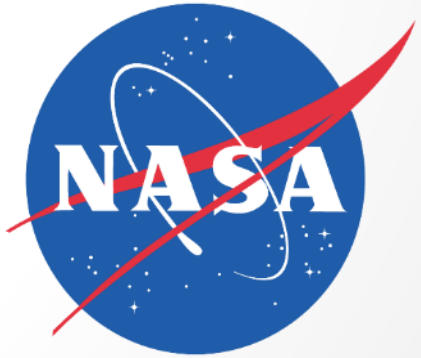
HRP Commanding Lessons Learned

Commanding to HRF Racks

Marc Perry / HRP
ISS Medical Projects (ISSMP)



Objective

- For the benefit of the PD community, highlight why we recently reevaluated how we perform technical tasks on console
- Communicate some of our Concept of Operations practices specific to:
  - Commanding
  - Building and analyzing telemetry displays using payload health and status
  - Redundancy and anomaly resolution responses
- Applicable to:
  - PDs who perform commanding to hardware on ISS
  - PDs who make operational decisions based on telemetry displays
  - PDs who have multiple pieces of hardware or hardware with duplicate commands

Background

- In Increment 43/44, ISSMP was commanding to the HRF Rack on ISS and unknowingly introduced a COL MDM error by sending a command to a non-powered Rack
- The result was that commanding could not be performed until the commanding queue buffer was cleared
- Our root cause analysis found:
  - **The console team was unaware of risk increase associated with sending the wrong command to ISS (PEP software update)**
  - **Communication and anomaly resolution practices relevant to this anomaly were insufficient and resulted in a long recovery time, impacting the POIF Cadre and adding risk to other ISS users**
  - **ISSMP console practices did not mature with the risk/probability of the errors that we could introduce to the ISS**
- As a result, ISSMP revisited what were considered best practices and sought to inject, and in some cases, re-integrate robust mistake-proofing measures

Anomaly Reaction and Resolution

Problem #1: Human Error

"It will be impossible to prevent an anomaly like this from occurring again."

This realization did not sit well with us and we know the ISS Program and our research colleagues deserved better.

Because of this, a focus was applied to the **reduction of human-introduced error** and the **communication surrounding anomaly responses**.

Those two focus areas will **reduce the impacts of human error** and **improve the community's ability to recover**.

Problem #2: Improving Human Factors (Mistake Proofing)

Problem #3: Anomaly Resolution Response and Communication

Problem #1 – Human Commanding Error

- Accepted we would not have the resources or the interfaces to fully mitigate the lack of awareness a PD might have to a changing ISS environment
- We chose to accept console errors and mitigate our highest risks via training and console mistake-proofing
- Our evaluated error rate is 0.1 % (~3662 commands over 1 year)
- For this specific error and impact, most PDs would not fall into this category
- The execution environment could change on ISS and you won't know that you have the ability to impact a system larger than your hardware
- This leads to problem 2.
  - If the best way to minimize risk is to mistake-proof our commanding, how can we do this?
  - And how close can we get to "target zero"?

Problem #2: Improving Human Factors

2.1 EPC commanding setup

2.2 Command and Data Handling Preparation

2.3 Reduce complacency and introduce some formality back into communicating commanding expectations

2.4 Other best practices to communicate

Problem #2.1: EPC Setup

- If a specific command will be used frequently, create a dataset instead of manually editing the user form each time
  - This introduces reliability and mitigates typo errors
- Filter commands in Command Operation that will only be used that day
  - Command Operation refreshes constantly to a default command instead of the queued command the PD is preparing to send
  - This helps the PD make sure the refresh doesn't go unnoticed
- Create displays that are payload/rack specific
  - Do not put commands to multiple racks in a single display
  - HRF had a duplicate payload in both racks so it built a display to handle commanding for both payloads
  - This introduced a chance for human error to inadvertently command to the wrong payload

