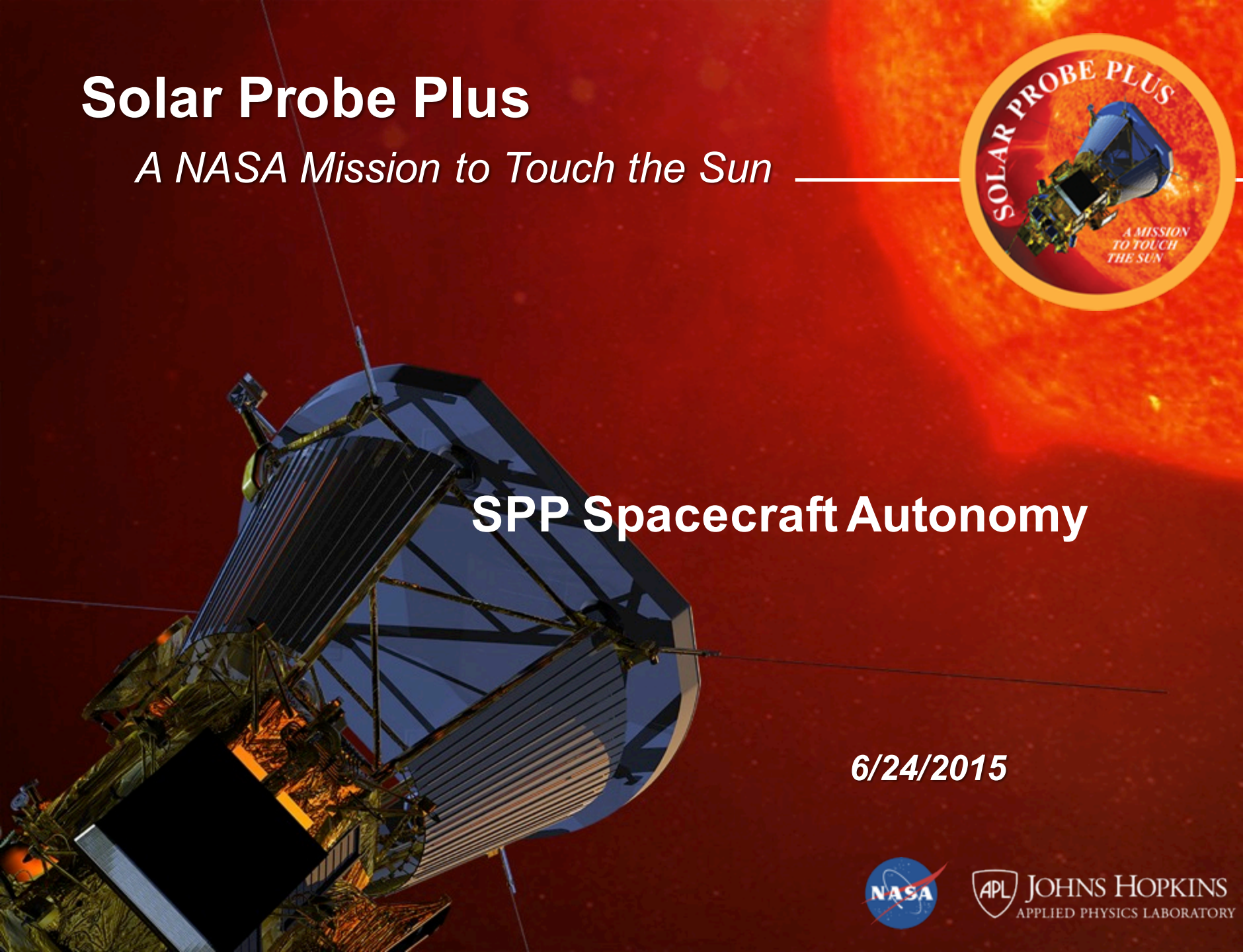
Solar Probe Plus

A NASA Mission to Touch the Sun



SPP Spacecraft Autonomy

6/24/2015

NASA

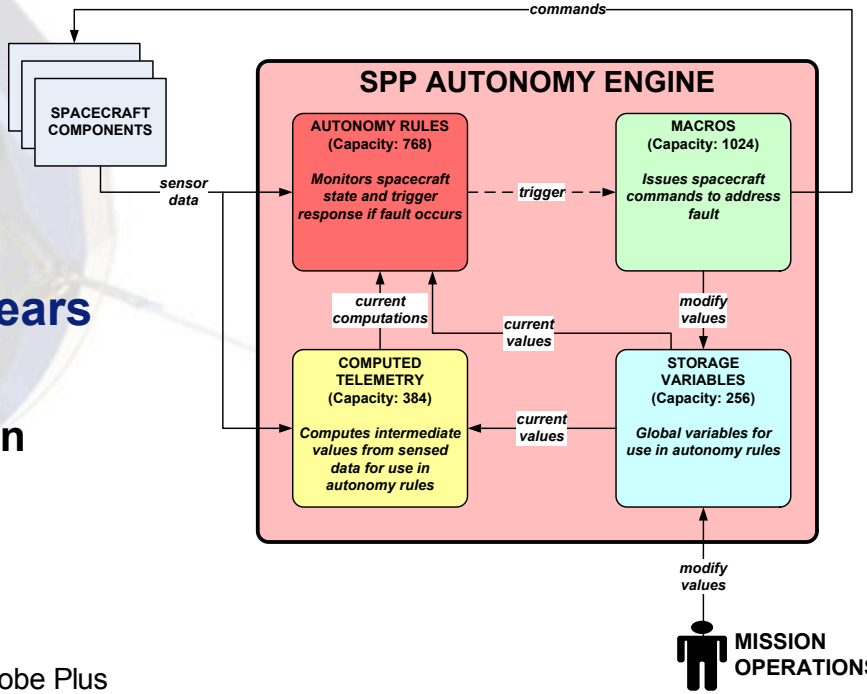
APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Spacecraft Autonomy Agenda

