Advanced Plug-and-Play Technologies (APT) Lessons Learned – Task Order #1

Steven Schenk
Stanley O Kennedy, Jr.

02 November 2010

COMTECH AA AEROASTRO, Inc.®

aeroastro.com

Why is CAA interested in PnP? (1 of 2)

- **Lower Cost Space Vehicles**
  - Common “core” vehicles retire Non-Recurring Engineering costs (NRE) which can amount to >15% of program costs
  - Permits CAA to be cost competitive with large primes who can invest in winning government programs
- **Rapid Reconfiguration**
  - Rapid component, subsystem, and/or payload reconfiguration measured in days or weeks versus years
  - Higher modularity does not necessarily guarantee greater flexibility (especially at the component level)
- **Multi-Mission Platforms**
  - Host a variety of Payload or mission types with minimal impacts to program cost and schedule (ie: Swap an EO MWIR with a Com PL)
- **Standard Interfaces**
  - Strict adherence to established, documented standards in all interface arenas (mechanical, thermal, electrical, and data) minimizes cost and lowers program risk

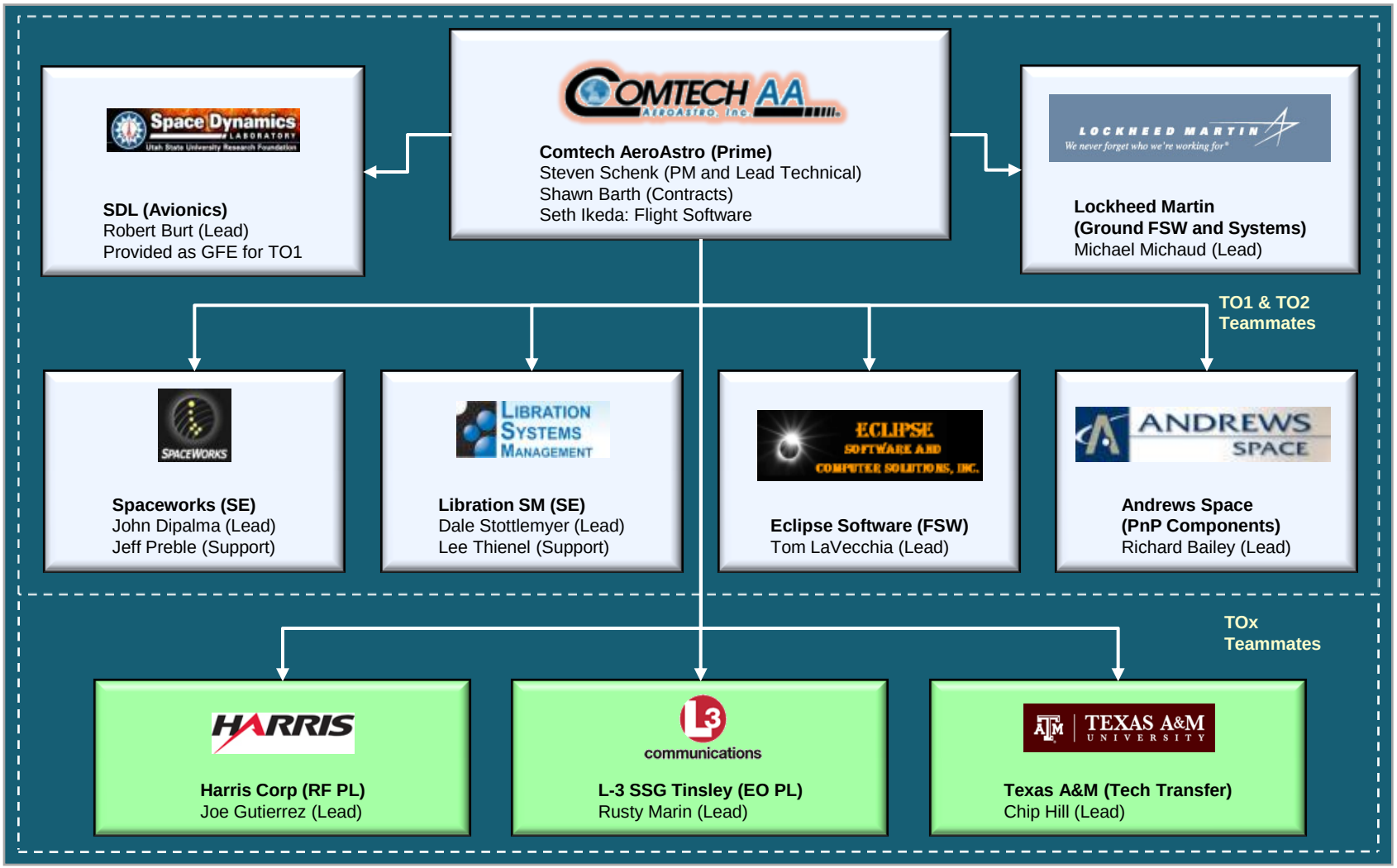
Why is CAA interested in PnP? (2 of 2)

