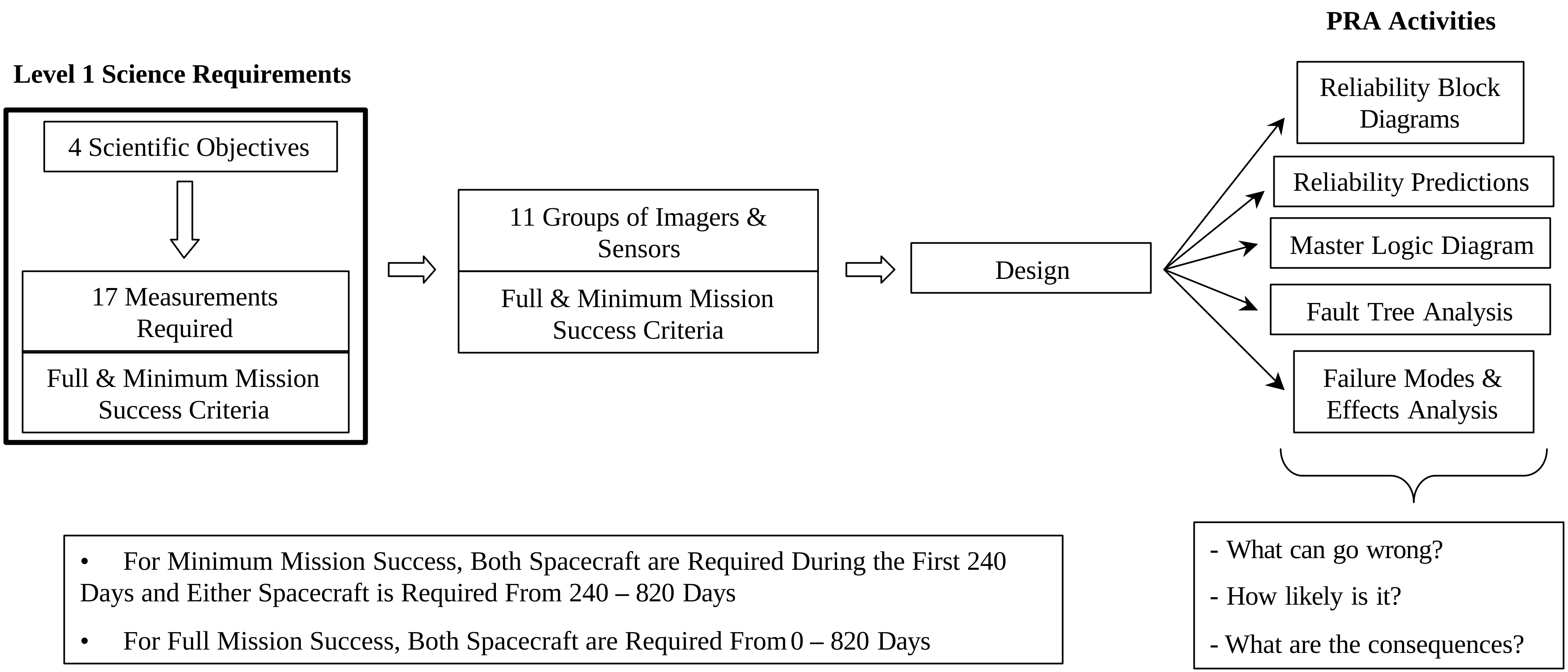
Probabilistic Risk Assessment (PRA)

