GPM Timeline Inhibits for I&T Processing

Shirley Dion
GPM Safety/ASRC
Agenda

• Scope of Discussion
• Motivation for Creation of the Tool
• Definition of Terms
• GPM Overview
• Tool Development Process Steps
  – Step 1 Define Inhibits and controls
  – Step 2 Define I&T testing
  – Step 3 Determine inhibit status during each test
  – Step 4 Determine software criticality
• Unique Hazard Report Controls and Verifications for Software
• Summary
Scope of Discussion

Development of S/C inhibit tracking for GPM during I&T at GSFC and at the range
Motivation for Creation of the Tool

1. How and why did this come up on GPM?
2. Why was developing this process/tool important?
Definition of Terms

1. Terms
   – Inhibits
   – Controls
   – Critical Software Commands/Controls
   – Fault (Failure) tolerance
   – Design for Minimum Risk
1. **Inhibits** An independent and verifiable mechanical and/or electrical device that prevents a hazardous event from occurring; the device has direct control and is not the monitor of such a device. (NPR 8715.7A) (Green circles)

2. **Controls** Hardware or software that affects the operation of an inhibit. (Shirley’s definition) (Tan circles)

3. **Critical Software commands** – A command that either removes (and/or activates) a safety inhibit or creates a hazardous condition. (NPR 8715.3C, App B) (yellow arrows)

4. **Fault (Failure) tolerance** The ability to sustain a certain number of failures and still retain capability. (NPR 8705.2B, NPR 8715.3C App B)

5. **Design for Minimum Risk** Structural members, pressure vessels, pressurized lines/valves, pyrotechnics, material compatibility, some mechanisms, flammability, etc., where fault tolerance design is not practically possible, shall be controlled by design standards or other established organizations (design using robust design margins and safety factors)
GPM Overview

1. What does GPM do?
2. How many instruments are there?
GPM Overview
GPM Overview

Instruments in Action
GPM Overview

What are the hazards?
GPM Overview

• What are the hazards?
  1 Deployables
    • HGAS – High Gain Antenna System
    • SA Solar arrays
    • GMI Instrument (GPM Microwave Imager)
  2 RF
    • S/C transmitter
    • DPR (Duel Precipitation Radar) 2 Radars at GHZ 13ish 35 ish
  3 Fuel System
    • Propulsion
GPM Overview

• What are the hazards?

1 Deployables
  • HGAS – High Gain Antenna System
  • SA Solar arrays
  • GMI Instrument (GPM Microwave Imager)

2 RF
  • S/C transmitter
  • DPR (Duel Precipitation Radar) 2 Radars at GHZ 13ish 35 ish

3 Fuel System
  • Propulsion
Agenda

- Scope of Discussion
- Motivation for Creation of the Tool
- Definition of Terms
- GPM Overview
- Tool Development Process Steps
  - Step 1 Define Inhibits and controls
  - Step 2 Define I&T testing
  - Step 3 Determine inhibit status during each test
  - Step 4 Determine software criticality
- Unique Hazard Report Controls and Verifications for Software
- Summary
### Tool Development Process Steps

#### Step 1: Define inhibits and controls

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>Inhibit</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Step 2: Define I&T Testing

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>Inhibit</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Step 3: Determine inhibit status during each test

- [ ] Determine inhibit status during each test

#### Step 4: Determine software criticality

- [ ] Determine software criticality
Step 1 Define inhibits and controls

HGAS stowed

LRM- Launch Restraint Mechanism
HGAS-High Gain Antenna System
Step 1 Define inhibits and controls

HGAS Electrical Inhibits

DFU - Deployment Firing Unit
PSE - Power Supply Electronics
NEA - Non-Explosive Actuators
Step 1 Define inhibits and controls

HGAS Inhibits and Controls

- HGAS – High Gain Antenna System
  - Mechanically (3) Deployment hinges
  - Electrically it is 2-fault tolerant for each hinge
- Inhibits include:
  1. FET in Power Systems Electronics
  2. 1st FET in Deployment Firing Unit
  3. 2nd FET in Deployment Firing Unit
  4. Power relay switch off
  5. Safety strap/tie
  6. Arming plug removed
  7. NEA’s are either removed or bypassed
  8. Keepout zone- (Not an inhibits but is a control)
Step 1: Define inhibits and controls