- **Rapid Space Vehicle Deployment**
  - Common “core” platforms, using standard interfaces can be rapidly fielded
  - SV acquisitions in several months versus several to tens of years
- **Space Vehicle Constellation Acquisition**
  - Enables a constellation made up of single sensor Space Vehicles with different sensors on each Space Vehicle using the common “core” platform
- **Commercial Space Vehicle Applications**
  - Commercial technology spawned AFRL PnP through the standard definition of interfaces, such as personal computers and the Universal Serial Bus (USB)
  - Enables CAA to compete in the commercial Space Vehicle market by maintaining rigorous DoD level mission assurance at very low cost
- **Advanced Technology Applications**
  - Adoption of PnP enables CAA to efficiently offer advanced technology on-ramps (power, propulsion, etc) during the program timeline for incorporation of high risk, high payoff technologies

So, What are the Disadvantages of PnP?

- **Loss of point designs that optimize payload performance**
  - Customers generally expect the system to be optimized for the mission, which is much more costly and time consuming than flying a common “core” bus that supports “good enough”, non-exquisite payload performance
- **Added complexity at the component level**
  - Adding several components into the architecture theoretically lowers reliability
- **Distributed power architecture**
  - Not necessarily a disadvantage, but suffers to gain acceptance because it is a new concept and is non-traditional
- **Distributed avionics architecture**
  - Not necessarily a disadvantage, but suffers to gain acceptance because it is a new concept and is non-traditional
  - In actuality, this approach adds reliability due to multi-processor operations (if it is designed and tested correctly)
- **Adherence to interface standards**
  - Engineers and Managers are “tinkerers” by nature, so strict adherence to standards, especially if they don’t agree with that specific standard, is ignored

APT TO#1 Program Team



CAA APT TO#1 Program Objectives/Tasks

- **Main Objectives**
  - Mature the System Architecture Design to a CDR-Level
    - CAA did not perform any hardware maturity in TO#1, but put in the hooks to accommodate any PnP hardware choice
    - CAA did not change any SDM FSW code or functionality, but did build a independent FSW module that can be implemented to any system using SDM FSW
    - Detailed design of the power distribution and essential bus approaches
  - Risk Reduction & maturation of applicable PnP/SPA Technologies
- **Main Program Tasks**
  - Work Package #1: System Architecture Design
  - **Work Package #2: FSW Fault Manager Module Development**
    - **Largest, most time-intensive task that we performed for TO1**
  - Work Package #3: Spacewire Fault Management & Response
  - Work Package #4: Power Hub Fault Management & Response
  - Work Package #5: ASIM Fault Management & Response
  - Work Package #6: MODAS Fault Management, Response, & Test
  - Work Package #7: Power Bus Implementation

Overall Summary of Results (1/2)