- Spacecraft Autonomy Overview
- Spacecraft Modes
- Instrument Autonomy Overview
  - EPI-Lo Instrument Autonomy
- Payload Autonomy Overview
- Instrument Heater Autonomy Overview
  - EPI-Lo Heater Autonomy

Spacecraft Autonomy System Overview

- The SPP Autonomy System is a Monitor→Response system where faults are detected and corrective actions are taken in response to the fault
  - All Monitors are evaluated at a 1 Hz rate
- The SPP C&DH Flight Software provides an on-board Autonomy Engine to facilitate the development of the Autonomy System. The Autonomy Engine supports four types of uploadable constructs that allow the Autonomy Engineer to independently develop the Autonomy System:
  - Autonomy Rules
  - Macros
  - Storage Variables
  - Computed Telemetry
- The Autonomy Engine has over 15 years of heritage.
  - Incremental enhancements have been made to the engine over the years



Spacecraft Autonomy System: Attributes Overview

- **Autonomy Rules**
  - Autonomy rules specify the fault condition to be monitored. The fault condition (*autonomy rule expression*) may be a combination of any engineering telemetry and common arithmetic and logical operators
    - Example expression: `( SC_MODE == OPERATIONAL ) && (BUS_VOLTAGE * BUS_CURRENT < 350.0)`
  - Rule Attributes
    - ***Persistence:*** How long a fault must persist *(M of N seconds)*
    - ***Maximum Fire Count:*** How many times an autonomy rule can fire
    - ***Priority:*** Priority of the autonomy rule's response macro when running concurrently with other macros
    - Initial State: Whether the autonomy rule is enabled or disabled by default
- **Macros**
  - Macros specify a list of spacecraft commands designed to address a fault. They are invoked in response to the firing of an autonomy rule.
  - Macros may call other macros (like invoking a subroutine). This allows a level of modularity to be applied to the macro design. Also, in the spirit of modularity, multiple autonomy rules may trigger the same macro

Spacecraft Autonomy System: Attributes Overview

- **Computed Telemetry**
  - Computed Telemetry allow intermediate calculations to be defined from engineering telemetry (*i.e., derived telemetry*). The calculation results can then be used in autonomy rule expressions. Like autonomy rules, the expressions may be a combination of any on-board telemetry and common arithmetic and logical operators
    - Example computed telemetry definition to calculate spacecraft power: `BUS_VOLTAGE * BUS_CURRENT`
    - The resulting calculation can now be used in other autonomy rules
- **Storage Variables**
  - Storage Variables are global variables for the exclusive use of the Autonomy System. The values of the storage variables are typically used in the premise of autonomy rules.
  - Commands are available to modify storage variables. Storage variables can be:
    - Set to specific value (Ex: `STOR_VAR_X = 13`)
    - Incremented and decremented (Ex: `INCREMENT STOR_VAR_X`)
    - Assigned to existing value of telemetry point (Ex: `STOR_VAR_X = BUS_CURRENT`)
  - Commands to modify storage variables are used in autonomy macros and by MOPS ground command

Instrument Autonomy Requirements & Documentation

- Autonomy requirements applicable to all teams are captured in the General Instrument ICD, 7434-9066, rev B
- Instrument specific requirements are captured in the ISIS to Spacecraft ICD, 7434-9058, rev B
- All autonomy requirements are captured in the SPP Level 4 Autonomy Systems Requirements Document, 7434-9072, rev A
  - Specific limits (current, temperature, power, etc.) are captured in a separate document known as the SPP Autonomy Engineering Limits Specification, 7434-9116
  - All spacecraft and instrument subsystems that own any limits in the Autonomy System will be approvers on the document

2 ENGINEERING LIMITS

2.1 EXCESS POWER CONSUMPTION MONITOR

The Autonomy System monitors the power consumption of selected spacecraft loads and takes a corrective action if the load power exceeds an engineering limit for a specified number of seconds (persistence). The engineering limits and persistences for each of the monitors is provided in Table 1. The table also includes the approximate resolution of power consumption reading (i.e., the engineering value that corresponds to one raw count). The corrective action is also included for reference.

Load	Power Consumption Limit (W, ±0%)	Persistence (Seconds)	Autonomous Corrective Action	Responsible Subsystem
Transceiver	6.40 (resolution: 0.2%)	10	Off Pulse Transceiver	RF
SSPA	38.20 (resolution: 0.8%)	10	Power off SSPA	RF
Battery Management Electronics (BME)	12.44 (resolution: 0.4%)	10	Disconnect from battery and power off BME	POS
PSE Interface Card (includes LSD)	16.52 (resolution: 0.4%)	10	Power off PSE Current Controller and PSE Interface Card	POS
REPT	8.00 (resolution: 0.2%)	10	Power off REPT	Payload
HOPE	27.50 (resolution: 0.5%)	10	Power off HOPE	Payload
EMFISIS Digital Electronics	13.32 (resolution: 0.4%)	10	Power off EMFISIS Analog and Digital Electronics	Payload
EMFISIS Analog Electronics	6.00 (resolution: 0.2%)	10	Power off EMFISIS Analog and Digital Electronics	Payload
EMFISIS Fluxgate Mag Heater	7.51 (resolution: 0.2%)	10	Power off EMFISIS Fluxgate Mag Heater	Payload
EFW	21.00 (resolution: 0.8%)	10	Terminate boom deployments and power off EFW	Payload
EFW Axial Boom Deployment Unit EFW Spin Plane Boom Deployment Unit	97.00 (resolution: 2.4%) See Note 1	10	Terminate EFW boom deployments	Payload
RBSPICE	2.69 (resolution: 0.1%)	10	Power off RBSPICE	Payload