Mathew Samuel
NASA/GSFC/MEI
(301) 286-6475
Mathew.V.Samuel.1@gsfc.nasa.gov

Mission Success Criteria & PRA Activities

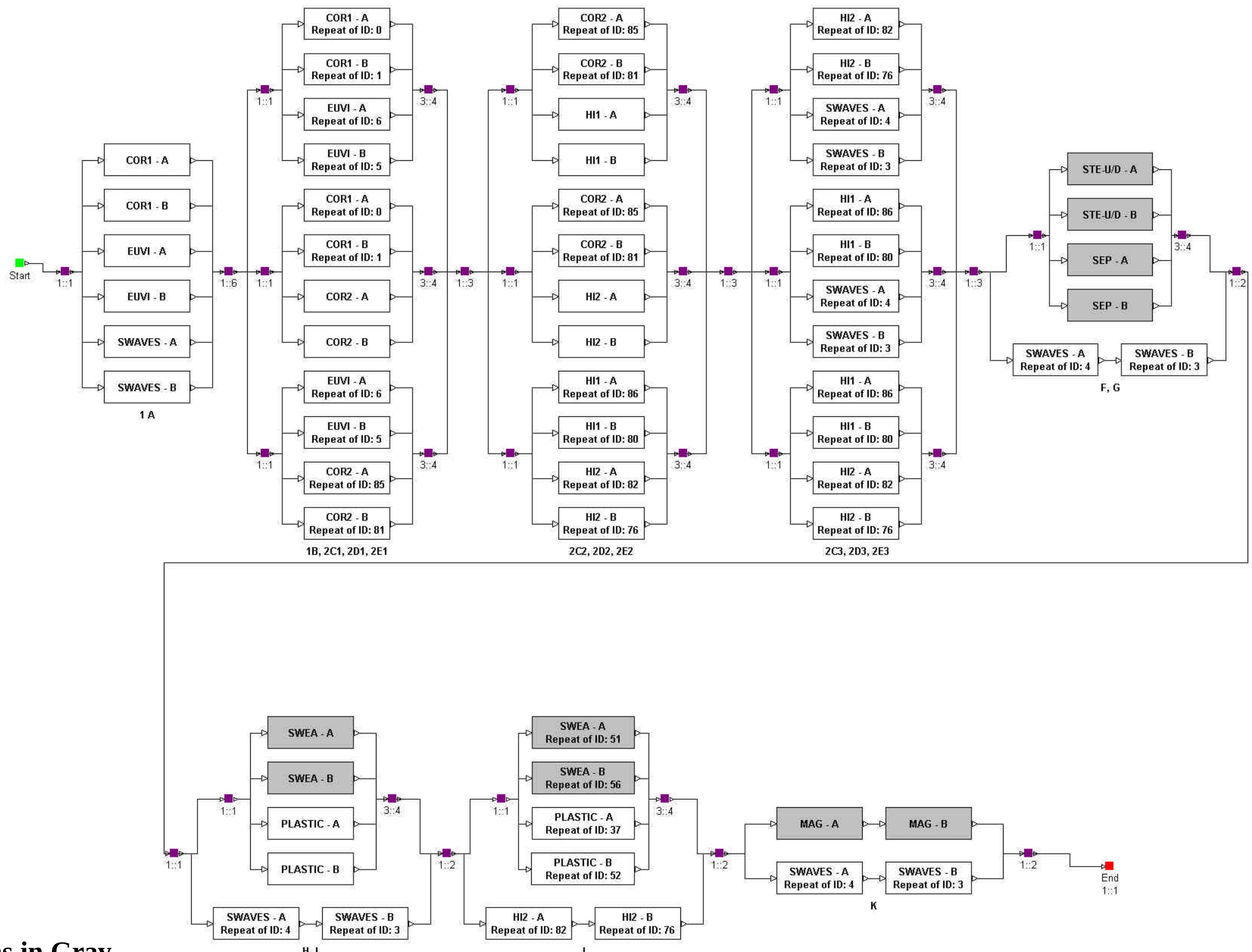


Level 1 Science Requirements

SCIENTIFIC OBJECTIVE		MEASUREMENT REQUIREMENT	
1	Understand the causes and mechanisms of CME initiation	A.	Determine the CME initiation time to an accuracy of order 10 minutes
		B.	Determine the location of CME initiation to within +/- 5 [15]degrees of solar latitude and longitude
2	Characterize the propagation of CMEs through the heliosphere	C1.	Determine the evolution of the CME mass distribution and the longitudinal extent to an accuracy of +/- 5 [15] degrees as it propagates in the low corona
		C2.	Determine the evolution of the CME mass distribution and the longitudinal extent to an accuracy of +/- 5 [15] degrees as it propagates in the upper corona
		C3.	Determine the evolution of the CME mass distribution and the longitudinal extent to an accuracy of +/- 5 [15] degrees as it propagates in the IPM.
		D1.	Determine the CME and MHD shock speeds accurate to +/- 10 [30]% as it propagates in the low corona
		D2.	Determine the CME and MHD shock speeds accurate to +/- 10 [30]% as it propagates in the upper corona
		D3.	Determine the CME and MHD shock speeds accurate to +/- 10 [30]% as it propagates in the IPM
		E1.	Determine the direction of CME and MHD shock propagation to within +/- 5 [15] degrees of latitude and longitude as the CME evolves in the low corona
		E2.	Determine the direction of CME and MHD shock propagation to within +/- 5 [15] degrees of latitude and longitude as the CME evolves in the upper corona
		E3.	Determine the direction of CME and MHD shock propagation to within +/- 5 [15] degrees of latitude and longitude as the CME evolves in the IPM
3	Discover the mechanisms and sites of energetic particle acceleration in the low corona and the interplanetary medium	F.	Develop distribution functions to an accuracy of ± 10% for electrons and/or ions with energies typical of solar energetic particle populations
		G.	Location of particle acceleration in the low corona to within 300,000 km [500,000 km] in radius and in interplanetary space to within 20 degrees [40 degrees] in total longitude
4	Develop a 3D time-dependent model of the magnetic topology, temperature, density, and velocity structure of the ambient solar wind	H.	Obtain a time series of the solar wind temperature accurate to +/- 30% at two points separated in solar longitude [at a single longitude]
		I.	Obtain a time series of the solar wind density accurate to +/- 30% at two points separated in solar longitude [at a single longitude]
		J.	Obtain a time series of the solar wind speed accurate to +/- 10% at two points separated in solar longitude [at a single longitude]
		K.	Determine the global magnetic field topology