- **System Architecture/Power Bus Implementation**
  - We designed an effective PnP Network that is PnP Hardware Agnostic
    - Design maintains the hinged, two piece internal PnP component panels
      - Internal positioning of router/power hub maximizes internal bus volume providing greater flexibility to rapidly reconfigure or locate components
      - Internal panel provides much better EMI/EMC performance
      - All side panels are identical, reducing cost, schedule, and parts count
    - Design is transparent to Spacewire Router or Power Hub hardware choice
      - Only exception is the 30A endpoint on the Goodrich router
    - Design can accommodate multiple CPU choices (SDL MODAS CPU or the Broadreach IAU, with some modifications)
  - We optimized the power distribution design to minimize cost, complexity, and mass
    - Elimination of a separate solar array bus, greatly simplifying the power design
    - Increases system reliability as solar array power is directly controlled at the array level, with robust fault protection at multiple levels (HW and SW)
    - Implemented a very effective Essential Bus/Non-Essential Bus Design

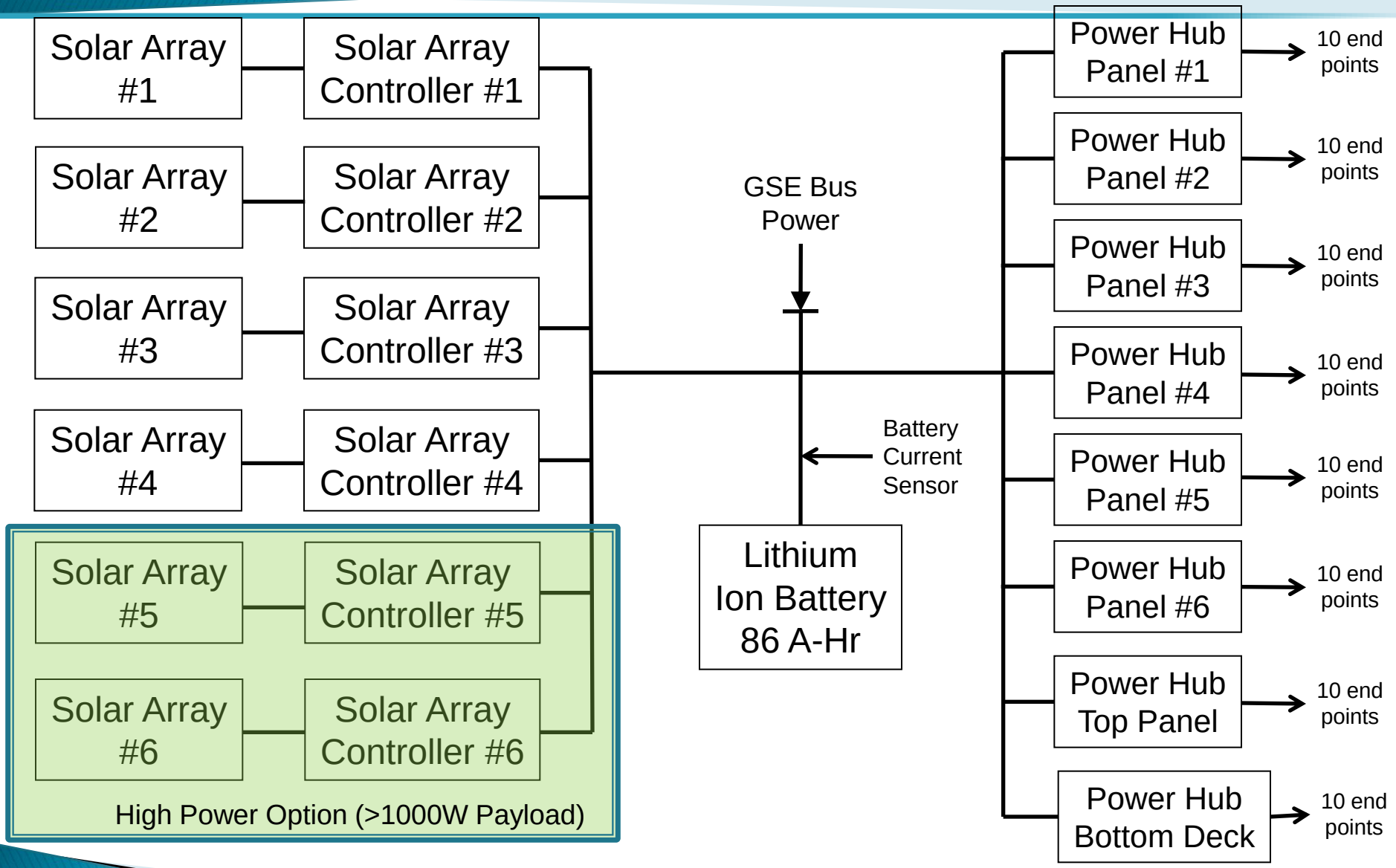
Overall Summary of Results (2/2)

