DR126366 Causal Analysis and Corrective/Preventive Actions

IFA STS-126-I-001

John Magley

01/15/09

Contents

- Background
- DR 126366 Causal Analysis
  - Flight Software Development
  - Flight Software Verification
  - Integrated Avionics Verification (SAIL)
  - Field Use Post-Release
  - Summary
- DR 126366 Fix Plan

Background

- PASS DR 126366 (IFA STS-126-I-001) addresses an issue with improper commanding from Systems Management (SM) to the Ground Command Interface Logic (GCIL) controller
- All GCIL commands must be issued as two consecutive command words
  - A reset (ALL ZERO) command that sets up the GCIL to receive a new configuration
  - A set (DATA) command that contains the new configuration command
- During the STS-126 flight it was discovered that a change on OI-33 could cause three incorrect command words to be issued
  - The DATA word commanding Payload Signal Processor (PSP) port moding from the Payload Interrogator (PI) to umbilical commanding
  - The DATA word commanding PSP port moding from the umbilical to PI commanding
  - The ALL ZERO word sent prior to both PSP moding commands and prior to automatic handovers between Ku-Band to S-Band communication
    - The DATA words for the Ku-Band/S-Band handovers were not affected
- Operational workarounds were used for the affected functions during STS-126
- MMT Action 126-MMT-001 was assigned to Flight Software to provide a root cause analysis for this anomaly to the PRCB

Causal Analysis: Development - 1

- A maintenance trap was set by the implementation of OI-20 SCR 89468B (1989)
  - Did not use methods to automatically force output data alignment on even addresses, violating the intent of a programming standard in force at the time (and still in force)
  - Placed warnings in code comments indicating need for monitoring of these addresses when subsequent changes were made
    - One warning was placed at a location following the compool change history that (at the time) would always be seen by teams making a subsequent change
- A compool change on OI-29 (2000) rendered the one obvious warning ineffective
  - Lack of space forced the change history for that and subsequent changes to the bottom of the compool
  - The alignment warning was not moved and therefore was not as obvious as before
    - The compool is fairly large and extensively commented
      - 130 lines between code changed on OI-33 and nearest affected parameter
      - 200 lines between code changed on OI-33 and the warning after the old change history

Causal Analysis: Development - 2

- An OI-33 SM software change (SCR 93122 – PSP Reject Indicator Fix to DR 122444) added one halfword of data in the middle of an SM data compool
  - SCR 93122 (2007) corrected an issue with downlist visibility of PSP command rejection indications
- The data insertion shifted some of the following data in the compool to an offset one address higher than before the change
- The affected command words are required to be on even addresses because they are output data (an Input/Output Processor (IOP) addressing restriction)
  - Referred to as “fullword alignment”
  - The shift moved them to odd addresses, so the IOP when attempting to access these addresses actually accessed the data at the next lower even address
    - I.e., if the IOP was instructed to pick up output data from address 0277, it actually output the data at address 0276
- The affected command words ARE NOT DIRECTLY RELATED to the function changed on OI-33 and the logic that controls the issuing of these commands WAS NOT MODIFIED on OI-33
- OI-33 reviews, inspections, and development testing missed the induced alignment problem

Causal Analysis: Development - 3

- Development Root Cause 1
  - The OI-20 development team apparently interpreted the wording of the standard ("… output buffers must be forced to fullword alignment") to require that the compool data layout result in fullword alignment, but not that programming techniques should be used to "lock down" that alignment
- Corrective and Preventive Actions (Dev Cause 1)
  - Audit the Primary Flight Software to identify all other cases where output data locations are not automatically forced to fullword alignment
    - Record all identified instances of these outputs as entries in the Action Item Data Base (AIDB) for the associated compools or modules
      - Development processes require examination of these AIDB entries during development, and again during design/code inspections, when a compool/module is modified
      - Does not rely on code comments
    - Modify the development edit panels to pop up a warning when a compool or module with one of the identified outputs is opened
    - This audit has also confirmed that no instances of improperly aligned outputs remain undetected in OI-33 flight systems
  - Modify the wording of the existing standard to clarify intent

Causal Analysis: Development - 4

- Development Root Cause 2
  - Developers and inspectors have not been provided with sufficient guidance for identifying problems that can result from a data insertion or deletion in the middle of a compool
    - Avoiding data location shifts was widely followed as good practice, but was not documented as such
    - No formal training describes the potential pitfalls of downstream data location shifts
    - No inspection checklist items or related guidance clearly remind developers/inspectors of specific impacts to consider
- Corrective and Preventive Actions (Dev Cause 2)
  - Audit OI-34 changes (complete with no issues – STS-128 deltas in work)
  - Enhance programming standards by prohibiting data changes within a compool that result in location shifts to existing parameters
    - Exceptions would require approval from an internal review board
    - Standard will describe the additional analysis required if an exception is to be granted
- Additional Actions
  - Training for all developers and inspectors on the audits, tool modifications, and updated standards