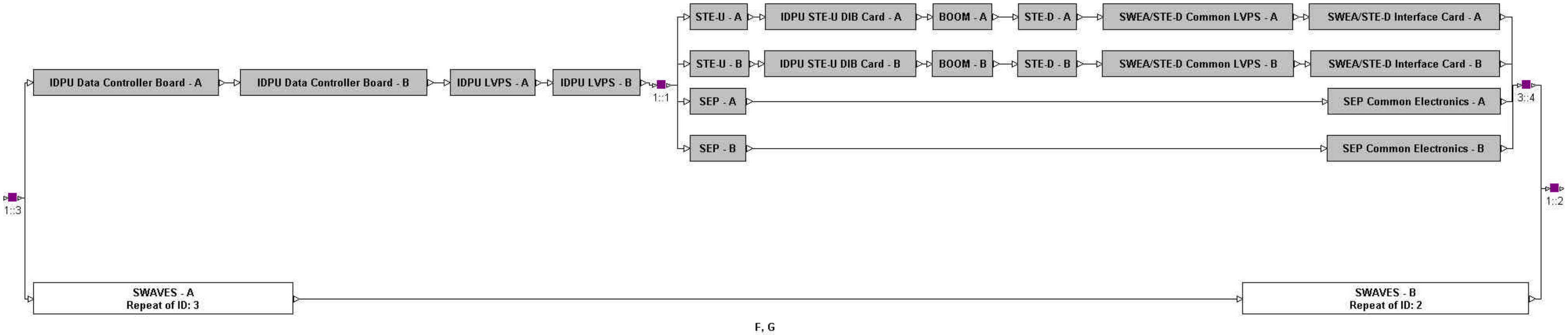
Full Mission (0-820 days)/Minimum Mission (0-240 days)

Reliability Block Diagram (RBD)



A – Ahead
B – Behind
IMPACT Items in Gray

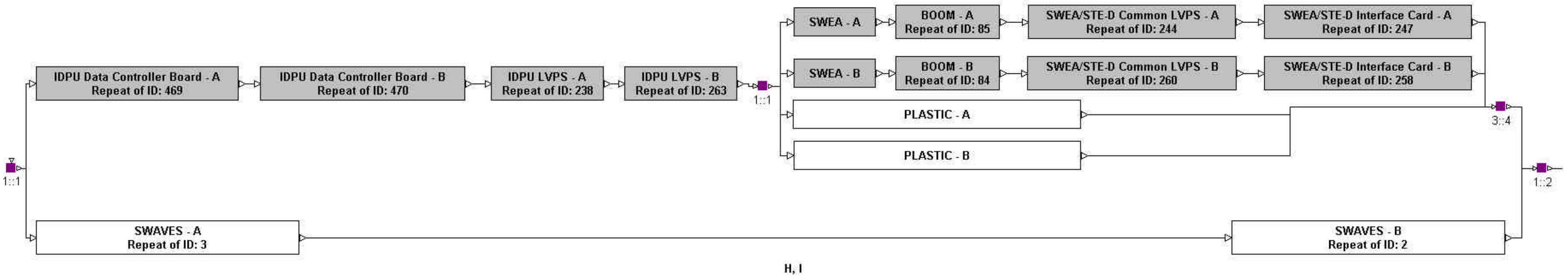
Full Mission (0-820 days)/Minimum Mission (0-240 days)
Measurements F, G



