Solar Probe Plus

A NASA Mission to Touch the Sun

Fault Management Peer Review Day 1

Sanae Kubota
Fault Management Lead Engr.
sanae.kubota@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Solar Probe Plus

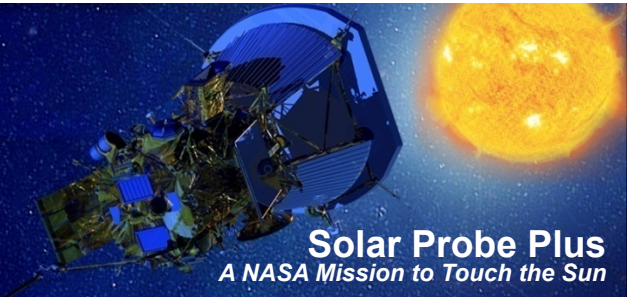
A NASA Mission to Touch the Sun

Introduction

Sanae Kubota
FM Lead Engineer
sanae.kubota@jhuapl.edu

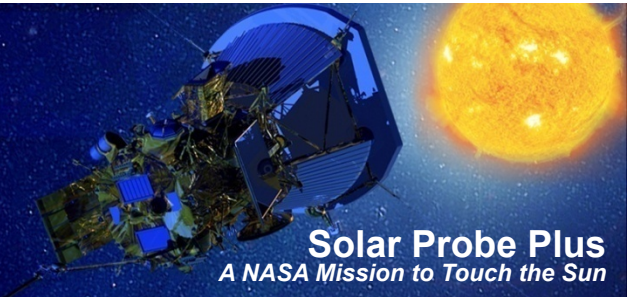
APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Review Panel



Reviewer	Organization
Adrian Hill (chair)	APL
Steven Battel	Battel Engineering
Ann Devereaux	NASA / JPL
Chris Jones	NASA / JPL
Steven Scott	NASA / GSFC

SPP FM Team Members

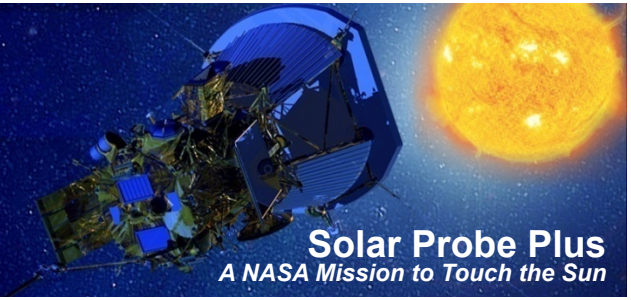


The Fault Management System design is the product of collaborative work with the entire SPP team.

Particular credit to:

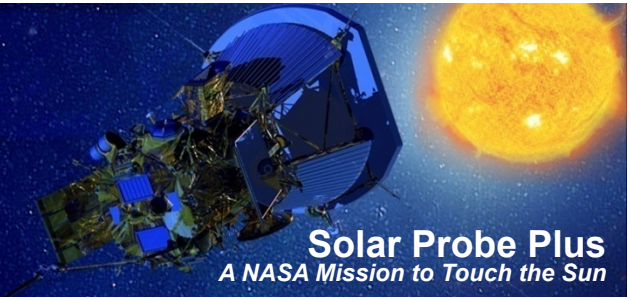
Liz Abel - thermal, Carson Baisden – solar array control, Stewart Bushman – propulsion, Weilun Cheng – mechanisms, Tim Cole – mechanical, Rich Conde – deputy spacecraft systems & electrical systems, David Copeland – telecomm, Jack Ercol – cooling system, Kristin Fretz – fault management, Mike Furrow – software systems, Ed Gaddy – solar array, Andrew Harris – testbed software, Melissa Jones - reliability, Jim Kinnison – mission systems, Chris Krupiarz – flight software, Mary Kae Lockwood – spacecraft systems, Danielle Marsh – solar array operations and safing, Gayle Martin – thermal, Eric Melin – ground system software, Alan Mick – data systems, Chris Monaco – command and data handling software, Geff Ottman - avionics, Gail Oxton – guidance and control software, Nick Pinkine – mission operations, Paul Rosendall - autonomy, Lew Roufberg – electrical power system, Sam Sawada – power distribution unit, Clay Smith - reliability, Robin Vaughan – guidance and control, Kyle Weber – avionics redundancy controller

Agenda: Day 1



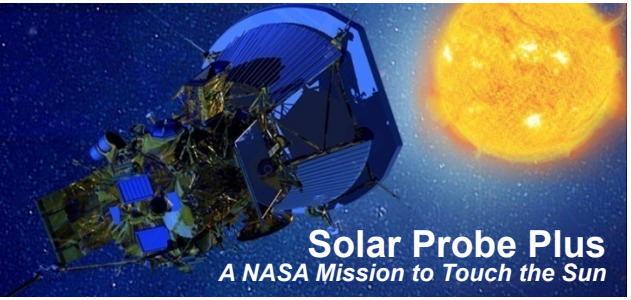
Topic	Speaker(s)	Start Time
Introduction	Sanae Kubota	9:00 am
Fault Management (FM) Process and Requirements Flow	Sanae Kubota	9:10 am
SPP Overview	Mary Kae Lockwood	9:30 am
*** *break (10 minutes)* ***		10:00 am
FM Prelim. Design & L3 Requirements - Redundancy Concept - Avionics Architecture	Sanae Kubota Geff Ottman	10:10 am 10:40 am
*** *lunch (60 minutes)* ***		11:40 am
FM Prelim. Design & L3 Requirements, continued - Critical Scenarios - Safing Concept / FM Modes - Ground Intervention Concept - Instrument FM	Sanae Kubota	12:40 pm
Fault Analysis Process Overview	Clay Smith	2:10 pm
*** *break (10 minutes)* ***		2:40 pm
Prelim. Fault Responses & L3 Requirements Mapping	Sanae Kubota	2:50 pm
Maintaining MET	Rich Conde	4:20 pm
Day 1 end		4:50 pm

Agenda: Day 2



Topic	Speaker(s)	Start Time
Critical Scenarios - Critical Sequence - Critical Faults - Safe Mode Review - Attitude Protection	Sanae Kubota Robin Vaughan	9:00 am 9:20 am
*** *break (10 minutes)* ***		10:50 am
Solar Array Control overview	Carson Baisden	11:00 am
*** *lunch (60 minutes)* ***		11:20 am
Solar Array Safing - Overview - System Temperatures - Solar Array Safing Approach	Danielle Marsh	12:20 pm
*** *break (10 minutes)* ***		1:50 pm
Solar Array Safing, continued - Solar Array Safing Approach, continued - TRL-6 Testing - Future Work	Danielle Marsh	2:00 pm
Preliminary Verification & Validation	Sanae Kubota	3:30 pm
Wrap Up	Sanae Kubota	3:45 pm
Review Board caucus		4:00 pm

Purpose of Review

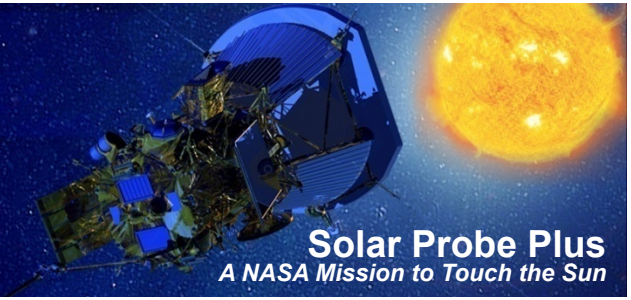


- **Ensure Fault Management System preliminary design is sufficiently sound and mature to support complete Level 3 requirements development.**

- **Ensure Level 3 Fault Management (FM) requirements are appropriate**
  - as flowed from mission and project requirements,
  - as indicated from fault analyses and response planning, and
  - as necessary for allocation to distributed Level 4 FM requirements.*

* Significant progress has been made on the development of L4 FM requirements & corresponding preliminary design. L4 FM requirements will be reviewed in depth at subsystem PDRs / requirements reviews.

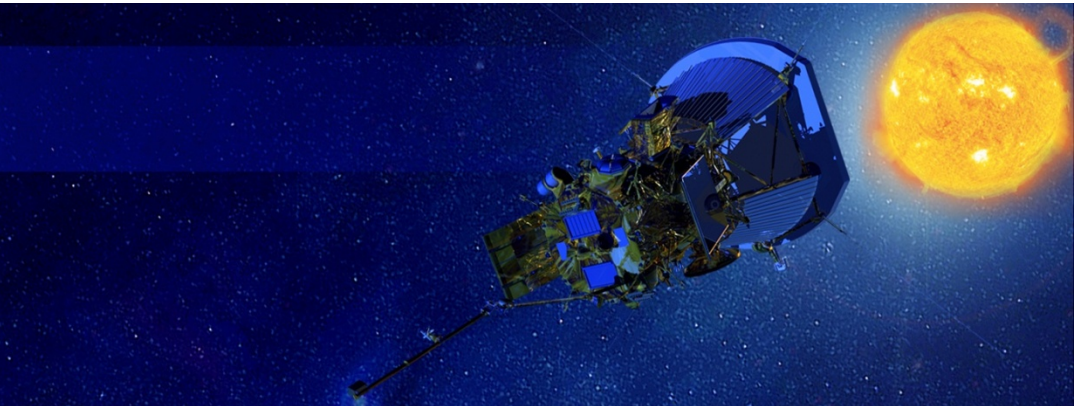
Logistics



- **Minutes and Action Item management**
  - To be documented via memorandum.
- **Please sign-in.**
- **Room: 200-E100**
- **Provided materials**
  - **Fault Management Peer Review slide package**
  - **Failure Modes and Effects Analyses**
- **Documentation Location:**
  \\davis\project\Solar Probe Plus\System Engineering\Fault Management\Reviews\FM Peer Review

Solar Probe Plus

A NASA Mission to Touch the Sun

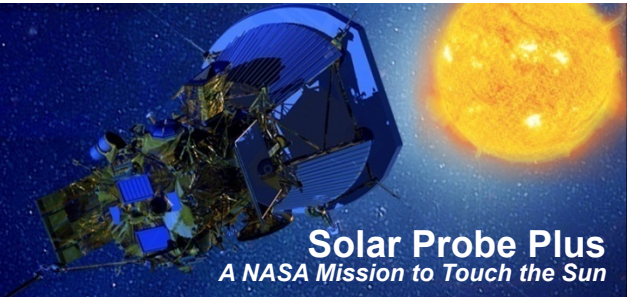


Fault Management Process

Sanae Kubota
FM Lead Engineer
sanae.kubota@jhuapl.edu

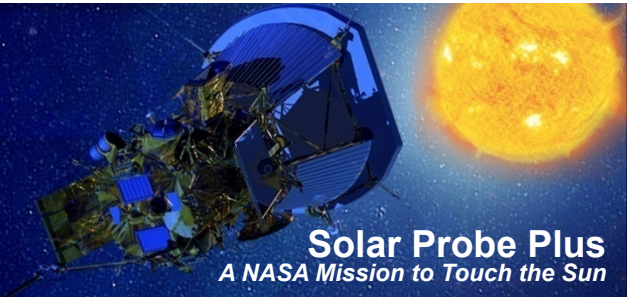
APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Fault Management Process



- Fault Management and Autonomy scope/roles
- APL FM Process
- Status of documentation
- Level 1 – Level 2 – Level 3 Requirements Flow

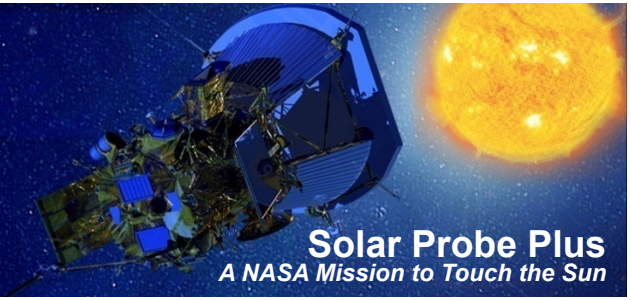
Fault Management and Autonomy Scope/Roles



- **Fault management is:**
  - A system engineering function
  - Defines the functional requirements distributed throughout the spacecraft and ground that enable detection, isolation, and recovery from events that upset nominal operations
  - Distributed design with allocations to:
    - Hardware
    - Flight Software
    - Autonomy
    - Ground/Mission Operations

- **Autonomy is:**
  - A spacecraft subsystem
  - Implements a subset of FM requirements

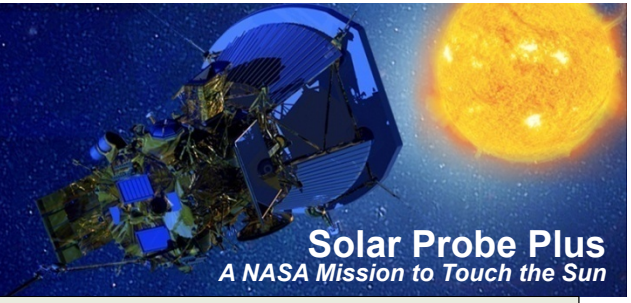
Summary of FM Process



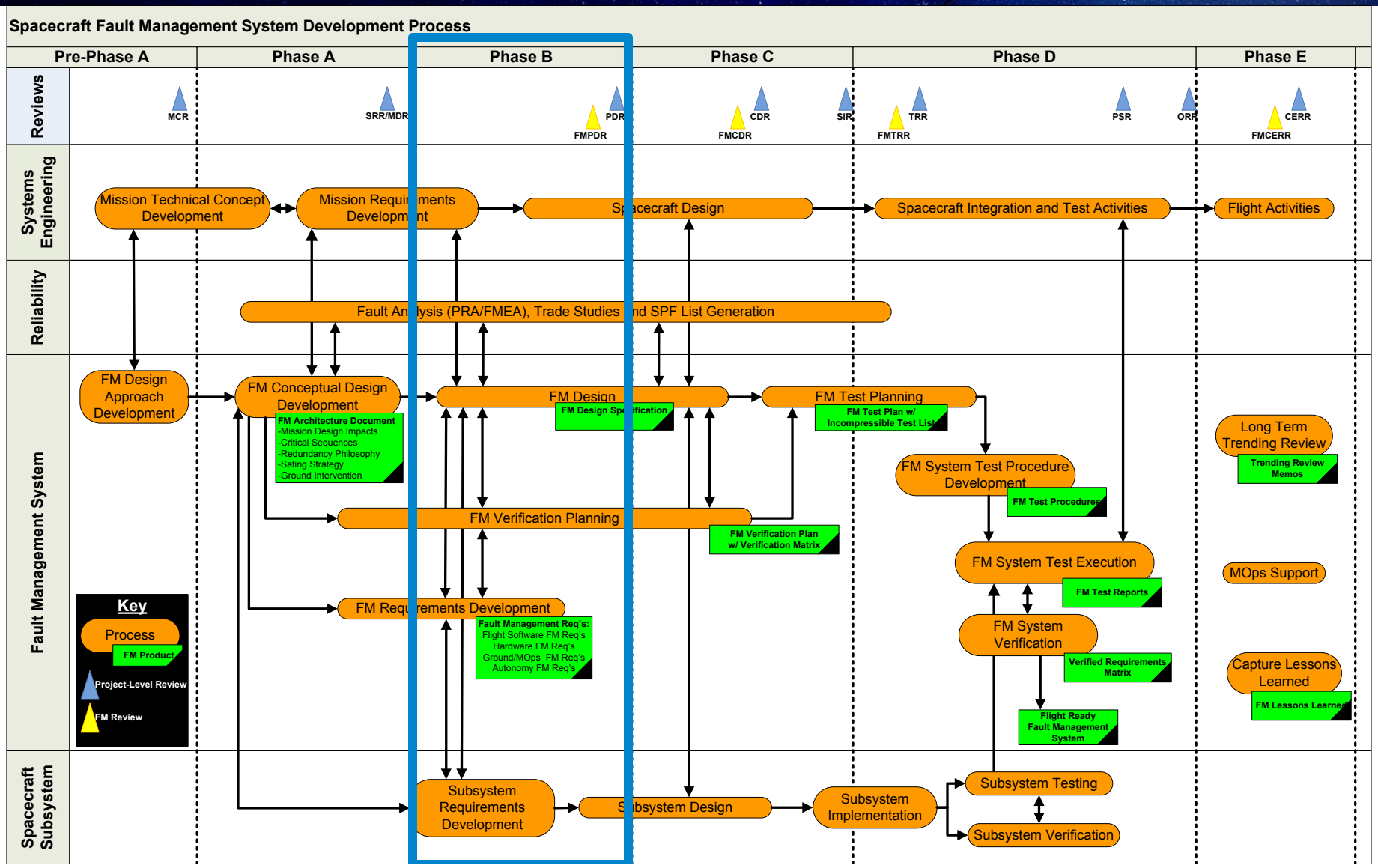
- Fault management architecture determined based on mission constraints, objectives, and driving requirements.
  - Analyze mission and system-level faults, in the context of mission constraints and objectives, to identify subset of faults to be protected against.
  - Develop fault management design and requirements that delineate these protections and allocate to subsystems that can most effectively accomplish the requirement
    - Based on simplicity, testability, and systems engineering rigor.
  - Verify requirements through unit, subsystem, spacecraft, and system-level scenario testing

- Results in the creation of a distributed fault management system

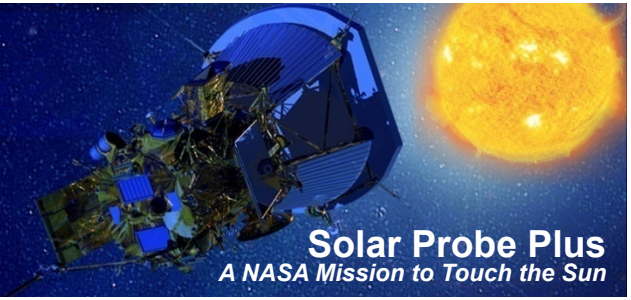
APL FM Process



Solar Probe Plus
A NASA Mission to Touch the Sun



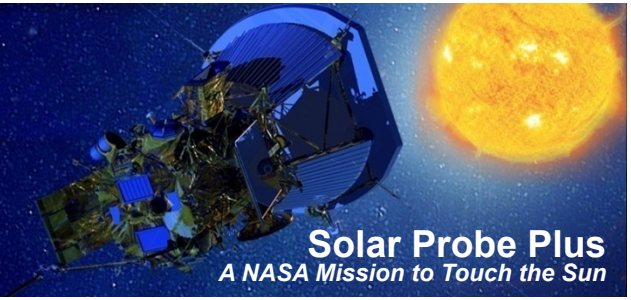
Status of Documentation



Document	Status
FM Architecture Document	Draft complete
FM Design Specification	Draft in-work
FM Level 2 Requirements	Rev. B configured and in DOORS
FM Level 3 Requirements	Drafts complete and in DOORS
FM Level 4 & below Requirements	Drafts in-work

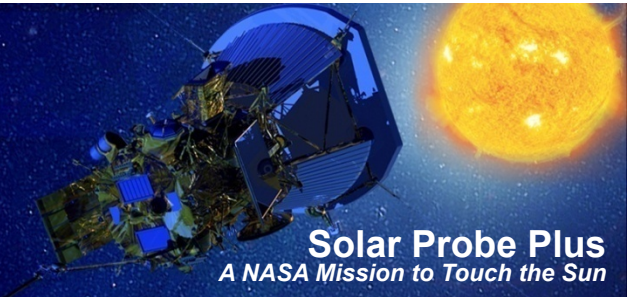
- **Fault Management is a distributed system; FM requirements are distributed across elements and will be distributed across subsystem and component levels.**
- **FM requirements will be flagged as such in DOORS with co-ownership of the requirement between the FM lead and the element/subsystem lead.**

Mission FM Requirements Overview



Level 1 (Project)	Level 2 (Mission)
4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.	MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.
	MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.
	MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.
4.2.4. Solar Probe Plus shall be categorized as Mission Category 1 per NPR 7120.5D and Risk Category B per NPR 8705.4.	MRD-70: The Mission shall have no single point failures except those on the single point failure list.

Requirements Flow L1-L2-L3



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

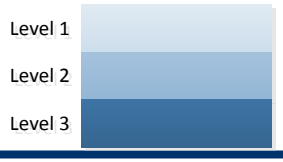
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

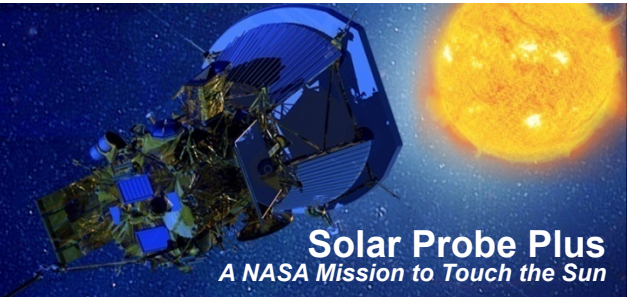
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



Requirements Flow L1-L2-L3



4.2.4. Solar Probe Plus shall be categorized as Mission Category 1 per NPR 7120.5D and Risk Category B per NPR 8705.4.

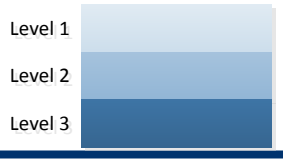
MRD-70: The Mission shall have no single point failures except those on the single point failure list.

REDUNDANCY
The Spacecraft shall …

(n/a; L2 requirement is a design implementation decision which spans multiple system elements)

MRD-72: The Mission shall provide instrument fault protection to include ground system monitoring of selected instrument health data, remote SOC notifications of critical fault conditions, and autonomous onboard instrument power-downs in response to instrument request and critical telemetry.

INSTRUMENT FM
The Spacecraft shall …
All SPP instruments shall …



Solar Probe Plus

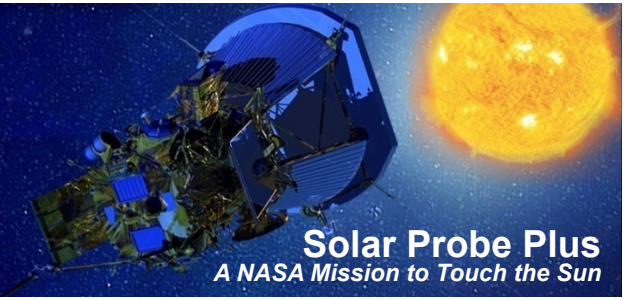
A NASA Mission to Touch the Sun

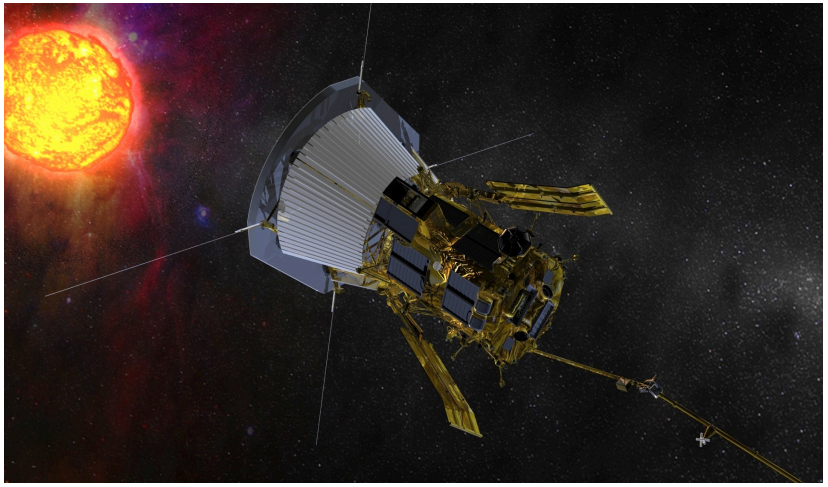
SPP Overview

MK Lockwood
Spacecraft System Engineer
(Deputy Mission System Engineer)
mk.lockwood@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Solar Probe Plus Quad Chart





Overview

Using in-situ measurements made closer to the Sun than by any previous spacecraft, SPP will determine the mechanisms that produce the fast and slow solar winds, coronal heating, and the transport of energetic particles.

Solar Probe Plus will fly to less than 10 solar radii (Rs) of the Sun, having "walked in" from 35.7 Rs over 24 orbits.

Sponsor: NASA SMD/Heliophysics Div

- Program Office – GSFC/LWS
- Project Scientist - APL
- Project Management - APL
- S/C Development & Operations – APL
- Science Investigations selected by AO:
  - SWEAP - Smithsonian Astrophysical Observatory
  - FIELDS - UC Berkeley
  - WISPR - Naval Research Laboratory
  - ISIS – Southwest Research Institute
  - HelioOrigins – Jet Propulsion Laboratory

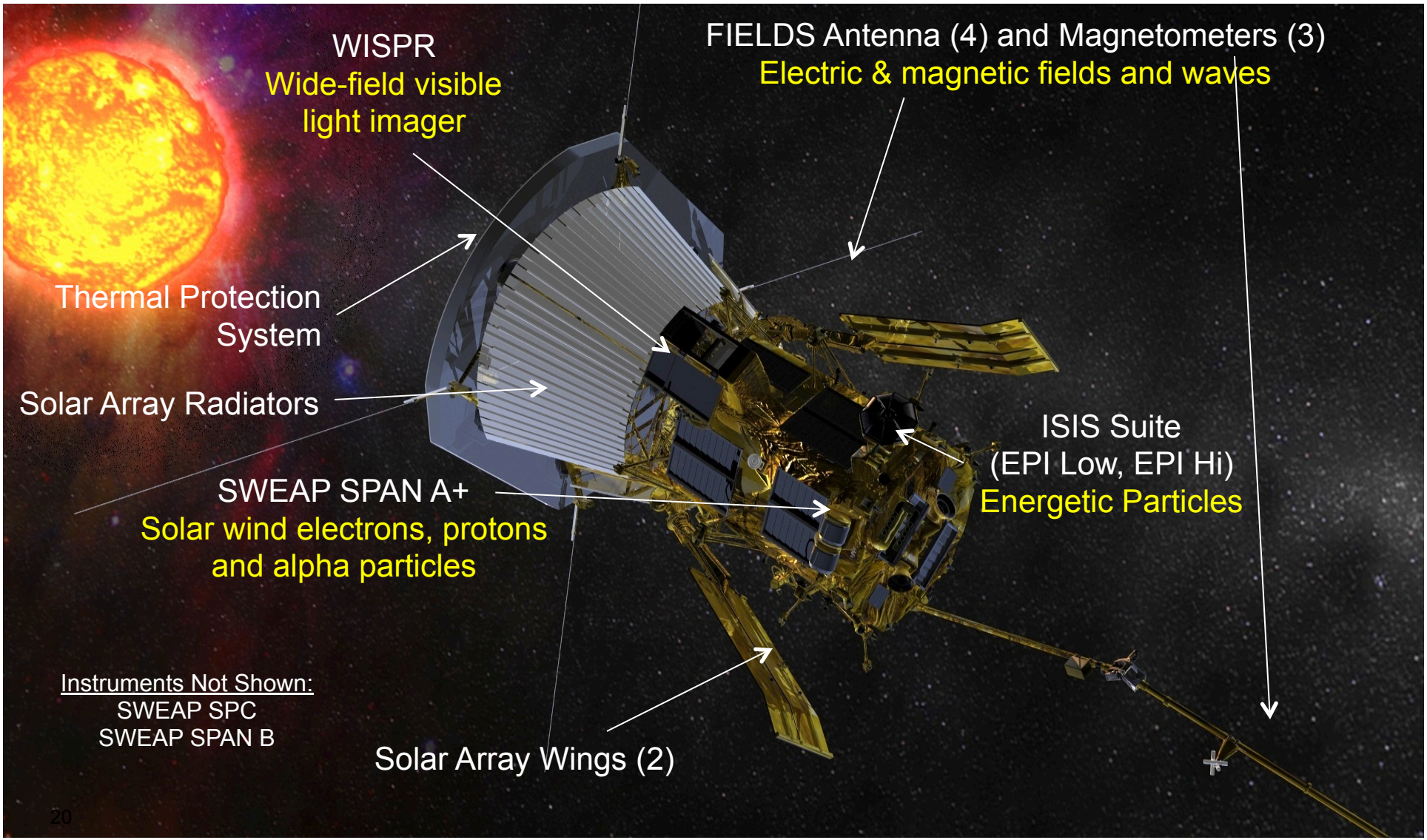
Preliminary Mission Milestones (Assuming 2018 Launch)

Pre-Phase A:	07/2008 – 11/2009
Phase A:	12/2009 – 01/2012
Phase B:	02/2012 – 03/2014
Phase C/D:	03/2014 – 08/2018
Phase E:	09/2018 – 09/2025

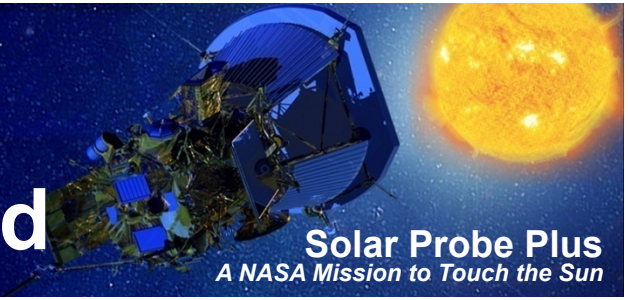
APL

Spacecraft Key Features

Solar Probe Plus
A NASA Mission to Touch the Sun



Trajectory
9.86Rs Min Perihelion Baselined



Launch

- Dates: Jul 31 – Aug 19, 2018 (20 days)
- Max. Launch C3: 154 km^2/s^2
- Requires Atlas V 551 class with Upper Stage

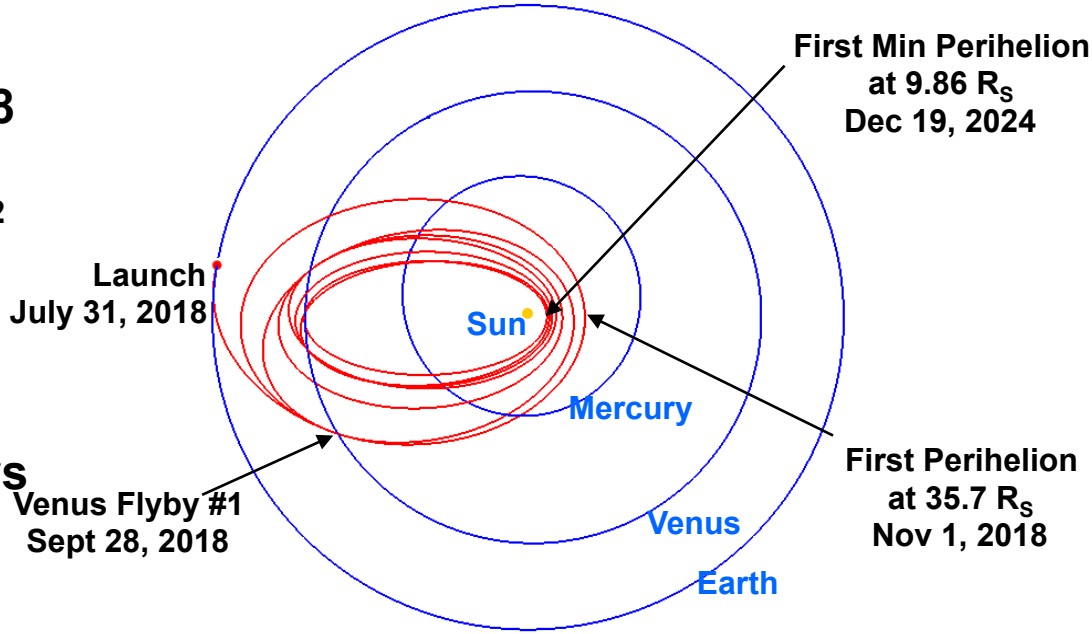
Trajectory Design

- 7 Venus gravity assist flybys

Final Solar Orbits

- Perihelion: 9.86 R_S
- Aphelion: 0.73 AU
- Inclination: 3.4 deg from ecliptic
- Orbit period: 88 days

Mission duration: 7 years



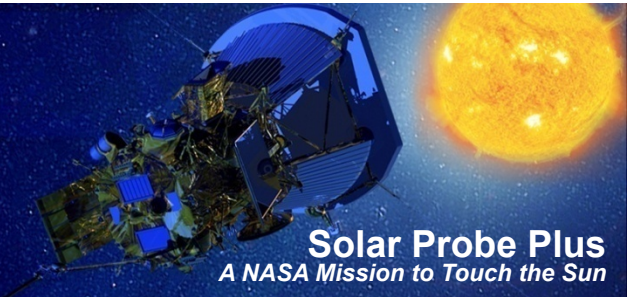
Change in mission design resulted in

- 665kg launch wet mass capability (from 618kg)
- 7% decrease in max solar load to TPS at closest approach: 475 suns at 9.86Rs
- 11% increase in umbra margin at closest approach: 5.82° umbra at 9.86Rs

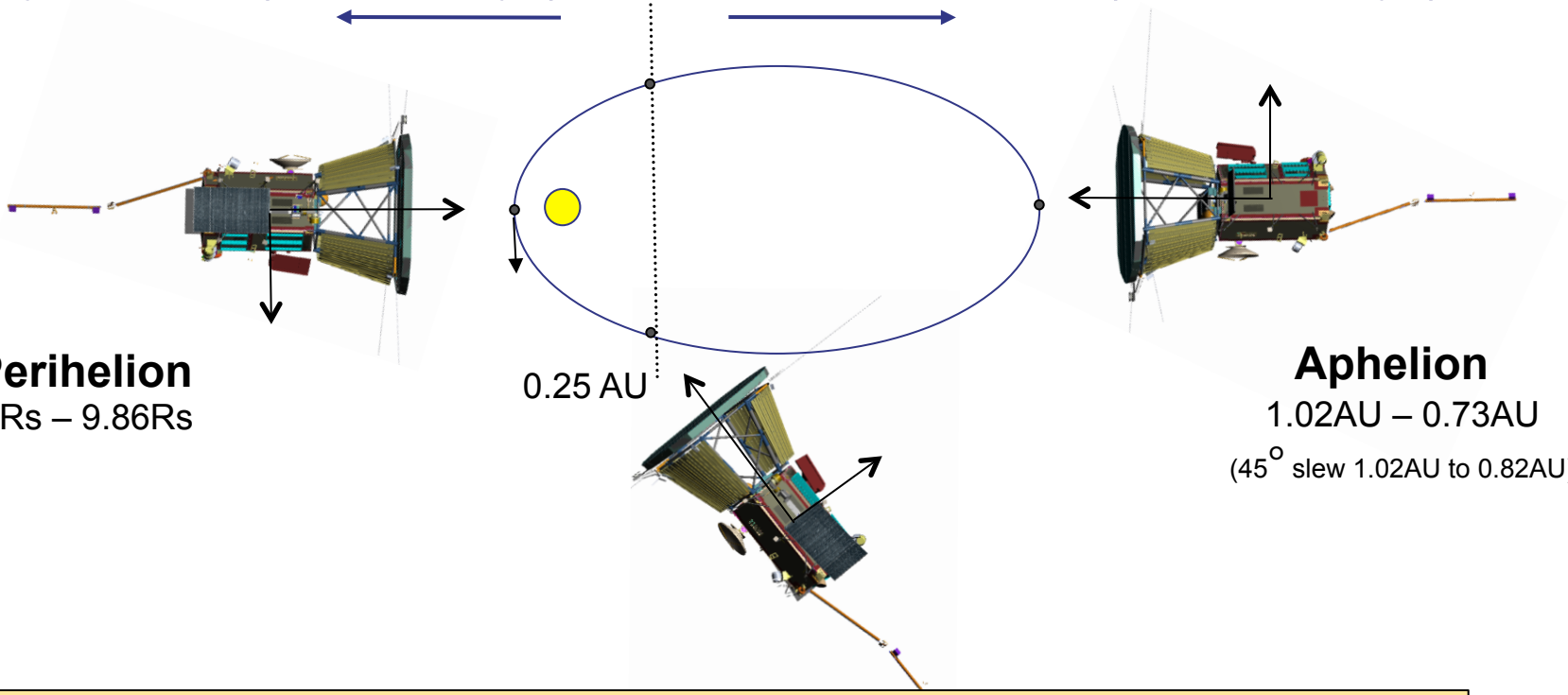
All other changes - insignificant

APL

SPP Orbit Configuration



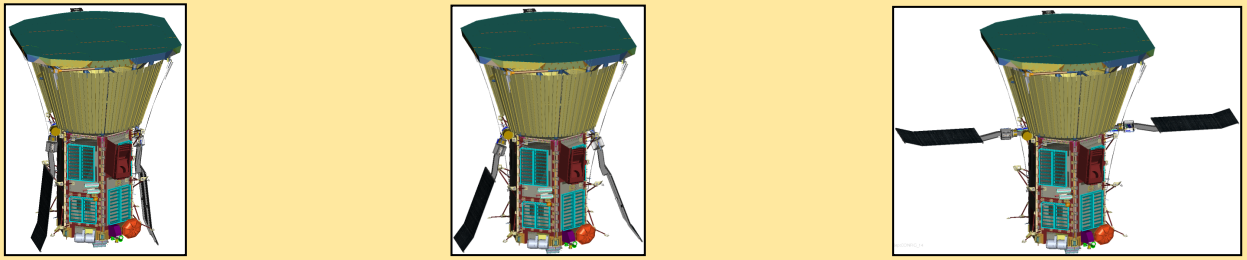
Primary Science (~11-12 days) ← → Cruise/Downlink (~156-78 days)



Perihelion
35.7Rs – 9.86Rs

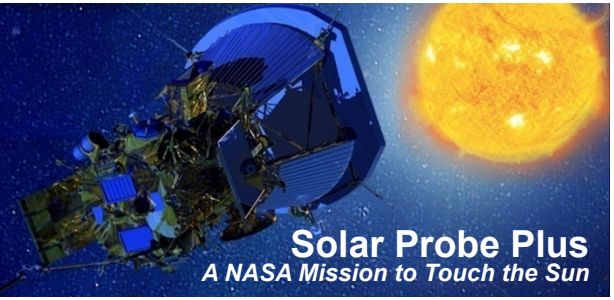
Aphelion
1.02AU – 0.73AU
(45° slew 1.02AU to 0.82AU)

Solar Array Position

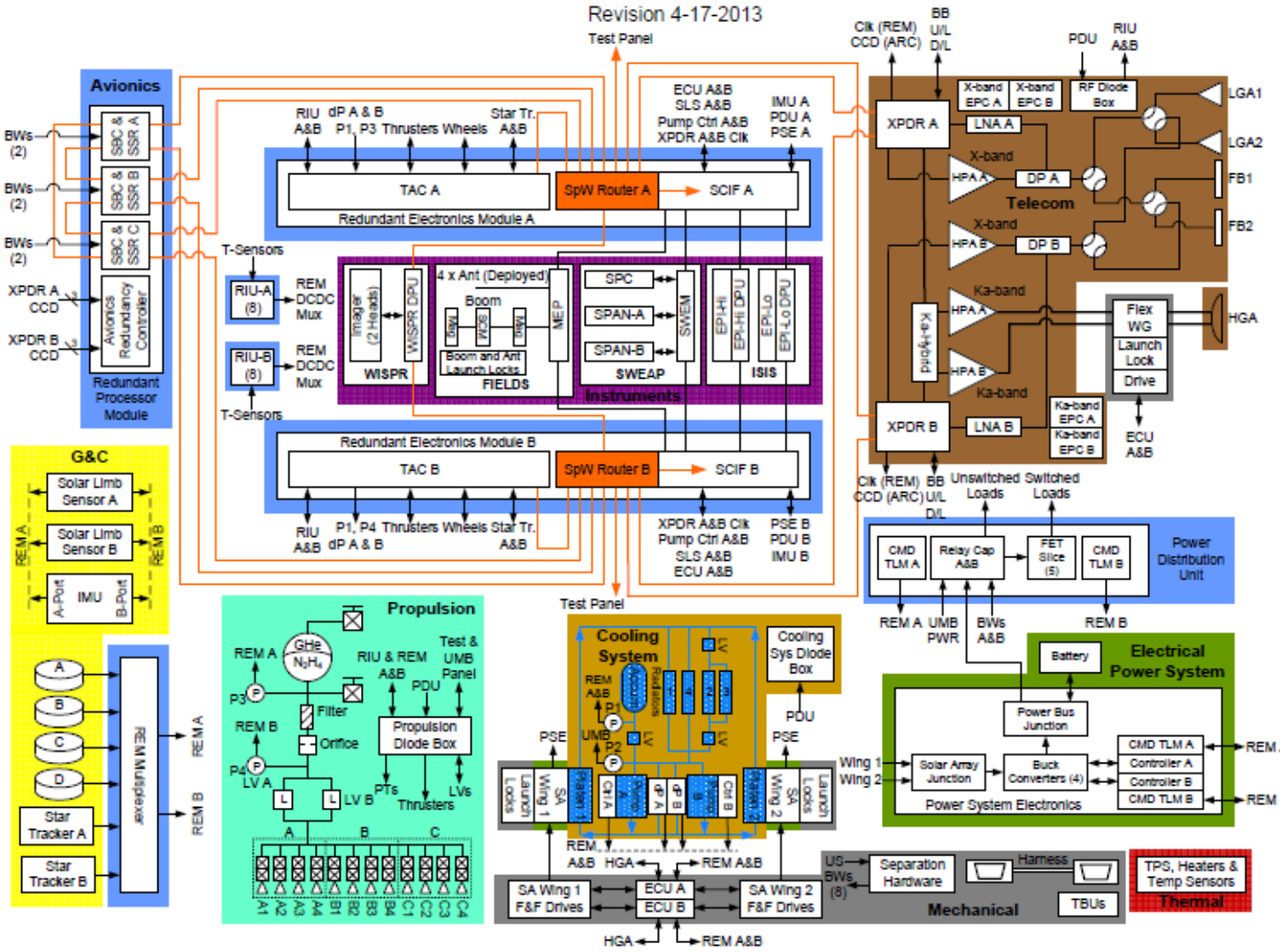


APL

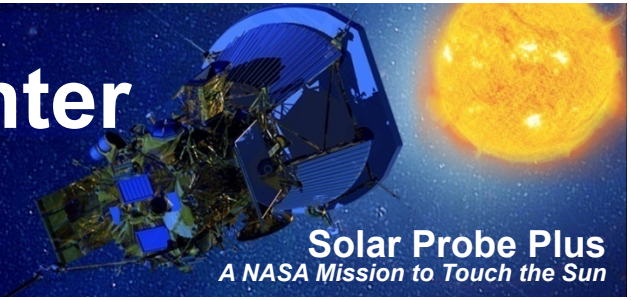
Block Diagram



Solar Probe Plus
A NASA Mission to Touch the Sun

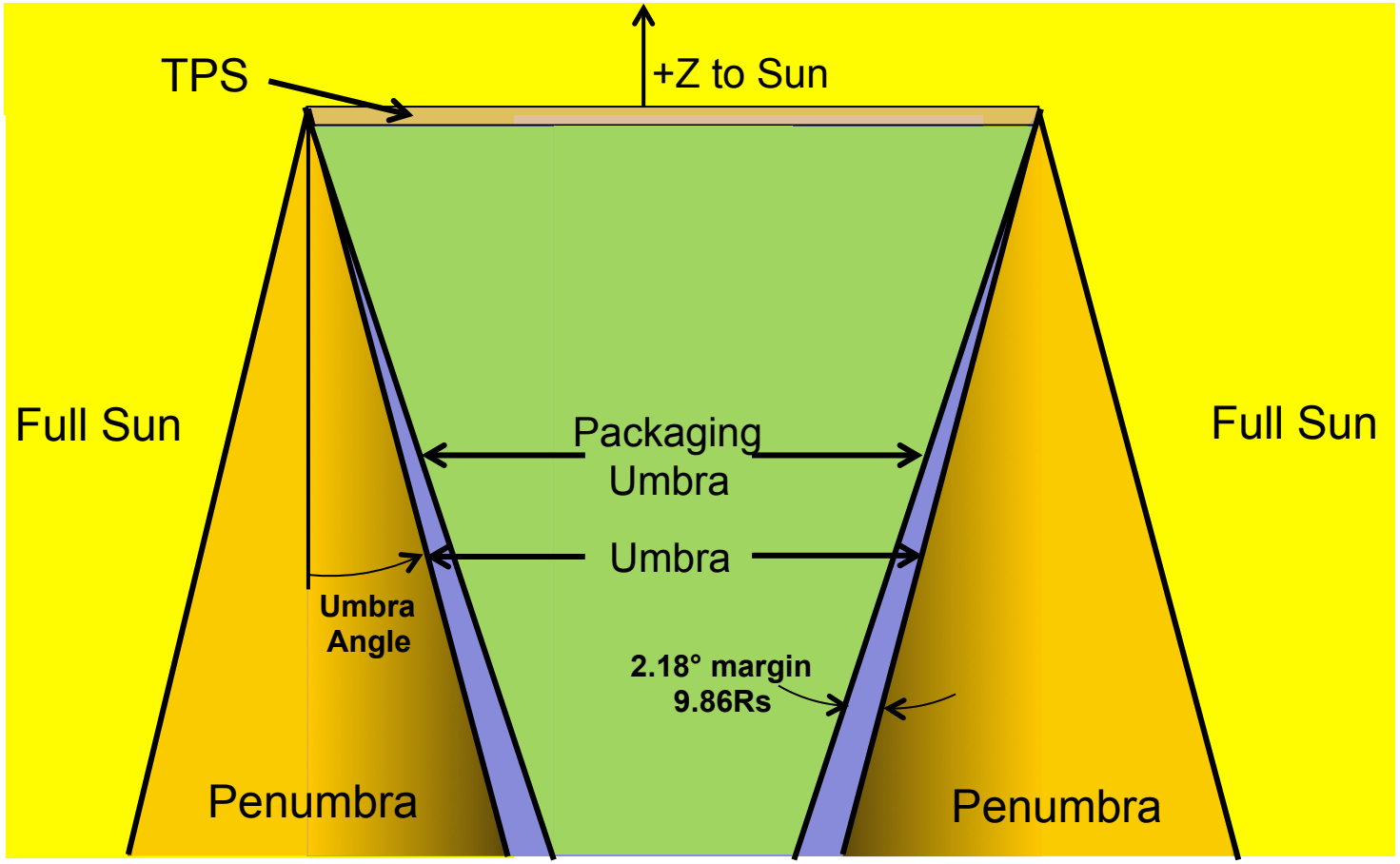


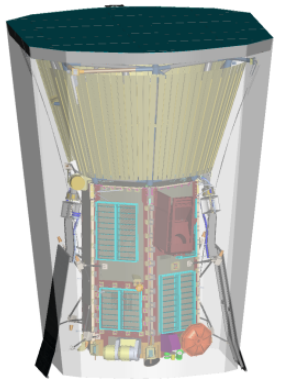
Protecting SPP During Encounter in Fault Conditions



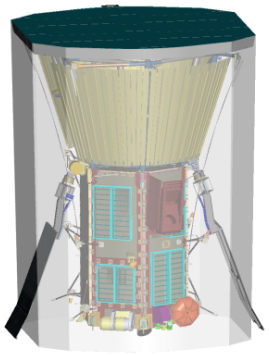
- Due to SPP solar environment, required fault response times preclude ground intervention to protect spacecraft
  - Faults response timeline requirements are measured in seconds and minutes
- Key autonomous fault management capabilities in event of fault
  - Ensures spacecraft is maintained within the TPS umbra
  - Ensures solar array and cooling system do not exceed survival temp limits – hot or cold
- Avionics architecture
  - Maximizes availability of sensors and actuators to G&C (spacecraft attitude and solar array angle control)
  - Supports time critical response timeline
- Additional sensors provide telemetry to support time critical fault detection
  - Solar limb sensors (SLS) provides direct measurement to warn of nearing umbra violation
  - Solar array Isc, Voc sensors, and cooling system temperature sensors warn of solar array or cooling system temperatures approaching survival limits.

Umbra, Penumbra



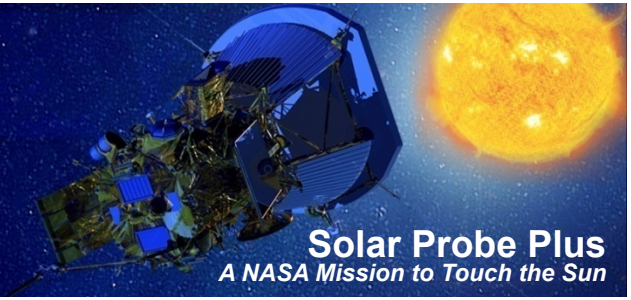


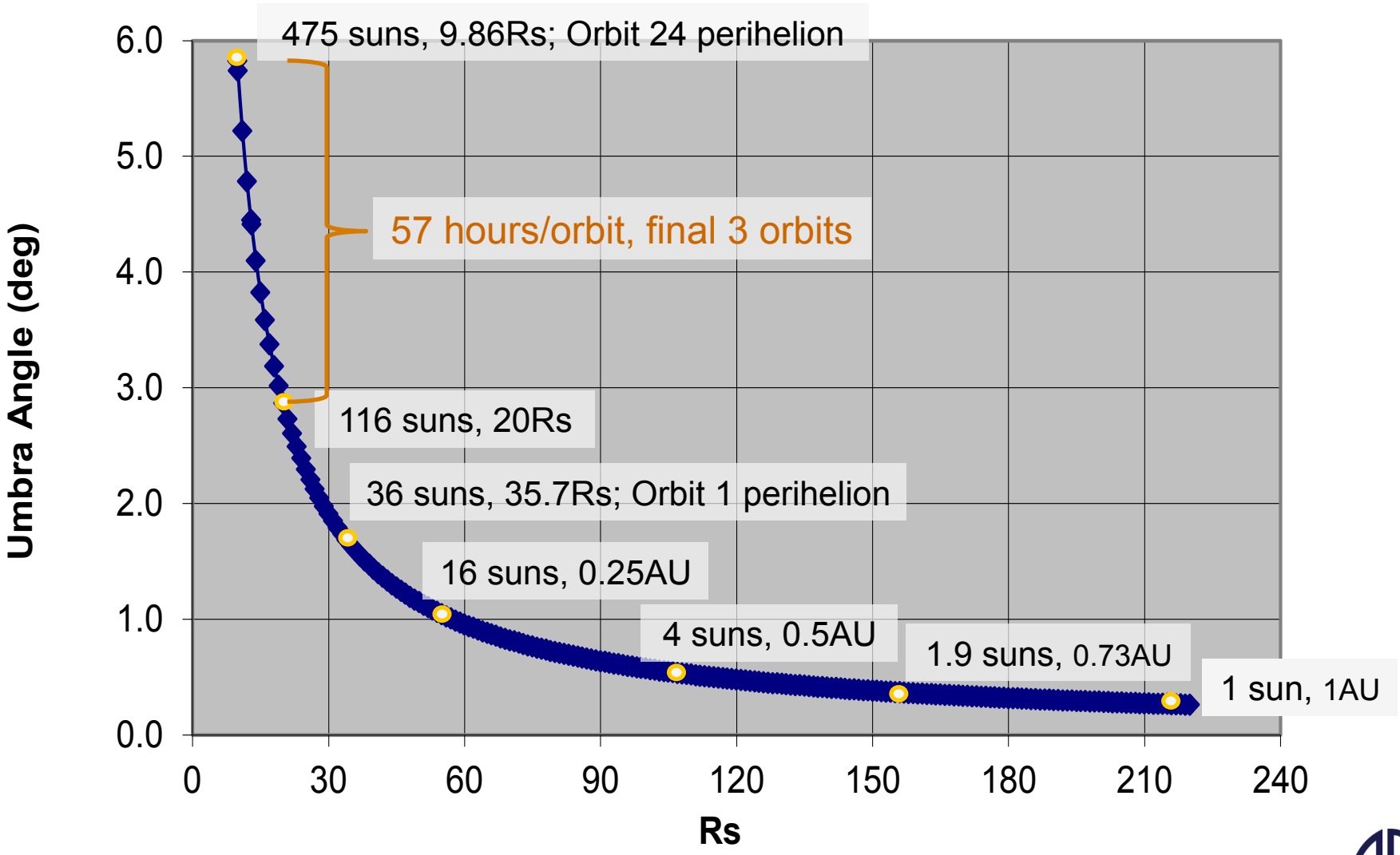
9.86Rs



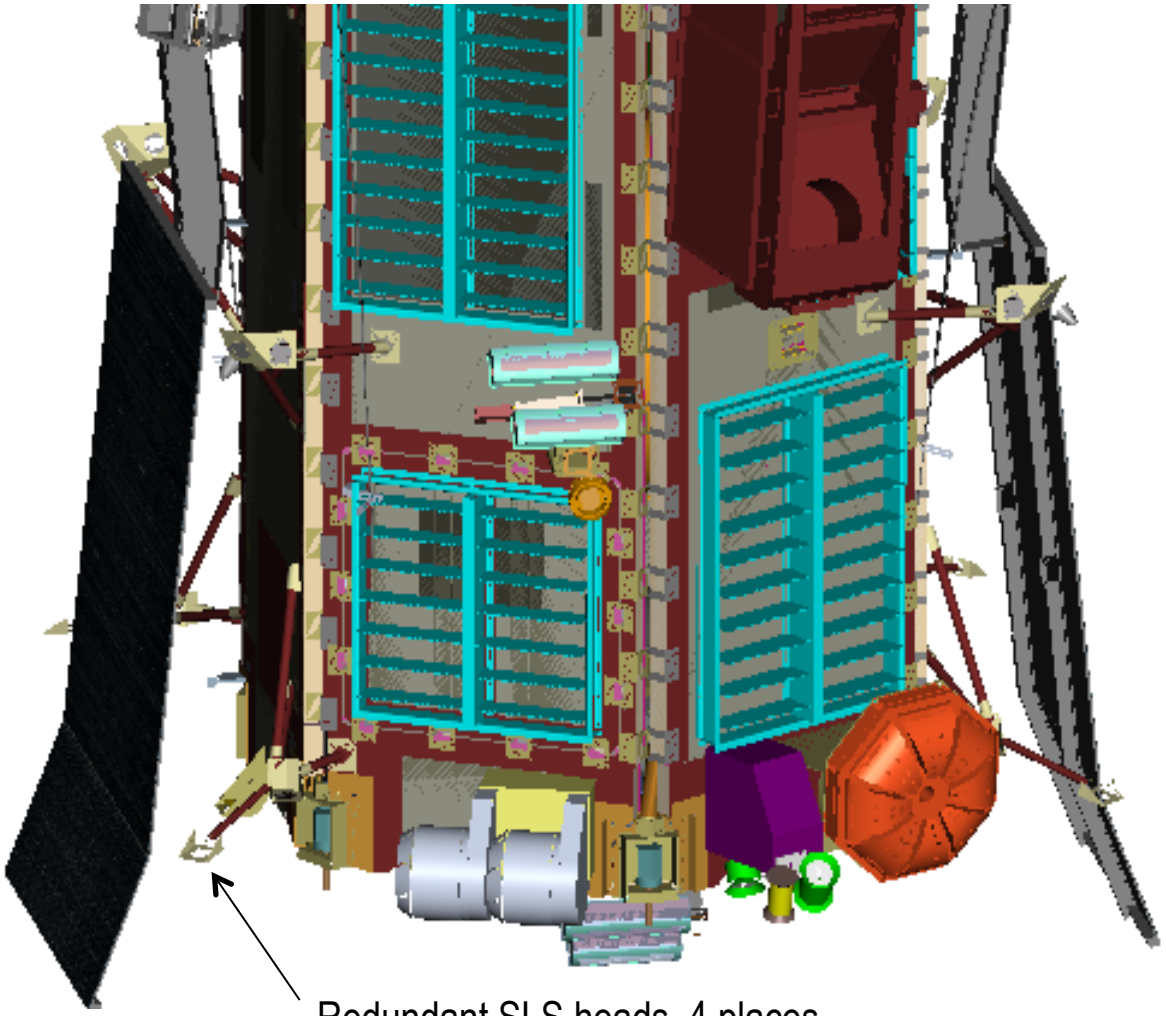
0.25AU

Solar Environment
Orbits 1, 24



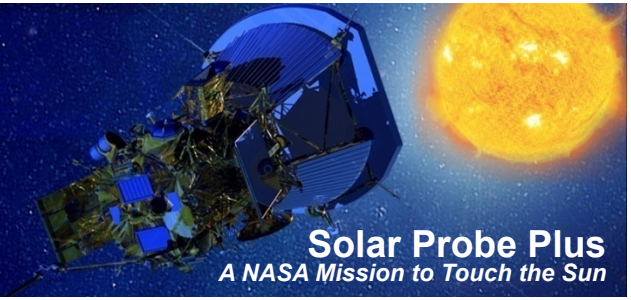


Solar Limb Sensors

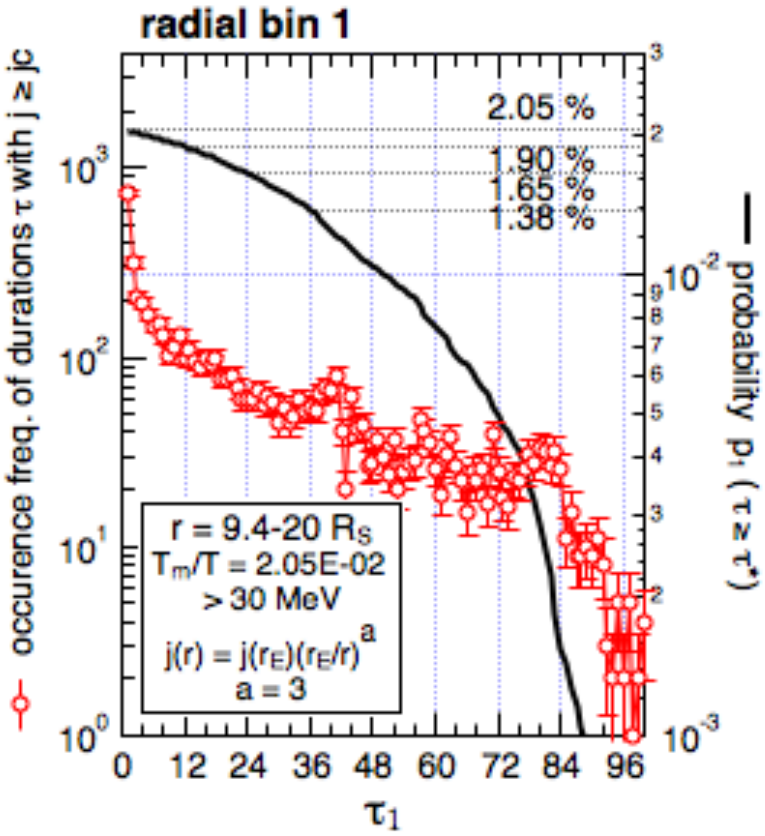


- Solar limb sensors (SLS) provide a warning of nearing umbra violation
- During encounter, SLS nominally do not see sun
- SLS sensors would become illuminated prior to any spacecraft component or instrument

Star Tracker Sensitivity to Energetic Protons



Probability that solar energetic protons intensities > 30 MeV will exceed 10^4 $(cm^2\ sec\ ster)^{-1}$ at 9.4 – 20Rs

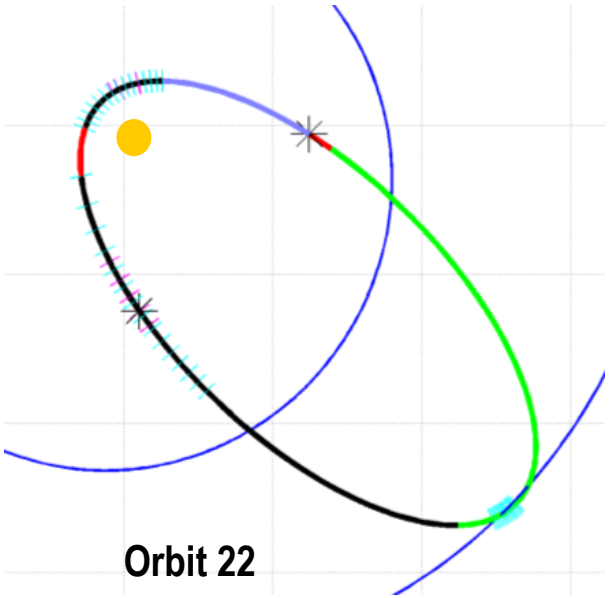


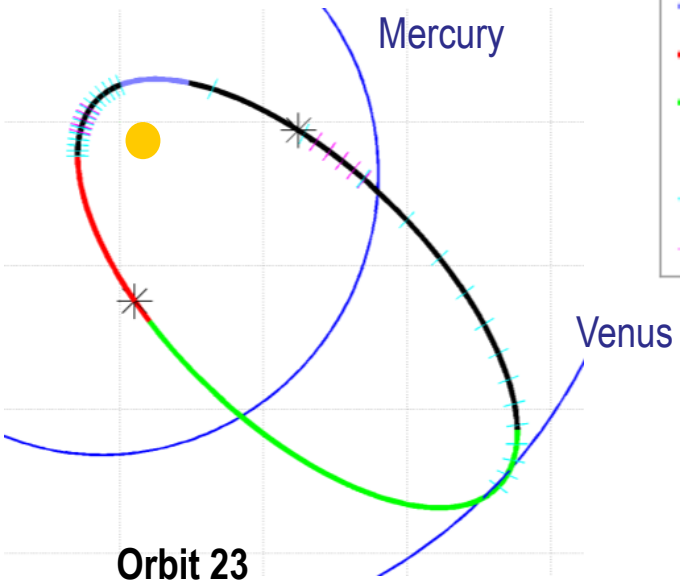
- Star trackers sensitive to ionization by energetic protons produced by SEP events in array images
- If proton flux is sufficiently intense (critical flux, j_c > 10^4 $(cm^2\ sec\ ster)^{-1}$), images suffer from "whiteout", resulting in loss of star tracker function until flux returns to operable levels.
- Sims using Earth-based data (conservative) show
  - Longest duration star tracker outages occur at closest solar distances
  - <2% probability that SEP event causing outage will have duration > 24 hours.
- During star tracker outage, spacecraft attitude propagated based on IMU gyros.
- Based on MESSENGER flight data, spacecraft attitude drift during a 24 hour outage is within SPP umbra margin.
- SPP IMU gyro reqs defined to accommodate 24 hour star tracker outage without umbra violation.
- SLS provides add'l protection against potential umbra violation

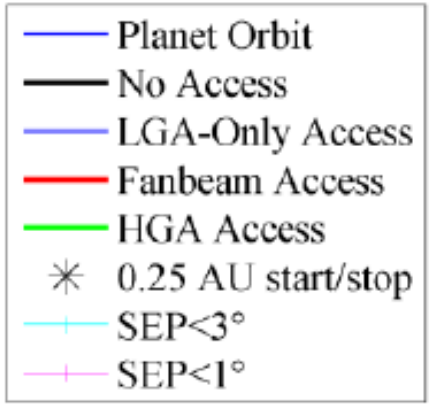
APL

Communication Outages

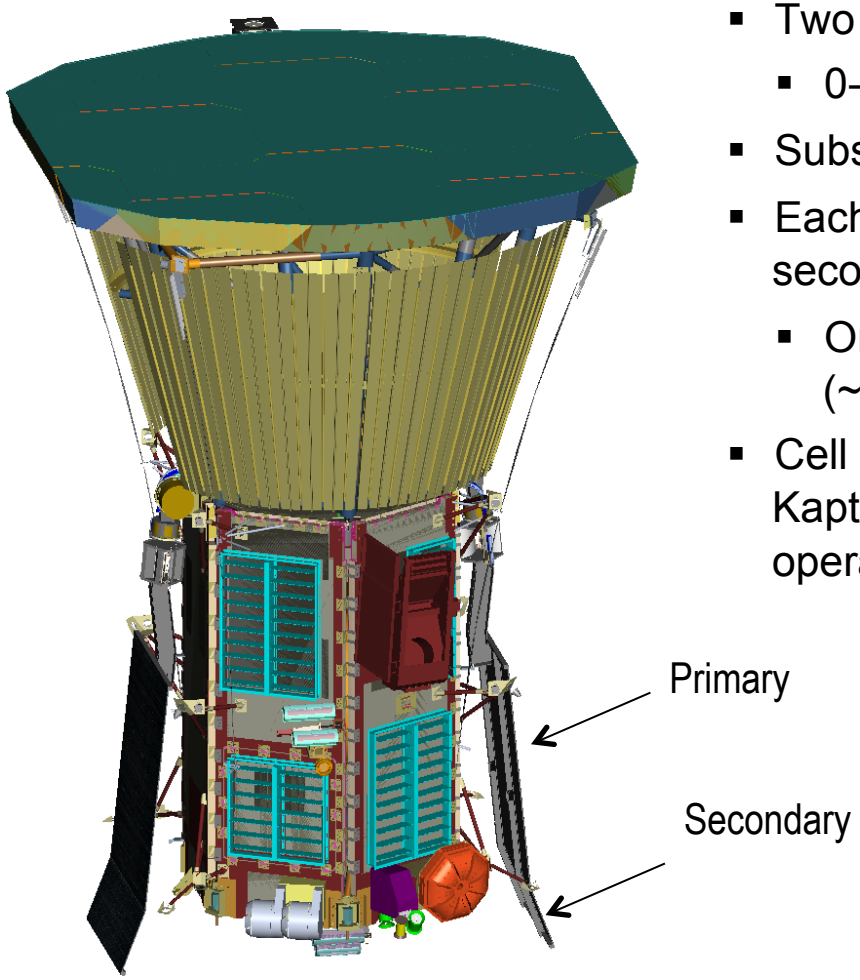
- Nominal contact frequency during encounter is 3x per week
- Contacts for science data downlink occur at solar distance >=.28AU, contact timing is orbit geometry dependent
- Long communication outages
  - Due to TPS blockage and SEP<3deg
  - Orbits 14-15; 18-19; 22-23 (shown)
  - Max outage duration 34 days





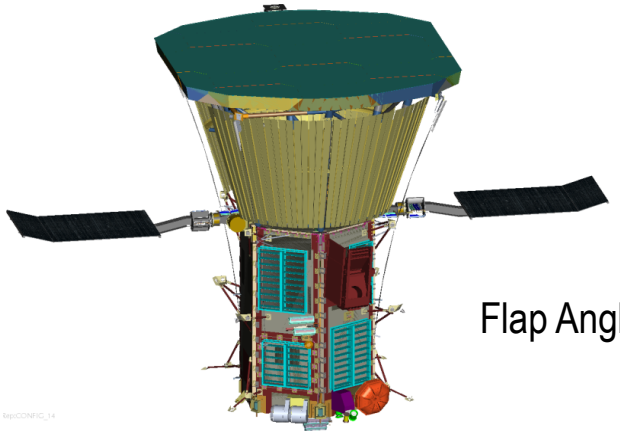


Solar Array



Flap Angle: ~81deg

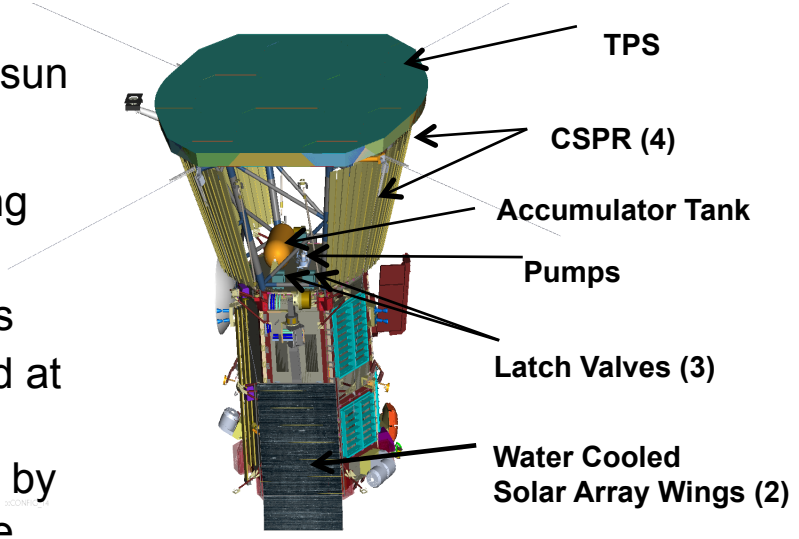
- Two deployable, articulated solar array wings
  - 0-90deg flap and +/-90deg feather
- Substrates (platens) are liquid cooled
- Each wing includes a primary section and a smaller secondary section at a fixed cant angle
  - Only the secondary section is illuminated at 9.86Rs (~25 suns)
- Cell stack uses ceramic “interposer” instead of usual Kapton insulator; substantially reduces cell stack operating temperatures at high irradiance