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>Trans</th>
<th>Inhibit</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>HGAS Deploy</td>
<td>Trans</td>
<td>Inhibit</td>
<td>Control</td>
</tr>
<tr>
<td>HGAS Deploy</td>
<td>Trans</td>
<td>Inhibit</td>
<td>Control</td>
</tr>
</tbody>
</table>

**Table: Inhibit Controls Matrix**

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>Trans</th>
<th>Inhibit</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>HGAS Deploy</td>
<td>Trans</td>
<td>Inhibit</td>
<td>Control</td>
</tr>
<tr>
<td>HGAS Deploy</td>
<td>Trans</td>
<td>Inhibit</td>
<td>Control</td>
</tr>
</tbody>
</table>

**Legend:**
- No inhibit = red
- Inhibit in place = green

**Notes:**
1. FET from TNSC to GSFC via interface.
2. DFU Power Source (arm) via interface.
3. DFU Power Source (fire) via interface.
4. Safety input.
5. Annunciation checked.
6. NEA removed.
7. S/C off.
8. Emergency input.

**ASRC Federal**

**Technical Services**
# Step 1 Define inhibits and controls

<table>
<thead>
<tr>
<th>Inhibits</th>
<th>Inhibit Type</th>
<th>Inhibit Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PSE</td>
<td>FET</td>
<td>FSW from C&amp;DH SC processor triggered by LV separation switch or ground command (same as SA)</td>
</tr>
<tr>
<td>2 DFU Power Source (arm)</td>
<td>FET</td>
<td>Ground Command over 1553 bus to DFU.</td>
</tr>
<tr>
<td>3 DFU Power Source (fire)</td>
<td>FET</td>
<td>Ground Command over 1553 bus to DFU.</td>
</tr>
<tr>
<td>4 Safety strap</td>
<td>restraint</td>
<td>I&amp;T procedure</td>
</tr>
<tr>
<td>5 Arming plug removed (test plug or safety cap installed)</td>
<td>plug</td>
<td>I&amp;T procedure</td>
</tr>
<tr>
<td>6 NEA removed/bypassed</td>
<td>disconnected</td>
<td>I&amp;T procedure</td>
</tr>
<tr>
<td>7 S/C off</td>
<td>relay</td>
<td>Battery and GSE power supply</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keepout zone (restricted access)</td>
<td>barrier</td>
<td>I&amp;T procedure</td>
</tr>
</tbody>
</table>
Step 1 Define inhibits and controls

Solar Array stowed

LRM- Launch Restraint Mechanism
Step1 Define inhibits and controls

Solar Array Electrical Inhibits

DFU-Deployment Firing Unit
PSE- Power Supply Electronics
NEA-Non-Explosive Actuators
Step 1: Define inhibits and controls

Solar Array Inhibits and Controls

- Solar array (red is the difference with HGAS)
  - Mechanically (5) Deployment hinges
  - Electrically it is 2-fault tolerant for each hinge
  - Inhibits include:
    1. FET in Power Systems Electronics
    2. 1st FET in Deployment Firing Unit
    3. 2nd FET in Deployment Firing Unit
    4. Power relay switch off
    5. Tether/pin
    6. Arming plug removed
    7. NEA’s are either removed or by-passed
    8. Keepout zone
### Step 2 Define I&T testing

<table>
<thead>
<tr>
<th>I&amp;T Phases at TnSC</th>
<th>Post Launch</th>
<th>I&amp;T Phases at GSFC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### I&T Procedures

<table>
<thead>
<tr>
<th>No Inhibit = red</th>
<th>Inhibit in place = green</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inhibit in place = green</td>
</tr>
<tr>
<td>2</td>
<td>Safety override = green</td>
</tr>
<tr>
<td>3</td>
<td>Safety override = green</td>
</tr>
<tr>
<td>4</td>
<td>Safety override = green</td>
</tr>
</tbody>
</table>

