

# Recent Progress in the APL Fault Management Process

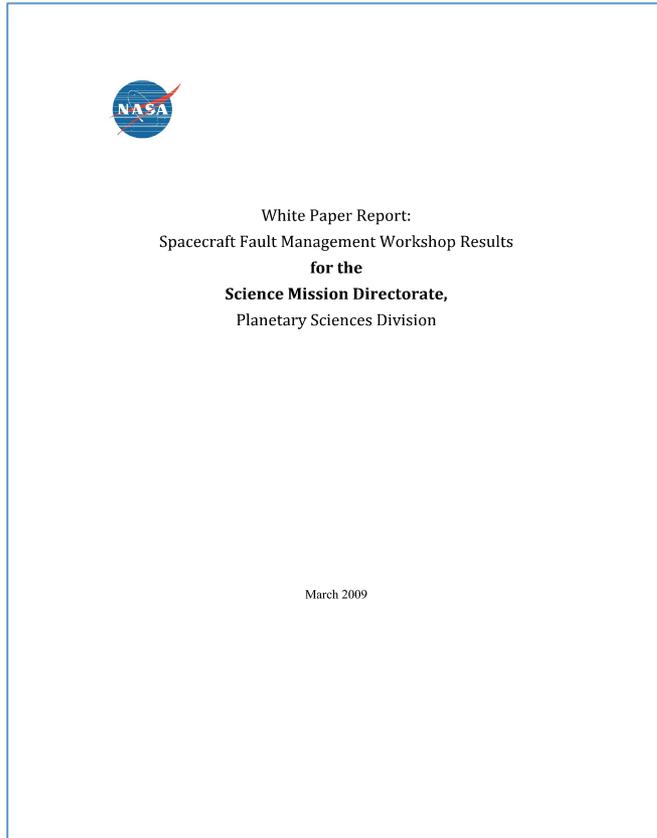
Kristin Fretz & Adrian Hill  
JHU/APL



# APL

JOHNS HOPKINS UNIVERSITY  
Applied Physics Laboratory

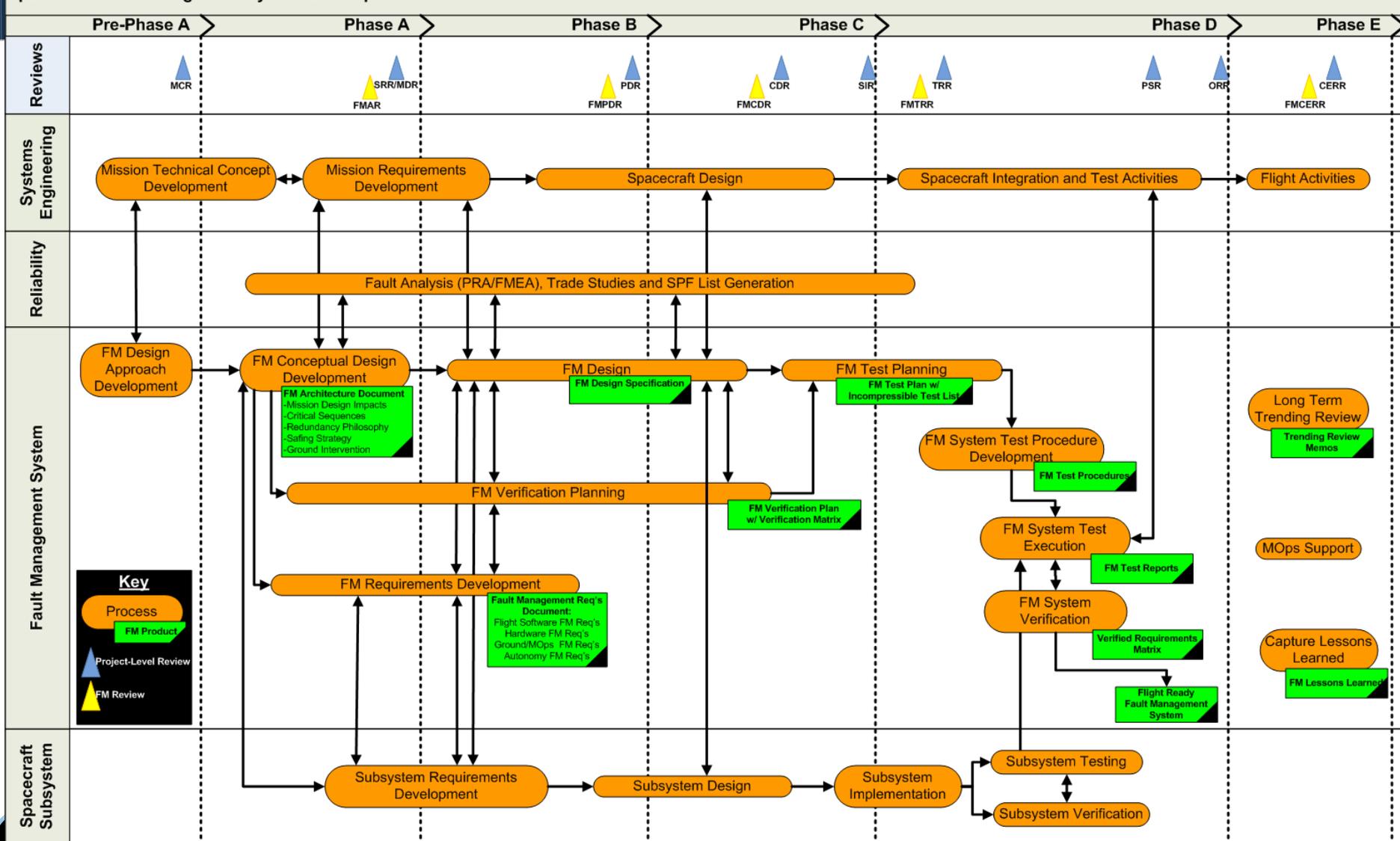
# Overview



- 2008 FM Workshop published a White Paper Report identifying 12 top-level findings and recommendations for improving FM systems
- APL recognized these needs and improved its FM and Autonomy processes to address many of these findings
  - Processes are part of APL's Quality Management System (QMS)
  - Changes implemented on the Radiation Belt Storm Probes (RBSP) project
- Presentation will highlight 6 of the findings, discuss the APL process changes, and the impact of the changes on both the FM and Autonomy processes

# APL FM Development Process

Spacecraft Fault Management System Development Process



# RBSP Overview

## Launch and Orbit Insertion



- Single EELV (Observatories Stacked)
- Launch from KSC
- Each observatory independently released Sun pointed
- LV performs maneuver to achieve nominal lapping rate
- Launch: May 2012

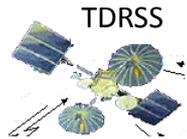
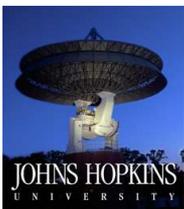
## 2 Observatories (RBSP-A, RBSP-B)

- Nearly identical, single string architecture