A – Ahead
B – Behind
IMPACT Items in Gray

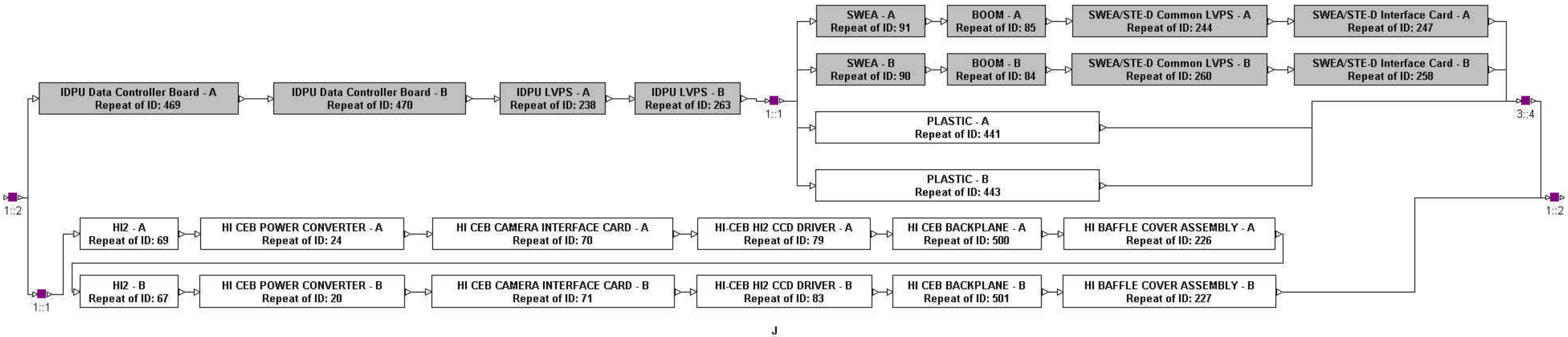
Full Mission (0-820 days)/Minimum Mission (0-240 days)

Measurements H, I



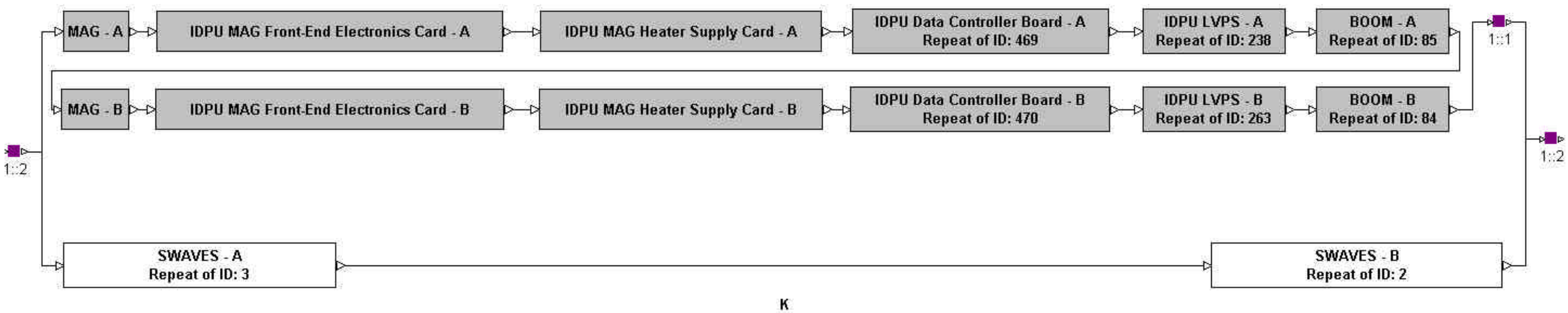
A – Ahead
B – Behind
IMPACT Items in Gray

