AUTONOMOUS FLIGHT SAFETY SYSTEM

A Prototype Development Project of Goddard Space Flight Center's Wallops Flight Facility and Kennedy Space Center

Presented by
James Simpson
NASA, Kennedy Space Center
Email: james.c.simpson@nasa.gov
Phone: (321) 867-6937

Definition

The Autonomous Flight Safety System (AFSS) is an independent self-contained subsystem mounted onboard a launch vehicle.

AFSS has been developed by and is owned by the US Government

Autonomously makes flight termination / destruct decisions using configurable software-based rules implemented on redundant flight processors using data from redundant GPS/IMU navigation sensors

- AFSS implements rules determined by the appropriate Range Safety officials

Applications

- Primary or back-up system for Range Safety Operations
- Crew advisory system for human space flights
- Training tool for traditional human-based flight termination systems

AFSS Advantages

- Global coverage
- Decreased need for ground-based assets
- Increased launch responsiveness

Motivation and History

"The Future Management and Use of the U.S Space Launch Bases and Ranges" by the Office of Science and Technology Policy and National Security Council, 2/8/2000, Recommendation #6

...the Air Force and NASA should develop a plan to examine, explore, and proceed with next-generation range technology development and demonstration...for reusable and expendable launch vehicles.

Phase 1, FY00 Contractor R&D Feasibility Demonstration

- Very limited subset of flight algorithms/destruct rules on PC

Phase 2, FY02 Contractor Bench Prototype with Simulation Testing

- Limited set of safety rules on PowerPC, VME bus, VxWorks
- Simulated launch scenarios using 2 Ashtech G-12 GPS receivers

Phase 3, FY2003-2009 NASA KSC/WFF project

- Goal is a flight qualifiable system
- Design and test to more rigorous requirements with improved algorithms
- Redundancy management
- More extensive simulation and flight testing

Key Concepts

- AFSS is a primarily a smart software system. Use commercial hardware whenever possible.
- Design to known requirements and take best guess at satisfying new requirements: RCC-319, RCC-324, AFSPCMAN 91-710, NASA-STD-8719.13B, NASA-STD-8739.8, Internal ConOps, Project Plan, etc.
- Simulations necessary for testing, debugging and certification.
- Configuration file contains mission-specific flight rules.
- Telemetry preferred for post-flight analysis.
- Simple instantaneous vacuum impact point is not enough for safety decisions.

Summary of Key Design Policies

- Independence-from-vehicle systems as much as practically possible
- Configurable hardware architecture (fixed for a specific vehicle)
- Configurable mission rules (fixed for a specific flight profile)
- NAV sensor redundancy management performed in software
- Redundancy management provides for graceful degradation as sensors and processors fail (within constraints set by Range Authorities)
- Flight Processor/Command Function redundancy management performed in hardware via redundant CSLIC architecture
- Processor-to-processor communications minimized
- Mission rules evaluated against one selected navigation solution
- Majority voting on ARM/FIRE with tie resulting in function
- AFSS application must generate a square-wave pulse train monitored by a circuit independent of processor

Core Simulation Set

A set of 20 core simulations for two different vehicles is used to test and validate the AFSS rules.

Vehicle 1 Wallops Express. A theoretical rocket composed of a Peacekeeper first stage and a Pegasus upper stage.

Vehicle 2 Kodiak Athena Star.

Nominal trajectory	No pitch-over
Stage-1 hang-fire	IIP Violations
Loss of all data at T+0	Loss of data-green time violation
Pitch over shoulder	Tracking solutions diverge
Obvious erratic flight	No fairing separation
Tumble turn	Fails to make orbit gate
No stage 2 or stage 3 ignition	Flight elevation limits