- Spin Stabilized ~5 RPM
- Spin-Axis 15°-27° off Sun
  - Attitude Maneuvers Every 21 days
  - No on-board G&C attitude control
- Operational Design Life of 2 years



APL Ground Station  
• Primary

NEN Station(s)  
• Data Augmentation  
• Back-up



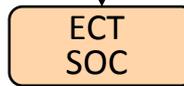
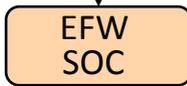
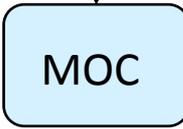
TDRSS  
Critical Events at Launch



Differing apogees allow for simultaneous measurements to be taken over the full range of observatory separation distances several times over the course of the mission. This design allows one observatory to lap the other every 75 days.

## Decoupled Operations

- Basic Approach Based on TIMED, STEREO



Commands & Telemetry

Instrument commands

Instrument Telemetry



# Finding 2: Diffused FM

## ***Finding:***

- *“Responsibility for FM currently is diffused throughout multiple organizations; unclear ownership leads to gaps, overlap and inconsistencies in FM design, implementation and validation”*

## ***Recommendation:***

- *“Establish clear roles and responsibilities for FM engineering”*
- *“Establish a process to train personnel to be FM engineers and establish or foster dedicated education programs in FM”*