Problem #2.1: EPC Setup

- Create a display if a set of commands will be frequently sent in a specific order
  - Create this display to flow in the order the commands will be sent
  - HRF has individual displays to activate the rack in different configurations, not just a generic rack activation display
  - Higher specialization is preferred as this removes command buttons from the display that could be selected by accident
- If off-nominal (infrequent) commands will be used, create a command plan with predefined user form inputs
  - Review command plan with console team during session pre-coordination meeting

Example in backup charts

Problem #2.2: C&DH Preparation

- Use naming conventions in PDL that are well defined and easily discernable
  - HRF's Rack 1 and Rack 2 commands were only differentiated by 1 digit
    - "H**1**C42_TWO_STAGE_CMD" vs "H**2**C42_TWO_STAGE_CMD"
  - Make command names that can easily be filtered
- Also allows PRO to monitor commanding through Command Track with better transparency

Problem #2.3: Reduce Complacency

- Accept that you need to put protections in place to protect you from yourself. Use your PRO/PSE experts to help with this!
- The more common the commanding sessions become, the more your brain goes on autopilot
- Mitigate the normalization of deviance
  - Gradual acceptance of sending the wrong command
  - Our operating environment allowed this as commands are no longer verbalized on the PRO loop as a mechanism for mistake proofing
  - Our internal HRF cadre reset the formality of the interface between our lead and our systems engineer, applied to the communication with the PRO as well

Problem #2.4: Other Human Factors

- As part of HRF's nominal console session, we bring down log files, create a command delog of all commands sent during the console shift, as well as an activity report with hardware times
- HRF has console checklists that are filled out each session to ensure all information is archived in the proper channels
- Quick access to console documentation detailing previous anomalies + cause + resolution (regardless of if a PAR was generated)

Problem #3: Anomaly Response

- Console Presence
  - Always alert PRO to off nominal responses immediately (regardless of how benign the issue appears to be)
  - Inclination may be to send for log files or other troubleshooting to better diagnose the issue and come to POIC with a more coherent story, but it's important to verify there is no risk to do so first
  - Always log commands sent (not just what was meant to be sent)
  - Do not assume a systemic issue outside of your payload wasn't caused by you
- Validate human steps prior to assuming broken hardware/software
- Communicate in real-time the expectation for anomaly characterization and recovery
- Start with the small things and work your way to larger systemic issues

