Space Shuttle Flight Software Potential Loss of Crew Errors

James K. Orr
Independent Consultant
jkorr@gatech.edu

Copyright James K. Orr 2015

Purpose

- Just over four years have passed since the last Space Shuttle Flight, STS-135, launch July 8, 2011, landed July 21, 2011.
- Analysis that I contributed ultimately resulted in risk due to Space Shuttle Flight Software (Primary Avionics Software System, or PASS) being added to the Space Shuttle Probabilistic Risk Assessment (PRA)
- On this fourth anniversary, I am publishing this analysis of PASS errors which placed crew lives at risk.
- My purpose is to capture both the details and the context of these loss of crew PASS errors so as to enable designers and managers of future manned space flight systems to maximize avoidance of similar loss of crew software errors.
  - While our accomplishments were great please
    - Learn From Our Mistakes

Copyright James K. Orr 2015

PASS Software in Shuttle PRA

- Reference 1 (*Shuttle Risk Progression: Use of the Shuttle Probabilistic Risk Assessment (PRA) to Show Reliability Growth*) shows overall risk of LOCV (Loss of Crew and Vehicle) at 1 in 12 for STS-1 (reference 1, page 6). NASA identified the risk of "Orbiter flight software error results in catastrophic failure during ascent and ejection seats fail to save the crew" at 1 in 600 (reference 1, page 9). This was the 7th highest risk.
- By STS-133, overall LOCV risk was 1 in 90 (reference 1, page 6) and "Flight Software error results in catastrophic failure during ascent" risk was 1 in 4400 (reference 1, page 11). This was now the 6th highest risk.

Copyright James K. Orr 2015

Presentation Strategy

- I have struggled with deciding exactly how to present.
  - During the shuttle operational life, PASS software loss of crew Discrepancy Reports, or DR, (formal error tracking document) were tracked by when the error was introduced and when found.
  - Focus was on LOCV DR's which were released to the Software Avionics Integration Lab (SAIL) and for crew training in the Shuttle Mission Simulator (SMS).
- This caused focus on some errors which were found during the normal course of verification – they were released to provide early SAIL testing and SMS training before verification was complete. Most of these posed no crew risk, but did assist in our search for other LOCV DR's.
- Data in this presentation is presented in a new format.
  - First, Space Shuttle Primary Avionics Software System (PASS) LOCV Discrepancy Requests (DR's) actually flown are presented by time period when discovered.
    - A one page generalized summary of each DR is first presented, later followed by multiple pages with additional detail. Much of the additional detail is in the acronym language used by the Space Shuttle program and may be difficult to follow.
    - Second, PASS LOCV DR's released, but not flown are presented.
  - Later, a final section is added which represents the PASS LOCV DR's as tracked during space shuttle operational life.

Copyright James K. Orr 2015

Presentation Strategy

- History of Loss of Crew PASS DR's will be presented as follows:
  - Loss of Crew and Vehicle (LOCV) prior to STS-1 launch 4/12/1981
  - LOCV PASS only DR's previously flown and discovered prior to STS-51L (loss of Challenger) launch on 1/28/1986
  - LOCV PASS only DR's previously flown and discovered during the "Return To Flight" period after STS-51L and prior to STS-26 (Return to Flight) launch on 9/29/1998
  - LOCV PASS only DR's previously flown and discovered after STS-26 launch on 9/29/1998 - NONE
  - LOCV PASS only DR's never flown and found after PASS Verification (including Software Avionics Integration Lab - SAIL) complete – including flight specific SAIL verification.
  - LOCV PASS only DR's never flown but found prior to PASS Verification (including SAIL) complete
- Starting at page 62 is a completely separate discussion of released LOCV PASS DR's in a different format.

Copyright James K. Orr 2015

Glossary

Acronym	Stands For
AP-101B	Original GPC's. See AP-101S.
AP-101S	Upgraded GPCs with a semiconductor memory of 256,000 32-bit words; the older AP-101B GPCs had a core memory of up to 104,000 32-bit words. AP-101S was up to three times the AP-101B processor speed.
ATO	Abort To Orbit
BFS	Backup Flight System
DAP	Digital Auto Pilot
DR	Discrepancy Report
ET	External Tank
FC	Flight Control String 1, 2, 3 or 4
FCOS	Flight Computer Operating System
FF	Flight Forward MDM (subset of FC)
FSW	Flight Software