# Implemented Change for Finding 2: Diffused FM

- APL split FM functionality into two distinct roles: Fault Management and Autonomy
- FM is a system engineering function that:
  - Develops concept of operations
  - Develops FM architecture
  - Oversees reliability analyses such as FMEA/PRA
  - Defines requirements and allocation of those requirements to hardware, software, autonomy, and operations
  - Verifies and validates system with mission-level tests during I&T
- Autonomy is a software engineering function that:
  - Designs and implements autonomy rule-based system derived from allocated FM requirements
  - Performs unit-level/subsystem-level verification



# Finding 4: Insufficient Formality of Documentation

## ***Finding:***

- *“There is insufficient formality in the documentation of FM designs and architectures, as well as a lack of principles to guide the processes”*

## ***Recommendation:***

- *“Identify representation techniques to improve the design, implementation and review of FM systems”*
- *“Establish a set of design guidelines to aid in FM design”*

# Implemented Change for Finding 4: Insufficient Formality of Documentation

- APL's QMS has formal FM and Autonomy engineering processes which define required documentation and reviews

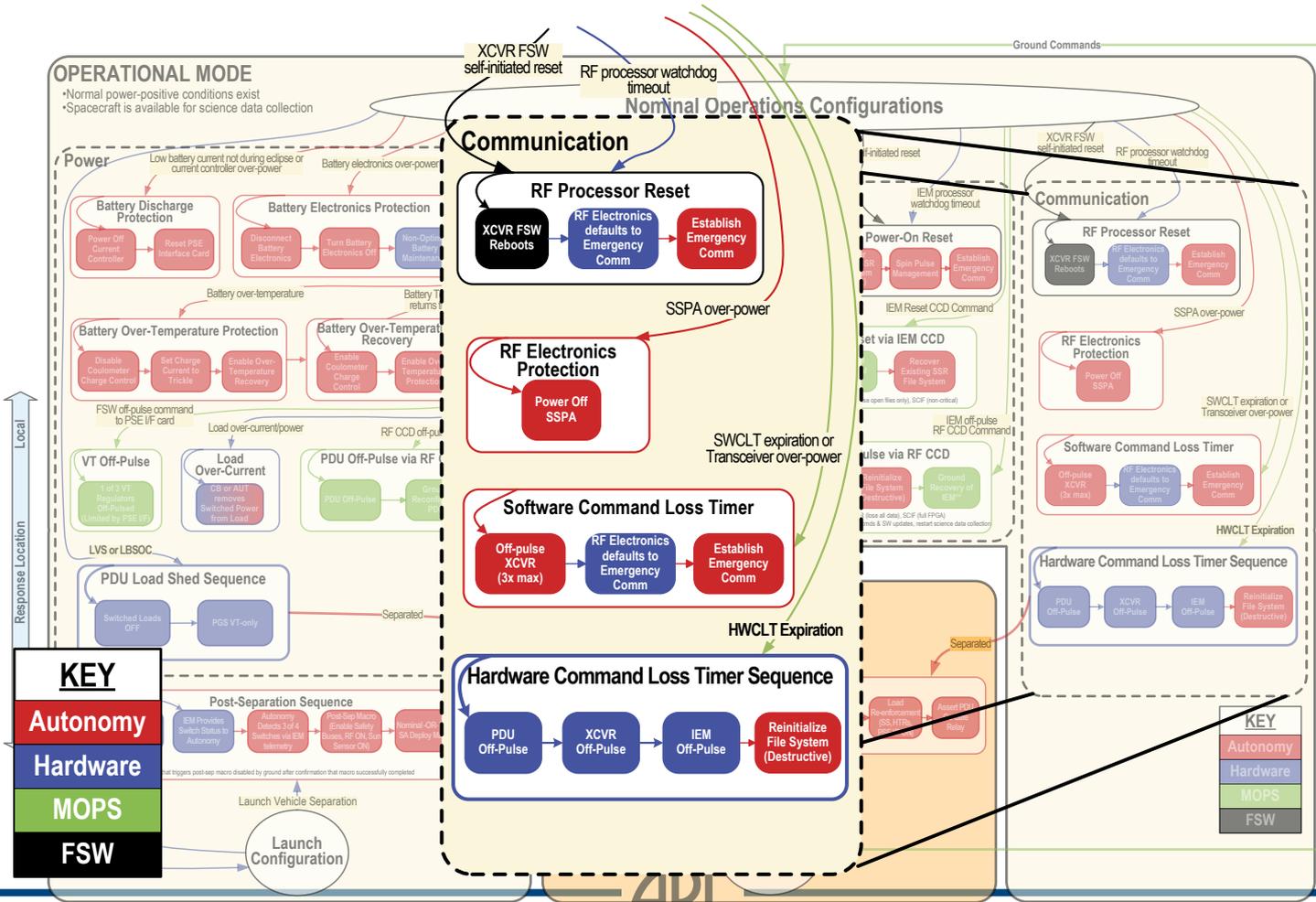
FM	Autonomy
FM Architecture Document	N/A
FM Requirements Document	Autonomy Requirements Specification
FM Design Specification	Autonomy Design Spec & Users Guide
FM Test Plan & Verification Matrix	Autonomy Acceptance Test Plan
FM Test Procedures	Autonomy Acceptance Test Specification
FM Test Reports	Autonomy Acceptance Test Report (includes verification matrix)