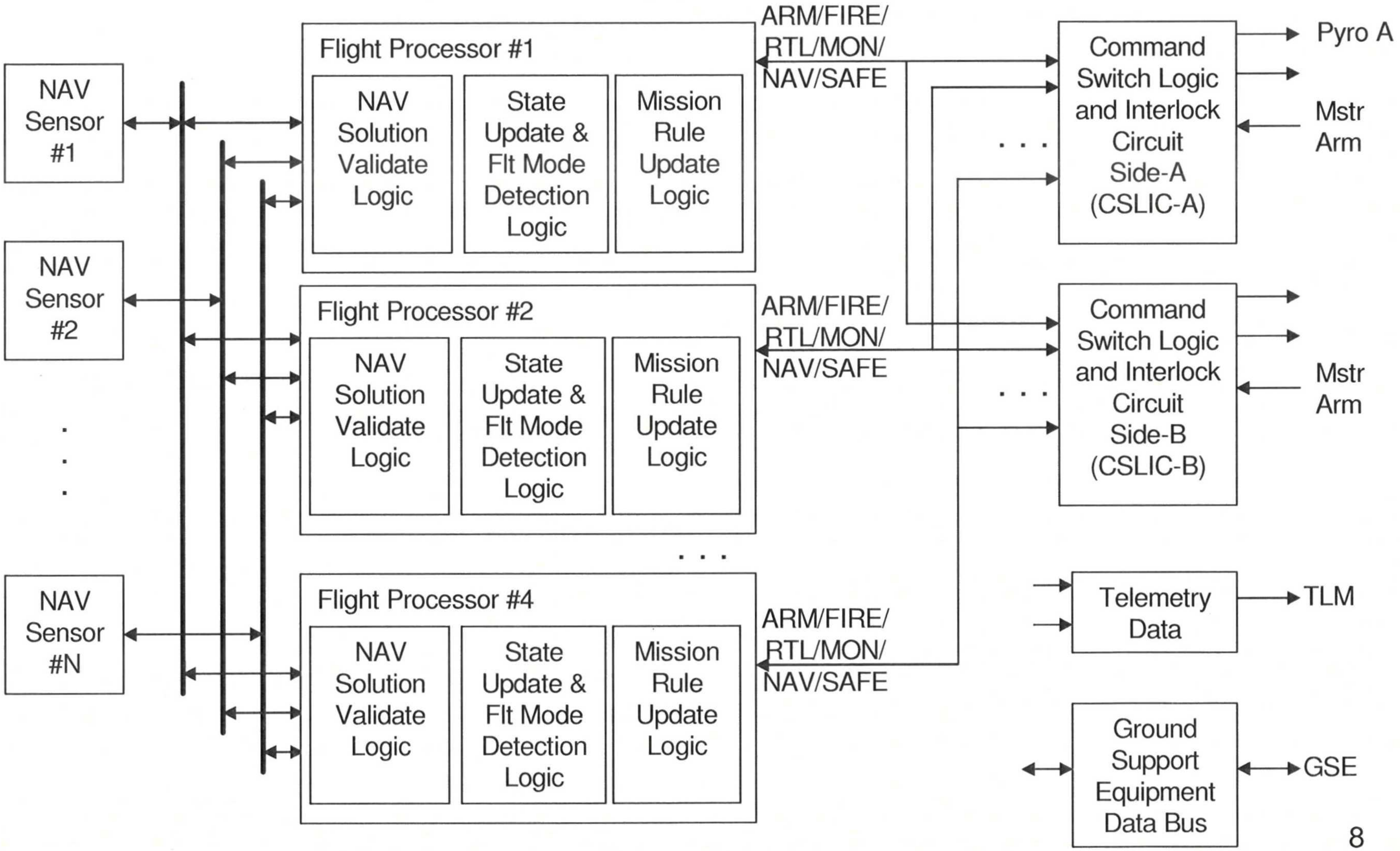
AFSS Mission Rules

- **Parameter Threshold Violation** – a trajectory value exceeds an allowed limit
  - Rocket stage ignition and burnout detection
- **Physical Boundary Violation** – present position or Instantaneous Impact Point (IIP) is out of a corridor or in an exclusion zone
- **Gate Rule**
  - **Two-Point Gate Rule** – determines if a current position or IIP has crossed a gate formed by two points
  - **Moving Gate Rule** – determines if the current position or IIP is in front of or behind a moving two-point gate
- **Green-Time Rule** – determines how long the rocket can safely fly without receiving valid updated tracking data

All mission rules can be dependent upon other mission rules.

