Distributed Fault Management

Mission Control Center

Spacecraft
- Design Robustness
- Fault Protection

On-board Crew

EVA
MOD flight controllers use system expertise gathered through training, interaction with the hardware, and significant real-time experience to develop nominal plans and procedures to achieve the goals established by the Agency and Programs.

- That knowledge is an agency asset and is also critical to evaluating risk and making effective trades on which failures to develop contingency plans for, either due to the potential mission impact, likelihood, or cost in terms of time and resources.
- Detailed mission development, integration, and planning begins 1 yr before launch, coordinating with Program requirements, customers, and system experts/hardware.
- Validation of plans and procedures are done via testing with hardware and simulators/mock-ups and are certified by MOD as part of the flight readiness process.

**Preparation:**

- Flight controllers certified in real-time operations and their system for emergency safing and basic operations within 18 months. They are then able to operate on-console during quiescent ops, and become specialists with expertise for complex ops, with experience and follow-on training regarding their systems typically completed within another year.
  - This process has been the focus of continuous improvement efforts to streamline and focus.
- Training of the crew for a mission by MOD using our expertise begins approx 9 months before launch.
Fault Management on ISS

- H&S driven from individual subsystem-level health mgmt data, not vehicle-level health state
- C&W data only one “piece of the puzzle” to determine the nature of the failure, and system propagation
- H&S data does not directly provide failure response information, or system impact severity
- Each C&W message has associated procedures for crew or ground execution. Diagnosis within procedures

Subsystems:
- Subsystem A
- Subsystem B
- Subsystem n

C&W Messages:
- C&W data
- Nominal Config:
  - Hear tone(s) and alarm.
  - C&W messages in C&w ALARM

Procedure:
- Determine corresponding WARNING TABLE.
- Look up Warning message (SODF: EMER:
- Address EPS Warning
- Determine Order to Execute
- Determine Procedural Response
- Assess Lab and Node
- Report to MCC.

- CSL
- ONC
- VCC
- CCS
- CCS

- Diagnose
- Respond
- C&W
• Failure of ISS External Thermal Coolant System (ETCS) Loop A Pump Module – provides half of the ISS systems cooling, resulted in immediate loss of 50% of ISS capability
  – Immediate assessment and response (critical to prevent hardware loss):
    • 13 hours of ground commanding to powerdown and reconfigure systems required to achieve a safe state that optimized capability
      – This set of contingency procedures had been developed by MOD and maintained/updated as ISS configuration changed through assembly [preparation]
    • ISS crew – trained by MOD for skills required in contingency ops (installation of jumpers, rack reconfigurations) [expertise]
    • Crew and ground ops choreography trained before launch to allow teams to be able to communicate crisply and effectively and function as a cohesive unit in critical time response situations [experience]
  – Recovery action: MOD team integrated with engineering support and Program management to perform 3 spacewalks and recover full system capability within 17 days of initial failure
    • Initial contingency EVA procedures developed by MOD several years in advance and taken to a state where a real-time team could then develop final procedures based on the actual configuration of the vehicle associated with the specific pump failure [risk assessment and upfront preparation/investment]
    • Plans and procedures required adjustments for robotics support, ammonia line hazards, tool configurations, and system repowering sequences using MOD experts and mission systems (NBL, MCC, ISS simulator) [assets, integration skills, and expertise]
    • Real-time quick responsiveness required well trained flight controllers and expertise to rapidly respond to additional contingencies during the EVA (ammonia quick disconnect failures, EMU suit sensor failures, connector and bolt issues, worksite and tool adjustments) [experience]
Annunciator Matrix and On-board Fault Summary data based on individual conditions or pre-defined “hard-coded” rules

Failures that impact multiple components result in the generation of many seemingly unrelated messages that the crew needs to isolate

Generated alerts are often not indicative of the real failure. E.g. ‘EPS bus undervolt’ failure generated ‘Fuel cell Ph low’
EFT-1 FM Capability Strategy/Groundrules