- RBSP FM and Autonomy developed system and subsystem diagrams to communicate information captured in architecture, requirements, and specifications



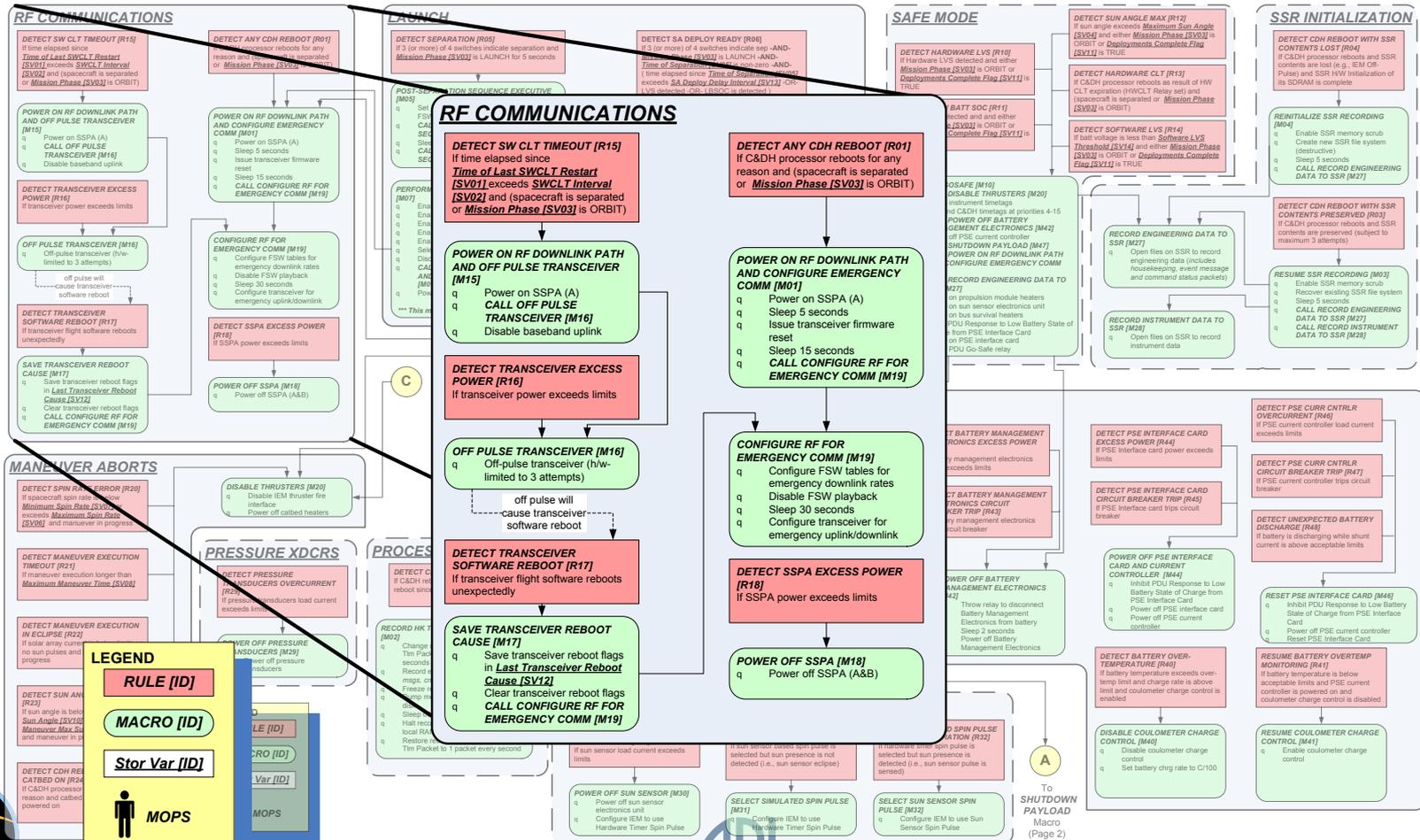
# Implemented Change for Finding 4: Insufficient Formality of Documentation