Full Mission (0-820 days)/Minimum Mission (0-240 days)
Measurement J



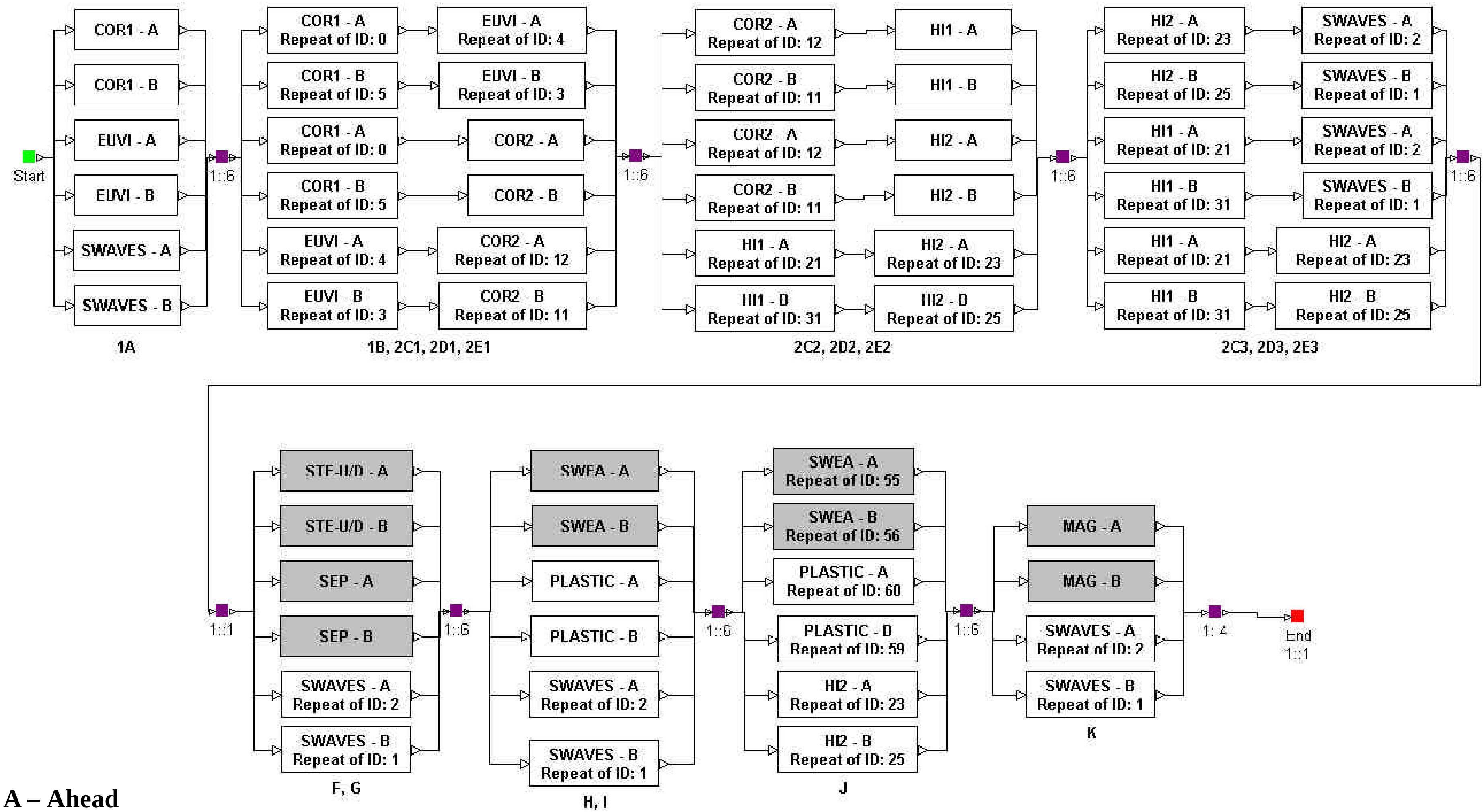
A – Ahead
B – Behind
IMPACT Items in Gray