- **Fault Manager Development**
  - Our FSW team ran into a lot of issues (both large and small) in interfacing with the current FSW infrastructure (xTEDS, ASIM, SDM, SDT,etc)
    - This was an positive benefit as we became much more experienced in FSW design, implementation, and test as a result
    - Our team now has an excellent understanding of the intricate details / interoperability between FSW components
  - Successfully completed development and test of FM FSW code that can be built as an add-on module that requires no change to the SDM core
  - Successfully developed and tested code that:
    - Detects and mitigates hardware faults (ASIM failure, Power Hub Failure)
    - Detects and mitigates low power states in FSW (ESB in FSW versus HW)
- **Component FMEA**
  - Reviewed the Goodrich ASIM, Power Hub, & SpW Router & SDL MODAS
  - Two critical failure modes found and addressed
    - Power MODAS
    - Power Hub
  - Several potential critical failure modes identified and addressed

Network System Architecture Overview

- **Baseline FSW: Satellite Data Model (SDM)**
- **Baseline PnP Hardware: SPA-S**
  - CAA APT bus is not designed to a specific SPA component and is transparent to the majority of available SPA-S hardware
    - Spacewire Router (Goodrich, SDL, Andrews Space, etc)
    - Power Hub (Goodrich, SDL, Andrews Space, etc)
    - ASIM (Goodrich, PnP Innovations, Andrews Space)
    - CPU (SDL, Broadreach IAU, PnP Innovations)
- **Other SPA Characteristics**
  - Adoption of PnPSat-2 modular panels with internal SPA-S
    - Minimizes custom harness work
    - Maximizes external (panel) surface area and volume
    - Each panel is identical and can be swapped with any other panel
  - Panel to Panel electrical attachments
    - Each panel has multiple interfaces to other panels
  - Main bus (Battery) with no solar array bus
    - Use of Solar Array Controllers at side panels to feed solar array power to main bus