- Example of **Fault Management Modes Diagram** used to convey interactions between *Hardware, Software, Autonomy, and Ground/Operations* for managing spacecraft faults



# Implemented Change for Finding 4: Insufficient Formality of Documentation

- Example of Autonomy Design Diagram used to convey implementation of monitors and responses that comprise the on-board autonomy system for responding to faults



# Findings 7 & 8: FM Complexity

## ***Finding 7:***

- *“The impact of mission-level requirements on FM complexity and V&V is not fully recognized”*
  - *“Review and understand the impacts of mission-level requirements on FM complexity; FM designers should not suffer in silence, but should assess and elevate impacts to the appropriate levels of management”*

## ***Finding 8:***

- *“FM architectures often contain complexity beyond what is defined by project specific definitions of faults and required fault tolerance”*
- *“Increased FM architecture complexity leads to increased challenges during I&T and mission operations”*
  - *“Assess the appropriateness of the FM architecture with respect to the scale and complexity of the mission, and the scope of the autonomy functions to be implemented within the architecture”*

# Implemented Change for Findings 7 & 8: FM Complexity

- FM involvement on RBSP started in early phase-A as a part of the systems engineering team
  - Involved in mission-level trades and assessed impact of mission-level decisions on FM
  - FM “ownership” of requirements at all levels with requirements allocated from mission-to-system-to-subsystem
- Development of FM Architecture Document defined FM approach for the project
  - Architecture document now a formal part of FM process which helped to communicate FM concepts/approach
  - Resulted in project “buy-in” on FM approach early in mission development



# Finding 11: Inadequate Testbed Resources

## ***Finding:***

- *“Inadequate testbed resources is a significant schedule driver during V&V”*

## ***Recommendation:***

- *“Develop high-fidelity simulations and hardware testbeds to comprehensively exercise the FM system prior to spacecraft level testing”*



# Implemented Change for Finding 11: Inadequate Testbed Resources

- RBSP flight software testbeds available for both FM and Autonomy testing
  - Available early and provided enough fidelity to verify Autonomy system
  - Allowed for dry-running portions of FM system-level tests
- RBSP project also developed high-fidelity hardware-in-the-loop (HIL) simulator
  - Purpose of HIL was to provide high-fidelity test platform for the development of FM system tests prior to spacecraft I&T
    - Due to hardware issues completion and availability of HIL was delayed until late I&T
  - FM system-level testing (dry-run and for-score) was performed on spacecraft without the opportunity to dry-run on the HIL



# Finding 1: Cost & Schedule

## ***Finding:***

- *“Unexpected cost and schedule growth during final system integration and test are a result of underestimated Verification and Validation (V&V) complexity combined with late resource availability and staffing”*

## ***Recommendation:***

- *“Allocate FM resources and staffing early, with appropriate schedule, resource scoping, allocation, and prioritizing; schedule V&V time to capitalize on learning opportunity”*
- *“Establish Hardware / software / “sequences” /operations function allocations within an architecture early to minimize downstream testing complexity”*
- *“Engrain FM into the system architecture. FM should be “dyeed into design” rather than “painted on””*

