

Initiate IMU trajectory correction maneuver (TCM)

HGA Hardware redundancy

Switch to LGA

What goals are affected by attitude determination failure?



Solar Probe Plus

System Goal

System Sub-goals

Failures

Faults

Mitigations

The Fault Management Viewer Application is planned to have different representations and functions driven by the same underlying data. The intention is to provide the most efficient display based on the information needed by the user.

Achieve Science Objectives

Maintain Positive Power

Maintain thermal balance

Maintain Periodic Communication with earth

Navigation

Science data downlink

Power Failure

Attitude determination failure

Attitude control failure

Inability to send system state to earth

High-rate communication unavailable

PSC fault

Battery temperature above pre-defined limit

Battery temperature below low limit

Critically low state of charge

Both star trackers blinded

Solar horizon sensor non-functional

Reaction wheels fault

Spacecraft temperature not within operating limits

Damaged HGA

HGA unable to point to earth

3-Tier Response:

- Soft-reset PSC
- Power cycle PSC
- Switch the PSC

If Battery heater is ON: power-off

Battery heater Power-On

Demote into Safe Mode

Thrusters for attitude control

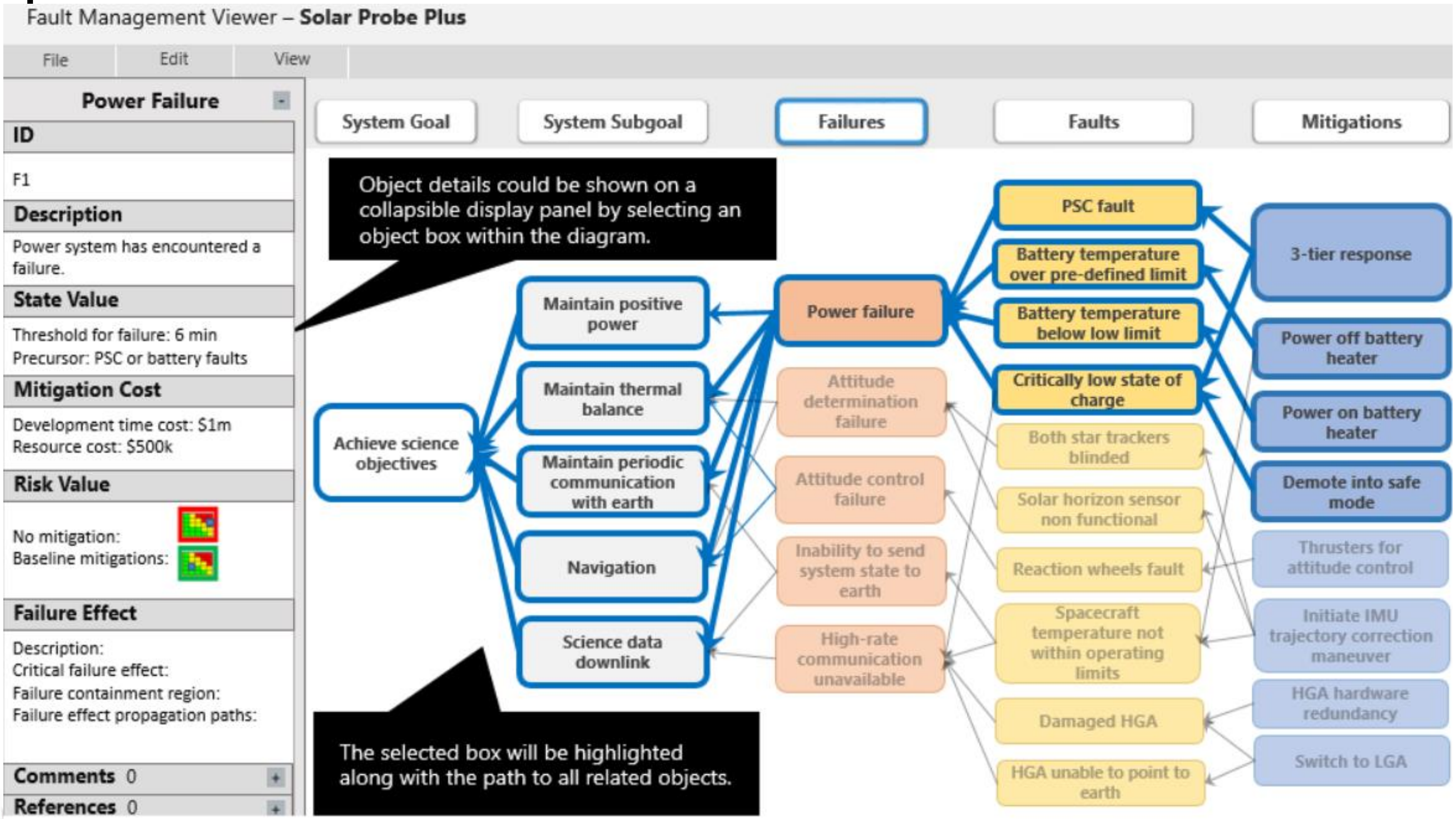
Initiate IMU trajectory correction maneuver (TCM)

HGA hardware redundancy

Switch to LGA

The highlighting of 'paths' is a proposed function of the application that is intended to assist the user with following causality between concepts regardless of how crowded the display chains may get.

How well have I protected against power failure?



Power Failure

ID

F1

Description

Power system has encountered a failure.

State Value

Threshold for failure: 6 min
Precursor: PSC or battery faults

Mitigation Cost

Development time cost: $1m
Resource cost: $500k

Risk Value

No mitigation:
Baseline mitigations:

Failure Effect

Description:
Critical failure effect:
Failure containment region:
Failure effect propagation paths:

Comments 0

References 0

System Goal | System Subgoal | Failures | Faults | Mitigations

System Goal: Achieve science objectives

System Subgoal: Maintain positive power; Maintain thermal balance; Maintain periodic communication with earth; Navigation; Science data downlink

Failures: Power failure; Attitude determination failure; Attitude control failure; Inability to send system state to earth; High-rate communication unavailable

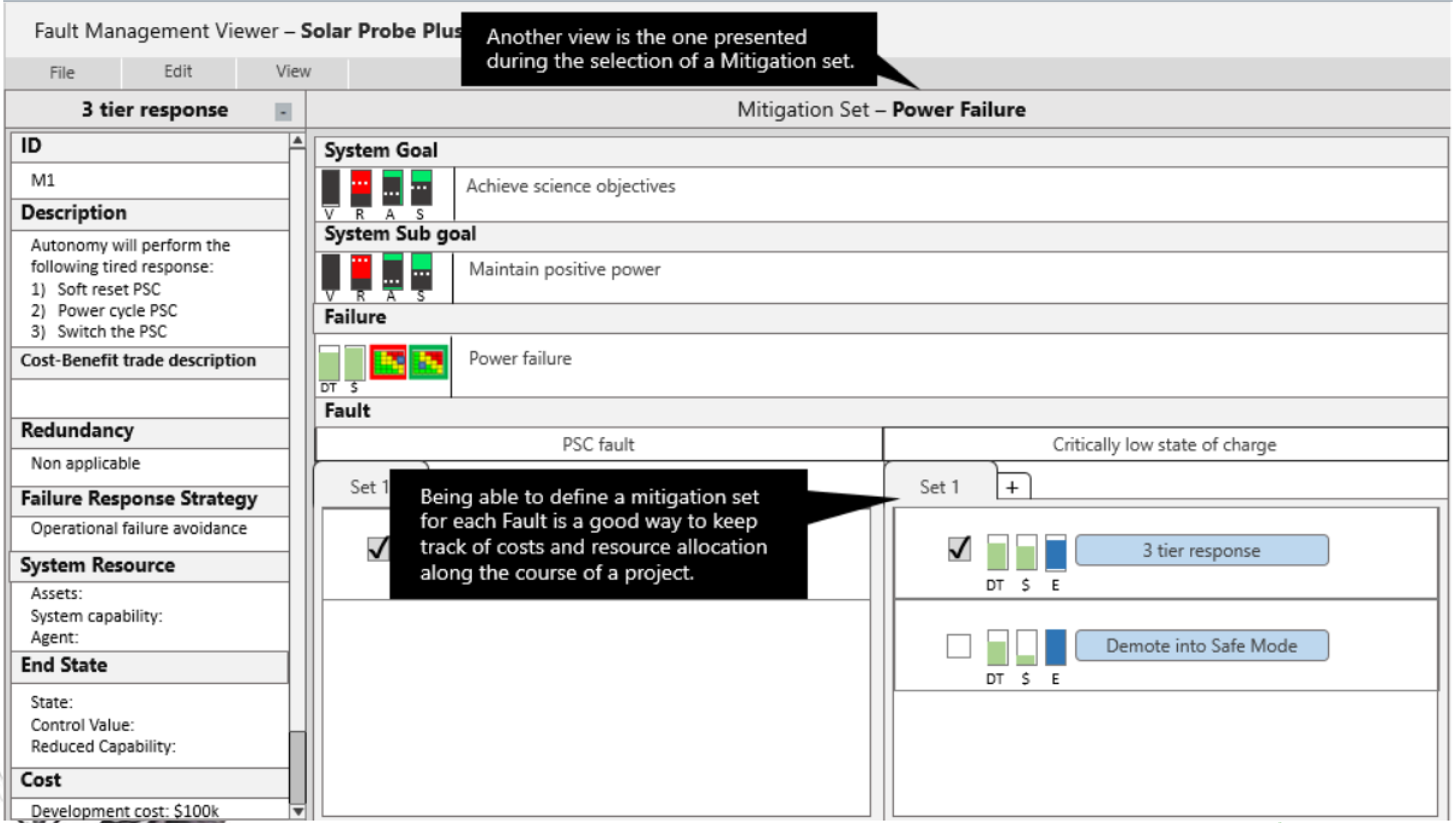
Faults: PSC fault; Battery temperature over pre-defined limit; Battery temperature below low limit; Critically low state of charge; Both star trackers blinded; Solar horizon sensor non functional; Reaction wheels fault; Spacecraft temperature not within operating limits; Damaged HGA; HGA unable to point to earth

Mitigations: 3-tier response; Power off battery heater; Power on battery heater; Demote into safe mode; Thrusters for attitude control; Initiate IMU trajectory correction maneuver; HGA hardware redundancy; Switch to LGA

Object details could be shown on a collapsible display panel by selecting an object box within the diagram.