Distributed Power Architecture

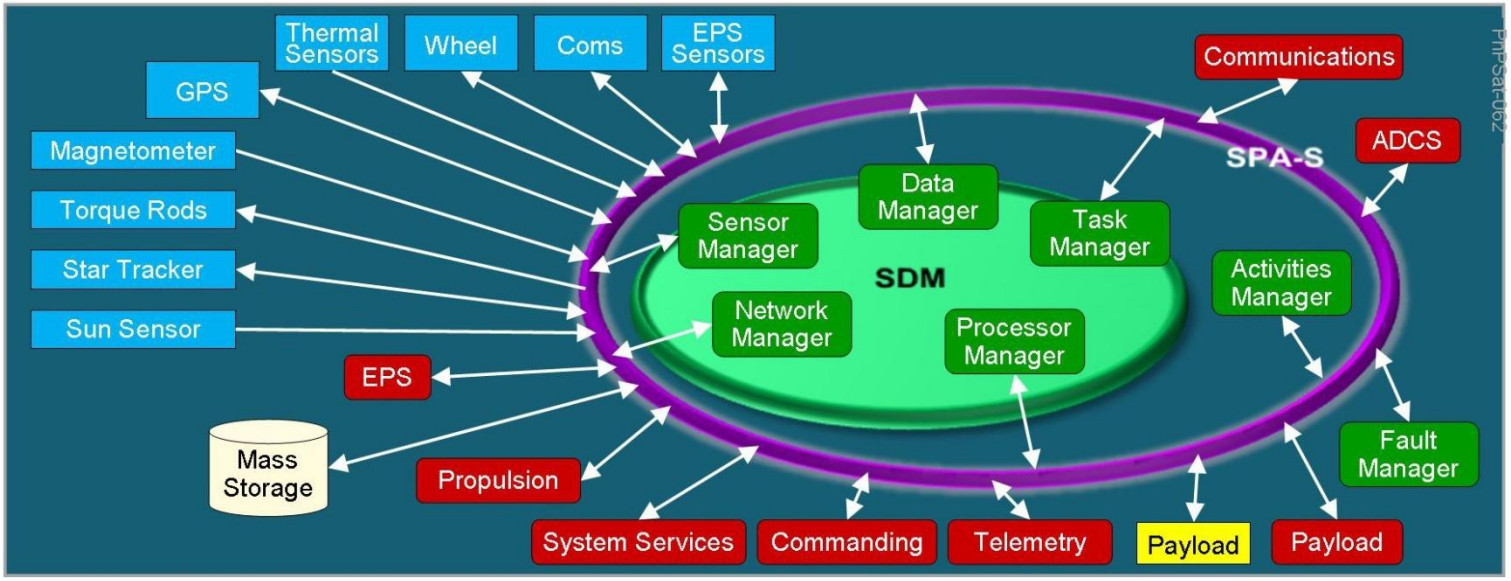


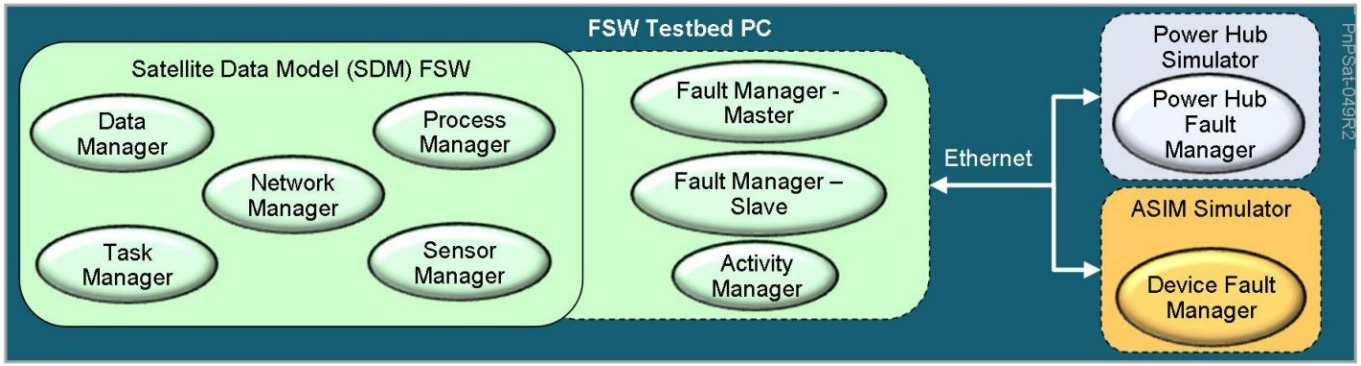
Essential Bus/Non-Essential Bus Approach

- **Traditional SC designs use an ESB/NEB architecture**
  - Launch with ESB **ON** (Battery on-line w/Command Receiver/Avionics)
  - Hard-wire between receiver and avionics to ensure communications
    - Contradicts the basic PnP philosophy
- **CAA implemented an ESB/NEB Design that does the following**
  - Launch with ESB **ON**
    - ESB on still allows for our APT bus design to meet ORS End-State goals of rapid launch as power consumption is low (EPS MODAS, PH, SGLS Rx only)
    - Eliminates a requirement for a launch controller component that senses separation switch activation
    - Provides fault management for separation switch chatter since the EPS MODAS is ON and monitors timing of the switch in OPEN/CLOSE
  - Power Hubs are on Essential bus & provide an extra level of fault management
  - Power control of ESB components through guarded commanding (several command scripts with prompts) to turn PH ports **OFF**
    - Initially focused on forcing several PH ports to Power ON at all times
      - Undesirable as this removes ability to power reset if SEU or latchup occurs
    - xTEDs need to define what components require ESB or NEB and controlled by the configuration file