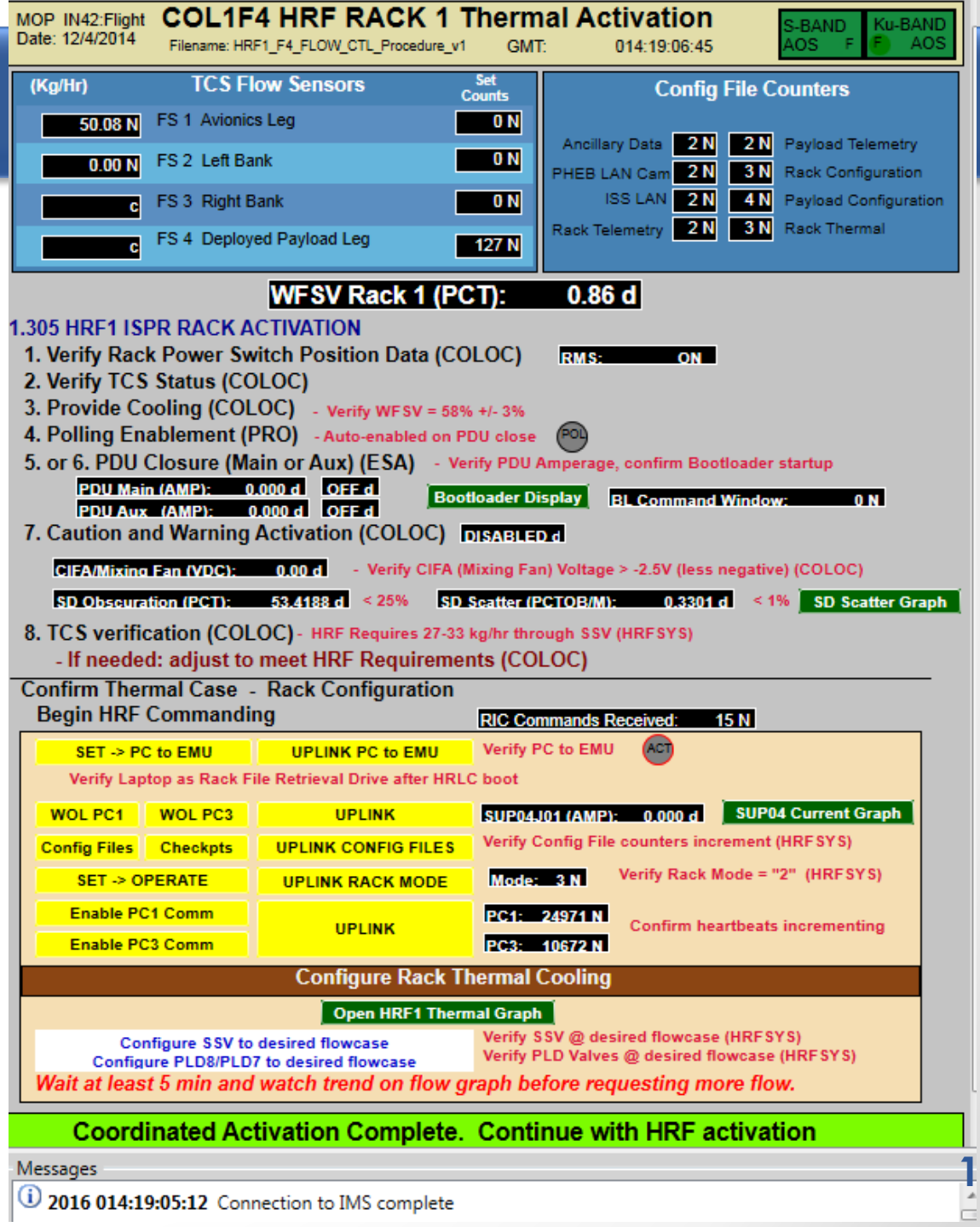
Additional Practices

- Two separate methods for viewing telemetry
  - HRF has a verified redundancy in place should one fail
  - MSIDs into commanding displays
  - Deconstruct the Payload Health & Status (PLHS) into in-house telemetry displays
- Develop and maintain backup crew procedures
  - HRF's crew rack activation/deactivation procedures were out of date in IPV
  - Crew intervention is an easier alternative to the POD with procedures in place
- Hardware used on ISS should be on console
- Simulations are used to reinforce anomaly decision tree