DWG NO	SIZE	DRAWING NO	REV
88898	A	7417-9169	-

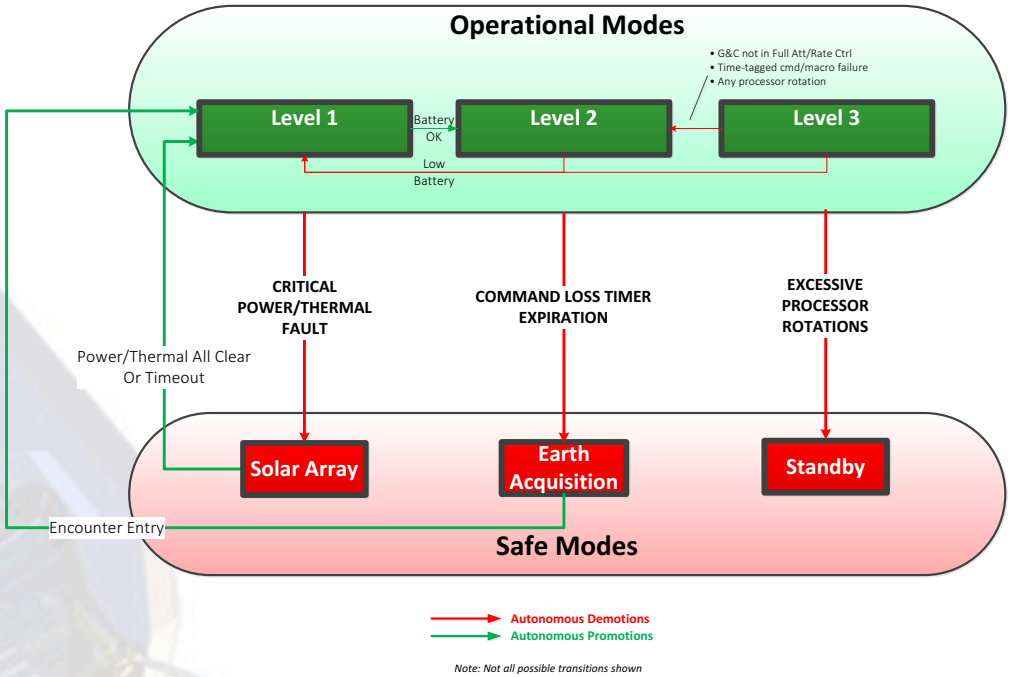
SCALE: NONE — DO NOT SCALE PRINT — SHEET 7 OF 13

Released 01/30/2012 09:27 Rev - UNCONTROLLED OUTSIDE OF PLM

Example from Van Allen Probes

Spacecraft Modes

- There are six main spacecraft modes:
  - Operational Mode – Level 3
  - Operational Mode – Level 2
  - Operational Mode – Level 1
  - Safe Mode – Solar Array
  - Safe Mode – Earth Acquisition
  - Safe Mode - Standby
- SPP allows both autonomous mode demotions and promotions
- The intent of this overview is to provide simple definitions for the spacecraft modes since some autonomy rules are contingent upon mode



Operational Modes

- **There are three Spacecraft Operational Modes**
  - ***Operational Mode - Level 3***: **Highest mode of operation. All spacecraft operations allowed. Full science achievable.**
  - ***Operational Mode - Level 2***: **Demotion to this mode if G&C indicates less than full attitude and rate control, there is a command failure in a MOPS time-tagged sequence or there is a processor rotation. MOPS time-tagged sequences inhibited in this mode. Autonomy ensures full science still achievable (e.g., powering on instruments inside of 0.25 AU). TCMs, G&C Off Pointing and HGA downlink are not allowed.**
  - ***Operational Mode - Level 1***: **Demotion to this mode if there is a low battery state of charge. Instruments are powered off. Science not achievable.**
    - **Autonomous promotion to *Operational Mode - Level 2* once battery state of charge is nominal (science operations would then resume)**

Safe Modes

- **There are three Spacecraft Safe Modes**
  - ***Safe Mode – Solar Array***: **Demotion to this mode for critical power/thermal fault. Instruments are powered off. Science not achievable in this mode.**
    - **Autonomous promotion to *Operational Mode - Level 1* when power/thermal fault has cleared (or 10 minutes have elapsed). If battery state of charge returns to nominal levels, promotion would continue to *Operational Mode – Level 2* (science operations would then resume)**
  - ***Safe Mode – Earth Acquisition***: **Demotion to this mode if Command Loss Timer expires outside of 0.25 AU. Instruments are powered off. Science not achievable in this mode.**
    - **Autonomous promotion to *Operational Mode - Level 1* if spacecraft crosses 0.25 AU inbound while in this mode. If battery state of charge is nominal promotion would continue to *Operational Mode – Level 2* (science operations would then initiate)**
  - ***Safe Mode – Standby***: **Demotion to this mode if there are excessive processor rotations. Instruments are powered off. Science is not achievable in this mode.**
    - **No avenue to autonomously promote from this mode**

Spacecraft Mode Capabilities

Spacecraft Modes	SPP Spacecraft Modes Capability						
	Autonony Initiated Processor Rotations	X-band Downlink	Instrument Ops	Time-tags Cmds	Ka Band (HGA) Downlink	ΔV Maneuvers	G &C Off-Pointing
Operational Mode - Level 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Operational Mode - Level 2	Yes	Yes	Yes	No	No	No	No
Operational Mode - Level 1	Yes	No	No	No	No	No	No
Safe Mode - Solar Array	Yes	No	No	No	No	No	No
Safe Mode - Earth Acquisition	Yes	Yes	No	No	No	No	No
Safe Mode - Standby	No	Yes	No	No	No	No	No

Instrument Autonomy Overview

- **The Spacecraft Autonomy System provides overarching protection which can either:**
  - **Power On an instrument**
  - **Power Off an instrument**
  - **Power Cycle an instrument**
    - **i.e., power instrument off for predefined number of seconds and then power it back on**
- **Each instrument has its own internal safing**
  - **Discussed in following presentations**

Design Overview (1 of 3)