The selected box will be highlighted along with the path to all related objects.

Which of these mitigation sets is most effective?



Fault Management Viewer – **Solar Probe Plus**

File | Edit | View

3 tier response

ID

M1

Description

Autonomy will perform the following tired response:

1) Soft reset PSC
2) Power cycle PSC
3) Switch the PSC

Cost-Benefit trade description

Redundancy

Non applicable

Failure Response Strategy

Operational failure avoidance

System Resource

Assets:
System capability:
Agent:

End State

State:
Control Value:
Reduced Capability:

Cost

Development cost: $100k

Mitigation Set – **Power Failure**

System Goal

V R A S — Achieve science objectives

System Sub goal

V R A S — Maintain positive power

Failure

DT $ — Power failure

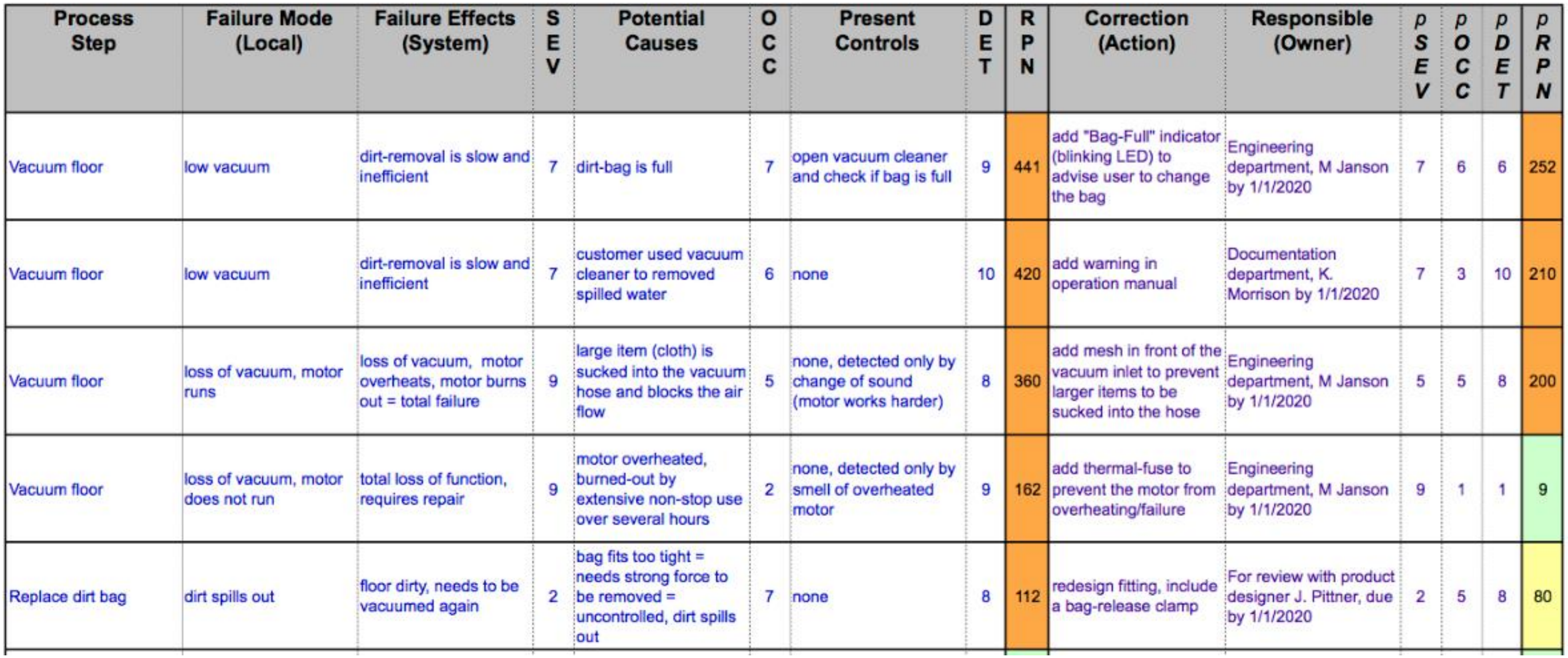
Fault

PSC fault	Critically low state of charge
Set 1 ☑	Set 1 + ☑ DT $ E — 3 tier response □ DT $ E — Demote into Safe Mode

Another view is the one presented during the selection of a Mitigation set.

Being able to define a mitigation set for each Fault is a good way to keep track of costs and resource allocation along the course of a project.