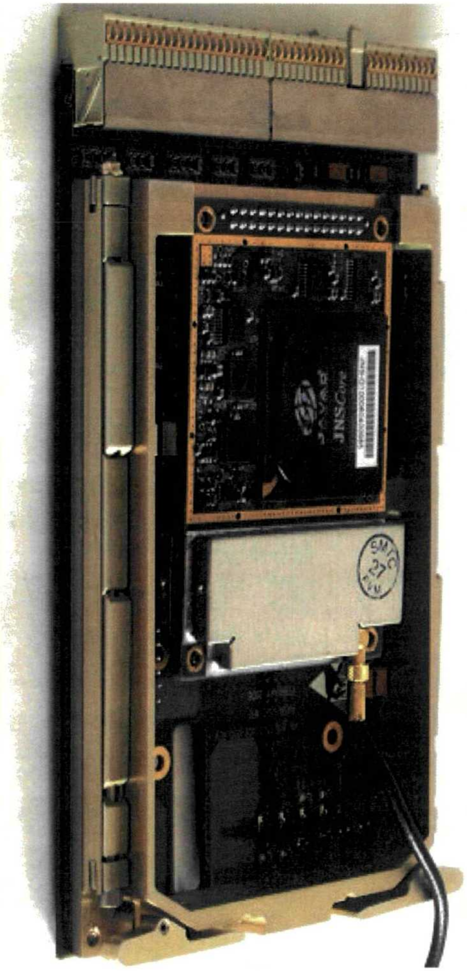
A rule violation does not need to result in a flight termination action.

Final Hardware Design


NAV Sensor #1
NAV Sensor #2
. . .
NAV Sensor #N
Flight Processor #1
NAV Solution Validate Logic
State Update & Flt Mode Detection Logic
Mission Rule Update Logic
Flight Processor #2
NAV Solution Validate Logic
State Update & Flt Mode Detection Logic
Mission Rule Update Logic
. . .
Flight Processor #4
NAV Solution Validate Logic
State Update & Flt Mode Detection Logic
Mission Rule Update Logic
ARM/FIRE/ RTL/MON/ NAV/SAFE
ARM/FIRE/ RTL/MON/ NAV/SAFE
ARM/FIRE/ RTL/MON/ NAV/SAFE
Command Switch Logic and Interlock Circuit Side-A (CSLIC-A)
Pyro A
Mstr Arm
Command Switch Logic and Interlock Circuit Side-B (CSLIC-B)
Mstr Arm
Telemetry Data
TLM
Ground Support Equipment Data Bus
GSE

AFSS CSLIC Overview

- Traditional ARM then FIRE destruct command sequence
- One master firing circuit with four inhibits in line with initiator during normal ground operations
- No (known) single point failures that could produce inadvertent firing
- Multiple single point logic gate failures that could inhibit FIRE command – two CSLIC units in parallel required for total system compliance to RCC319
- Majority voting performed in hardware to activate FIRE
- Unanimous 'voting' performed in hardware for RTL
- Continued use of redundant/parallel CRD and ADS must be supported external to AFSS
- CSLIC is the only custom hardware used by AFSS.



Vehicle Tests

Feb. 3, 2005, van test Kennedy Space Center industrial area

- MIP 405 computer, Javad JNS-100 GPS receiver, roof-mounted commercial GPS antenna, battery pack, laptop computer for monitor and control
- Tested Parameter Thresholds Violation (speed limit), present position boundary, exit gate
- Successful test
- Lessons learned on ignition/staging events and timing tolerance to compensate for multitasking processing delays