FSW Fault Manager

- Generate a FSW Fault Manager Module to work within the SDM FSW
- Dedicated FSW testbed





Fault Management

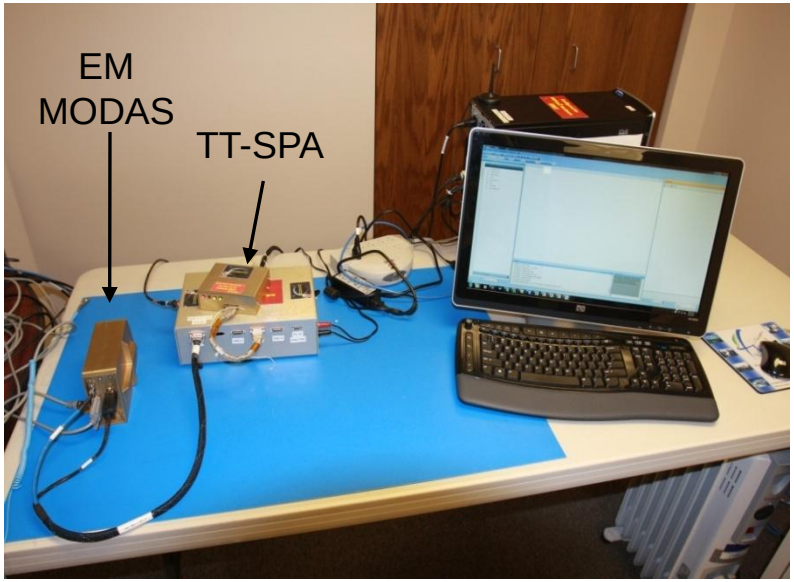
- **Device Fault Manager (DFM)**
  - No support in current SDM for hardware device fault management
  - FM supports hardware device failure and recovery
  - FM supports hardware/ASIM heartbeat and poling
  - Fault Management for device defined in xTEDS
  - Hardware devices register with DFM at system discovery/initialization
  - Tracks device messages and restarts noisy devices
  - DFM will force the deregistration of non functioning devices
  - Device control via power hub port control
- **Power Fault Manager (PFM)**
  - No power fault management provided by SPA
  - PFM supports vehicle control while managing vehicle power health
  - PFM supports hardware/ASIM control
  - PFM was not in our original proposed Task List, but ended up being developed out of necessity of controlling an ESB/NEB philosophy at the FSW level

Device Fault Manager

- **Supports Fault Management For Hardware Devices**
- **Two Components**
  - Device Fault Manager
    - Maintains configuration of hardware devices fault responses
    - Maintains heartbeat or polling history of devices
    - Resets devices in the event of a device failure
    - Communications to power hub and devices via active messaging
  - Device/ASIM Fault Manager
    - Resides on ASIM
    - Receives registers with DFM to define fault management
    - Responds to DFM polling or issues a heartbeat to FM
    - Responds to configuration requests
    - Responds to configuration commands
    - Processors are handled the same as other devices

Device Fault Manager

- **Secondary DFM**
  - Only exists in multiprocessors systems
  - Must run on a different processor than primary DFM
  - Secondary DFM becomes primary if primary DFM heartbeat is lost
  - **Did not work due to incompatibility of SDM between Operating Systems**
- **Initialization**
  - Device fault management definition via xTEDS during vehicle discover or when a device comes on line
  - Power Hub port look up during registration
- **Operation Loop**
  - Maintains communication with HW devices to validate health & status
  - If communications is lost then DFM resets the device