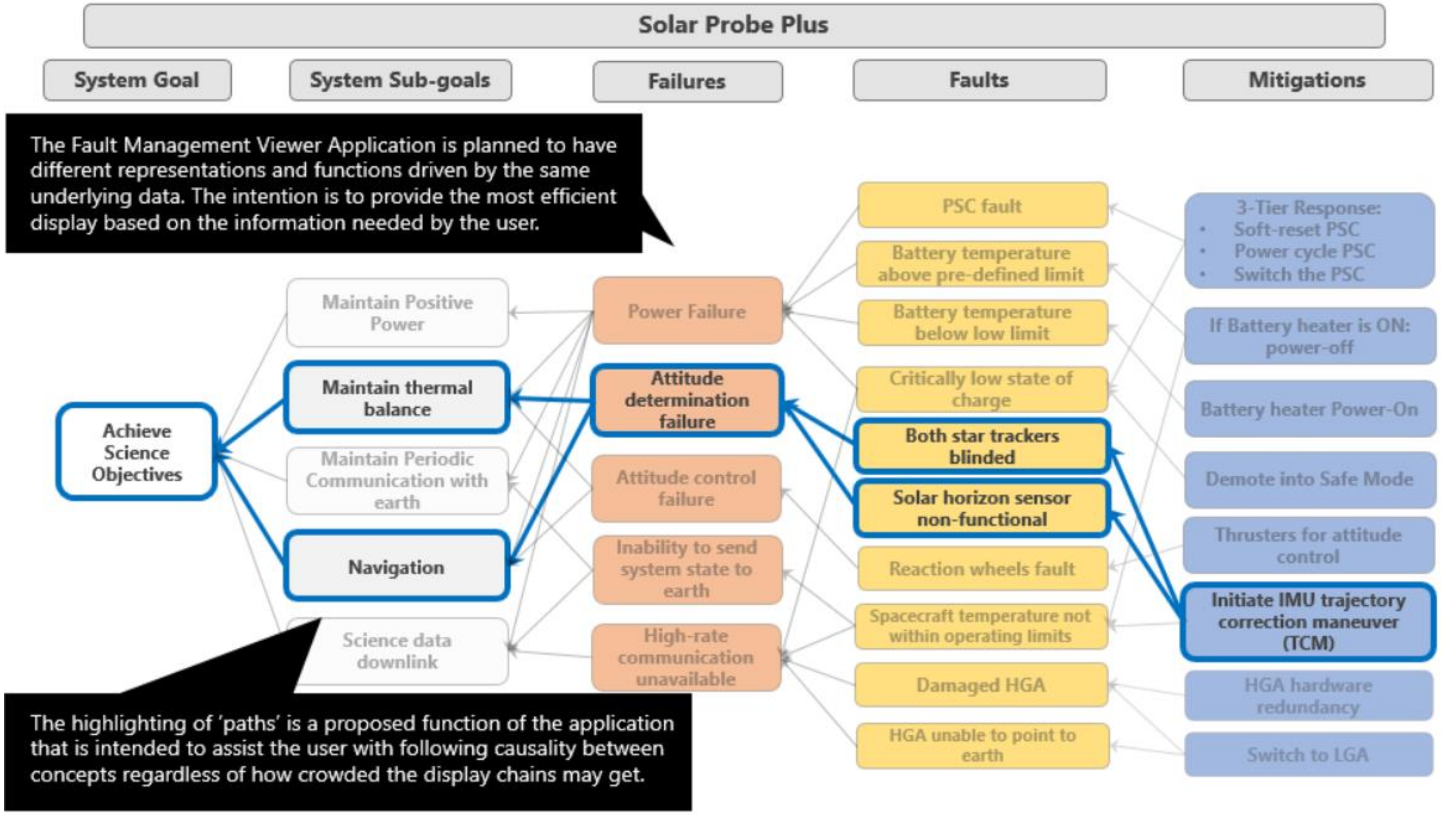
Traditional FMEA View



Process Step	Failure Mode (Local)	Failure Effects (System)	SEV	Potential Causes	OCC	Present Controls	DET	RPN	Correction (Action)	Responsible (Owner)	*p SEV*	*p OCC*	*p DET*	*p RPN*
Vacuum floor	low vacuum	dirt-removal is slow and inefficient	7	dirt-bag is full	7	open vacuum cleaner and check if bag is full	9	441	add "Bag-Full" indicator (blinking LED) to advise user to change the bag	Engineering department, M Janson by 1/1/2020	7	6	6	252
Vacuum floor	low vacuum	dirt-removal is slow and inefficient	7	customer used vacuum cleaner to removed spilled water	6	none	10	420	add warning in operation manual	Documentation department, K. Morrison by 1/1/2020	7	3	10	210
Vacuum floor	loss of vacuum, motor runs	loss of vacuum, motor overheats, motor burns out = total failure	9	large item (cloth) is sucked into the vacuum hose and blocks the air flow	5	none, detected only by change of sound (motor works harder)	8	360	add mesh in front of the vacuum inlet to prevent larger items to be sucked into the hose	Engineering department, M Janson by 1/1/2020	5	5	8	200
Vacuum floor	loss of vacuum, motor does not run	total loss of function, requires repair	9	motor overheated, burned-out by extensive non-stop use over several hours	2	none, detected only by smell of overheated motor	9	162	add thermal-fuse to prevent the motor from overheating/failure	Engineering department, M Janson by 1/1/2020	9	1	1	9
Replace dirt bag	dirt spills out	floor dirty, needs to be vacuumed again	2	bag fits too tight = needs strong force to be removed = uncontrolled, dirt spills out	7	none	8	112	redesign fitting, include a bag-release clamp	For review with product designer J. Pittner, due by 1/1/2020	2	5	8	80

FM Diagram W/ FMEA Labels

Process Process Step Failure Cause Mitigation



Solar Probe Plus

System Goal

System Sub-goals

Failures

Faults

Mitigations

The Fault Management Viewer Application is planned to have different representations and functions driven by the same underlying data. The intention is to provide the most efficient display based on the information needed by the user.

Achieve Science Objectives

Maintain Positive Power

Maintain thermal balance

Maintain Periodic Communication with earth

Navigation

Science data downlink

Power Failure

Attitude determination failure

Attitude control failure

Inability to send system state to earth

High-rate communication unavailable

PSC fault

Battery temperature above pre-defined limit

Battery temperature below low limit

Critically low state of charge

Both star trackers blinded

Solar horizon sensor non-functional

Reaction wheels fault

Spacecraft temperature not within operating limits

Damaged HGA

HGA unable to point to earth

3-Tier Response:
- Soft-reset PSC
- Power cycle PSC
- Switch the PSC

If Battery heater is ON: power-off

Battery heater Power-On

Demote into Safe Mode

Thrusters for attitude control

Initiate IMU trajectory correction maneuver (TCM)

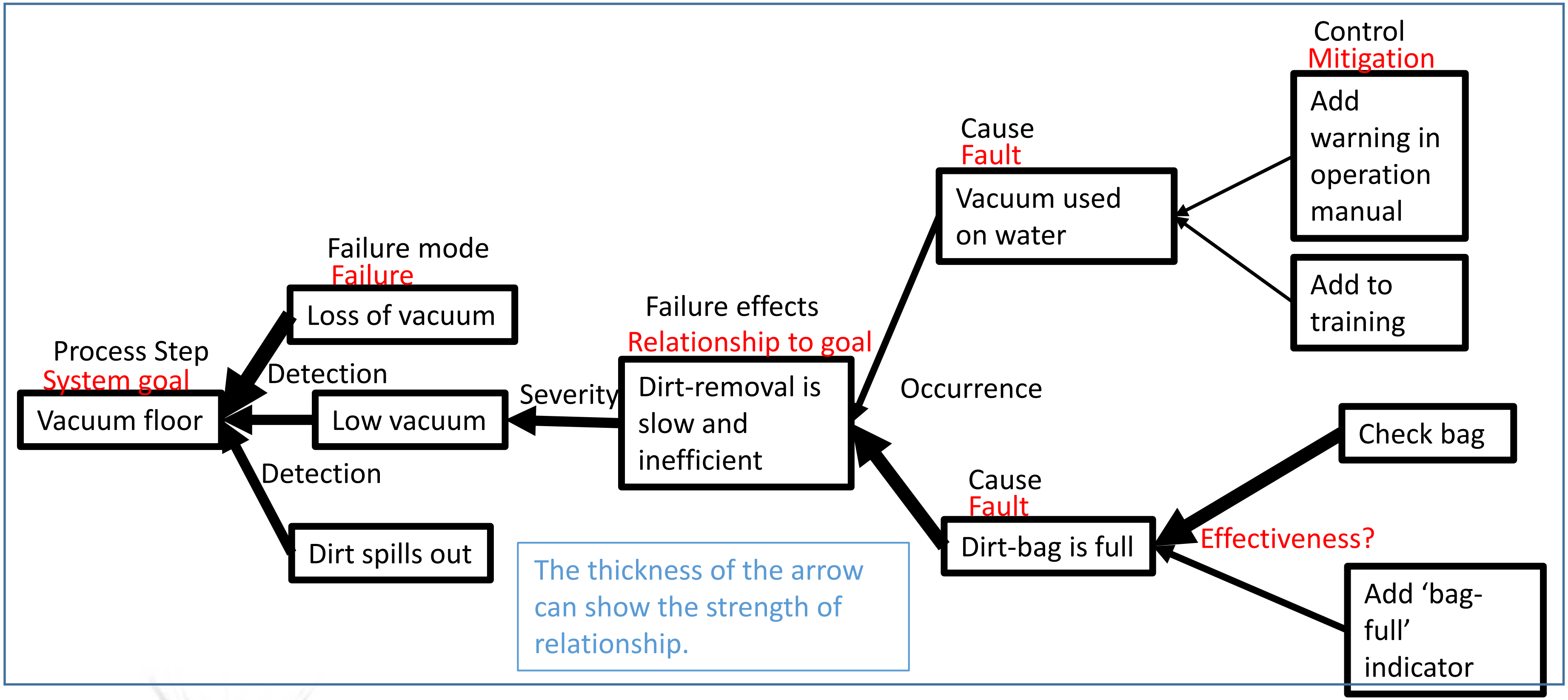
HGA hardware redundancy

Switch to LGA

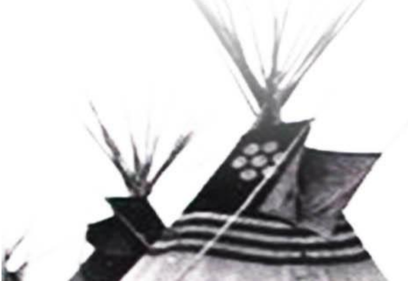
The highlighting of 'paths' is a proposed function of the application that is intended to assist the user with following causality between concepts regardless of how crowded the display chains may get.