Sept. 27, 2005, single engine plane near Kennedy Space Center

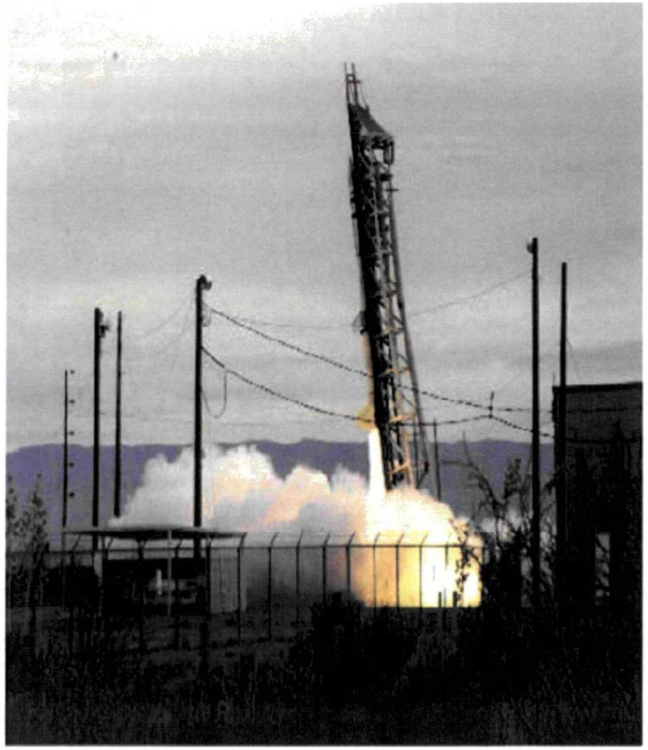
- MIP 405 computer, Javad JNS 100 GPS receiver, dash-mounted commercial GPS antenna, battery pack, laptop computer for monitor and control
- Tested present position and IIP boundaries, moving and exit gates, green time
- Successful test, system performed as expected