Acronym	Stands For
FTS	Fail To Sync
GNC	Guidance, Navigation, and Control
GPC	General Purpose Computer
HFE	High Frequency Executive in PASS, 25 Hz execution of flight control and other critical functions.
I-Load	Initialization value for mission specific constant. Used to reconfigure generic software for mission specific performance.
I/O	Input / Output
LOCV	Loss of Crew and Vehicle
MEC	Master Events Controller, hardware device that separated the SRB and External Tank from the Orbiter
MECO	Main Engine Cut-off

Copyright James K. Orr 2015

Glossary

Acronym	Stands For
MDM	Flight Critical Multiplexer/De-Multiplexers
MM	Major Mode
OMS	Orbital Maneuvering Systems (maneuver engines for orbit insertion, deorbit, and on-orbit)
PASS	Primary Avionics Software System
RCS	Reaction Control System (control jets)
RM	Redundancy Management
PRA	Probabilistic Risk Assessment

Acronym	Stands For
PSW	Program Status Word
ROTA	Rota, Spain (Space Shuttle Abort Landing site)
RTLS	Return To Launch Site Abort
SAIL	Software Avionics Integration Lab
SM	System Management
SSME	Space Shuttle Main Engine
SRB	Solid Rocket Boosters
TAL	Trans-Atlantic Abort Landing

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

Flown LOCV DR’s

Found Prior To STS-1

Copyright James K. Orr 2015

LOCV DR's Prior To STS-1

- Following STS-1, more information including DR severity was collected on every DR. There is no direct knowledge of the number of LOCV DR's found prior to STS-1.
- In 1986, analysis of DR data after STS-1 data indicated 1 in 50 of ascent/entry PASS DR's were LOCV.
- Prior to STS-1, 2764 PASS DR's were disposition as errors during the 16 major releases to SAIL integrated avionics verification, SMS crew training, other laboratories, vehicle checkout and KSC ground processing.
- Prior to STS-1, there were on the order of 55 LOCV PASS DR's (i.e., 2764/50). Not all of the 2764 DR's were ascent/entry, but the frequency of LOCV DR's was likely greater than 1 in 50 during early releases.

Copyright James K. Orr 2015

LOCV DR's Prior To STS-1

- Context – Verification Resources
  - Resources for testing prior to release of PASS systems to SAIL and SMS was very constrained.
  - These testing resource constraints remained until after the orbiter fleet had been completely transitioned to the upgraded AP-101S computer (completed in 1991 around STS-43, the first flight off OI-20).
  - Pre STS-1, development and verification testing of PASS and BFS had the ability to run 3 “single string” tests simultaneously, or 1 “triple string” test.
    - “Single string” was running one single General Purpose Computer (GPC).
    - “Triple string” was running three GPCs together. This could be 3 PASS computers running in redundant Guidance, Navigation, and Control (GNC) set; else it could be 2 PASS computers running in redundant Guidance, Navigation, and Control (GNC) set plus one PASS Computer running System Management; or else it could be 2 PASS computers running in redundant Guidance, Navigation, and Control (GNC) set plus one Backup Flight System (BFS) Computer tracking PASS.

Copyright James K. Orr 2015

LOCV DR's Prior To STS-1

- Context – Verification Resources
  - Anecdote – Prior to STS-1, I initially did verification of the Orbit and Transition Digital Auto Pilots (DAP). Just prior to STS-1, I did regression verification of the Inertial Measurement Unit (IMU) ground calibration and alignment software.
    - One IMU ground calibration required running 6 hours on the actual vehicle. Due to simulation requirements, this test ran 18 hours in the test environment on a flight equivalent GPC.
    - I was allocated 3 hours each weekend to do my verification.
    - It required 6 to 7 calendar weeks to complete one test execution
  - After the orbiter fleet had been completely transition to the upgraded AP-101S computer (1991), our testing capability expanded greatly.
    - Development and verification testing of PASS and BFS had the ability to run 6 “single string” tests simultaneously, or up to 6 “triple string” tests.
    - This increase in capability to run multiple computer tests greatly increased the ability to test System Software (SSW) and combined PASS / BFS tests