- Failure Effects are shown as relationship between failure and goals

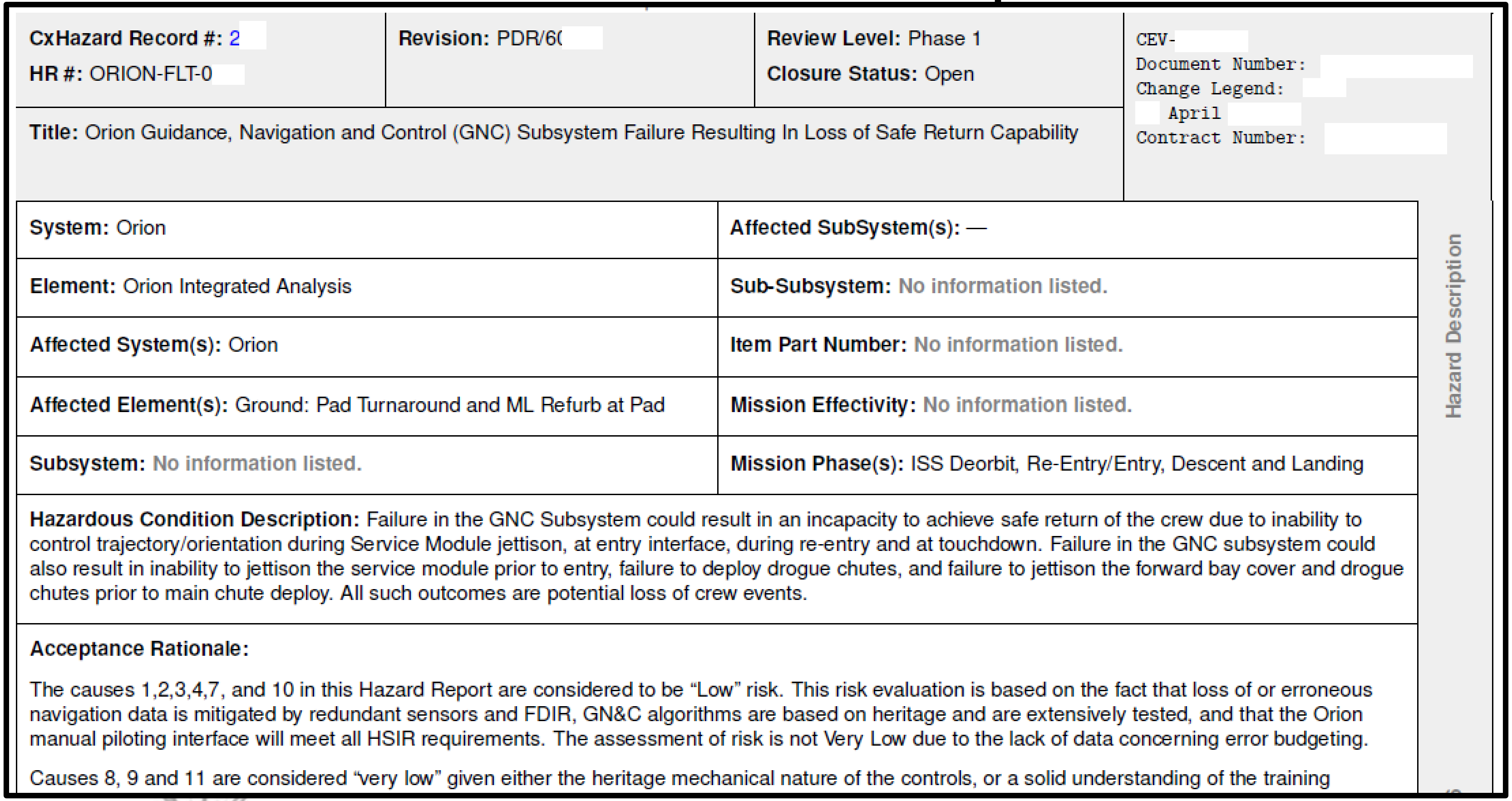
Failure Modes and Effects Analysis Extension: FMEA (Graphical View)



The thickness of the arrow can show the strength of relationship.



Traditional Hazard Report View



CxHazard Record #: 2[redacted] **HR #:** ORION-FLT-0[redacted]	**Revision:** PDR/6([redacted]	**Review Level:** Phase 1 **Closure Status:** Open	CEV-[redacted] Document Number: [redacted] Change Legend: [redacted] [redacted] April [redacted] Contract Number: [redacted]
Title: Orion Guidance, Navigation and Control (GNC) Subsystem Failure Resulting In Loss of Safe Return Capability			

System: Orion	**Affected SubSystem(s):** —
Element: Orion Integrated Analysis	**Sub-Subsystem:** No information listed.
Affected System(s): Orion	**Item Part Number:** No information listed.
Affected Element(s): Ground: Pad Turnaround and ML Refurb at Pad	**Mission Effectivity:** No information listed.
Subsystem: No information listed.	**Mission Phase(s):** ISS Deorbit, Re-Entry/Entry, Descent and Landing

Hazard Description

Hazardous Condition Description: Failure in the GNC Subsystem could result in an incapacity to achieve safe return of the crew due to inability to control trajectory/orientation during Service Module jettison, at entry interface, during re-entry and at touchdown. Failure in the GNC subsystem could also result in inability to jettison the service module prior to entry, failure to deploy drogue chutes, and failure to jettison the forward bay cover and drogue chutes prior to main chute deploy. All such outcomes are potential loss of crew events.

Acceptance Rationale:

The causes 1,2,3,4,7, and 10 in this Hazard Report are considered to be "Low" risk. This risk evaluation is based on the fact that loss of or erroneous navigation data is mitigated by redundant sensors and FDIR, GN&C algorithms are based on heritage and are extensively tested, and that the Orion manual piloting interface will meet all HSIR requirements. The assessment of risk is not Very Low due to the lack of data concerning error budgeting.

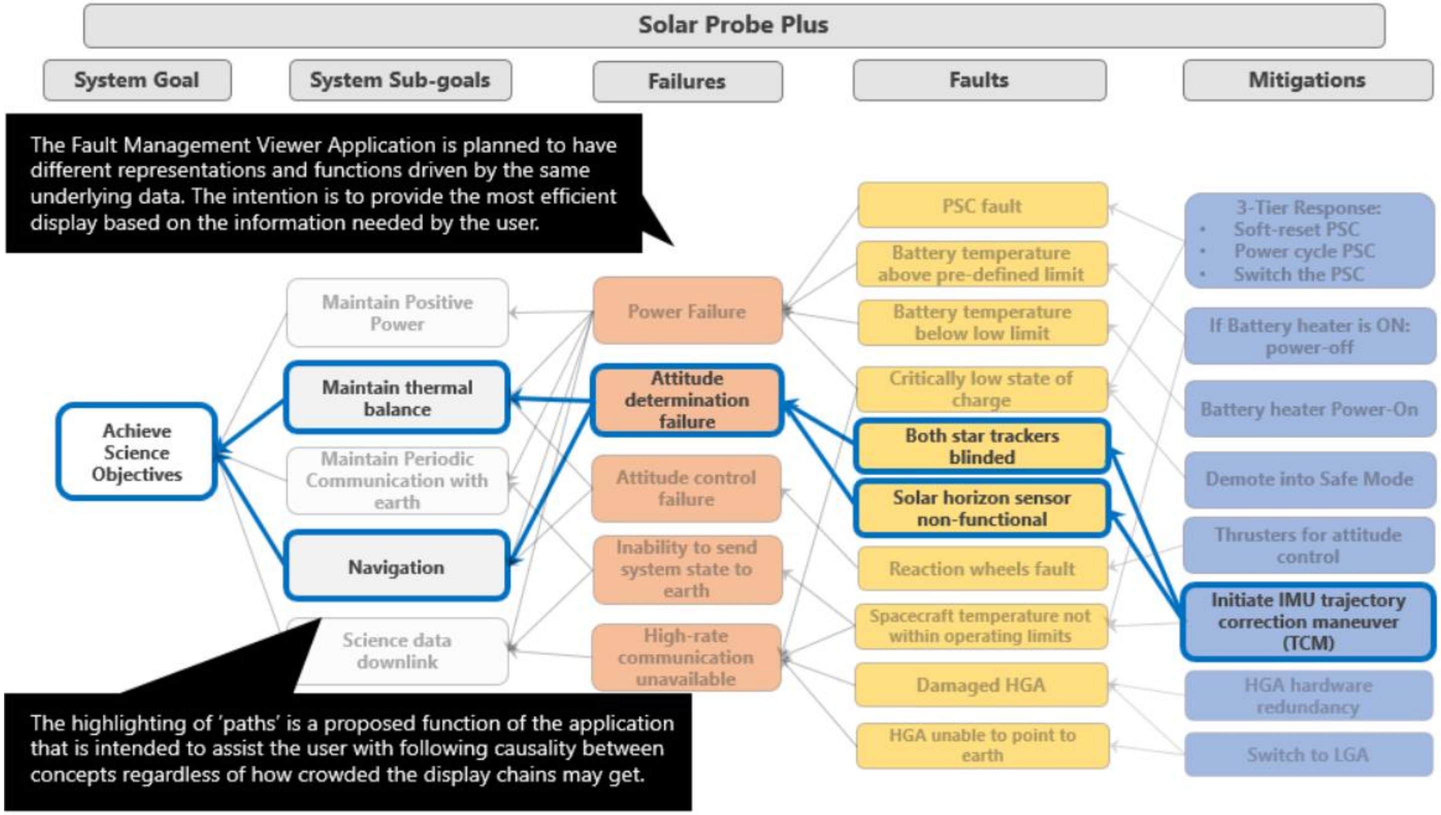
Causes 8, 9 and 11 are considered "very low" given either the heritage mechanical nature of the controls, or a solid understanding of the training

FM Diagram W/ Hazard Report Labels

Hazard

Fault

Controls



Solar Probe Plus

System Goal

System Sub-goals

Failures

Faults

Mitigations

The Fault Management Viewer Application is planned to have different representations and functions driven by the same underlying data. The intention is to provide the most efficient display based on the information needed by the user.