BACKUP CHARTS

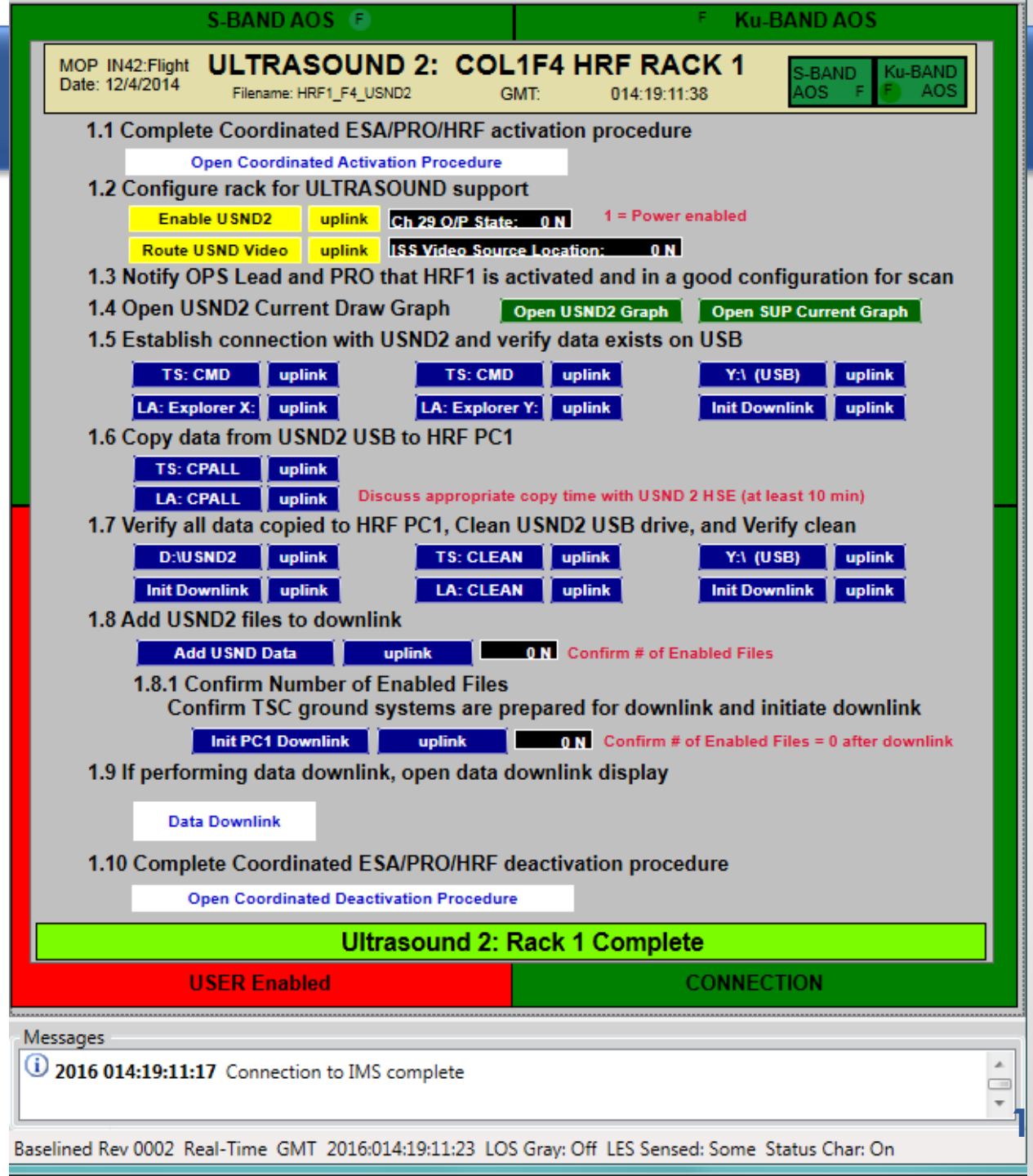
Commanding Display

- Screenshot of the Rack Activation display (Thermal)



Commanding Display

- USND2 display
- Separate display for USND2 on Rack 2



Commanding Error - How did it happen?

- Changes to PEP software allowed what was once a benign human-introduced error to become something more serious
- PD community was notified of the release of the software update, but not all of the implications were understood
- Commands that are sent are put into a queue to be executed
- Before the software change, each remote terminal (so each HRF Rack) had a unique queue
- After the software upgrade, all payloads on the same PL MDM bus had the same queue
- The command to the unpowered rack clogged up the queue for all other payloads on the PL Bus (including other PLs in Col module)
- Our specific command error in this case only applies to command data sets that have the same commands for two different pieces of hardware

HRF Perspective

- The HRF Racks (HRF1 and HRF2) are modified Express Racks…
- We can send upwards of 100 commands in a single console shift depending on the session
  - Increments 39-42 (1year) HRF sent 3662 commands and 4 commands were sent to an unpowered rack
  - 0.1 % error rate
- Average # of commands that we send for a
  - Rack Activation,
  - Downlink,
  - Rack Deactivation

Mistake Proofing

- Lean Six Sigma overview of the techniques we applied
- Applicable waste – Human Error:
  - Unintentional mistakes or errors relating to fatigue or distraction
  - Misapprehension or making conclusions even if the information is not complete
  - Classification or seeing the circumstances incorrectly
  - Deficient in set of standards
- Guidelines for correcting process:
  - If it is unfeasible for the mistake to happen, think of means to discover the mistake and reduce its consequences.