APT TO#1 Flight Software Testbed

Fault Management – Bus Power

- **Power level detection & handling**
- **All power consuming devices must support PFM registration**
- **Send and receive power state to registered devices**
- **Shut down & start up devices (SW/HW) depending on device priority**
- **Devices types/kind have default power priorities**
  - Used to generate list of devices for the PFM
  - Configurable during integration
- **Device bus power thresholds are set to defaults**
  - Configurable during integration
- **EPS must be integrated with PFM**
  - EPS sends power status to PFM for proper handling of vehicle health
- **Autonomous recovery after low power events**
  - As power level recovers, PFM restarts devices it shut down
- **Bus power levels**
  - 0 lowest (essential devices only)
  - 9 highest (all devices are powered on)

Fault Management Conclusions (1 of 2)

- **Generated a number (>25) of Fault Management Algorithms that were coded, tested and executed successfully**
- **Device Fault Manager worked flawlessly detecting device faults and providing a response system response to those faults**
  - ASIM failures detected and resolved
  - Power Hub failures detected and resolved
  - Our fault management system successfully responded to the AFRL chop shop worm installation at our final presentation until the worm shut down our network manager, which we did not have specific code for at that time
    - We are working on a fault response to network manager anomalies that will reside as a hardware solution to combat this type of failure
  - Unable to fully test the Multi-Processor failure scenario as the SDM was unsuccessful in communicating over two different operating systems

Fault Management Conclusions (2 of 2)

- **Low Power Fault Manager functioned flawlessly**
  - Used SDM discovery process, messaging, and xTEDs formats
  - No changes to SDM were necessary
  - Identified Red/Yellow/Green Limits for power
  - Flight like event driven power safing manager
    - Shuts down non-essential devices (device priority based “kind” in xTEDS and a configurable priority table)
    - If command to device doesn’t succeed then power source for that device is turned off
    - Commands ACS to point at the sun
    - Autonomously restarts devices as power state improves

Component FMEA Overview

- **Generation of an FMEA on four key pieces of PnP enabling HW**
  - Spacewire Router (Goodrich Gen#2 Hardware)
  - Power Hub (Goodrich Gen#2 Hardware)
  - ASIM (Goodrich Gen#2 Hardware)
  - MODAS (SDL Engineering Model)
  - **Note: All SPA-S components are single-string with no redundancy**
- **Develop failure scenarios that can occur, the optimum detection methods, and most appropriate responses**
  - Leverages the current fault checking used on our CAA heritage bus designs to support fault assessment
  - This approach incorporates both HW signal checks and SW exceptions to generate and handle faults
  - The solutions identified are incorporated into the PnP specifications and product functional specifications
- **Each component has items identified that merit further investigation to reduce performance uncertainty**

Component FMEA Summary

- **All test bypass connections (RS-422) need to be capped prior to flight to minimize any EMI/EMC issues on orbit**
  - Need to ensure connections don't act as antennas for signal or noise input
- **Two critical failure modes were found (Critical Failure results in immediate loss of mission)**
  - EPS MODAS
    - Power (+28V) Open Circuit
  - Power Distribution Hub
    - Power (+28V) Open Circuit
- **Potential Critical items with no redundancy identified with a response plan where applicable**
  - ASIM
  - MODAS: EPS and Payload
  - Power Distribution Hub
  - SpaceWire Router
- **Failures of PnP components will not result in safety concerns**
- **All PnP Component FMEA workbooks incl. in backups & Final Report**

CAA Contact Information

- **Steve Schenk**
  - Director, Advanced Concepts
  - Comtech AeroAstro, Inc.
  - 8100 South Park Way, Unit A-9
  - Littleton, CO 80120
  - PH: (480) 390-1171
  - E-Mail: steve.schenk@aeroastro.com
- **Stanley O. Kennedy, Jr.**
  - Vice President and General Manager Programs
  - Comtech AeroAstro, Inc.
  - 8100 SouthPark Way, Unit A-9
  - Littleton, Colorado 80120
  - (cell) 303.815.7343 - Primary
  - (work) 303.798.2121 ext. 311
  - (fax) 303.942.3742
  - Email: stanley.kennedy@aeroastro.com

Summary

- **Thank you for your time and opportunity to share our PnP TO1 findings/conclusions**

- **Questions/Comments????**