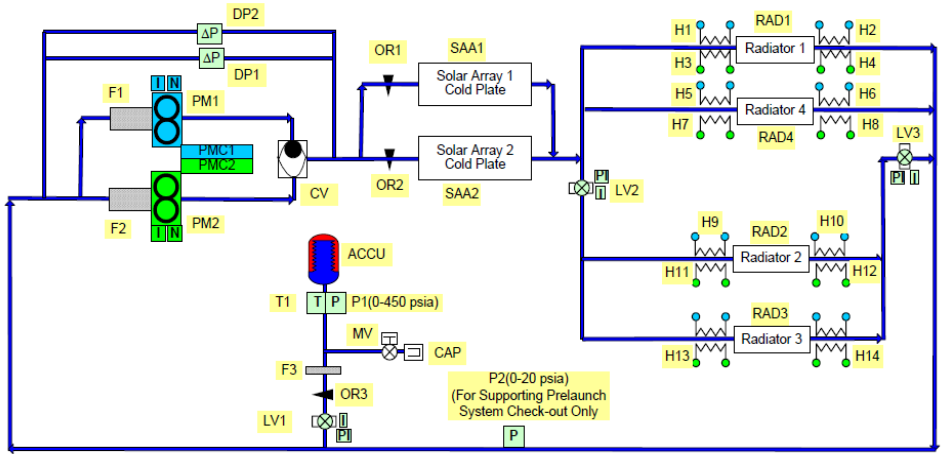


Flap Angle: 0deg

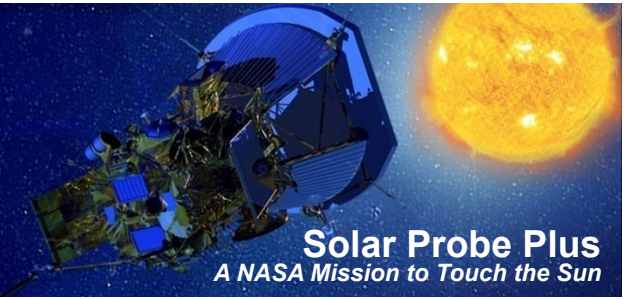
Solar Array Cooling System

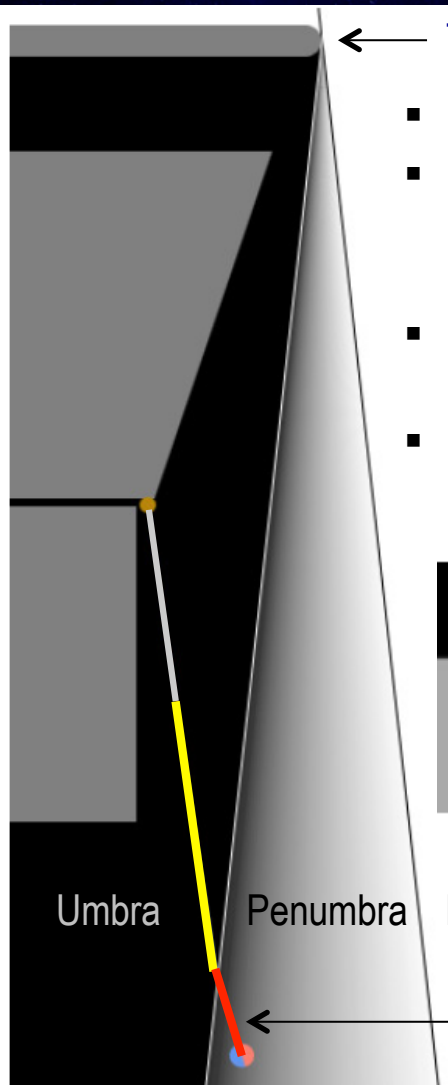
- SPP liquid cooling system dissipates high solar flux absorbed by solar array during closest approach to sun
  - 6480 W cooling system capacity
- Water pumped through solar array wings into cooling system primary radiators to dissipate heat.
- Single loop, redundant pump and control electronics
- Solar array fully extended at 1AU, partially extended at closest approach
- Cooling system operating temperatures determined by solar distance, spacecraft pointing, solar array angle, pump speed (2 speed)
- Thermal design drivers
  - 9.86Rs – max cooling system load
  - Communication 45deg slews
  - 0.73AU – 1.02AU Aphelion
  - Venus eclipse
  - Launch and post launch activation sequence



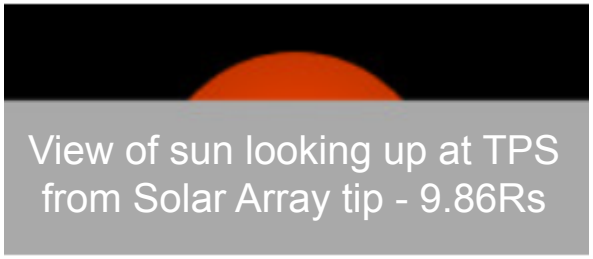


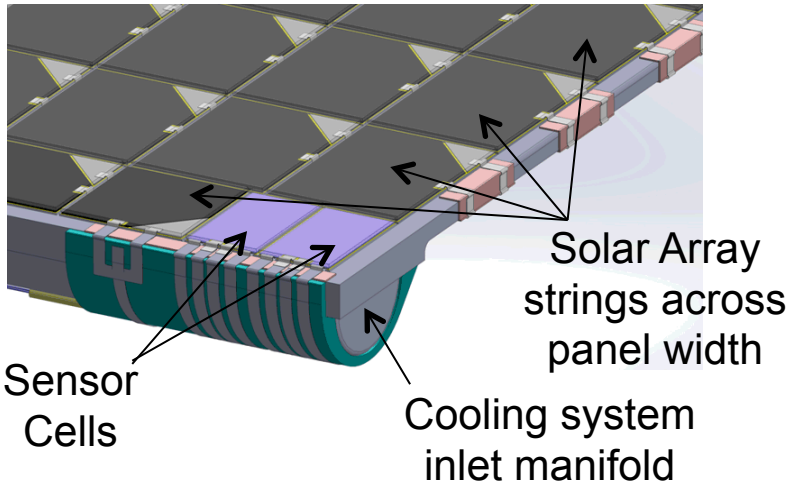
Solar Array Operation





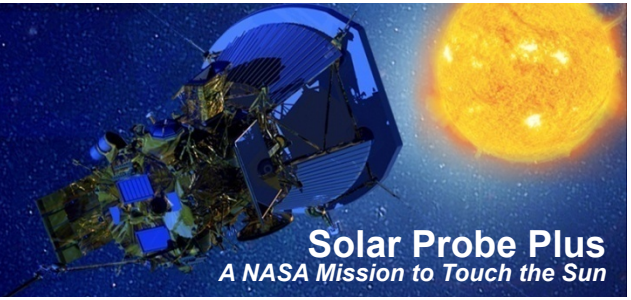
- Solar Array performance highly coupled to Cooling System, EPS, G&C
- High sensitivity of power, cooling system load to solar array wing angle
  - Electrical: 12.5 W/ 0.1° /wing
  - Thermal: 131.5 W/ 0.1° /wing (2% cooling system capacity)
- Autonomous wing angle control ensures power load is met while maintaining solar array and cooling system within thermal constraints
- Add'l sensors enable protection of solar array and cooling system from thermal violation (cooling system temp sensors not shown)





Note: Fig indicates 1 pair of sensor cells /wing corner; flight wing includes 2 pairs/wing corner

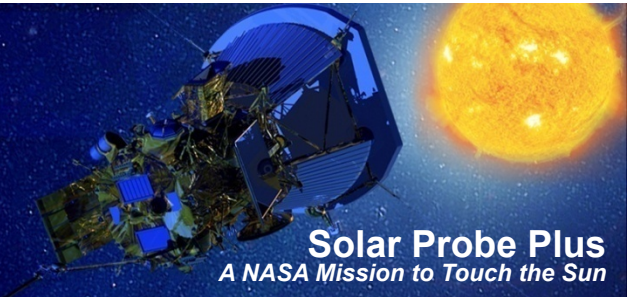
Review Scope and Related Reviews



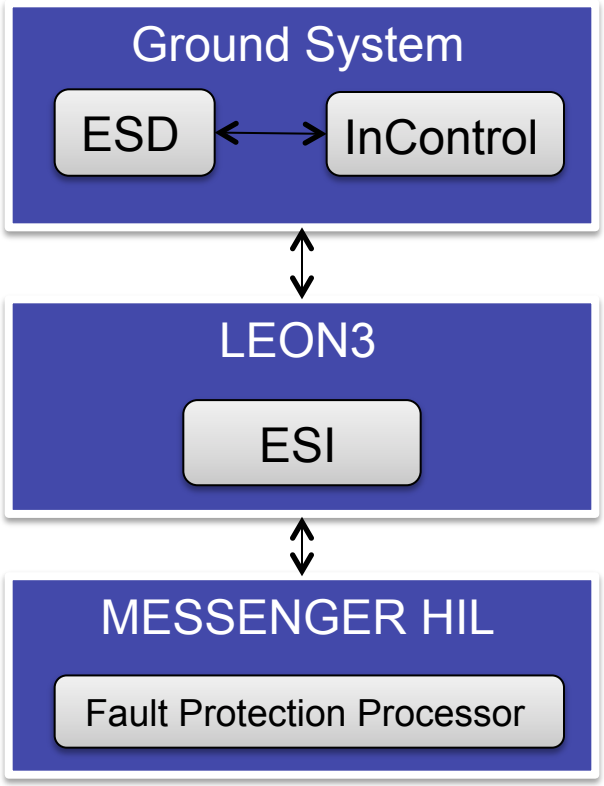
- To provide context, Fault Management Peer Review includes introductory subsystem material, however
  - Subsystems will be reviewed at Subsystem PDRs
    - Avionics architecture – reviewed as part of C&DH PDR
    - G&C – reviewed at G&C PDR
    - Solar array control – reviewed as part of Electrical Power System PDR
  - Subsystem PDRs will include:
    - Level 4 Fault Management Reqs
    - Preliminary design to meet Level 3 and 4 Fault Management Reqs
- Spacecraft Reqs Review will incorporate any modifications to requirements resulting from Fault Management Peer Review
  - Level 3 Fault Management Reqs are included within Level 3 Spacecraft Reqs Doc

- Not included in this review
  - Upper stage fault management – reviewed as part of Upper Stage PDR
  - Internal instrument fault management – reviewed as part of instrument PDRs
  - Autonomy - reviewed following Mission PDR, standard APL project approach

ExecSpec Autonomy System

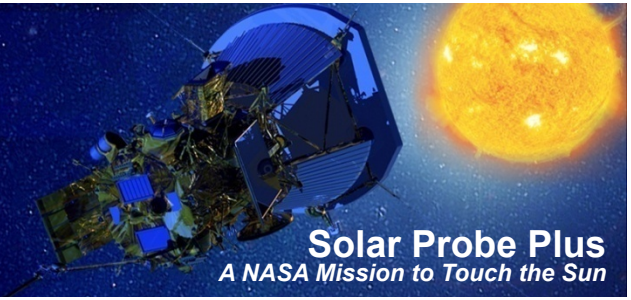


- Phase A Study Examined Advantages of ExecSpec
  - Domain Experts or system engineers draw state diagrams to represent desired behavior using interactive development environment (IDE)
  - Design can be easily reviewed
  - User-driven or user-scripted simulation
  - Automatic Verification based on project requirements
  - Diagrams uploaded into the spacecraft (no code)
  - On-board diagram interpreter
  - Design can be further modified in real-time at any time pre- or post-launch (no patching or recompiling)
  - Autonomy is visualized during test or flight by animating diagrams (same consistent interface from design to test to operate)
- Phase B Study Two-Prong Risk Reduction Effort
  - Verify ExecSpec can meet FSW operating constraints
  - Evaluate usability and advantages compared to rules and macros



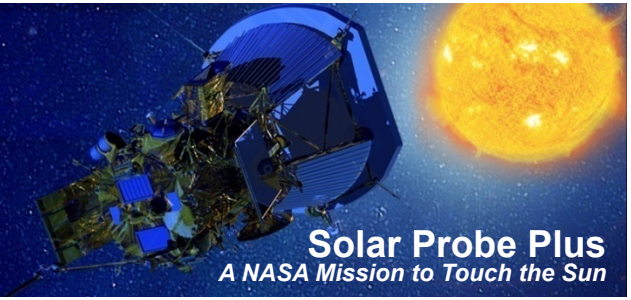
The Phase B risk reduction intercepts MESSENGER telemetry to operate ExecSpec Interpreter in a flight-like environment.

Additional Relevant Reviews



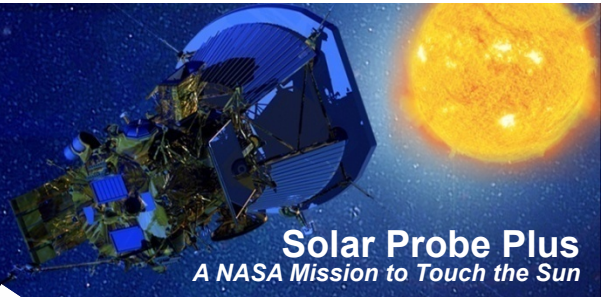
- 13May13 FMEA Review
- 21,22May13 FM Peer Review
- 12,13Jun13 Spacecraft Reqs Review
- 27Sep13 Propulsion Pre-PDR Review
- 9,10Oct13 Flight Software PDR
- 11Oct13 Mechanical PDR
- 18Oct13 Cooling System PDR
- 21Oct13 Thermal PDR
- 22Oct13 Ground System PDR
- 24Oct13 SpaceWire PDR
- 25Oct13 Telecom PDR
- 29Oct13 PDU PDR
- 31Oct13 Solar Array PDR
- 4Nov13 Ground Software PDR
- 8Nov13 Electrical Power System PDR
- 11Nov13 C&DH PDR
- 12Nov13 G&C PDR
- 6-8Jan14 Mission PDR
- 22Apr14 Autonomy PDR

Backup



APL

Orbit Phases: Orbits 1 - 5



Solar Probe Plus
A NASA Mission to Touch the Sun

Ram

S/C to Sun

S/C Coord (translated to ~center of gravity, cg)

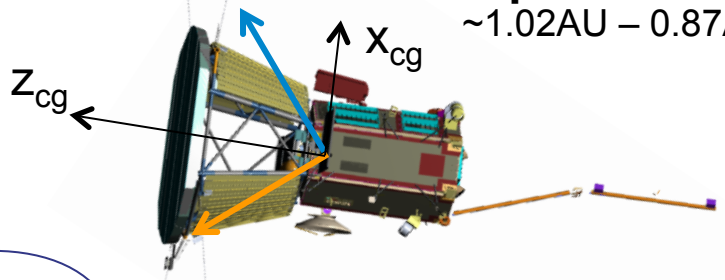
Cruise/Downlink ~156-108 days

Primary Science ~12 days

0.25 AU

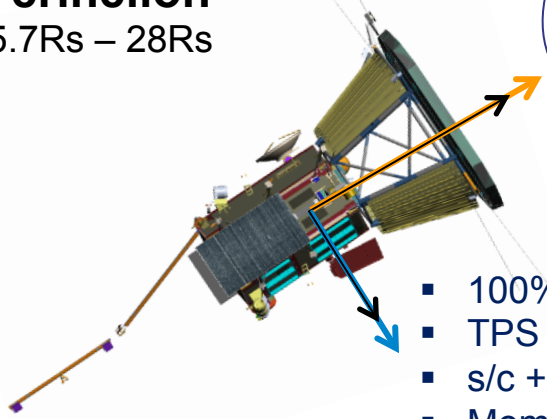
0.25 AU

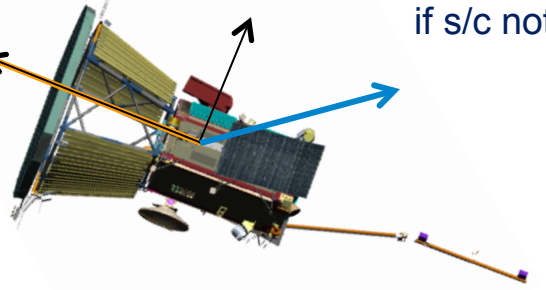
Aphelion
~1.02AU – 0.87AU



- DL science data
- TPS to sun except, slews
  - >0.82AU (thermal)
  - cooling system activation
  - >0.7AU (data DL)
- s/c rotates about s/c-sun line
- Power avail for inst <0.82AU if s/c not DL data, etc

Perihelion
~35.7Rs – 28Rs

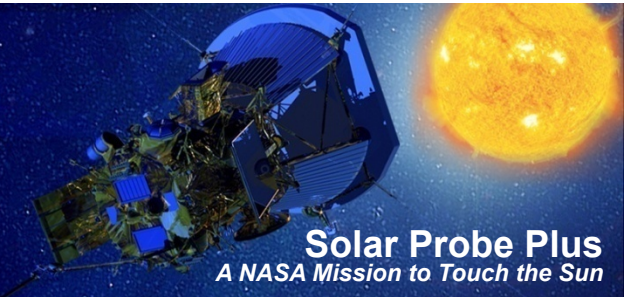




- 100% inst duty cycle
- TPS to sun
- s/c +x near ram
- Momentum dumps

APL

Orbit Phases: Orbits 6 - 24



Solar Probe Plus
A NASA Mission to Touch the Sun

Ram

S/C to Sun

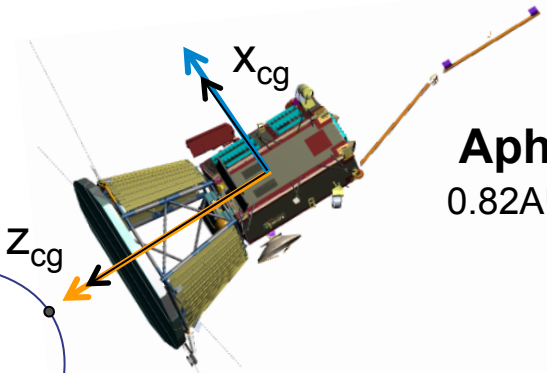
S/C Coord (translated to ~center of gravity, cg)

Cruise/Downlink ~100-78 days

Primary Science ~12-11 days

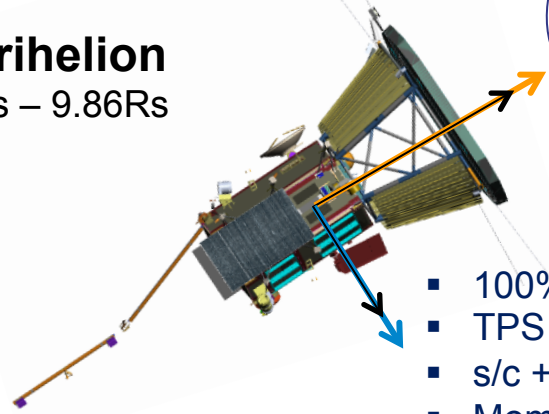
0.25 AU

0.25 AU

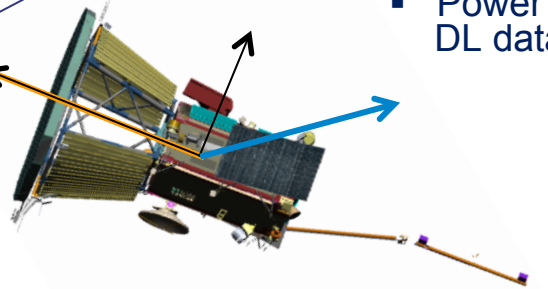


Aphelion
0.82AU – 0.73AU

- DL science data
- TPS to sun except, slew
  - >0.7AU (data DL)
- s/c rotates about s/c-sun line (momentum management)
- Power avail for inst if s/c not DL data, etc



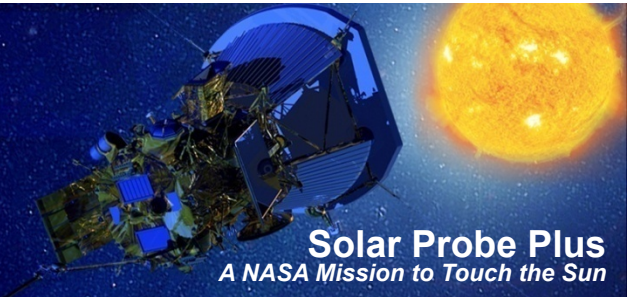
Perihelion
~21Rs – 9.86Rs



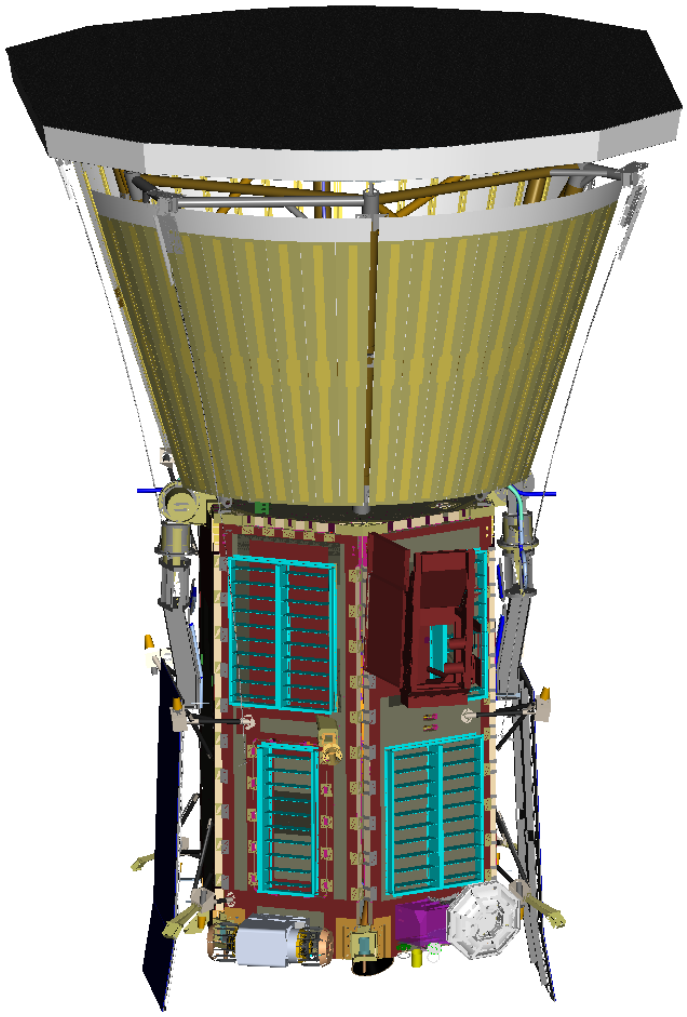
- 100% inst duty cycle
- TPS to sun
- s/c +x near ram
- Momentum dumps

APL

Spacecraft Overview



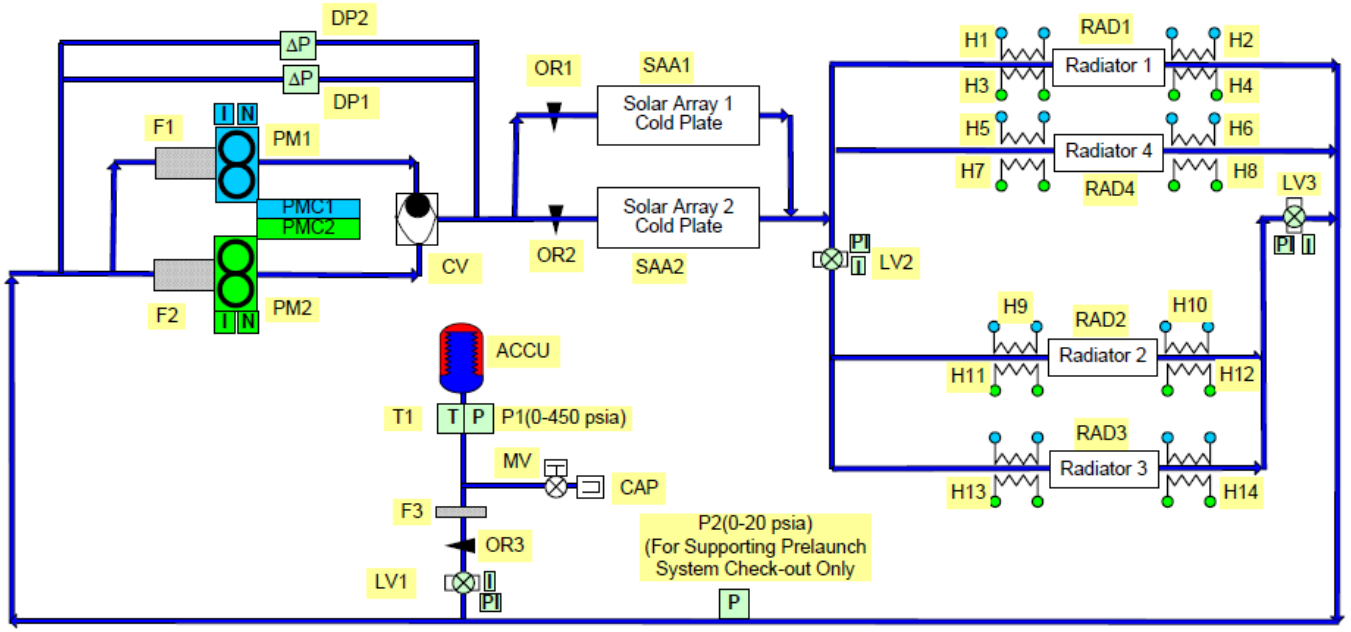
Solar Probe Plus
A NASA Mission to Touch the Sun



- NASA selected instrument suites
- 665kg max launch wet mass
- Reference Dimensions:
  - S/C height: 3m (TBR)
  - TPS max diameter:2.3m (TBR)
  - S/C bus diameter: 1m (TBR)
- C-C Thermal protection system
- Hexagonal prism s/c bus configuration
- Actively cooled solar arrays
  - 364W (TBR) electrical power at encounter
  - Solar array total area: 1.54m^2 (TBR)
  - Radiator area under TPS: 4.4m^2 (TBR)
- 0.6m HGA, 34W TWTA Ka-band science DL
- Science downlink rate: 163kb/s (TBR) at 1AU
- Blowdown monoprop hydrazine propulsion
- Wheels for attitude control

APL

Cooling System Schematic



Manual Valve (MV)

Fixed Flow Resistance (ORx)

Check Valve (CV)

Valve Cap

Heater (Hx)

Latching Valve (LVx) with One Redundant Coils to Open and Single Coil to Close - Electrically Actuated

Pump Assembly, Including Motor (PMx)

Accumulator Tank (ACCU)

Filter (Fx)

ΔP Pressure Differential Sensor (DPx)

T Temperature Sensor (Tx)

P Pressure Sensor (Px)

N Speed Sensor

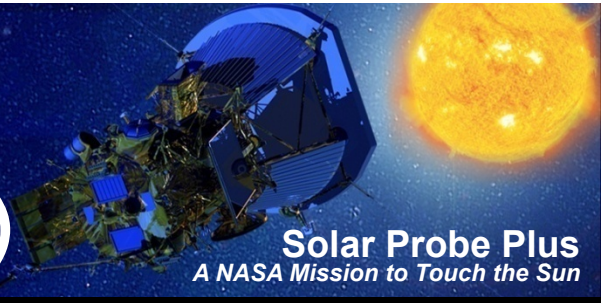
I Current Sensor

PI Position Indicator Sensor

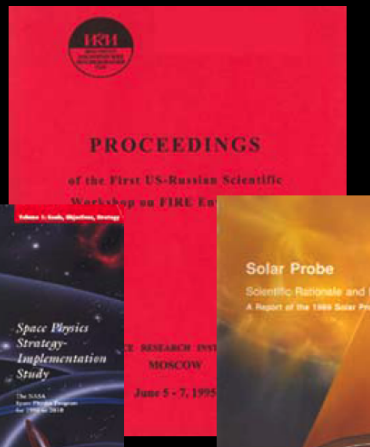
Water

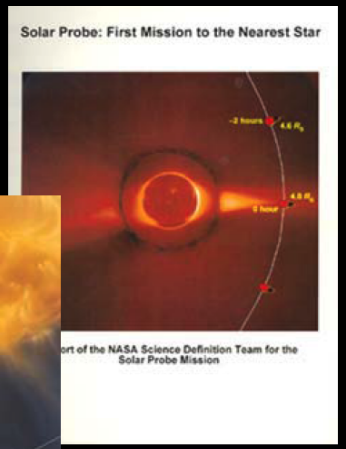
Nitrogen

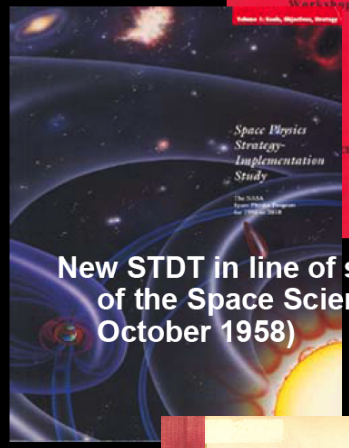
Solar Probe History (1958 - present)



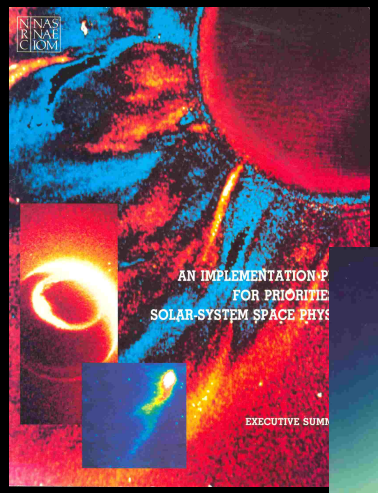
Solar Probe Plus
A NASA Mission to Touch the Sun

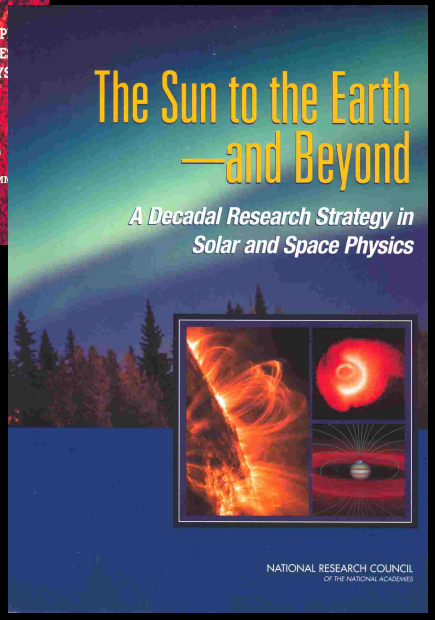


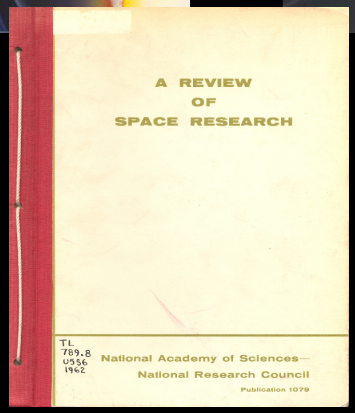


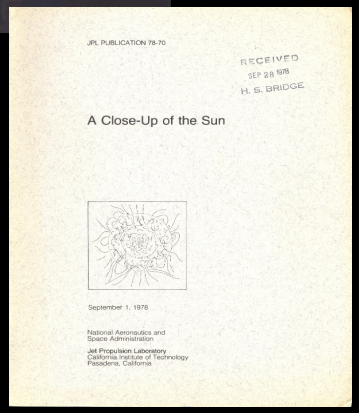


New STDT in line of studies dating back to "Simpson's Committee" of the Space Science Board (National Academy of Sciences) (24 October 1958)



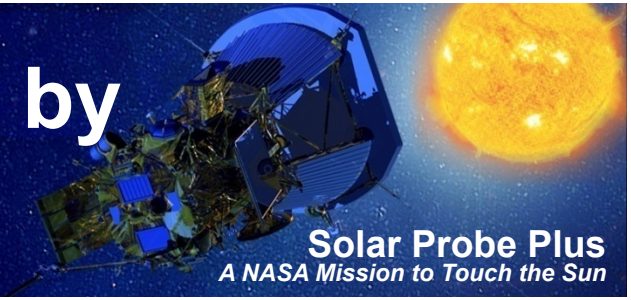






Solar Probe studies, reports; NAS: 1962, 1985, 1995, 2003

Science Questions Addressed by Solar Probe Plus



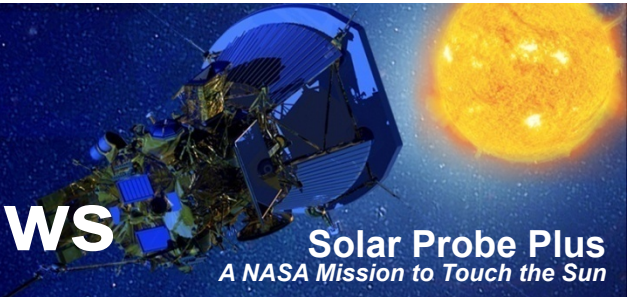
Overarching Science Objective

- To determine the structure and dynamics of the Sun's coronal magnetic field, understand how the solar corona and wind are heated and accelerated, and determine what mechanisms accelerate and transport energetic particles.

Detailed Science Objectives

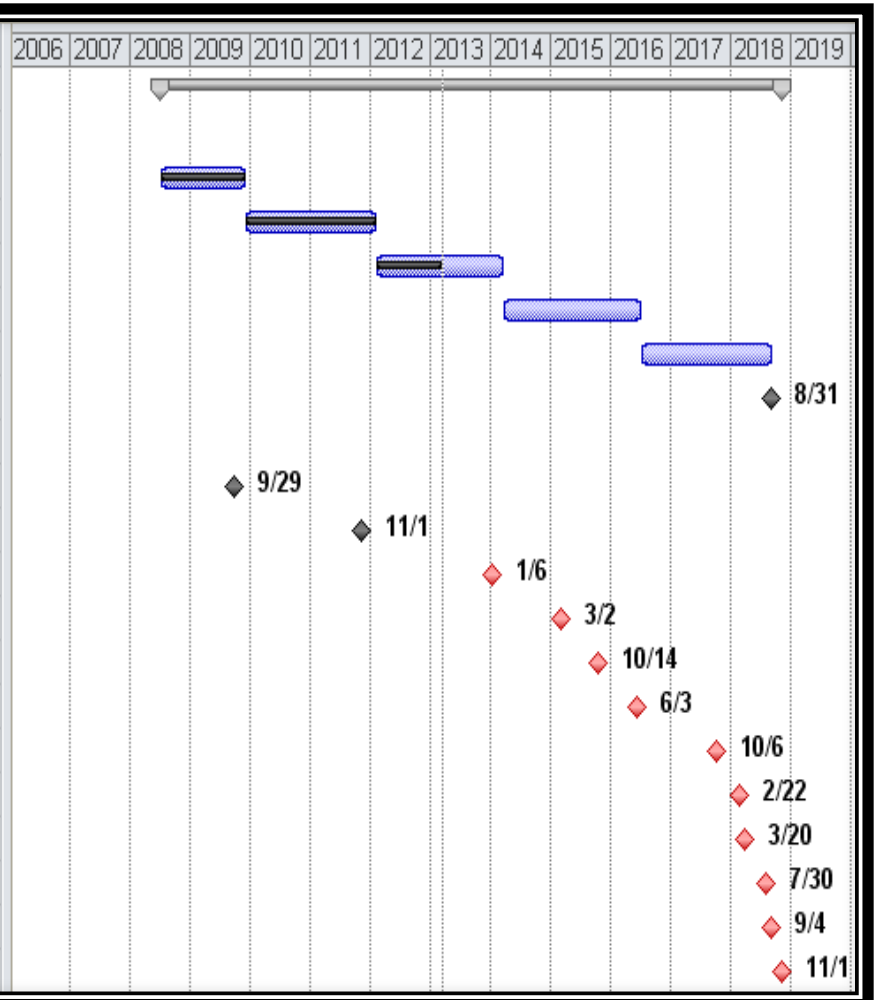
- Trace the flow of energy that heats and accelerates the solar corona and solar wind.
- Determine the structure and dynamics of the plasma and magnetic fields at the sources of the solar wind.
- Explore mechanisms that accelerate and transport energetic particles.

Phase Duration and Key Reviews



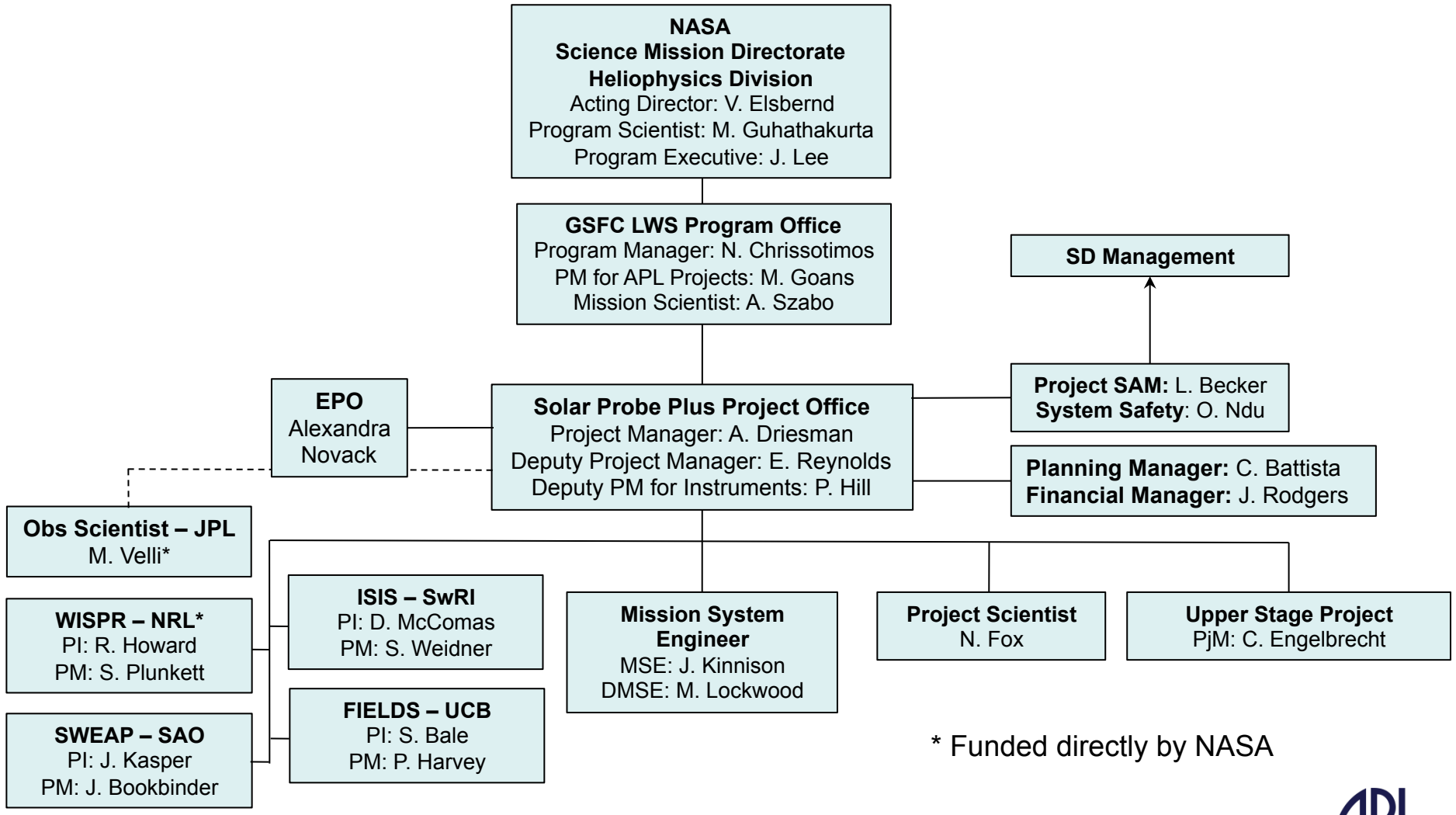
Solar Probe Plus
A NASA Mission to Touch the Sun

Task Name	Start	Finish
Solar Probe Plus Mission Schedule	**7/2/08**	**11/1/18**
Mission Phases	**7/2/08**	**8/31/18**
Pre-Phase A	7/2/08	12/1/09
Phase A	12/2/09	1/31/12
Phase B	2/1/12	3/14/14
Phase C	3/15/14	6/23/16
Phase D	6/24/16	8/30/18
Phase E Start (Ends 9/1/25)	8/31/18	8/31/18
Mission-Level Milestones	**9/29/09**	**11/1/18**
MCR	9/29/09	9/30/09
MDR	11/1/11	11/3/11
PDR	1/6/14	1/8/14
CDR	3/2/15	3/4/15
MOR	10/14/15	10/14/15
SIR	6/3/16	6/3/16
PER	10/6/17	10/6/17
PSR	2/22/18	2/22/18
ORR	3/20/18	3/20/18
LRR/LRD	7/30/18	7/30/18
Orbital Checkout Complete	9/4/18	9/4/18
First Perihelion	11/1/18	11/1/18



Solar Probe Plus Organizational Chart

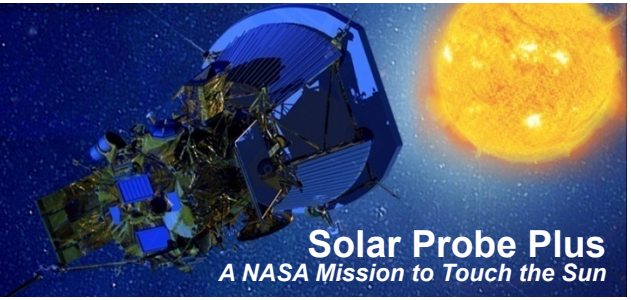
Solar Probe Plus
A NASA Mission to Touch the Sun

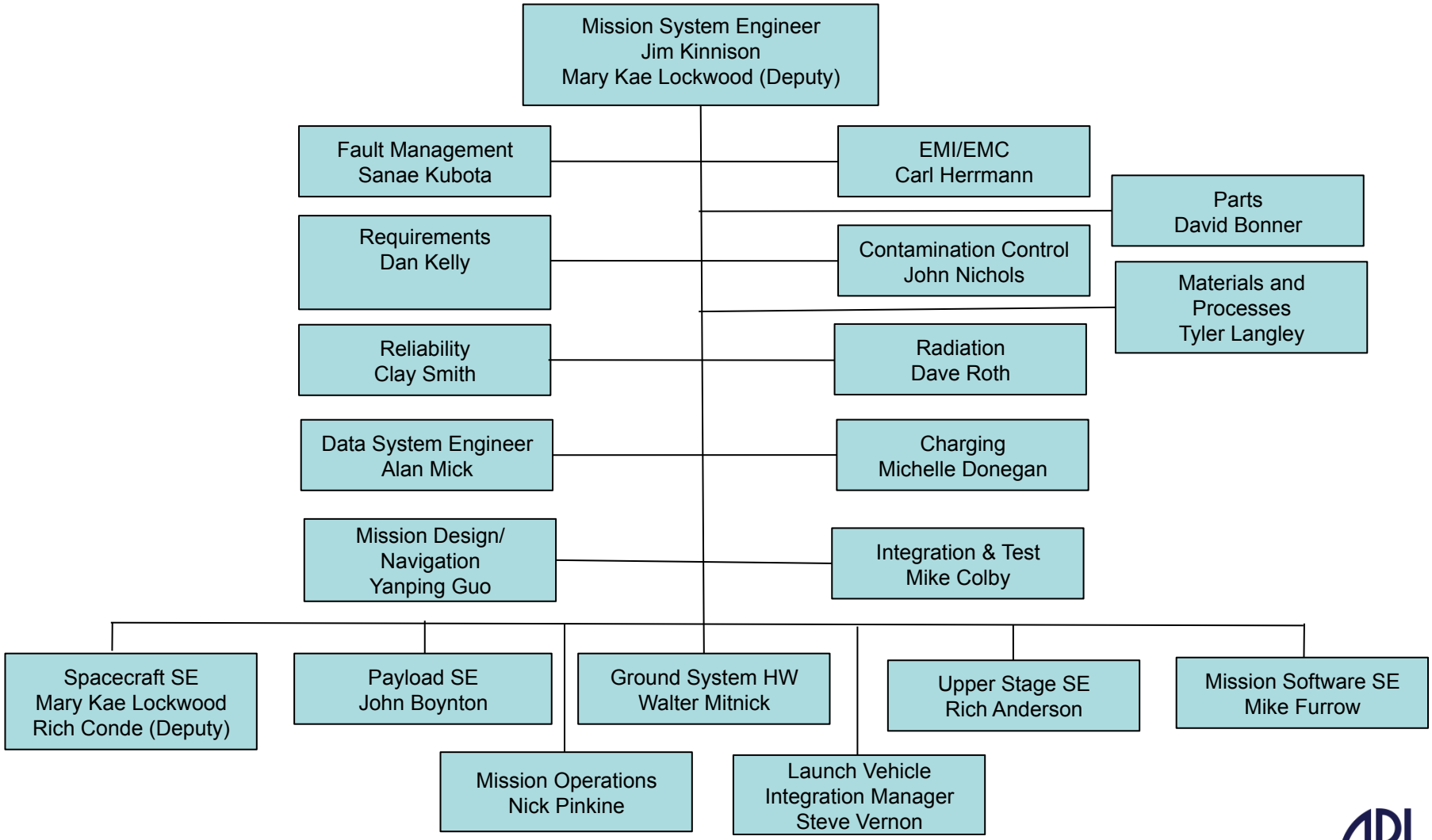


* Funded directly by NASA

APL

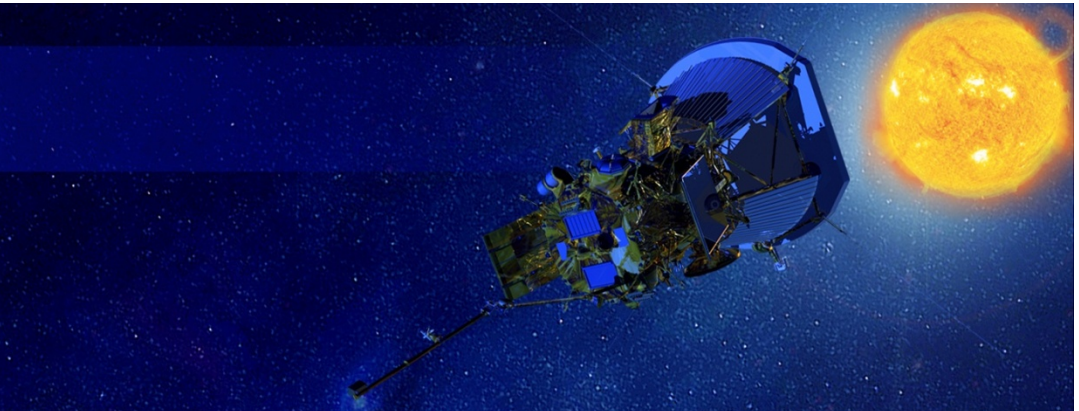
System Engineering Organization





Solar Probe Plus

A NASA Mission to Touch the Sun

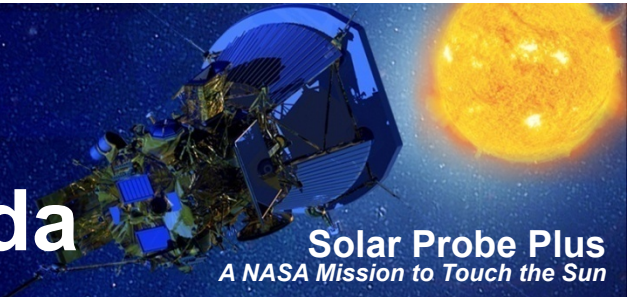


Fault Management Preliminary Design

Sanae Kubota
FM Lead Engineer
sanae.kubota@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

FM Preliminary Design - Agenda

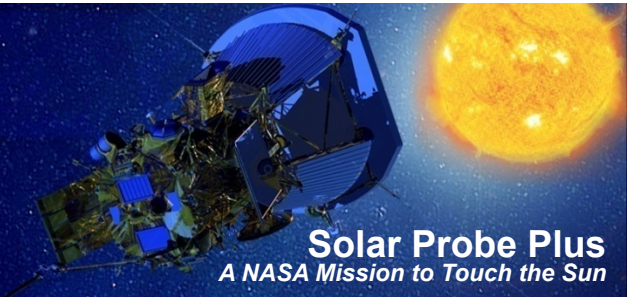


Solar Probe Plus
A NASA Mission to Touch the Sun

An overview of the SPP FM architecture and how it is mapped with requirements

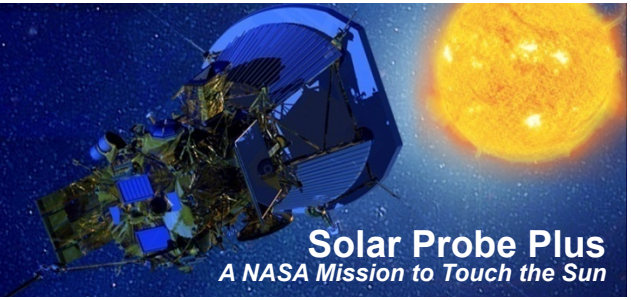
FM Architecture	L3 Requirements group
Redundancy concept	Redundancy Continuity of control
Avionics architecture: design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios Safing concept / FM modes Ground intervention concept	Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM	Instrument FM

FM Design: Redundancy Concept



FM Architecture		L3 Requirements group
Redundancy concept		Redundancy Continuity of control
Avionics architecture:	design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios Safing concept / FM modes Ground intervention concept		Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM		Instrument FM

Redundancy Concept



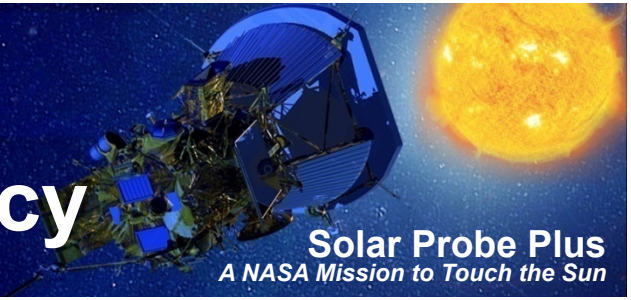
- **Per Level 1 requirement, the SPP mission is classified as risk category B as defined by NPR 8705.4, Risk Classification for NASA Payloads.**
  - Essential spacecraft functions and key instrument measurements are typically fully redundant for category B missions.
  - Critical single point failures for Level 1 requirements may be permitted, but are minimized and mitigated by the use of high reliability parts and additional testing.

- **Level 2 requirement: The Mission shall have no single point failures except those on the single point failure list.**
  - Exceptions to single fault tolerance will be managed by the SPP reliability engineer.

- **SPP does not consider a processor reset to be a failure.**
  - Single fault tolerance includes the ability to maintain attitude control during a processor reset, and even if one processor has failed.
  - Drives the design of a unique avionics architecture for SPP.

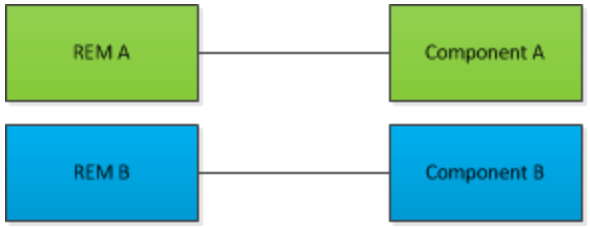
- **SPP preference is for block redundancy of components to avionics, with cross-strapping implemented as time-criticality or component-specific interface issues warrant.**
  - Block redundancy offers fewer configurations, and is typically lower mass; simplicity of design favors testability and reliability.

Overview: Types of Redundancy



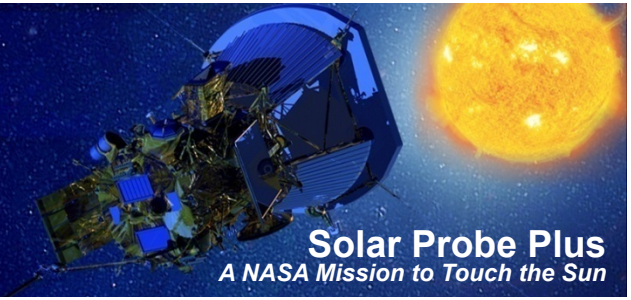
- **Block redundant**
- **Cross-strapped**
- **Cross-strapped internally redundant unit**

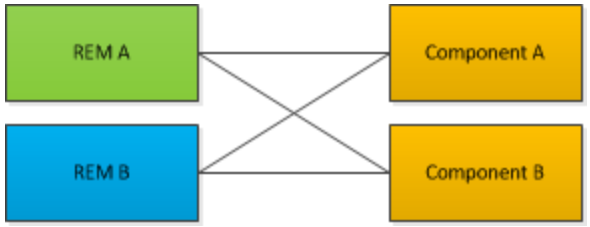
Redundant Interface Types: Block Redundant



- **Component A accessible only from REM A; Component B accessible only from REM B**
- **Failure of *any* A-side component requires switch of *all* A-side components**

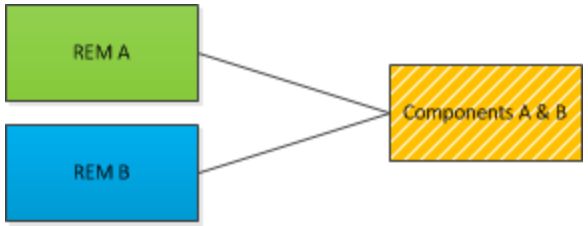
Redundant Interface Types: Cross-Strapped





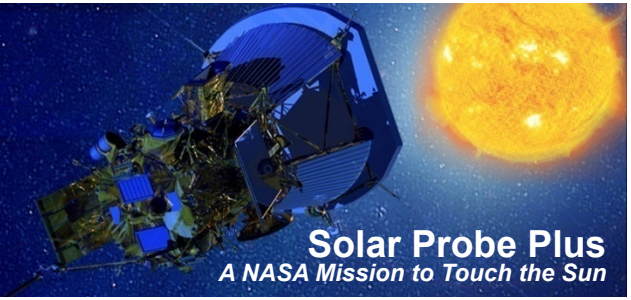
- Component A accessible from REM A or REM B; Component B accessible from REM A or REM B
- Failure of a cross-strapped component does not require REM (and associated block) side-switch
- REM side switching does not require switching of a cross-strapped component
- Both Component A and Component B may be accessed from a single active REM if necessary

Redundant Interface Types: Cross-Strapped Internally-Redundant unit



- Internal redundancy connects Components A and B, and the aggregate unit is accessible from REM A or REM B.
- Failure of part of an internally redundant unit is handled internally and does not require a REM (and associated block) side switch.
- REM side switching does not require switching of active components within an internally redundant unit

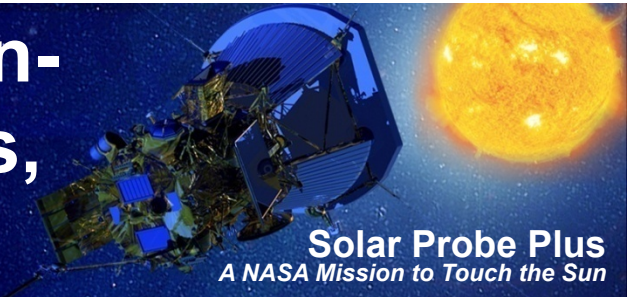
Component-Avionics Interface Types



Block	Cross-Strapped	Cross-Strapped Internally Redundant
PDU	Processors	IMU* (need 3 of 4 gyros & accels)
PSE (includes platen temp sensors & Isc, Voc measurements)	Solar Limb Sensors	Star Trackers* (need 1 of 2 for umbra protection)
Breakwires	Pump Controllers	Wheels* (need 3 of 4)
Propulsion system pressure transducers	ECUs (includes drive potentiometers)	Thrusters (need 11 of 12)
	Transponders	Payload suite
	Cooling system dP sensors*	
	Cooling system accumulator pressure sensor (leak detection)	
	RIUs (temp sensors)	

*pending component selection

Rationale for Cross-Strapped (non-internally redundant) components, p1 of 2



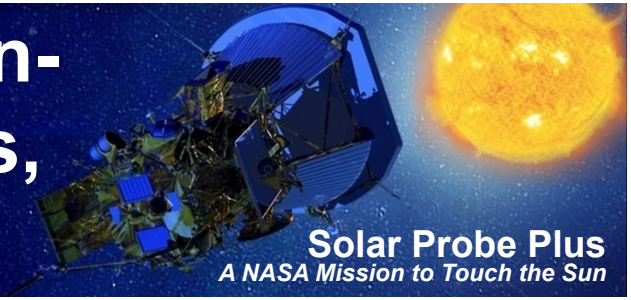
- **Processors**
  - Three processors are required to meet SPP requirement for single fault tolerance through processor reset. Three processors need to be accessible from two REM sides.
  - Decouple from REM; processor reset/demotion does not cause block side switch, and vice-versa.

- **Solar Limb Sensors**
  - Availability of both SLS signals when/if their data is needed provides redundancy. Unable to test SLS functionality, and determine if side-switch is necessary, prior to critical fault.

- **Pump Controllers**
  - Time criticality of continuous cooling system operation. Cross-strapped pumps allow pump operation to be decoupled from spacecraft side-switching.

- **ECUs**
  - Cross-strapping allows data from both to be accessible from the active REM. ECUs include potentiometers which measure actuator position; potentiometer data is used as 2 of 3 voting members for solar array position knowledge.

Rationale for Cross-Strapped (non-internally redundant) components, p2 of 2



- **Transponders**
  - Accessibility of either transponder from active REM maximizes the probability of ground communication.
  - Precision clock sources are currently integrated into the transponders; both are available to the active REM.
  - Prevents a frozen coax switch from causing spacecraft side-switch.
- **Cooling system dP sensors**
  - Time criticality of continuous cooling system operation. dP sensors are used (in addition to motor speed and current) to assess pump health.
- **Cooling system accumulator pressure sensor**
  - Non-redundant (non-critical) sensor.
- **RIUs**
  - Cross-strapping, with selected redundancy for critical temperature sensors, provides mass savings.

Cross-Strapped and A-side components

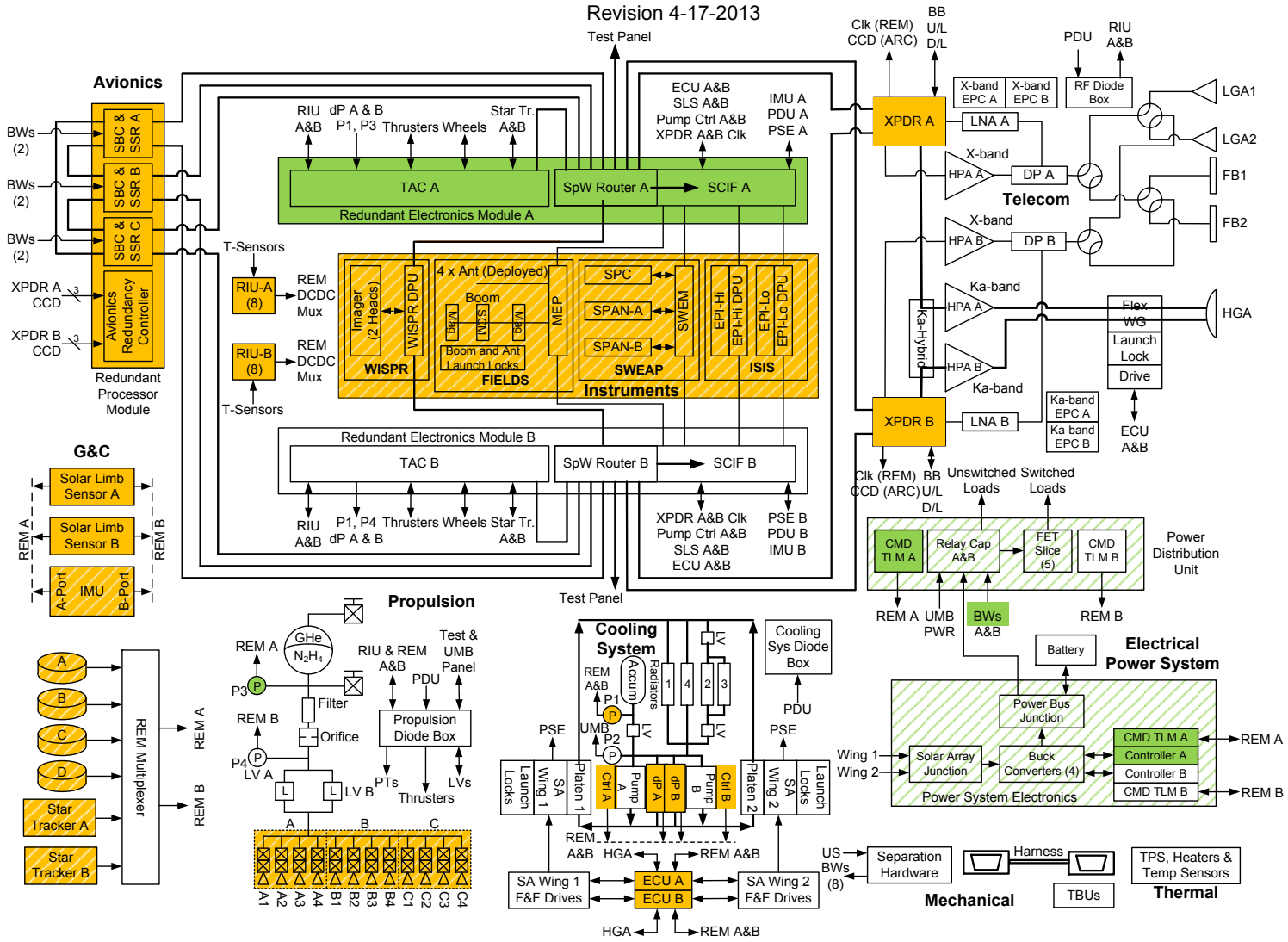
Cross-Strapped with Avionics

Internally Redundant Unit Cross-Strapped with Avionics

Block Redundant with Avionics – Block A

Block Redundant with Avionics – Block B

Solar Probe Plus Spacecraft Block Diagram



Cross-Strapped and B-side components

Cross-Strapped with Avionics

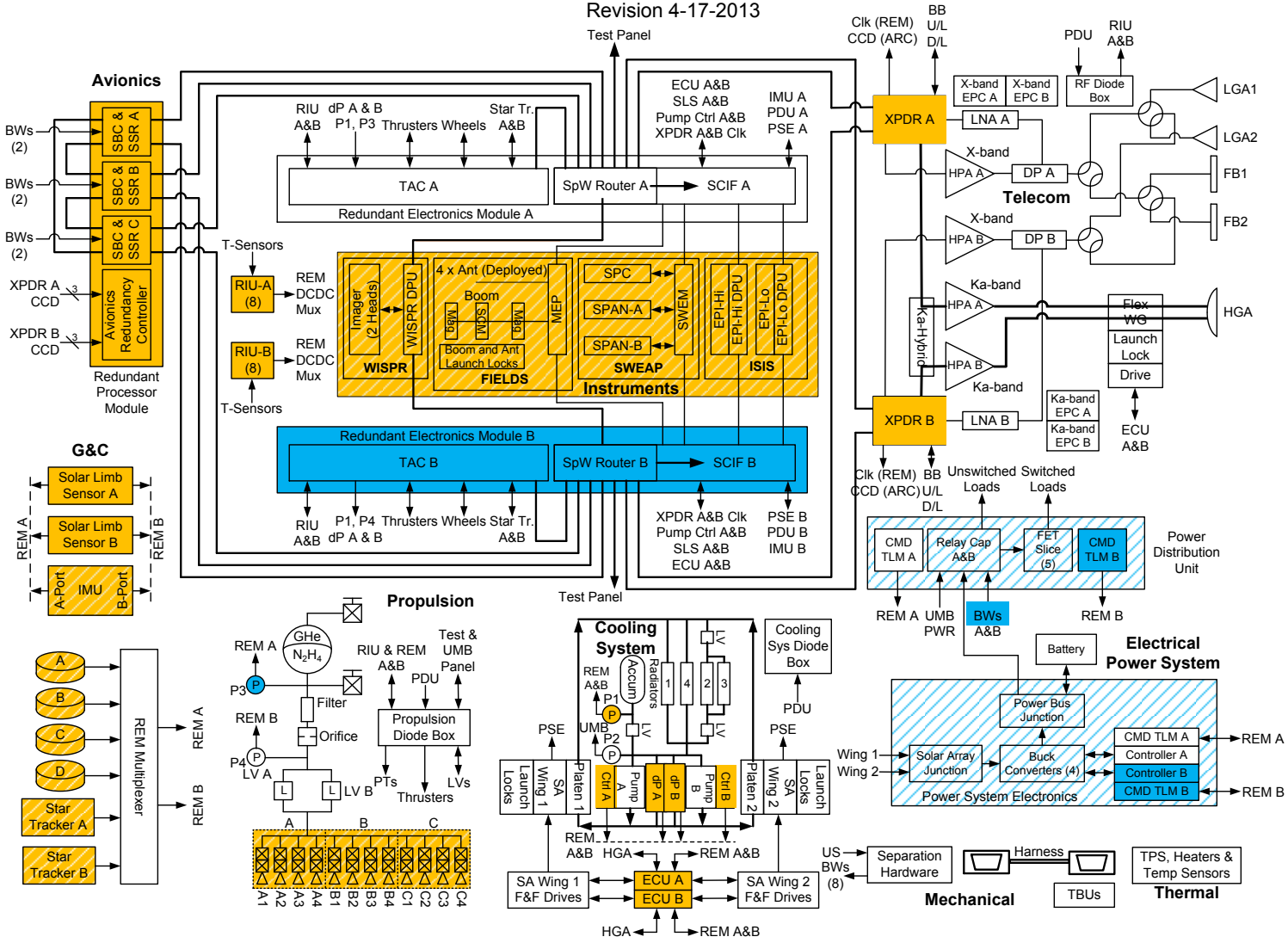
Internally Redundant Unit Cross-Strapped with Avionics

Block Redundant with Avionics – Block A

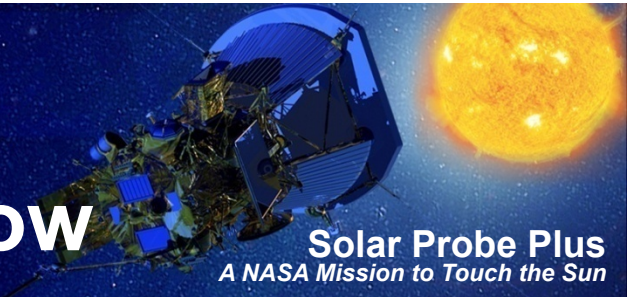
Block Redundant with Avionics – Block B

Solar Probe Plus Spacecraft Block Diagram

Revision 4-17-2013



Redundancy Requirements Flow



Solar Probe Plus
A NASA Mission to Touch the Sun

4.2.4. Solar Probe Plus shall be categorized as Mission Category 1 per NPR 7120.5D and Risk Category B per NPR 8705.4.

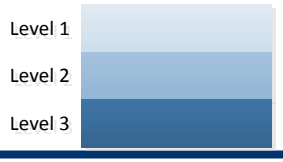
MRD-70: The Mission shall have no single point failures except those on the single point failure list.