- **Each instrument sends Interface Transfer Frames (ITFs) to the Prime CDH at a 1 Hz (or higher) rate.**
  - **Each ITF contains an 8-bit sequence counter that is incremented by the instrument. The Prime CDH Flight Software monitors the sequence counter and declares a failed aliveness if the sequence counter fails to increment or if the ITFs are not valid.**
    - **This provides a mechanism for the Autonomy System to monitor instrument aliveness.**
  - **Each ITF also contains a pair of bits so that each instrument can self-request a power off or power cycle of the instrument.**
    - **A power off request trumps a power cycle request if both bits are asserted.**
- **Autonomy can send an individual instrument a shutdown warning prior to removing power from the instrument**
  - **In general, Autonomy will provide an instrument a 60-second shutdown warning if the power-down is not urgent**

Design Overview (2 of 3)

- **For each instrument the Autonomy System provides the following protection:**
  - ***Self-Power Down Request:*** **Power off an instrument that requests it**
  - ***Self-Power Cycle Request:*** **Power cycle an instrument that requests it**
  - ***Instrument Stale Aliveness:*** **Power off an instrument whose aliveness fails**
  - ***Instrument Excessive Power Consumption:*** **Power off an instrument if its power consumption exceeds limits**
  - ***Instrument LVDS Over-Voltage:*** **Power off an instrument if it applies LVDS over-voltage**

Design Overview (3 of 3)

- **Because of the mission criticality of keeping the instruments operating, the Autonomy System includes provisions for powering on instruments in Operational Mode – Level 2 or 3.**
  - **Instruments are powered on at 0.25 AU Inbound**
  - **"Second-chance" power-on after specific power-downs**
- **The Second-chance power-on in Operational Mode – Level 2 or 3 is selectively performed based on solar distance and based on the manner in which the instrument had been powered down.**

		SECOND CHANCE INSTRUMENT POWER-ON	
		Inside 0.25 AU	***Outside 0.25 AU***
Instrument Power-Down Cause	*Stale Aliveness*	POWER BACK ON ONCE	POWER BACK ON ONCE
	Excess Power	POWER BACK ON ONCE	POWER BACK ON ONCE
	LVDS Over-Voltage	POWER BACK ON ONCE	POWER BACK ON ONCE
	Power-Down Request	LEAVE POWERED OFF	LEAVE POWERED OFF
	Circuit Breaker Trip	LEAVE POWERED OFF	LEAVE POWERED OFF
	MOPS Command	LEAVE POWERED OFF	LEAVE POWERED OFF
	S/C Mode Demotion	POWER BACK ON ONCE †	LEAVE POWERED OFF
		† - *upon promotion to Op Level 2*	

ISIS EPI-Lo Requirements

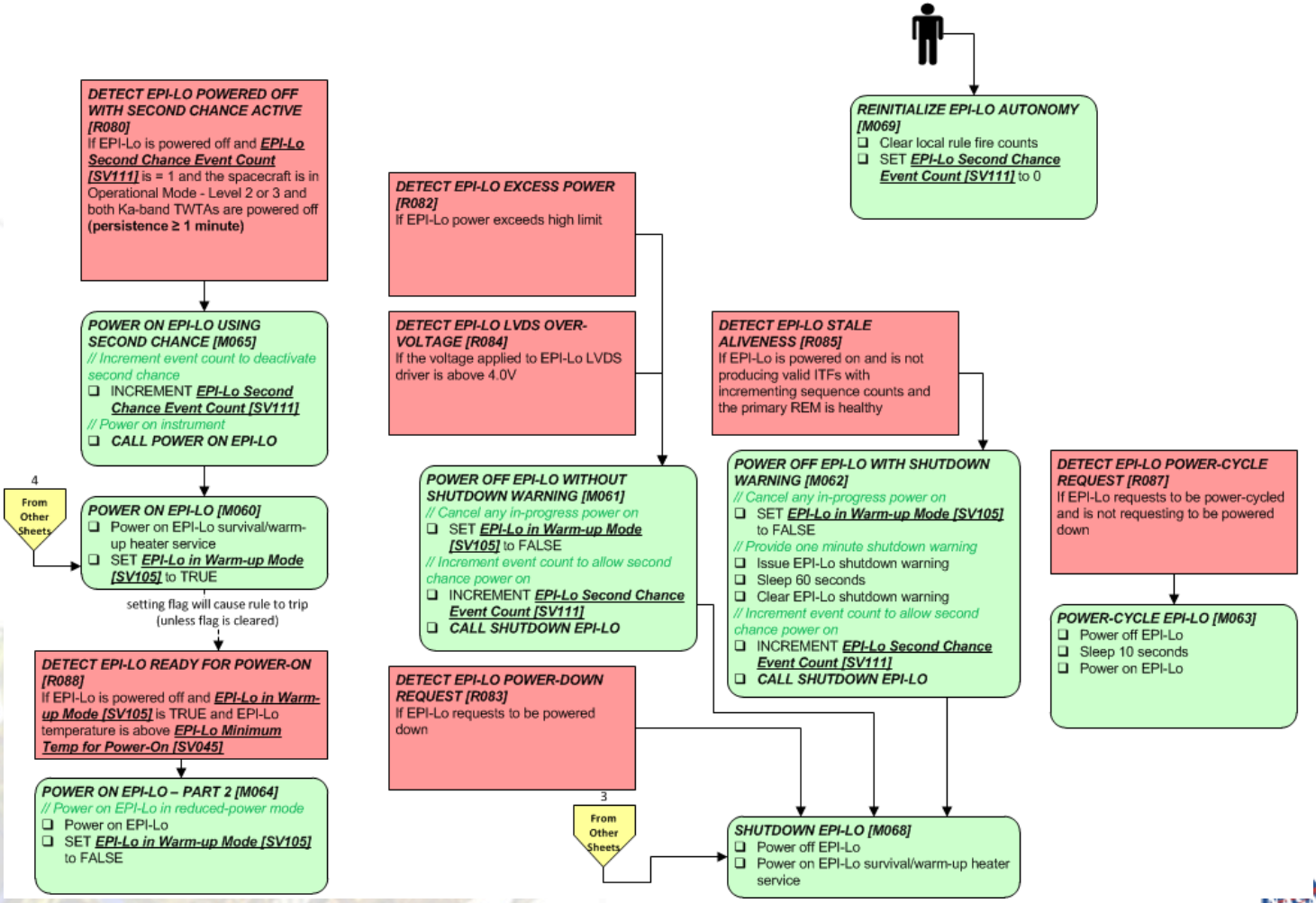
AUT-21	Autonomy shall power off the EPI-Lo instrument if it is powered on and its flight software is not producing valid ITFs with incrementing sequence counts.
AUT-29	Autonomy shall power off the EPI-Lo instrument if the instrument requests to be powered down.
AUT-36	Autonomy shall power cycle the EPI-Lo instrument if the instrument requests to be power-cycled and is not simultaneously requesting to be powered down.
AUT-43	Autonomy shall power off the EPI-Lo instrument if its power consumption is above a pre-defined limit.
~~AUT-210~~	~~Autonomy shall power off the EPI-Lo instrument if its temperature is above a pre-defined limit.~~
AUT-337	Autonomy shall power off the EPI-Lo instrument if the voltage applied to an LVDS device is above 4.0V
AUT-467	Autonomy shall power on the EPI-Lo instrument when the spacecraft transitions inside 0.25 AU of the Sun (inbound) if the instrument is powered off and the spacecraft is in Operational Mode - Level 2 or Operational Mode - Level 3.
AUT-655	Autonomy shall provide the capability to autonomously restore power to the EPI-Lo instrument if was powered off due to a fault and its temperature is below a pre-defined value and the spacecraft is in Operational Mode - Level 2 or Operational Mode - Level 3.
AUT-171	Autonomy shall provide an EPI-Lo power-on macro that performs the following actions: * Power on the EPI-Lo survival/warm-up heaters * Indicate that EPI-Lo is being warmed-up for power-on * Wait until EPI-Lo's temperature is above a programmable low limit for power-on * Power on EPI-Lo * Indicate that EPI-Lo is no longer being warmed-up for power-on