Full Mission (0-820 days)/Minimum Mission (0-240 days)
Measurement K



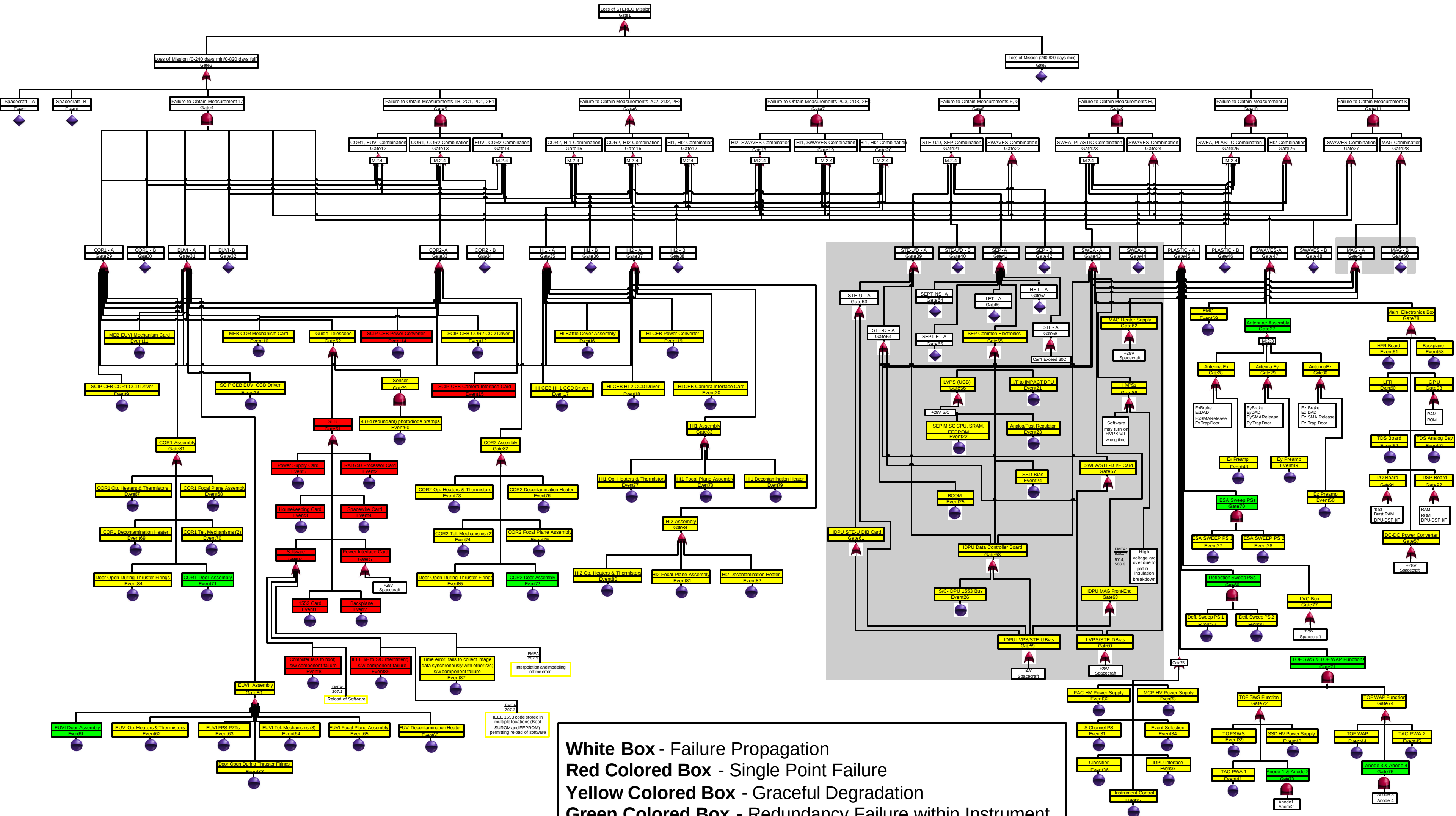
A – Ahead
B – Behind
IMPACT Items in Gray

Minimum Mission RBD (240-820 days)