REDUNDANCY
The Spacecraft shall …

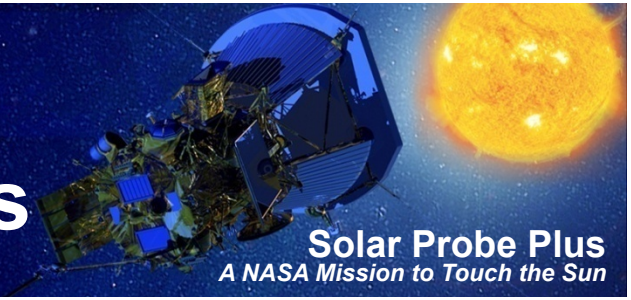
(n/a; L2 requirement is a design implementation decision which spans multiple system elements)

MRD-72: The Mission shall provide instrument fault protection to include ground system monitoring of selected instrument health data, remote SOC notifications of critical fault conditions, and autonomous onboard instrument power-downs in response to instrument request and critical telemetry.

INSTRUMENT FM
The Spacecraft shall …
All SPP instruments shall …



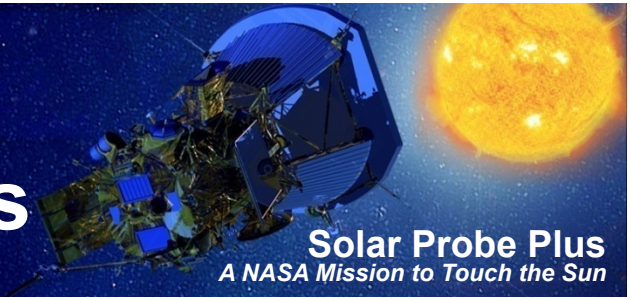
Redundancy:
L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Cross-strapping	cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.	ME, CS, GC, PRP, TEL, AV
Prime processor commanding	be designed such that the prime processor issues all onboard spacecraft commanding.	AV, FSW, TST
Prime processor autonomy	be designed such that the prime processor performs all autonomy, with the exception of prime processor demotion via ARC acknowledge timer.	FSW, AUT, TST
Redundant system management	be designed to manage redundancy	AV, FSW, AUT, TST, MOP

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics,
PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

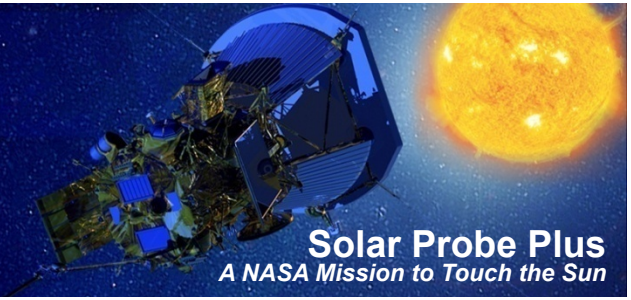
Redundancy:
L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Protection of power, commanding, and communication	be designed such that at least one SCIF, at least one PDU side, at least one XPDR, and at least two processors are powered at all times.	AV
Health check capability	provide the capability to perform health checks on redundant components.	ME, TH, CS, EPS, GC, PRP, TEL, AV, PDU, FSW, TST
Health check protection	ensure that health checkout of redundant side does not interfere with operation of primary side.	ME, TH, CS, EPS, PRP, TEL, AV, PDU, FSW, TST
Diagnostics	capable of gathering diagnostic data from a failed processor.	AV, FSW, TST

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics,
PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Continuity of Control Requirements Flow



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

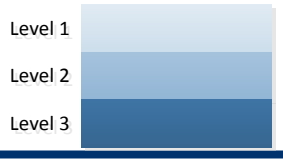
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

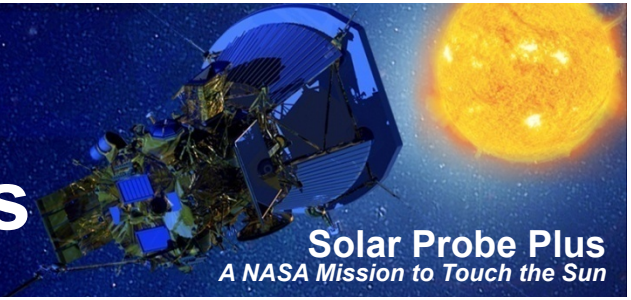
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



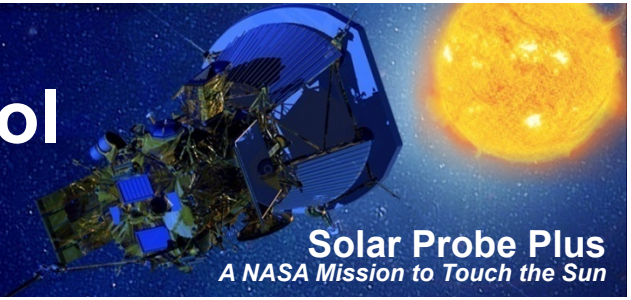
Continuity of Control: L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Attitude control through reset	be capable of attitude control within 4 seconds TBR in the event of a prime processor reset at <= 0.5 AU and 30 seconds TBR > 0.5 AU	GC, AV, FSW, AUT, TST
Wing angle control through reset	be capable of wing angle control within 2 seconds TBR in the event of a prime processor reset for solar distance <=0.5AU and 30 seconds TBR for solar distance > 0.5AU.	ME, EPS, GC, AV, FSW, AUT, TST
Attitude control through critical fault	be capable of attitude control within 5 seconds TBR of safe mode initiation in the event of critical faults as defined in the FM Design Specification 7343-**** at < 0.5 AU and 30 seconds TBR > 0.5 AU	GC, AV, FSW, AUT, TST
Wing angle control through critical fault	be capable of wing angle control within 5 seconds TBR of safe mode initiation in the event of critical faults as defined in the FM Design Specification 7343-**** at <0.5 AU and 30 seconds TBR > 0.5 AU.	ME, EPS, GC, AV, FSW, AUT, TST
Availability of a Prime processor	ensure that three processors are powered on when the spacecraft is <= 0.5 AU from the Sun.	AV, FSW, AUT, MOP
Continuous cooling	ensure that the redundant pump is operational within 10 seconds TBR of pump failure.	CS, AV, PDU, AUT

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

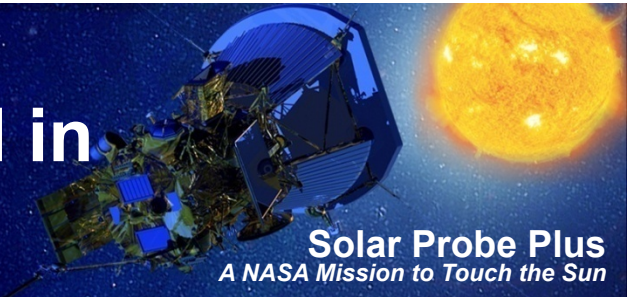
Redundancy & Continuity of Control requirements flow to Level 4



- **Requirements for single fault tolerance and continuity of control drive avionics architecture.**
  - With three processors, a Hot Spare processor is available to assume control if Prime resets (not a failure), even if one processor has failed.
  - Decoupled RPM and REM allows
    - REM side-switching without removing Prime processor from control.
    - Prime reset/demotion without REM side-switching.

- **Avionics Redundancy Controller (ARC) has been designed to manage the 3 processor architecture.**
  - Contains 3 identical mode controller (MC) cards whose output is triple-voted (2 for 3 redundancy)
  - Controls processor logical states and state transition paths
  - Provides Prime and Hot Spare processor acknowledge timers
    - Prime processor will be demoted to Back-Up Spare if resetting or unresponsive
    - Hot Spare is allowed to reset; will be demoted to Failed if unresponsive
  - Controls power switching for processors, REMs, PDUs, and XPDRs to meet FM requirement

FM Design: Redundancy concept implemented in avionics architecture



FM Architecture	L3 Requirements group
Redundancy concept	Redundancy Continuity of control
Avionics architecture: design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios Safing concept / FM modes Ground intervention concept	Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM	Instrument FM

Solar Probe Plus

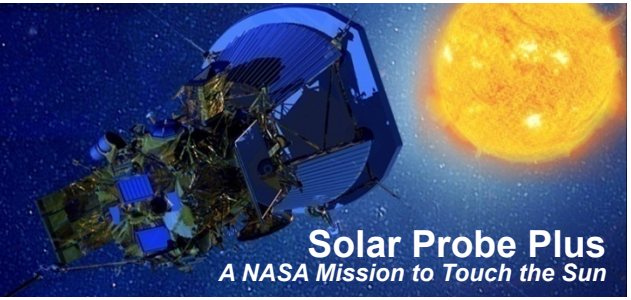
A NASA Mission to Touch the Sun

Avionics Architecture Overview

Geff Ottman
Avionics Lead Engineer
geffrey.ottman@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Agenda



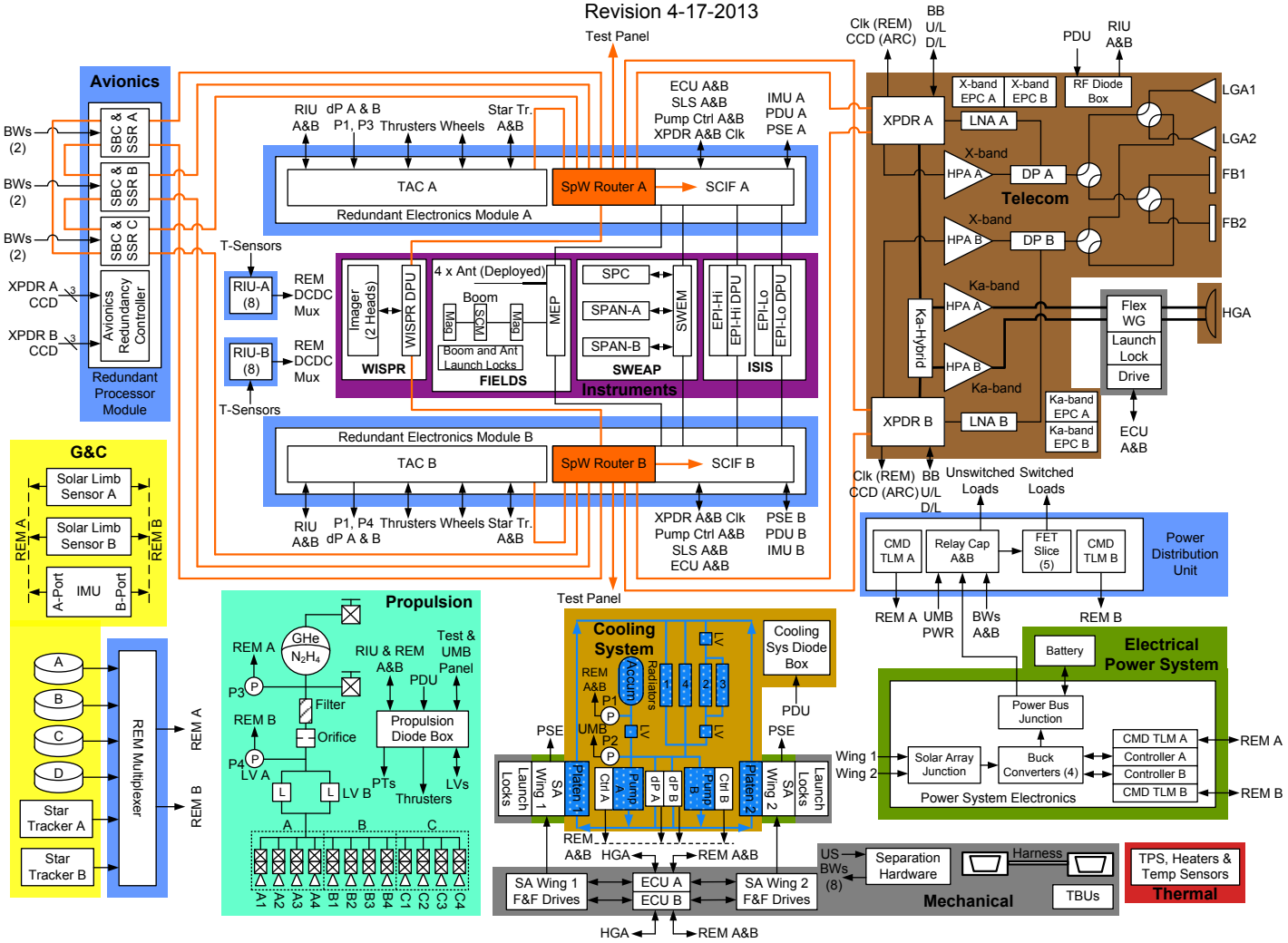
- Subsystem Block Diagrams
- Subsystem / RPM / REM Fault Management Requirements
- Avionics Redundancy Controller (ARC) Requirements Specification
- ARC SBC Logical State Transitions
- ARC MC Implementation Information

SPP Spacecraft Block Diagram

Solar Probe Plus
A NASA Mission to Touch the Sun

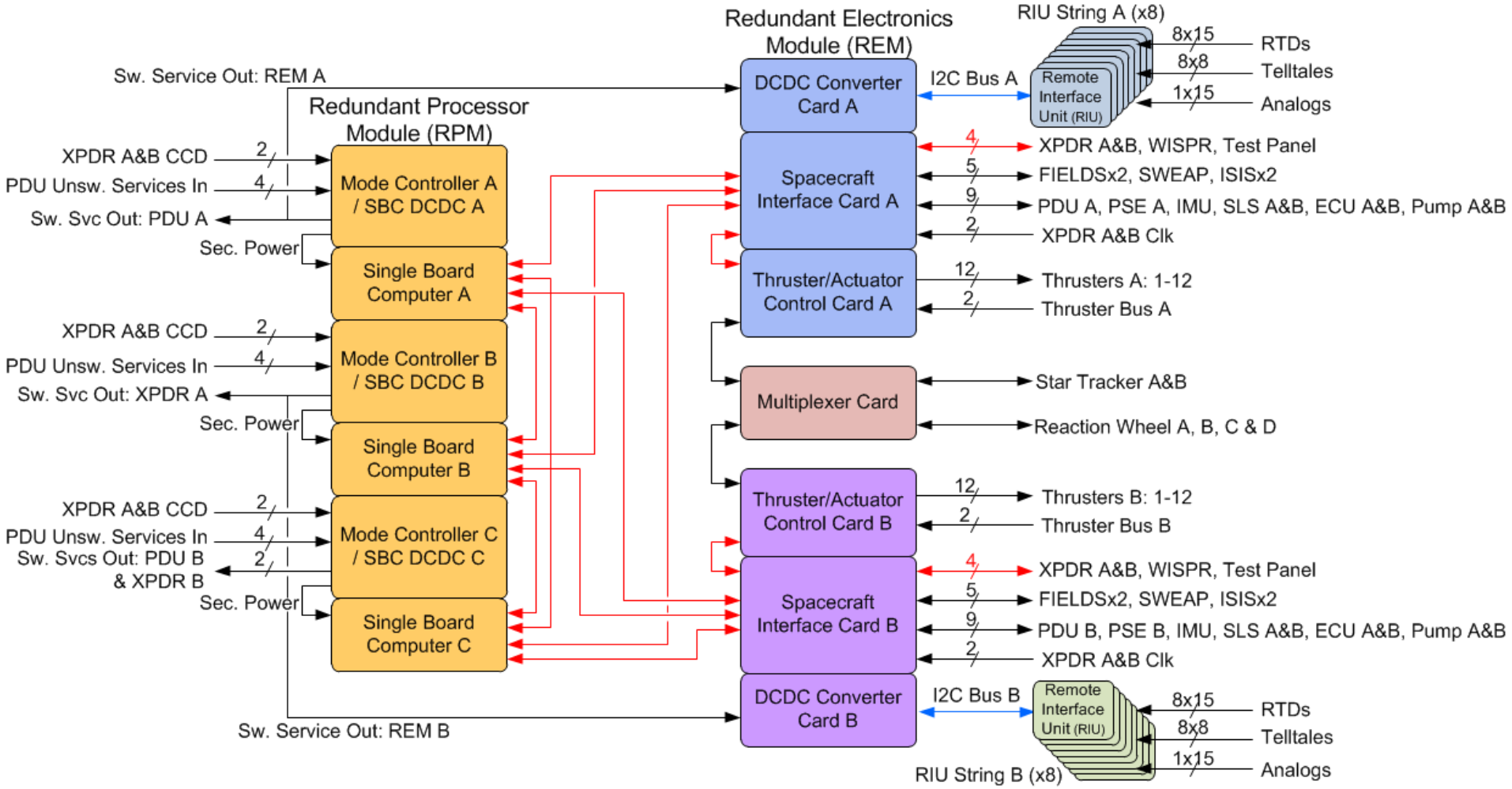
Solar Probe Plus Spacecraft Block Diagram

Revision 4-17-2013

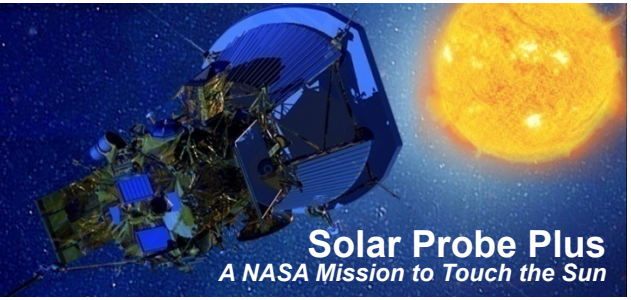


Avionics Subsystem Block Diagram

Solar Probe Plus
A NASA Mission to Touch the Sun

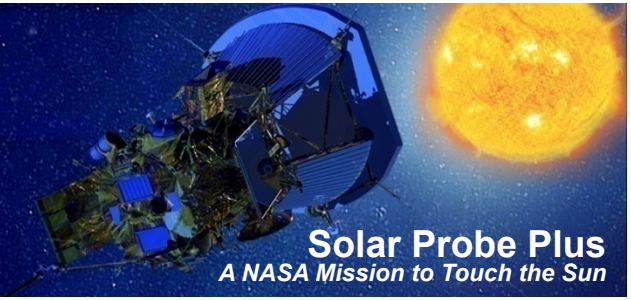


Subsystem Fault Management Requirements (1 of 2)



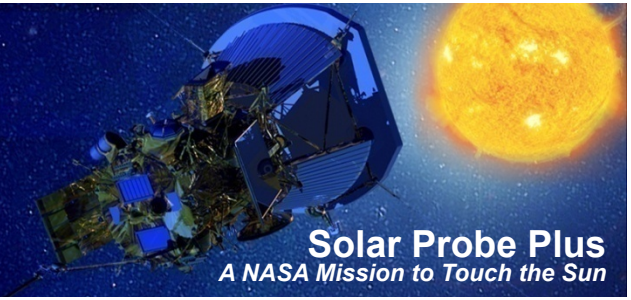
- **Meet time-critical FM response requirements:**
  - Be capable of attitude control within 4 seconds TBR in the event of a prime processor reset at <= 0.5 AU and 30 seconds TBR > 0.5 AU.
  - Be capable of wing angle control within 2 seconds TBR in the event of a prime processor reset for solar distance <=0.5AU and 30 seconds TBR for solar distance > 0.5AU.
  - Be capable of attitude control within 5 seconds TBR of safe mode initiation in the event of critical faults as defined in the FM Design Specification 7343-**** at < 0.5 AU and 30 seconds TBR > 0.5 AU.
  - Be capable of wing angle control within 5 seconds TBR of safe mode initiation in the event of critical faults as defined in the FM Design Specification 7343-**** at <0.5 AU and 30 seconds TBR > 0.5 AU.
- **Have no single point failures except those on the single point failure list (The MUX Slice PWB contains interfaces between the REM and all four Reaction Wheels and the two Star Trackers).**
- **No unrecoverable states for the Subsystem; specifically, the ARC Mode Controllers.**

Subsystem Fault Management Requirements (2 of 2)

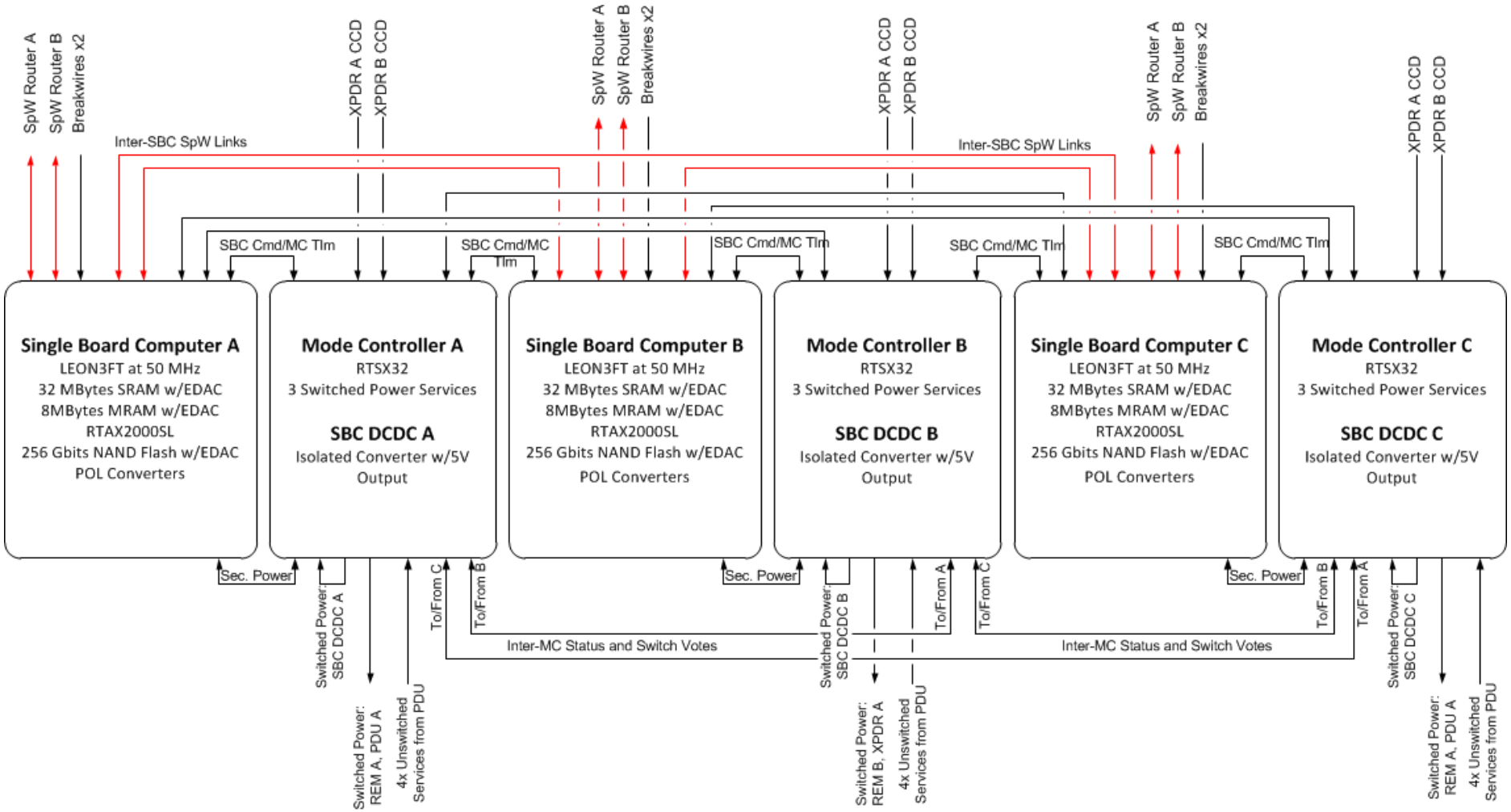


- Support health check outs on redundant components.
- Provide spacecraft telemetry to enable health evaluation by autonomy and fault diagnosis on the ground.
- Interface-IC driver and receiver isolation.
- LVDS-interface fault propagation protection.
- Connector signal segregation.

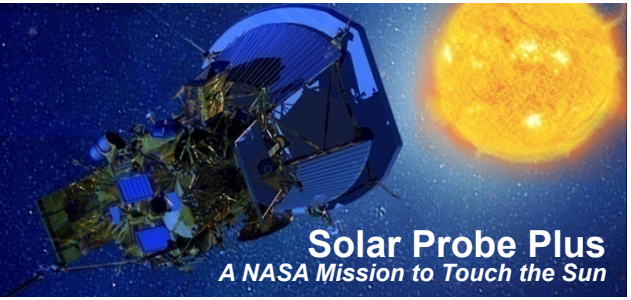
Redundant Processor Module (RPM) Block Diagram



Solar Probe Plus
A NASA Mission to Touch the Sun

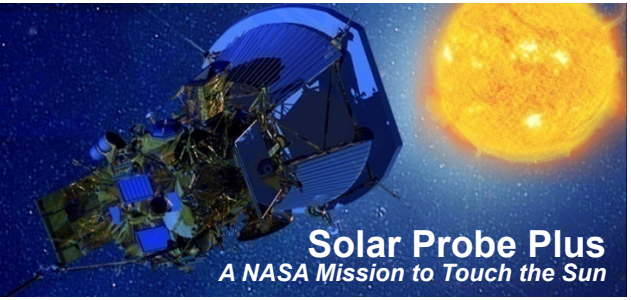


RPM Fault Management Requirements (1 of 2)



- The RPM Single Board Computers (SBC) are 2 for 3 redundant:
  - Each SBC implements 2 of 3 voting of MC status - All SBCs can assume all states:
    - SBC Physical location: A, B, or C
    - SBC Logic state: Prime, Hot Spare, Backup Spare, Fail
    - SBC FSW Application Select, NV Memory Write Enable and Reset
  - Each SBC has SpW Links to REM-side A&B Routers and the other two SBCs
  - Each SBC has bulk memory on card (previously on REM SSR A&B)
  - Each SBC has a command and telemetry interface with the three Mode Controllers
  - Block Redundant Interfaces with the Breakwires
  - Note: A failure or reset of any SBC is not a mission ending fault

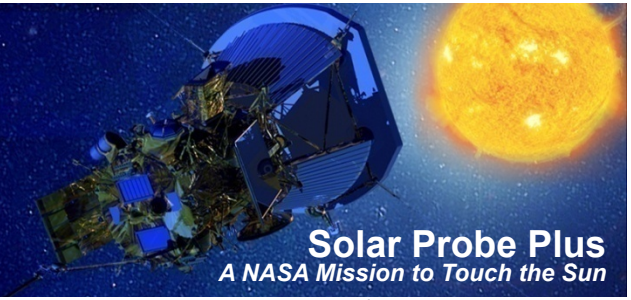
RPM Fault Management Requirements (2 of 2)



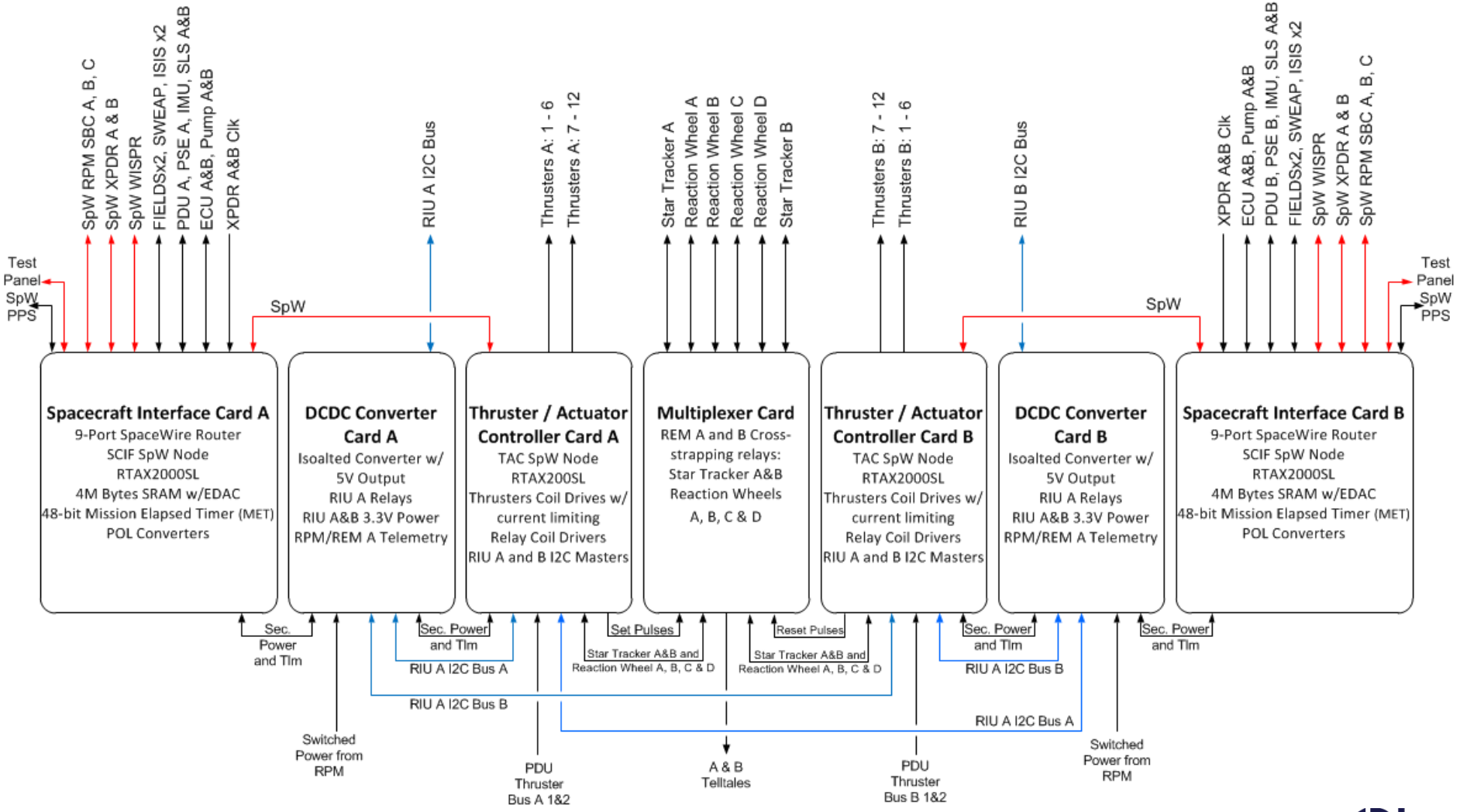
- The RPM Avionics Redundancy Controller (ARC) Mode Controllers (MC) are 2 for 3 redundant:
  - MCs are on PDU-unswitched-services with MC-current-limiting
  - MCs implement 2 of 3 voting for switched power services (defined power states):
    - SBC DCDC A, B, and C (only BS or F can be powered off)
    - REM A and B (A or B, or A&B – coupled with PDU services)
    - PDU A and B (A or B, or A&B – coupled with REM services)
    - XPDR A and B (A or B, or A&B)
  - Each MC has a command and telemetry interface with the three SBCs and a telemetry interface with the other two MCs
  - MCs monitor SBC Prime and Hot Spare health via ack timers
  - MCs maintain transition state history in SBC telemetry
  - MCs capable of resynchronization of processor logical states
  - Cross-strapped Interfaces with XDPR A&B CCDs
  - Note: A failure of any MC is not a mission ending fault

APL

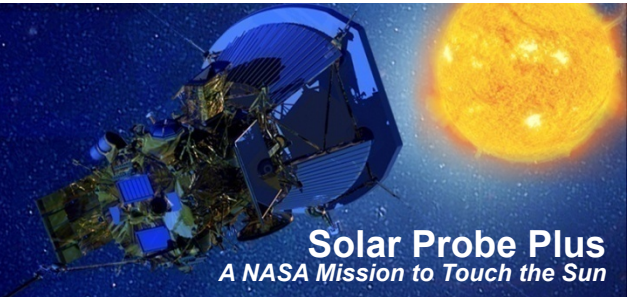
REM Block Diagram



Solar Probe Plus
A NASA Mission to Touch the Sun

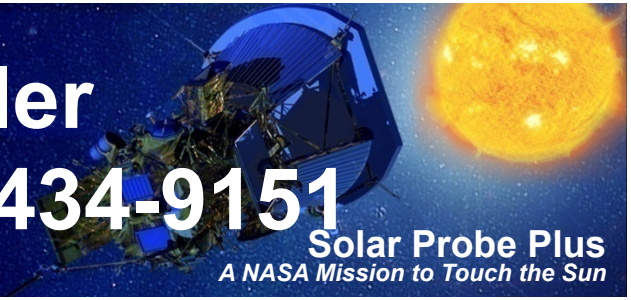


REM Fault Management Requirements



- The REM SCIF/TAC/DCDC are A/B Block Redundant with a single MUX Card
  - Block Redundant Interfaces with PDU, PSE and Prop System Pressure Transducers
  - Cross-Strapped Interfaces with SBC A, B and C; Solar Limb Sensor A and B; Pump Controller A and B; ECU A and B; XPDR A and B; and Cooling System Pressure Transducers dPA and dPB
  - Relay-Isolated, Cross-Strapped Interfaces with RIU String A and B; Star Tracker A and B; and Reaction Wheels A, B, C and D.
  - Cross-Strapped Internally Redundant Interface to IMU, Instruments , Thrusters and Cooling System Accumulator Pressure Transducer
  - Thruster coil drivers with individual thruster valve fault containment

Avionics Redundancy Controller Requirements Specification, 7434-9151

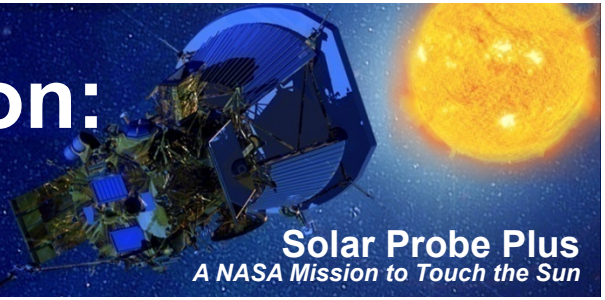


- **ARC Purpose - The purpose of the ARC is to:**
  - **SBC Promotion and Demotion –**
    - Provide a mechanism to promote and demote Single Board Computers (SBCs) between the logical states of Prime (P), Hot Spare (H), Backup Spare (B), and Failed (F).
    - The power state of logical state Backup Spare is under the control of the Prime and may be referred to as Cold Spare when off or Warm Spare when on...
  - **Power Control of Critical Components -** Control the power state of redundant elements of the Avionics subsystem, Power Distribution Unit, and Transponders.
  - **CCD Functions -** Implement a Critical Command Decoder CCD to allow Mission Operations to send commands via the redundant Transponders.

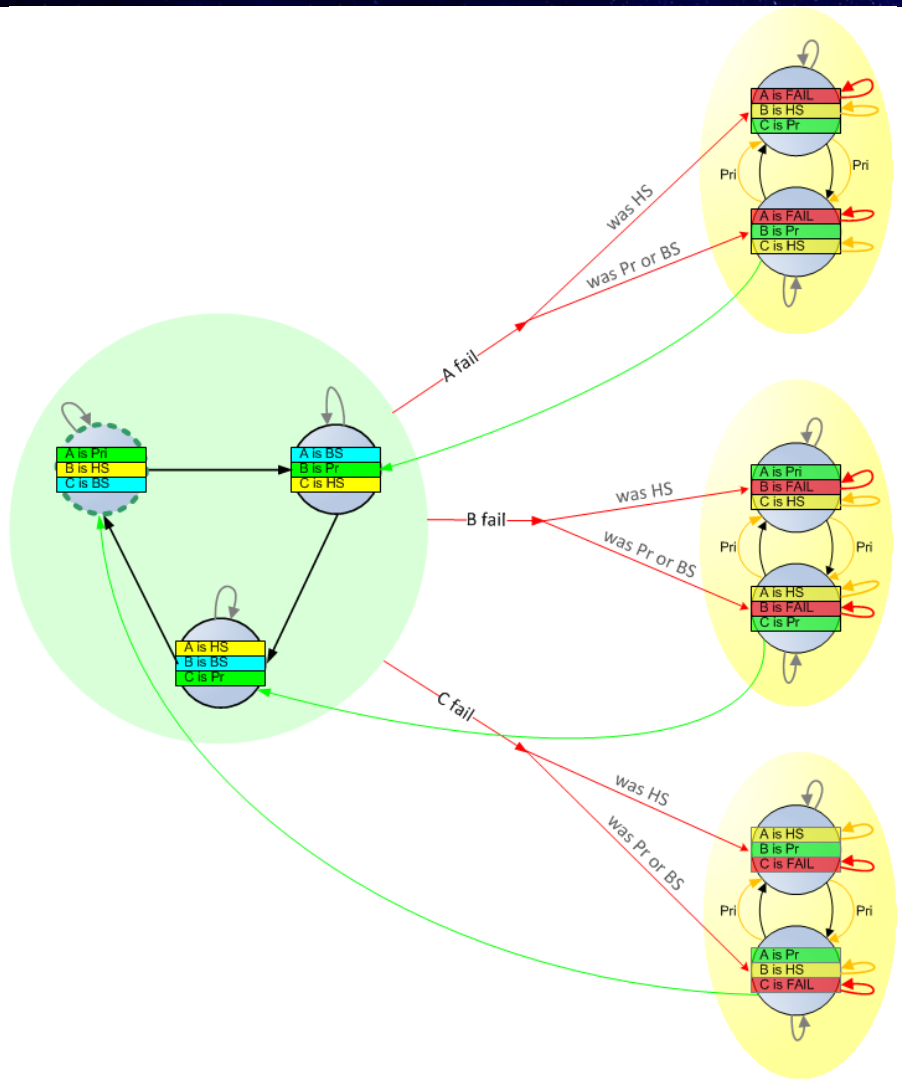
The following material was originally presented at the SPP Avionics ARC Reqs Peer Review, 4/10/13.
Slides and info courtesy of K. Weber.

Avionics Redundancy Controller

ARC Requirements Specification: SBC Logical State Transitions



Solar Probe Plus
A NASA Mission to Touch the Sun



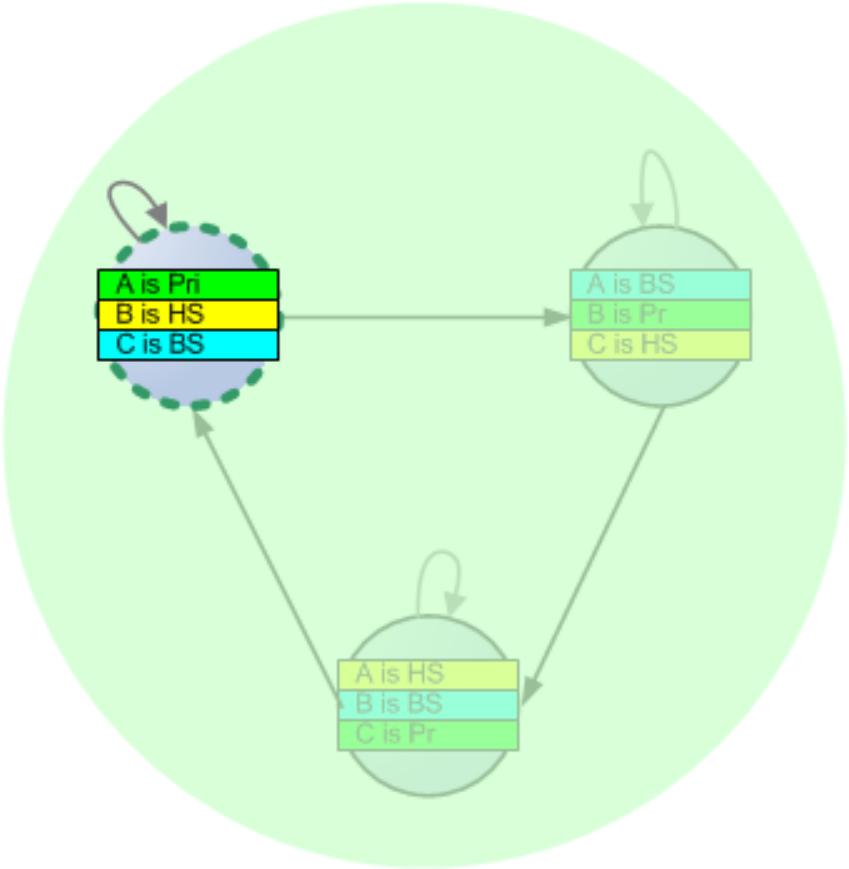
ARC Mode Controller firmware-centric view

- 9 valid combinations of SBC Logical States for the three processors
- Figure does not address MC Resynchronization
- INV opcode demotion is only enforced after rotation wait period
- Processor power switch state tied in hardware to logical state.
  - Power on for BS (Off) to HS change is automatic in HW

	Fail (by CCD CMD, INV opcode, or HS ACK)
	Fail (by INV opcode, or HS ACK ONLY)
	Ground All OK (by CCD command)
	Demote (by Pri ACK [RST])
	HS, BS, or FAIL Reset, no change
Pri	Prime, power = ON
HS	Hot Spare, power = SLEEP
BS	Encounter: Warm Spare, power = SLEEP Non-Encounter: Cold Spare power = OFF
	Default power-on state

APL

SBC Logical State Transitions 1: Default State

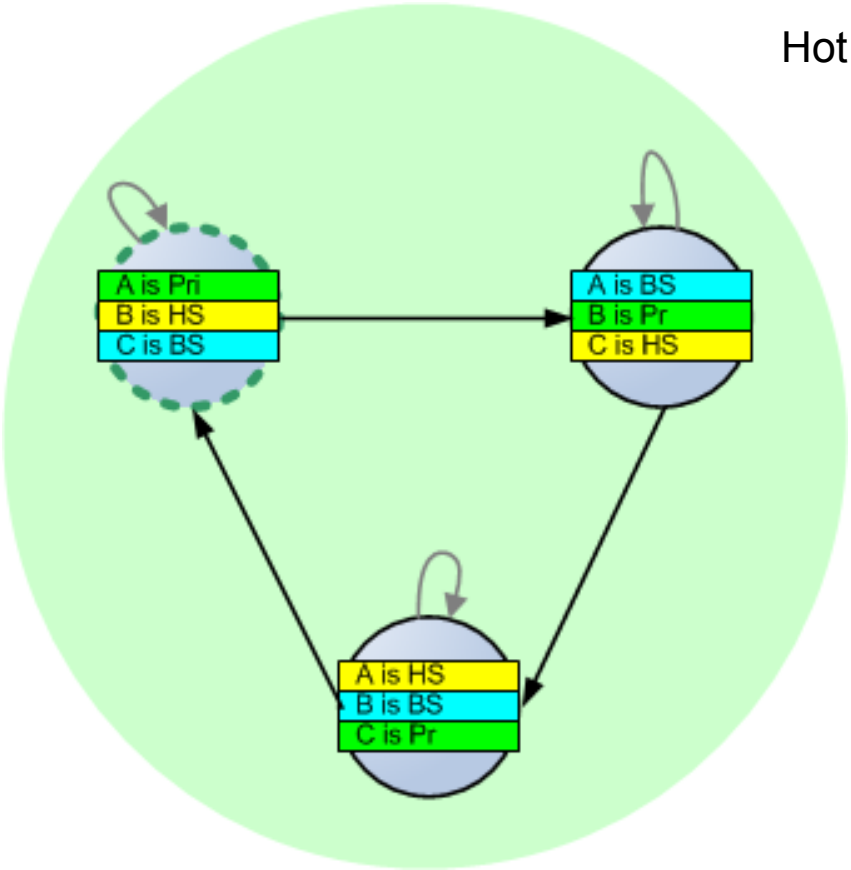


	Fail (by CCD CMD, INV opcode, or HS ACK)
	Fail (by INV opcode, or HS ACK ONLY)
	Ground All OK (by CCD command)
	Demote (by Pri ACK [RST])
	HS, BS, or FAIL Reset, no change
Pri	Prime, power = ON
HS	Hot Spare, power = SLEEP
BS	Encounter: Warm Spare, power = SLEEP Non-Encounter: Cold Spare power = OFF
	Default power-on state

RPM SBC Logical State Transitions 2: Prime Acknowledge Timer Expirations

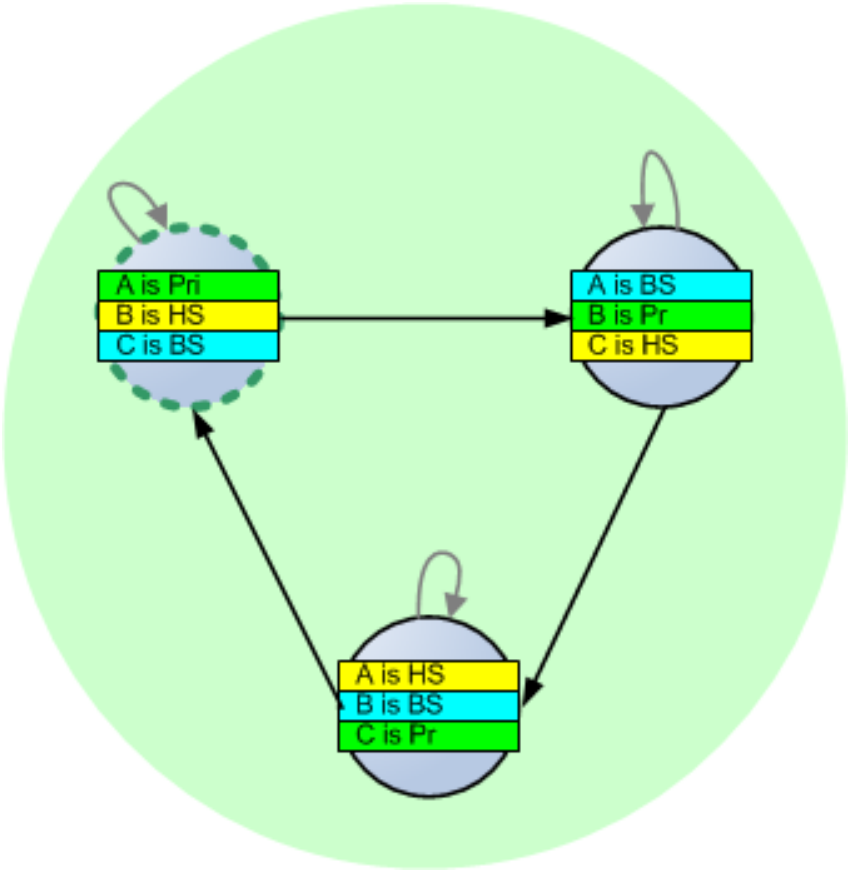
Solar Probe Plus
A NASA Mission to Touch the Sun

Prime Ack Timer = 0.515 Seconds
Hot Spare Ack Timer = 2x SBC Reboot Time



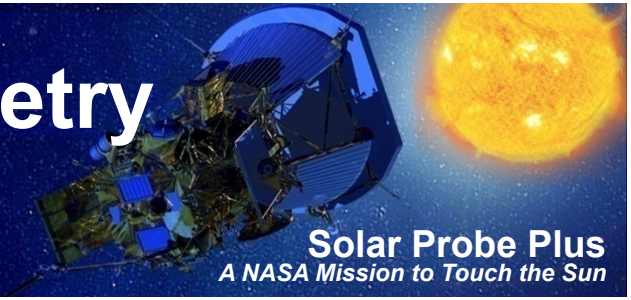
	Fail (by CCD CMD, INV opcode, or HS ACK)
	Fail (by INV opcode, or HS ACK ONLY)
	Ground All OK (by CCD command)
	Demote (by Pri ACK [RST])
	HS, BS, or FAIL Reset, no change
Pri	Prime, power = ON
HS	Hot Spare, power = SLEEP
BS	Encounter: Warm Spare, power = SLEEP Non-Encounter: Cold Spare power = OFF
	Default power-on state

RPM SBC Logical State Transitions
3: Failed SBC Scenario



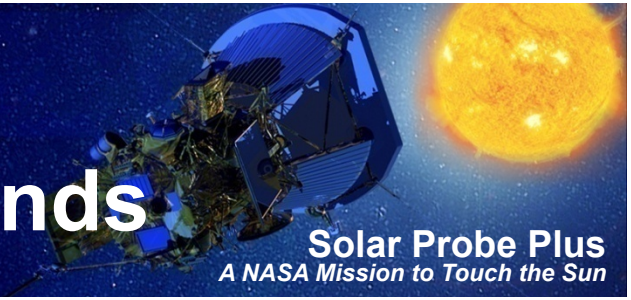
	Fail (by CCD CMD, INV opcode, or HS ACK)
	Fail (by INV opcode, or HS ACK ONLY)
	Ground All OK (by CCD command)
	Demote (by Pri ACK [RST])
	HS, BS, or FAIL Reset, no change
Pri	Prime, power = ON
HS	Hot Spare, power = SLEEP
BS	Encounter: Warm Spare, power = SLEEP Non-Encounter: Cold Spare power = OFF
	Default power-on state

ARC MC Command and Telemetry Concept



- Each MC operates asynchronously with respect to the other MCs.
- Each MC will transmit telemetry sequentially to SBC A->B-> C at a 6 Hz rate
- Each MC will accept commands from the three SBCs. Maximum SBC command rate is ~6Hz, defined by a command start-start delay of 1/6 sec.
  - SBC commands processed in the order received; and A>B>C order when coincident in time.
  - Pending CCD commands take precedence in the queue over pending SBC commands and will interrupt natural order.
  - Incoming commands will be buffered during telemetry transmission.
  - Commanding which exceeds the defined rate may produce an increment to the overflow error count, along with the invalid command counter.
- Each MC will transmit SBC states to the other two MCs.

ARC Mode Controller: Commands



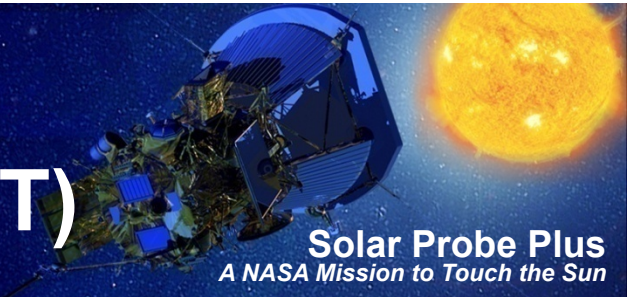
- **SBC Commands:**
  - **Pri Ack Timer Reset**
  - **Pri Backup Spare/Fail Power Control**
  - **Pri REM/PDU Power Cntrl**
  - **Pri Transponder Power Cntrl**
  - **Pri Resynch Exec Flag Clear**
  - **HS Ack Timer Reset**
  - **Increment Command Counter (x4), one per logical state**
  - **Resynch Command, no logical state descriptor req.**
- **CCD Commands:**
  - **SBCs All Okay***
  - **SBC Fail (x3 SBCs)**
  - **SBC Image A/B Sel. (x3 SBCs)**
  - **SBC Reset (x3 SBCs)**
  - **SBC NV Memory Bank 1&2 Write Protect Enable/Disable (x3 SBCs)****
  - **Increment Counter**
  - **SBC Command Pass Through**

** Note: All Okay is constrained to ensure a Failed SBC returns to the BS position without interruption to the Prime and HS states.*

***Note: Mem Bank Protect Requires Max 12 CMDs, 2 Banks x 2 States (EN/DIS) x 3 SBCs*

APL

ARC MC Local State Table (LST)



- Each MC will keep a LST which corresponds to:
  - Internally derived states at the time of the last TLM transmission.
  - External MC states based on the last TLM receipt from the MCs.
- Provides a consistent snapshot from which the MCs can act upon if a Resynch command is received.
- Prime – 'P', Hot Spare – 'H', Backup Spare – 'B', Failed – 'F'
- ARC functionality is preserved during anomalous conditions and/or faults.

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	B	P	H
MC-C	B	P	H
Vote	B	P	H

Good Vote

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	F	H	P
MC-C	B	P	H
Vote	B	P	H

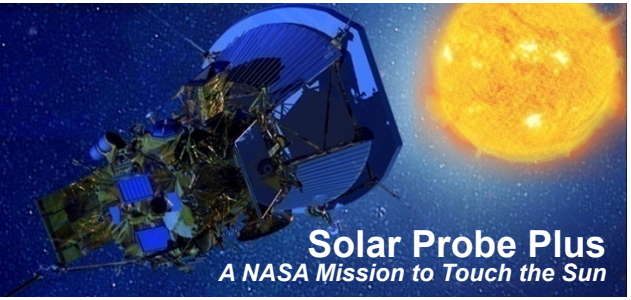
2of3 Vote

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	F	H	P
MC-C	B	P	H
Vote	B	P	H

NoVote

APL

ARC MC LST and Resynch



- **Resynch capability allows recovery of any ARC LST combination, i.e no dead-end processor states.**
- **A MC will evaluate the need to update its LST upon receipt of the Resynch command from any SBC.**
- **The result of the 2of3 Vote is that only MC-B takes Resynch action.**
- **The NoVote condition results in all three MCs reverting to their default LST states.**

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	B	P	H
MC-C	B	P	H
Vote	B	P	H

Good Vote
No Change

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	F	H	P
MC-C	B	P	H
Vote	B	P	H

2of3 Vote
MC-B adjusts to match vote

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	F	H	P
MC-C	B	P	H
Vote	B	P	H

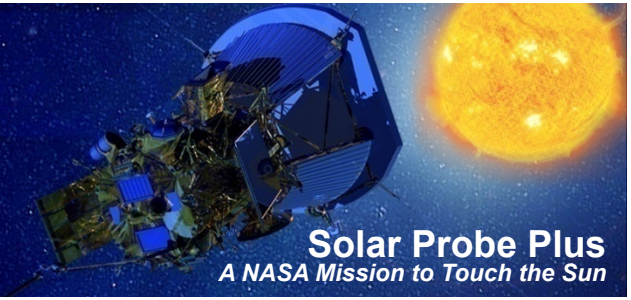
NoVote
All MCs restored to default states

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	B	P	H
MC-C	B	P	H
Vote	B	P	H

	SBC-A	SBC-B	SBC-C
MC-A	B	P	H
MC-B	F	H	P
MC-C	B	P	H
Vote	B	P	H

	SBC-A	SBC-B	SBC-C
MC-A	P	H	B
MC-B	P	H	B
MC-C	P	H	B
Vote	P	H	B

Conclusion



- Agenda:
  - Subsystem Block Diagrams
  - Subsystem / RPM / REM Fault Management Requirements
  - Avionics Redundancy Controller (ARC) Requirements Specification
  - ARC SBC Logical State Transitions
  - ARC MC Implementation Information

Solar Probe Plus

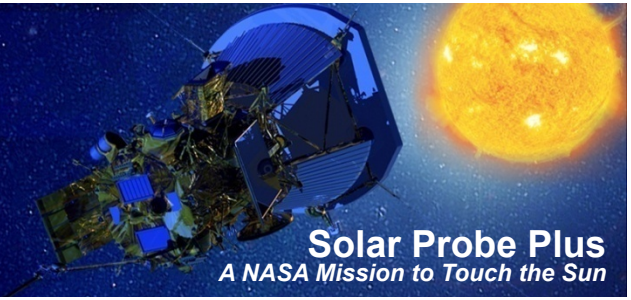
A NASA Mission to Touch the Sun

Fault Management Preliminary Design

Sanae Kubota
FM Lead Engineer
sanae.kubota@jhuapl.edu

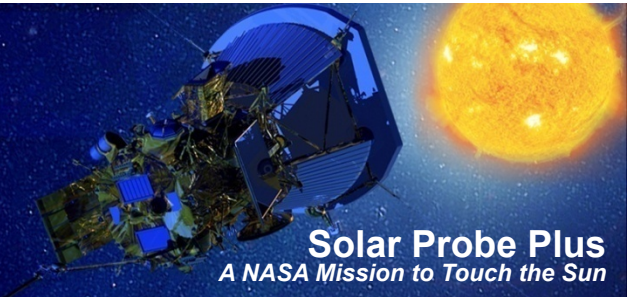
APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

FM Design: Critical Scenarios



FM Architecture	L3 Requirements group
Redundancy concept	Redundancy Continuity of control
Avionics architecture: design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios Safing concept / FM modes Ground intervention concept	Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM	Instrument FM

Critical Scenarios overview

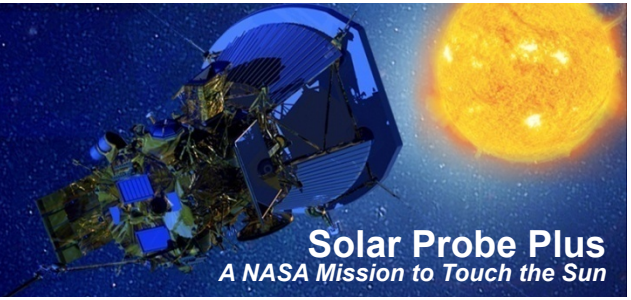


- **Planned mission events (critical sequence) or unanticipated faults which create conditions (critical faults) that require a timely response to preserve the mission.**

- **Critical Fault**
  - Persistent,
  - Not identified in advance or diagnosed in flight,
    - "unknown unknowns"
    - Responses are designed for identified potential faults to prevent the system from reaching a critical fault condition
  - Could be attributed to one or more subsystems, and
  - Pose an immediate risk to mission success.
    - Create a condition in which there is a time-critical threat to spacecraft thermal, power, communication, or commanding ability.

- **Critical Sequence**
  - An event, or sequence of events, which must be executed within a specified time in order to achieve mission success.
    - common examples: orbit insertion or landing maneuvers

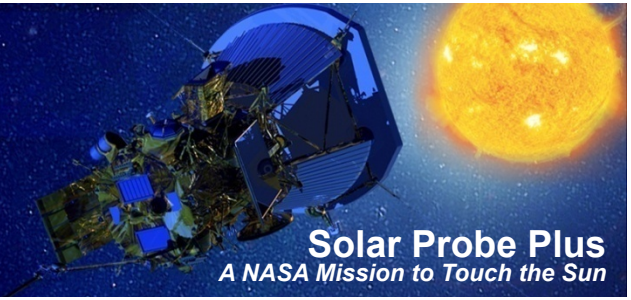
SPP Critical Scenarios



- SPP conditions resulting from critical faults:
  - Thermal
    - Umbra Violation – Orange Warning
    - Aphelion Thermal Violation
    - Solar Array / Cooling System over-temperature
    - Cooling System under-temperature
  - Power
    - Low Battery State of Charge
  - Communication
    - Command Loss Timer expiration
  - Commanding
    - Processor Overcycling

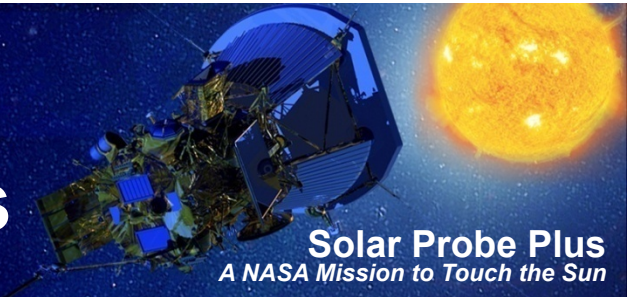
- SPP critical sequence:
  - Launch through initial cooling system activation and battery recharge

FM Design:
Safing Concept / FM Modes



FM Architecture	L3 Requirements group
Redundancy concept	Redundancy Continuity of control
Avionics architecture: design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios **Safing concept / FM modes** **Ground intervention concept**	Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM	Instrument FM

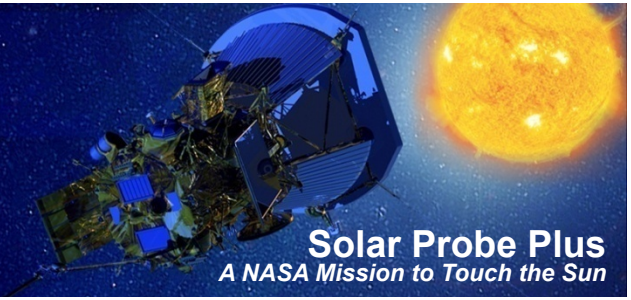
Safing Concept and FM Modes



- SPP FM utilizes a layered approach to protect the mission, with faults categorized by severity and responses executed at two redundant levels.

- Fault response concept is designed to
  - Implement a simple process with minimized impact to the observatory in the detection and response to less severe and isolated (local) faults.
    - Observatory remains in Operational Mode.
  - Enable a power-, communication-, commanding-, and thermally-safe observatory in the event of critical faults through a system-wide response to protect against "unknown unknowns."
    - Observatory demoted to Safe (Non-Operational) Mode.
    - Meets L2 requirement to autonomously detect and safe in response to a critical fault.