EPI-Lo Power-On Sequence

- **Before powering on EPI-Lo, the instrument must be warmed up using its survival/warm-up heaters to a temperature suitable for power-on**
- **The Autonomy System provides a macro that can be used by Mission Operations and Autonomy to perform the EPI-Lo power-on sequence**
  - **Power on the EPI-Lo survival/warm-up heaters**
  - **Wait until EPI-Lo's temperature is suitable for power-on**
  - **Power on EPI-Lo (into reduced-power mode)**
  - **Wait for EPI-Lo to promote itself into full-power mode**
  - **Power off the EPI-Lo survival/warm-up heaters**

EPI-Lo Design

Instrument - *ISIS EPI-Lo* | **Sheet 10 of 95**



JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Payload Design Overview

- **Autonomy powers down the entire payload with shutdown warnings when configuring for the following spacecraft modes**
  - **Operational Mode – Level 2 (outside 0.25 AU)**
  - **Operational Mode – Level 1**
  - **Safe Mode – Standby**
  - **Safe Mode – Earth Acquisition**
  - **Safe Mode – Standby + Earth Acquisition**
- **Autonomy powers down the entire payload without shutdown warnings when**
  - **an instrument is powered on outside 0.25 AU while Ka-band TWTA is on**
- **Autonomy powers on the entire payload when configuring for the following spacecraft modes**
  - **Operational Mode – Level 3 (inside 0.25 AU)**
  - **Operational Mode – Level 2 (inside 0.25 AU)**
- ***Note: Flight Software will directly shutdown payload without warning on a demotion into Safe Mode – Solar Array***

Payload Design (1 of 2)

Instrument Payload - *Shutdown*

Sheet 3 of 95

DETECT 0.25 AU INBOUND CROSSING [R010]
If solar distance is ≤ 0.25 AU and the previous solar distance is > 0.25 AU

DETECT 0.25 AU OUTBOUND CROSSING [R011]
If solar distance is > 0.25 AU and the previous solar distance is ≤ 0.25 AU

75 76 77 78 79 From Other Sheets

PREPARE INSTRUMENTS FOR ENCOUNTER [M004]
// Set all instrument startup mode bits to Full Science
- ❑ Set WISPR Startup Mode to 'Full Science'
- ❑ Set FIELDS-1 Startup Mode to 'Full Science'
- ❑ Set FIELDS-2 Startup Mode to 'Full Science'
- ❑ Set SWEAP Startup Mode to 'Full Science'
- ❑ Set SWEAP Boot Mode Indicator to 'Promote to Operational Mode'
- ❑ Set EPI-Hi Startup Mode to 'Full Science'
- ❑ Set EPI-Lo Startup Mode to 'Full Science'

// Reinitialize all instrument second chance rules
- ❑ ***CALL CLEAR INSTRUMENT SECOND CHANCE EVENT COUNTS***

SHUTDOWN PAYLOAD WITH WARNINGS [M005]
// Only take the time to perform these operations if any instrument is powered on or being warmed up for power on
- ❑ IF any instrument is powered on OR ***EPI-Hi in Warm-up Mode [SV104]*** is TRUE OR is ***EPI-Lo in Warm-up Mode [SV105]*** is TRUE
  - *// Issue shutdown warnings to all instruments (whether powered or not)*
  - ❑ Issue WISPR shutdown warning
  - ❑ Issue FIELDS-1 shutdown warning
  - ❑ Issue FIELDS-2 shutdown warning
  - ❑ Issue SWEAP shutdown warning
  - ❑ Issue EPI-Hi shutdown warning
  - ❑ Issue EPI-Lo shutdown warning
  - *// Perform a single 60 second wait to allow all instruments to shutdown concurrently*
  - ❑ Sleep 60 seconds
  - *// Power off each instrument using "immediate" shutdown routines now that 60 second wait has been honored*
  - ❑ ***CALL SHUTDOWN PAYLOAD WITHOUT WARNINGS***
  - *// Clear shutdown warnings*
  - ❑ Clear WISPR shutdown warning
  - ❑ Clear FIELDS-1 shutdown warning
  - ❑ Clear FIELDS-2 shutdown warning
  - ❑ Clear SWEAP shutdown warning
  - ❑ Clear EPI-Hi shutdown warning
  - ❑ Clear EPI-Lo shutdown warning
- ❑ ENDIF