A – Ahead
B – Behind
IMPACT Items in Gray

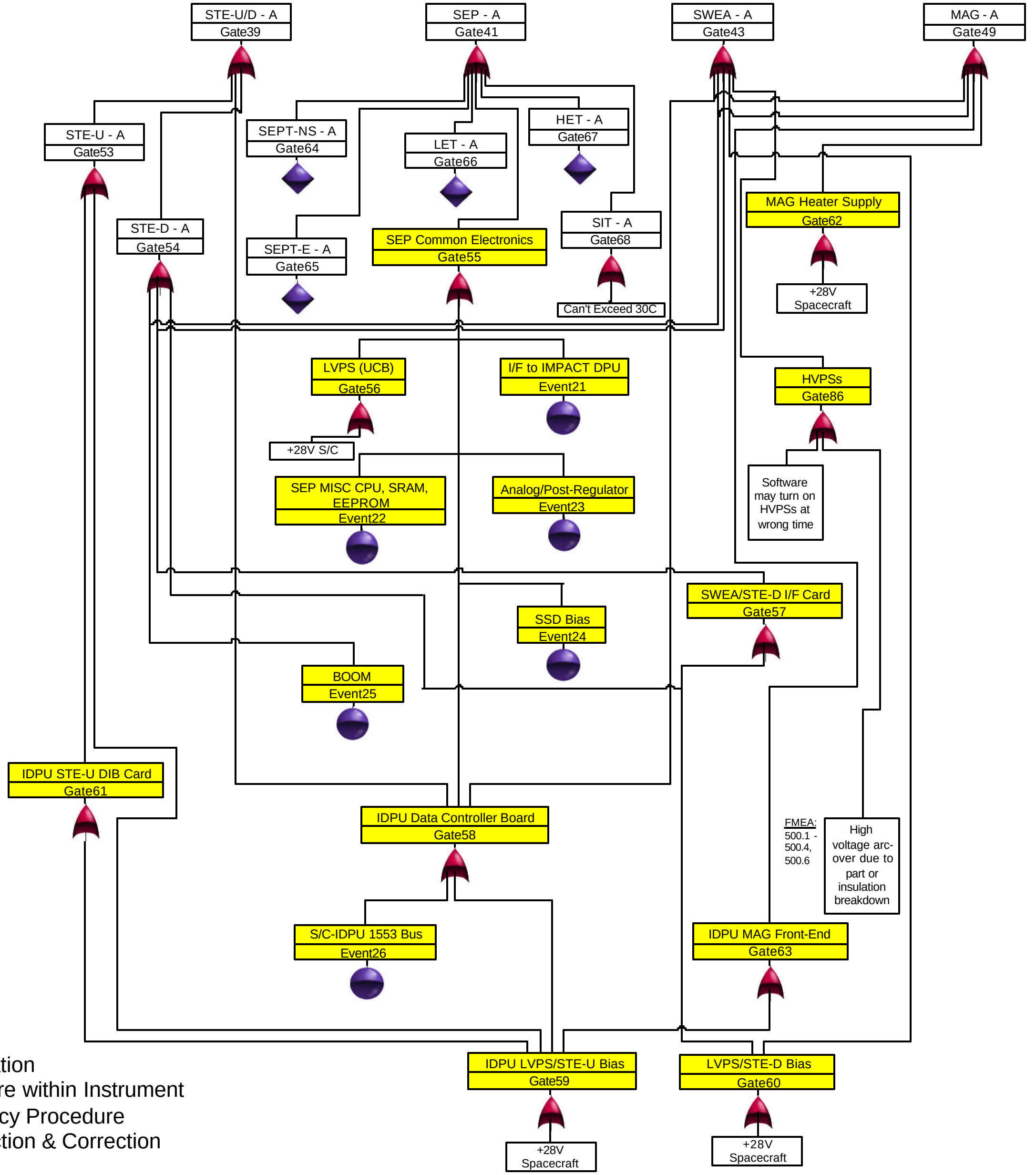
Mission Master Logic Diagram



White Box - Failure Propagation
Red Colored Box - Single Point Failure
Yellow Colored Box - Graceful Degradation
Green Colored Box - Redundancy Failure within Instrument
Yellow Outline Box - Ground Contingency Procedure
Blue Outline Box - Onboard Fault Detection & Correction

IMPACT Items in Gray

IMPACT Master Logic Diagram



White Box - Failure Propagation
Red Colored Box - Single Point Failure
Yellow Colored Box - Graceful Degradation
Green Colored Box - Redundancy Failure within Instrument
Yellow Outline Box - Ground Contingency Procedure
Blue Outline Box - Onboard Fault Detection & Correction

OR Gate
AND Gate
Basic Event
Undeveloped Event

IMPACT FMEA

Failure Mode Number	Identification A. Instrument B. Item Analyzed	A. Failure Mode B. Failure Cause	Failure Effects A. Local B. Next Higher Level C. End Effect	Severity Category	Remarks A. Retention Rationale B. Failure Detection Method C. Compensating Features/Actions
550.1	A. IMPACT B. BOOM	A. Tube Jam B. Inadequate clearances	A. Boom partially deploys B. MAG, STE-D and SWEA cannot provide accurate data and causes pointing accuracy degradation which affects SECCHI Instruments C. Loss of Mission*	2	A. Single Point Failure* B. Boom does not fully deploy – instrument responses do not meet requirements C. 1. Design clearances, ground testing and excess deployment force in design to prevent jamming 2. Other spacecraft instrument set
550.2	A. IMPACT B. BOOM Stacer Spring	A. Fails to deploy B. Jammed stacer mechanism	A. Boom fails to fully deploy B. MAG, STE-D and SWEA cannot provide accurate data and causes pointing accuracy degradation which affects SECCHI C. Loss of Mission*	2	A. Single Point Failure* B. Instrument responses do not meet requirement C. 1. Design clearances, ground testing and excess deployment force in design to prevent jamming 2. Other spacecraft instrument set
550.3	A. IMPACT B. BOOM Harness	A. Harness jams or hangs up B. Irregular surfaces on harness catch in deployment mechanism	A. Boom fails to fully deploy B. MAG, STE-D and SWEA cannot provide accurate data and causes pointing accuracy degradation which affects SECCHI C. Loss of Mission*	2	A. Single Point Failure* B. Boom does not fully deploy – instrument responses do not meet requirements C. 1. Design clearances, ground testing and excess deployment force in design to prevent jamming 2. Other spacecraft instrument set
700.8	A. IMPACT B. IDPU 1553 Interface	A. 1553 channel locked up due to "Blabbermouth" mode B. Component failure	A. No output data from IDPU B. All intra observatory communication blocked C. Loss of Mission	2	A. Single Point Failure B. Loss of communication with spacecraft C. 1. B channel of 1553 data bus (if not involved in "Blabbermouth" failure) 2. Not an issue if S/C can turn off instrument