FM Modes: Critical Fault Responses



Operational Mode

Level 1 | Level 2 | Level 3

Launch | Cruise | Solar Encounter | Science Downlink

* deltaV & spacecraft slews allowed only with G&C full rate and full attitude control

time, temp Safe-SA exit thresholds met

ground command

ground command

Aphelion Thermal Violation
Low Battery State of Charge
SA/CS Over-Temperature
CS Under-Temperature
Umbra Violation – Orange Warning

Processor Overcycling

Command Loss Timer expiration

Solar Array

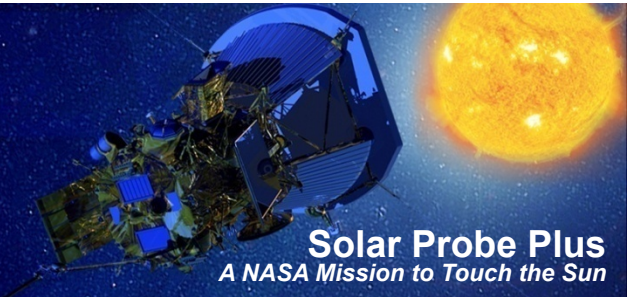
Standby

Earth Acquisition

Safe Mode

(cmd safe attitude, suspend/inhibit Ka d/l attempts, load shed)

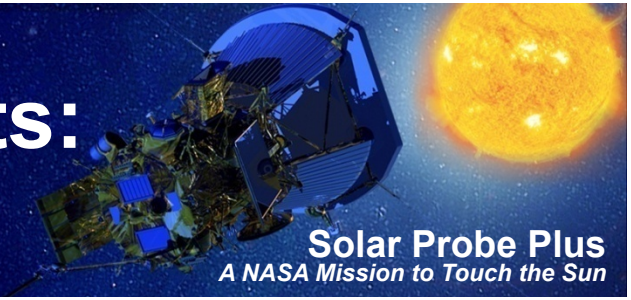
Safe Mode operations

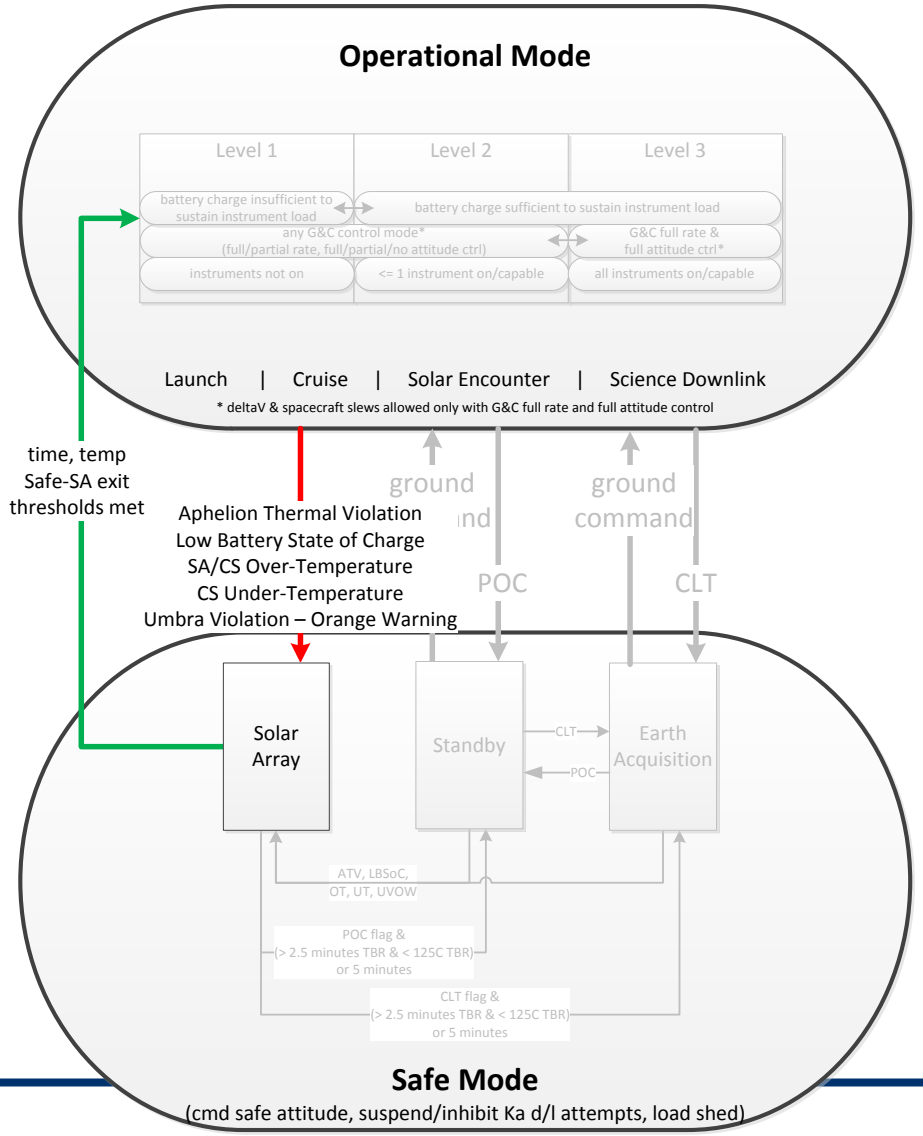


- System-wide recovery procedure
  - Processor switch (except in Processor Overcycling response)
  - Avionics (block) side switch
  - Power-cycle
  - Load shed

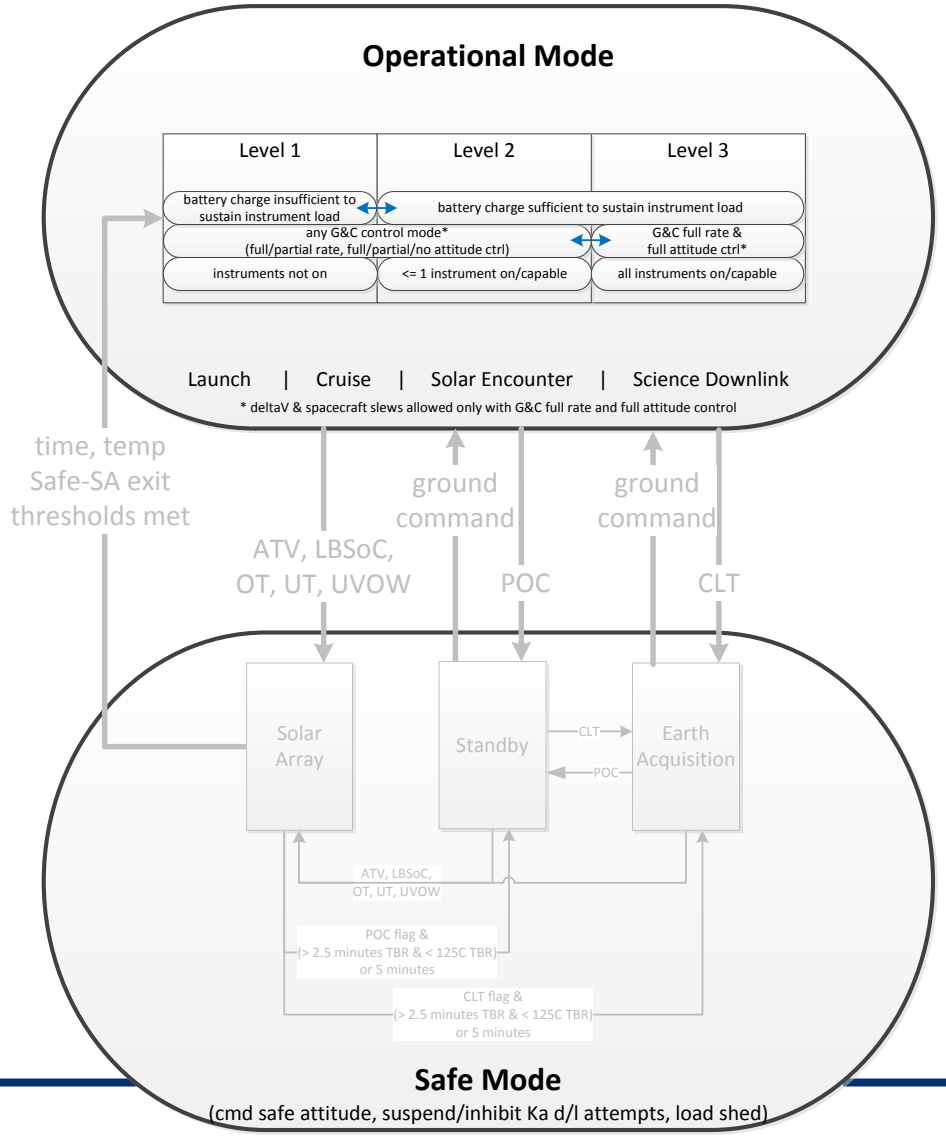
- Limited spacecraft activity; the following are not executed while the spacecraft is in Safe Mode:
  - Delta V maneuvers
  - Spacecraft slews (except to mission default or Earth comm)
  - Ka downlink

Power & Thermal Critical Faults: Safe Mode – Solar Array

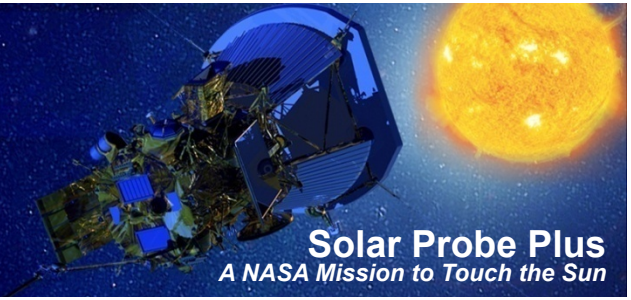


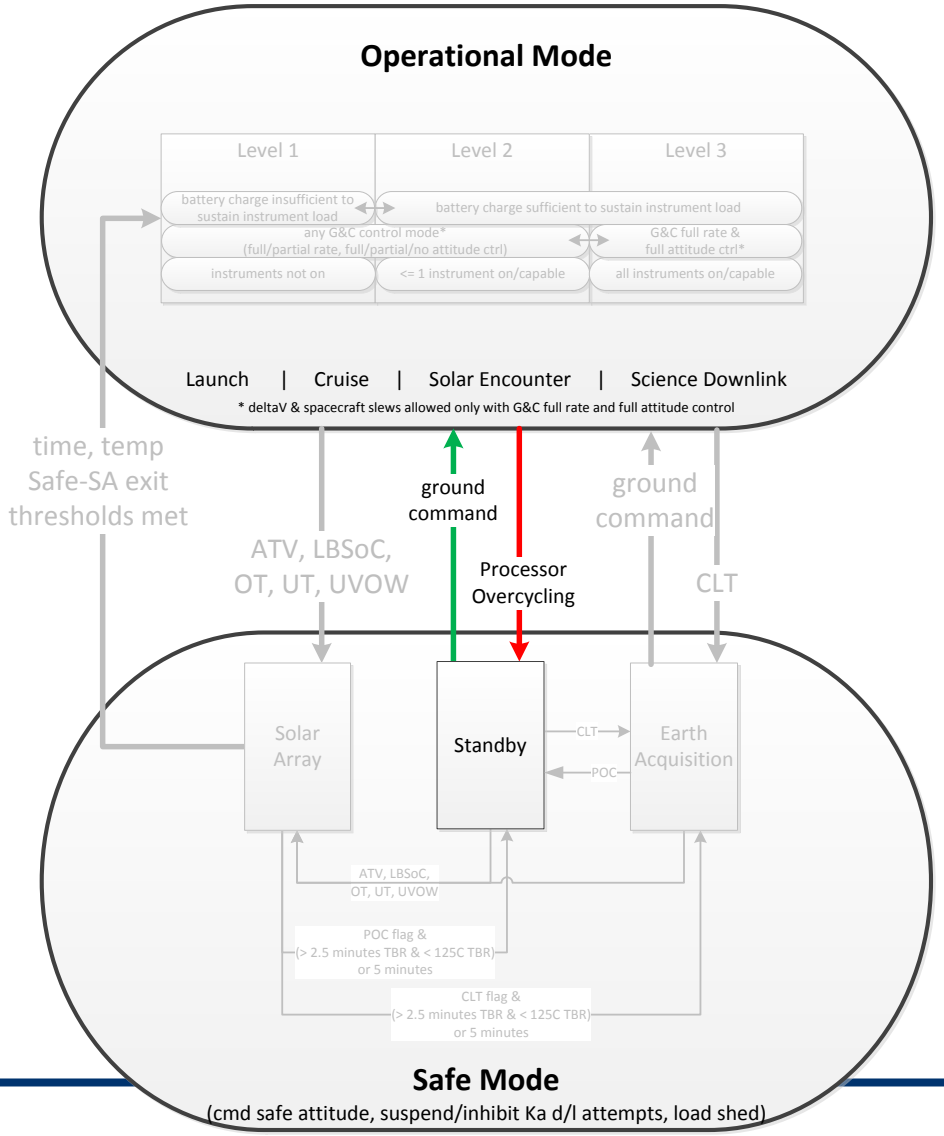


Operational Mode

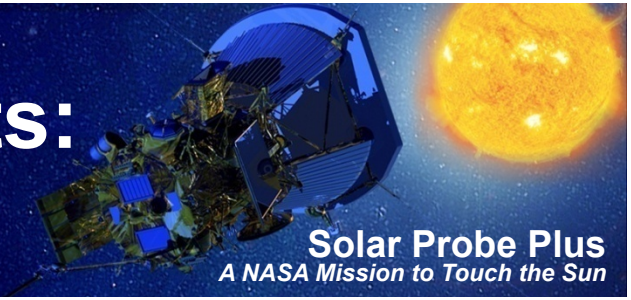


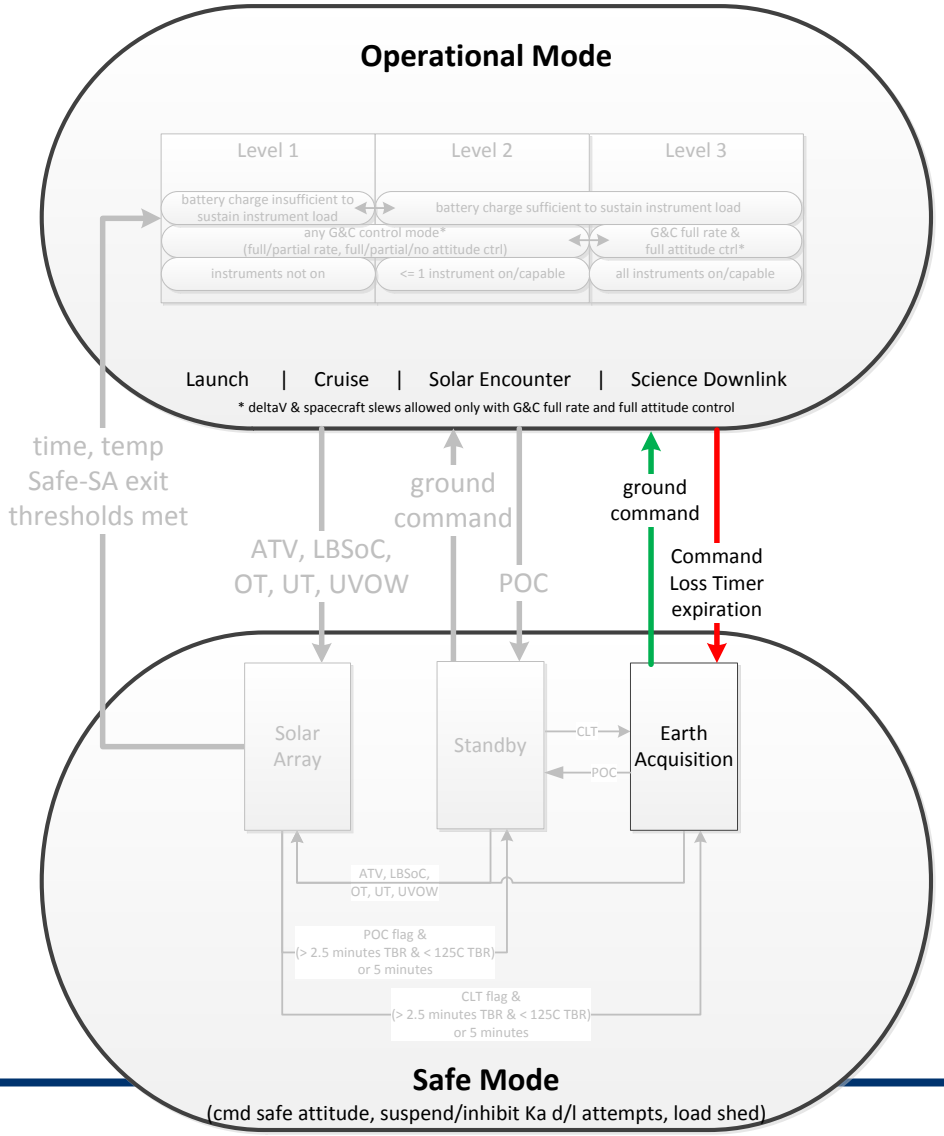
Commanding Critical Faults: Safe Mode - Standby



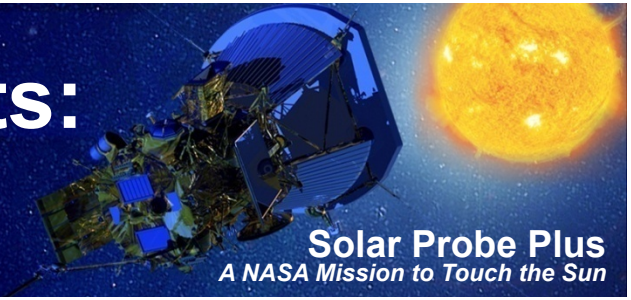


Communications Critical Faults: Safe Mode – Earth Acquisition

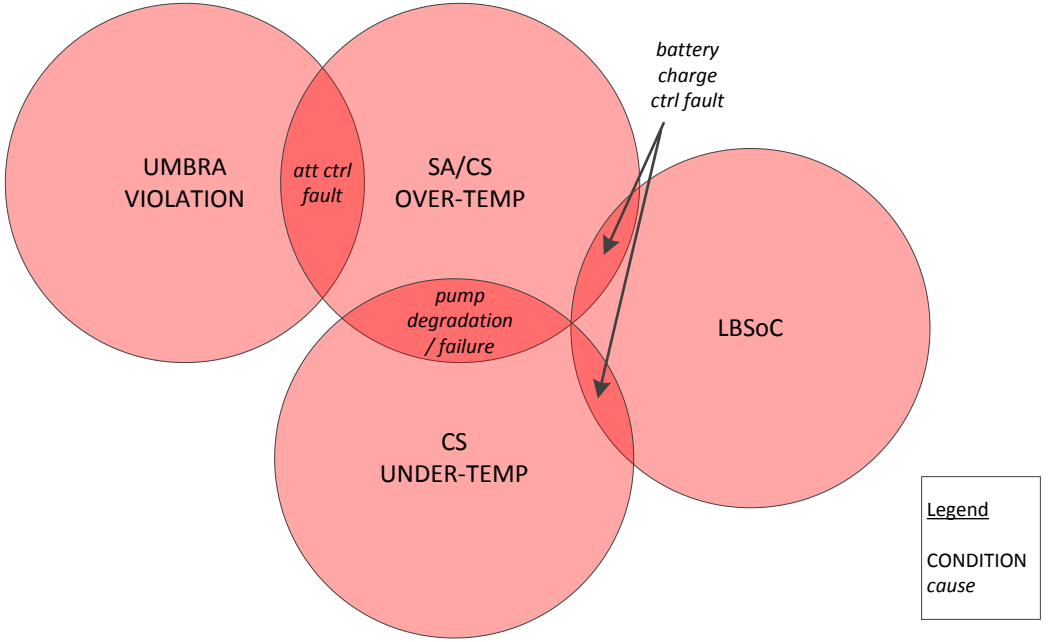




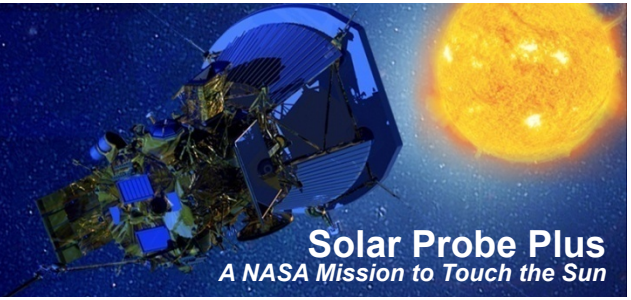
Power & Thermal Critical Faults: Safe Mode – Solar Array



- ***Discussed in detail in dedicated Solar Array Safing section.***
- **SPP's G&C, power, and cooling systems are tightly coupled; multiple critical scenarios may result from a single fault source.**
- **Safing responses to all power and thermal critical fault symptoms are identical, allowing the response to simultaneously provide recovery action to multiple critical scenarios.**



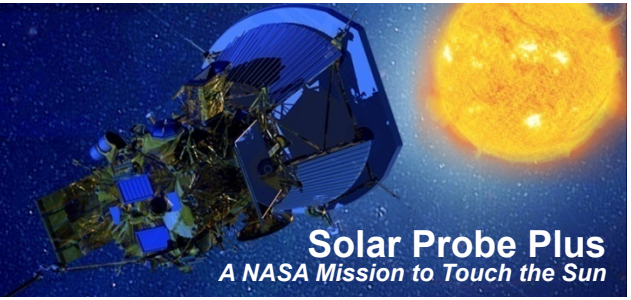
Safe Mode – Solar Array Availability



- In the event of power and thermal critical faults within 0.35 AU, a steady state safe mode is not available to SPP.
  - There is no fixed solar array wing angle that will maintain the cooling system within thermal limits (steady-state) and allow attitude error up to umbra violation.

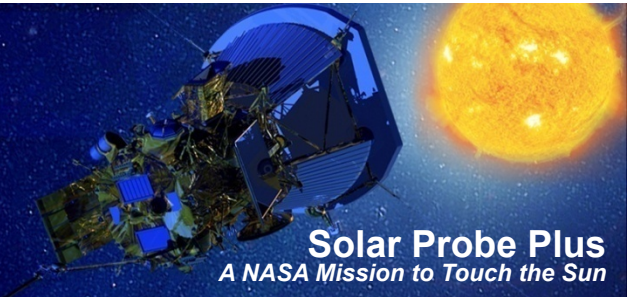
- SPP implements a transient solar array safing operation within Safe Mode – Solar Array for power and thermal critical faults.

Transient Solar Array Safing

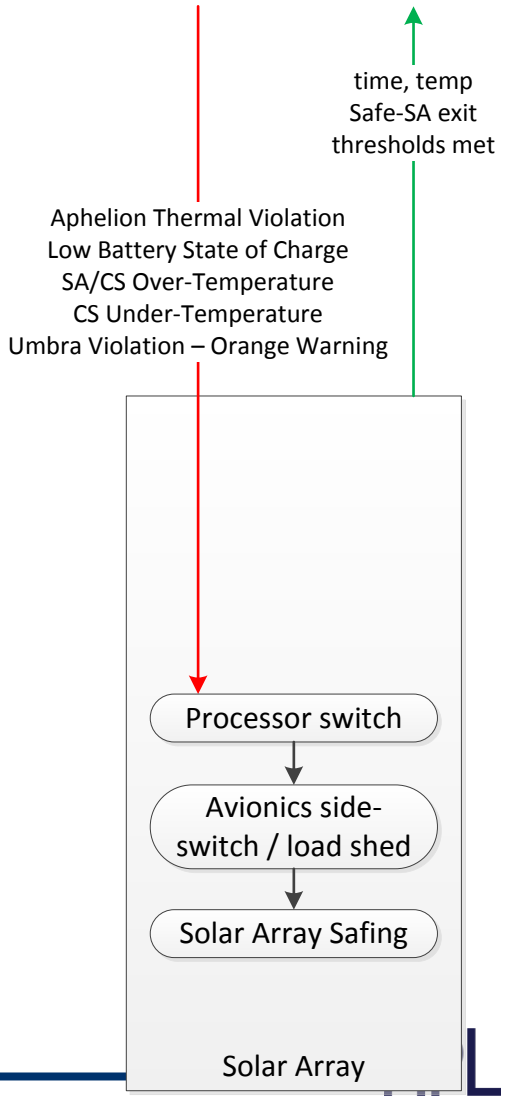


- Solar array wings are moved to a position which minimizes load into the cooling system for attitude errors up to umbra violation.
- Cooling system low-temperature and low battery state of charge thresholds, and duration of transient SA safing, are set such that cooling system temperature and battery SoC remain above critical levels during transient SA safe.
- Available time to move SA wings to transient safe angle, and corresponding selection of angle, is bounded by solar array over-temperature scenario.
  - Fast response needed to ensure SA wings reach transient safe position prior to critical over-temperature
    - 10 seconds allocated from when safing threshold met until commanding of SA to transient safe position
    - Maximum solar array drive speed: 0.5 deg/second
- Provides sufficient time with reduced load to enable recovery from over-temperature conditions.
- SPP must return to nominal solar array control at the conclusion of the transient solar array safing to prevent further power and/or thermal risk.

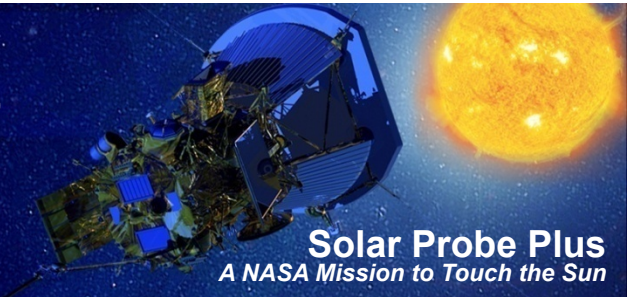
Solar Array Safing Sequence



- **Prime processor demotion takes place first**
  - **Allows remaining safing to be commanded from new Prime**
- **Prime processor demotion and side-switching / power-cycling take place prior to solar array safing**
  - **Allows SA safing to be commanded and implemented by new components**
- **Most components will be power-cycled during safing side-switch**
  - **Exceptions include cooling system pump, solar limb sensors, star trackers, IMUs (TBD), new Prime**
  - **Instruments will be powered off**
- **Command solar arrays to target safing angle**
- **Exit criteria:**
  (> 90 seconds TBR from safing start & <= 125C TBR)
  or 280 seconds TBR from SA safe angle achieved



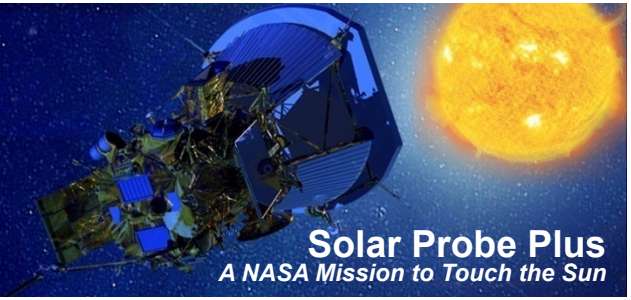
Solar Array wing movement to safe angle



- Both ECUs will be powered-on (original will be power-cycled).
- New ECU will be used for control.
- Prime will collect potentiometer measurements from both ECUs and vote them against its commanded step count to determine solar array wing position.
- Original ECU will be powered-off immediately after potentiometer telemetry is obtained.
- Prime will reference stored table of safing angles and determine target angle based on MET.*
- Prime, via SA control software, will command the ECU to execute SA drive steps to reach safing angle.

* Protection of MET will be discussed in upcoming presentation section

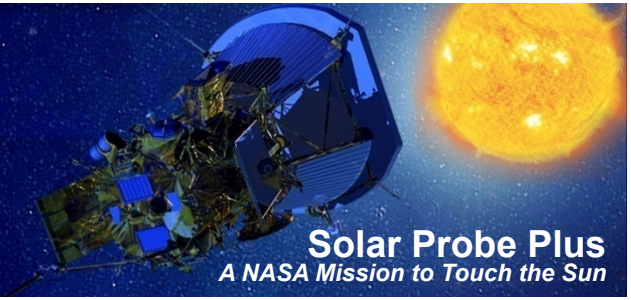
Power-Cycling Exceptions: Cooling system pump



- If the cooling system is at full capacity, a pump failure resulting in pump switch may result in SA platen temperature reaching safing threshold before the new pump is fully operational.
  - Undesirable to power-cycle the new pump while it is attempting to recover the system.
  - Resulting Safe Mode-Solar Array operations will include moving the SA wings to a minimal load position, increasing the rate of temperature drop.

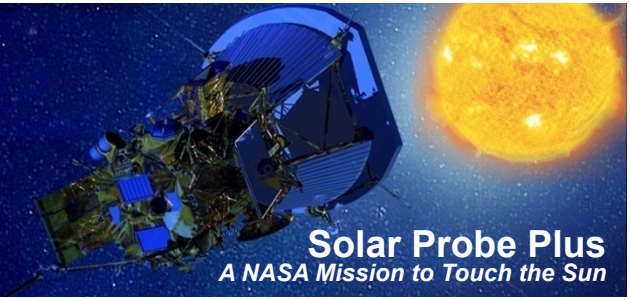
- At solar distances < 0.5 AU TBR dP, motor speed, OR current reading indicating pump failure will initiate pump switch.

Power-Cycling Exceptions: Solar Limb Sensors



- Removal of SLS power interferes with the ability to detect changes in Sun offset angle
  - Computation of Sun offset angle requires continuous monitoring of the two Sun intensity levels
  - Sun presence determination remains available following loss of power

Power-Cycling Exceptions: Star Trackers

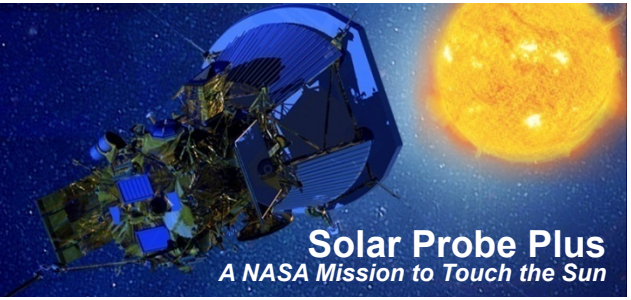


- Removal of star tracker power induces start-up transients which
  - Delays determination of valid attitude solution due to loss of prior attitude knowledge, and
  - Removes potential ability to maintain generation of valid attitude solutions when radiation or stray light is increasing

- If SLS are illuminated,
  - G&C will assume star tracker data is invalid and enter partial attitude and full rate control mode, not using star tracker data
  - Star trackers will be power-cycled upon SLS illumination

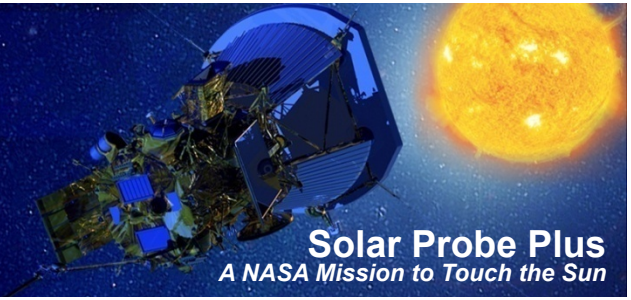
- If Safe Mode – Solar Array is entered but SLS have not been illuminated,
  - G&C has been maintaining attitude control
  - Star trackers are assumed to be operating nominally
  - Star tracker power-cycling not necessary

Power-Cycling Exceptions: IMU



- Removal of IMU power induces start-up transients for gyros which
  - Invalidate prior trending of biases, and
  - Degrades attitude knowledge, most significantly when propagating on gyro rates when star trackers are not available

Detection and Response to Power & Thermal Critical Faults: Timing Budget Summary



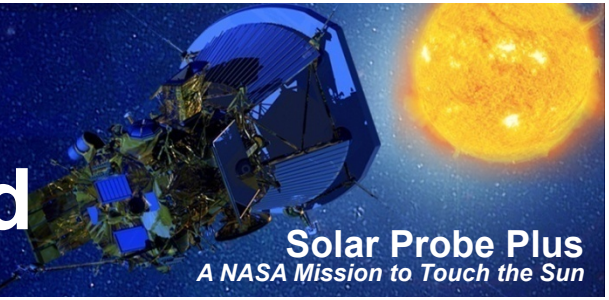
- In selection of transient solar array safe angle, 10 seconds is allocated from when safing threshold met until commanding of SA to transient safe position.

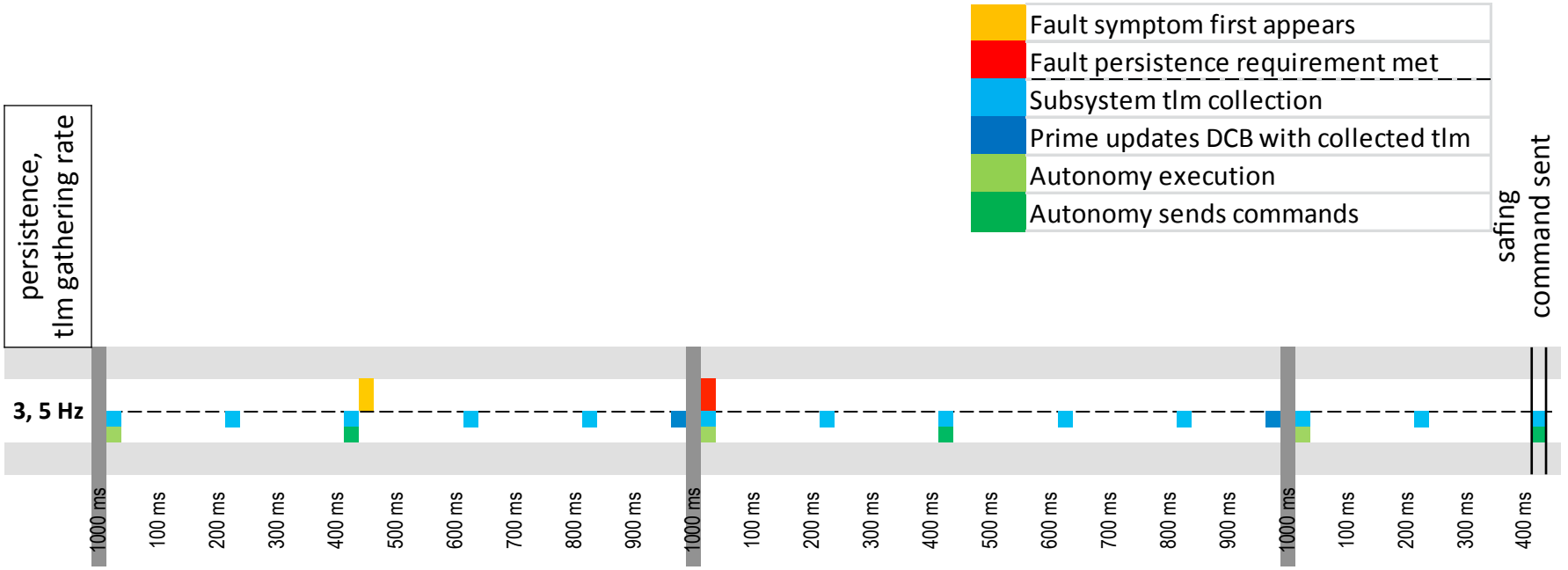
- CBE: ~5.4 seconds

  Steps:

  1. Fault detection to safe mode command sent: ~ 1.8 seconds
  2. Prime processor demotion: ~ 1.5 seconds
  3. Side-switch / power-cycle: ~ 1.3 seconds until ready to evaluate SA position & command safing
  4. Solar array safe: ~ 0.8 seconds to evaluate SA position & command SA movement to safe angle

Step 1:
Fault detection until safing cmd

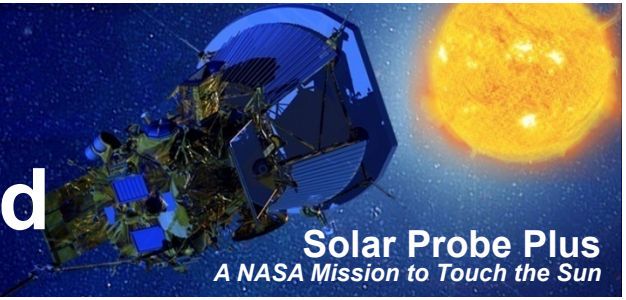




Worst-case:

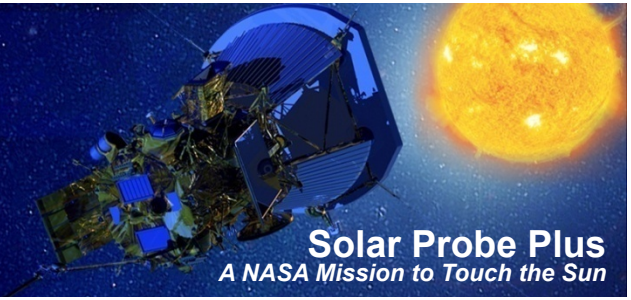
- Fault symptoms appear just late enough to have required persistence met just after the next telemetry load into the DCB.
- Must wait 1 additional second to have persistent fault indication in telemetry load into DCB.
- Autonomy receives telemetry indicating fault at the start of the next second, and issues command to safe ~400 ms later.

Step 1:
Fault detection until safing cmd



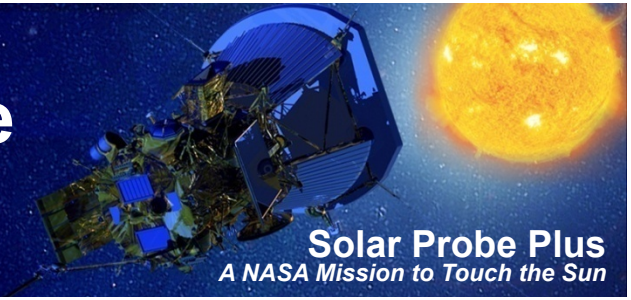
Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
fault occurs and fault symptoms persist			Assumes 3 of 5 persistence requirement 5 Hz single buffered subsystem tlm collection	400 ms	0.40
next subsystem tlm collection	SCIF A	collection of subsystem tlm	Assumes fault persistence met concurrently with previous subsystem tlm collection	200 ms	0.60
max time from subsys tlm collection to tlm in DCB	SCIF A	send subsystem tlm to Prime DCB	1Hz Assumes fault persistence met just after last Prime DCB update	800 ms	1.40
autonomy execution			Autonomy reads DCB, analyses telemetry, & generates cmds	400 ms	1.80
autonomy commands response	SCIF A	cmd Prime to initiate safe-mode entry	25 Hz commanding Assumes safing command priority is sufficiently high to be executed immediately.	40 ms	1.84

Step 2:
Prime processor demotion



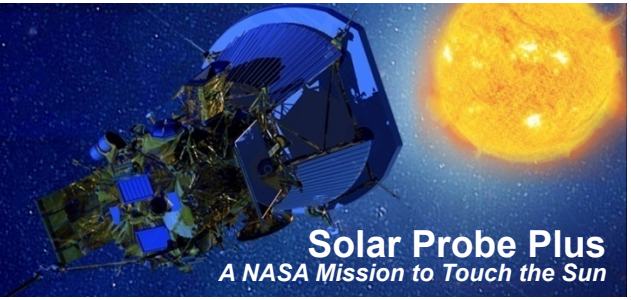
Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
halt 50 Hz SpW bus schedule			20 ms to complete current minor frame & receive notice at start of next minor frame to halt bus sched.	20ms	1.86
Prime informs HS of safe-mode entry & time	HS & SCIF A	cmd setting 'safe-mode entered' flag in HS & indicating safe mode entry & time, & target config, & step count, sent via direct-connect cmd setting 'safe-mode entered' flag in HS & indicating safe mode entry & time, & target config, & step count, sent via SpW router	2 redundant commands via separate paths Feeds soon-to-be-Prime with information necessary to immediately continue safing process, sent via two paths for redundancy	< 1 ms	1.86
Prime self-demotes	ARC	suppresses commands to ARC, timing-out acknowledge timer	max of 515 ms to time-out one MC	515 ms	2.38
new Prime triple-votes logical state to see that it is Prime			max of 186 for all three MC ack timer time-outs and transmit new logical states to SBCs + SBC role voting time (negligible)	186 ms	2.56
contingency for resetting HS scenario			if original HS is resetting (not a fault), it may not ack ARC timer when promoted to Prime and ARC will promote original BS to Prime	701 ms	3.26

Step 3a: Side-Switch / Power-Cycle powering on the new side



Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
new Prime recognizes 'safe-mode entered' flag & initiates safing side-switch			New Prime continues safing operation		
power-off SCIF/ TAC A and power-on SCIF/TAC B and PDU B	ARC	select "SCIF/TAC B, PDU A&B" power state	~20 ms to change power state + max of 1/6 sec until next opportunity for Prime to send command (6 Hz cmding of ARC by SBCs)	187 ms	3.45
		SCIF B & PDU B power-on delay	Assumes 250 msecs for the box converter to turn-on and stabilize + 100 msecs for POR to clear	350 ms	3.80
		Prime cmds SCIF B SpW connect PDU B power-on default initialization	PROM initialization sequence	200 ms	4.00
configure SCIF B	SCIF B	configure routing table select precision oscillator initialize MET initialize time code master select which UART interfaces to enable	this set of commands sent as one RMAP command	< 1 ms	4.00

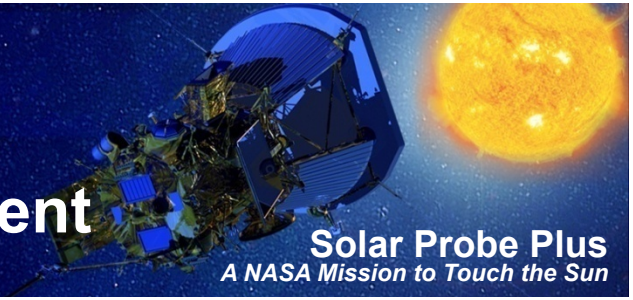
Step 3b: Side-Switch / Power-Cycle maintain power to select loads, power-on/cycle/shed remaining loads



Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
power-on default safing side-switch loads	SCIF B to PDU B	Pump Electronics A Pump Electronics Enable A x2cmds Pump Electronics B Pump Electronics Enable B x2cmds Cooling System dP sensor A Cooling System dP sensor B SLS A SLS B ST A ST B IMU A IMU B TAC B thruster bus x2cmds Prop System PT B	maintain power to active pump, SLS, ST, IMU (TBD) power-on B-side-only loads FSW to start bus controller but not use bus schedule. 5 Hz commanding of PDU, 10 cmds per slot. < 5 ms for execution of 10 cmds.	205 ms	4.21
power-off PDU A*	ARC	selects “SCIF/TAC B, PDU B” power state	powers down PDU A (switched in ARC) Time allocation for this step not included in timeline; completion of PDU A power-down not required for start of next step.	20 ms	4.21

* Removes power from all components (including solar array drive) except those listed in previous step.

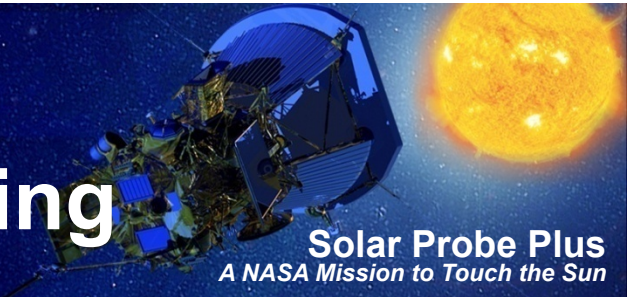
Step 3c: Side-Switch / Power-Cycle: power-on new side to enable SA movement



Solar Probe Plus
A NASA Mission to Touch the Sun

Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
configure PDU B & begin configuration of REM multiplexer	SCIF B to PDU B & SCIF B or TAC B	power on/off loads as appropriate given known previous power configuration and desired changes: ECU A x2cmds ECU B x2cmds Power down Pump Electronics A or B as approp. Power down Pump Electronics Enable A or B as approp. PSE CMD/TLM IF B Wheel A x3cmds Wheel B x3cmds Wheel C x3cmds Wheel D x3cmds cmd to configure relays in REM multiplexer for B-side	table of active components & desired config post-switch maintained in FSW & updated by autonomy, & sent to HS in 1Hz msg & with 'safe-mode entered' flag 5 Hz commanding of PDU, 10 cmds per slot. 180ms remaining since last PDU cmd, given 20ms in last step. < 5 ms for execution of 10 cmds. ECU power first so that they are ready to accept cmds (next step) ASAP	385 ms	4.59

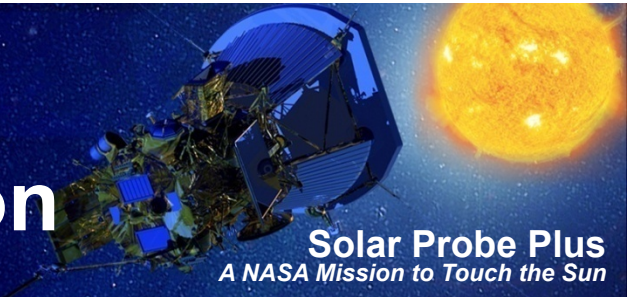
Step 4:
Preparation for solar array safing



Event	Prime cmds:	Command(s)	Notes	time (ms)	cumulative time (s)
collect ECU potentiometer tlm	SCIF B	cmd ECU-A to send potentiometer tlm cmd ECU-B to send potentiometer tlm	5 Hz commanding of ECU, cmds sent to both ECUs at same time 399ms remaining of 600ms ECU power-on delay + 100ms for 10 Hz cmd execution rate = 499 ms	499 ms	5.09
Prime votes 2 ECU potentiometer readings and commanded step count to determine current SA position.					5.09
power-off ECU A	SCIF B to PDU B	power-off ECU A	Time allocation for this step not included in timeline; completion of ECU A power-down not required for start of next step.	200 ms	5.09
Prime determines target SA safing angle with MET-based table reference.					5.09
command SA safing	SCIF B	cmd ECU-B to execute step commands to move wings to target angle with flag indicating safing operation (increased step rate).	5 Hz commanding of ECUs need to maintain 200ms gap since last ECU cmd 10 Hz cmd execution rate	300 ms	5.39

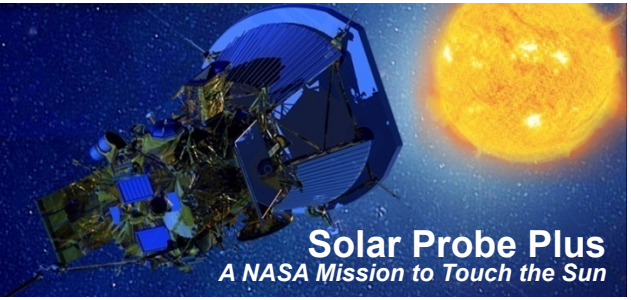
~5.4 seconds from fault occurrence until execution of command to safe solar arrays

Complete side-switch operation



- **Remaining side-switch steps:**
  - Resume 50 Hz SpaceWire bus schedule
  - Configure IMU (pending component selection and IMU interface trade study)
  - Reinforce enable of active pump
  - Configure PSE
  - Power-on non-time-critical loads

New Prime G&C Initialization

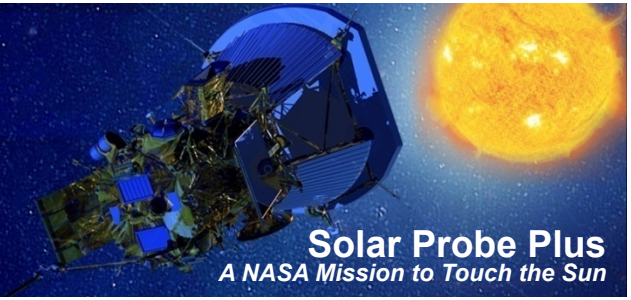


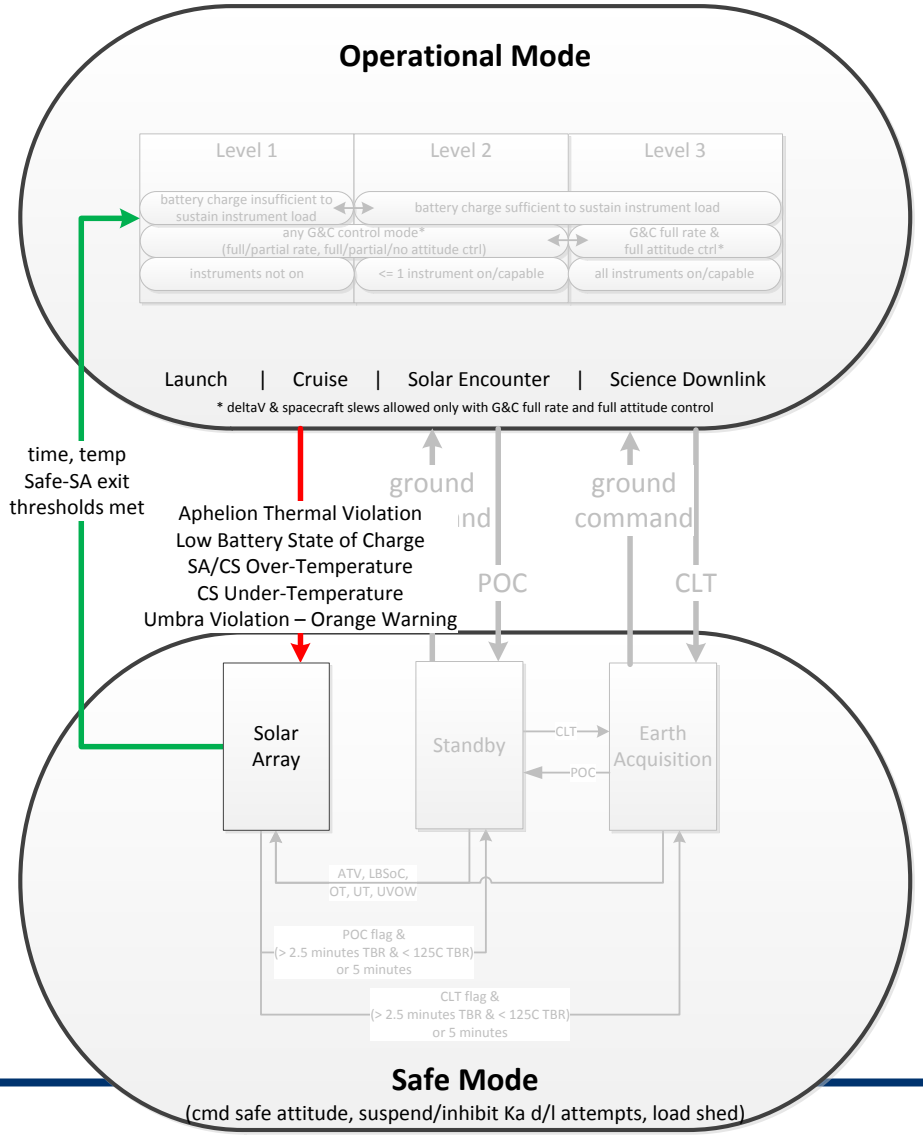
- **ST data provided to HS from Prime at 1 Hz**
  - HS performs initial validation checks on ST data and buffers only compliant data (older data will remain available if newer data is non-compliant)
  - Limited Prime processing of ST data lowers likelihood of corruption of data (vs Prime sending computed attitude solution)
  - New Prime uses buffered ST data only if new ST data is not immediately available

- **G&C software starts running with the new Prime 50 Hz bus schedule initialization**
  - Nominally this is immediate
  - In Safe Mode – Solar Array, this is ~3.5 seconds after safing response initiation

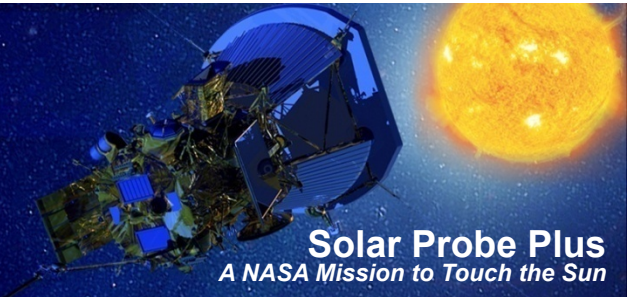
- **New attitude estimate is available after 2 seconds from G&C start on new Prime**
  - High rate collection of new sensor data begins immediately
  - In the 2nd second, G&C calculates attitude estimate based on
    - New data if available
    - Buffered data if new data not available
  - Validity check or wait period may follow acquisition of first new attitude estimate prior to commanding of actuators

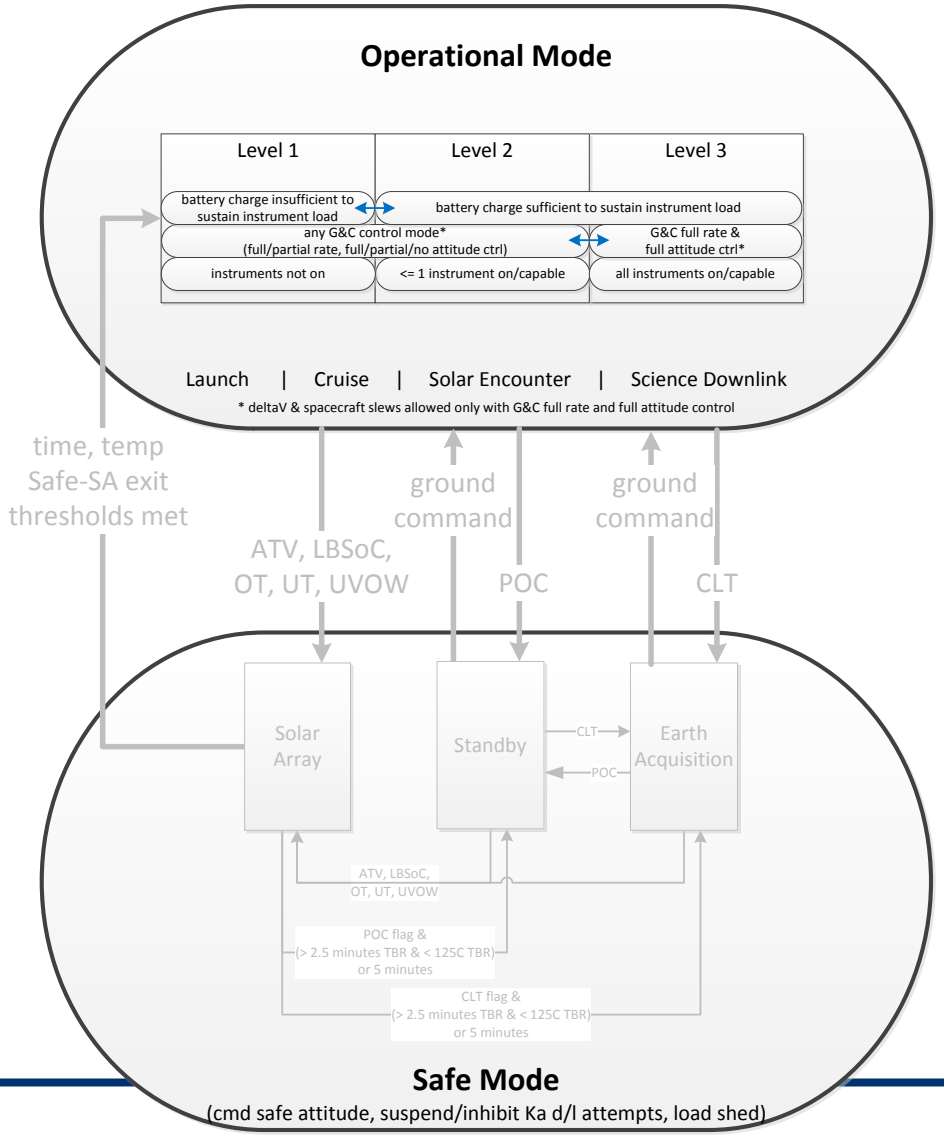
FM Modes diagram: Safe Mode – Solar Array



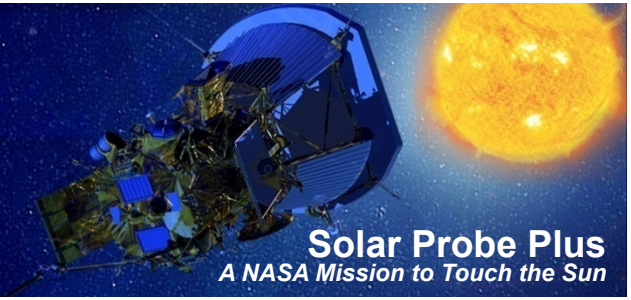


FM Modes diagram: Operational Mode





Operational Mode

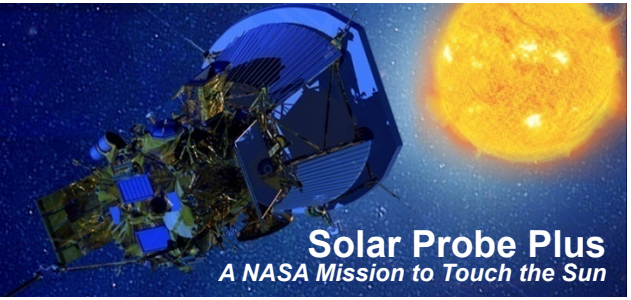


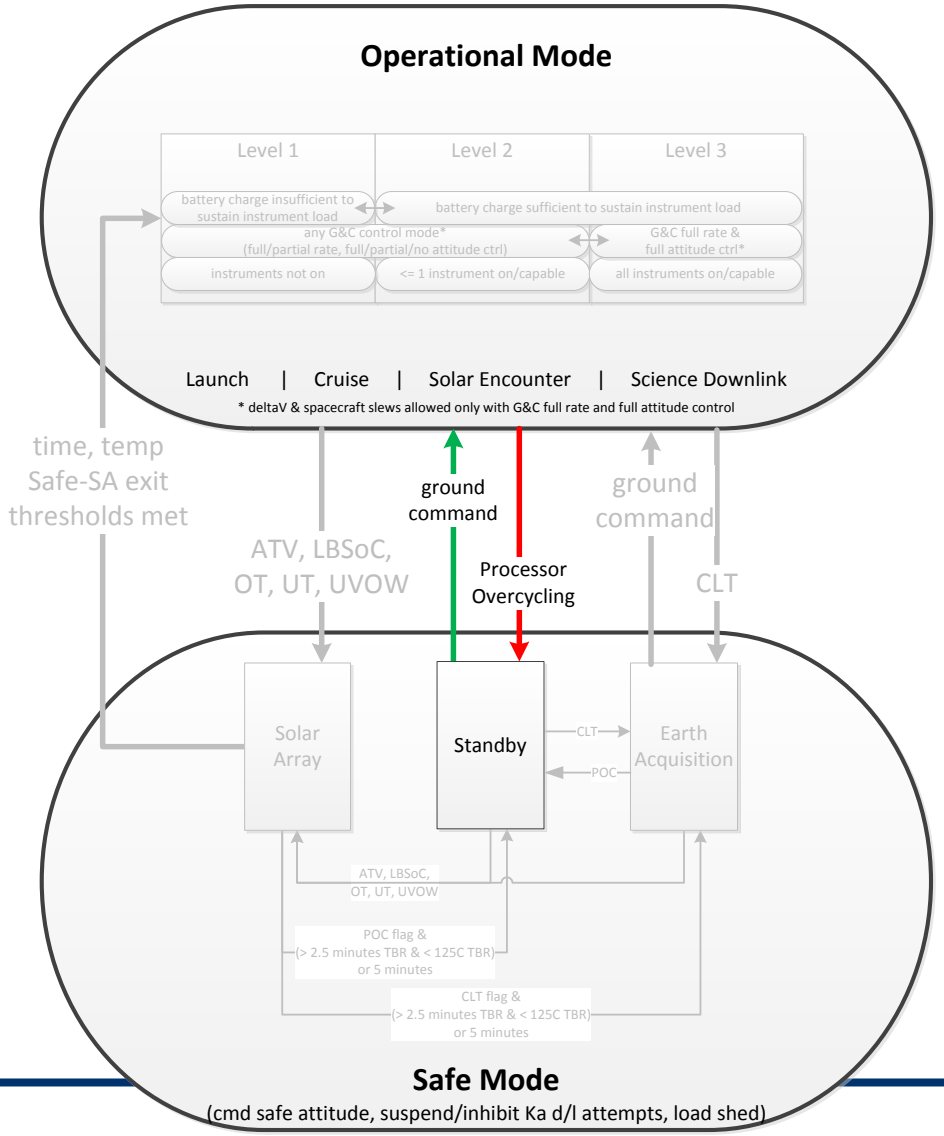
- **SPP will autonomously return to Operational Mode Level 1 following the transient solar array safing response to thermal and power critical faults.**
- **Operational Mode contains three levels:**
  - **Level 1: Returns autonomous solar array wing angle control.**
  - **Level 2: Entered upon sufficient battery recharge to support return of instrument loads.**
  - **Level 3: G&C full rate and full attitude control. Battery charge level sufficient to support all instrument loads.**

Level 1	Level 2	Level 3
battery charge insufficient to sustain instrument load	⟷ battery charge sufficient to sustain instrument load	
any G&C control mode* (full/partial rate, full/partial/no attitude ctrl)		⟷ G&C full rate & full attitude ctrl*
instruments not on	<= 1 instrument on/capable	all instruments on/capable

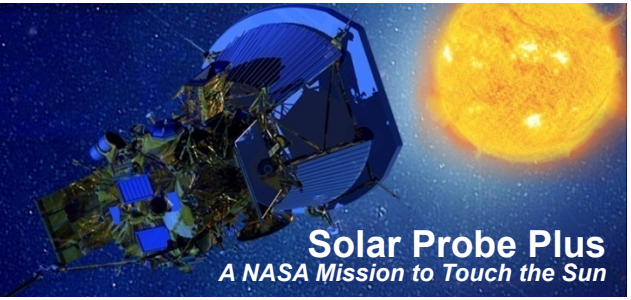
* delta V & spacecraft slews allowed only with G&C full rate and full attitude control

FM Modes diagram: Safe Mode - Standby

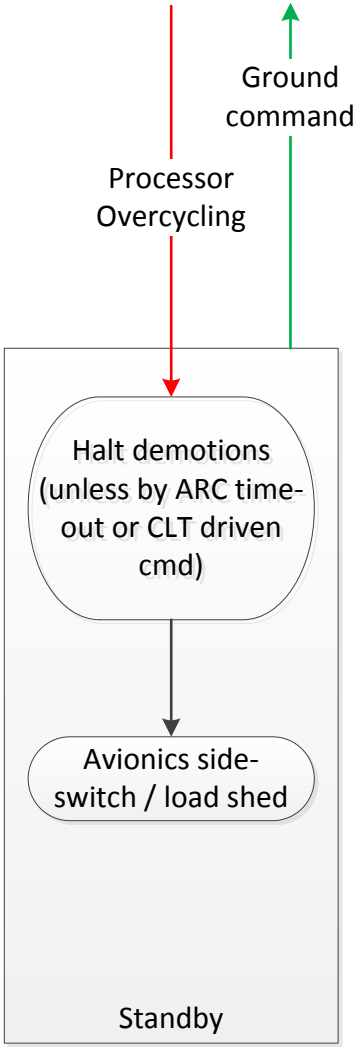




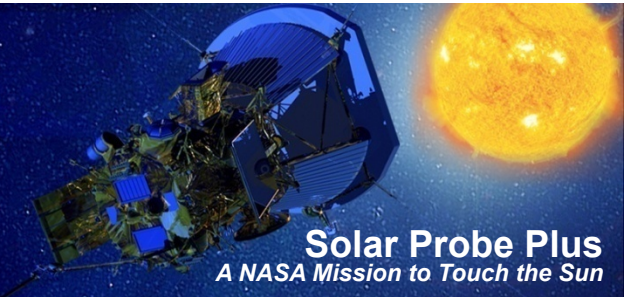
Commanding Critical Fault: Safe Mode - Standby



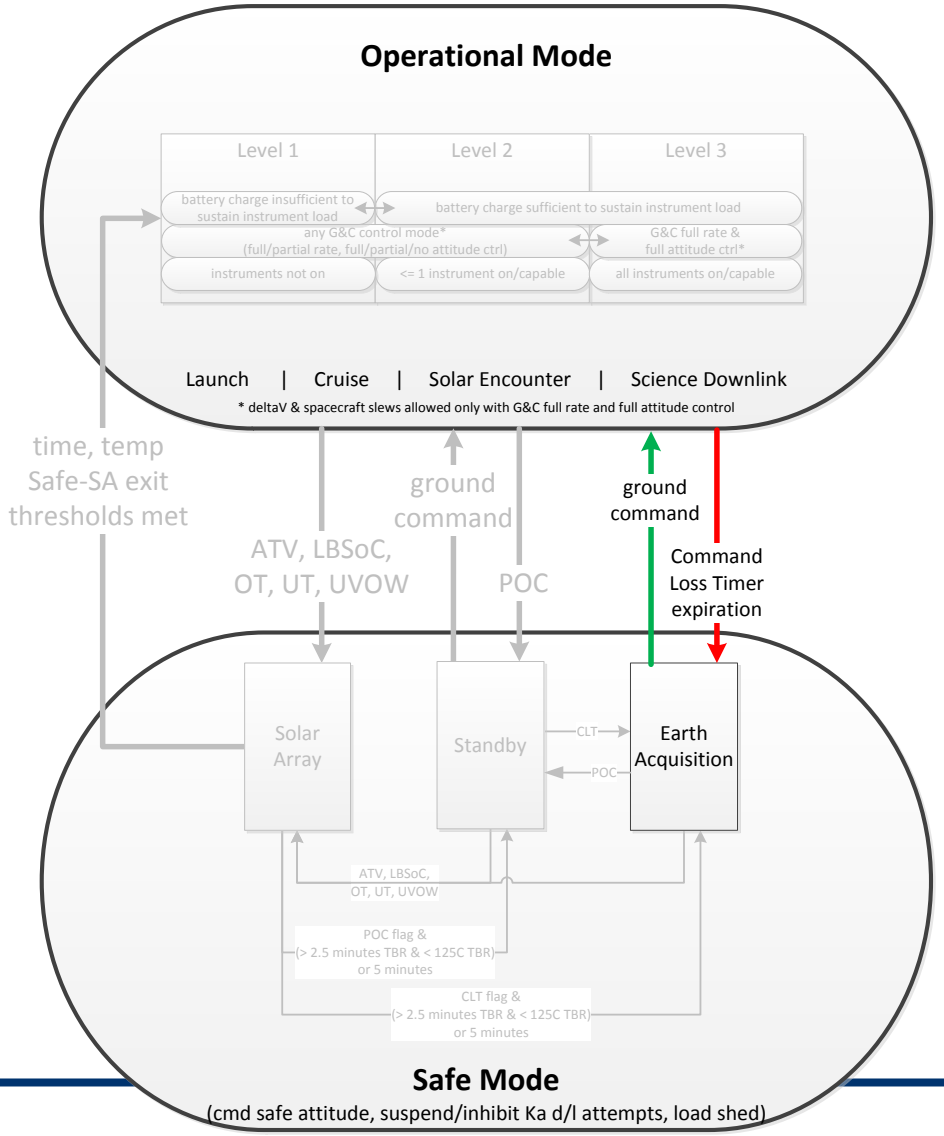
- **Processor Overcycling**
  - **Excessive Prime processor demotions**
- **Safing operation**
  - **Halt Prime processor demotions**
  - **Avionics side switch / load shed**
- **Exit criteria**
  - **Ground command**



FM Modes diagram: Safe Mode – Earth Acquisition

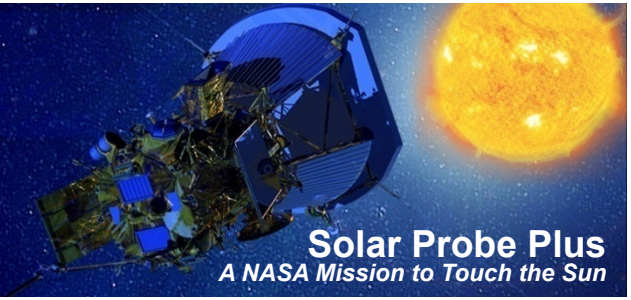


Solar Probe Plus
A NASA Mission to Touch the Sun

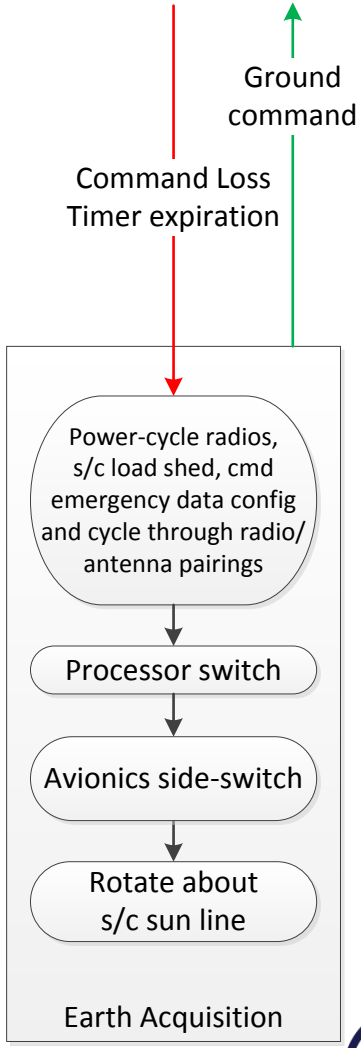


APL

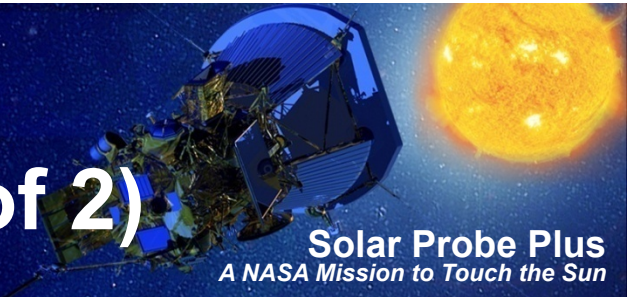
Communication Critical Fault: Safe Mode – Earth Acquisition



- **CLT expiration** (TBD hours wait time for ground contact between each step)
  - **Power-cycle radios, s/c load shed**
  - **Command emergency data configuration**
    - **7.8bps u/l, 10bps d/l, X-band transmitter on, Earth comm pointing**
  - **Configure pre-defined radio/antenna pair sets**
  - **Processor switch**
  - **Avionics side/switch**
  - **Rotate about s/c sun line**
    - **Configure pre-defined radio/antenna pair sets**
- **Exit criteria**
  - **Ground command**



Earth Acquisition Telecomm Reconfiguration Strategy (p1 of 2)

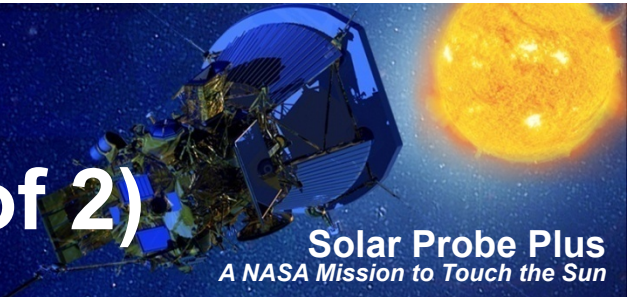


- Step through radio/antenna pairs at defined intervals
  - Ensures predictability of configuration at any given time (keyed off of last CLT-reset command from MOps)

- First level of response assumes valid Earth ephemeris
  - Pairs fanbeam antennas with a transmit & receive radio
  - Pairs –X low gain antenna with a receive-only radio

Transponder A mode	antenna	Transponder B mode	antenna	S/C attitude
Tx/Rx	FB 1	Rx	-X LGA	Comm
Tx/Rx	FB 2	Rx	-X LGA	Comm
Rx	-X LGA	Tx/Rx	FB 1	Comm
Rx	-X LGA	Tx/Rx	FB 2	Comm

Earth Acquisition Telecomm Reconfiguration Strategy (p2 of 2)

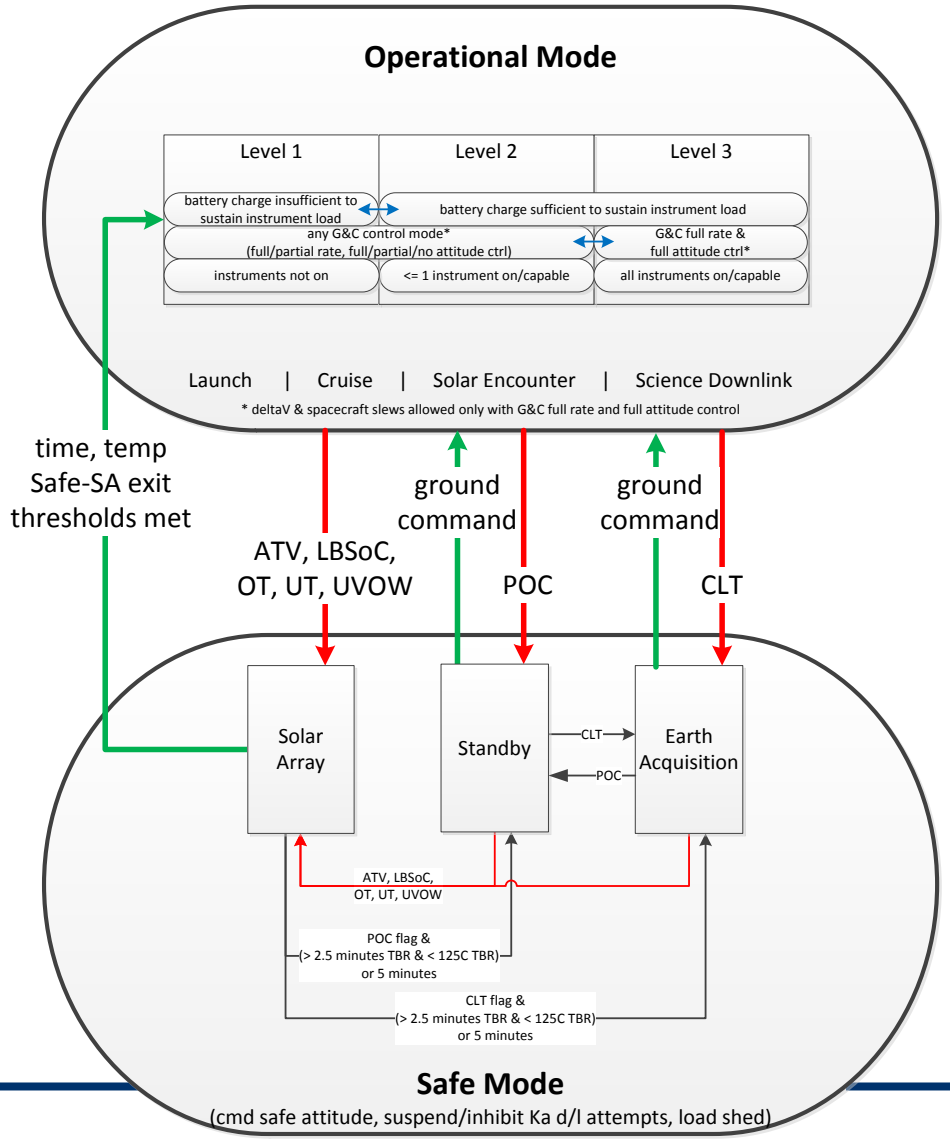


- Second level of response allows for invalid Earth ephemeris
  - Includes s/c rotation about the s/c-Sun line (maintains thermal-safe attitude)
  - Pairs fanbeam antennas with a transmit & receive radio
  - Pairs –X low gain antenna with a receive-only radio
  - Includes all LGA-only permutations

Transponder A mode	antenna	Transponder B mode	antenna	S/C attitude
Tx/Rx	FB 1	Rx	-X LGA	EA Rotation
Tx/Rx	FB 2	Rx	-X LGA	EA Rotation
Rx	-X LGA	Tx/Rx	FB 1	EA Rotation
Rx	-X LGA	Tx/Rx	FB 2	EA Rotation
Tx/Rx	-X LGA	Rx	+X LGA	EA Rotation
Tx/Rx	+X LGA	Rx	-X LGA	EA Rotation
Rx	-X LGA	Tx/Rx	+X LGA	EA Rotation
Rx	+X LGA	Tx/Rx	-X LGA	EA Rotation

APL

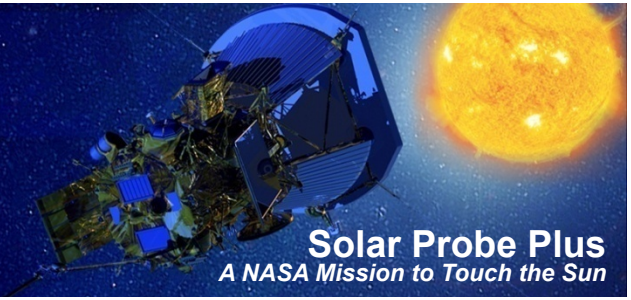
FM Modes



Acronym Definition:

ATV	= Aphelion Thermal Violation
CLT	= Command Loss Timer expiration
LBSoC	= Low Battery State of Charge
OT	= Solar Array / Cooling System Over-Temperature
POC	= Processor Overcycling
UT	= Cooling System Under-Temperature
UVOW	= Umbra Violation – Orange Warning

Safe Mode power loads

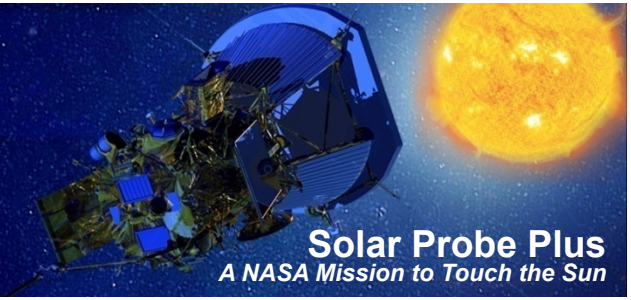


Component	Safe - SA	Safe - Stby	Safe - EA
Instruments			
FIELDS PWI, LNPS, MEP			
FIELDS FGM, SCM, Mag Elec Board			
SWEAP SPC			
SWEAP SPAN A+ and B			
SWEAP SWEM			
WISPR			
ISIS EPI-Hi			
ISIS EPI-Lo			
WISPR DPU			
Telecommunications			
X-band TWTA			x
Radio A rcv only	x	x	
Radio B rcv only	x	x	x
Radio A (rcv+X only)			x
Thermal Control			
Pump, Motor Controller	x	x	x
S/A Drive Heater	x	x	x
Instrument survival heaters	x	x	x

Component	Safe - SA	Safe - Stby	Safe - EA
Avionics and Power Distribution			
RPM	x	x	x
REM	x	x	x
RIU	x	x	x
Power Distribution Unit	x	x	x
Power			
ECU	x	x	x
Power System Electronics	x	x	x
Guidance and Control			
IMU	x	x	x
Star Tracker	x	x	x
Reaction Wheels	x	x	x
Solar Limb Sensor	x	x	x
Propulsion			
Thruster Valves	x	x	x
Catbed Heaters (8)	x	x	x
Valve Heaters	x	x	x
Line Heater	x	x	x
Pressure Transducer	x	x	x

Note: Nominal power load configurations vary by solar distance and activity.