**Notes:**
- Inhibit in place = green
- Safety override = green
- No inhibit = red
Step 2 Define I&T testing

- **Performance Tests**
  - CPT Comprehensive Performance Test
  - Functional test
  - Aliveness test
  - Alignment test
  - Mass properties
  - Magnetic Survey
  - End-to-End/MOC test
  - Deployment test and stow
  - Walkout test and stow

- **Environmental Testing**
  - Thermal Vacuum/Thermal Balance
  - EMI tests
  - Vibration tests
  - Acoustics test
  - Shock Separation test
Step 2 Define I&T testing

Deployable circuitry during testing

1. Top figure is the operational configuration of the NEA in place with 3 inhibits and arming plug. Functional test.

2. Middle figure is the Observatory functional test. Power to the box. For deployables, arming plug removed and NEA simulator used so NEA’s won’t fire.

3. Bottom is the CPT test. (comprehensive performance test). Arming plug in place but NEA’s electrically disconnected.
Step 2 Define I&T testing

• Performance Tests
  – CPT Comprehensive Performance Test
  – Aliveness test
  – Functional test
  – Alignment test
  – Mass properties
  – Magnetic Survey
  – End-to-End/MOC test
  – Deployment test
  – Walkout test

• Environmental testing
  – Thermal
  – Vacuum/Thermal Balance
  – EMI tests
  – Signal injection (DPR specialty test)
  – Vibration tests
  – Acoustics test
  – Shock Separation test
Step 2 Define I&T testing – Test order on GPM Timeline Tool

1 Mechanical Integration for each subsystem
2 Deploy HGAS, Gimbal Func. Test and stow
3 HGAS Align
4 HGAS Walk-out
5 Pre-inst Mag Survey
6 CPT and actuator tests
7 HGAS Walk-out
8 Mag Survey
9 CPT (baseline OBS)
10 HGAS Walk-out
11 TV, Therm Bal, CPT, Miss Sim #1
12 Aliveness Test
13 MOC Int #1, CTV, E-T-E, & miss sim #2 Tests
14 HGAS Walk-out
15 OBS Aliveness & EMI
16 S/A Deploy
17 HGAS Walk-out
18 OBS Functional Test
19 OBS Aliveness Test
20 Limited OBS Functional Test
21 Mass Properties
22 Vibration & Aliveness Test
23 Acoustics & Aliveness Test
24 Shock Separation & Aliveness Test
25 limited Functional Test
26 Deploy HGAS
27 E-T-E #2
28 Solar Array Deploy
29 HGAS Walk-out
30 Magnetic Survey
31 CPT
32 E-T-E#3 Test, Mission Sim #3
33 Solar Array Deploy
34 STA2 LS Dry Run CPT
35 OBS LS/ PAD Functional Test
36 Mass Properties #2
37 Transfer to Launch Site
38 Alignment test
39 Aliveness test
40 Contingency HGAS deploy test
41 Contingency Solar Array deploy test
42 CPT
43 MOC I/F #2, E-T-E #4, Mis Sim#4 Test
44 Fueling
45 Encapsulation
46 Limited Functional Test
47 Launch
48 Fairing Separation
49 Launch Vehicle Separation
Step 3 Determine Inhibit status During Each Test – High Gain Antenna Deploy

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>I&amp;T Phases at TnSC</th>
<th>I&amp;T Phases at GSFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inhibit</td>
<td>antigen</td>
<td>antigen</td>
</tr>
<tr>
<td>PSE</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>DFU Power Source (arm)</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>DFU Power Source (fire)</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Safety stop</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Amming plug removed (no plug or safety cap inserted)</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>NEA removed &amp; bypassed</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>S/C off</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Selectivity bar (restricted)</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

- No inhibit = red
- Inhibit in place = green
Step 3 Determine Inhibit status During Each Test - Solar Array Deployment