CLEAR INSTRUMENT SECOND CHANCE EVENT COUNTS [M008]
// Reinitialize all instrument second chance rules
- ❑ SET ***WISPR Second Chance Event Count [SV106]*** to 0
- ❑ SET ***FIELDS-1 Second Chance Event Count [SV107]*** to 0
- ❑ SET ***FIELDS-2 Second Chance Event Count [SV108]*** to 0
- ❑ SET ***SWEAP Second Chance Event Count [SV109]*** to 0
- ❑ SET ***EPI-Hi Second Chance Event Count [SV110]*** to 0
- ❑ SET ***EPI-Lo Second Chance Event Count [SV111]*** to 0

59 85 From Other Sheets

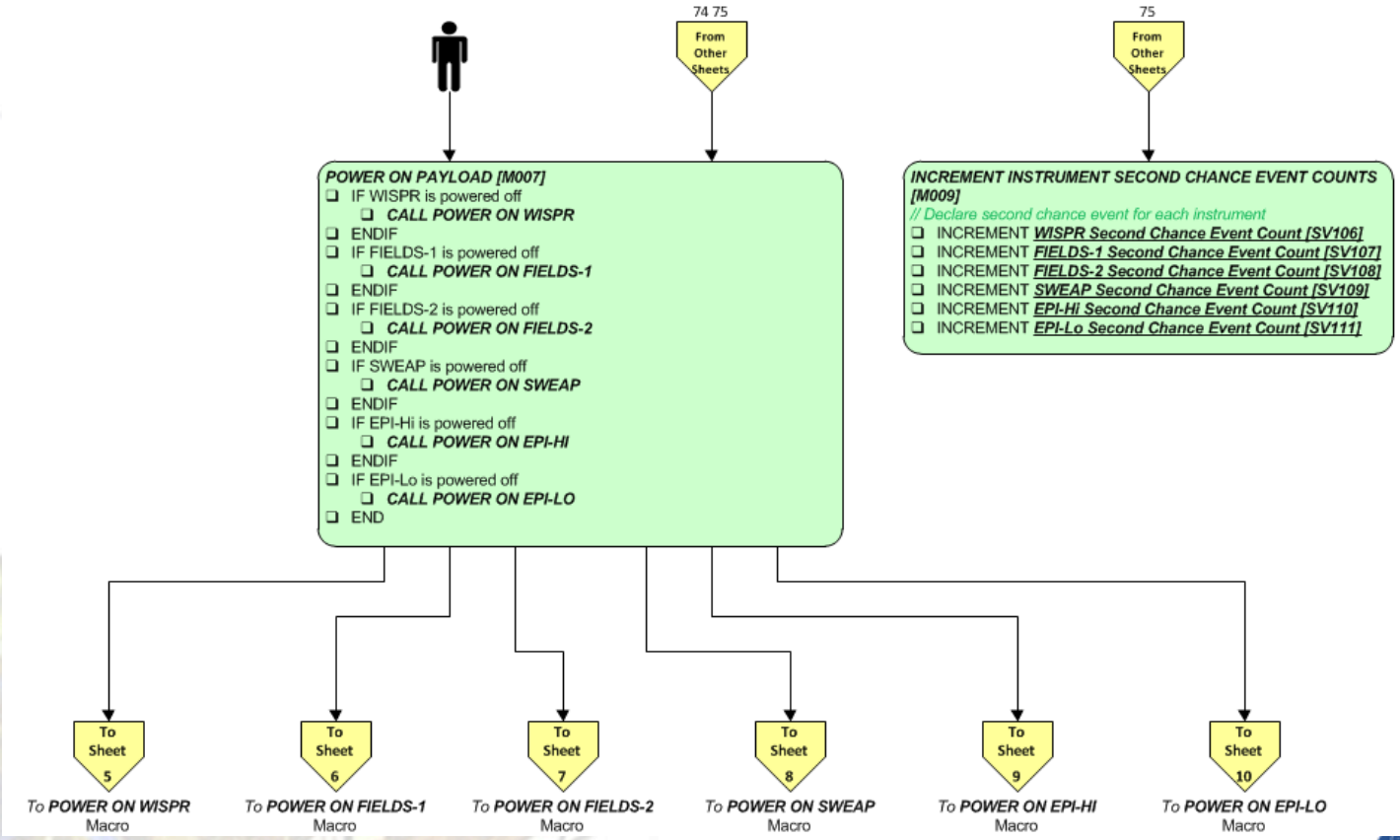
SHUTDOWN PAYLOAD WITHOUT WARNINGS [M006]
- ❑ ***CALL SHUTDOWN WISPR***
- ❑ ***CALL SHUTDOWN FIELDS-1***
- ❑ ***CALL SHUTDOWN FIELDS-2***
- ❑ ***CALL SHUTDOWN SWEAP***
- ❑ ***CALL SHUTDOWN EPI-HI***
- ❑ ***CALL SHUTDOWN EPI-LO***

To Sheet 5 — *To **SHUTDOWN WISPR** Macro*
To Sheet 6 — *To **SHUTDOWN FIELDS-1** Macro*
To Sheet 7 — *To **SHUTDOWN FIELDS-2** Macro*
To Sheet 8 — *To **SHUTDOWN SWEAP** Macro*
To Sheet 9 — *To **SHUTDOWN EPI-HI** Macro*
To Sheet 10 — *To **SHUTDOWN EPI-LO** Macro*