Critical fault responses during planned mission activities



	umbra violation - orange warning	solar array / cooling system over-temp	cooling system under-temp	aphelion thermal violation	LBSoC	CLT	processor overcycling
	Safe - SA	**Safe - SA**	**Safe - SA**	**Safe - SA**	**Safe - SA**	**Safe - EA**	**Safe - Stby**
launch	n/a	n/a	n/a	n/a	inhibit SA movement cmd	comm pointing delayed until G&C in full att/ rate ctrl	=
release SA, detumble, activate SA, rad 1&4	n/a	n/a	n/a	=			=
passive momentum management	=	=	=	=	=	=	=
fanbeam d/l	maintain event pointing & feather angle						
HGA d/l							
activate rad 2&3							
deltaV	abort activity & return to mission default attitude						
instrument & s/c calibration							
fixed inertial attitude							

Critical Faults Requirements Flow

Solar Probe Plus
A NASA Mission to Touch the Sun

4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

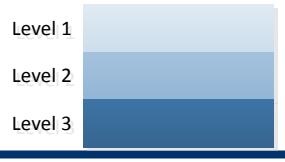
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

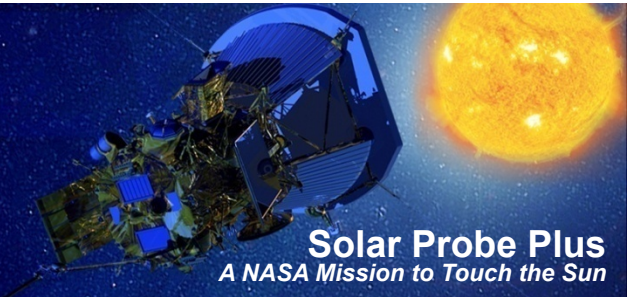
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



Autonomy



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

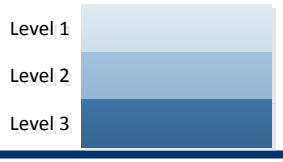
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

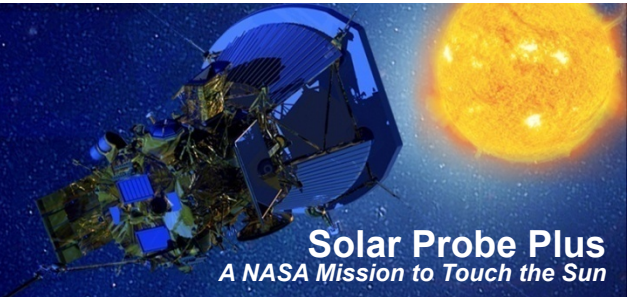
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



Autonomy: L3 Requirements

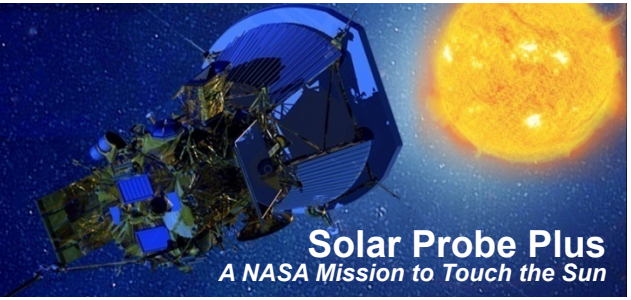


Solar Probe Plus
A NASA Mission to Touch the Sun

The Spacecraft shall …	Allocations
provide an on-board autonomous system to detect and respond to faults.	AV, PDU, FSW, AUT, TST
be designed to provide spacecraft telemetry to enable fault detection on-board.	ME, TH, CS, EPS, GC, PRP, TEL, AV, PDU, FSW, HAR, TST

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Detection of Critical Fault Conditions



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

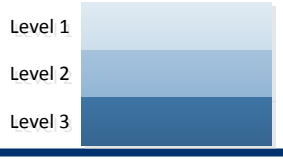
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

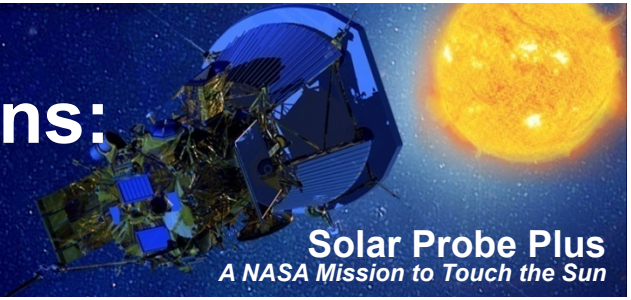
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



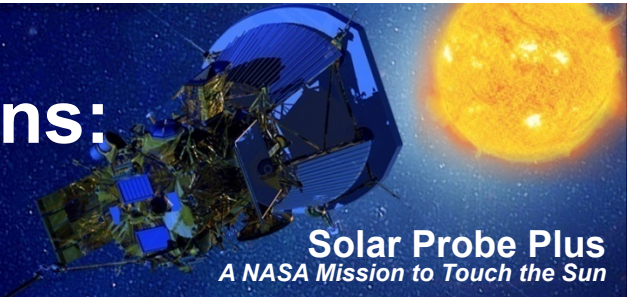
Detection of Critical Fault Conditions: L3 Requirements & Allocations



Critical Fault	The Spacecraft shall …	Allocations
Command Loss Timer expiration (CLT)	provide a Command Loss Timer.	TEL, FSW, AUT, TST, MOP
	provide telemetry to indicate CLT-expired condition.	TEL, FSW, AUT, TST
Processor Overcycling (POC)	detect Processor Overcycling.	AV, FSW, AUT
	provide telemetry to indicate Processor Overcycling condition.	AV, FSW, AUT
Low Battery State of Charge (LBSoC)	detect LBSoC.	EPS, AUT
	provide telemetry to support diagnosis of LBSoC condition at 5 Hz.	EPS, AV, FSW
Umbra Violation – Orange Warning (UVOW)	be designed to provide a warning to attitude control prior to an umbra violation for the Observatory for solar distances <0.7AU.	TPS, TH, GC, AV, FSW, AUT, TST
	provide telemetry to indicate Umbra Violation - Orange Warning condition at 5 Hz TBR.	GC, AV, FSW
Aphelion Thermal Violation	be designed to provide warning to attitude control prior to an aphelion thermal violation for the Observatory for solar distances >= 0.7 AU.	TPS, TH, GC, AV, FSW, AUT, TST
	provide telemetry to indicate an aphelion thermal violation condition.	GC, AV, FSW

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

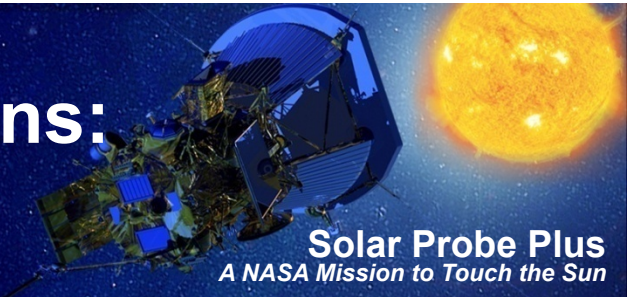
Detection of Critical Fault Conditions: L3 Requirements & Allocations



Critical Fault	The Spacecraft shall …	Allocations
Solar Array / Cooling System over-temperature (OT)	be designed to autonomously monitor the solar flux and thermal conditions of each end of the outboard-most string of each solar array wing to indicate nominal environments, thermal violations, and survival environments.	EPS, FSW, AUT
	be designed to autonomously monitor the thermal conditions of each solar array platen (at inlet and outlet) to indicate nominal environments, thermal violations, and survival environments.	CS, EPS, FSW, AUT
	provide telemetry to support diagnosis of SA over-temperature condition at 5 Hz TBR.	CS, EPS, AV, FSW
Cooling System under-temperature (UT)	be designed to autonomously monitor the thermal conditions of each cooling system radiator to indicate nominal environments, thermal violations, and survival environments.	CS, FSW, AUT
	provide telemetry to support diagnosis of CS under-temperature condition at 1 Hz TBR.	CS, AV, FSW

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

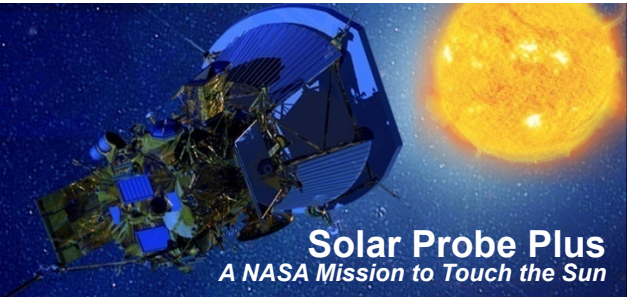
Detection of Critical Fault Conditions: L3 Requirements & Allocations



Critical Fault	The Spacecraft shall …	Allocations
OT, UT, LBSoC, UVOW, ATV	use a parametric table of Suns thresholds vs. MET to define the solar flux safe mode entry criteria.	EPS, FSW, AUT, TST, MOP
	ensure ephemeris is single fault tolerant.	GC, AV, FSW, MOP
	ensure that MET and TDT are single fault tolerant.	TEL, AV, FSW, TST
	respond to detected time fault.	AV, FSW, AUT, TST

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Safing for Critical Fault Conditions



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

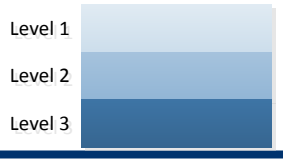
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

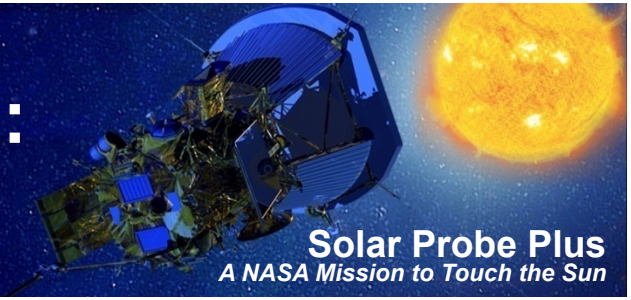
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



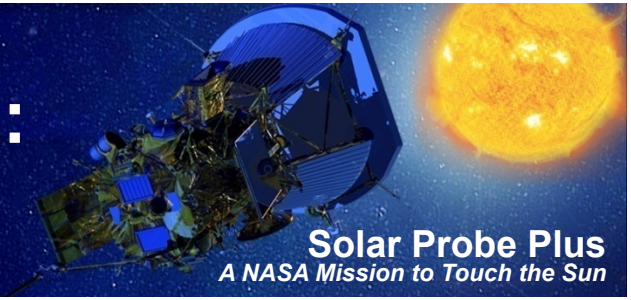
Safing for Critical Fault Conditions: L3 Requirements & Allocations



Critical Fault	Safing Type	The Spacecraft shall …	Allocations
CLT expiration	Safe Mode – Earth Acquisition	autonomously initiate Safe Mode-Earth Acquisition in the event of CLT expiration.	AUT
Processor Overcycling	Safe Mode - Standby	autonomously initiate Safe Mode-Standby in the event of processor overcycling.	AUT
Umbra Violation – Orange Warning	Safe Mode – Solar Array	shall enter safe mode if SLS indicates Umbra Violation-Orange Warning.	GC, AUT
Solar Array Over-Temperature		be capable of autonomously reducing the load to the cooling system to <=2050W (TBR) in response to a hot cooling system thermal violation within 1) 28s at <=9.9Rs (TBR) 2) 40s at > 9.9Rs and <=20Rs (TBR) 3) 80s at > 20Rs and < 0.5AU (TBR)	CS, EPS, GC, FSW, AUT, TST
		be capable of autonomously reducing the load to the cooling system to <=2050W (TBR) in response to a solar flux violation within 1) 28s at <=9.9Rs (TBR) 2) 40s at > 9.9Rs and <=20Rs (TBR) 3) 80s > 20Rs and < 0.5AU (TBR)	CS, EPS, GC, FSW, AUT, TST

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

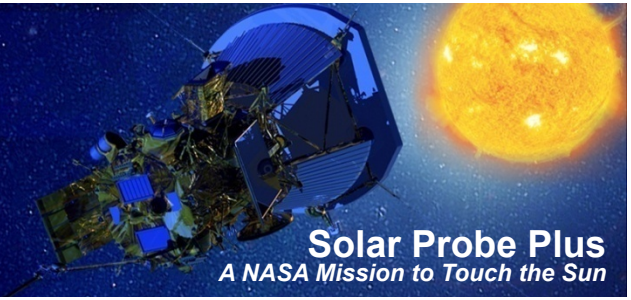
Safing for Critical Fault Conditions: L3 Requirements & Allocations



Critical Fault	Safing Type	The Spacecraft shall …	Allocations
Cooling System Under-Temperature	Safe Mode – Solar Array	be capable of autonomously pointing the solar array normal to the sun in response to a cold thermal violation at >= 0.7AU (TBR) within 3 min (TBR).	CS, EPS, GC, FSW, AUT, TST
		be capable of autonomously pointing the solar array normal to the sun in response to a cold thermal violation at < 0.7AU and >=0.5AU (TBR) within 5 min (TBR).	CS, EPS, GC, FSW, AUT, TST
		be capable of autonomously moving to safe angle (per parametric table) in response to a cold thermal violation at < 0.5AU (TBR)	CS, EPS, GC, FSW, AUT, TST
Low Battery State of Charge		autonomously initiate Safe Mode-Solar Array in the event of LBSoC condition.	AUT
Aphelion Thermal Violation		autonomously initiate Safe Mode-Solar Array in the event of Aphelion Thermal Violation.	AUT
SA/CS Over-Temp, CS Under-Temp, Umbra Violation – Orange Warning, LBSoC		begin execution of Safe Mode-Solar Array initiation command within 80 ms TBR in the event of LBSoC, SA/CS over-temperature, CS under-temperature, Aphelion Thermal Violation, or Umbra Violation - Orange Warning.	FSW, AUT

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Safe Mode Responses



Solar Probe Plus
A NASA Mission to Touch the Sun

4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

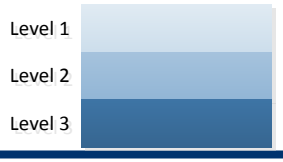
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

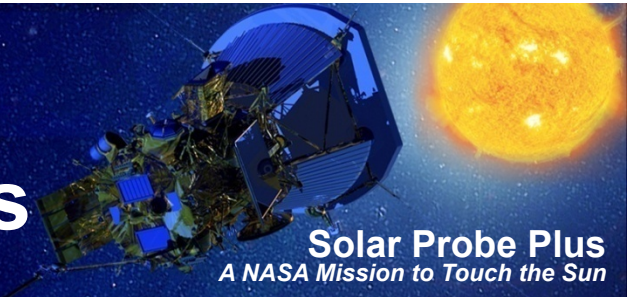
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



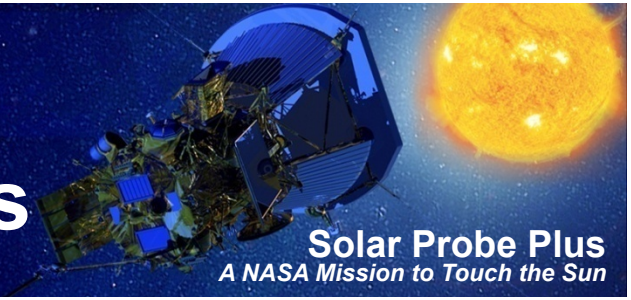
Safe Mode Responses: L3 Requirements & Allocations



Safing Type	The Spacecraft shall …	Allocations
All	be designed to shed non-critical loads in Safe Mode.	TH, EPS, TEL, AV, PDU, FSW, AUT, TST
	suspend and inhibit deltaV maneuvers while in Safe Mode.	GC, FSW, AUT
	suspend and inhibit spacecraft slews, except to mission default or Earth comm attitude, while in Safe Mode.	GC, FSW, AUT
	suspend and inhibit Ka downlink while in Safe Mode.	GC, TEL, FSW, AUT
Safe - Standby	shall not allow further Prime processor demotions in the event of Processor Overcycling.	FSW, AUT
Safe - EA	shall execute telecomm subsystem reconfiguration when in Safe Mode-Earth Acquisition.	TEL, AV, FSW, AUT
	shall be capable of spacecraft rotation about the spacecraft-sun line when in Safe Mode-Earth Acquisition.	GC, FSW, AUT

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

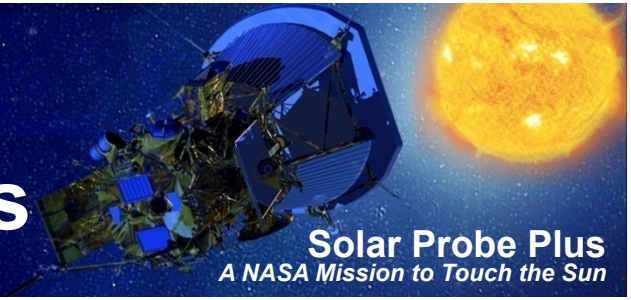
Safe Mode Responses: L3 Requirements & Allocations



Safing Type	The Spacecraft shall …	Allocations
Safe Mode – Solar Array	remove power from the solar array drive within 2.5 seconds TBR of Safe Mode-Solar Array initiation.	AV, PDU, FSW
	complete a processor rotation and side switch, and follow the sequence specified in the FM Design Specification, 7343-****, prior to commanding the solar array to a safe angle.	EPS, GC, AV, PDU, FSW, AUT
	promote new Prime processor within 1.5 seconds TBR from Safe Mode-Solar Array initiation.	AV, FSW, AUT
	execute Safe Mode-Solar Array side-switch operation to enable solar array commanding, as defined in FM Design Specification 7343-****, within 2 seconds TBR.	AV, PDU, FSW
	be capable of determining current solar array angle, determining target solar array angle, and commanding solar array movement within 1 second TBR when in Safe Mode-Solar Array.	EPS, GC, AV, FSW

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

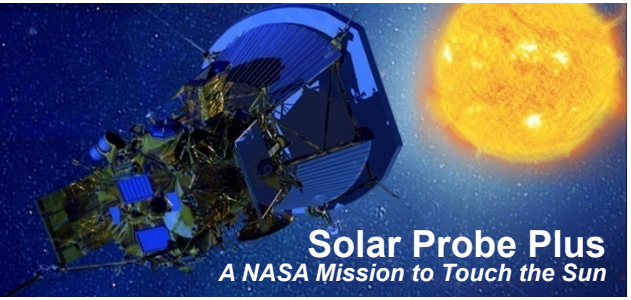
Safe Mode Responses: L3 Requirements & Allocations



Safing Type	The Spacecraft shall …	Allocations
Safe Mode – Solar Array	be capable of receiving telemetry from both redundant coarse potentiometers.	ME, EPS, AV, FSW
	be capable of receiving telemetry from both redundant fine potentiometers.	ME, EPS, AV, FSW
	use a parametric table of solar array safe angles vs. MET to define the solar array safe angle in a critical fault response.	EPS, FSW, AUT, TST, MOP

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Return to Operational



4.2.1. Solar Probe Plus shall complete at least three orbits with a minimum perihelion distance of less than 10 Rs from the center of the Sun.

MRD-71: The Mission shall ensure that the observatory is protected from the sun at solar distances less than 0.7 AU with the exception of the TPS, solar array wings, SLS, FIELDS PWI antennas, and SWEAP SPC.

MRD-74: The Mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.

MRD-75: The Mission shall provide a means to recover to an operational state from critical faults.

CONTINUITY OF CONTROL
The Spacecraft shall …

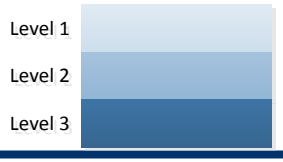
AUTONOMY
The Spacecraft shall …

DETECTION OF CRITICAL FAULT CONDITIONS
The Spacecraft shall …

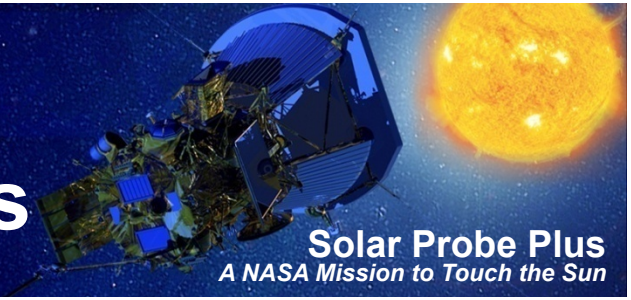
RETURN TO OPERATIONAL
The Spacecraft shall …
The Ground System shall …

SAFING FOR CRITICAL FAULT CONDITIONS
The Spacecraft shall …

SAFE MODE RESPONSES
The Spacecraft shall …



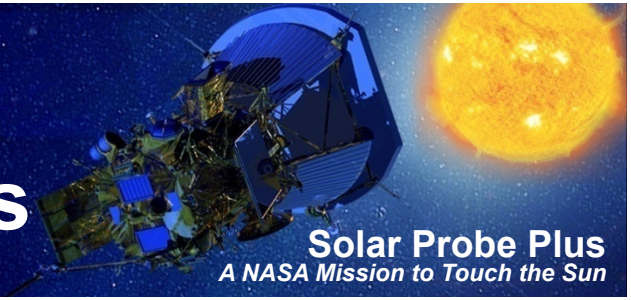
Return to Operational: L3 Requirements & Allocations



Safing Type	The Spacecraft shall …	Allocations
Safe Mode – Solar Array	be capable of returning the solar array to autonomous control from safe angle within 5 minutes (TBR) of solar array safe mode initiation if initial temperature is <=125C (TBR) and 15 min (TBR) of Safe Mode – Solar Array initiation if initial temperature is > 125C (TBR), when < 0.35AU (TBR).	EPS, GC, FSW, AUT, TST
	be capable of returning from Safe Mode - Solar Array to Operational Level 1 in sufficient time to ensure the SA remains within temperature constraints.	TH, CS, EPS, GC, PRP, TEL, AV, PDU, FSW, AUT, TST
Safe Mode – Earth Acquisition	provide the capability for ground commanded promotion from Safe Mode to Operational Mode.	AV, FSW, AUT
	reset the CLT only upon receipt of dedicated CLT-reset ground command.	AUT
Safe Mode - Standby	provide the capability for ground to re-enable processor cycling capability.	FSW, AUT

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

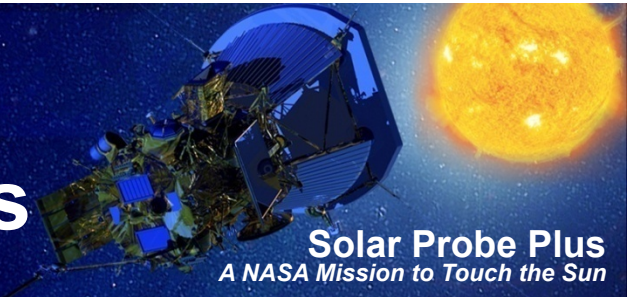
Return to Operational: L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Operational Mode Transitions	shall transition from Operational Level 1 to Operational Level 2 when battery state of charge is consistent with power configurations defined in Spacecraft System Engineering Power Loads Budget.	EPS, FSW, AUT
	shall transition from Operational Level 2 to Operational Level 3 when G&C has full rate and full attitude control.	GC, FSW, AUT
	shall transition from Operational Level 3 to Operational Level 2 if G&C does not have full rate and full attitude control.	GC, FSW, AUT
	shall transition from Operational Level 2 to Operational Level 1 if battery state of charge is below the level specified in power configurations as defined in Spacecraft System Engineering Power Loads Budget.	EPS, FSW, AUT

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

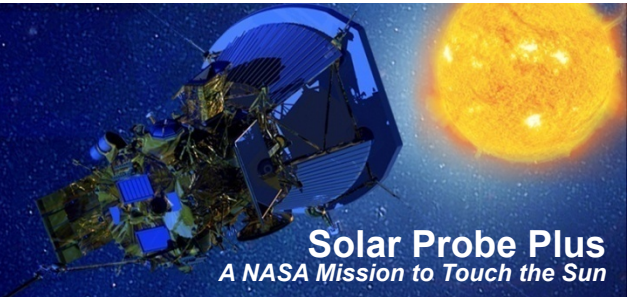
Return to Operational: L3 Requirements & Allocations



Safing Type	The Ground System shall …	Allocations
Safe Mode – Earth Acquisition	provide a dedicated command to reset CLT.	

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Ground Intervention Concept

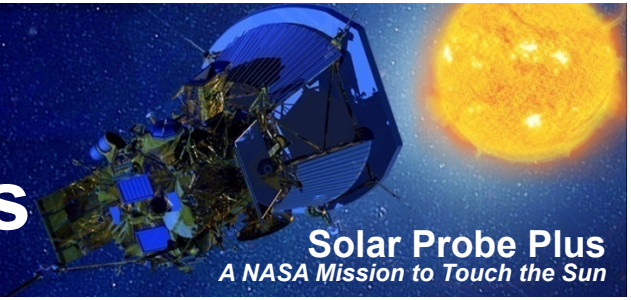


- **Fault resolution via ground commanding is accommodated, however the system is designed for autonomous fault detection, diagnosis, and response.**

- **Reliance on ground intervention is precluded due to**
  - **Short fault-resolution time requirements**
  - **Long spacecraft-Earth distances**
  - **Periods of link unavailability**

- **In the event of processor overcycling or command loss timer expiration, the spacecraft will autonomously detect the fault condition and demote to Safe Mode.**
  - **The spacecraft is capable of remaining in this condition until ground contact is available, and**
    - Spacecraft will resume mission default attitude if in Safe – EA at 0.25 AU and traveling inward toward perihelion, at 0.7 AU traveling inward, or at 0.82 AU inward or outward.
  - **Ground command is required for promotion from Safe – Standby and Safe – EA to Operational Mode.**

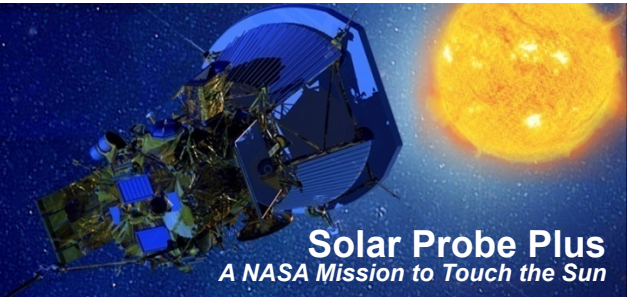
Ground Intervention Concept: L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Spacecraft Critical Commanding	be capable of receiving and executing uplinked critical commands to control critical avionics functions via a path that is not dependent on flight software.	TEL, AV, TST
Spacecraft Provision of Telemetry for Fault Protection on Ground	be designed to provide spacecraft telemetry to enable fault diagnosis on Ground.	ME, TH, CS, EPS, GC, PRP, TEL, AV, PDU, FSW, AUT

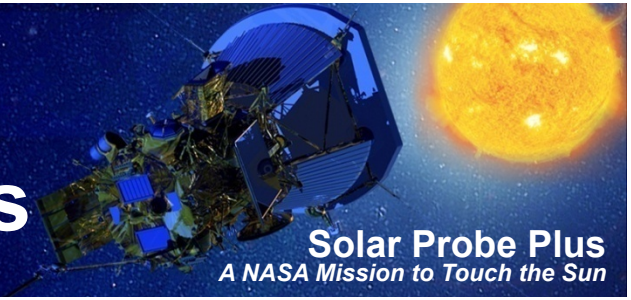
ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

FM Design: Instrument FM



FM Architecture		L3 Requirements group
Redundancy concept		Redundancy Continuity of control
Avionics architecture:	design as driven by FM requirements on redundancy & continuity of control	
Critical Scenarios Safing concept / FM modes Ground intervention concept		Autonomy Detection of critical fault conditions Safing for critical fault conditions Safe mode responses Return to operational
Instrument FM		Instrument FM

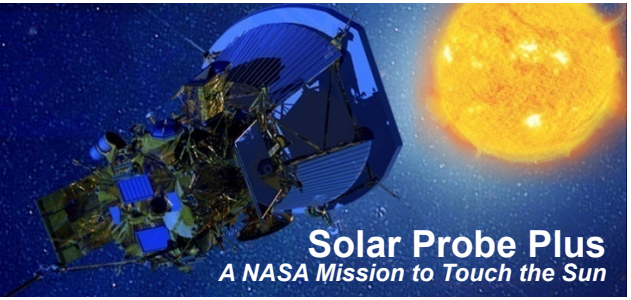
Decoupled Payload Operations



- SPP will implement decoupled payload operations.
  - Mission operations will be unable to issue instrument commands, and
  - Instrument teams will be unable to issue spacecraft commands.
  - Instruments are responsible for their own internal fault management.

- The spacecraft will provide limited instrument fault protection (per MRD-72).
  - Ground system monitoring of selected instrument health data,
  - Remote SOC notification of spacecraft critical fault conditions, and
  - Autonomous onboard removal of instrument power in response to
    - Instrument request,
      - May request to power-down until ground commanded power-up, or
      - Reset: power-down then power-up following pre-determined wait
    - Detection of stale instrument heartbeat,
    - Overcurrent, or
      - Instrument may pre-define a requested number of re-tries (ie power back up, if fault remains then power down, then try again)
    - Spacecraft critical fault (and subsequent spacecraft safe mode initiation).

Instrument Fault Management Requirements Flow



4.2.4. Solar Probe Plus shall be categorized as Mission Category 1 per NPR 7120.5D and Risk Category B per NPR 8705.4.

MRD-70: The Mission shall have no single point failures except those on the single point failure list.

REDUNDANCY

The Spacecraft shall …

(n/a; L2 requirement is a design implementation decision which spans multiple system elements)

MRD-72: The Mission shall provide instrument fault protection to include ground system monitoring of selected instrument health data, remote SOC notifications of critical fault conditions, and autonomous onboard instrument power-downs in response to instrument request and critical telemetry.

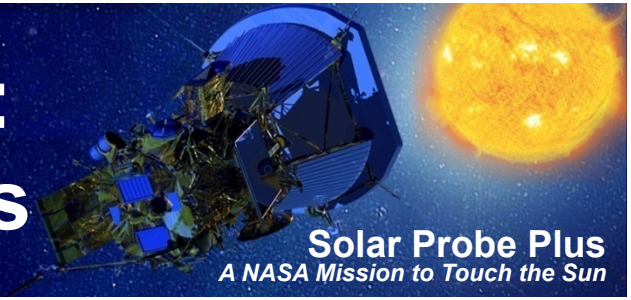
INSTRUMENT FM

The Spacecraft shall …

All SPP instruments shall …

Level 1
Level 2
Level 3

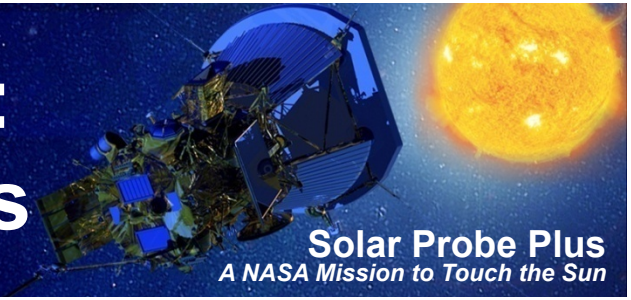
Instrument Fault Management: L3 Requirements & Allocations



	The Spacecraft shall …	Allocations
Autonomous instrument power-down	be designed to provide autonomous onboard instrument power-downs in response to instrument request and critical telemetry.	FSW, AUT
Instrument power-down notification	provide a bit in the s/c status msg to request an instrument put itself in a safe state for power down.	FSW, TST
Protection against instrument failure	be designed such that a fault or failure of one instrument does not propagate to one or more instruments or to the spacecraft.	AV, PDU, FSW, AUT, HAR

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Instrument Fault Management: L3 Requirements & Allocations



	All SPP instruments shall …	Allocations
Instrument health telemetry	provide data to support instrument fault protection (including ground system monitoring of selected instrument health data, remote SOC notifications of critical fault conditions, and autonomous onboard instrument power-downs in response to instrument request, detection of stale instrument heartbeat, or overcurrent).	INS
Safe power-down	be capable of entering a safe state or powering down upon receipt of a spacecraft-provided bit in the s/c status msg to request an instrument put itself in a safe state for power down.	INS
Immediate loss of power accommodation	be designed to accommodate immediate loss of power (without warning) without damage to the instrument.	INS

ME = Mechanical, TH = Thermal, CS = Cooling System, EPS = Electrical Power System, GC = Guidance & Control, PRP = Propulsion, TEL = Telecomm, AV = Avionics, PDU = Power Distribution System, FSW = Flight Software, AUT = Autonomy, HAR = Harness, TST = Testbed, MOP = Mission Operations, IT = Integration & Test, INS = Instruments

Solar Probe Plus

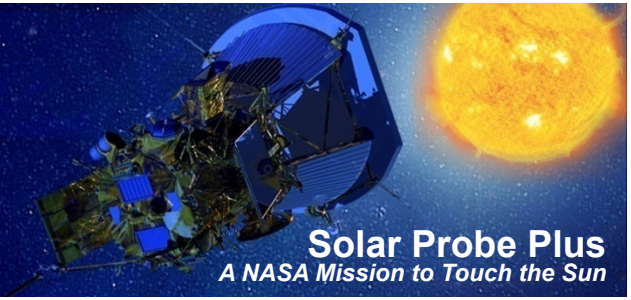
A NASA Mission to Touch the Sun

Fault Analysis Process Overview

Clayton Smith
Reliability Lead Engineer
clay.smith@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

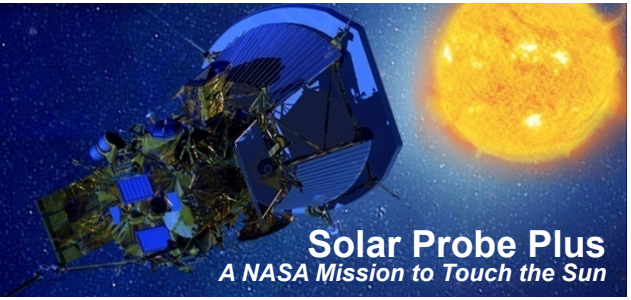
Agenda



- **Process**
  - Requirement
  - Scope
  - Purpose
  - How developed
- **Forward Work**
- **Conclusions**

SPP Reliability Requirements

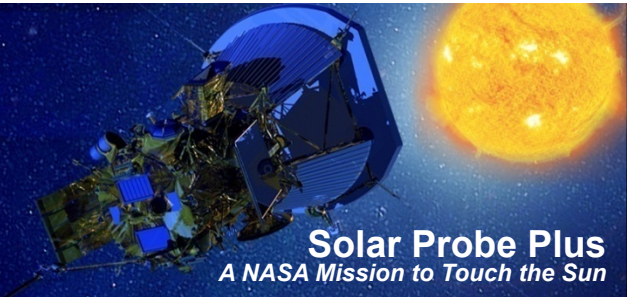
NASA Procedural Requirements



- **NPD 8720.1 "NASA Reliability and Maintainability Program Policy"**
  - Establish reliability performance requirements
  - Integrate all reliability activities with systems engineering, risk management, and other processes, assessments, and analyses including, but not limited to, safety, security, quality assurance, logistics, probabilistic risk assessment, life-cycle cost, configuration management, and maintenance
- **NPR 8705.4 "Risk Classification for NASA Payloads"**
  - Classification Level B
- **Class B requires detail down at "black box (or circuit block diagram) level as minimum"**
  - Functional FMEA (Phase B)
  - Detailed FMEA (Phase C)
  - FMEAs performed consistent with MIL-STD-1629A
  - Instrument providers to perform FMEAs to same level of detail

Reliability Engineering

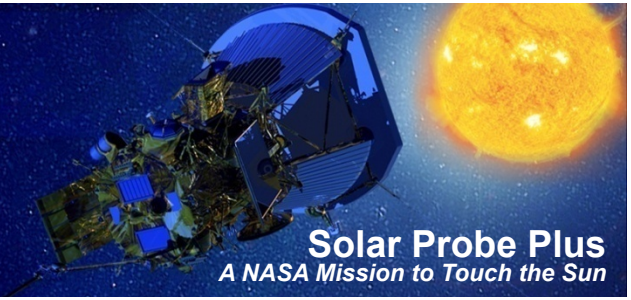
Philosophy



- **Redundancy as directed by Class B mission**
  - Critical single point failures may be permitted but are minimized and mitigated by use of high reliability parts and additional testing
  - Essential spacecraft functions and key instruments are typically fully redundant
  - Other hardware has partial redundancy and/or provisions for graceful degradation
- **Design implementation**
  - Block redundancy as much as possible
    - Less complex system
    - Fewer configurations to test
  - Cross-strap redundancy where timing, local control, or reliability issues warrant
  - Single point failures where unavoidable
- **Qualitative and quantitative assessments to identify risks and validate mitigation strategies**

Failure Mode and Effects Analysis

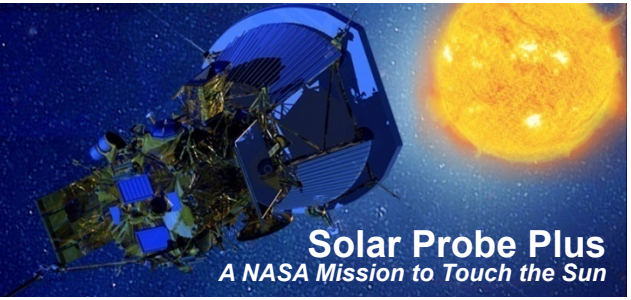
Description



- **FMEA is a systematic approach for identifying potential failures in the design**
  - "Failure modes" means the ways, or modes, in which something might fail
  - "Effects analysis" refers to studying the consequences of those failures
- **Analysis addresses hardware and software**
- **Provides a basis for identifying root failure causes and developing effective corrective actions**
  - Identifies single point failures
  - Facilitates investigation of design alternatives at all stages of the design
  - Provides a foundation for identifying failures and faults for the Fault Management System responses
  - Provides input to the reliability quantification effort, PRA
- **Limitations**
  - Only one item is analyzed at a time, no combinations
  - Worst case consequence

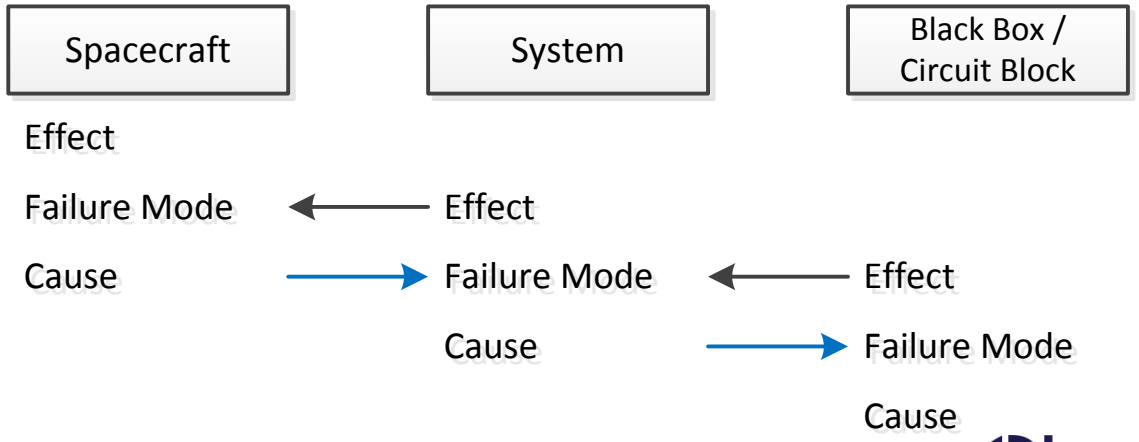
Failure Mode and Effects Analysis

Level of Detail



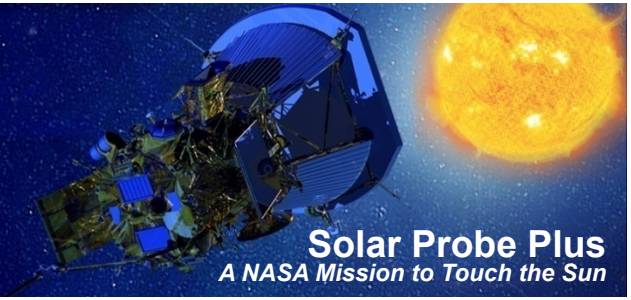
- **At this point the FMEA is analyzed down to a level consistent with design maturity**
  - Lowest level of detail varies from system to system
  - Slice level for PDU and REM
  - Components such as RF switches and mechanisms where necessary to adequately describe the failure mode and cause
  - Box level for COTS items such as G&C components

- **FMEA analysis shows cascading interactions among level of detail**



Failure Mode and Effects Analysis

Structure

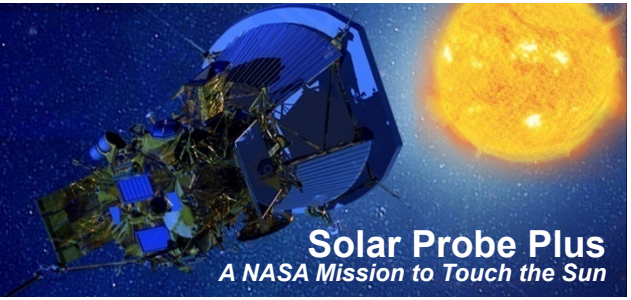


- **FMEA is a spreadsheet format**
- **MIL-STD-1629A is used as a guide to establish the base set of questions**
- **These have been adapted specifically to support the SPP FM activity**
  - Columns added to address fault detection and response
  - Columns added for testing
    - Sets up traceability and documentation form fault identification through verification testing
  - Rows added to include more sources of system responses

Base Structure	Fault Management		Testing & Verification
	Detection	Responses	
Extended Scope (Limit violations, faults, combination pairs, inputs)			

Failure Mode and Effects Analysis

Base Structure

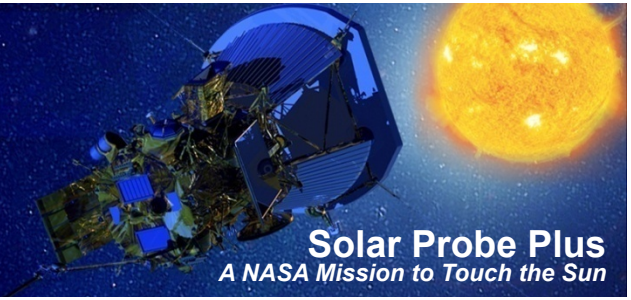


						Effect				
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity

FMEA ID	Unique ID for each failure mode
Name	HW or SW element name
Function	Function the element performs
Failure Mode/ Limit/ Constraint	Specific failure mode, i.e., sensor failure, SW error, electronic part failure
Possible Causes	Credible causes for failure, i.e., radiation upset on FPGA
Phase	Operational phase (Launch, Commissioning, Cruise, Encounter)
Effects	Effects of the failures at various levels
Local	Effect on the failed element
Next Higher	Effect of failed element on subsystem/instrument
Mission	Effect of failed element on mission
Umbra Violation	Is there an effect that can lead to umbra violation? How?
Severity	Rating of severity should failure occur

Failure Mode and Effects Analysis

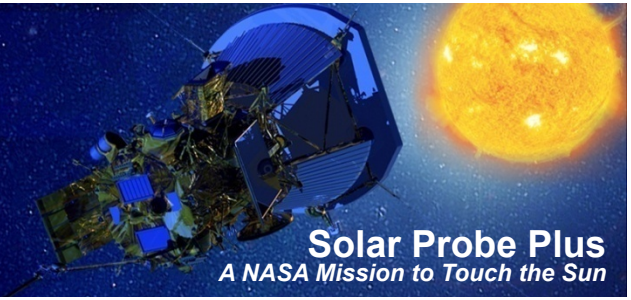
Severity Categories



1	Catastrophic	Failure modes that could result in serious injury, loss of life, or loss of spacecraft.
1R		Failure modes of identical or equivalent redundant hardware or software elements that could result in Category 1 effects if all failed.
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2	Critical	Failure modes that could result in loss of three or more mission objectives
2R		Failure modes of identical or equivalent redundant hardware or software that could result in Category 2 effects if all failed.
2S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 2 consequences.
3	Significant	Failure modes that could cause loss to any mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

Failure Mode and Effects Analysis

Extended Structure

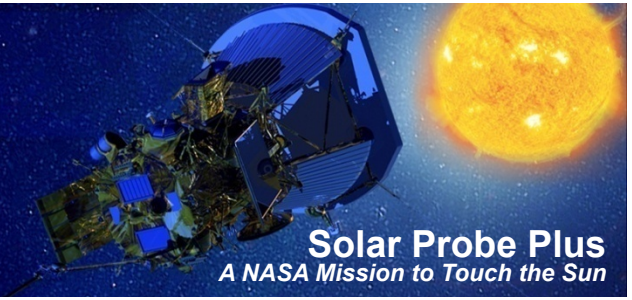


	Detection					
Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)

Type of FM	Active, Passive, None
Observable	Yes/No
How Observed?	How is the fault observed (narrative) / Who observes the fault (HW, FSW, Autonomy, Ground)?
Tlm for diagnosis	Telemetry needed for diagnosis of fault
Tlm path for diagnosis	Where does the telemetry come from, who it is sent to/through
Time to Detect (Local)	Time detect locally (is this persistence?)
Time to Detect (System)	Time to detect at system level (is this persistence?)

Failure Mode and Effects Analysis

Extended Structure

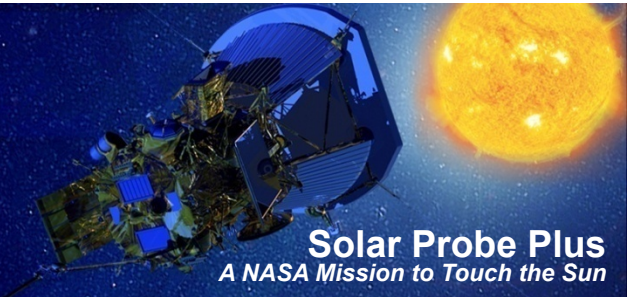


	Response								
Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired SC response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response/ Contingency

Response Level	Local, System, Instrument, or, None
Desired local response	Narrative description of desired action taken locally at subsystem/instrument level
Allocation of local response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before local response begins?
Time to Fix Locally	Time to fix for local response
Desired SC response	Narrative description of desired action taken at system level
Allocation of SC response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before system response begins?
Time to Fix System	Time to fix for system response
Ground Response/ Contingency	Ground response needed (narrative); ideas for steps in contingency plans

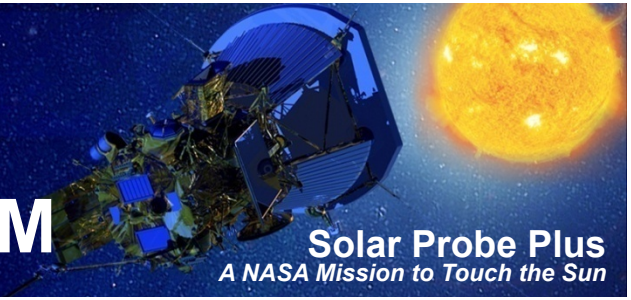
Failure Mode and Effects Analysis

Extended Structure



- **Quick look flags added for sorting purposes**
  - System Side Switch
  - Processor Switch
  - Safe Mode
- **Columns still to be added for test verification**
  - Test name
  - Test report identifier
  - …
- **Line items added to expand completeness of fault space**
  - Limit violations and constraints imposed by system
  - Selected combinations of double failures, failure and responses as identified in the PRA
  - Interfaces with other systems, failure of inputs to an item

Interface between Reliability and FM



Validates FM Design:

1) Timing – can faults be detected, contained, or corrected before becoming critical or missing ending?
2) Interference – can responses interact in a way that results in undesirable state or precludes FM from mitigating fault?
3) Coverage – do all credible faults have a mitigation?

Fault Analysis
(FMEA/PRA)

Fault Set Analysis

List of credible faults to consider

Mitigation Assessment
(Detection/Responsibility)

What needs to be done to mitigate the fault

FM Design Analysis
(Timing, Interference, Coverage)

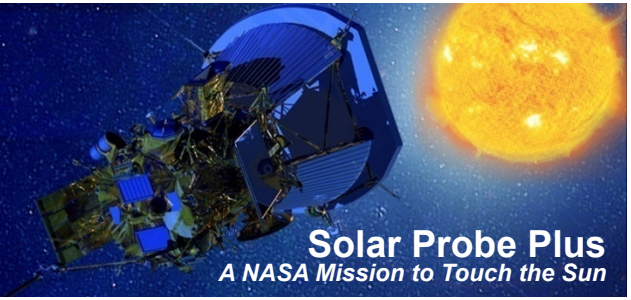
Observables List

FM Design

List of telemetry needed for detection

Failure Mode and Effects Analysis

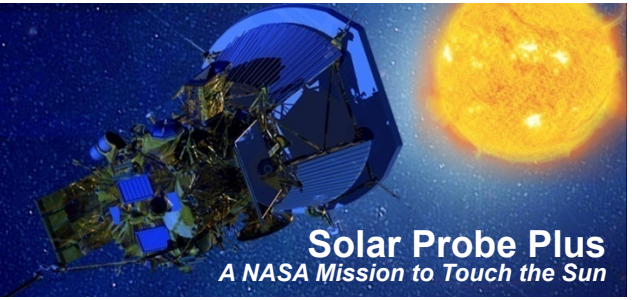
Scope



- **Spacecraft bus (completion consistent with design maturity)**
  - Avionics
  - Electrical Power System
  - Electronics Control Unit
  - Guidance and Control
  - Cooling System
  - Telecom
  - Mechanical
  - Propulsion
  - Thermal
- **Instruments (in progress, due at instrument PDRs)**
- **Third Stage (in progress, preliminary results from motor vendor)**
- **GSE (not yet started)**
- **Mission Control Center (not yet started)**

Failure Mode and Effects Analysis

Process



Created initial FMEA template based on MDR slides and MEL. Compared against RBSP to get initial failure modes

Met with sub-system leads again, reviewed previous work and discussed:
- Inputs
- How failures would be observed
- Remediation

Extracted FP information from FMEA responses

Initial meetings with leads

Follow-up meetings with leads

Meetings with systems and leads

Fault Protection information

Severities added and FMEA cleaned up

Compared against PRA

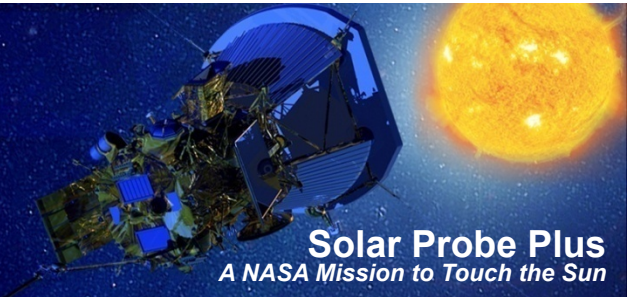
Current state

Met with sub-system leads individually, discussed:
- Addition/ removal of failure modes for each component
- Effects to system

Met with sub-system leads, FM lead, and systems engineers, reviewed previous work, focusing on the system-level effects

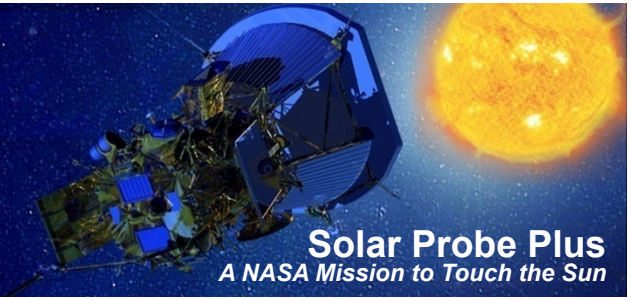
Verified that PRA and FMEA contain the same SPFs, improving both reliability products

Forward Work



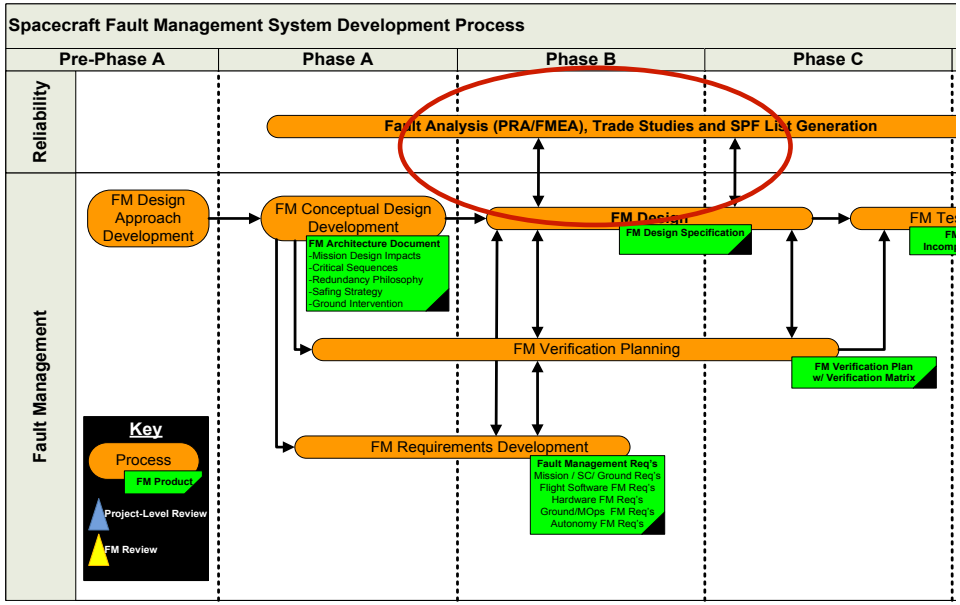
- **By PDR**
  - The FMEA is to the functional level (or lower) already
  - Instruments, software, third stage and all remaining spacecraft bus components will be added (multiplexer)
- **By CDR**
  - The FMEA will be to the circuit/black box level (already there in many cases)
  - Third Stage FMEA will be completed
  - The MOC will be added
  - The FMEA will be used to support the creation of contingency operations
- **By I&T - all electrically-connected GSE used at the spacecraft level will be added**

Summary



- **Developed comprehensive tool which builds on standard FMEA format to:**
  - Generate a more complete fault set
  - Assess mitigations for FM
  - Determine responsibility for detection and response for FM
  - Validate FM design for timing, interference, and coverage
    - ***Timing:*** Can faults be detected, contained, or corrected before becoming critical or mission ending?
    - ***Interference:*** Can responses interact in a way that results in an undesirable state or precludes FM from mitigating the fault?
    - ***Coverage:*** Do all credible faults have a mitigation?
  - Provide traceability to FM system-level testing
- **Plans for continued work matches FM and project milestone schedules**

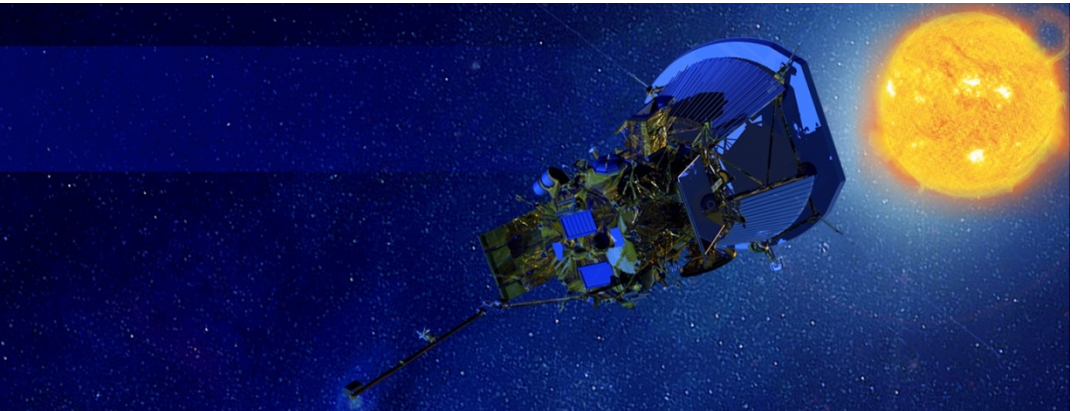
Interface between Reliability and FM



- **Utilize reliability analyses as a systematic way to identify faults for FM**
- **Tailor reliability analyses to support FM by identifying additional information needed for the detection and response to faults**
- **System and subsystem engineers determine the best way to detect and respond to faults via:**
  - Design/redundancy
  - HW or autonomous protections
  - Ground contingency procedures

Solar Probe Plus

A NASA Mission to Touch the Sun

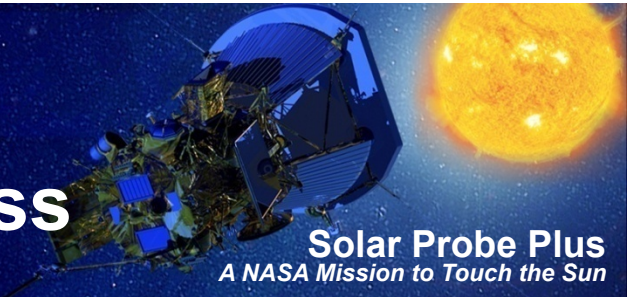


Preliminary Fault Responses & L3 FM Requirements Mapping

Sanae Kubota
FM Lead Engineer
sanae.kubota@jhuapl.edu

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Fault ID, Effect Analysis, and Management Development Process



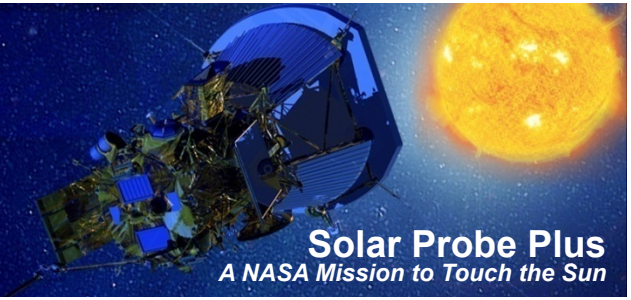
Three step iterative process:

1. **Bottom-up fault analysis: FMEA**
   - **Identification of failure modes, analysis of effects, and preliminary response planning**

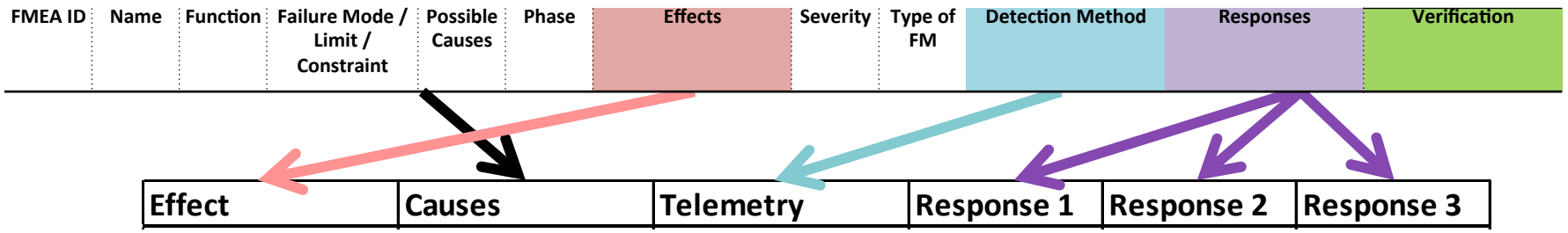
2. **Top-down fault analysis: "EFMA"**
   - **Analysis of effects, completeness of list of causes, and further development of response planning**

3. **Response development:**
   - **Planning of fault responses based on symptoms**

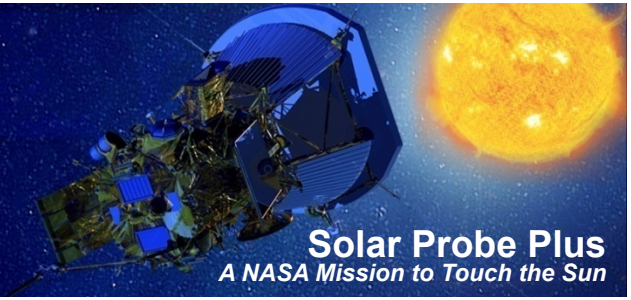
Step 2: Iteration on fault identification & response



- **FMEA identified component failure modes and assessed effect on system**
  - Bottom-up analysis
  - Initial fault response planning
- **FMEA used as input to "EFMA"**
  - "EFMA" = Effects and Failure Modes Analysis
  - Top-down analysis
  - Effects identified in FMEA gathered
  - Potential causes of effects listed and re-examined for completeness
  - Review and further development of fault responses

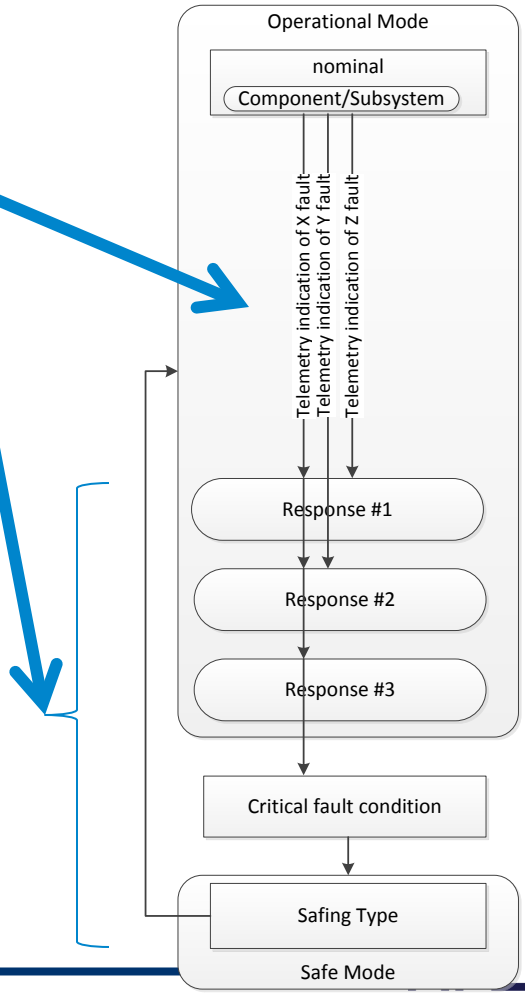


Step 3: Fault Detection and Response Development

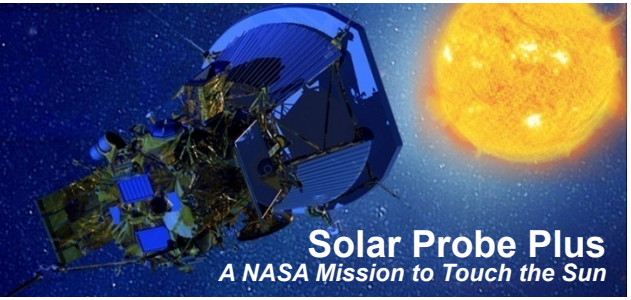


Effect	Causes	Telemetry	Response 1	Response 2	Response 3

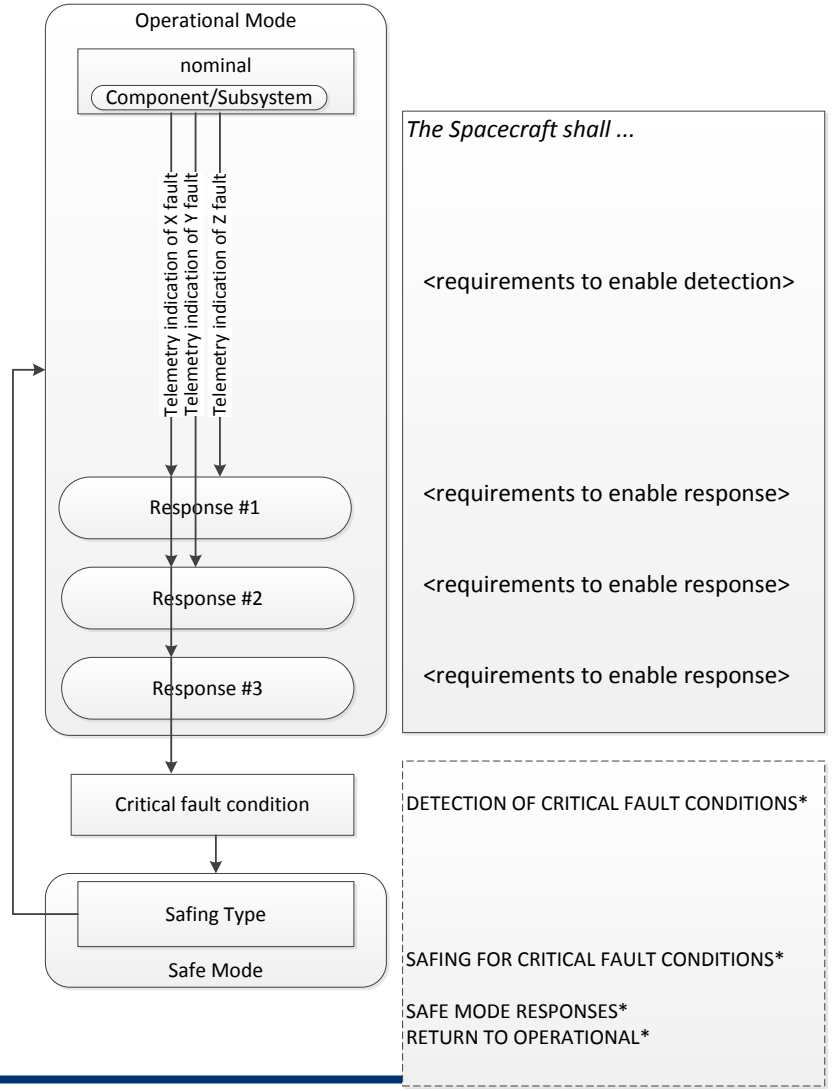
- FMEA and "EFMA" used as input to fault detection and response development
  - Telemetry indications (symptoms) gathered
  - Responses mapped to symptoms
    - Tiered responses



Fault Analysis Mapping to L3 Requirements

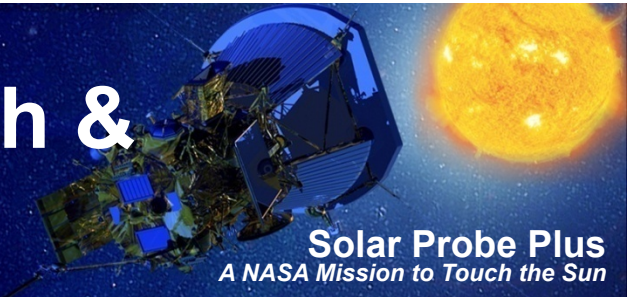


- **Fault analysis identified**
  - Failure modes
  - Effects
  - Telemetry required for detection
  - Response capabilities required
  - Potential paths to critical fault conditions
  - System-wide responses required for critical fault conditions
- **L3 requirements mapped to fault analysis**
  - *Ensures appropriate L3 requirements are in place to enable fault detection and response*
- **Preliminary fault analysis mapping has been completed for all subsystems.**
  - Examples: Avionics, G&C, Cooling System
  - Remaining subsystems are included in back-up



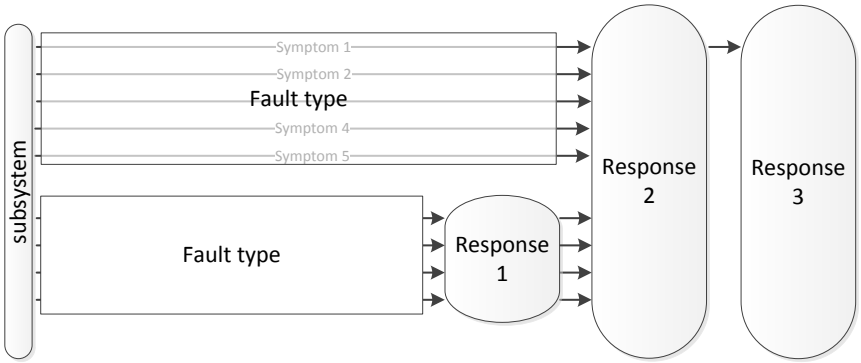
*discussed in detail in Safing Concept section

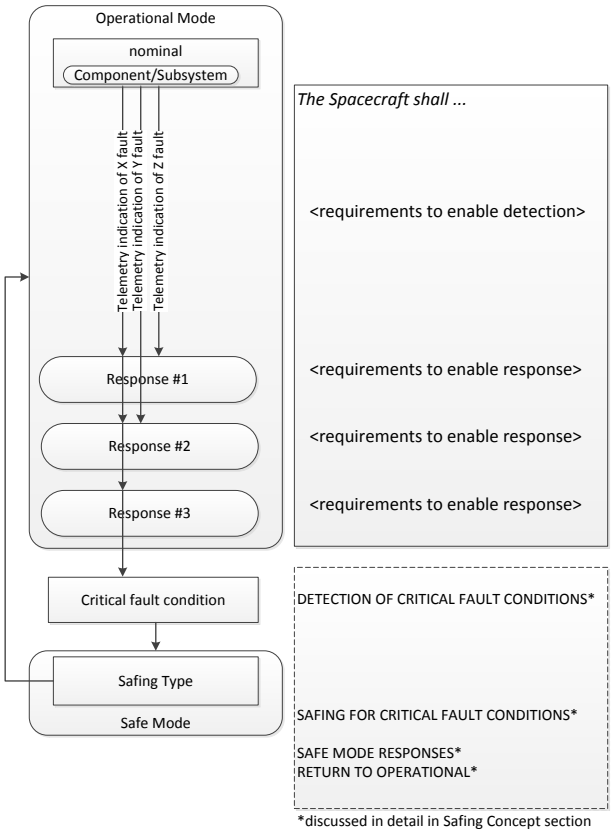
Fault Responses Walk-Through & L3 FM Requirements Review



Solar Probe Plus
A NASA Mission to Touch the Sun

Walk-through preliminary fault detection and local response plan.