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

Flown LOCV DR’s

Found Prior To STS-51L

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

When Found	September 30, 1981 By Prime Crew In SMS
Missions Flown At Risk	STS-1 (4/12/1981) Commander John W. Young and Pilot Robert L. Crippen
Error Title	DR 25365R - PASS SYSTEM HUNG IN OPS 602 DURING SMS SIMULATION OF CONTINGENCY ABORT TO ROTA, SPAIN
Probability Of PASS Error	Less than 1 in 240. Per Reference 1, Page 9, this was the risk of SSME-induced SSME catastrophic failure and ejection seats fail to save the crew. The required scenario for this PASS DR was 3 Space Shuttle Main Engines (SSME) out contingency abort plus failure detection of the 3rd SSME within 0.91 to 1.42 seconds of the failure detection of the 2nd SSME.
BFS Engage	When this DR occurred in the Shuttle Mission Simulator (SMA) during crew training, the Backup Flight System (BFS) was successfully engaged.
Error Introduced	The PASS error was introduced sometime prior to STS-1.
Visibility	Extremely high within NASA community due to (a) occurring in the SMS with prime crew training and (b) first total lockup of the PASS flight system after completion of testing prior to STS-1. Mitigated somewhat by successful BFS engage.

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

When Found	July 23, 1984 (risk elevated on August 27, 1984 after MEC hardware test)
Missions Flown At Risk Pad Abort Only	STS-41D During Launch Attempt On June 26, 1984, there was a launch abort at T-6 seconds, followed by a pad fire about ten minutes later. Abort occurred after starting all three SSME's. Commander Henry W. Hartsfield, Jr.; Pilot Michael L. Coats; Mission Specialist 1 Richard M. Mullane; Mission Specialist 2, Steven A. Hawley; Mission Specialist 3, Judith A Rsnick and Payload Specialist 1 Charles D. Walker
Error Title	DR 56938 - STS-41D MEC HOMOGENEITY ISSUE
Probability Of PASS Error	1 in 6. Scenario for PASS error required two software modules to execute on the same High Frequency Executive (HFE), which delayed the timing between issuing "arm" and "fire" commands to the Master Events Controller (MEC)
BFS Engage	On June 26, 1984, there would have been only a four-second limit on the BFS engage window following PASS-attempted SRB separation due to a PASS requirement to disconnect 28 volt power to the SRBs (PASS FSW was per existing requirements, changed prior to flight of STS-41D on August 30, 1984))
Error Introduced	Error introduced due to the accumulation of changes since STS-1. STS-41D was the first flight at risk. Additionally, it was believed that MEC hardware would work correctly for the PASS error scenario. Requested hardware test discovered risk.
Visibility	Flight schedule for August 28 was delayed two days to provide a PASS software fix.

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

DR 25365R

PASS SYSTEM HUNG IN OPS 602 DURING SMS SIMULATION OF CONTINGENCY ABORT TO ROTA

Copyright James K. Orr 2015

Space Shuttle Contingency Abort

- Reference 5 presents a good summary of all Space Shuttle Abort Modes. Contingency Abort is defined as:
  - "Contingency aborts involved failure of more than one SSME and would generally have left the orbiter unable to reach a runway. These aborts were intended to ensure the survival of the orbiter long enough for the crew to bail out. Loss of two engines would have generally been survivable by using the remaining engine to optimize the orbiter's trajectory so as to not exceed structural limits during reentry. Loss of three engines could have been survivable outside of certain 'black zones' where the orbiter would have failed before bailout was possible. These contingency aborts were added after the destruction of Challenger."
- Obviously, Contingency Aborts were valid for STS-1, STS-2, STS-3 and STS-4 (2 man crew with ejection seats).
- See Reference 2, pages 27 to 29, for an explanation of PASS changes that significantly contributed to increased crew survivability in the case of abort scenarios.
  - "After STS-1, a TAL capability was added that provided the guidance and control necessary to facilitate a European or African landing if engine failures occurred too late in the ascent profile to make RTLS an effective option
    - Addition of TAL as a certified abort mode drastically closed the black - zone (region of unsurvivability) for the period where the orbiter had too much energy to return to Florida (RTLS) but did not have enough energy to achieve a stable orbit (ATO). "

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

- September 30, 1981.
  - Jack Clemons, Reference 3, page 886 - “just before STS-2 was scheduled to takeoff, some fuel was spilled on the vehicle and a number of tiles fell off. The mission was therefore delayed for a month or so. There wasn't much to do at the Cape, so the crew came back to Houston to put in more time on the SMS. One of the abort simulations they chose to test is called a "Trans Atlantic abort." which supposes that the crew can neither return to the launch site nor go into orbit. The objective is to land in Spain after dumping some fuel. The crew was about to go into this dump sequence when all four of our flight computer machines locked up and went "catatonic."”
- STS-2 prime crew was training for ROTA abort (trans Atlantic abort to Rota, Spain) with 3 Space Shuttle Main Engines (SSME’s) failed.
- Following the third SSME failure, Transitioned to Major Mode 602 (abort entry flight control mode). PASS computers suddenly appear to freeze as indicated by “Big X” on all PASS controlled displays (Displays no longer receiving output data from GPC).
- BFS successfully engaged after 10 seconds.
- Obviously, crew and NASA management were concerned.
  - Jack Clemons, Reference 3, page 886 – “Our machines all stopped. Our greatest fear had materialized - a generic software problem. We went off to look at the problem. The crew was rather upset, and they went off to lunch.”