<table>
<thead>
<tr>
<th>Solar Array Deploy</th>
<th>I&amp;T Phases at GSFC</th>
<th>Trans</th>
<th>I&amp;T Phases at TnSC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inhibit</strong></td>
<td><strong>Control</strong></td>
<td><strong>I&amp;T Phases at GSFC</strong></td>
<td><strong>Trans</strong></td>
<td><strong>I&amp;T Phases at TnSC</strong></td>
</tr>
<tr>
<td>PSE to deployment</td>
<td>FSW from C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DFU Power Source (arm)</td>
<td>FSW from C&amp;DH SC processor triggered by LV separation breakwires or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DFU Power Source (fire)</td>
<td>FSW from C&amp;DH SC processor triggered by LV separation breakwires or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>tether pin</td>
<td>I&amp;T procedure</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Arming plug removed (test plug or safety cap installed)</td>
<td>I&amp;T procedure</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>NEA removed/ bypassed</td>
<td>I&amp;T procedure</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>S/C off</td>
<td>Battery and GSE power supply</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td><strong>I&amp;T Phases at GSFC</strong></td>
<td><strong>Trans</strong></td>
<td><strong>I&amp;T Phases at TnSC</strong></td>
<td><strong>Post Launch</strong></td>
</tr>
<tr>
<td>Keepout zone (restricted access)</td>
<td>I&amp;T procedure</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Inhibit status:
- No inhibit = red
- Inhibit in place = green
# Step 4 Determine Software Criticality - HGAS Deployment

<table>
<thead>
<tr>
<th>HGAS Deploy</th>
<th>I&amp;T Phases at TnSC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HGAS</th>
<th>ID</th>
<th>Name</th>
<th>I&amp;T Phases at TnSC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## HGAS Deploy

<table>
<thead>
<tr>
<th>PSE</th>
<th>DFU Power Source (dfu)</th>
<th>Safety strap</th>
<th>Arming plug removed</th>
<th>WEA removed</th>
<th>S/C off</th>
<th>Request zone cleared</th>
<th>Safety Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### I&T Phases at TnSC

1. **PSE**
   - SC processor triggered by LV separation switch or ground command
2. **DFU Power Source (dfu)**
   - Ground Command over 1553 bus
3. **Safety strap**
4. **Arming plug removed (test plug or safety cap installed)**
5. **WEA removed (suppressed)**
6. **S/C off**

### Software (SW) Safety Support

- Software (SW) Safety Support to certify all SW verifications are complete

---

**Software Controller (SC) operational for all functions (controlled)***

---

**Inhibit in place (green)**

---

**No inhibit= red**

---

**Safety Support to certify all SW verifications are complete**

---

**Software Controller (SC) operational for all functions (controlled)**

---

**Software Controller (SC) operational for all functions (controlled)**
## Step 4 Determine Software Criticality - Solar Array Deployment

### Solar Array Deploy

<table>
<thead>
<tr>
<th>Inhibits</th>
<th>I&amp;T Phases at GSFC</th>
<th>I&amp;T Phases at TnSC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSE to deployment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFU Power Source (arm)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFU Power Source (fire)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Isotherm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arming plug removed (test plug or safety cap installed)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEA removed/bypassed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIC off</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keepout zone (restricted access)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software safety Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Inhibits

<table>
<thead>
<tr>
<th>Inhibit Type</th>
<th>Inhibit</th>
<th>Control 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSW</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td></td>
</tr>
<tr>
<td>DFU Power</td>
<td>Source (arm)</td>
<td></td>
</tr>
<tr>
<td>DFU Power</td>
<td>Source (fire)</td>
<td></td>
</tr>
<tr>
<td>I&amp;T procedure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I&amp;T procedure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I&amp;T procedure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery and GSE power supply</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### I&T Phases at GSFC

<table>
<thead>
<tr>
<th>Phase</th>
<th>FET</th>
<th>Mag Survey</th>
<th>CPT</th>
<th>LV Tests</th>
<th>Bal</th>
<th>Alien Tests</th>
<th>Extern Test</th>
<th>EMF</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FSW</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>DFU Power Source (arm)</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>DFU Power Source (fire)</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### I&T Phases at TnSC

<table>
<thead>
<tr>
<th>Phase</th>
<th>FET</th>
<th>Mag Survey</th>
<th>CPT</th>
<th>LV Tests</th>
<th>Bal</th>
<th>Alien Tests</th>
<th>Extern Test</th>
<th>EMF</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FSW</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>DFU Power Source (arm)</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>DFU Power Source (fire)</td>
<td>From C&amp;DH SC processor triggered by LV separation switch or ground command</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Post Launch