On-board

- All planned mission events will be automatic
- FDIR should align to planned Orion 2 FDIR to the extent that HW is in place for OFT-1
  - Defer FDIR for which there is no OFT-1 HW
  - Defer all FDIR that does not have associated responses (e.g., system reconfiguration)
  - Defer FDIR intended for crew situational awareness (e.g., C&W)
- FDIR must provide 1FT for mission completion (CM recovery) for credible failure modes as determined by FMEA and System Analysis
  - Where high value and practical to accommodate, FDIR should allow ground to command back to original string – Via approved contingency commands only
  - Fault recovery capability may be allocated to the flight control team for cases where FDIR would be complex and scenario is considered low risk by the FM team (e.g., long time available to respond). Ground commands needed for these cases would be verified
- Uplink commands will be verified for a subset of priority events associated with FCT Fault Response requirements
  - Additional command /manual control capability will be provided for all individual items, but use of these commands will be restricted to “last resort” type scenarios and therefore will have minimal verification
    - Classified commands into 4 categories: CAT 1-3 meet (small set) meet verification criteria above, and CAT 4 require Program authorization prior to uplink.

Flight Control Team (FCT)

- Will monitor automatic events for proper operation
- Manually command/alter events if determined to be needed
- Monitor health of systems as backup to FDIR
- Monitor FDIR response to ensure proper response to first failure
- Manually command events or individual components (verified capability) where 1-failure cases are allocated to the ground
- Manually command events or individual components for multi-failure cases

- Flight Telemetry Maps built to follow the following priorities:
  1. Support In-flight Commanding
  2. Support Anomaly Resolution
  3. Support Gathering of Primary FTO data
  4. Support Gathering of Secondary FTO data

April, 2012
Enhancing Fault Management in the Cockpit

- Cockpit Avionics Upgrade (CAU)
  - Color Coded Messages
  - Revised error message text
    - Describes error in greater detail

- Enhanced Caution & Warning (ECW)
  - Root Cause Analysis
  - Parent-child relationships
  - Message grouping
ECW Scripting Tool

- Developed in Visual Basic
  - Build and save scripts to display C&W Messages
  - Assign Parent Child Relationships
  - Adjust message display timing
  - Depict CRT messages as they would appear in
    - Legacy Shuttle Display
    - CAU Display
    - ECW Display
- Playback Controls to interact with script
Fault Summ

3.2 Coast

- W EPS  Load Sw Card 2 Fail
- W EPS  Htr Cntl Card 3 Fail
- W EPS  Intl Pwr Supply A Fail
- W EPS  AC1 Multi $ Short
- C EPS  AV Bay 1 Sig Pwr Lost

April, 2012
### Fault Log

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEPS</td>
<td>Pwr Bus 2 Volt Hi</td>
<td>214/18:37:57</td>
</tr>
<tr>
<td>CEPS</td>
<td>Batt 5 Temp Hi</td>
<td>214/18:37:52</td>
</tr>
<tr>
<td>WEPS</td>
<td>Cab Air Cntl Pwr Lost</td>
<td>214/18:37:47</td>
</tr>
<tr>
<td>WEPS</td>
<td>Load Sw Card 2 Fail</td>
<td>214/18:37:42</td>
</tr>
<tr>
<td>CEPS</td>
<td>AV Bay 1 Sig Pwr Lost</td>
<td>214/18:37:37</td>
</tr>
<tr>
<td>WEPS</td>
<td>Htr Cntl Card 3 Fail</td>
<td>214/18:37:32</td>
</tr>
<tr>
<td>WEPS</td>
<td>Intl Pwr Supply A Fail</td>
<td>214/18:37:27</td>
</tr>
<tr>
<td>WEPS</td>
<td>AC1 Multi &amp; Short</td>
<td>214/18:37:22</td>
</tr>
</tbody>
</table>

---

*April, 2012*
Electronic procedures are the heart of an effective spacecraft glass cockpit.

Electronic Procedures, by directly interacting with system displays, cue operator actions. These cues greatly reduce workload and errors.
ECW Prototyping