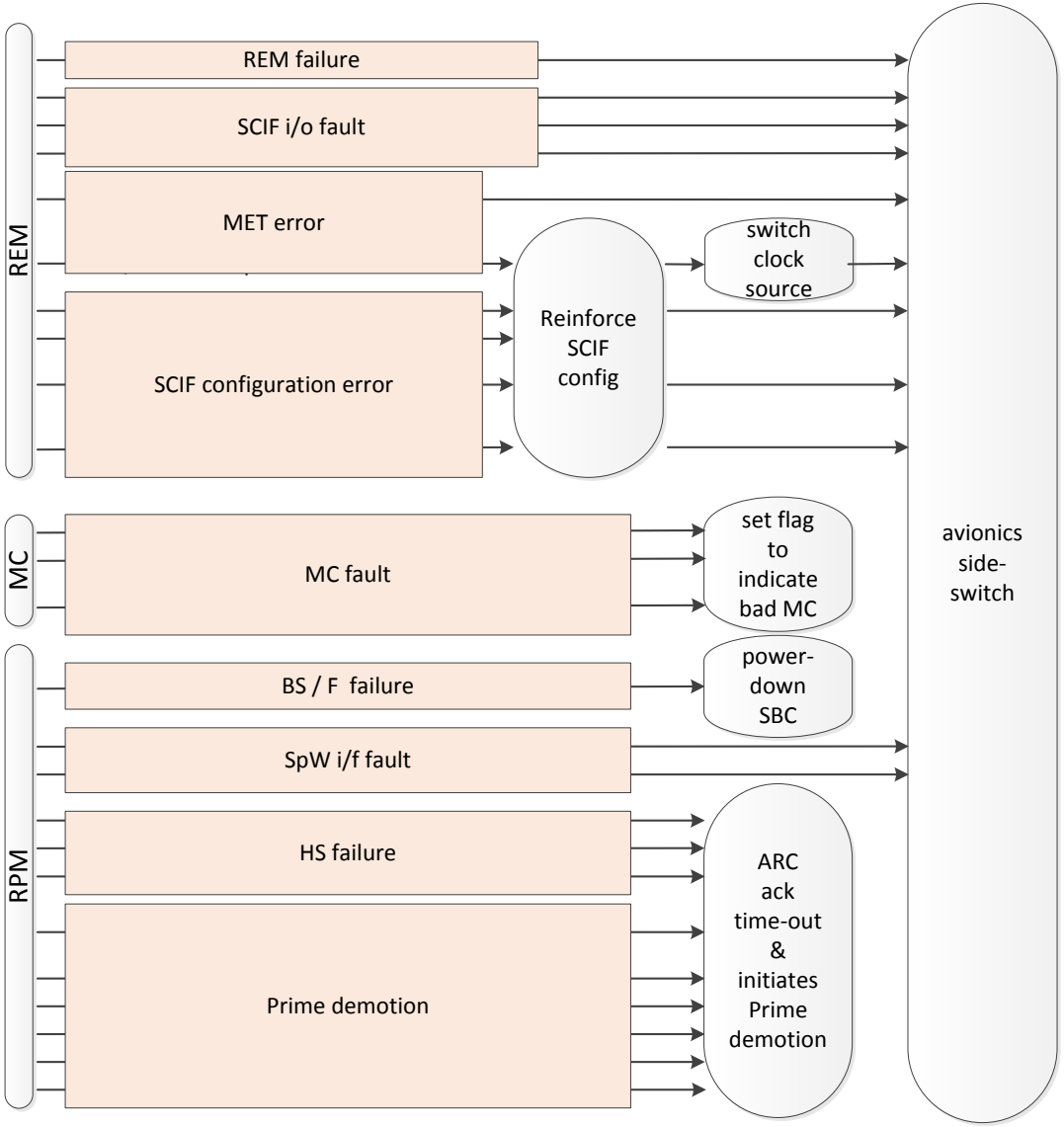




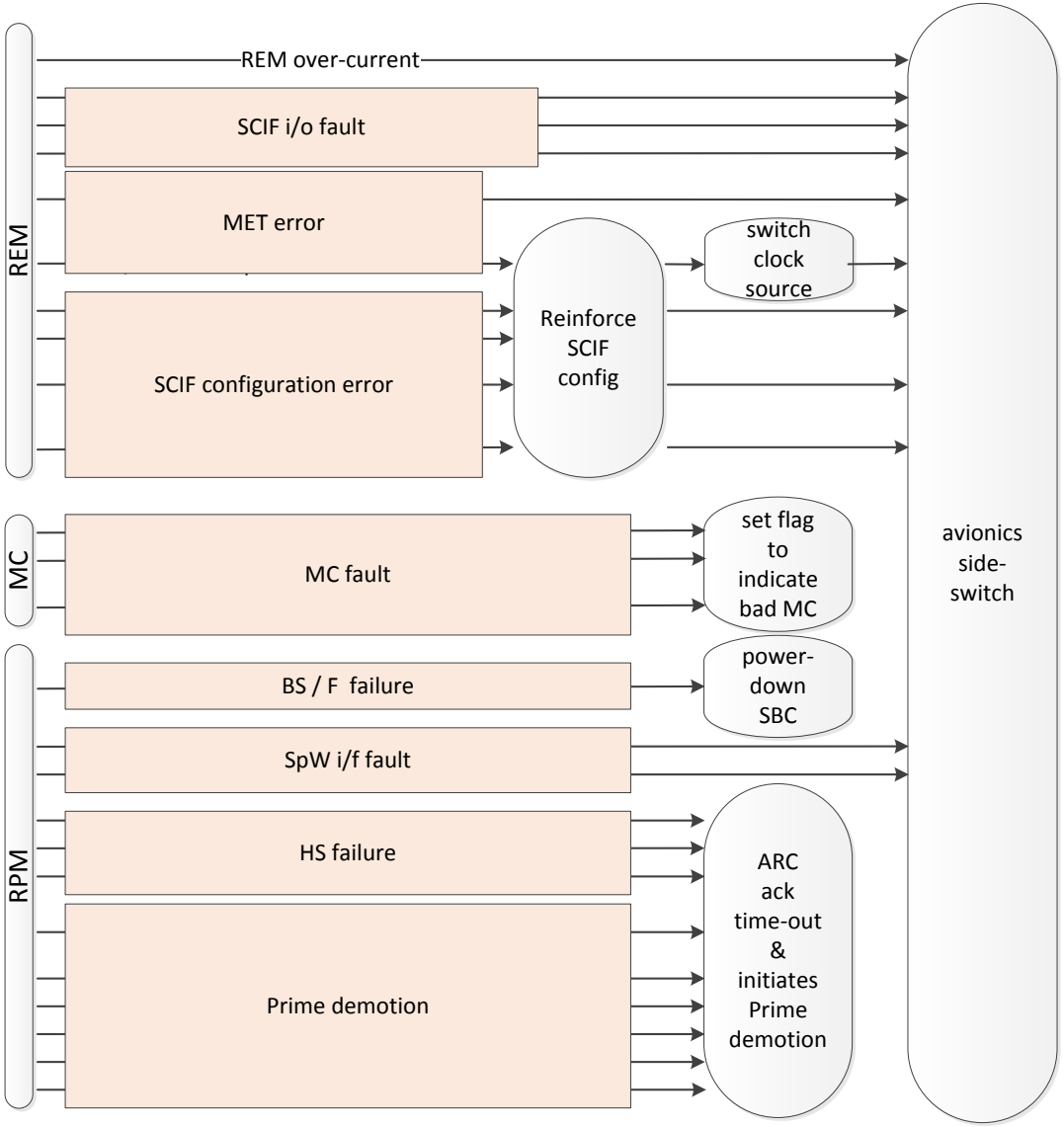
Highlight potential paths from local faults to critical faults.

Map fault detection and response plan to Level 3 FM requirements.

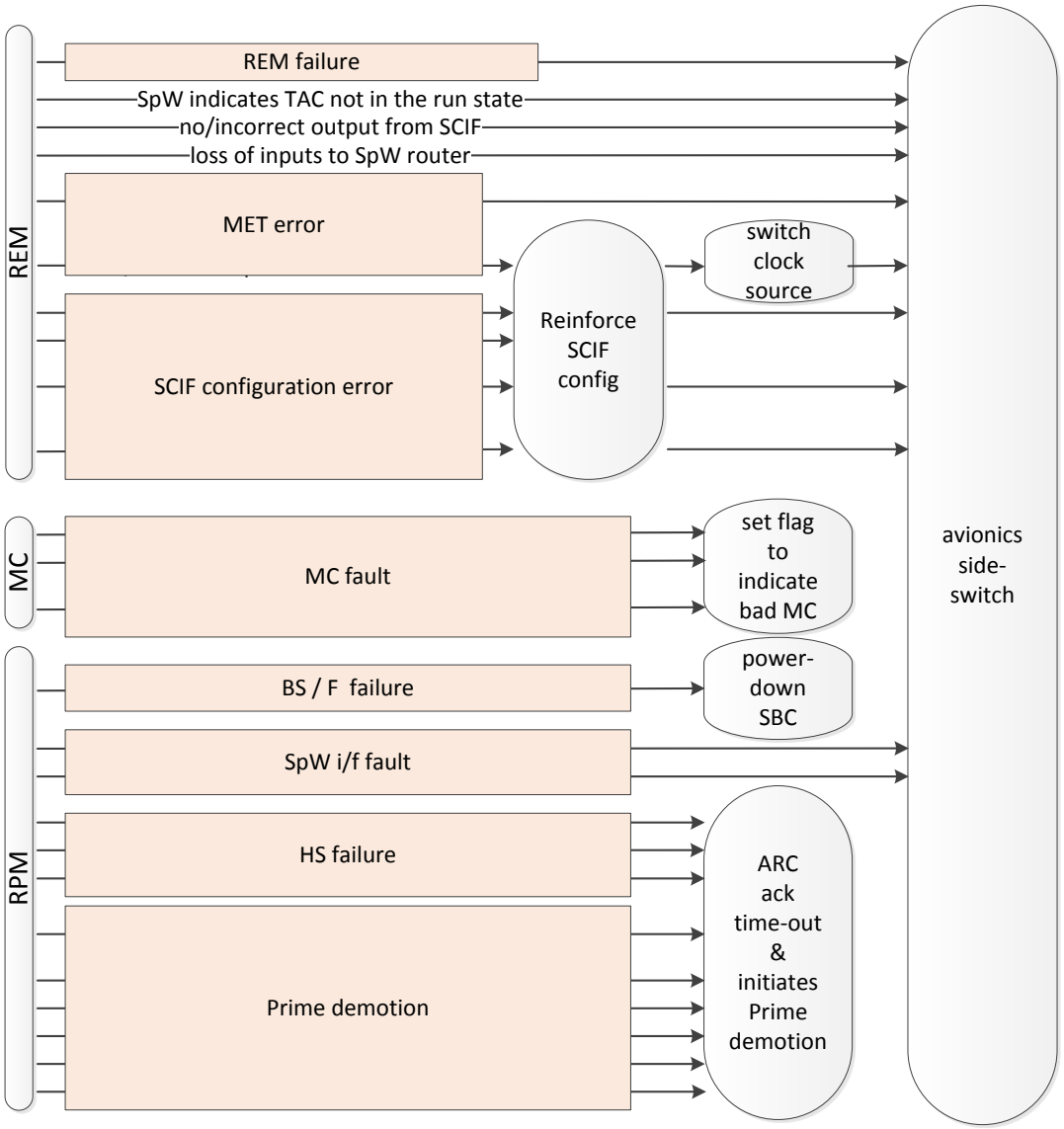
Fault Responses: Avionics



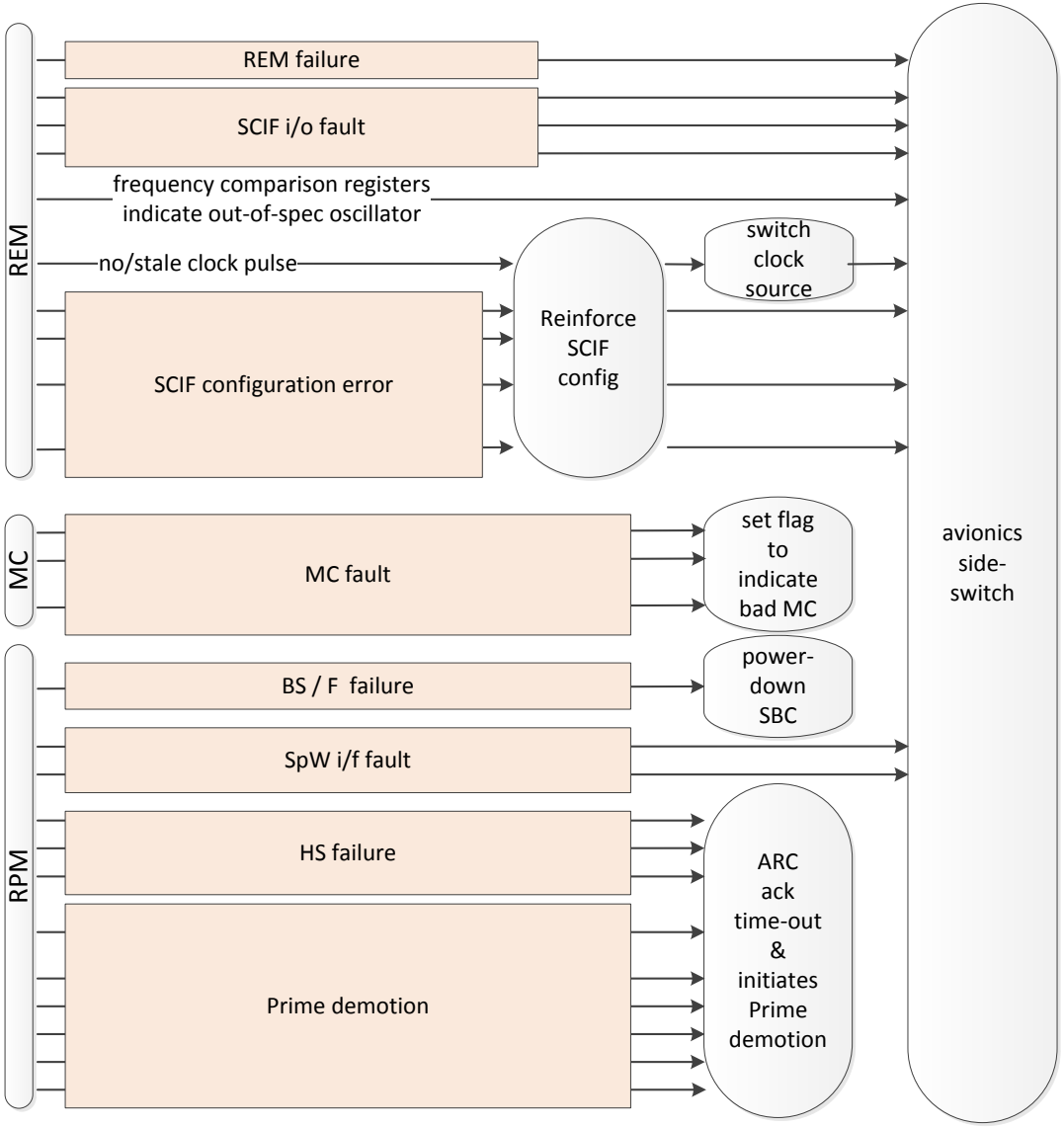
Fault Responses: Avionics



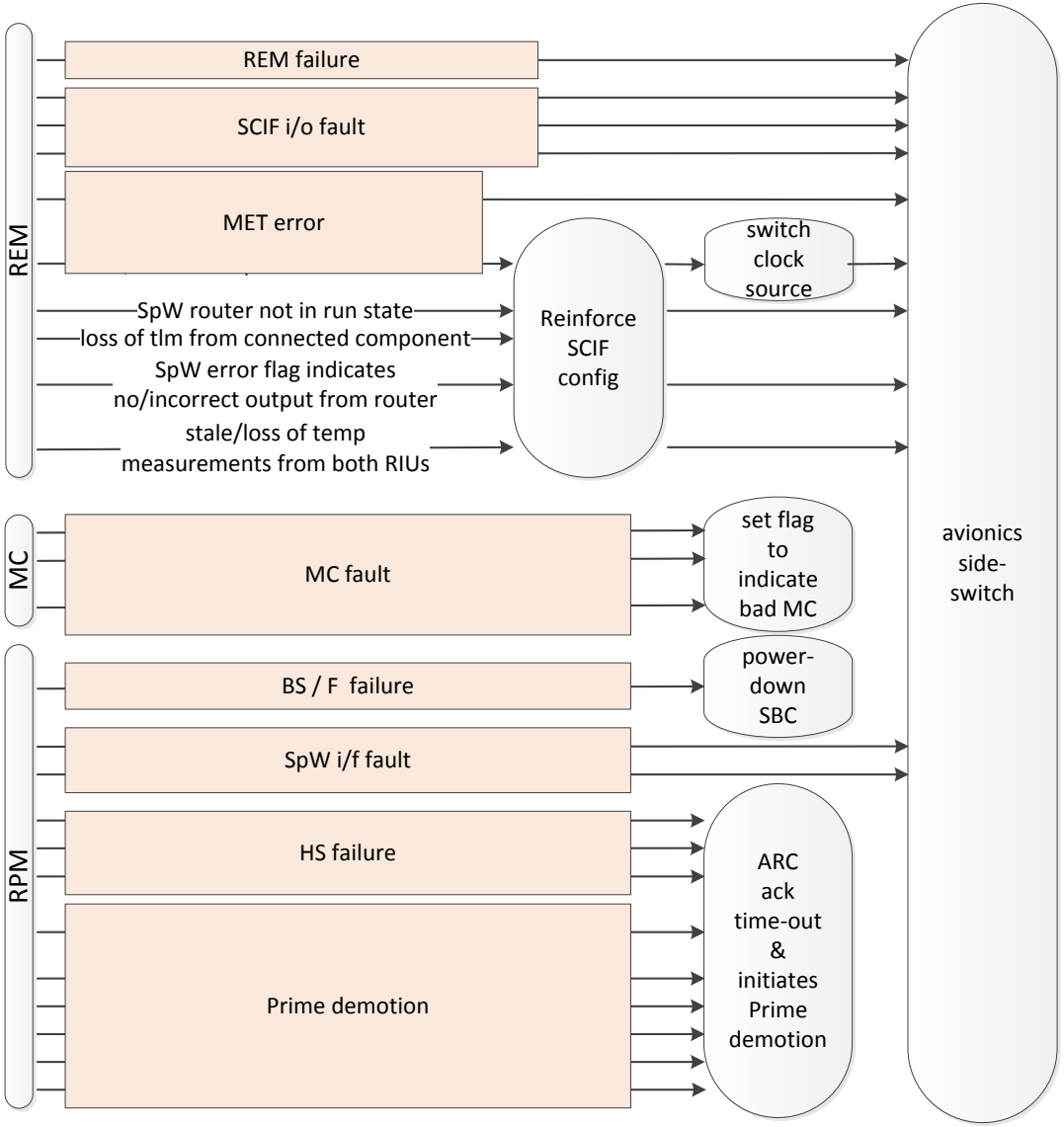
Fault Responses: Avionics



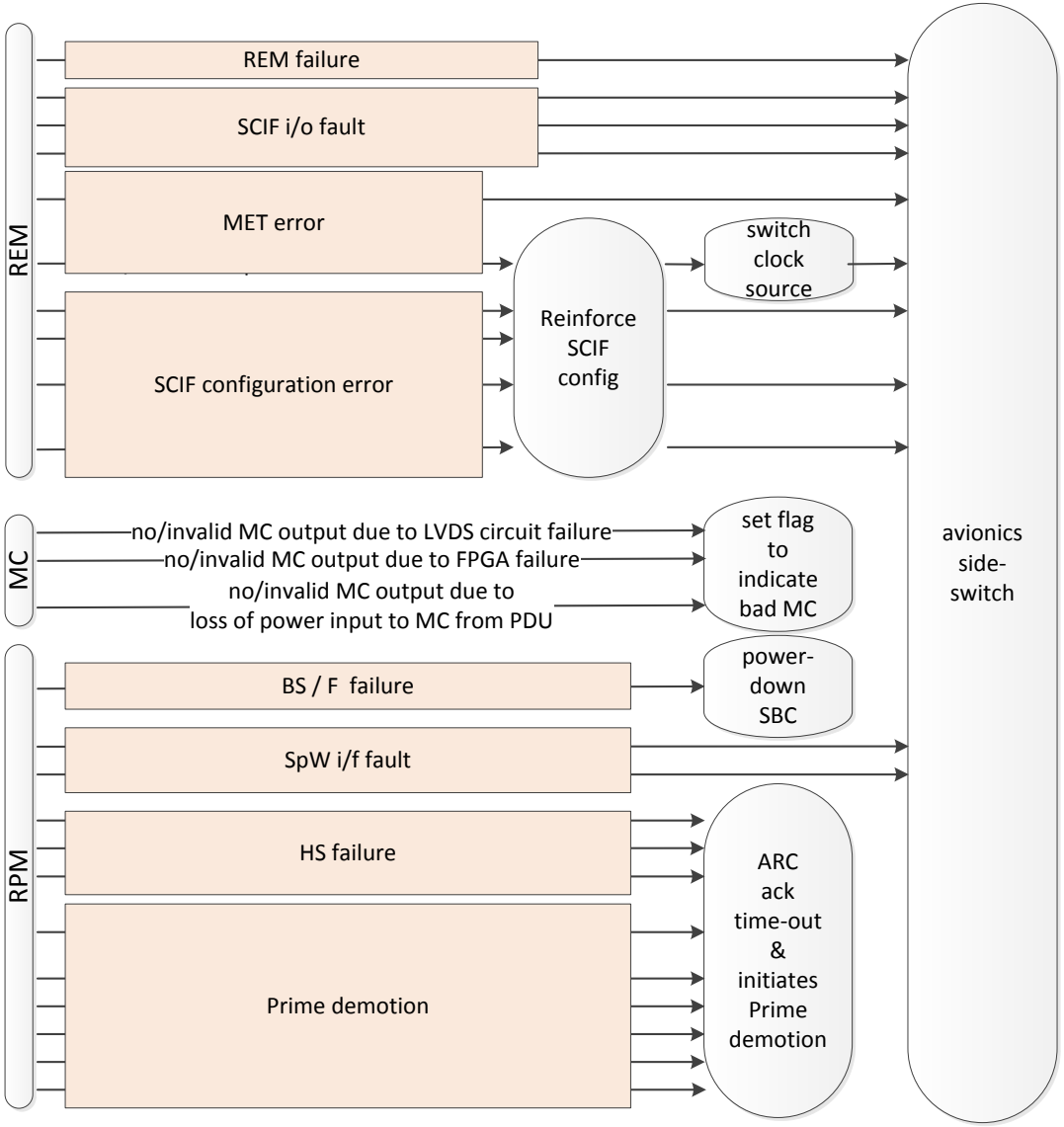
Fault Responses: Avionics



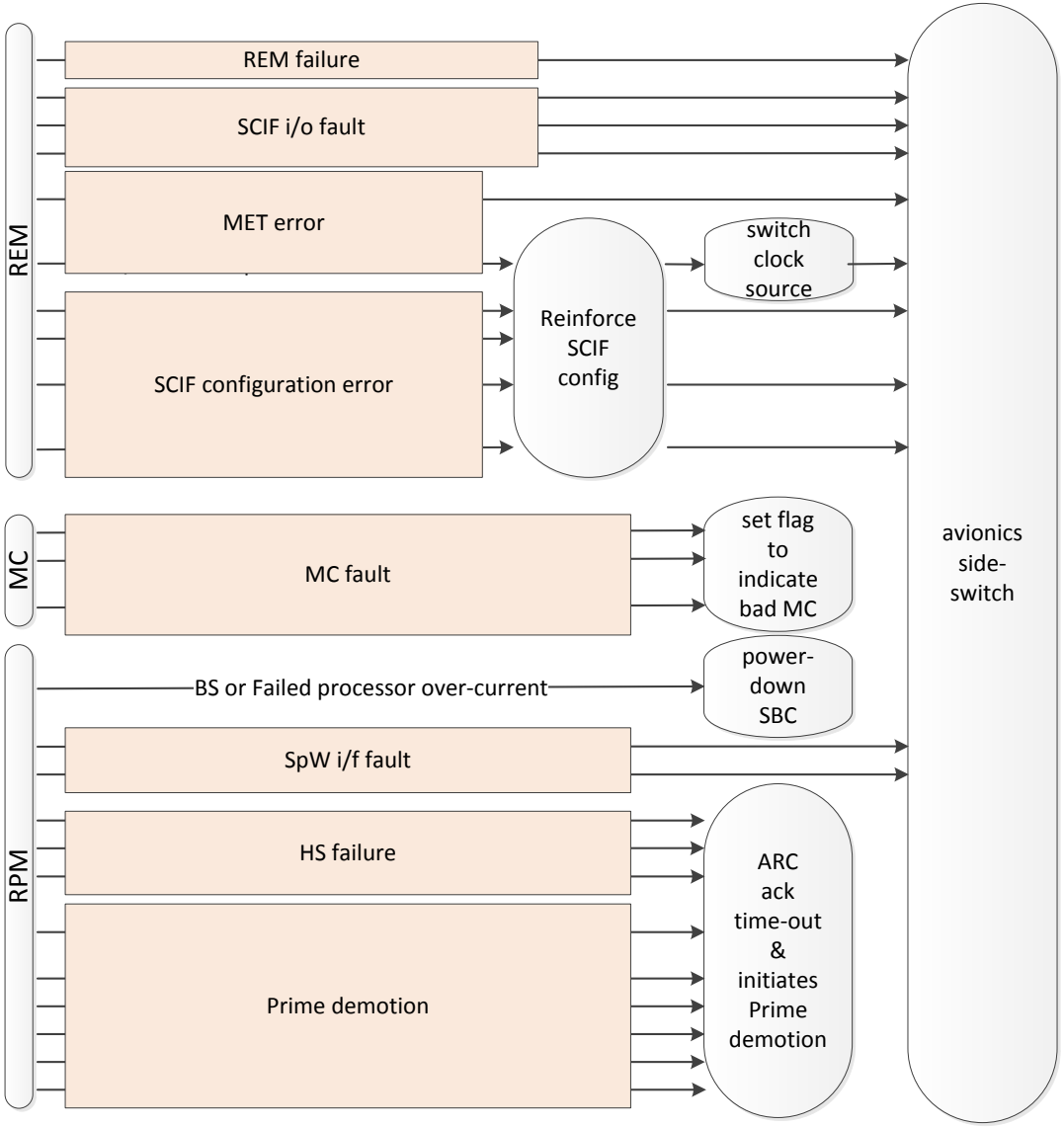
Fault Responses: Avionics



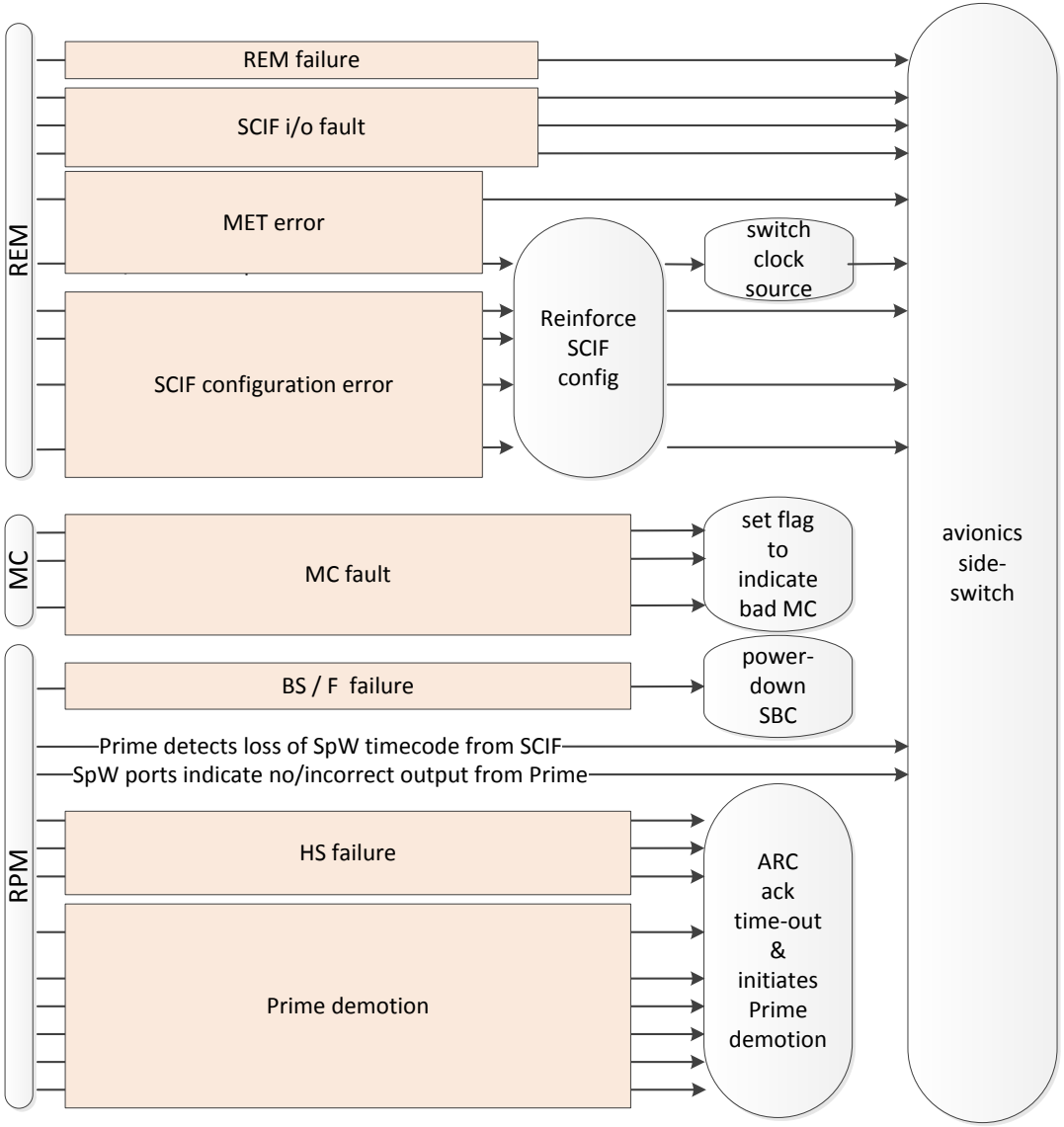
Fault Responses: Avionics



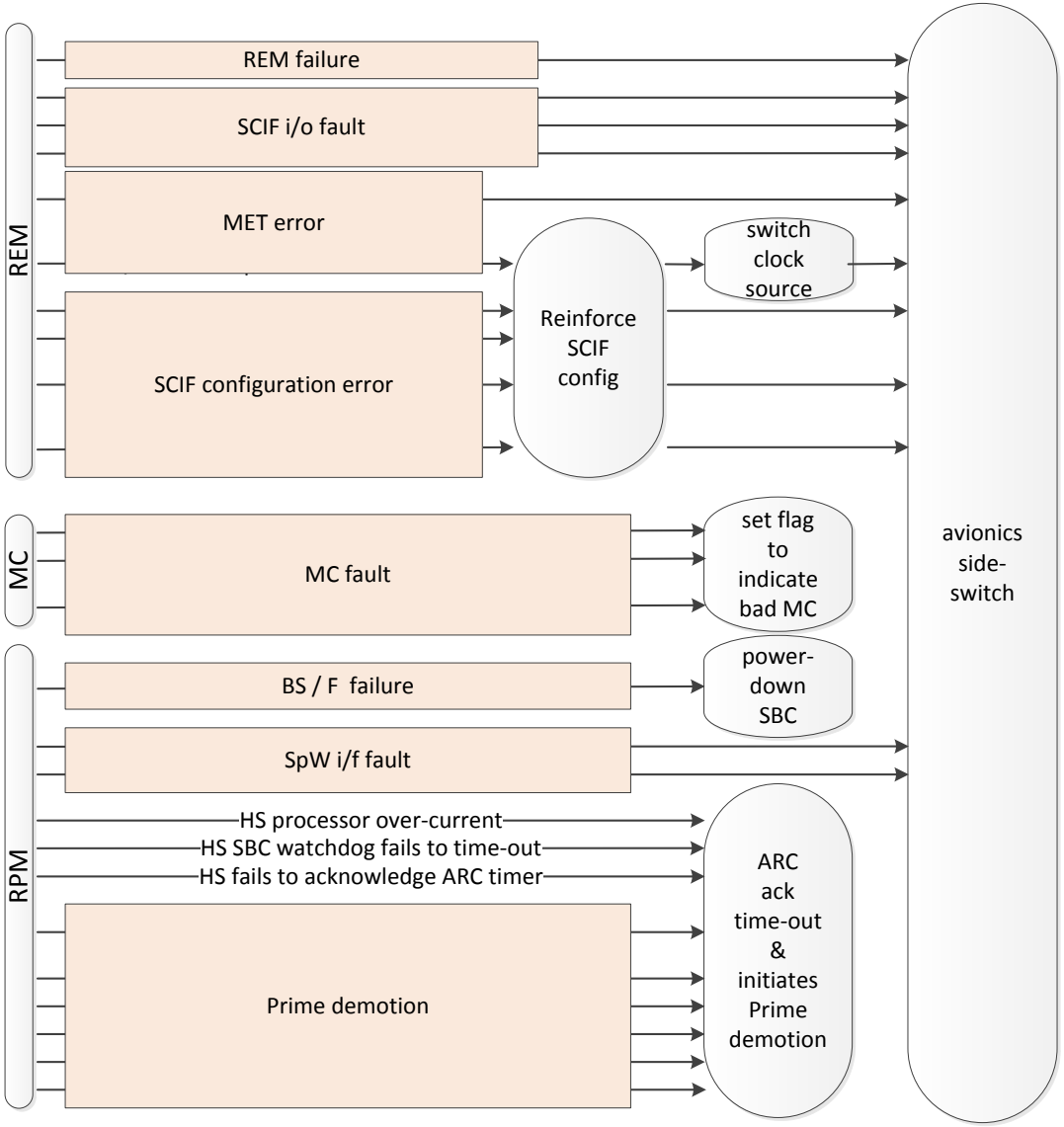
Fault Responses: Avionics



Fault Responses: Avionics

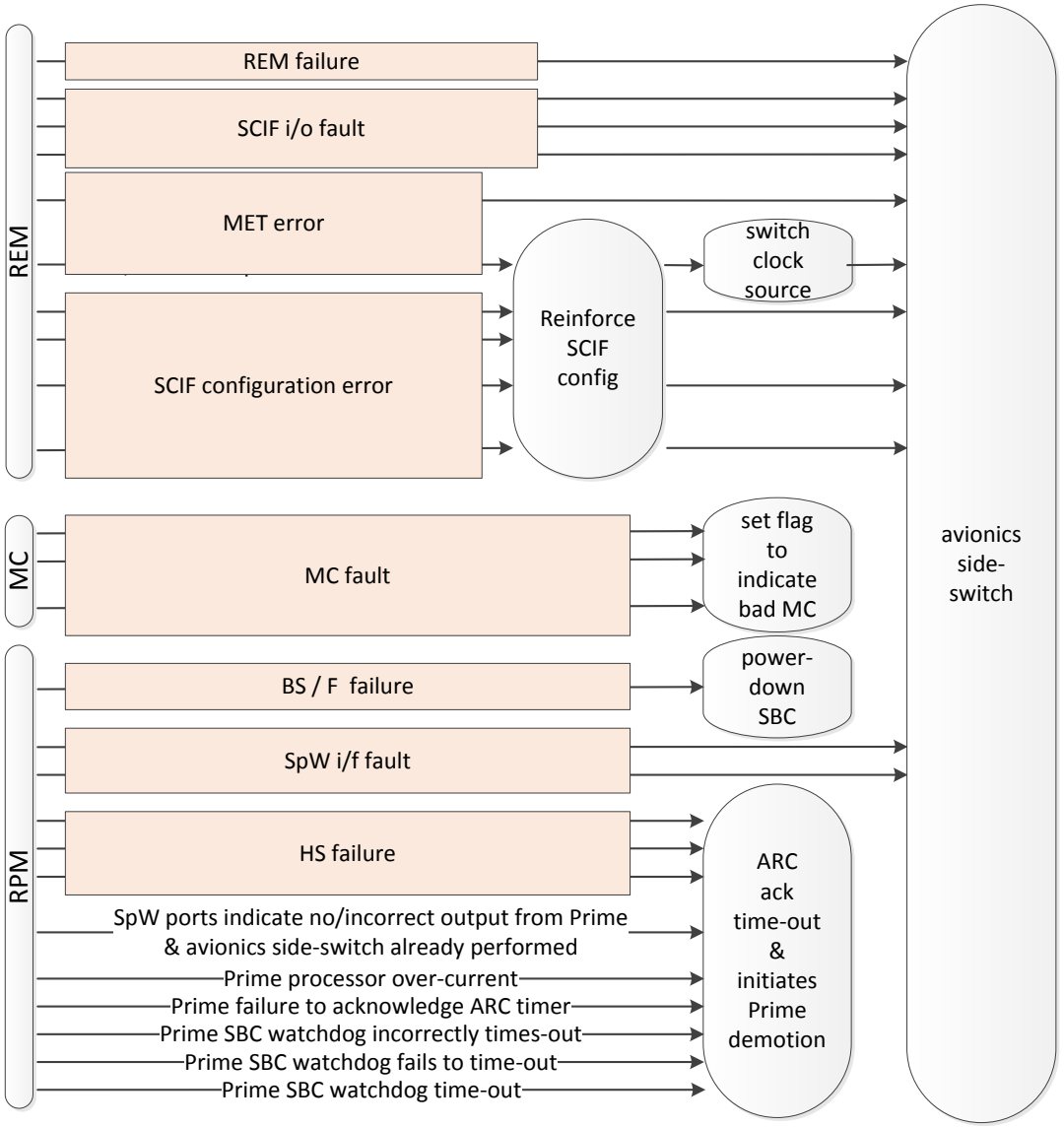


Fault Responses: Avionics

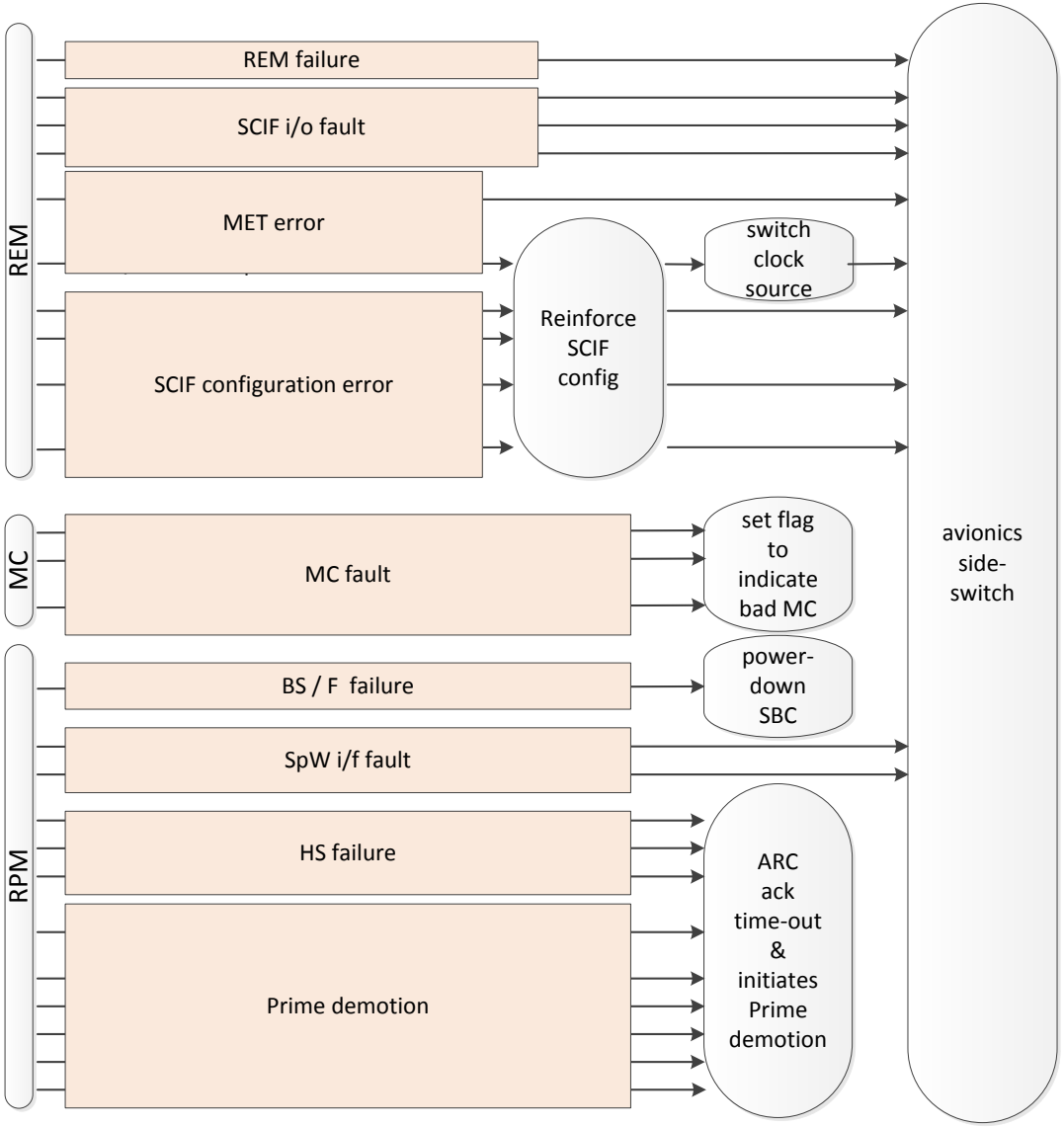


APL

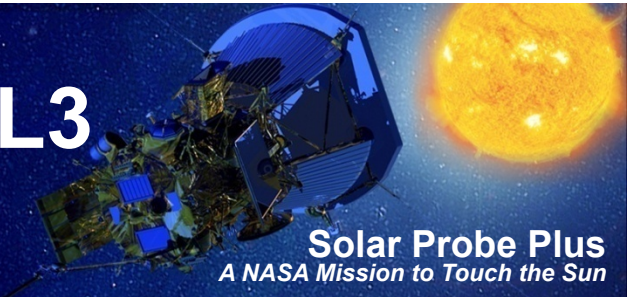
Fault Responses: Avionics

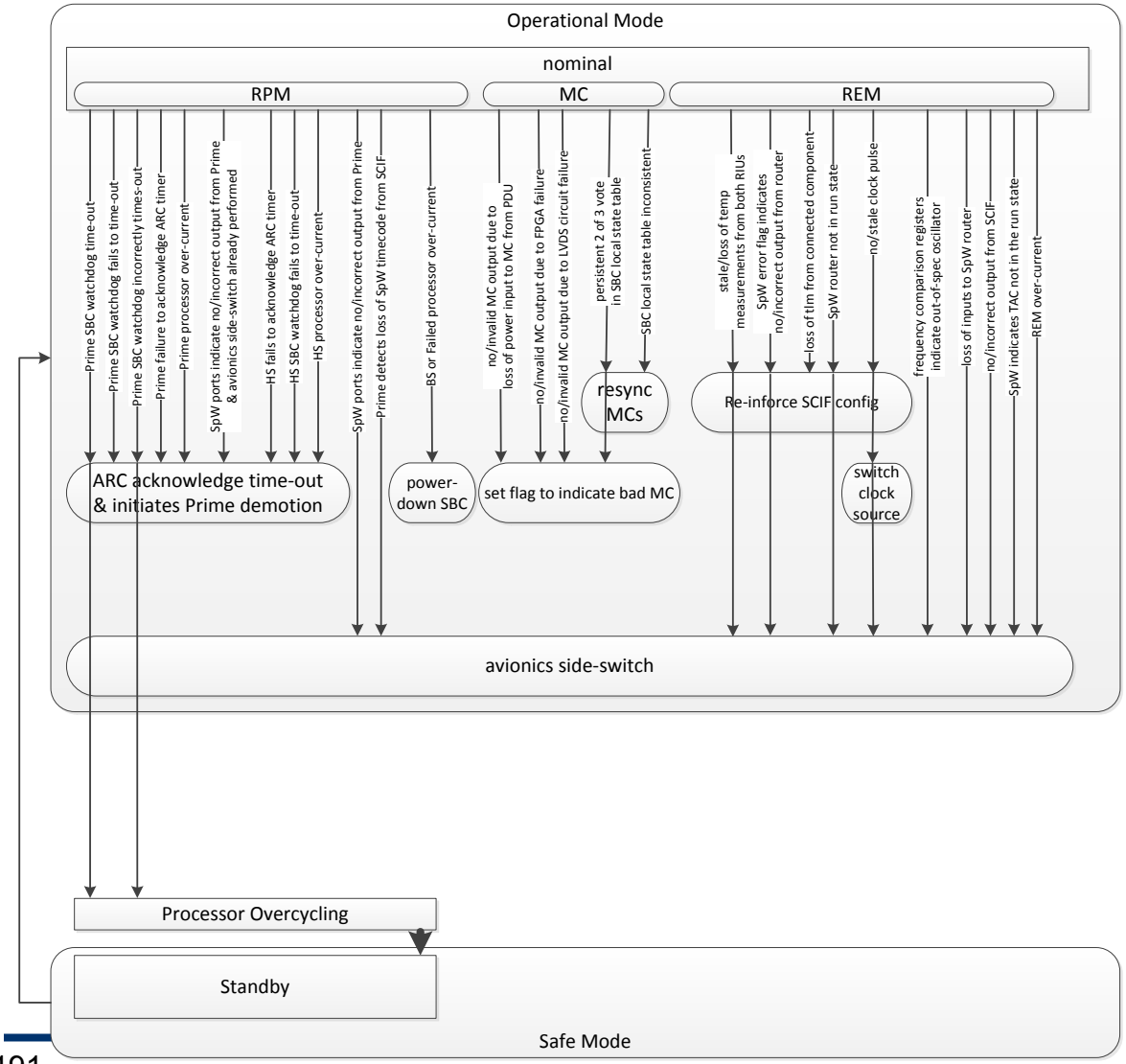


Fault Responses: Avionics



Avionics Fault Management – L3 Requirements Map





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

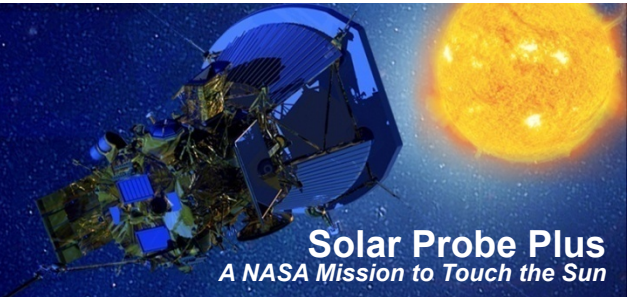
DETECTION OF CRITICAL FAULT CONDITIONS*

SAFING FOR CRITICAL FAULT CONDITIONS*

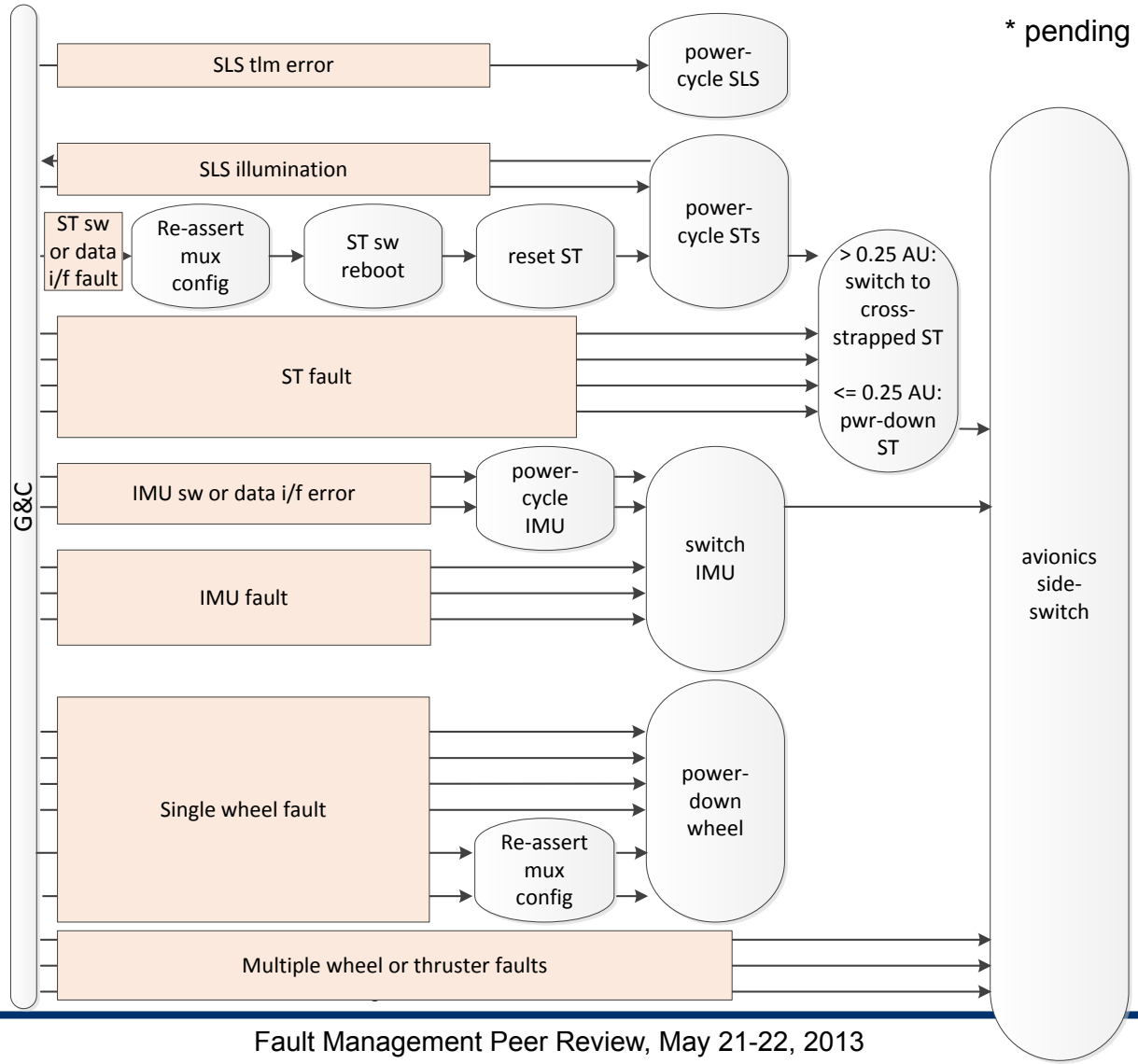
SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