<table>
<thead>
<tr>
<th>Phase</th>
<th>FET</th>
<th>Mag Survey</th>
<th>CPT</th>
<th>LV Tests</th>
<th>Bal</th>
<th>Alien Tests</th>
<th>Extern Test</th>
<th>EMF</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
<th>PSE &amp; Alle</th>
<th>AC &amp; Alle</th>
</tr>
</thead>
</table>
### Step 4 Determine Software Criticality - GMI Deployment

<table>
<thead>
<tr>
<th>Step</th>
<th>I&amp;T Phases at TnSC</th>
<th>I&amp;T Phases at GSFC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- No Inhibit= red
- Inhibit in place= green
- Software Control is in place and Critical (no other physical inhibits in place) = green with X
- Software Control is in place and Critical (no other physical inhibits in place) with another physical inhibit in place = green with slash
- Software Control is in place and Critical (no other physical inhibits in place) with another physical inhibit in place = grey
### Step 4 Determine Software Criticality - S/C Transmitter Activation

#### S/C RF Transmitters

<table>
<thead>
<tr>
<th>Inhibit</th>
<th>Inhibit Control for Transmitter B Omni</th>
<th>Inhibit Control for Transmitter A N &amp; B</th>
<th>Init at</th>
<th>I&amp;T Phases at GSFC</th>
<th>I&amp;T Phases at TNSC</th>
<th>Post Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSE 1 to Transmitter</td>
<td>FSW from C&amp;DH SC processor over 1553 bus triggered by fairing breakwires plus timer</td>
<td>Ground Command over 1553 bus</td>
<td>N/A</td>
<td>Red</td>
<td>Green</td>
<td>Gray</td>
</tr>
<tr>
<td>PSE 2 to Transmitter</td>
<td>FSW from C&amp;DH SC processor over 1553 bus triggered by fairing breakwires plus timer</td>
<td>Ground Command over 1553 bus</td>
<td>N/A</td>
<td>Red</td>
<td>Green</td>
<td>Gray</td>
</tr>
<tr>
<td>Transponder</td>
<td>FPGA from C&amp;DH via 422 initiated by FSW triggered by T-01 or T-02 breakwires plus timer</td>
<td>Ground Command over 1553 bus</td>
<td>N/A</td>
<td>Red</td>
<td>Green</td>
<td>Gray</td>
</tr>
<tr>
<td>Hat couplers</td>
<td>I&amp;T procedure</td>
<td>I&amp;T procedure</td>
<td>N/A</td>
<td>Red</td>
<td>Green</td>
<td>Gray</td>
</tr>
<tr>
<td>S/C off</td>
<td>Battery and GSE power supply</td>
<td>Battery and GSE power supply</td>
<td>N/A</td>
<td>Red</td>
<td>Green</td>
<td>Gray</td>
</tr>
</tbody>
</table>

#### Software (SW) Safety Support

- No software safety assessment
- Supporting Hazard Inhibits/Contri
- Software Control is in place (and another physical inhibit in place) = green with slash
- Software Control is in place and critical (no other physical inhibit in place) = green with X
- No software control (S/C unpowered or inhibit removed) = gray

#### Control

- Keepout zone
- Software (SW) Safety Support to certify all SW verifications are complete

#### Software Safety Assessment

- No inhibit = red
- Inhibit in place = green

---

**ASRC FEDERAL**

---

**ARES TECHNICAL SERVICES**
## Step 4 Determine Software Criticality - DPR Radar Activation

RF (Ku PR and/or Ka PR)

<table>
<thead>
<tr>
<th>Inhibits</th>
<th>Inhibit Type</th>
<th>Inhibit Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/C PSE 1</td>
<td>FET1</td>
<td>GRF off from C&amp;H DC processor</td>
</tr>
<tr>
<td>S/C PSE 1</td>
<td>FET2</td>
<td>GRF off from C&amp;H DC processor</td>
</tr>
<tr>
<td>DPR internal power</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>SSPA</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>Test Div/Comb</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>RF absorber panel</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>RF detector chn</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>S/C off</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>DPR powered off</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>Control</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
<tr>
<td>Software safety Assessment</td>
<td>GRF</td>
<td>GRF off from instrument controller to each monitor</td>
</tr>
</tbody>
</table>

### Inhibit Control

- **No inhibit (red)**
- **Inhibit in place (green)**

### Software Control

- Software Control in place and another physical inhibit in place
- Software Control in place and another physical inhibit in place
- No Software Control

**Note:** The table and diagram above illustrate the various inhibits and controls in place for the DPR Radar Activation process. Each inhibit has a corresponding control mechanism to ensure system safety and functionality during various phases of the mission.