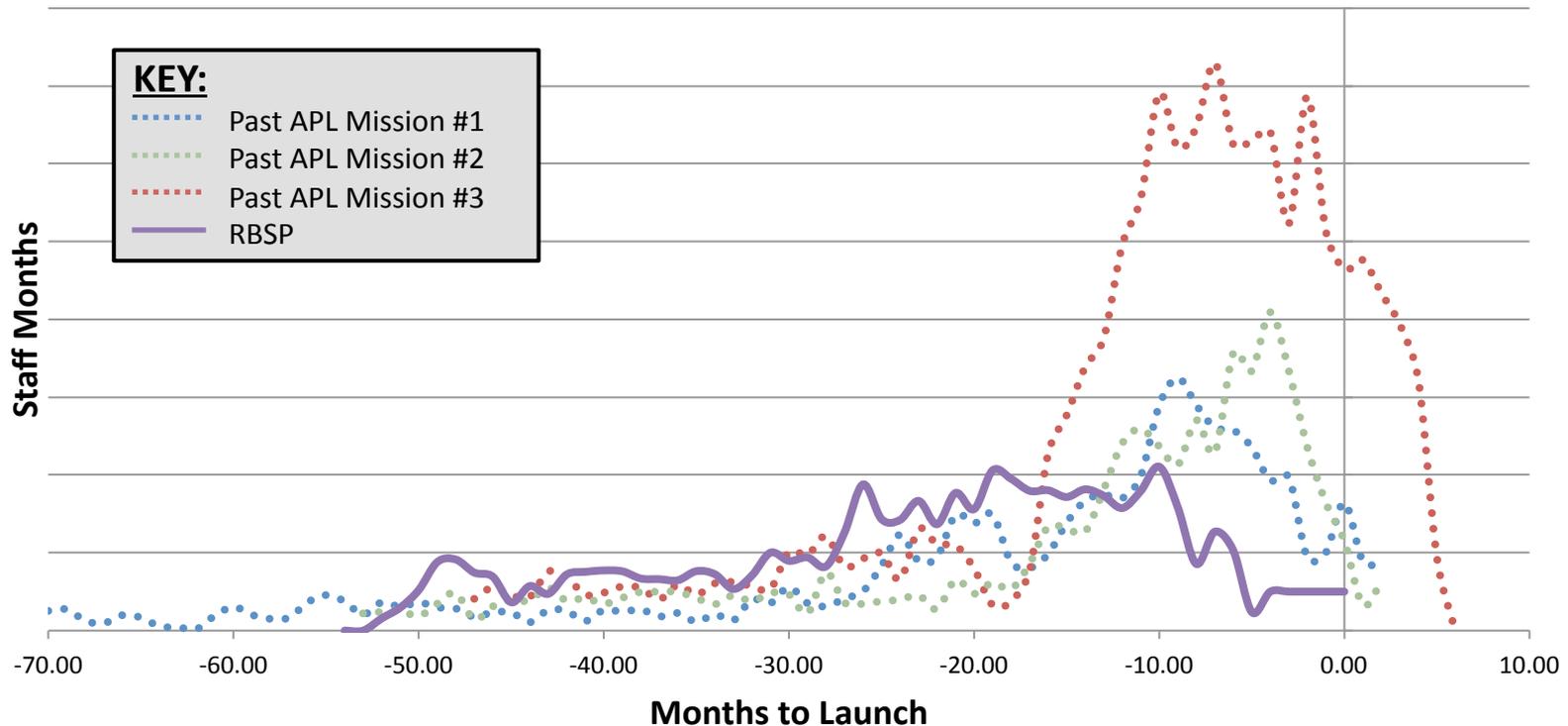
# Implemented Change for Finding 1: Cost & Schedule

- RBSP spacecraft-level testing for both FM and autonomy started early in I&T
  - FM tests were ready at start of I&T which allowed for dry-running of tests (utilized partially integrated spacecraft)
  - Staffing for FM and Autonomy testing increased in response to lessons learned from New Horizons and MESSENGER
- FM Design Specification clearly defined allocations of FM functions to hardware, software, autonomy, and operations
- Improved approach, planning, and staffing resulted in avoiding “death spiral” and staffing “bump” during I&T



# Implemented Change for Finding 1: Cost & Schedule

- Past missions resulted in staffing “bump” during I&T
- Noticeable change in shape of staffing curve for RBSP
  - FM/Autonomy waited on the spacecraft for testing rather than spacecraft waiting on FM/Autonomy
  - Remaining RBSP time is projected



# Conclusion

- Significant changes seen in staffing curve for RBSP as compared to previous APL missions
- Credit process changes for these improvements:
  - Better defined FM/Autonomy roles
  - Required documentation at key milestones
  - Use of diagrams as communication tool for documentation
  - Early program involvement to manage complexity
  - Improved testbed resources
- APL FM/Autonomy processes continuing to evolve by using lessons learned from RBSP and findings from 2008 FM Workshop