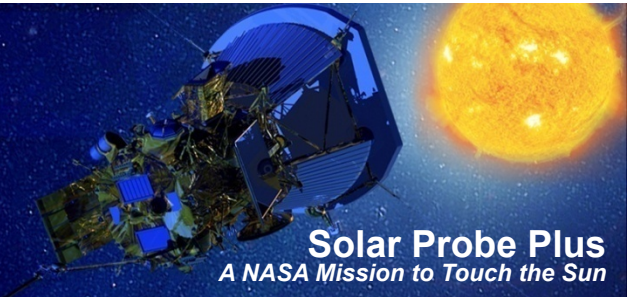
Fault Response: Guidance & Control*



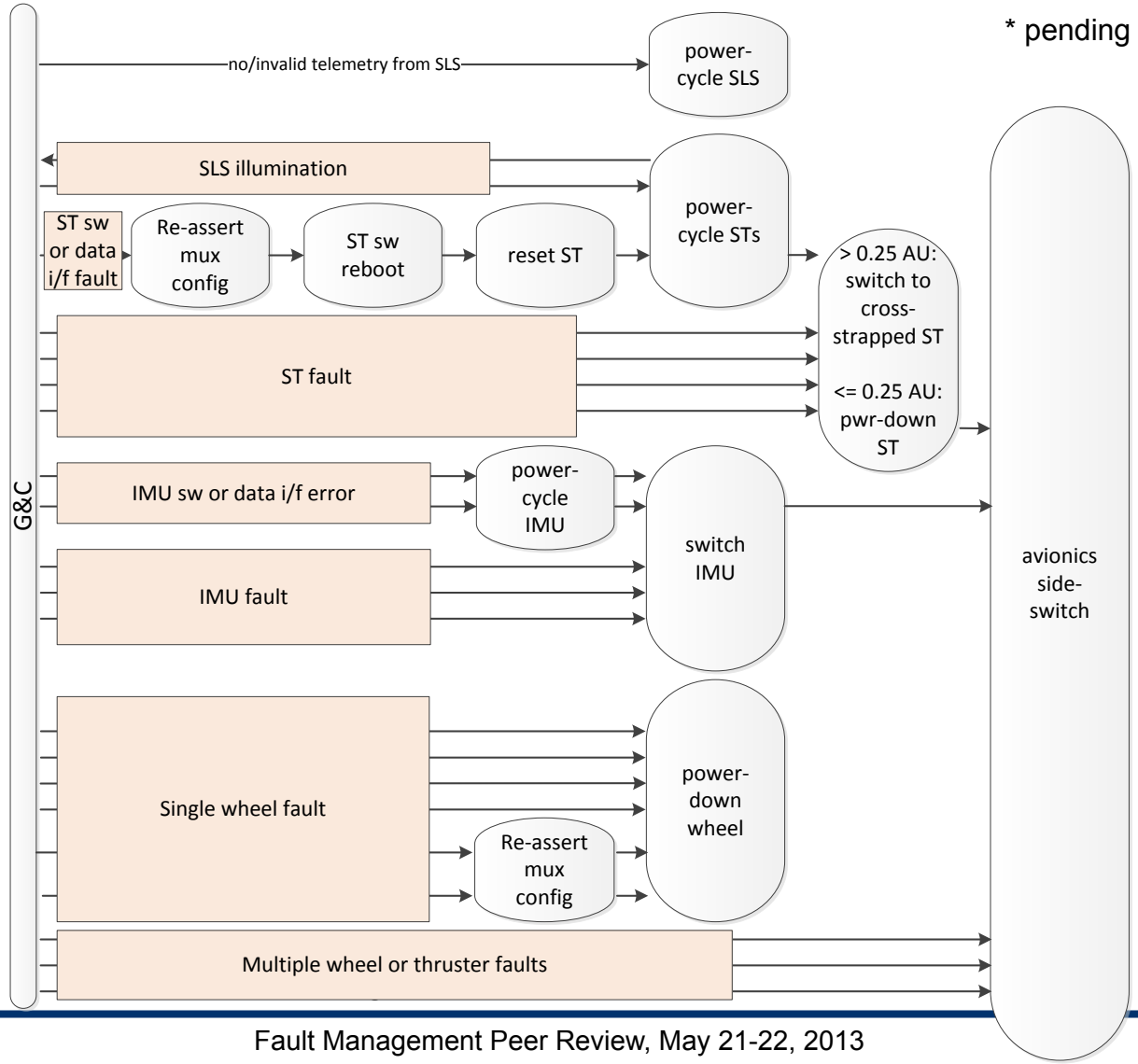
* pending component selection



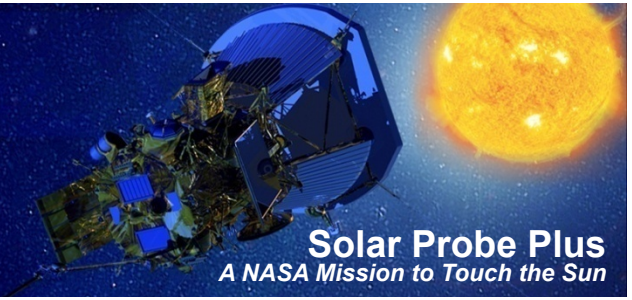
Fault Response: Guidance & Control*



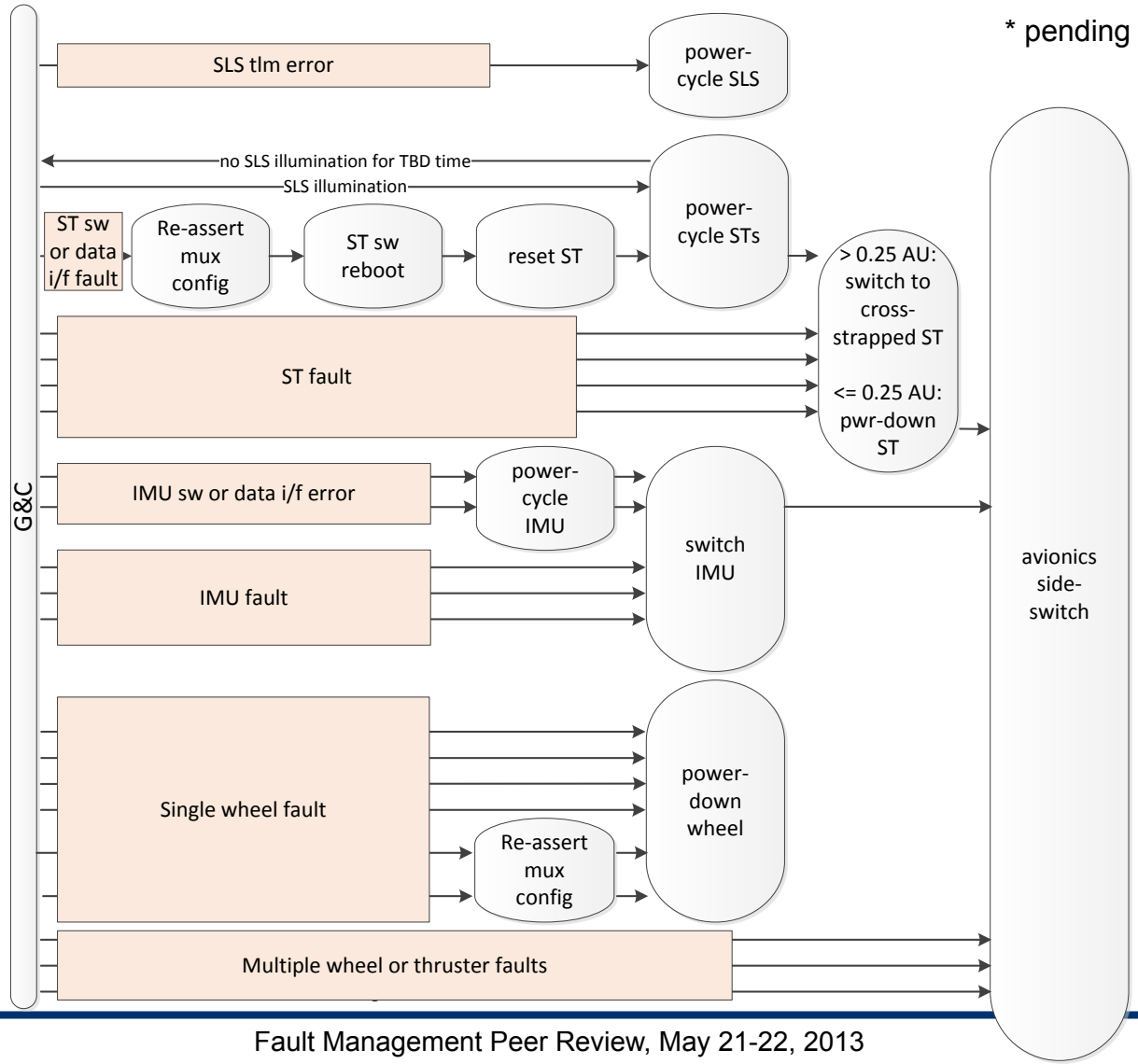
* pending component selection



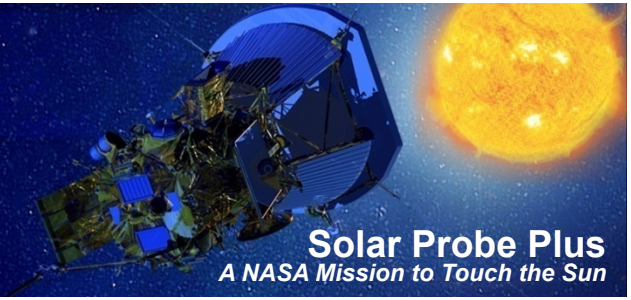
Fault Response: Guidance & Control*



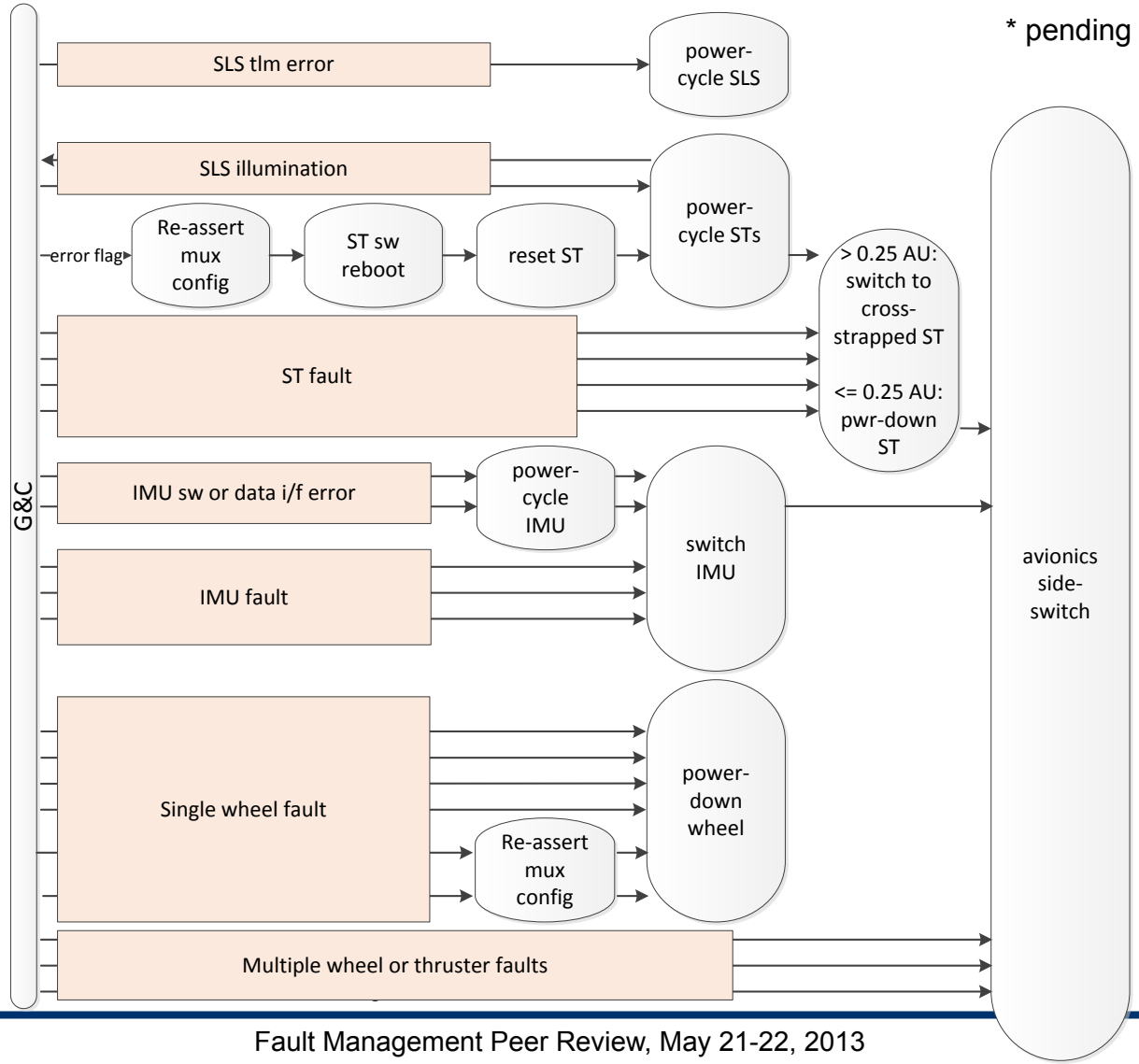
* pending component selection



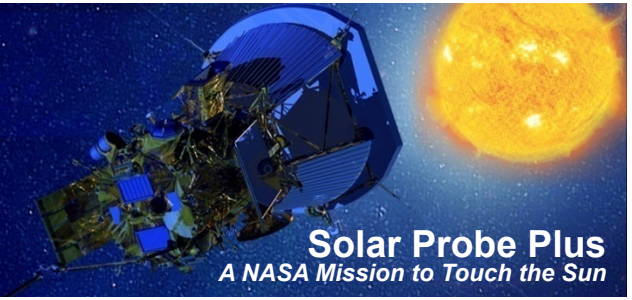
Fault Response: Guidance & Control*



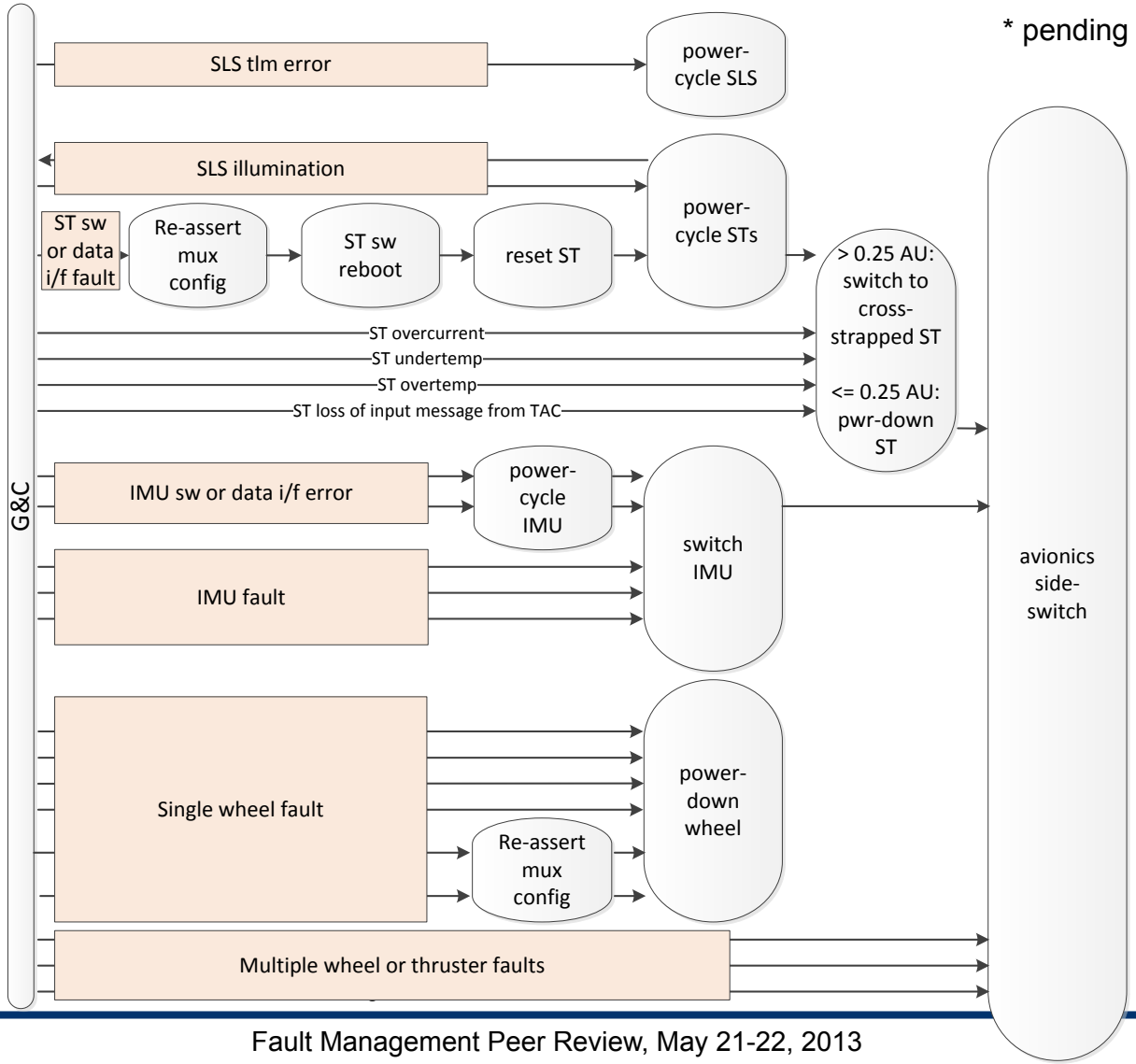
* pending component selection



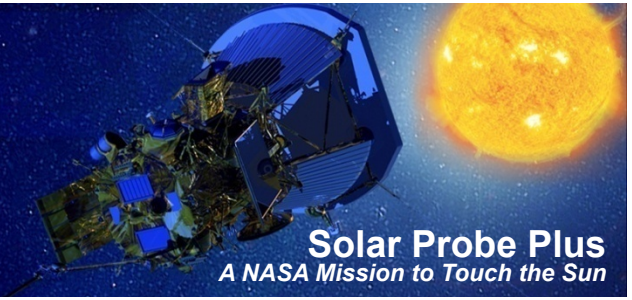
Fault Response: Guidance & Control*



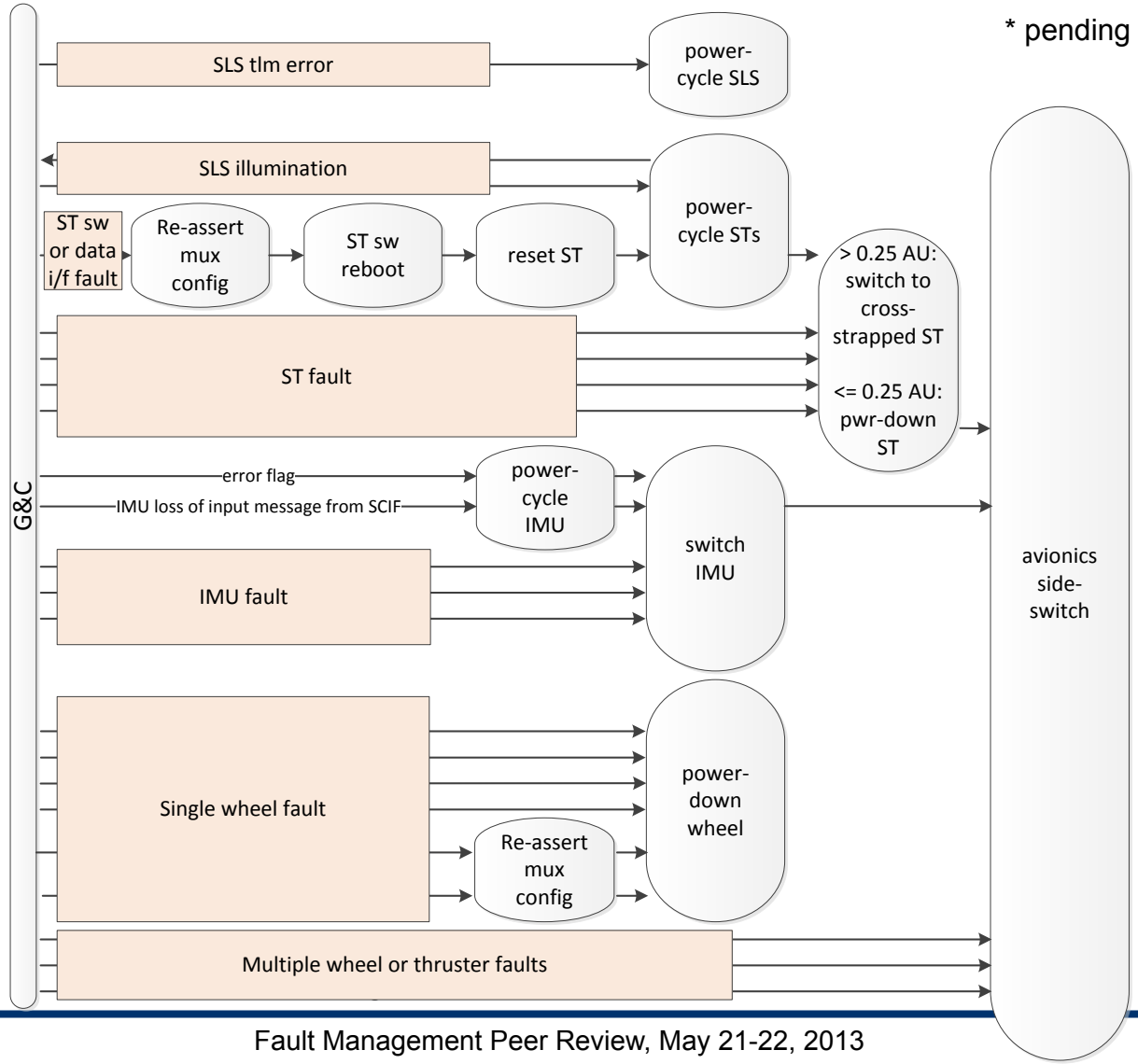
* pending component selection



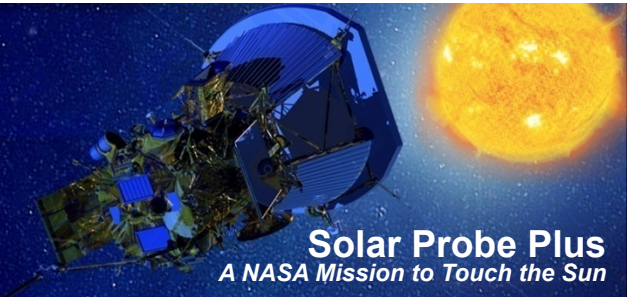
Fault Response: Guidance & Control*



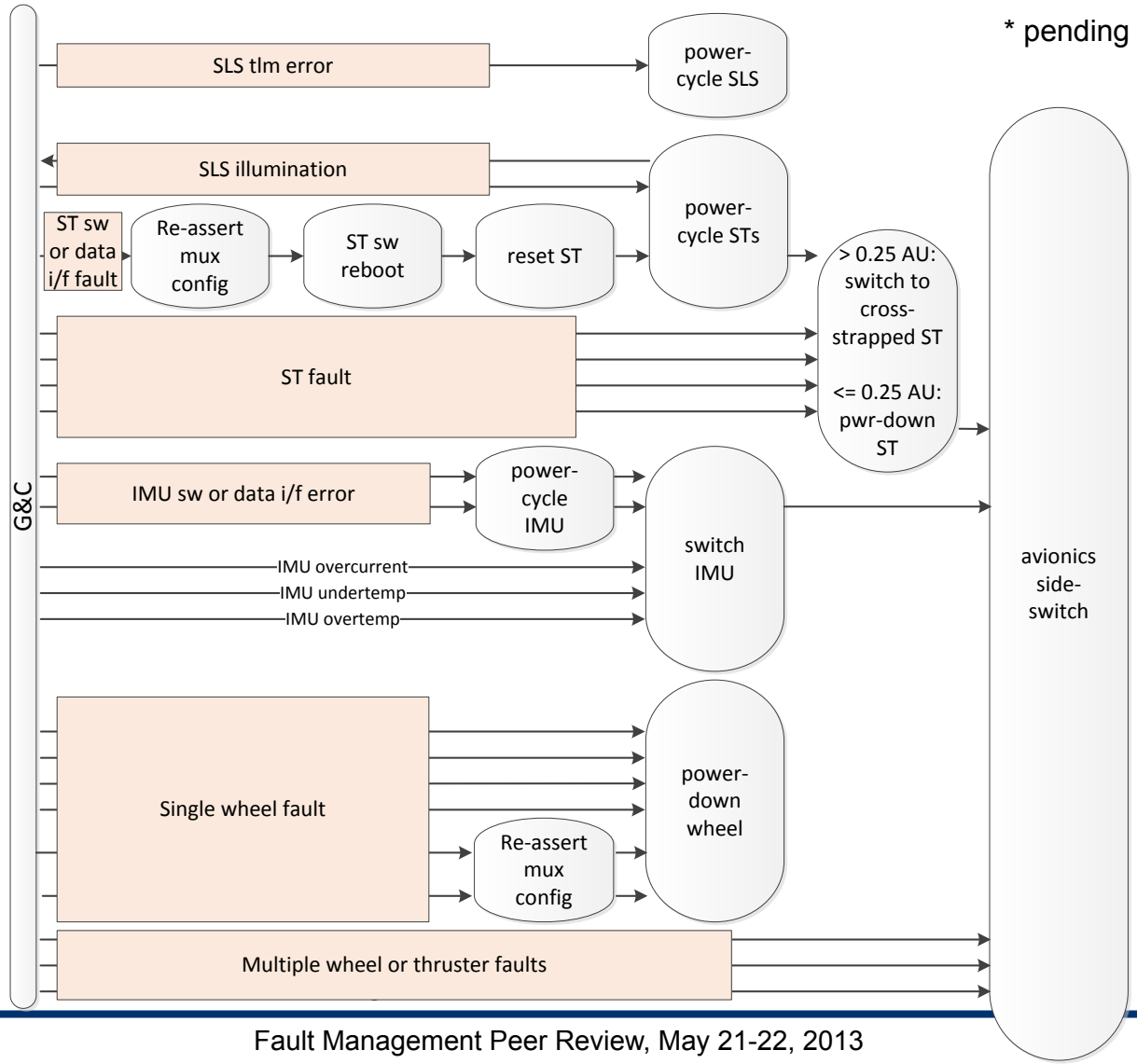
* pending component selection



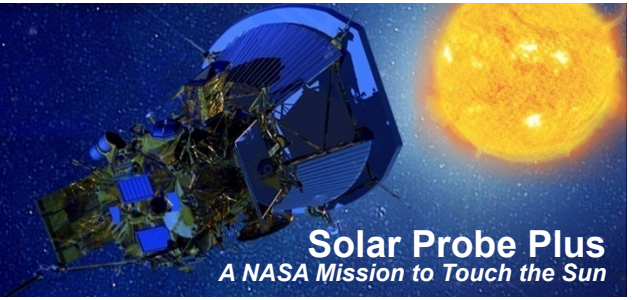
Fault Response: Guidance & Control*



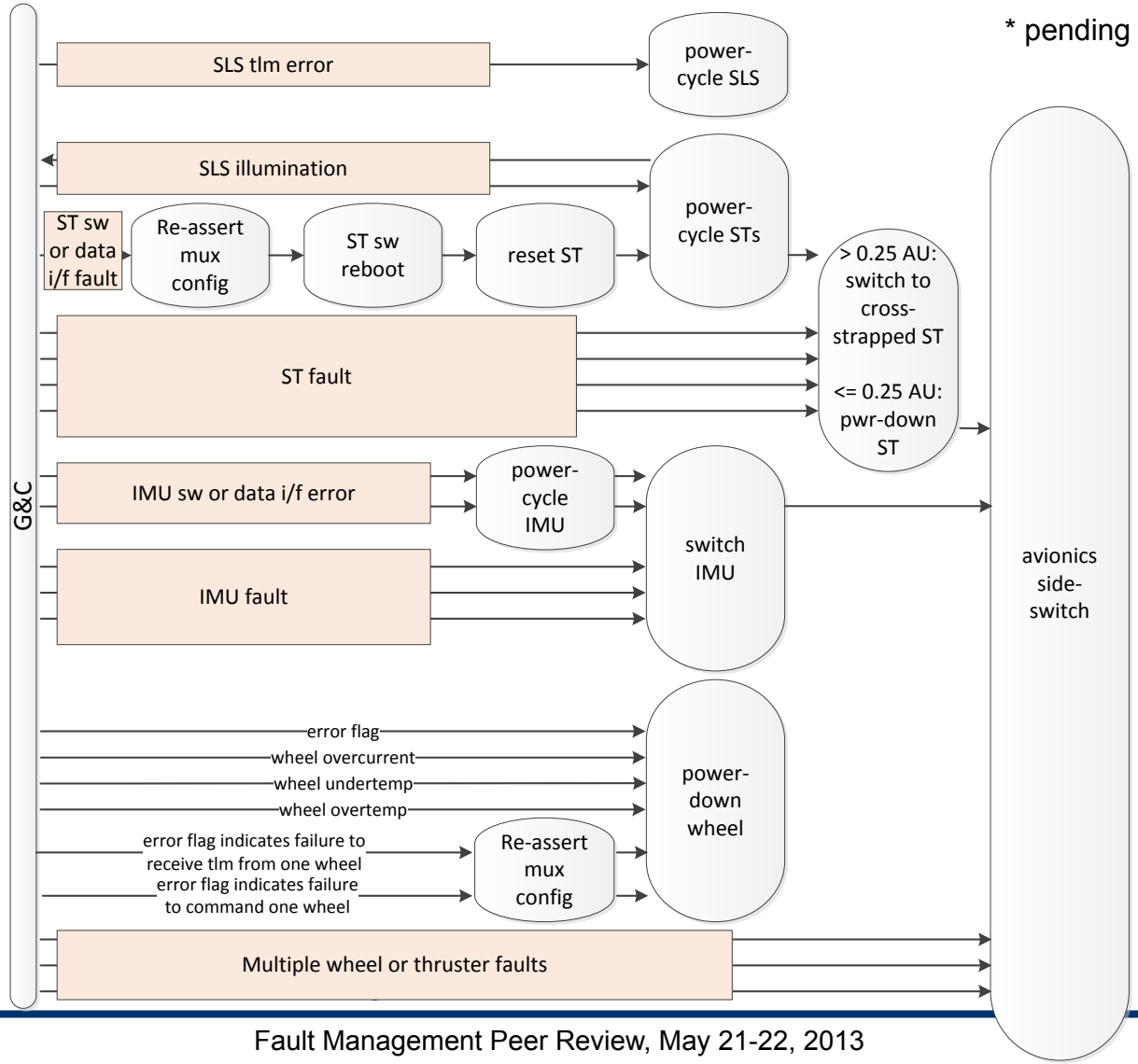
* pending component selection



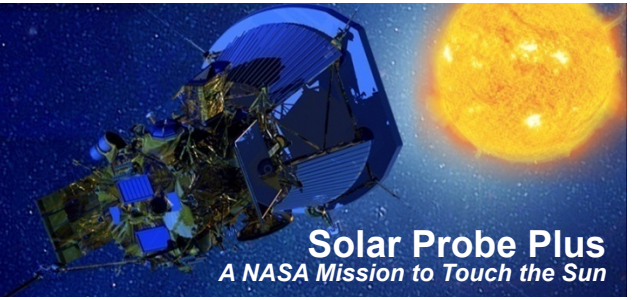
Fault Response: Guidance & Control*



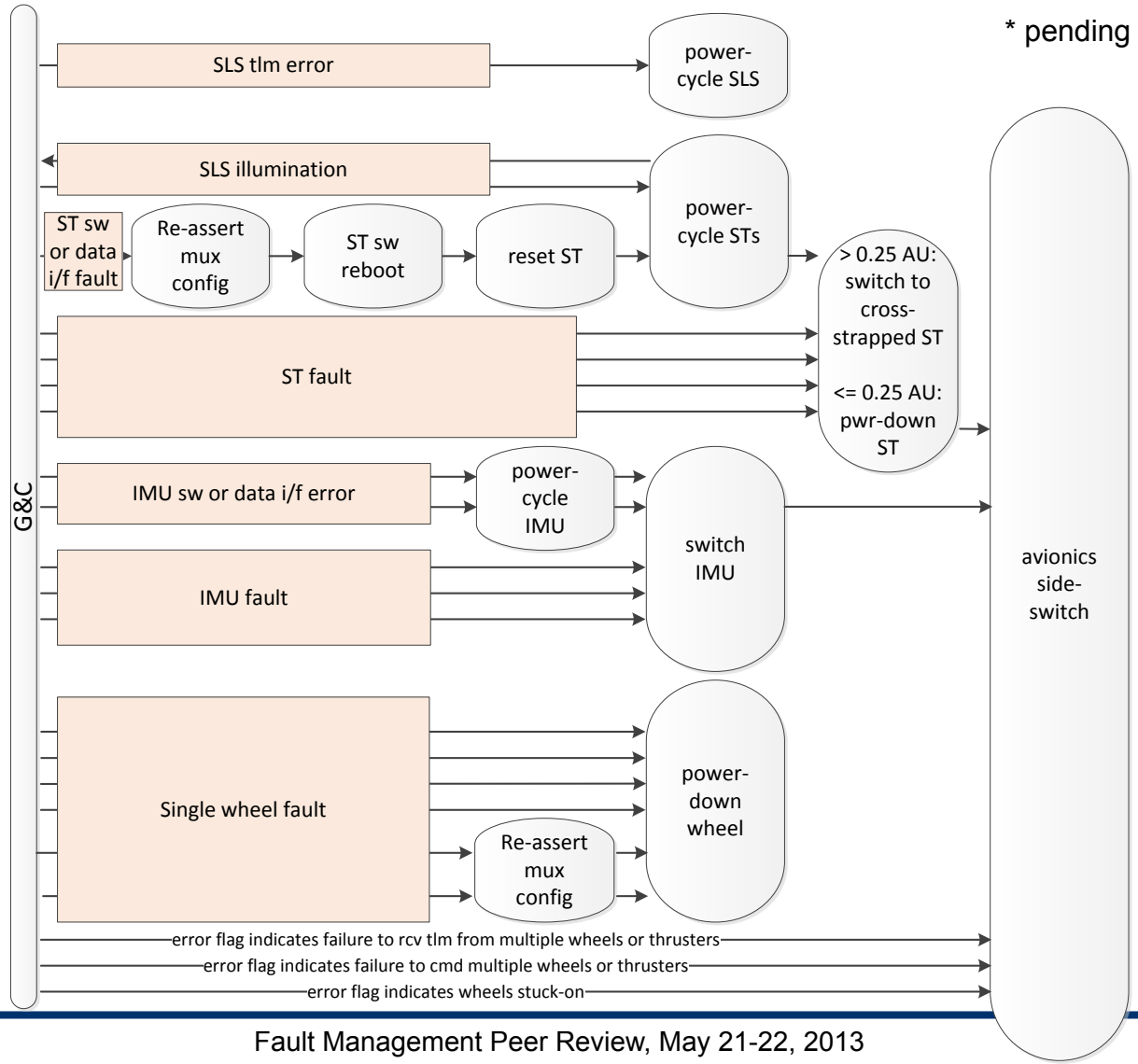
* pending component selection



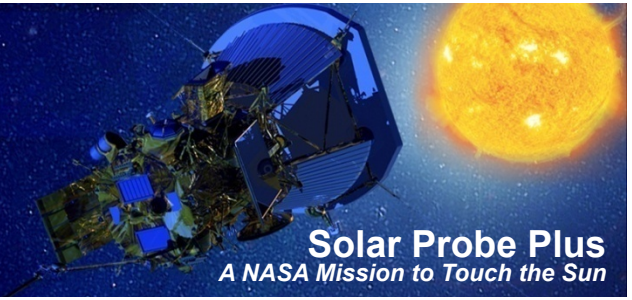
Fault Response: Guidance & Control*



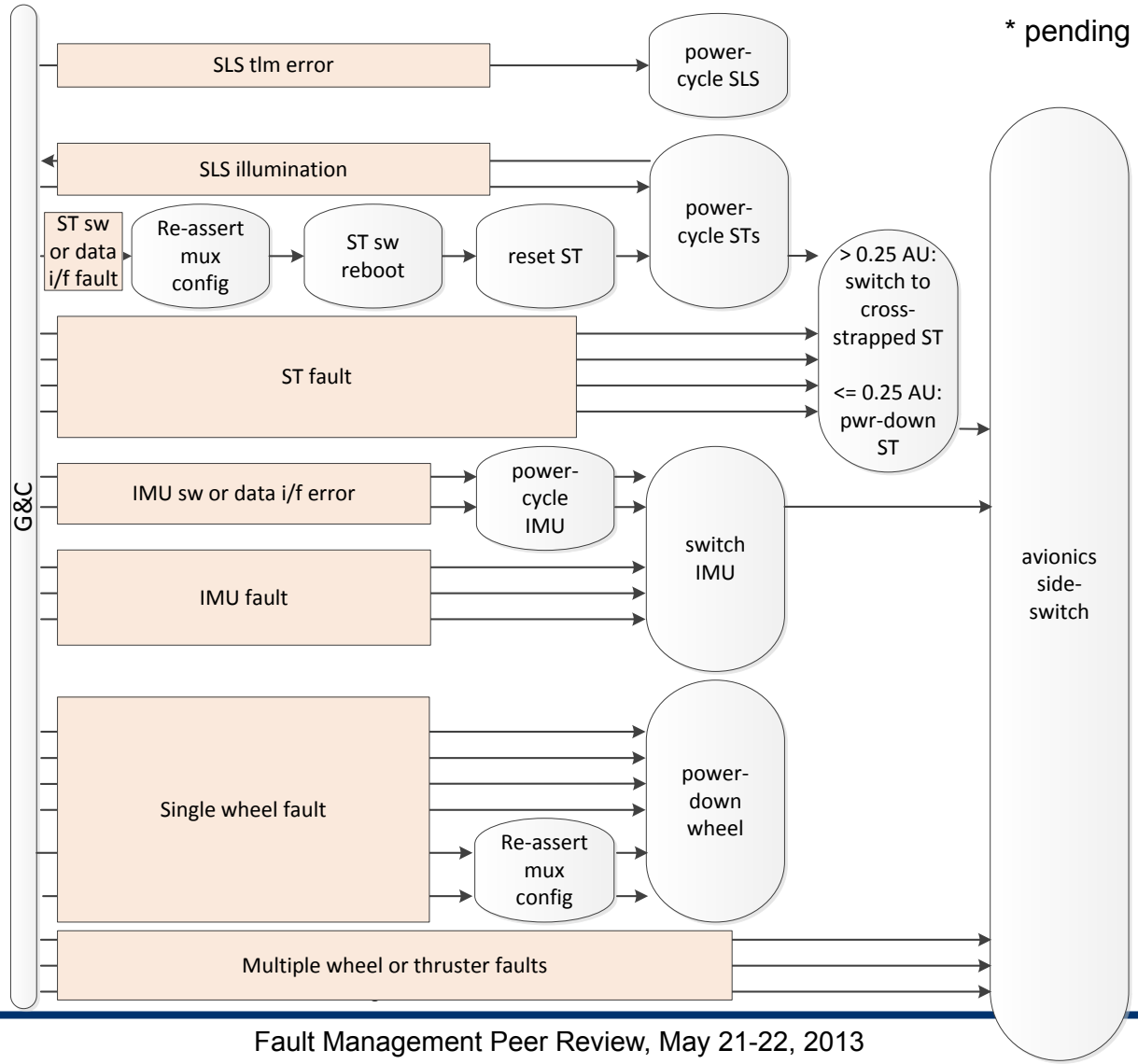
* pending component selection



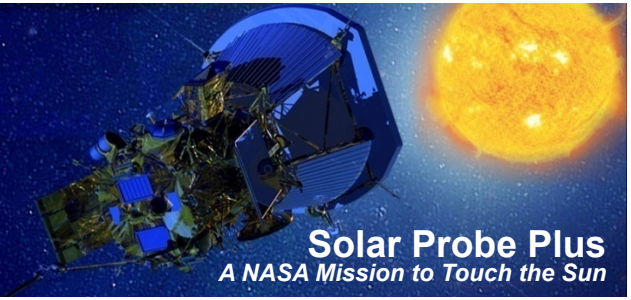
Fault Response: Guidance & Control*

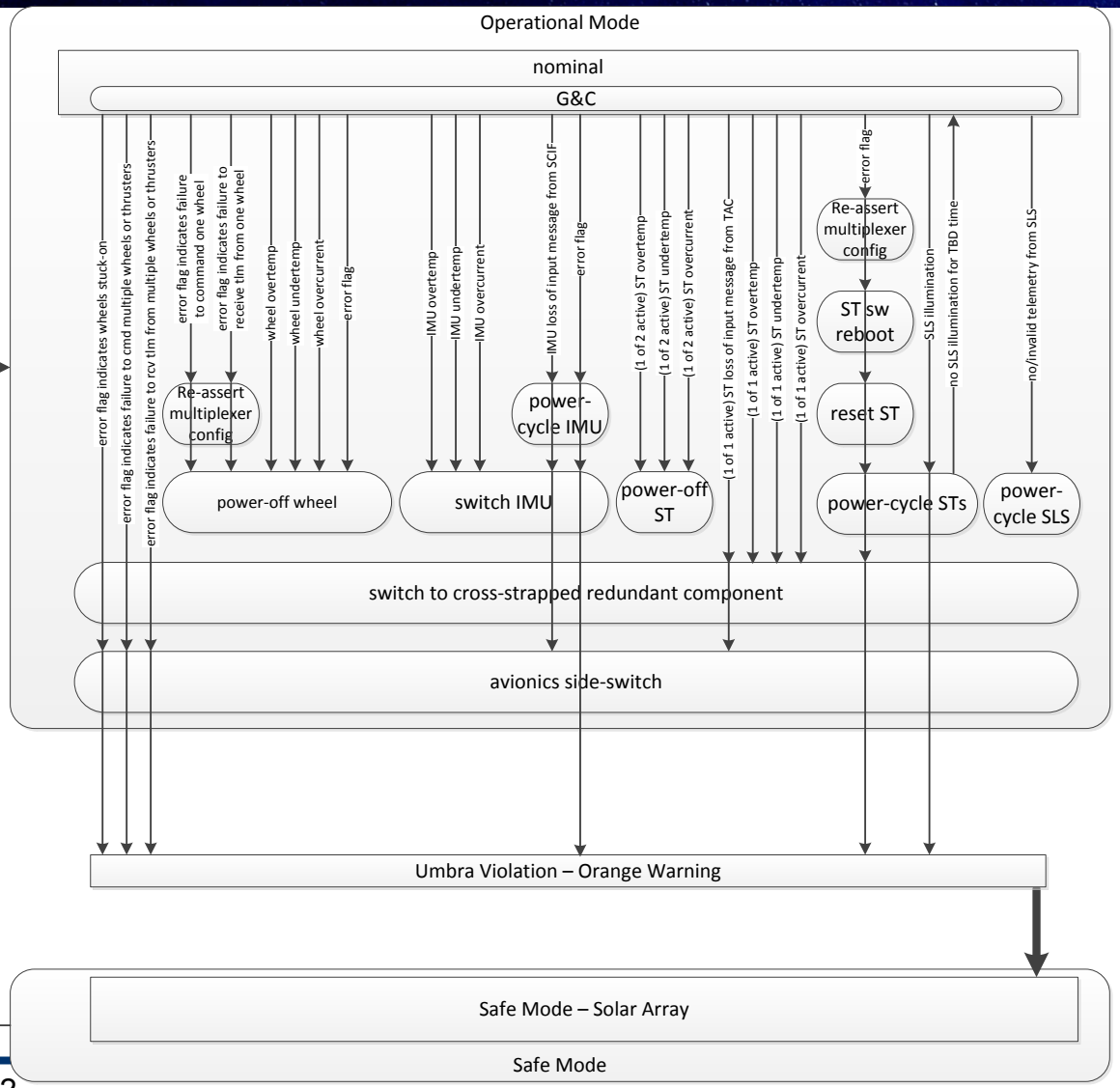


* pending component selection



G&C Fault Management* - L3 Requirements Mapping





* pending component selection

The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

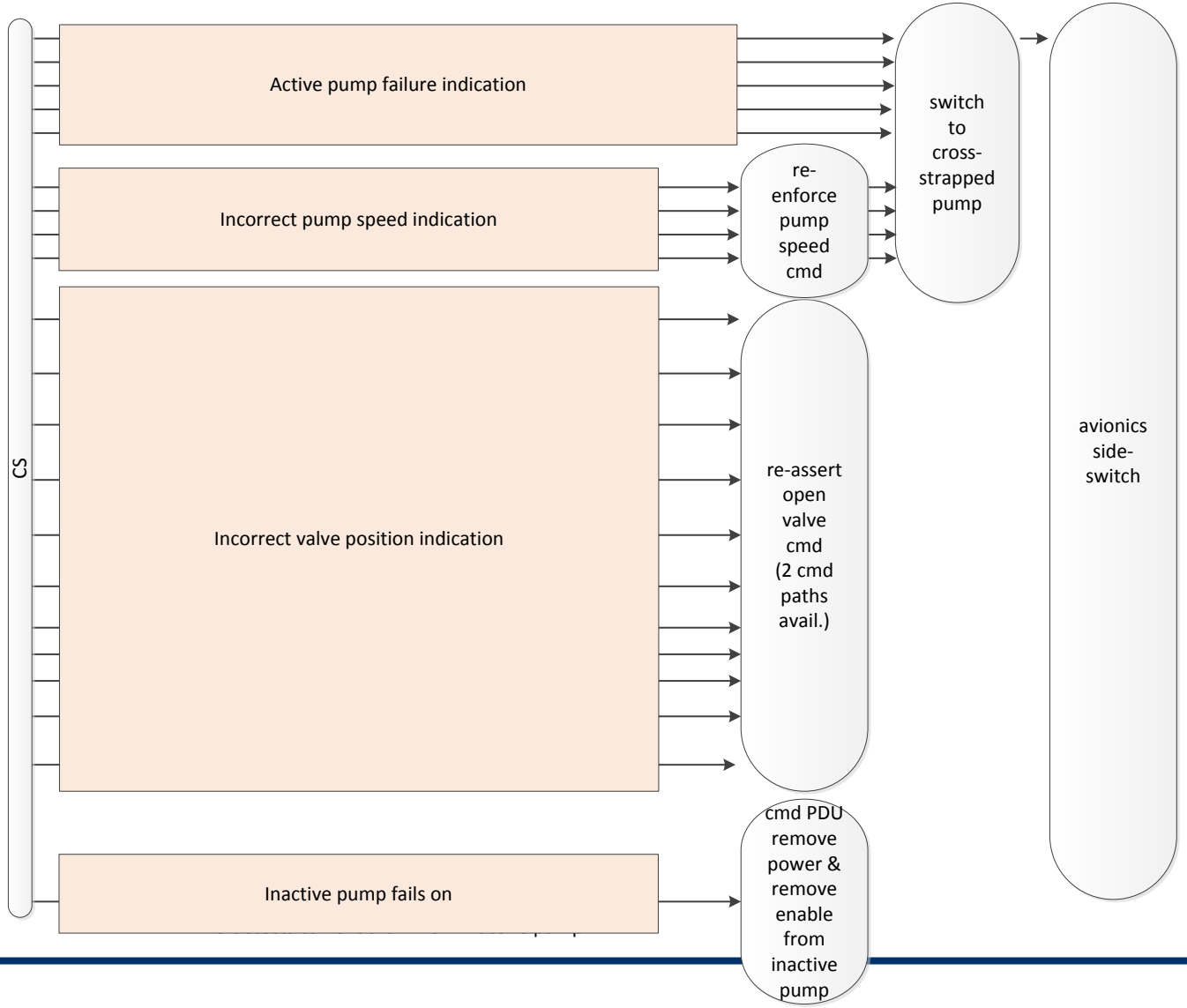
DETECTION OF CRITICAL FAULT CONDITIONS*

SAFING FOR CRITICAL FAULT CONDITIONS*

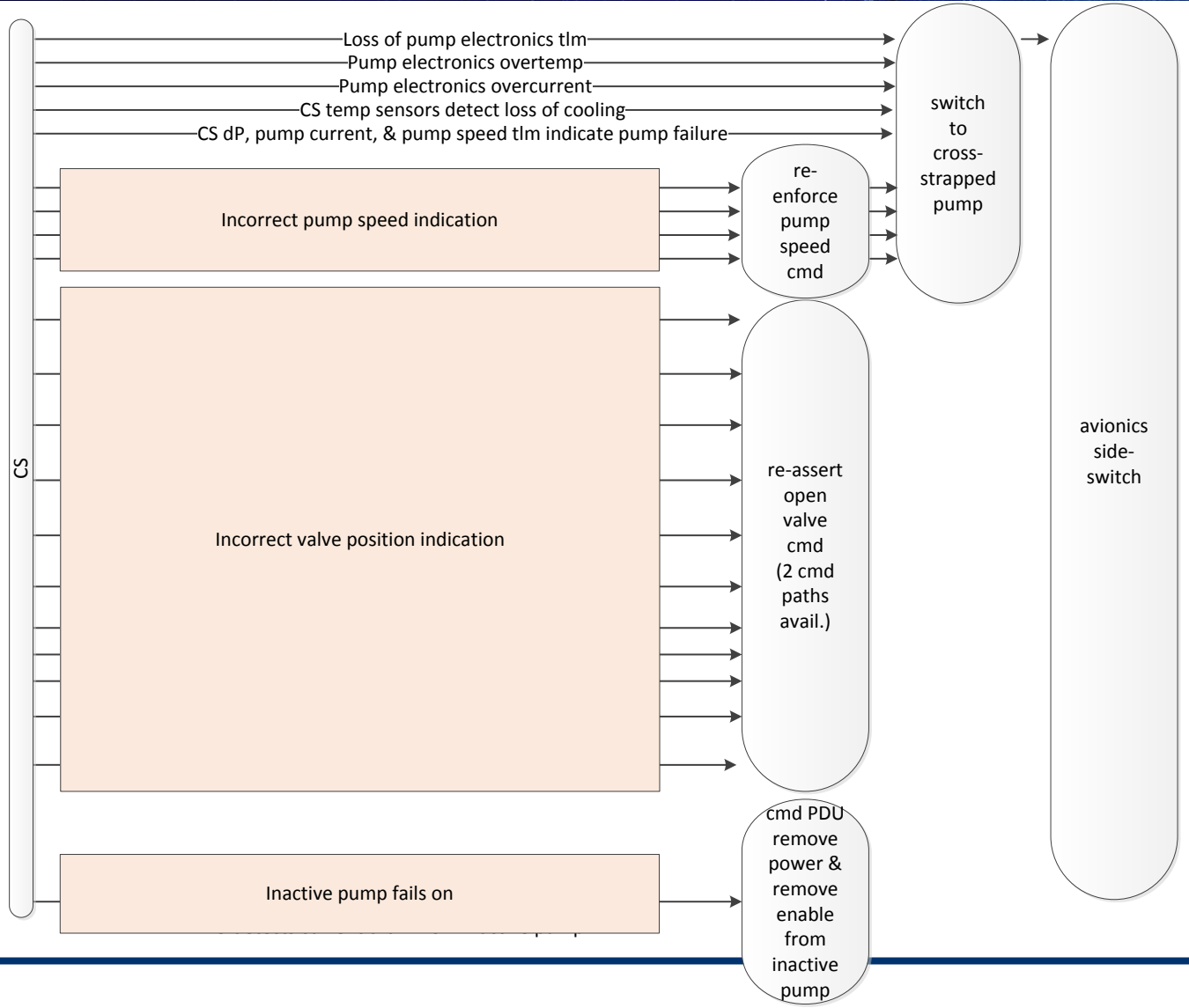
SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

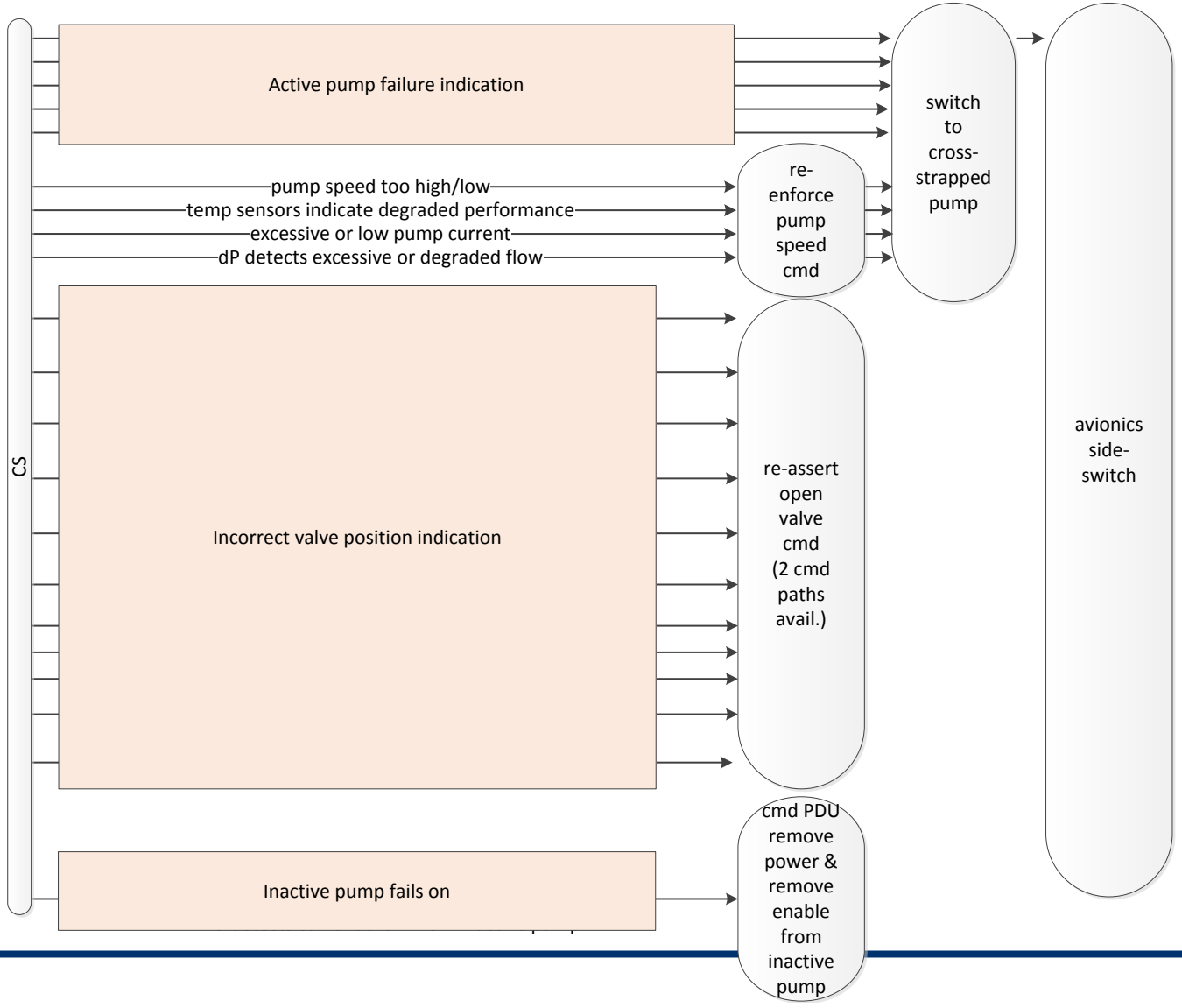
Fault Response: Cooling System



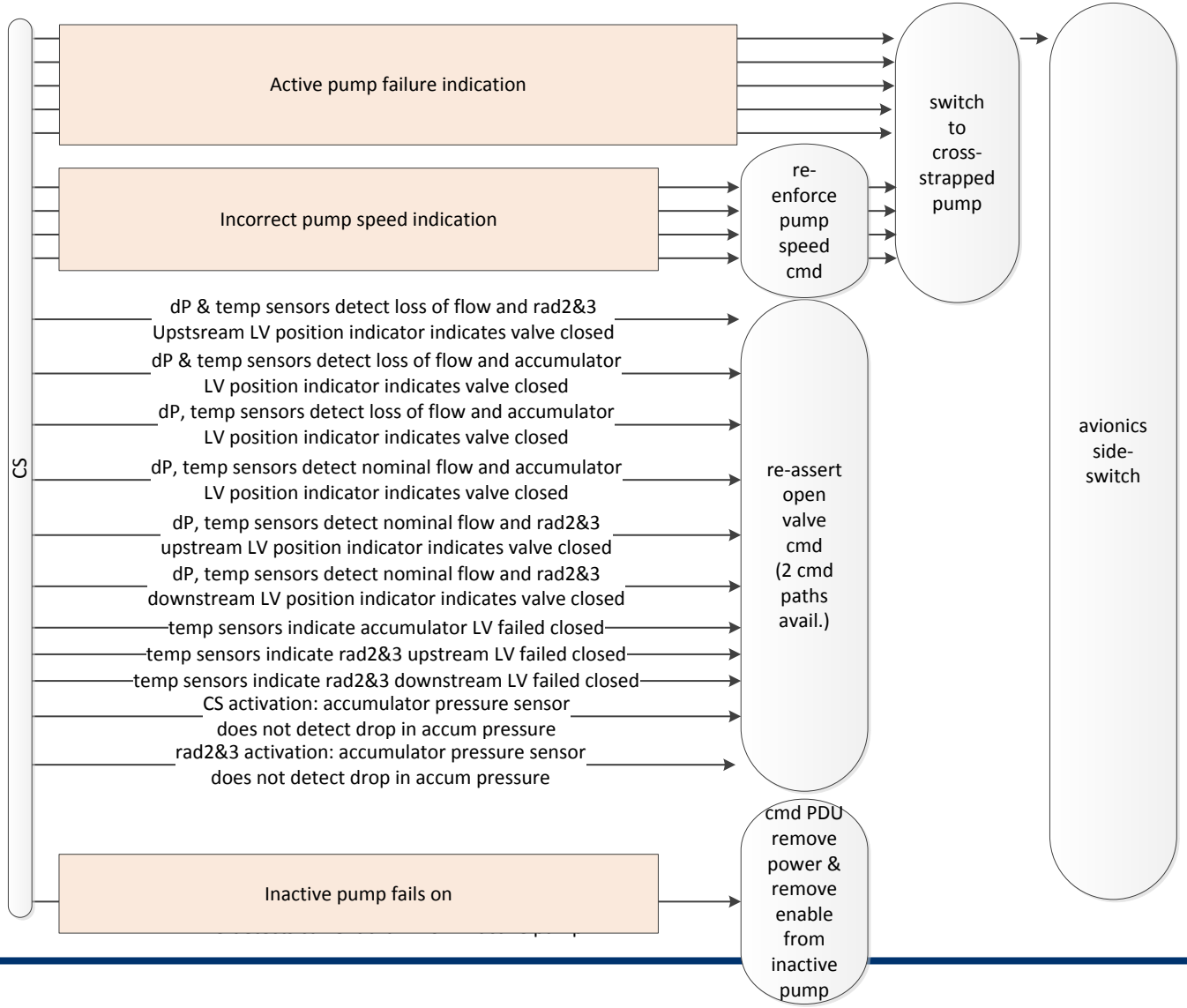
Fault Response: Cooling System



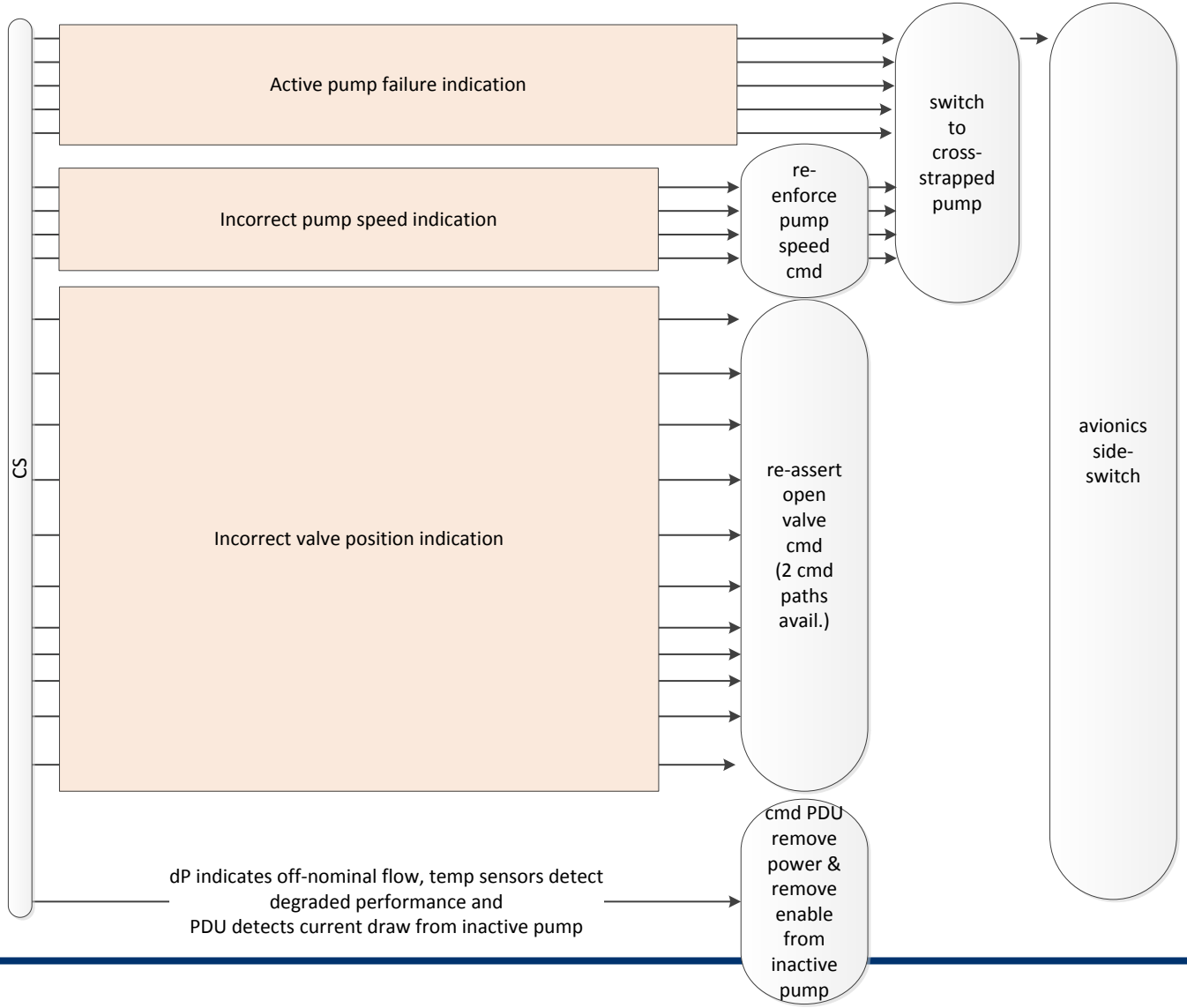
Fault Response: Cooling System



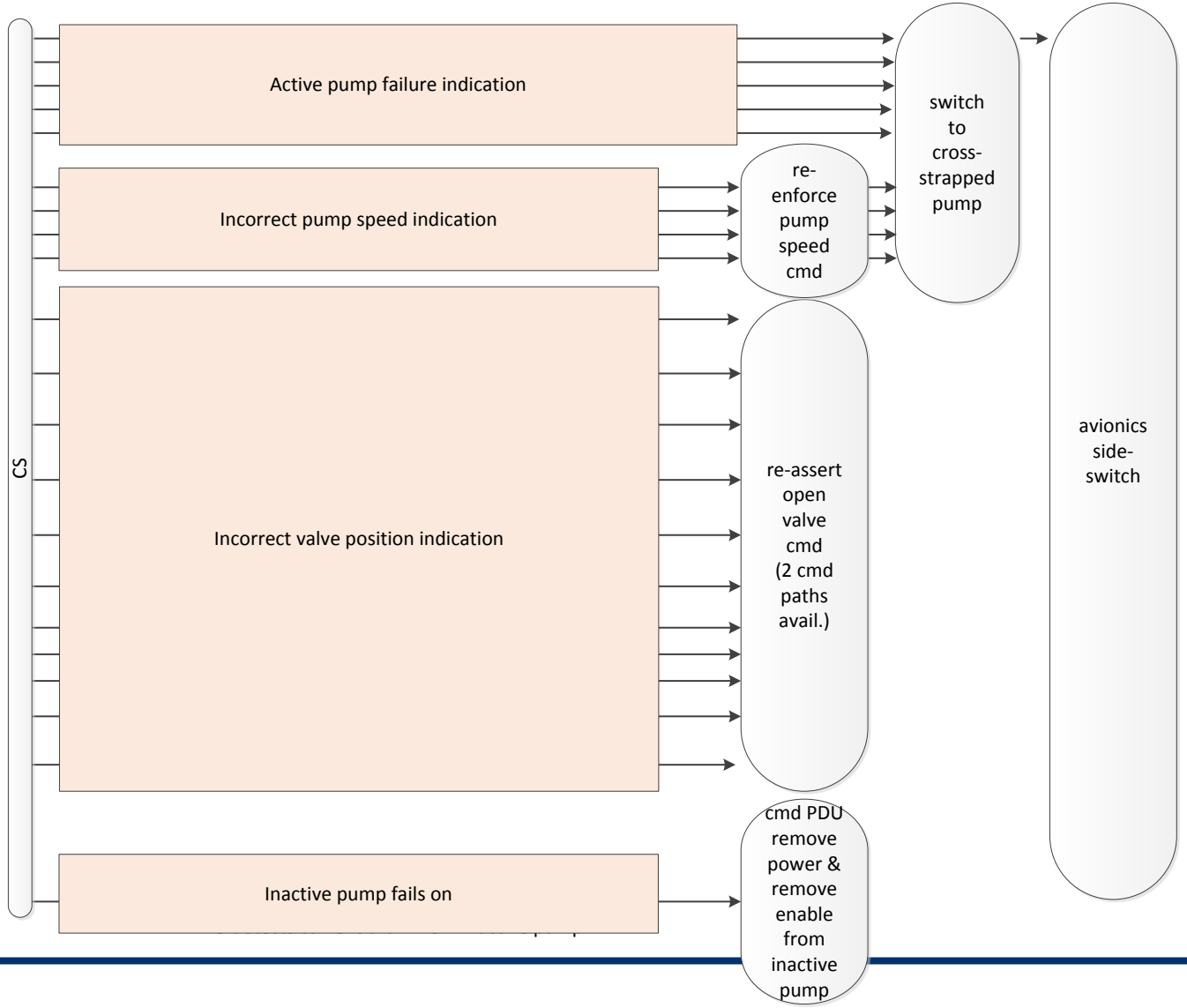
Fault Response: Cooling System



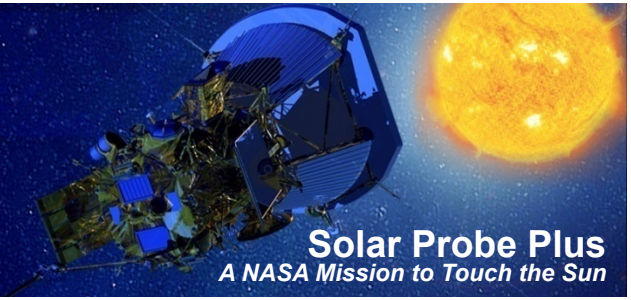
Fault Response: Cooling System

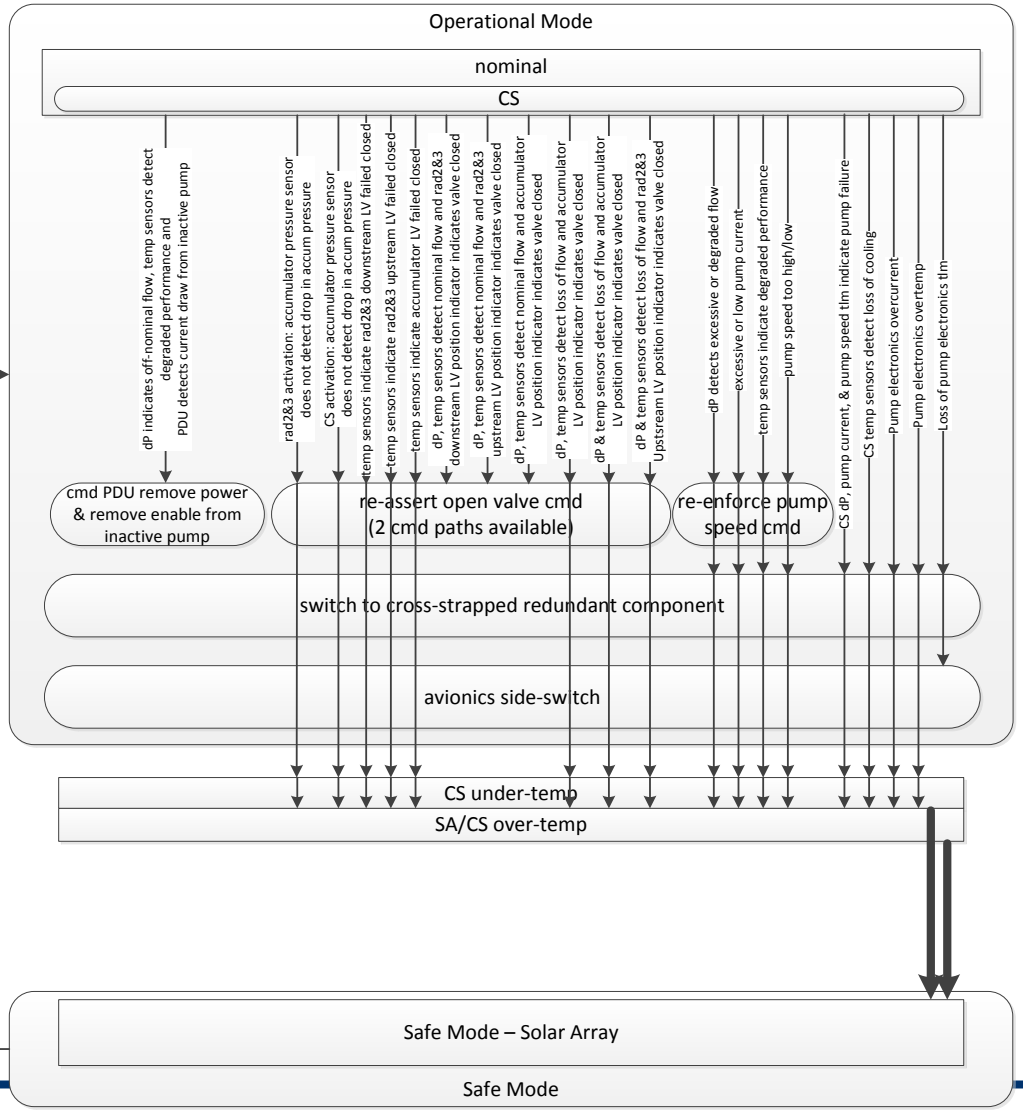


Fault Response: Cooling System



Cooling System FM – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

DETECTION OF CRITICAL FAULT CONDITIONS*

SAFING FOR CRITICAL FAULT CONDITIONS*

SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

Solar Probe Plus

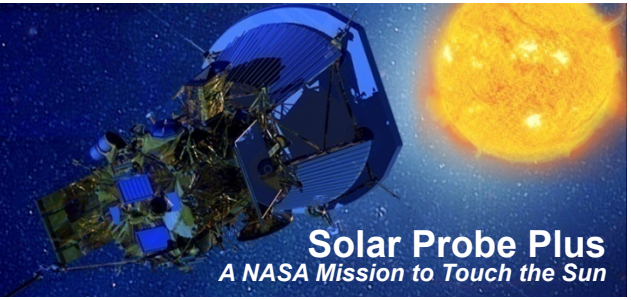
A NASA Mission to Touch the Sun

Maintaining Mission Elapsed Time (MET)

Rich Conde
Deputy Spacecraft Systems Engineer
Electrical Systems Engineer
rich.conde@jhuapl.edu

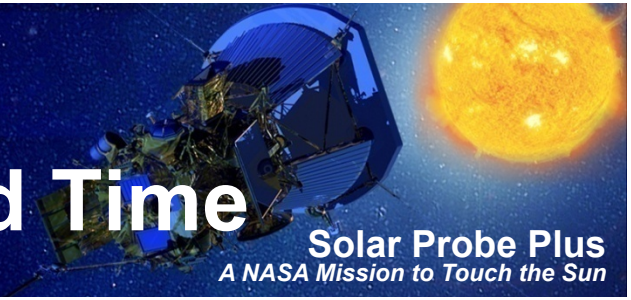
APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Topics



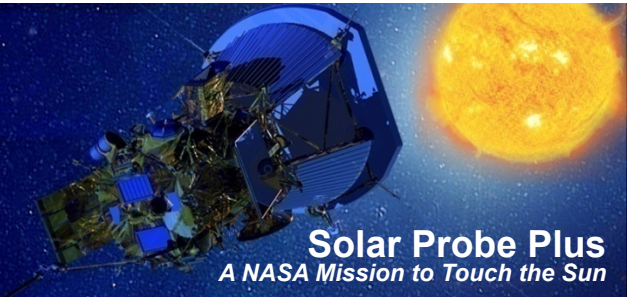
- Why must Mission Elapsed Time (MET) be fault tolerant?
- MET fault tolerance overview
- Hardware architecture
- Software architecture
- Fault Scenarios
- Conclusion

Importance of Mission Elapsed Time



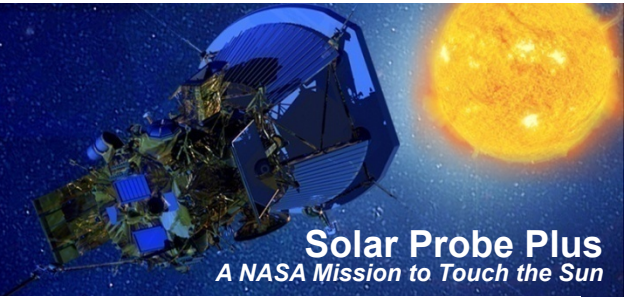
- Spacecraft target attitude (= where the spacecraft is trying to point to) is not determined from a real time measurement of the sun location, but on the ephemeris stored in each processor plus the time
  - A timekeeping process is used to maintain an onboard clock kernel that allows MET to be converted to Terrestrial Dynamic Time (TDT) with a specified worst case accuracy
  - Ephemeris + TDT allows position of astronomical objects to be computed by the Prime processor
  - If the MET is corrupted or lost the position of the sun cannot be determined
- Solar array safing angles and safing thresholds are dependent on MET

MET fault tolerance overview

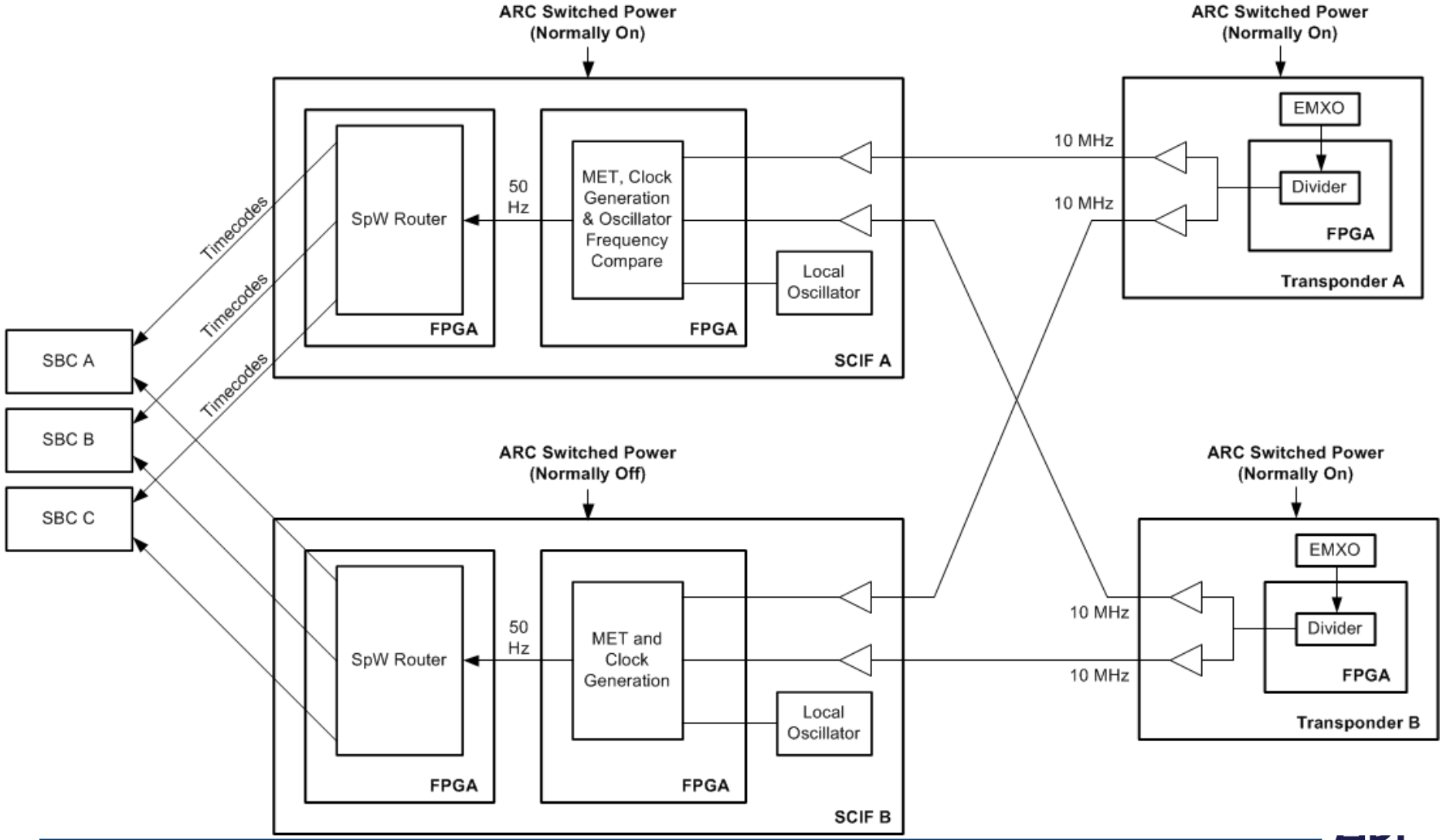


- Mission Elapsed Time (MET) is stored redundantly in 4 places during encounter:
  - MET is maintained in each of three processors as “cFE MET”
    - Each processor has a local oscillator used to maintain its own cFE MET
  - MET is maintained in one Spacecraft Interface (SCIF) card
    - One of two Spacecraft Interface (SCIF) boards is powered and is configured as the “Timecode Master”
    - The SCIF uses one of two cross-strapped precision clocks received from the Transponders as the time base for generating MET
- Each processor resyncs itself to SCIF MET once per second but will flywheel using local oscillator if resync not possible or desirable
- If the SCIF fails and loses MET, the Prime processor can initialize MET in the backup SCIF with an accuracy of at least 20 milliseconds
- Even if the Prime processor corrupts SCIF MET and its own cFE MET, a backup processor will take over and correct the SCIF MET