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

- Detail Description From Software Perspective
  - THE ATTEMPTED EXECUTION OF THE INTERCONNECT MODULE WHILE IN AN UN-INITIALIZED STATE RESULTED IN INVALID CODE BRANCHES INTO SOFTWARE UNRELATED TO THIS FUNCTION.
    - Due to re-entry to interconnect module after third SSME failure within a small time window of the second SSME failure.
    - Software structured as a Do Case (branch to a specific subsection of code based on a Case number)
    - Interconnect module code interrupted prior to completing entire initial sequence
    - Re-entry was done without proper software re-initialization of Case number
    - Result was a non-valid Case number, which was executed without protection. Result was random branch into executable code. Incorrect branching is unpredictable.
  - THIS BAD BRANCHING EVENTUALLY CAUSED ERRONEOUS MODIFICATION OF THE PROGRAM STATUS WORD (PSW CONTAINS SUCH INFORMATION AS "NEXT INSTRUCTION TO EXECUTE," INTERRUPT INDICATORS, ETC)
  - THE ERRONEOUS MODIFICATION OF THE PSW INVOLVED BOTH THE SETTING OF A FIXED POINT OVERFLOW INDICATOR AND ENABLING OF THE INTERRUPT WHICH IS NORMALLY NOT ENABLED DURING PASS EXECUTION.
  - THIS CAUSED THE OPERATING SYSTEM TO ENTER A "HARD LOOP" AS FOLLOWS:
    - THE OPERATING SYSTEM DETECTS THE INTERRUPT IN THE PSW,
    - FIELDS THE INTERRUPT AND LOGS IT,
    - RESTORES THE ORIGINAL PSW, AND
    - IMMEDIATELY RE-DETECTS THE FIXED POINT OVERFLOW INTERRUPT
  - THE PASS SYSTEM THEN ENDS UP IN A "HARD LOOP," LOGGING FIXED POINT OVERFLOWS EVERY 345 MICRO SECONDS. NO OTHER PASS PROCESSES, FCOS, OR I/0 OCCUR AGAIN.

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

MULTI-PASS IMPLICATIONS CONSIDERED

- A multi-pass activity is code which required more than one pass to complete its defined task. It could be a module, portion of a module collection of modules, or scheduled process.
- In general, an analysis must be performed to determine how each multi-pass activity will respond to unexpected occurrences. Specifically, the following questions must be answered for each multi-pass activity:
  - What are the start and end criteria (e.g., crew item entries, timers, events, transitions)?
  - What does the code do while the multi-pass activity is in progress if:
    - Data that is assumed to be static changes?
    - Dynamic data used in decision blocks takes on an unexpected value?
    - Activity restarts before completion (e.g., initialization flag is set true)?
    - Activity is terminated before completion (new activity is requested)?
    - Completion of activity is delayed beyond expected time?
    - Activity is restarted after normal or abnormal completion?
- See page 14 of Reference 2 for more discussion.

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

- Key lessons
  - Always insure correct initialization and cleanup is done for multi-pass functions that execute over a limited period of time.
  - For all code structures (Do-Case, If Test, etc.), make sure appropriate action is taken if an unexpected value is received. In almost all cases, this should include setting an error condition which marks where the code executed the unexpected value and the nature of the unexpected value.
  - During testing, make certain the error conditions are recorded for post test analysis.
  - Make certain the error condition record is reviewed after each and every test.