Achieve Science Objectives

Maintain Positive Power

Maintain thermal balance

Maintain Periodic Communication with earth

Navigation

Science data downlink

Power Failure

Attitude determination failure

Attitude control failure

Inability to send system state to earth

High-rate communication unavailable

PSC fault

Battery temperature above pre-defined limit

Battery temperature below low limit

Critically low state of charge

Both star trackers blinded

Solar horizon sensor non-functional

Reaction wheels fault

Spacecraft temperature not within operating limits

Damaged HGA

HGA unable to point to earth

3-Tier Response:
- Soft-reset PSC
- Power cycle PSC
- Switch the PSC

If Battery heater is ON: power-off

Battery heater Power-On

Demote into Safe Mode

Thrusters for attitude control

Initiate IMU trajectory correction maneuver (TCM)

HGA hardware redundancy

Switch to LGA

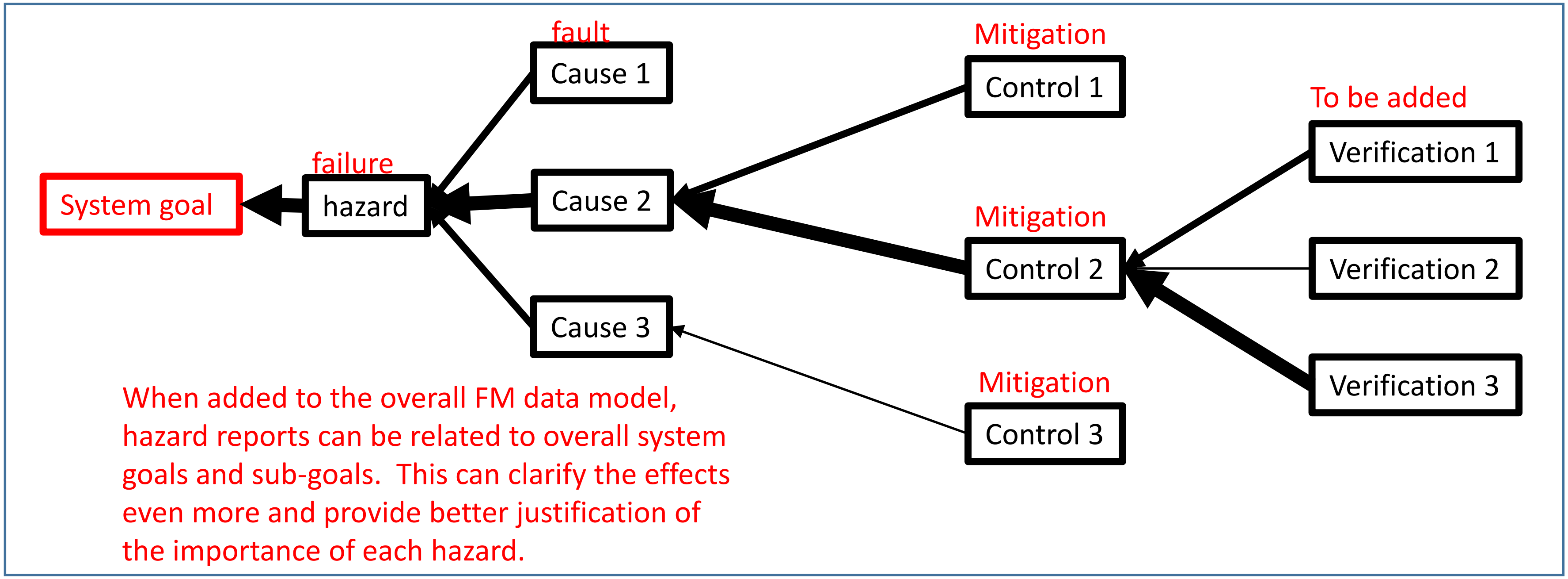
The highlighting of 'paths' is a proposed function of the application that is intended to assist the user with following causality between concepts regardless of how crowded the display chains may get.

- Verifications need to be added to the data model

5/13/2018

Slide 18

Extension: Hazard Report (Graphical)



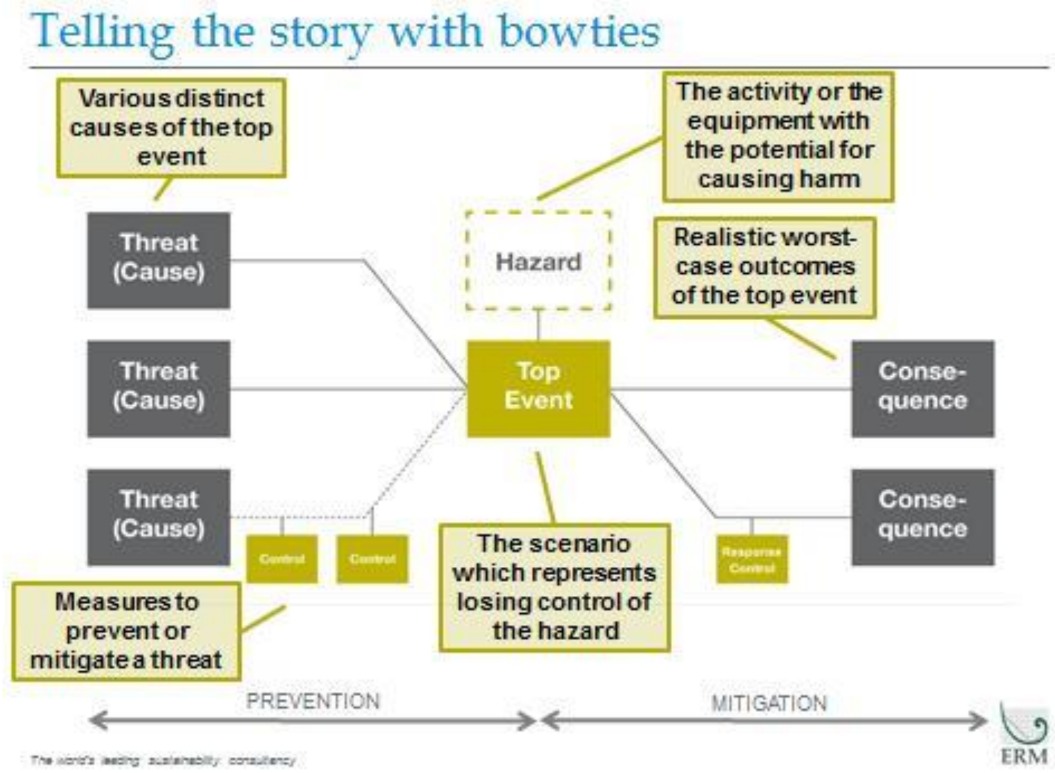
When added to the overall FM data model, hazard reports can be related to overall system goals and sub-goals. This can clarify the effects even more and provide better justification of the importance of each hazard.

Next Steps, Suggestions

- Expand prototype to full functionality viewer
  - Only prototyped some views so far
  - Test with more projects ensure realistic expectations
- New Phase I SBIR proposals
  - Resilience Management Tool (RMT)
    - Resilience is more than fault management (unknown faults, timelines, contingency actions)
  - Fault Management Analysis Tool (FMAT)
    - Workflow assistance in designing FM for a new system
    - Semi-autonomous generation of verification tests
    - Inferring higher level metrics from lower levels (roll up effects of multiple mitigations to estimate how well a system capability is protected)
- Suggestions
  - Needs, opportunities overlooked?
  - Good places to expand?
  - New ways to extend?
  - Possible partnerships?
  - New references?

backups

Bowtie – Before, During, and After Losing Control



Telling the story with bowties

Various distinct causes of the top event

The activity or the equipment with the potential for causing harm

Threat (Cause)

Threat (Cause)

Threat (Cause)