MET Hardware Architecture

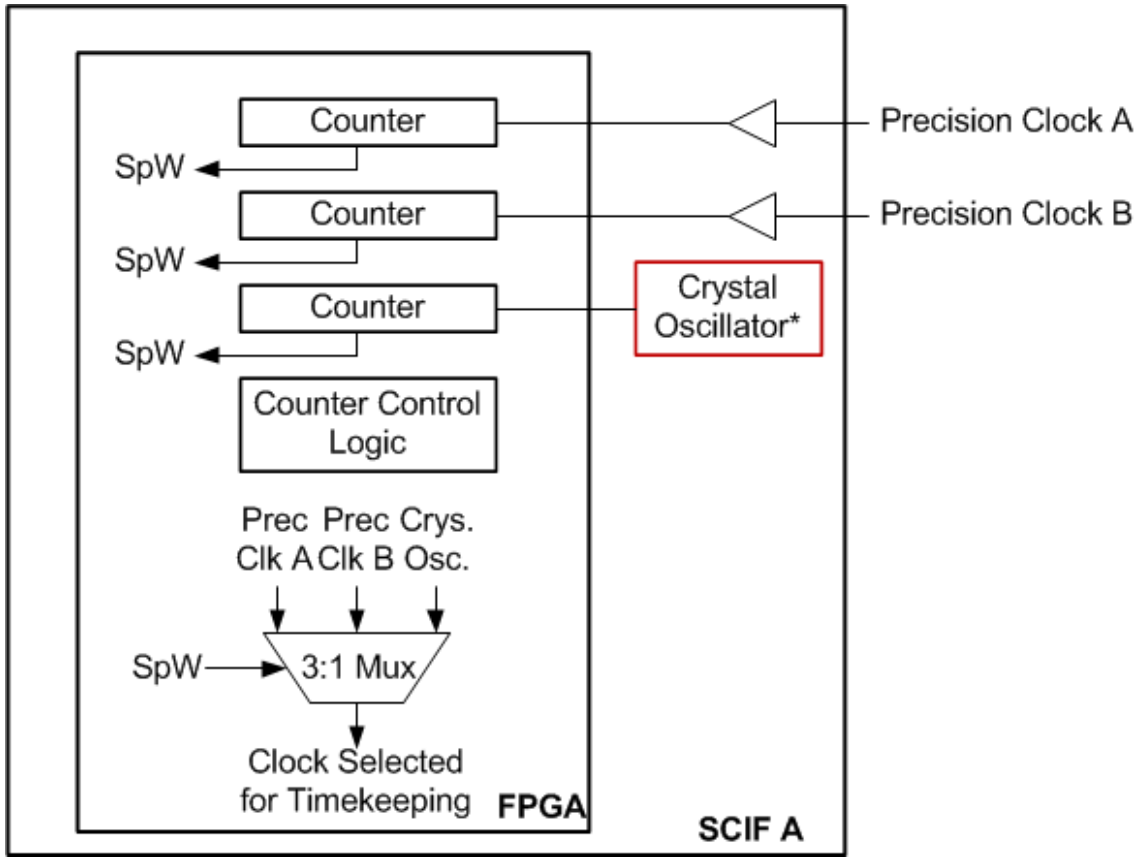


Solar Probe Plus
A NASA Mission to Touch the Sun



SCIF Includes capability to measure frequency offsets between oscillators

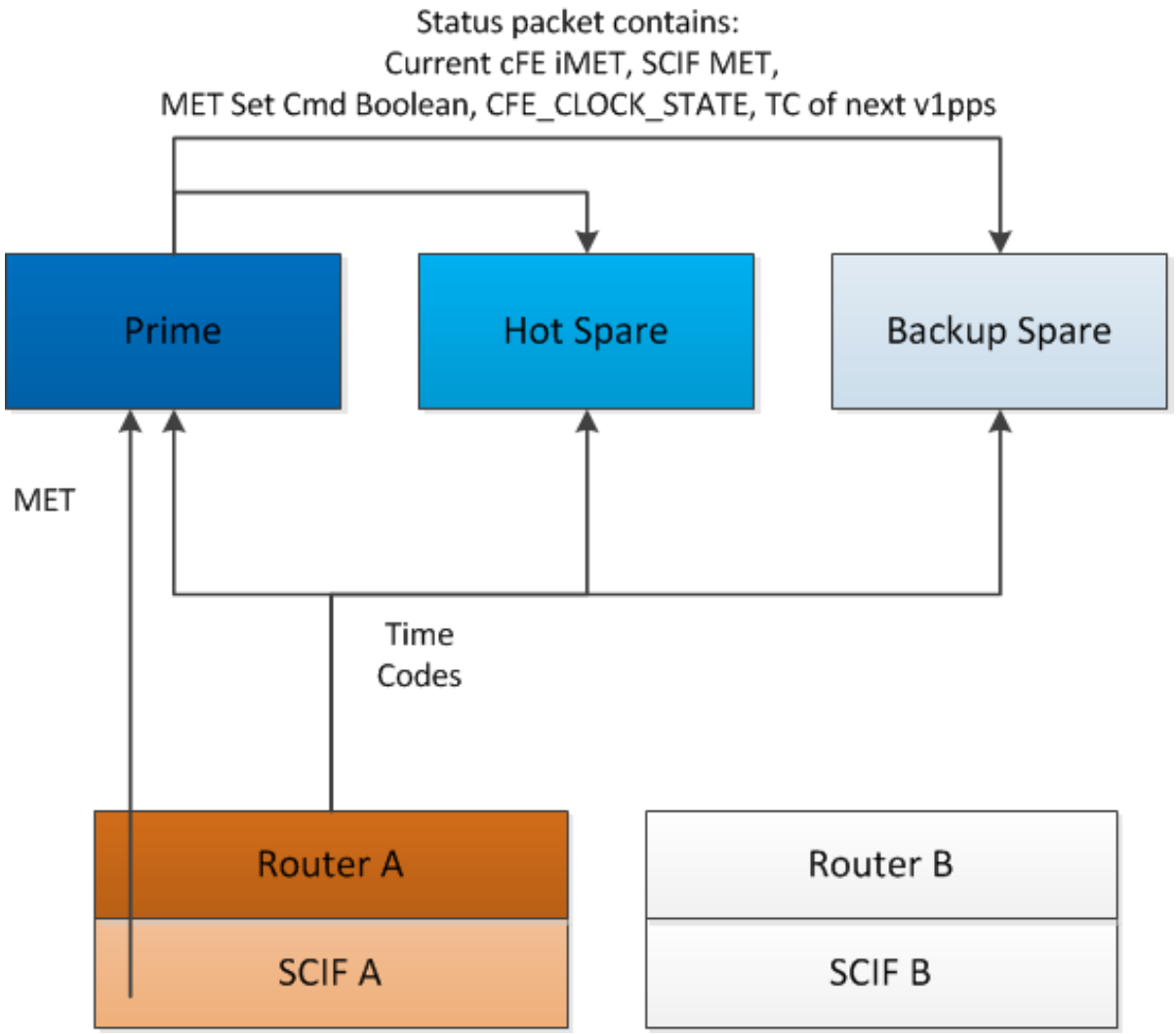
Concept only, actual implementation TBD



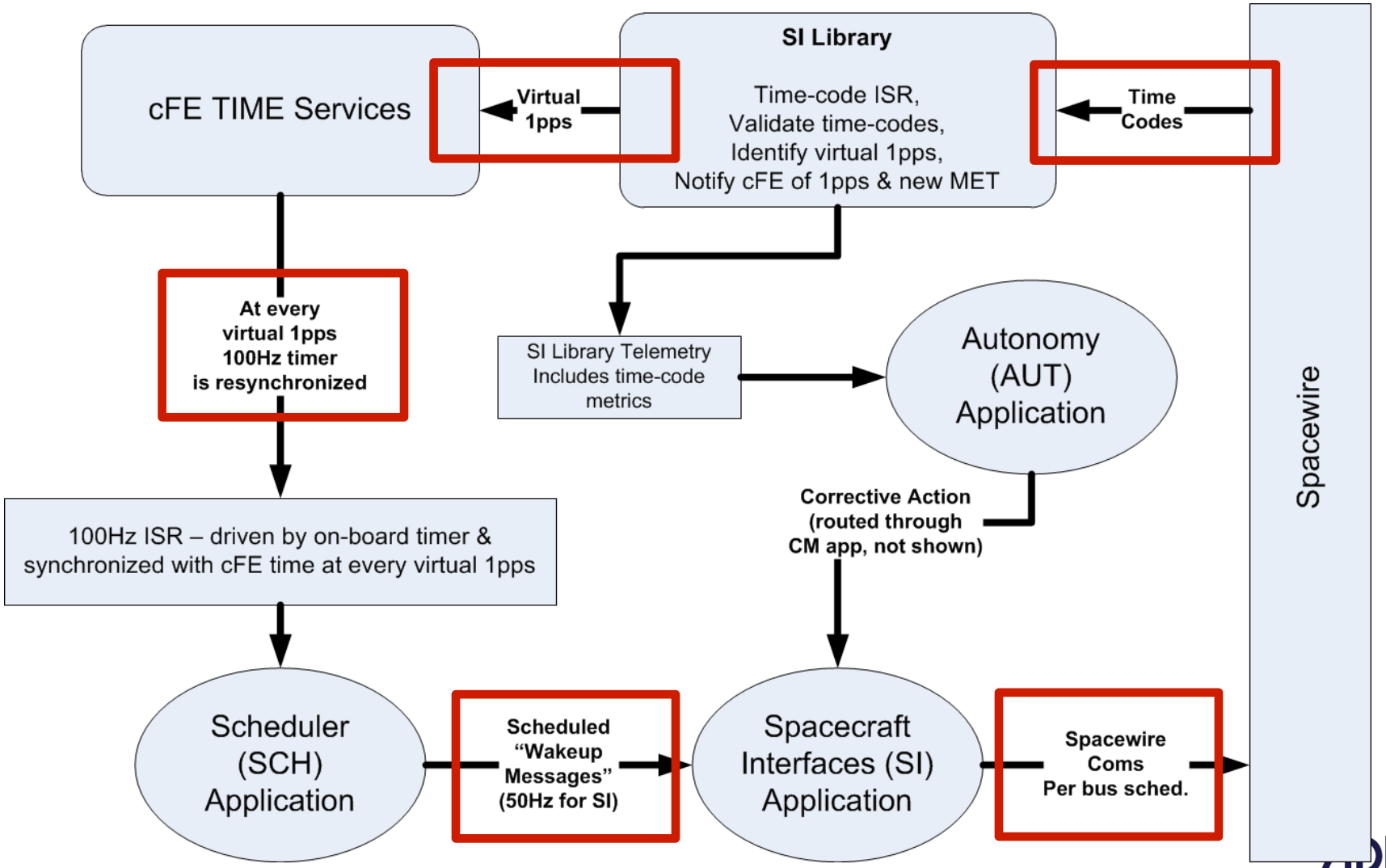
Counter values used by autonomy to identify an out-of-bounds oscillator

***Accommodation of TCXO vs. crystal oscillator is an ongoing Avionics trade study**

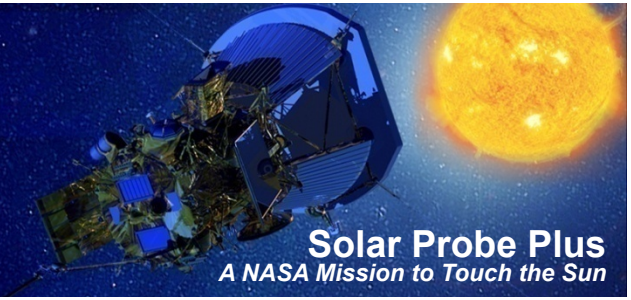
MET Distribution to Processors



Processing of Time Codes by FSW



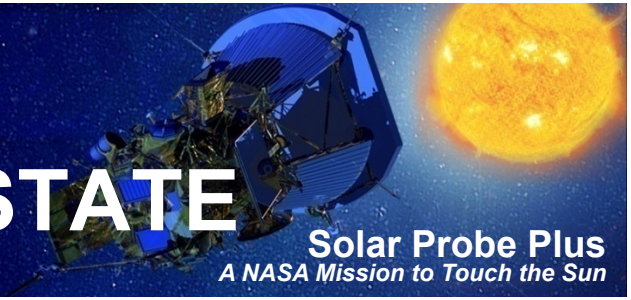
cFE Clock State



- **The cFE Clock State enumerations identify the three recognized states of cFE time-keeping.**
  - **CFE_TIME_INVALID - If the clock has never been successfully synchronized with the primary onboard clock source**
  - **CFE_TIME_VALID - If the time is currently synchronized (i.e. – the primary synchronization mechanism has not been dropped for any significant amount of time).**
  - **CFE_TIME_FLYWHEEL - If the time had, at some point in the past, been synchronized, but the synchronization with the primary onboard clock has since been lost. Since different clocks drift at different rates from one another, the accuracy of the time while in CFE_TIME_FLYWHEEL is dependent upon the time spent in that state.**

- Command between any states.
- System starts up in CFE_TIME_INVALID.
- Needs to be commanded to valid.
- If MET is changed by command, the clock must be commanded to invalid, then back to valid for the new MET to be accepted by cFE.
- Nominal state is CFE_TIME_VALID

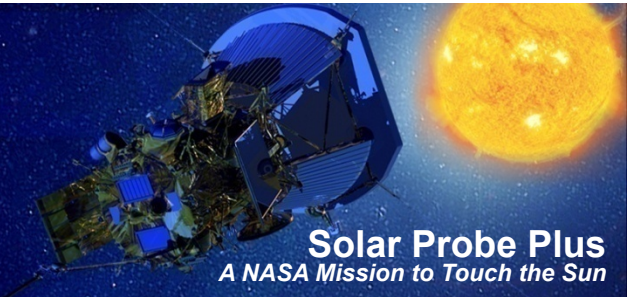
Initialization of CFE_CLOCK_STATE



Solar Probe Plus
A NASA Mission to Touch the Sun

- **Each SBC FSW may autonomously (AUT) advance CFE_CLOCK_STATE to VALID once per role per reset.**
  - **Prime AUT to advance CFE_CLOCK_STATE→ VALID after:**
    - **POR reset after TBD seconds of good SCIF MET (occurs during spacecraft power-up on pad)**
    - **Rotation into Prime (was HS with CFE_CLOCK_STATE = INVALID)**
  - **Spare AUT to advance CFE_CLOCK_STATE → VALID after:**
    - **TBD seconds of good MET from Prime**

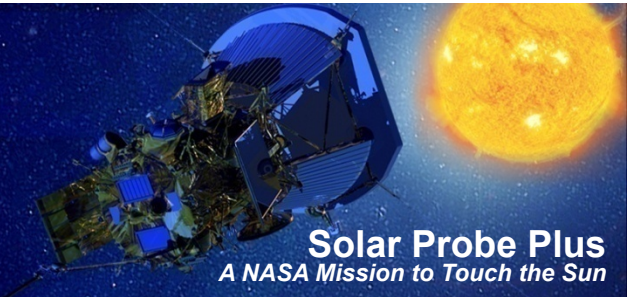
MET validity checking



- cFE
  - When the clock state has been commanded to “valid”, cFE will ignore time values that disagree with its own by more than configurable threshold
  - If MET is changed by command, the cFE clock must be commanded “invalid” then back to “valid” for it to accept the MET value from H/W (do not expect to do this in flight)
- G&C
  - To do sanity check on time before doing calculations: Will check if current time is within +/- 1 second of previous read of time.
  - G&C also to be given warning that SCIF MET will be / did change by command

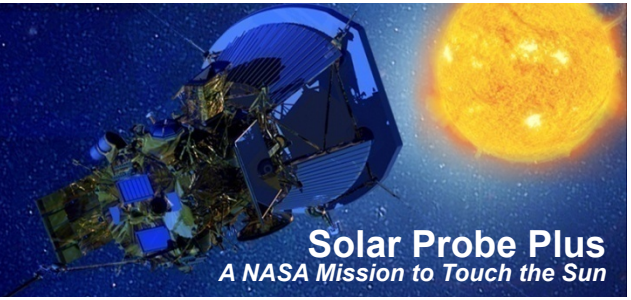
MET Fault Scenarios

MET Fault Scenarios



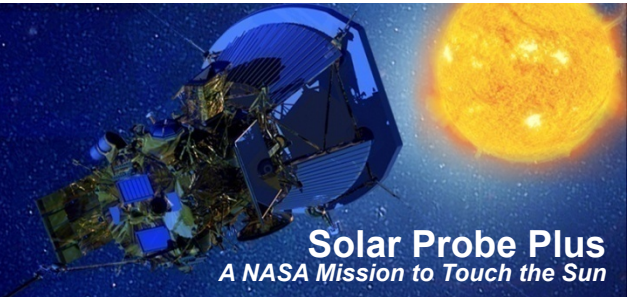
Fault #	MET Faults
1	Transient Loss of Time Code (1 PPS)
2	Transient Loss of Time Code (non-1 PPS)
3	SpW Transient failure - misread of MET or corrupted message
4	MET value in SCIF FPGA corrupted
5	Hard failure causing loss of EMXO Precision Clock to SCIF
6	MET oscillator frequency more then TBD ppm out of spec
7	Any fault requiring REM side switch
8	Prime FSW executes erroneously and corrupts SCIF MET and cFE MET
9	Backup Spare Oscillator fails to a low or high frequency
10	Hot Spare Oscillator fails to a low or high frequency
11	Prime Oscillator fails to a low or high frequency

Fault: Transient Loss of Time Code at 1 PPS



- Effects:
  - Missing TC interrupt in SBCs
- Detection:
  - SBC would detect a jump in TC value (due to missing TC)
- Response:
  - cFE flywheels MET
  - Re-initialize SCIF MET-related registers the first time a 1 PPS Timecode does not arrive
  - Side switch REM if it happens again

Fault: Transient Loss of Time Code other than 1 PPS

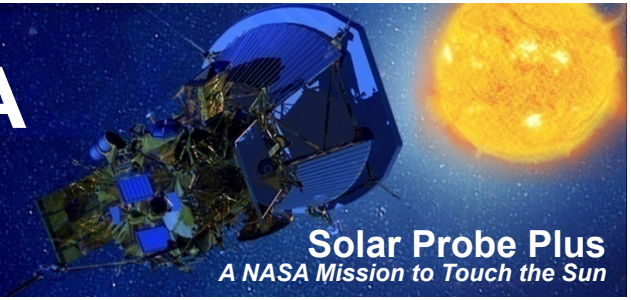


- Effects:
  - Missing TC interrupt in SBCs
- Detection:
  - SBC would detect a jump in TC value (due to missing TC)
- Response:
  - None required

Fault: SpW Transient failure - misread of MET or corrupted message

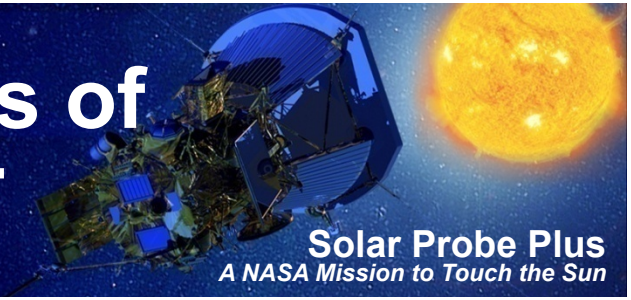
- Effect:
  - Value of SCIF MET when read does not match expected MET +/- configurable threshold or
  - SCIF MET value not delivered to cFE
- Detection:
  - cFE detects out-of-bounds MET value
  - Bad transaction detected
- Response:
  - cFE flywheels MET
  - Re-initialize MET register the first time a bad value is received
  - Side switch REM if it happens again

Fault: MET value in SCIF FPGA corrupted



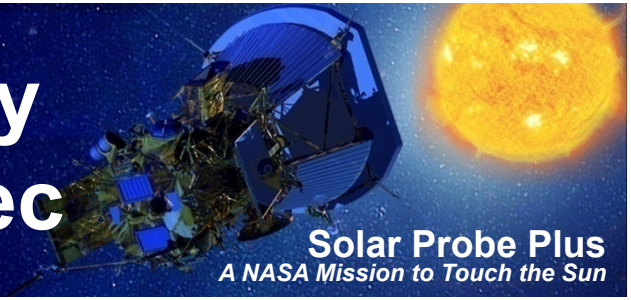
- Effect:
  - Value of SCIF MET when read does not match expected MET +/- configurable threshold
- Detection:
  - cFE detects out-of-bounds MET value
- Response:
  - cFE flywheels MET
  - FSW re-initializes MET register the first time this happens
  - Autonomy side switches REM if it happens again

Fault: Hard failure causing loss of EMXO Precision Clock to SCIF



- Effects:
  - Loss of time codes
  - MET freezes
- Detection:
  - cFE detects missing TC and possible bad MET value
  - SCIF + Autonomy detects out-of-bounds oscillator
- Response:
  - cFE flywheels MET
  - Switch to other EMXO & re-initialize SCIF MET register with cFE MET

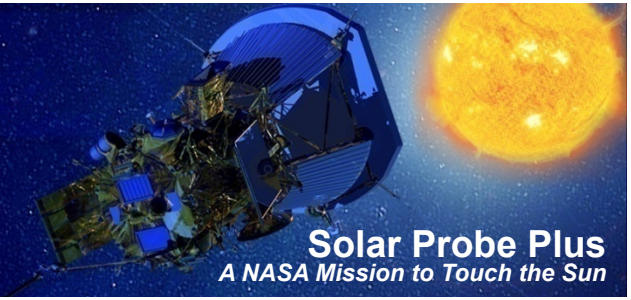
Fault: MET oscillator frequency more then TBD ppm out of spec



- Effect:
  - MET incrementing much faster or slower than expected (> +/- XXX PPM, sensitivity depends on the selected SCIF oscillator)
- Detection:
  - Autonomy detects out-of-spec oscillator using SCIF frequency comparison registers
- Responses:
  - If EMXO used for MET out of spec then switch to other EMXO
  - If non-selected EMXO out of spec no response
  - If SCIF oscillator out of spec then side switch

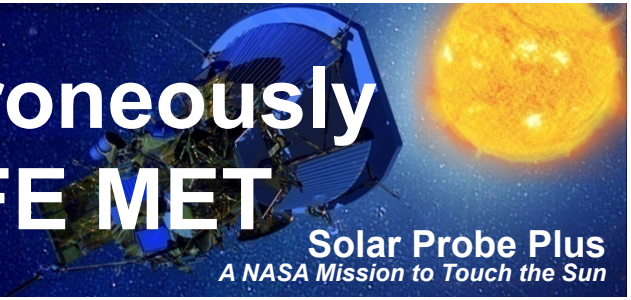
Note, sensitivity of detecting a faulted oscillator depends on whether SCIF can accommodate a TCXO or crystal oscillator

Fault: Any fault requiring REM side switch



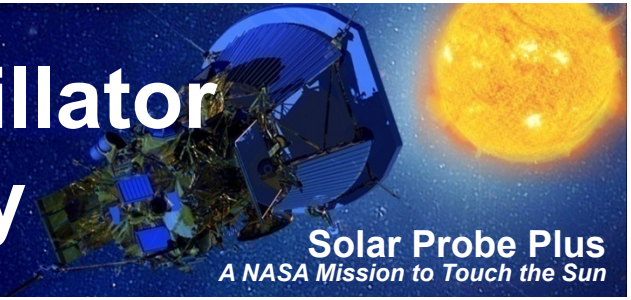
- Effect:
  - New SCIF has uninitialized MET
- Detection:
  - Fault was detected by something other than MET-related fault management
- Response:
  - cFE flywheels MET
  - Prime initializes new SCIF MET register with cFE MET

Fault: Prime FSW executes erroneously and corrupts SCIF MET and cFE MET



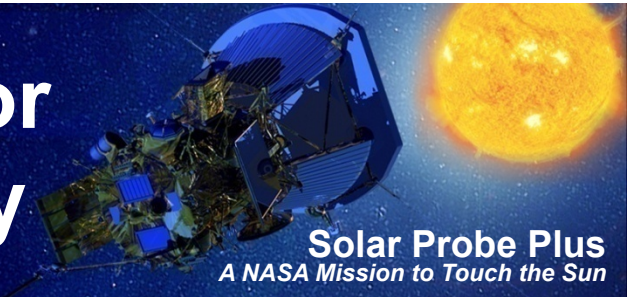
- Effect:
  - SCIF MET corrupted and bad MET sent to Hot Spare and Backup Spare
  - From FSW team: not credible for this to happen without either 1) SBC hardware generated reset due to EDAC error OR 2) timeout of SBC Watchdog Timer (either due to explicit "starving" of WDT by the watchdog task or implicit "starving" of WDT due to erroneous FSW)
  - SBC WDT reset results in timeout of ARC Prime Acknowledge Timer
- Detection:
  - ARC Prime Acknowledge Timer
- Response:
  - ARC promotes Hot Spare to Prime
  - Hot Spare re-initializes SCIF MET with own cFE MET if necessary (would not have refreshed own MET with a bad MET in 1 Hz message from Prime if exceeded configurable threshold)

Fault: Backup Spare SBC Oscillator fails to a low or high frequency



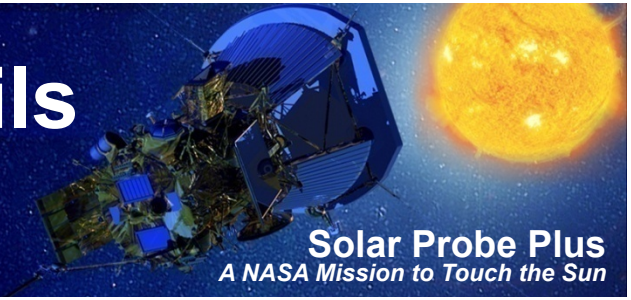
- Effect:
  - Backup Spare could falsely think there was a MET or timecode fault and switch to flywheel mode, propagating cFE MET with its own oscillator
- Detection:
  - Cruise phase (during ground contact): faulty BS would be detected by Mission Ops and demoted to Failed
  - Encounter phase (out of ground contact):
    - If BS is not promoted, not detected (other than BS itself going to flywheel mode)
    - If BS was promoted to Hot Spare see next slide
- Response:
  - Cruise phase: Mission ops demotes BS to Failed
  - Encounter phase: No effect unless promoted to Prime (see slide 24)

Fault: Hot Spare SBC Oscillator fails to a low or high frequency



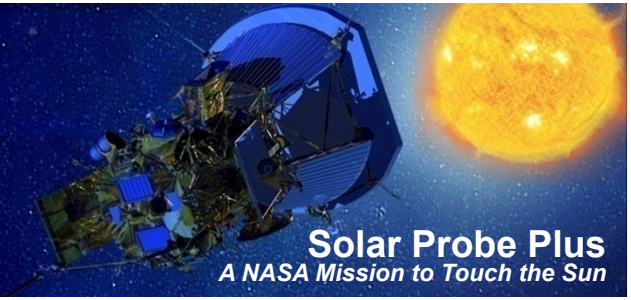
- Effect:
  - Hot Spare could falsely think there was a MET or timecode fault and switch to flywheel mode, propagating cFE MET with its own oscillator
- Detection:
  - Cruise phase (during ground contact): faulty HS would be detected by Mission Ops and demoted to Failed
  - Encounter phase (out of ground contact):
    - If HS is not promoted, not detected (other than HS itself going to flywheel mode)
    - If HS was promoted to Prime see next slide
- Response:
  - Cruise phase: Mission ops demotes HS to Failed
  - Encounter phase: No effect unless promoted to Prime (see next slide)

Fault: Prime SBC Oscillator fails to a low or high frequency



- Effect:
  - Prime could falsely think there was a MET or timecode fault and switch REM sides (after entering flywheel mode); the same fault would be detected on the other REM
  - Prime could get out of sync with 50 Hz registers by the end of each second
- Detection:
  - Autonomy would detect that faults were detected on both REMs
- Response:
  - Prime would demote itself; Hot Spare would take over as Prime
  - New Prime would re-initialize MET if necessary

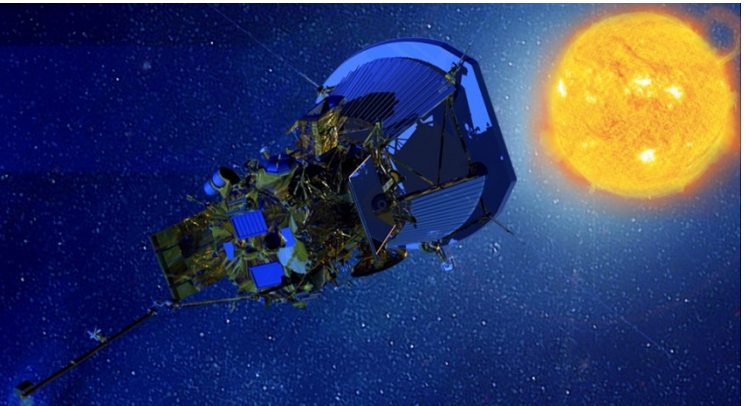
Conclusion



- **The MET hardware and software architecture enables MET to be tolerant to all single faults**

Solar Probe Plus

A NASA Mission to Touch the Sun

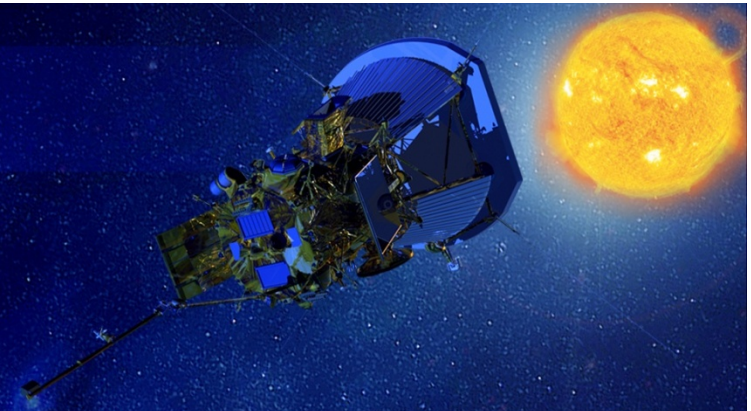


End of Day 1

The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Solar Probe Plus

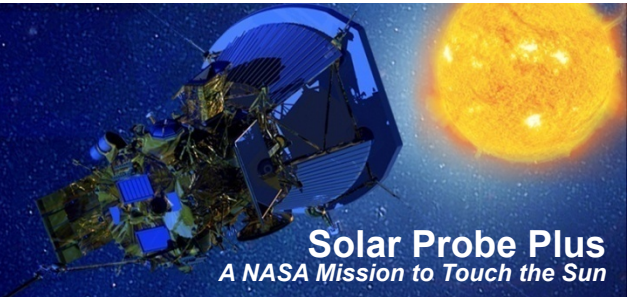
A NASA Mission to Touch the Sun

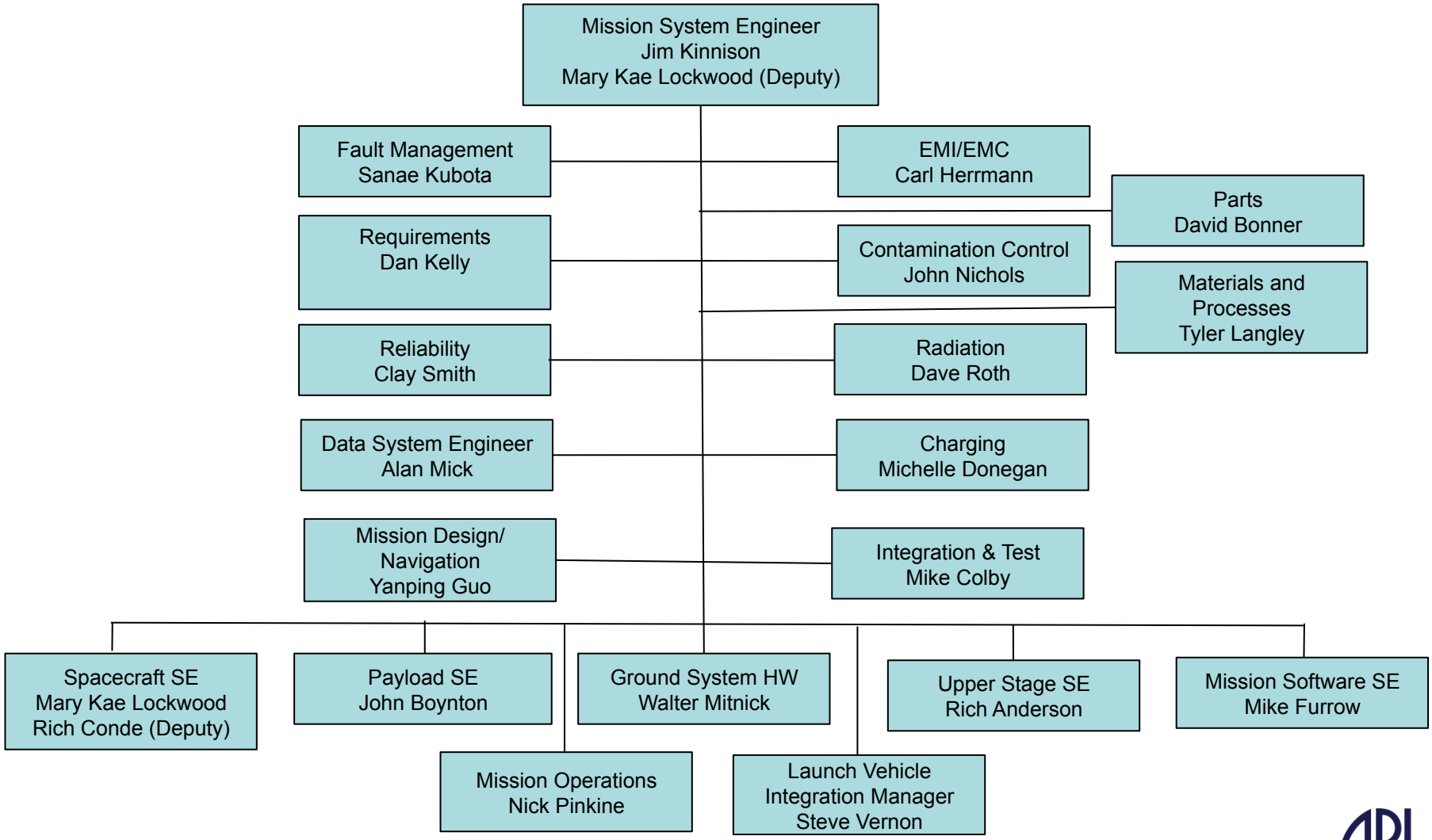


BACK-UP

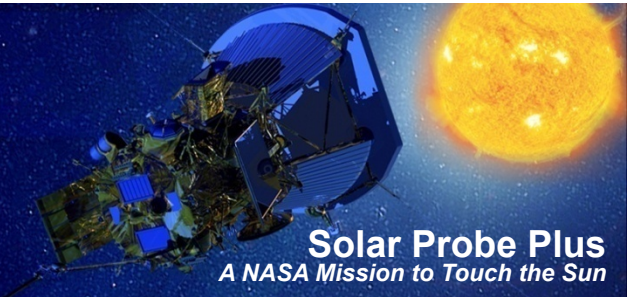
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

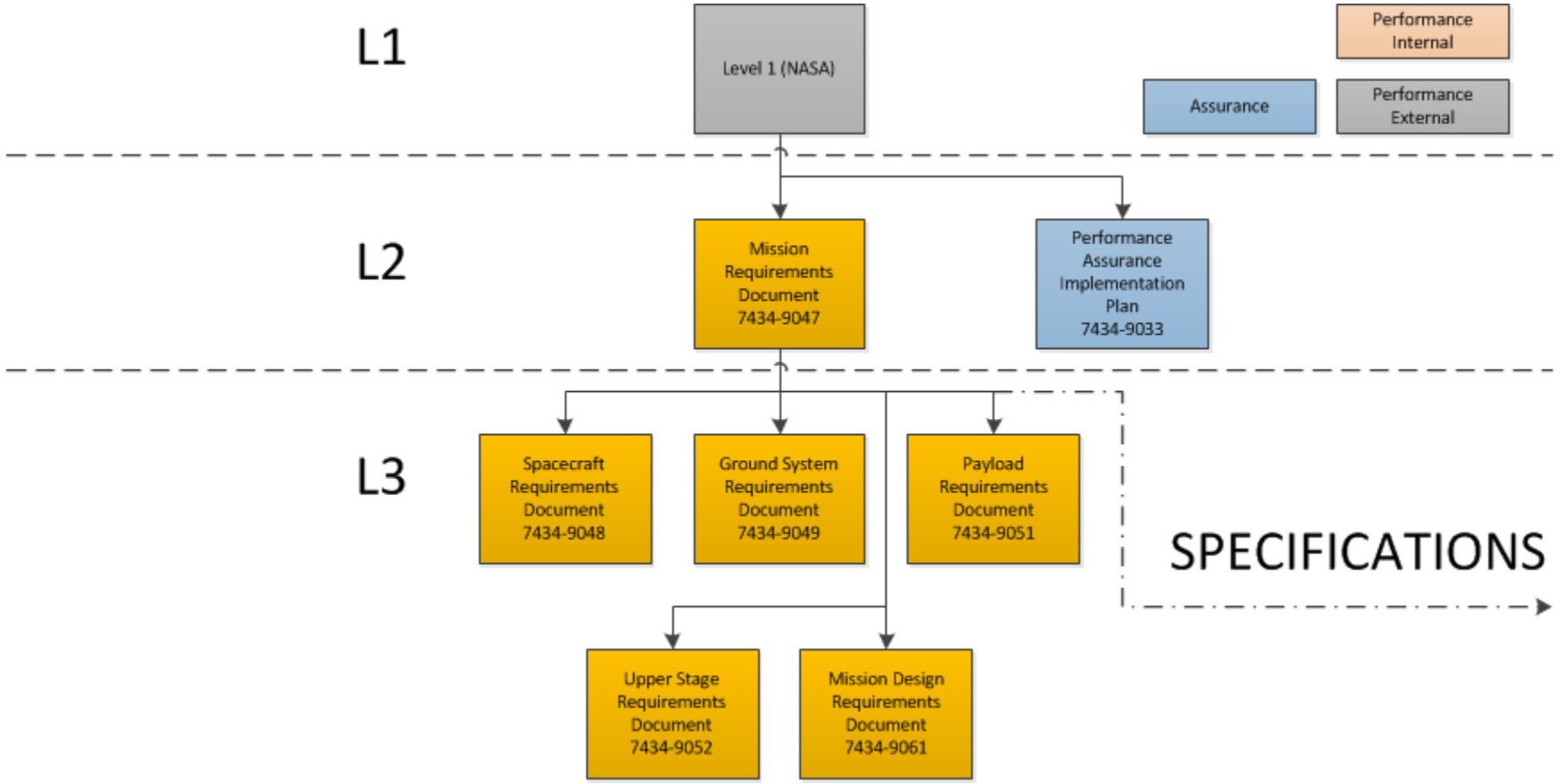
System Engineering Organization





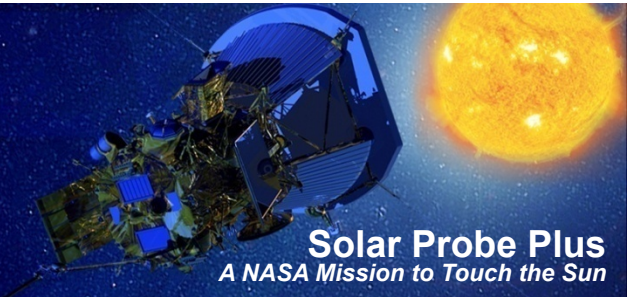
Level 2 – Mission (MRD)

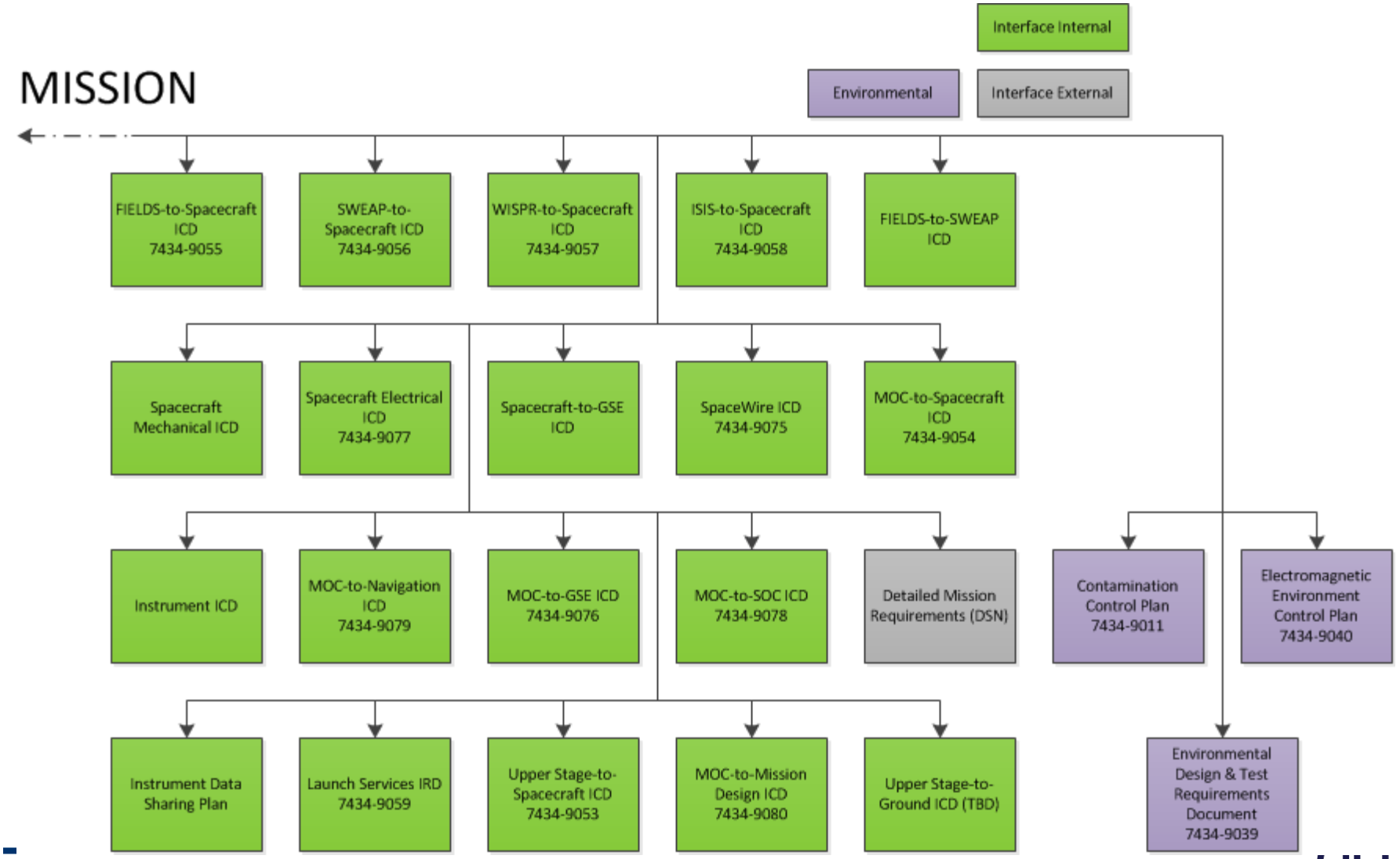




Source: Dan Kelly, 5/9/13

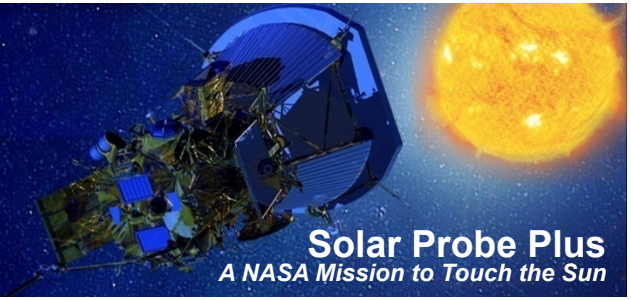
Specification Documents

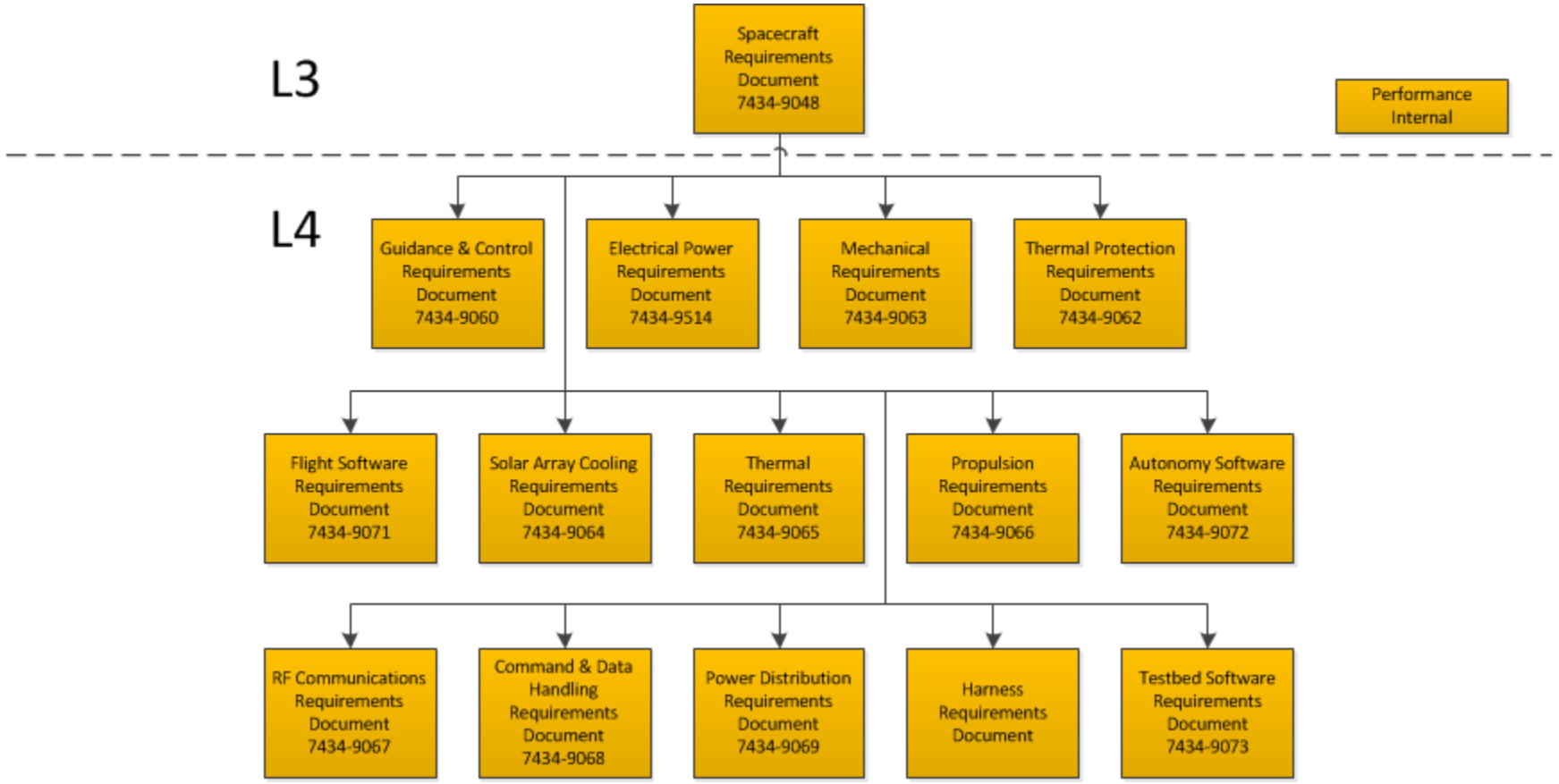




 Source: Dan Kelly, 5/9/13

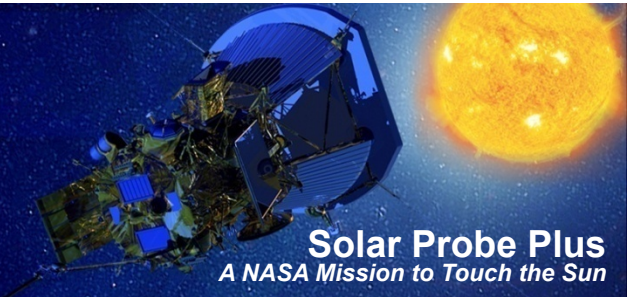
Level 3 – Spacecraft (SCRD)



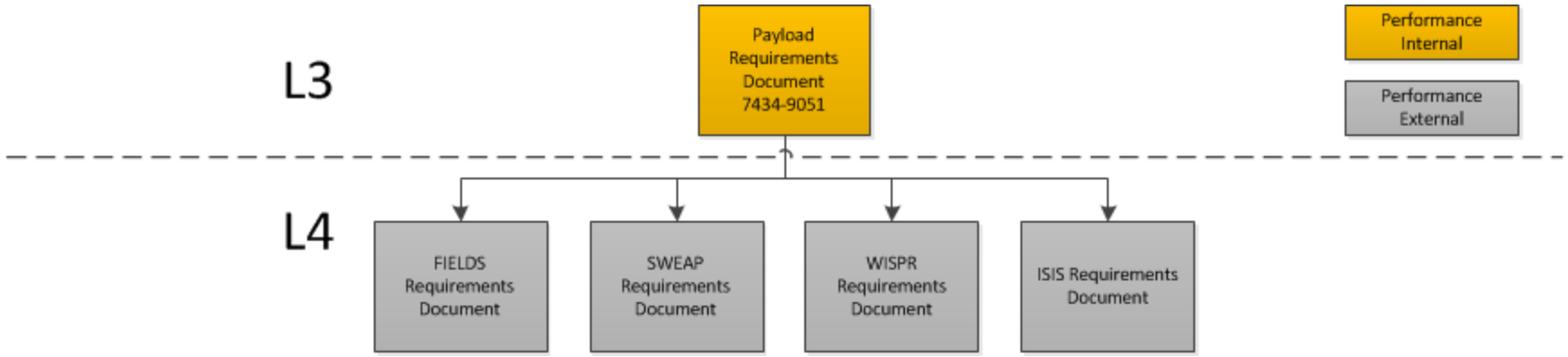


Source: Dan Kelly, 5/9/13

Level 3 – Payload (PAY)

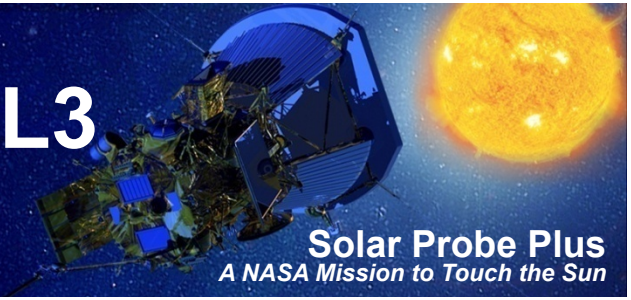


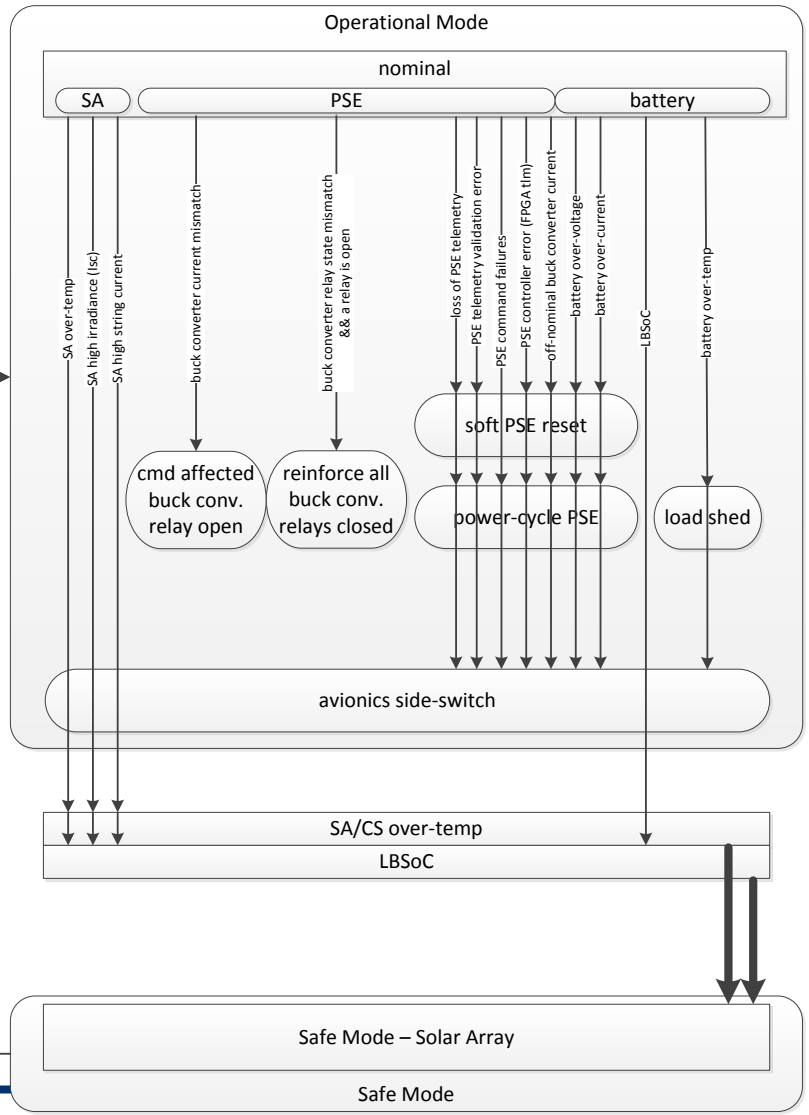
Solar Probe Plus
A NASA Mission to Touch the Sun



Source: Dan Kelly, 5/9/13

Electrical Power System FM – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

be designed to manage redundancy

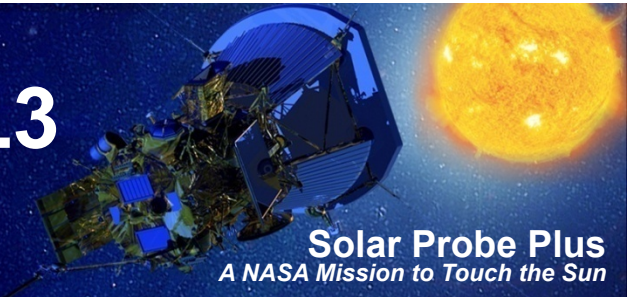
DETECTION OF CRITICAL FAULT CONDITIONS*

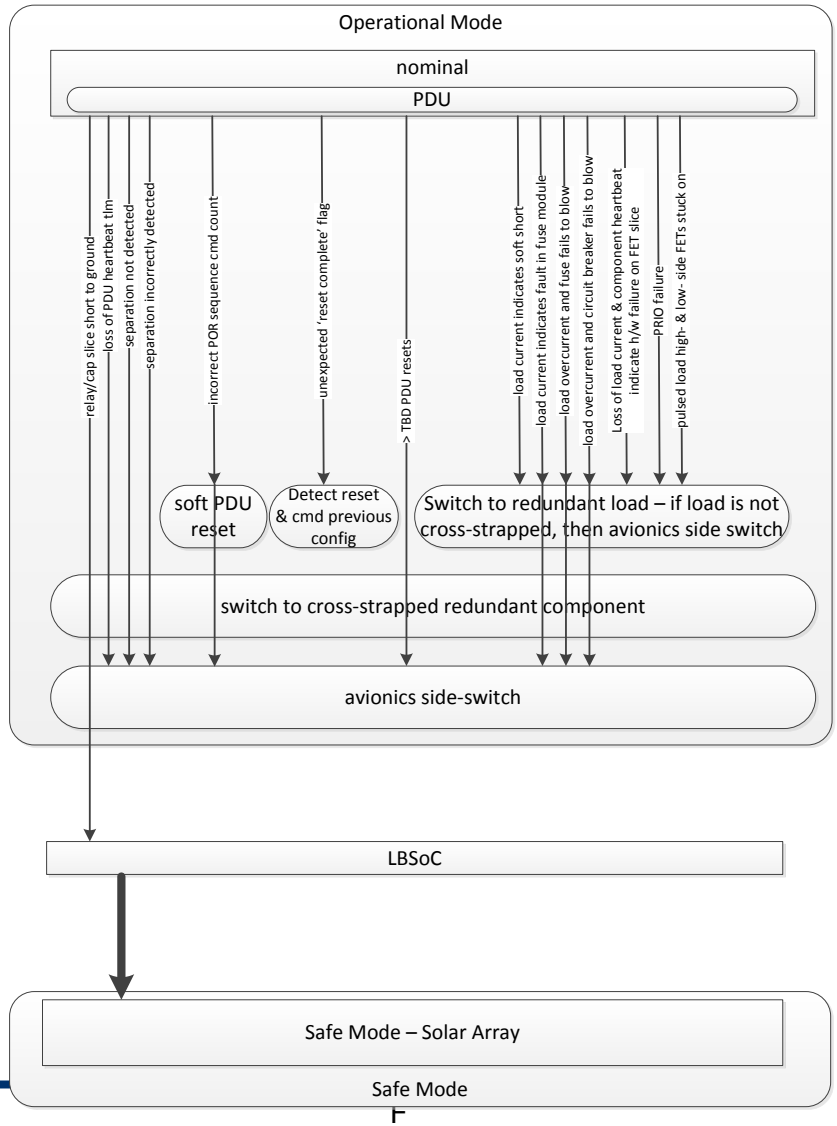
SAFING FOR CRITICAL FAULT CONDITIONS*

SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

Power Distribution Unit FM – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

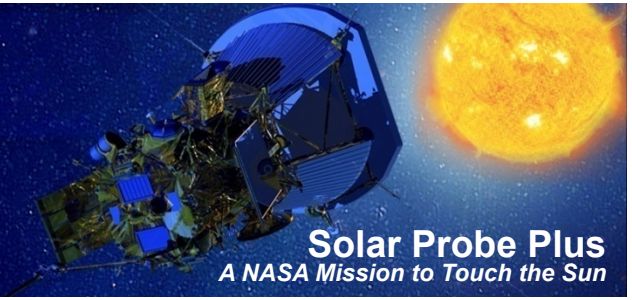
DETECTION OF CRITICAL FAULT CONDITIONS*

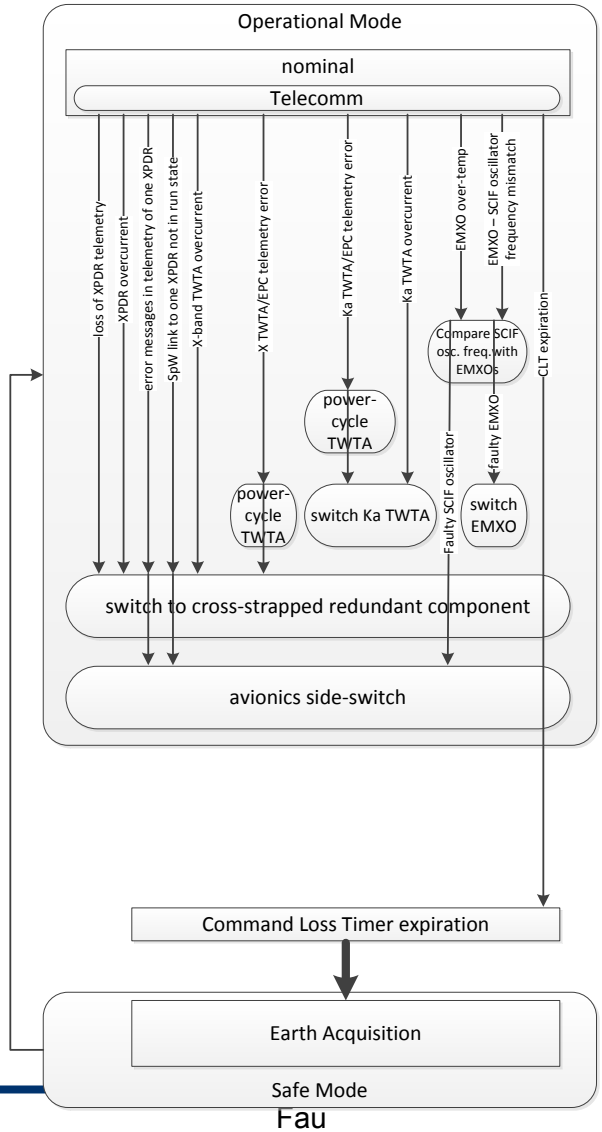
SAFING FOR CRITICAL FAULT CONDITIONS*

SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

Telecomm System FM – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

DETECTION OF CRITICAL FAULT CONDITIONS*

SAFING FOR CRITICAL FAULT CONDITIONS*

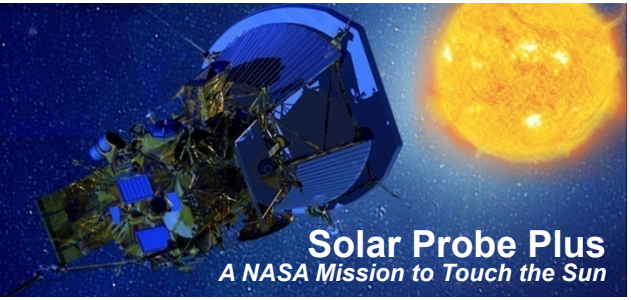
SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

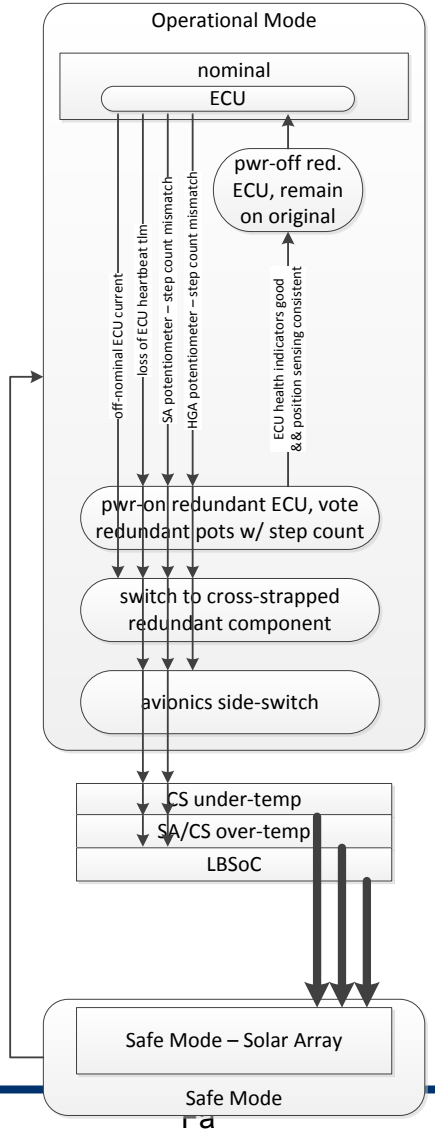
*discussed in detail in Safing Concept section

Fau

APL

ECU Fault Management – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

be capable of receiving telemetry from both redundant coarse potentiometers.

be capable of receiving telemetry from both redundant fine potentiometers.

cross-strap the transponders, pump controllers, ECUs, IMUs, star trackers, wheels, thrusters, SLS, processors, and instruments, to the redundant avionics interfaces.

be designed to manage redundancy

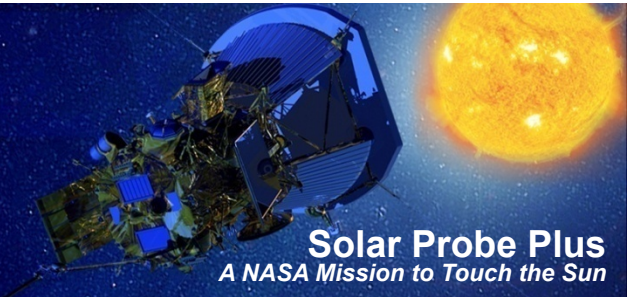
DETECTION OF CRITICAL FAULT CONDITIONS*

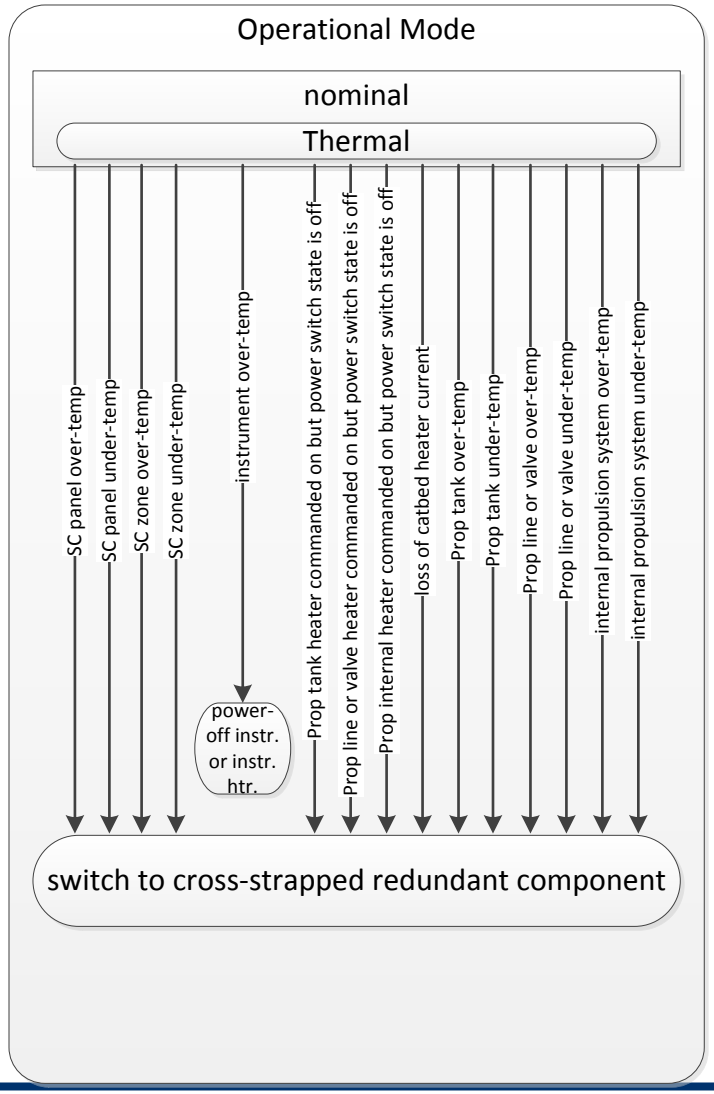
SAFING FOR CRITICAL FAULT CONDITIONS*

SAFE MODE RESPONSES*
RETURN TO OPERATIONAL*

*discussed in detail in Safing Concept section

Thermal System FM – L3 Requirements Mapping





The Spacecraft shall ...

provide an on-board autonomous system to detect and respond to faults.

be designed to provide spacecraft telemetry to enable fault detection on-board.

be designed to manage redundancy