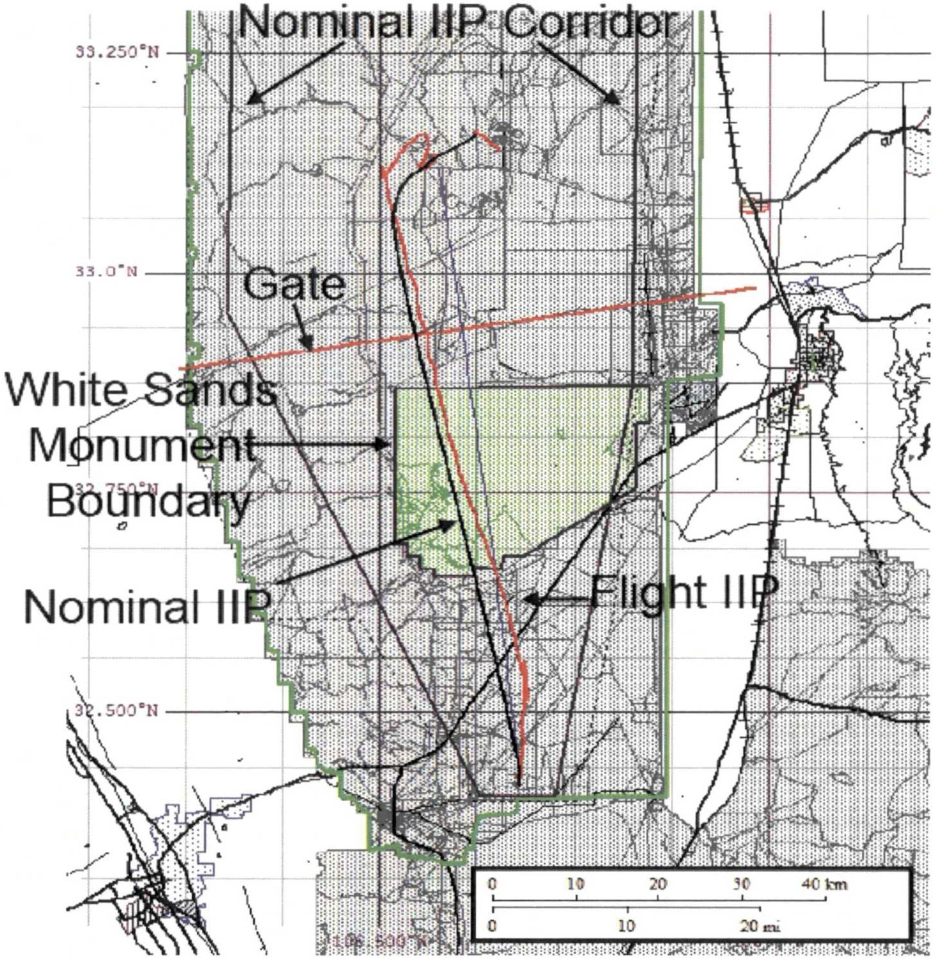
First Rocket Test, Test Article #1

Apr.6, 2006, Modified Terrier Orion sounding rocket at WSMR

- Internal Javad JNS100 and external Ashtech G12 GPS receivers, skin-mounted wraparound GPS antenna, two MIP405 single-board computers, payload power
- Data recorded onboard and sent via vehicle telemetry to the launch head
- Two sets of flight rules—one for each processor. One nominal, one non-nominal
- Environmental testing to rocket specifications
- Prelaunch testing included loading/verifying the application and configuration files, simulated sensor data
- All flight rules performed as expected
- Ashtech G12 receivers lost lock at ignition and did not reacquire during flight
- Flash memory hardware problem on one processor but data was in telemetry