Causal Analysis: FSW Verification - 1

- The Development Test and Level 6 (detailed) verification philosophies focus on verification of changed code or code that was directly impacted by a change (e.g., impacted by an interface change)
  - The functions affected by the problem did not fit the criteria for detailed Level 6 testing on OI-33
- General health testing of SM and VU functions that should not have been affected by code changes is an intended function of Vehicle Cargo Systems (VCS) Level 7 system integrity testing and to some extent VCS Level 8 reconfiguration testing
- There is no closed-loop modeling support for the affected functions in the Software Production Facility (SPF)
  - This means extra steps are required for a tester to detect a problem in GCIL commanding compared to, for example, detecting a problem in the commands to GNC effectors
  - There are test scripting capabilities in the SPF that can ease the collection and analysis of these command outputs to devices lacking direct model support

Causal Analysis: FSW Verification - 2

- Review of the Level 6 testing for OI-33 SCR 93122 revealed one missed opportunity to detect DR 126366
  - One test step required the generation of a PSP Port Mode Reject status
  - Given the absence of a GCIL model, the test produced the expected response (no change in selection)
    - The actual (incorrect) output to the GCIL was not examined at the time of the test
      - the PSP port mode function itself was not being verified
- The affected functions were not exercised in the OI-33 VCS Level 7 tests or in the STS-126 VCS Level 8 tests
  - The current VCS Level 7 process documents a requirement to update the health tests to include new or modified functions
  - This requirement has been effective over the last several OIs
  - However, review of the health tests against SM and VU requirements has determined that there are gaps in the coverage of functions that were added many years ago
    - Includes the functions impacted by DR 126366

Causal Analysis: FSW Verification - 3

- FSW Verification Root Cause 1
  - Outputs from SM and VU functions to devices that are not supported by SPF models (e.g., the GCIL) were not routinely monitored to verify they are still correct after (apparently) unrelated code changes
- Corrective and Preventive Actions (Ver Cause 1)
  - Add test script commands to standard VCS Level 6 and 7 test setups that support easy monitoring of correct outputs
    - Based on modifications/extensions to the test scripting that was used to facilitate verification of the Remote Control Orbiter capabilities

Causal Analysis: FSW Verification - 4

- FSW Verification Root Cause 2
  - VCS health testing did not include coverage of the affected functions
- Corrective and Preventive Actions (Ver Cause 2)
  - Review OI-33 VCS Level 7 tests, STS-126 VCS Level 8 tests, SAIL tests, and STS-126 flight experience and identify any functions that have not been demonstrated to operate on OI-33
    - Health test of Freon Loop Accumulator Quantity Monitor function completed with no issues found
  - Perform similar review for STS-125 considering unique functions that may be used in the Hubble mission vs. the flown OI-32 ISS missions
    - Any additional testing to be performed in line to STS-125 Delta SRR
  - Modify the VCS Level 7 tests to ensure coverage of functions currently in use
  - Add a process requirement that the appropriate subset of the VCS Level 7 health tests be run on any flight system with a Class 1 (non-reconfiguration) SM or VU source change
    - Testing would be required to complete in line to flight SRR

Causal Analysis: FSW Verification - 5

- Changes to the VCS Level 8 process or tests are not recommended at this time
  - Current VCS Level 8 tests are focused on the reconfiguration data and the reconfigured VCS functions
  - VCS Level 8 testing relies heavily on automatic test case generation and analysis driven by the input reconfiguration data
  - The new VCS Level 7 requirement for flight systems will serve the purpose of system integrity testing for VCS Class 1 changes
- Additional Actions
  - Training for all VCS verification analysts on updated Level 7 tests and process change

Causal Analysis: IAV Testing and SAIL - 1

- SAIL does have GCIL and PSP hardware that is used during testing
- IAV testing typically uses models for parts of the Ku-Band and S-Band systems
  - There are some limitations to the models, but nothing affecting the ability to test the affected functions
- IAV OI-33 core testing did perform a test that explicitly verified the automatic Ku-Band to S-Band handover function
  - Function worked, but only because the handover command was the first one issued after the GCIL decoders were turned on via uplink
    - The decoder select output also has zeros in the 9 bits that the GCIL interprets as the reset (ALL ZERO) command
      - A separate ALL ZERO command is not required for the first command only
    - The SM computer sent the correct set (DATA) command for the handover
- The IAV testing did not have a documented requirement to verify the correct operation of
  - The automatic S-Band to Ku-Band handover
  - The automatic PSP port moding function

Causal Analysis: IAV Testing and SAIL - 2

- The Ku-Band to S-Band handover verification test had setup steps that included an automatic S-Band to Ku-Band handover
  - The handover did not occur and was manually worked around
    - Test deviation was recorded
  - This was not a step with a formal “verify” requirement
- The Ku-Band to S-Band handover did not occur the first time it should have in the test run
  - The test run was suspended after the failed handover and then later restarted at a point prior to the expected handover
  - The restart included the GCIL reset that permitted the handover to succeed in the restarted run
- Steps in the run following the successful Ku-Band to S-Band handover incidentally established the conditions for another automatic handover back to Ku-Band
  - This handover also did not occur
  - The failure was not noticed because there was again no formal “verify” requirement