Hazard

Realistic worst-case outcomes of the top event

Top Event

Conse-quence

Conse-quence

Control

Control

Response Control

Measures to prevent or mitigate a threat

The scenario which represents losing control of the hazard

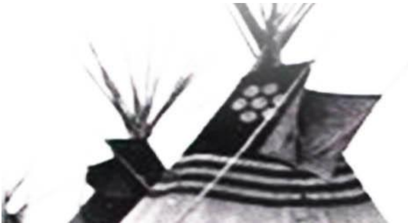
PREVENTION

MITIGATION

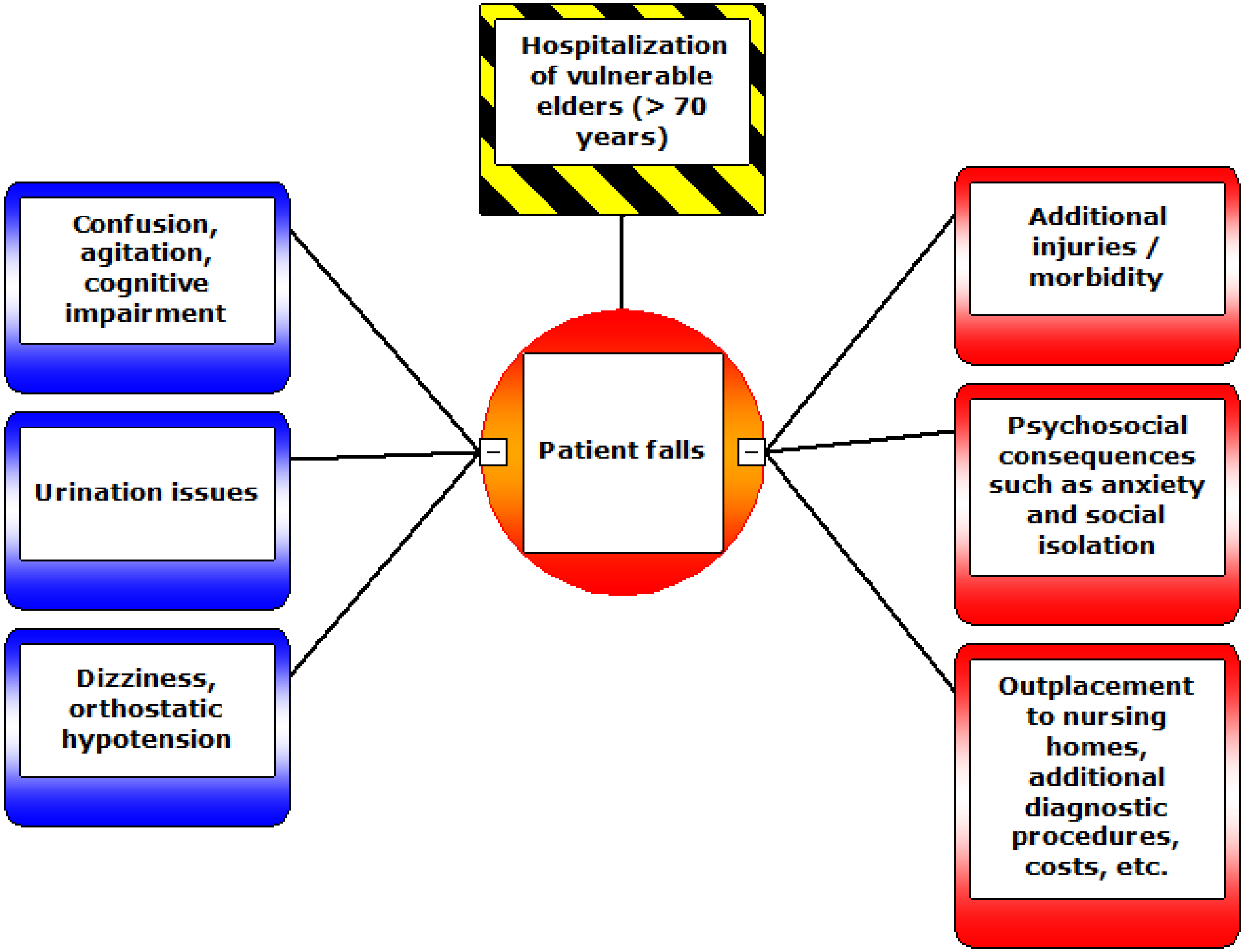
The world's leading sustainability consultancy

ERM

- Helps with close-up view of failure, faults, mitigations, contingency actions.
- Doesn’t show it when individual mitigations, contingency actions address multiple failures
- Nice additional view for FM Viewer
  - Different strengths
  - Different weaknesses



Bowtie with Medical Content



Hospitalization of vulnerable elders (> 70 years)

Confusion, agitation, cognitive impairment

Urination issues

Dizziness, orthostatic hypotension

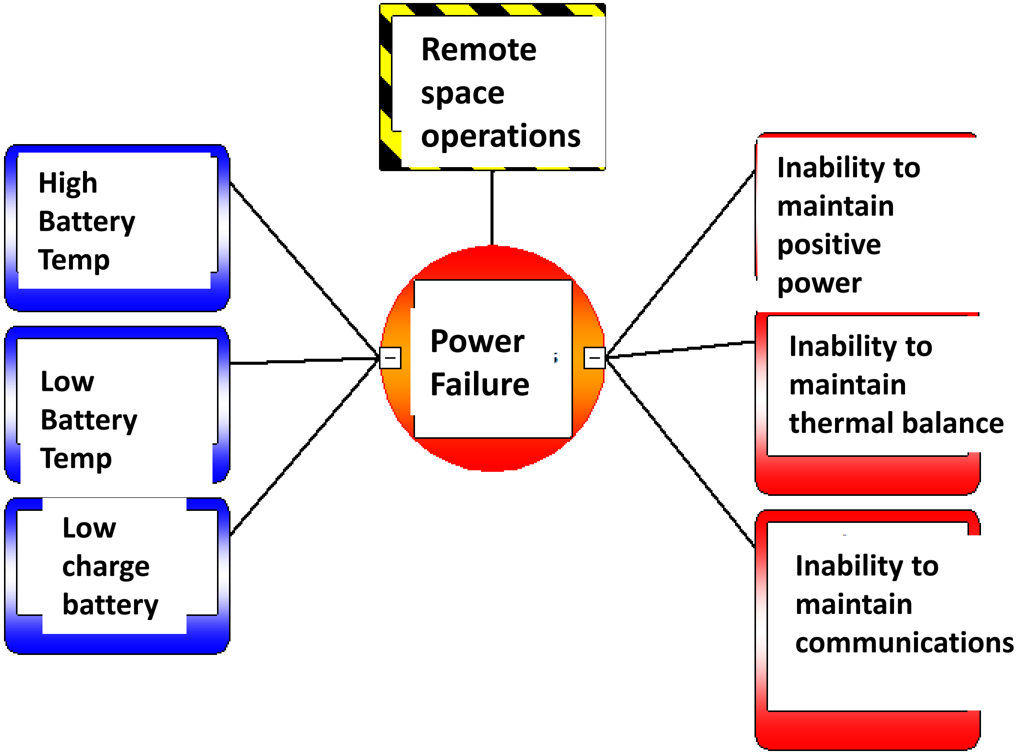
Patient falls

Additional injuries / morbidity

Psychosocial consequences such as anxiety and social isolation

Outplacement to nursing homes, additional diagnostic procedures, costs, etc.