Payload Design (2 of 2)

Instrument Payload – *Power On*

Sheet 4 of 95



Instrument Heaters Overview

- **Instrument heaters are single string**
- **EPI-Lo survival and warm-up heaters are software controlled**
  - **EPI-Lo does not have operational heaters**
- **Autonomy also enforces instrument heater ground rules (individually negotiated with each instrument team)**
  - **Instrument heater over-conductance rules eliminated post-Autonomy CDR with agreement from all instrument teams**

Instrument Heater Service	INSTRUMENT ON		INSTRUMENT OFF	
	Inside 0.25 AU	Outside 0.25 AU	Inside 0.25 AU	Outside 0.25 AU
FIELDS 1 Op & Survival Heaters	ON ►►►			
FIELDS 2 Op & Survival Heaters	ON ►►►			
WISPR Survival Heaters	ON ►►►			
SWEAP SPAN A+ & B Survival Heaters	OFF	ON ►►►		
SWEAP SPC Survival Heater	OFF	ON	OFF	ON
ISIS EPI-Hi Survival and Warm-up Heaters	OFF ►►►		{Autonomy Thermostat}	
ISIS EPI-Lo Survival and Warm-up Heaters	OFF ►►►		{Autonomy Thermostat}	
ISIS EPI-Hi Operational Heaters	ON ►►►		OFF ►►►	
WISPR Operational Heaters	ON ►►►		OFF ►►►	

Instrument Heater Requirements

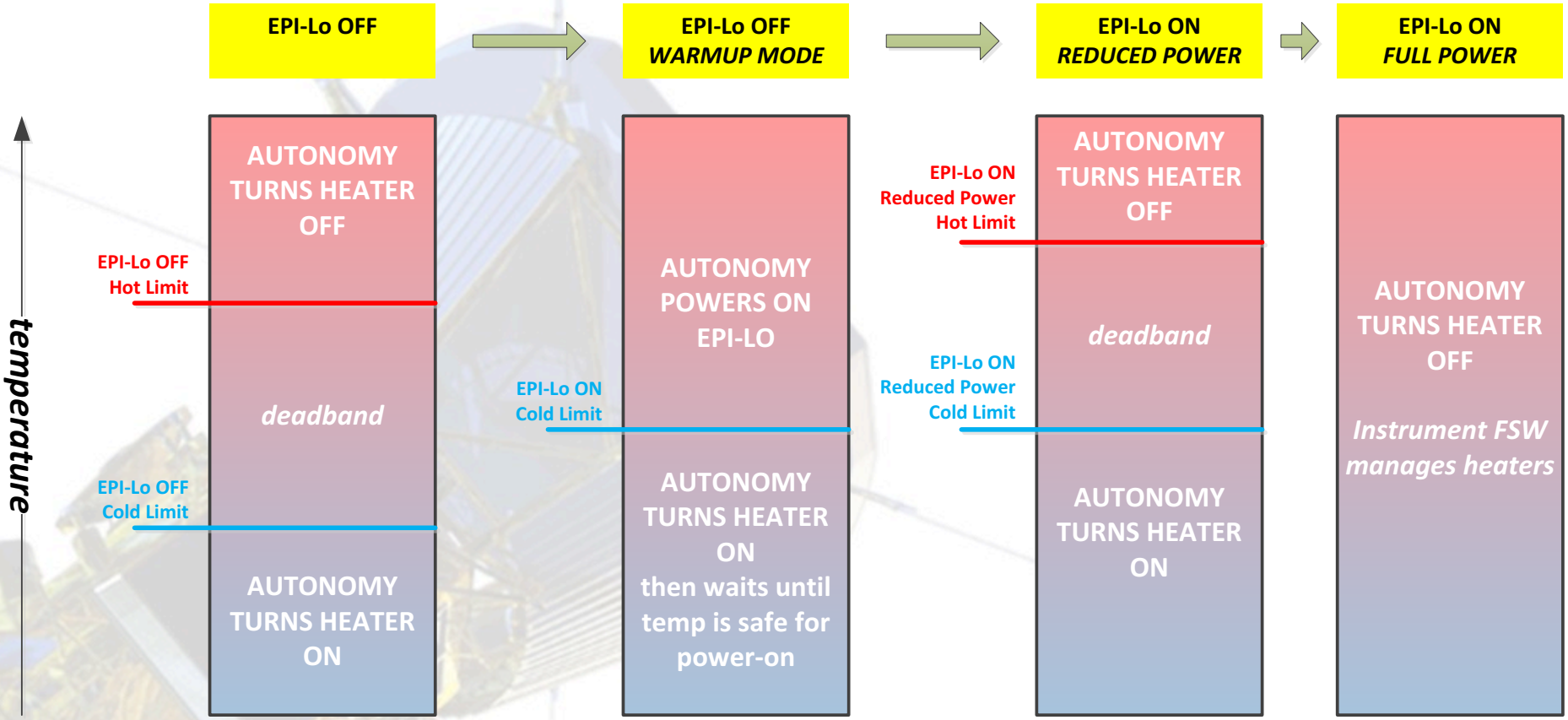
AUT-169	Autonomy shall power on the EPI-Lo survival/warm-up heaters if the heaters are powered off and any of the following conditions are true: 1. EPI-Lo is powered off and EPI-Lo's temperature is below a programmable powered-off low limit -OR- 2. EPI-Lo is powered on in reduced-power mode and its temperature is below a programmable reduced-power/warm-up low limit
AUT-170	Autonomy shall power off the EPI-Lo survival/warm-up heaters if the heaters are powered on and any of the following conditions are true: 1. EPI-Lo is powered off and is not being warmed-up for power-on and its temperature is above a programmable powered-off high limit -OR- 2. EPI-Lo is powered on in reduced-power mode and its temperature is above a programmable reduced-power high limit -OR- 3. EPI-Lo is powered on in full-power mode