**Image:** ASRC Federal

**Page:** 34
### Step 4 Determine Software Criticality - Propulsion Hydrazine Release

#### Propulsion Inhibits

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PSE PROP I/O</td>
<td>FET</td>
<td>Ground command to PSE</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>MACE A power source (Latch and Thruster)</td>
<td>FET</td>
<td>Ground command to PSE for MACE A PROP I/O FPGA 1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>3</td>
<td>MACE A return (Latch and Thruster)</td>
<td>FET</td>
<td>Ground command to PSE for MACE A PROP I/O FPGA 2</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>S/C off</td>
<td>Battery and GSE power supply</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

#### Control

- **Keep out zone (operators in SCAPE)**: Barrier I&T procedure

- **Software safety Assessment**: Software (SW) Safety Support to certify all SW verifications are complete

- **No inhibit= red**

- **Inhibit in place= green**

- **Software Control in place (and another physical inhibit in place)= green with slash**

- **Software Control in place and Critical (no other physical inhibits in place) = green with X**

- **No Software Control (S/C unpowered or inhibits removed)= grey**
Unique Hazard Report Controls for Software

Inadvertent Commanding via Ground or Flight Software

1. Safety critical commands and telemetry database for the C&DH flight software and ground systems loaded with configured database (ASIST) operates properly.

2. Restrict the use of safety critical software that removes deployment inhibits commands to one per flight command sequence (script).

3. NASA software safety will review build test plans and results used to test the loaded flight image to ensure full coverage of safety critical functions.

4. The flight software will require three independent “signals” following independent software and hardware paths to remove the three independent safety inhibits.

5. Monitor health and safety of flight software system. The safety critical functionality is listed below:
   a) Hardware memory scrubbing
   b) Routine which detects faulted tasks (Health and Safety task)
   c) Hardware which detects faulted tasks (Health and Safety task)
   d) Flight processor watchdog timer
   e) Background checksum
   f) Verify initial flight command sequence (i.e. Tables)

6. Prohibit safety critical commands from the ground system from post encapsulation through planned L/V separation. (Flight Rule).

7. The on board memory will be protected against memory errors by incorporating a memory scrubbing routine that will correct single bit errors (via hardware) and report multi bit errors.

8. The on board flight software will require double checking telemetry values (persistency check) before executing on board scripts (capable of removing safety inhibits).

9. If the redundant processor is activated it boots using a certified flight image (flight SW image and tables).

10. NASA will provide independent analyses of flight code.

Controls developed by C. Rogers of EFSI
Agenda

- Scope of Discussion
- Motivation for Creation of the Tool
- Definition of Terms
- GPM Overview
- Tool Development Process Steps
  - Step 1 Define Inhibits and controls
  - Step 2 Define I&T testing
  - Step 3 Determine inhibit status during each test
  - Step 4 Determine software criticality
- Unique Hazard Report Controls and Verifications for Software
- Summary
Summary

1. I&T is complicated and safety inhibit philosophy can be different from test to test.
2. Software criticality depends on testing’s use of the hardware inhibits.
3. Tool helped Safety bridge a gap of understanding of the I&T testing plans
   - Allowed the safety team to make a more informed decision on use of inhibits and a summary of what needed to be in the WOA’s/procedures. Time savings when reviewing procedures.
   - Provided a communication tool with Systems Engineers and Project Management. Was able to point out inconsistencies, potentials risks and hazards.
4. Tool can be used on other missions for the same purpose.
Questions?
THANK YOU VERY MUCH!!

ありがとうございます

THANK YOU VERY MUCH!!