Bowtie: Solar Probe Plus Content



Remote space operations

High Battery Temp

Low Battery Temp

Low charge battery

Power Failure

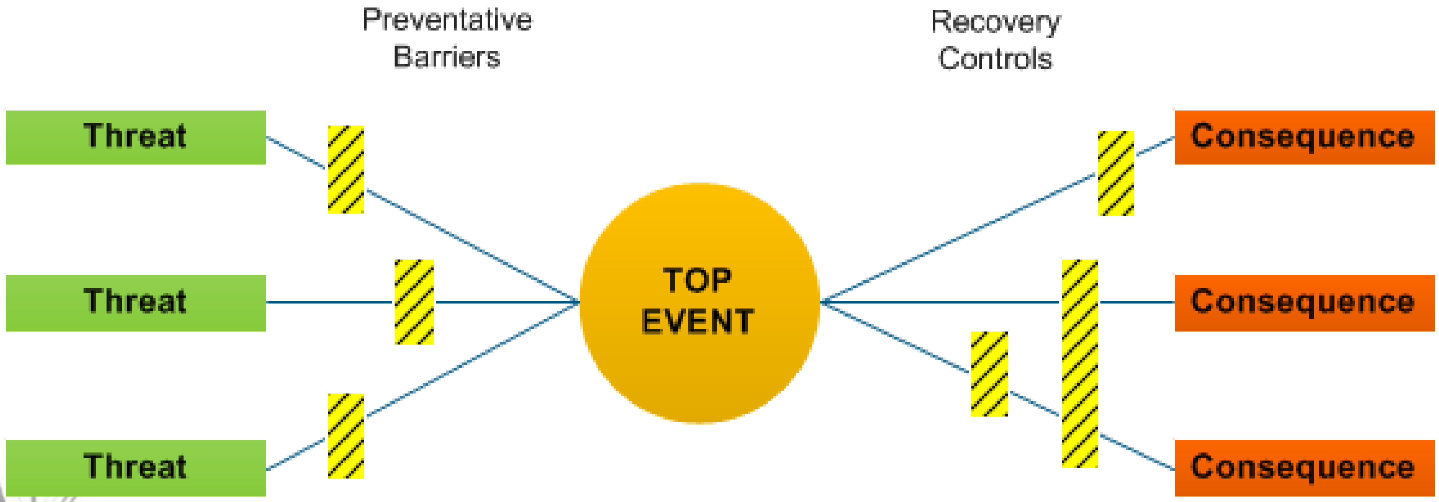
Inability to maintain positive power

Inability to maintain thermal balance

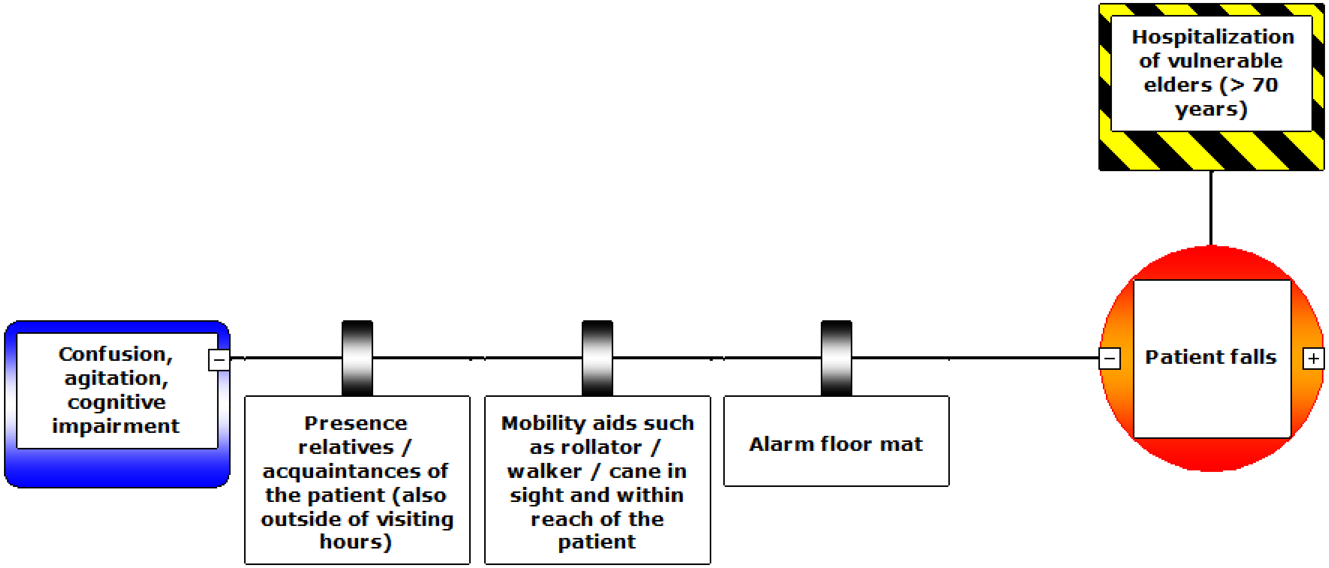
Inability to maintain communications

Bowtie Also Includes Barriers

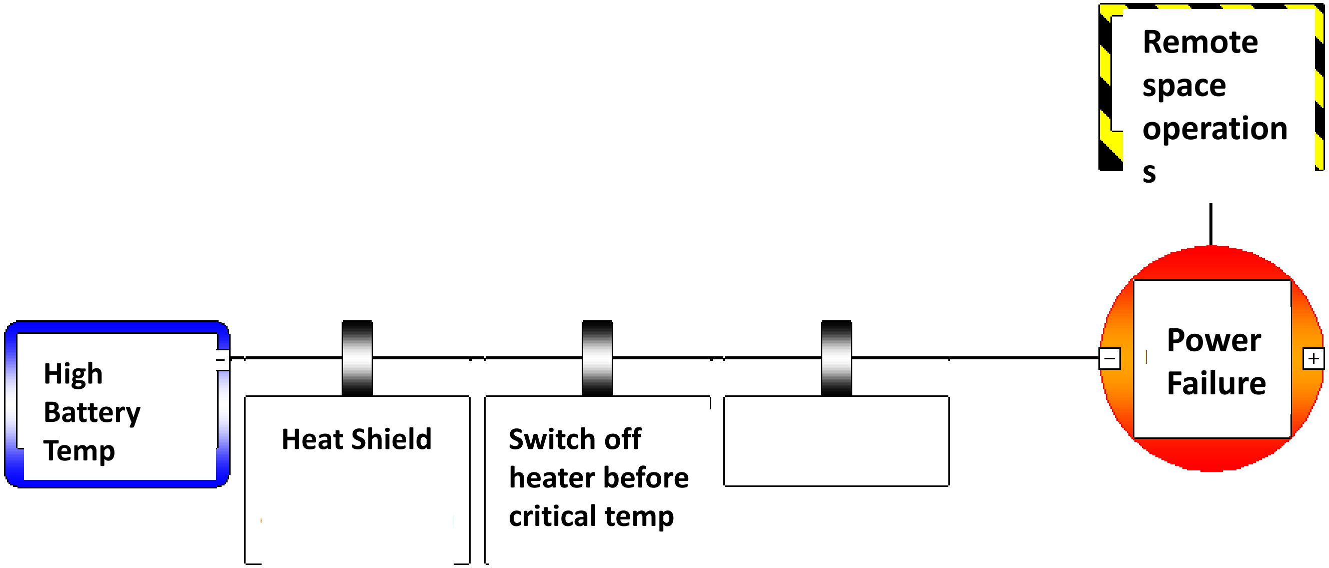
- Helps Analyst Consider
  - Preventive barriers (mitigations)
  - Recovery controls (contingency actions)



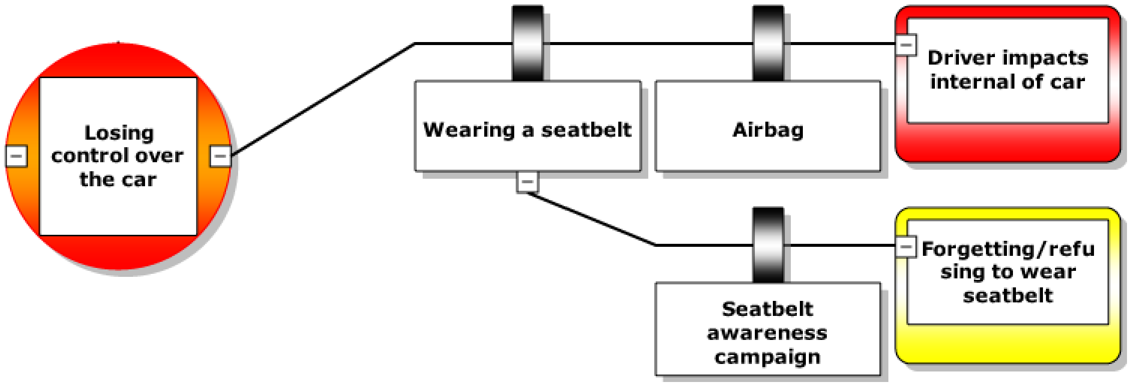
Bowtie Controls (Mitigations) - Medical


Hospitalization of vulnerable elders (> 70 years)
Confusion, agitation, cognitive impairment
Presence relatives / acquaintances of the patient (also outside of visiting hours)
Mobility aids such as rollator / walker / cane in sight and within reach of the patient
Alarm floor mat
Patient falls