EPI-Lo Heater Power-On Sequence Details

- **EPI-Lo (*differences from EPI-Hi shown in purple*)**
  - **When the instrument is off Autonomy operates the survival/warm-up heater service as a "software thermostat" between two programmable thresholds**
  - **When the instrument is in Warm-up mode, Autonomy turns the heaters on and drives up the temperature**
  - **Autonomy then waits until the instrument's temperature is safe for power-on before applying power to the instrument**
    - ***When the instrument is powered it will start in Low Power mode***
  - ***Autonomy will continue to operate the survival/warm-up heater as a "software thermostat" between two different programmable thresholds while the instrument is in Low Power Mode***
    - ***The instrument will autonomously transition itself into Full Power Mode***
  - **When the instrument is powered *in Full Power Mode*, Autonomy powers off the survival/warm-up heaters (instrument's FSW will manage internal heaters)**
  - ***Note: Although the EPI-Lo survival/warm-up heater service includes a thermostat, it is only used only as a backup mechanism to mitigate a PDU failure. The primary temperature control is via Autonomy.***

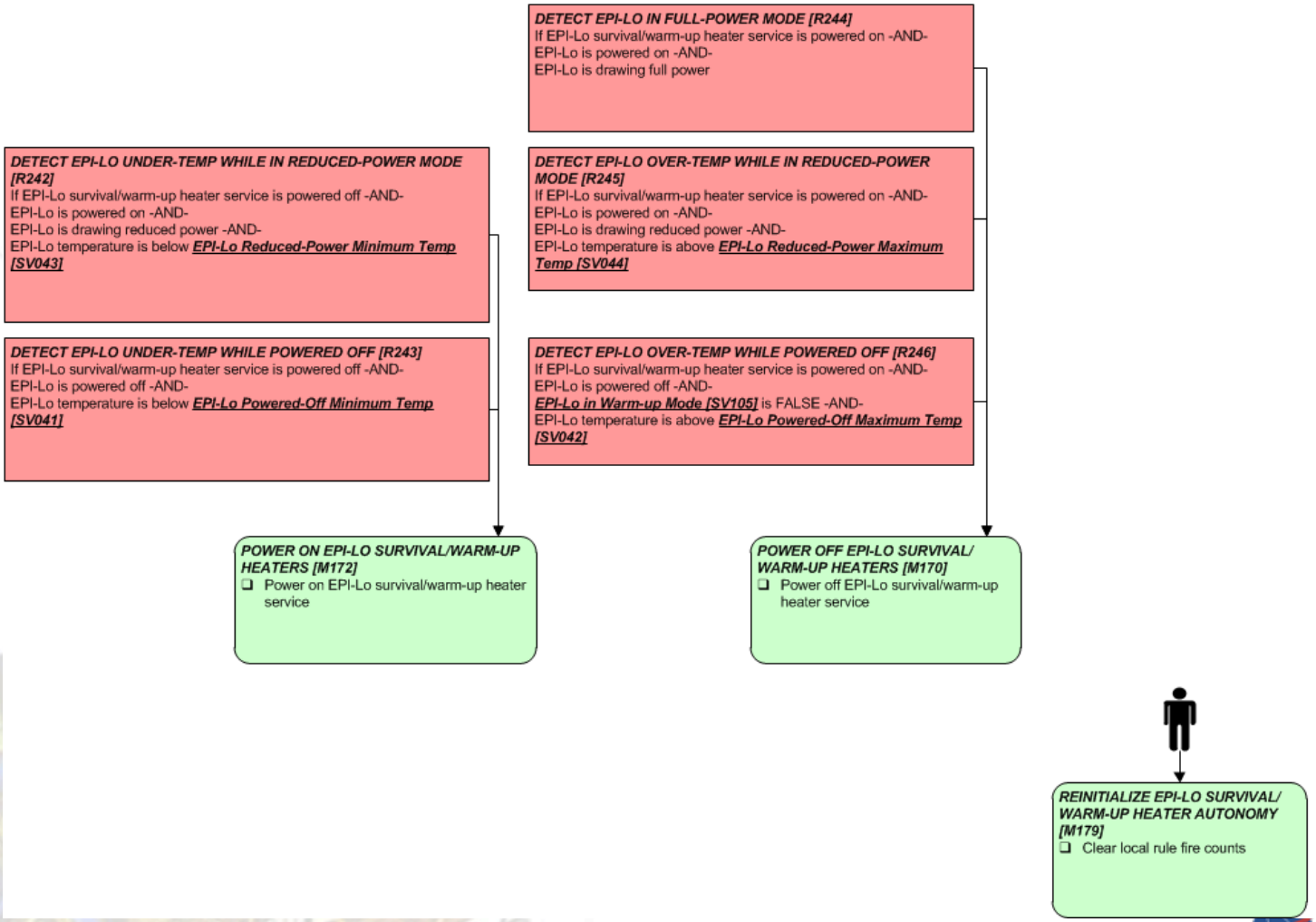
EPI-Lo Power-On Sequence Diagram

EPI-Lo Power On Sequence



EPI-Lo Design

Instrument Heaters – *EPI-Lo Survival/Warm-up*



Summary

- **Instrument autonomy needs are well understood**
- **Spacecraft autonomy team is staffed and ready to start rule development**
- **Key Milestones:**
  - **June 2015 FSW Build 1 Delivered and Available**
    - **Includes Autonomy Engine and FSW interfaces to components**
    - **Autonomy implementation and testing can proceed in earnest**
  - **January 2016 FSW Build 2 Delivered and Available**
    - **Includes most planned FSW functionality**
    - **Autonomy implementation and testing continues**
  - **July 2016 FSW Build 3 Delivered and Available**
    - **Includes all planned FSW functionality**
  - **August 2016 Delivery of Autonomy System to Spacecraft I&T**
    - **Autonomy implementation and unit testing should be complete**
    - **Start of autonomy testing on spacecraft and high fidelity simulators**
    - **Fault Management testing begins on spacecraft and simulators**