Causal Analysis: IAV Testing and SAIL - 3

- None of the Ku-Band/S-Band handover failures were documented in SAIL anomaly reports
  - At least two of them were noted during the runs and should have been documented
  - Factors contributing to this oversight:
    - The misleading success of the verified Ku-Band to S-Band handover
    - A history of problems with this part of the test on previous OIs that were not due to FSW problems
    - The lack of changes on OI-33 that overtly impacted the handover logic
- The OI-33 core testing did not exercise the automatic PSP port moding function
  - Payload test began with the control switch in PANEL with umbilical selected
    - Forced PSP output to the umbilical
  - All STS-126 payload commands were to the umbilical configuration
    - Port moding was not required during the SAIL testing
  - STS-126 flight configuration had control switch in COMMAND and the PSP initialized with PI selected
    - Port moding was required one time in-flight

Causal Analysis: IAV Testing and SAIL - 4

- IAV and SAIL Root Cause 1
  - SAIL Standard Operating Procedure (SOP 2.23 Anomaly Processing) was not followed
    - The two noted cases of failed Ku-Band/S-Band handovers should have eventually resulted in SAIL Interim Discrepancy Reports (IDRs) that would have to be analyzed for potential FSW problems
  - The team incorrectly assumed the Ku-Band/S-Band handover problems were the same as the non-FSW problems encountered previously
    - Reinforced by the successful handover in the test
- Corrective and Preventive Actions (IAV/SAIL Cause 1)
  - Training for all SAIL test participants to reinforce the requirement to strictly adhere to the SAIL IDR process
    - Briefings for all test participants (SAIL personnel, IAV test sponsors and CB representatives) have been completed
  - All SAIL test personnel are required to pass an annual SAIL SOP examination to maintain certification
    - Testing has been updated to ensure questions on anomaly writing procedures are included in each exam
  - SAIL also has an ongoing activity to document common lab “funnies” and the analysis required to confirm reoccurrences

Causal Analysis: IAV Testing and SAIL - 5

- IAV and SAIL Root Cause 2
  - Differences between the flight configuration and event sequences and the SAIL tests masked some opportunities to detect DR 126366
    - In flight, a different switch configuration and sequence of GCIL commands revealed the PSP port moding problem
    - In flight, a Ku-Band/S-Band handover command that was not the first one to the GCIL revealed the automatic handover problem
- Corrective and Preventive Actions (IAV/SAIL Cause 2)
  - Review test procedures and update where possible to make them more flight-like
    - Add steps to verify automatic Ku-Band/S-Band handovers in both directions (complete)
    - Modify payload commanding switch configuration (complete)
    - Other changes as identified
  - When splitting tests on the same day, specify that no box should be reset between runs

Causal Analysis: Field Use Post-Release

- Both INCO and KSC report that the PSP port moding function was not exercised during STS-126 training simulations or STS-126 vehicle processing
  - Would have seen that effect of the problem
  - This function is now typically only used once per flight (at most)
  - There was one missed opportunity to detect the PSP port moding problem during an SMS development run
    - The PSP port mode rejection was not noted at the time
- The Ku-Band/S-Band handover problem was not seen during SMS simulations due to a limitation in the SMS GCIL model
  - The SMS model does not require an ALL ZERO command before a DATA command
    - It only looks for and responds to a DATA command
  - Updates to the SMS MDM model to output the ALL ZERO command and the SMS GCIL model to check the ALL ZERO command have been informally developed and tested
    - Formal authorization to incorporate these changes is in work

Causal Analysis Summary

- A full root cause analysis has been performed on PASS DR 126366
  - Causes contributing to the introduction of the DR have been identified
  - Causes contributing to the failure to detect the DR in FSW Verification and Integrated Avionics Verification have been identified
- Effective corrective and preventive actions have been identified
  - Actions to verify no similar problems remain undetected
  - Actions to prevent reoccurrence of this type of problem
  - The identified actions are complete or actively in work
    - All actions required in line to STS-119 are complete
    - All actions are being tracked to completion by the Flight Software Office (FSO)

DR 126366 Fix Plan

- The SASCB has approved fixing DR 126366 on all remaining OI-33 and OI-34 flights
  - Patch implementations on STS-119 and STS-127
    - Patch will place the affected output commands in correctly aligned memory locations in patch space and modify the code to obtain the commands from the new locations
    - Patch is straightforward, only impacts the affected functions, and is fully testable
  - Source implementations on STS-128 and subsequent OI-34 flight systems
  - No change to STS-125 or STS-400 is required
    - Problem is not present on OI-32
- STS-119 Details
  - UPF patch available – 12/15/08
  - SAIL testing complete – 12/22/08
  - STS-119 Comp Load Mass Memory release – 02/02/09