Bowtie Controls (Mitigations) – Solar Probe Plus



Bowtie
Barriers after – contingency actions
Car accident



Losing control over the car

Wearing a seatbelt

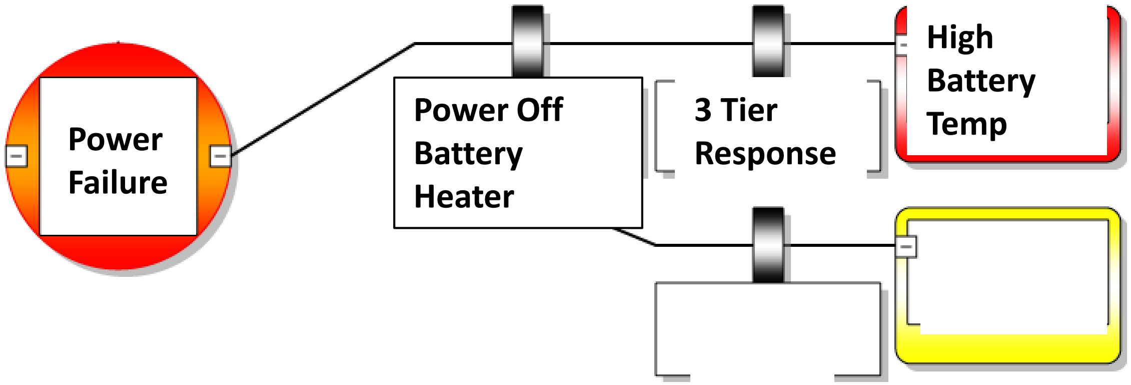
Airbag

Driver impacts internal of car

Seatbelt awareness campaign

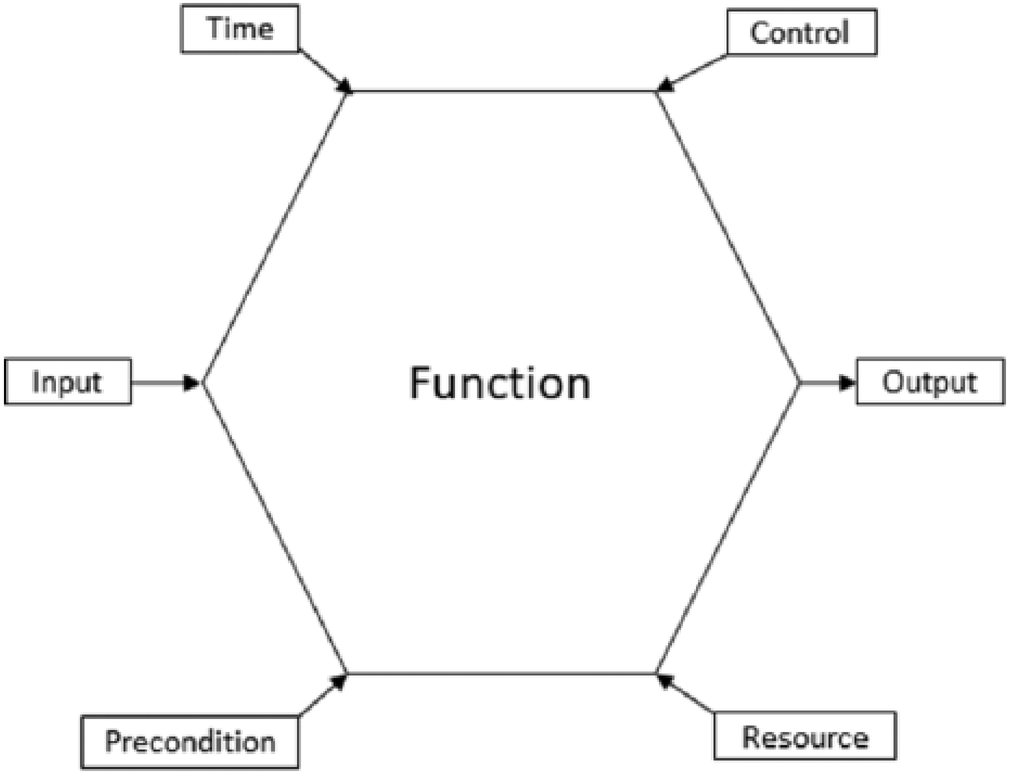
Forgetting/refusing to wear seatbelt

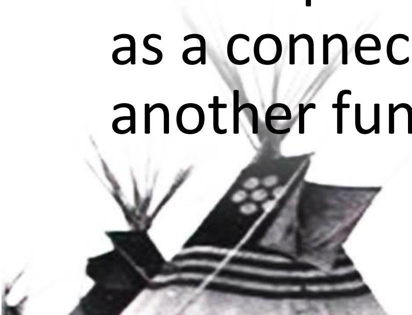
Bowtie – Barriers after – contingency actions
Solar Probe Plus



Functional Resonance Analysis Method (FRAM)

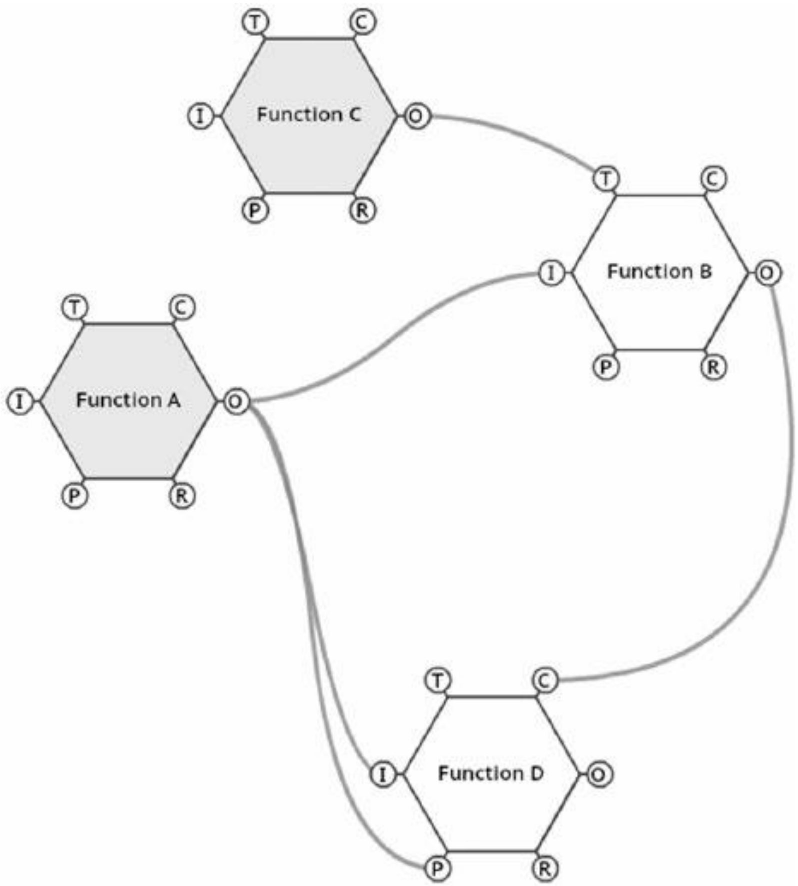
- FRAM provides the means to understand how multiple functions or activities in a "system" relate to one another, and provides a visualization of how adverse outcomes can occur.
- Each node represents a function, with 6 aspects
- Each aspect can serve as a connection to another function



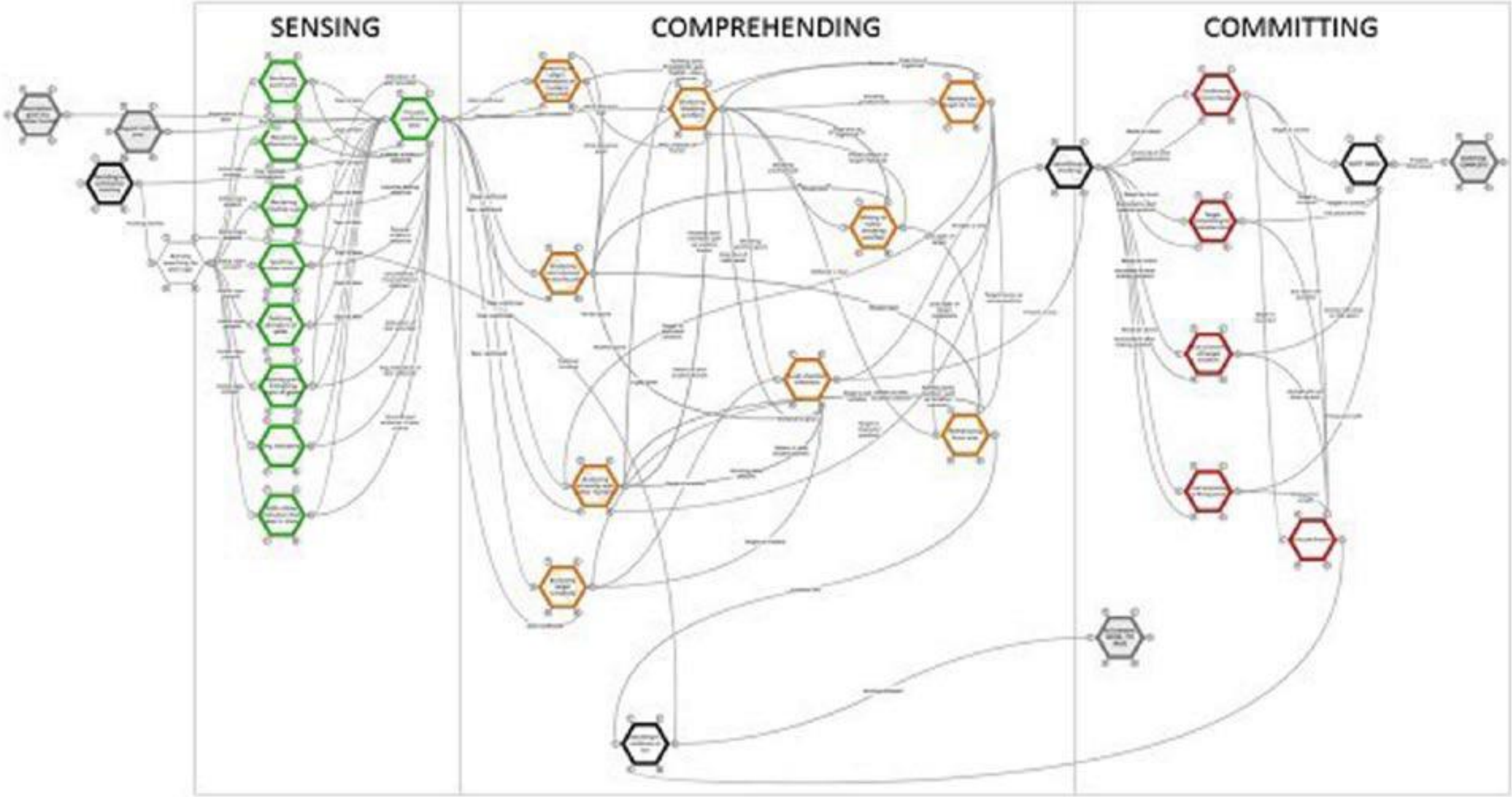


Connected FRAM Model

- Functions (nodes) can be linked to show relationships among them
- The relevant aspect (input, output, etc.) shows how functions are linked



A FRAM to Show Target ID in Hunting



Pros, Cons in Adding FRAM to FM Viewer

- Possible benefits
  - Different strengths and weaknesses from FM diagram
  - Richer set of function aspects to add to FM data model
  - Additional set of analyses to vet the completeness of the FM model
  - Could be especially strong for vetting accuracy and interactions of functions (system goals, sub-goals, capabilities)
  - Could expose system function design vulnerabilities
  - Should be especially valuable for human tasks, identifying needs for improved task and training designs
  - FRAM analysis specifically targets ways to increase resilience
- Possible disadvantages
  - Possibly over-complicating the data model – discouraging developer from using it
  - Complexities in auto drawing implied model so all lines are visible