Test Article #1, Test Corridor



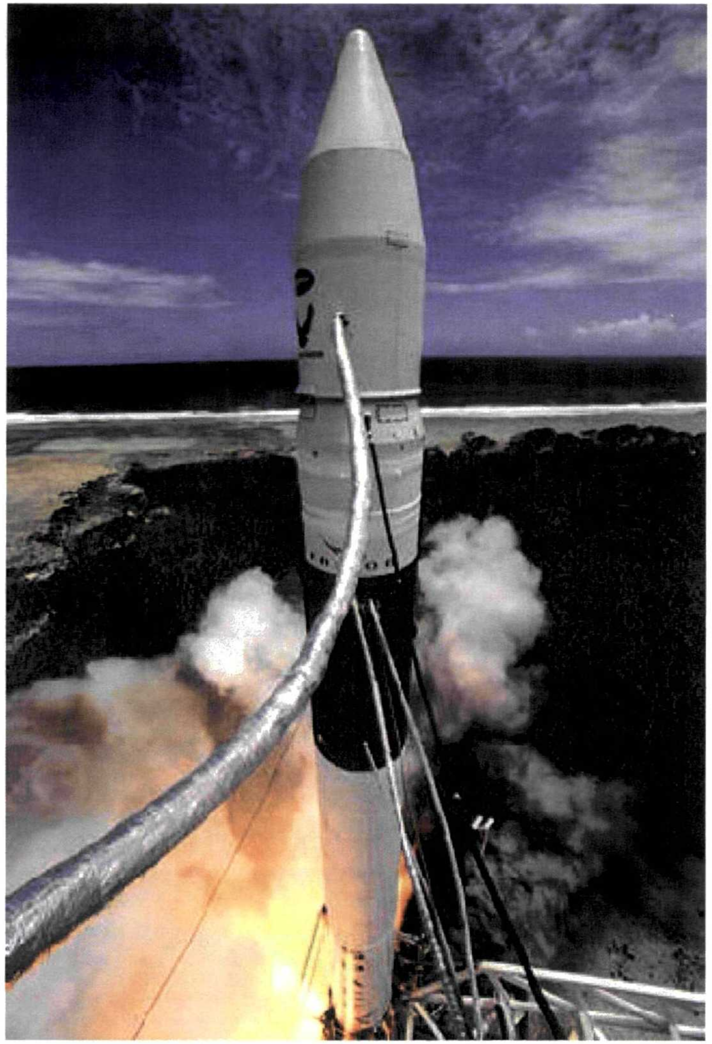


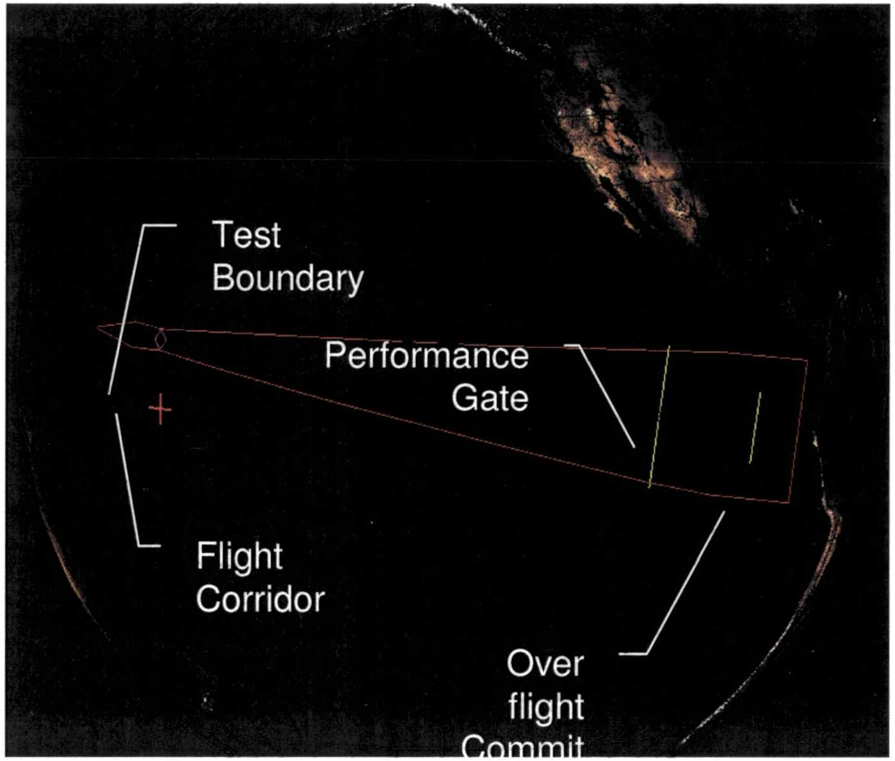
Second Rocket Test, Test Article #2

March 21, 2007, SpaceX Falcon 1 at Reagan Test Site

- Internal and external Javad JNS100 receivers, single skin-mounted patch GPS antenna, two Radstone IMP2A flight processors, custom-designed and built voting circuit, payload power
- Data sent via vehicle telemetry to the launch head
- Same set of flight rules for both processors
  - Test boundary rule to artificially produce a destruct condition with a nominal trajectory
- More extensive testing of Concept of Operations
  - Vehicle integration and test, range integration and test flow, countdown operations, vehicle launch and flight operations, post-boost system safing
- Both processors properly detected hang fire and lift-off
- Anomaly in externally housed GPS data caused early spurious detection of stage-1 burnout and stage-2 ignition events on one flight processor
- Both processors correctly issued and safed ARM/FIRE commands when flying into and out of planned IIP exclusion zone
- Both processors issued ARM/FIRE commands due to a violation of a moving gate rule set up to catch erratic flight from in-plane vehicle failures
- Both GPS receivers maintained navigation solution throughout flight

Test Article #2, Test Corridor





Upcoming Test Article #3

February 2010, sounding rocket at WFF

- Loosely-coupled GPS/IMU Solution
  - Kalman Filtered Javad 100 GPS receiver and a Honeywell HG 1700 IMU
- Backplane redesign
  - Redesigned backplane and improved processors
- Software Upgrades
  - Include additional coding. Safing commands will be included and pre-launch test code has been upgraded.
- Simulated FTS Circuit
  - Simulate actual voltage and current requirements.
- Graphical User Interface
  - The ground support equipment will have a modified graphical user interface to relieve operators from manual commands
- Low Cost TDRSS Transceiver—first test in receive mode

What's Next?

We believe we have shown that AFSS is viable.

Our ultimate goal is commercialization or transfer to industry or government agencies as government-furnished software with the NASA team maintaining an advisory role.

Need to finish:

- IVV
- Software standards
- Orbital launch
- Miniaturized hardware if possible
- Better requirements–AFSS is a new paradigm and it needs to "emulate a Range Safety officer's mind". The current requirements do not exist for this.
- NASA will finish its development in 2-3 years with adequate funding and support.