*To be verified through analysis being performed with Boom partially deployed

SEVERITY CLASSIFICATIONS:

Category 1 – Catastrophic - Failure modes that could result in serious injury or loss of life, or damage to spacecraft or launch vehicle and result in loss of mission.
Category 2 – Critical - Failure modes that could result in loss of one or more minimum mission science objectives as defined by the GSFC Project office.
Category 3 – Significant - Failure modes that could cause degradation to mission objectives, but still meet minimum science objectives.
Category 4 – Minor - Failure modes that could result in insignificant or no loss of mission objectives.

Analysis Results (1 of 3)

- Reliability Block Diagrams
  - IMPACT has backups to obtain measurements for the mission
    - SWAVES, PLASTIC, and SECCHI – HI2
  - Combination failures of SWAVES and either IDPU DCB or IDPU LVPS will lead to the loss of measurements F, G, H, I and K
  - Combination failures of SWAVES and any of the following IMPACT items will lead to the loss of measurement K: MAG, IDPU Front-End Electronics Card, IDPU MAG Heater Supply Card, IDPU DCB, IDPU LVPS, or the BOOM
  - Enables the calculation of mission reliability
- Reliability Predictions
  - Identify reliability drivers based on failure rate calculations
    - Reliability drivers to be provided at the Observatory CDR
    - Graceful degradation elements turn out to be robust due to backups
  - Reliability predictions used in other PRA activities for the mission

Analysis Results (2 of 3)

- Master Logic Diagram (MLD)
  - Top-down, identification of what causes mission failures and categorized into Single Point Failures (SPF), graceful degradation failures and redundancy failures. MLD includes non-parts related causes (those not evaluated by RBDs, FTAs and reliability predictions, like operator/software and environment).
    - IMPACT provides graceful degradation modes for the mission
    - BOOM could be a SPF, if partially deployed
      - MAG, STE-D, SWEA cannot provide accurate data
      - Could cause pointing accuracy degradation which affects SECCHI instruments
      - Analysis being performed with Boom partially deployed
    - No operator induced failures identified
    - Considered time critical contingency procedures and on-board autonomy rules necessary to save instrument after first failure
      - Turning instrument off if a “Blabbermouth” condition occurs
- Fault Tree Analysis (FTA)
  - Minimal cut set analysis identifies and ranks single & combination failures along with probabilities for loss of mission
    - Confirm failures identified in RBD and Master Logic Diagram
    - Confirm likelihood of failures by ranking from the highest contribution to unreliability to the lowest

Analysis Results (3 of 3)

- Failure Modes and Effects Analysis (FMEA)
  - Bottom-up analysis of postulated failures and their consequences
    - Cross checked MLD and causes of failures with FMEA consequence of lower level failures
    - Considered propagation of failures from instrument to spacecraft
      - Power - Spacecraft fuse blows
      - Data - Corrupt 1553 bus, consider protection from “Blabbermouth” on the bus
      - Cross-checked spacecraft I/F ICD and FMEA causes
- Summary
  - Any design changes or recommendations? None
  - Be sure that we don’t have a latent design or manufacturing problem

Risk Mitigations

- Moving Surfaces (BOOM, Covers)
  - Instruments have backups
  - Design margin, redundancy, peer reviews, testing
- Software and Operations
  - Software is reloadable, should not result in mission loss
  - Software and operational plan, peer reviews, testing
- Parts Applications
  - Parts stress analysis per PPL21/MIL-STD-975, peer reviews, testing
- Understanding of Environment
  - Analysis with single common environment spec, peer reviews, testing
- Workmanship
  - Inspection to NASA-STD-8739 or equivalent, material and process control, PCB coupons, testing
- Random Failures
  - Grade 2 parts, simplicity, robust design with graceful degradation, redundancy, peer reviews, testing