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

DR 56938

STS-41D MASTER EVENTS CONTROLLER HOMOGENEITY ISSUE

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

- Reference 2, pages 35 – 37 provides a detail explanation of this error.
- Reference 4, Houston Post front page article:
  - "The problem, discovered Tuesday, was with the split-second timing of the essential orders from the space shuttle's general purpose computers to an electronic switchboard in the rear of the ship called the master events controller.
  - A 'software patch,' a new section of computer program, was written and it worked perfectly in multiple tests around the country Tuesday, said Arnold Aldrich, the manager of the space shuttle project office at Johnson Space Center in Houston.
  - But since it handles such critical jobs as making the huge external fuel tank and solid rocket boosters drop off at precisely the right time, technicians wanted the extra day to 'put all eyeballs together and decide we haven't missed anything,' Aldrich said. Anything less could have been disastrous, he said."
- NASA and contractor management processes worked perfectly in this situation.
- NASA Orbiter Mission Evaluation Room was notified of concern by IBM management and technical team.
- Initial assessment was that the MEC hardware would function correctly, BUT an expedited hardware test was performed, which revealed that the hardware would not work correctly in the PASS error condition.
- Flight preparations were immediately halted (launch was schedule within hours).
- Software fix was prepared, and other related issues were identified and addressed.
- Arnold Aldrich then directed an additional delay to ensure adequate time for any remaining issues to be elevated.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior To STS-26

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

- The loss of Challenger and the crew of STS-51L was a profound event.
- The IBM PASS team had continued to incrementally improve processes and define new audits to seek out latent errors. However, at the time of STS-51L there were still over 300 errors (reference 2, page 20) in the PASS software that would be discovered over the next 25 years.
- The period after STS-51L and STS-26 was a period of significant effort to find and eliminate as many risk as possible.
  - Mandatory PASS requirement changes prior to STS-26
  - Effort call “Flight Software Re-validation” which involved a large number of focused audits to use insights from prior errors to find additional similar errors.
  - Re-focus on all testing processes including SAIL and SMS crew training to identify all residual issues.
- Several flown LOCV PASS DR's were found in this period. These discoveries did not bring the drama of errors found while actively flying, but did contributed to the long term safety of future crews.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

When Found	March 11, 1986 By IBM Level 7 Verification Testing
Missions Flown At Risk	STS-1, STS-2, STS-3, STS-4, STS-5, STS-6, STS-8, STS-9, STS-41B, STS-41C, STS-41D, STS-41G, STS-51A, STS-51C, STS-51D, STS-51B, STS-51G,STS-51F, STS-51I, STS-51J, STS-61A, STS-61B, STS-61C, STS-51L
Error Title	DR 63507 - INTERCOMNECT NOT PROTECTED AGAINST INTACT-TO-CONTINGENCY MODE TRANSITION
Probability Of PASS Error	Less than 1 in 240. Per Reference 1, Page 9, this was the risk of SSME-induced SSME catastrophic failure and ejection seats fail to save the crew. The required scenario for this PASS DR was transition from intact to contingency abort within 1.5 seconds of starting OMS to RCS interconnect or Return To Normal (propellant from RCS tanks).
BFS Engage	BFS engage would not result in recovery. PASS error results in no fuel path to RCS jets.
Error Introduced	Error was officially recorded as introduced prior to STS-1. OMS/RCS Interconnect was an area of many changes over decades complicated by an unlimited number of scenarios.
Visibility	Relatively minor as situation was identified when implementing a change for later systems with more GPC memory and speed with AP-101S upgrade during a period of no flights after STS-51L.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

When Found	April 30, 1986 By IBM Developers.
Missions Flown At Risk	STS-41D, STS-41G, STS-51A, STS-51C, STS-51D, STS-51B, STS-51G,STS-51F, STS-51I, STS-51J, STS-61A, STS-61B, STS-61C, STS-51L
Error Title	DR54961 - INCORRECT PROCESSING FOR INVALID PORT ID
Probability Of PASS Error	1 in 1,000 (Order of Magnitude). These entry activities on the Entry Control Display are mostly done while On-orbit or on the ground. The chance for error to have occurred and to cause LOCV is probably zero due to infrequent usage during Ascent and Entry and the obvious severity of the error's impact if occurred. Note that a crew error is required to create the scenario for the problem.
BFS Engage	BFS Engage Would Be Successful. If On-orbit, re-IPL (redo Initial Program Load) PASS.
Error Introduced	0I04.04 (September, 1983)
Visibility	Relatively minor as situation was identified when implementing a change for later systems with more GPC memory and speed with AP-101S upgrade during a period of no flights after STS-51L.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

When Found	July 30, 1986
Missions Flown At Risk	STS-1, STS-2, STS-3, STS-4, STS-5, STS-6, STS-8, STS-9, STS-41B, STS-41C, STS-41D, STS-41G, STS-51A, STS-51C, STS-51D, STS-51B, STS-51G,STS-51F, STS-51I, STS-51J, STS-61A, STS-61B, STS-61C, STS-51L
Error Title	DR 65325 - MM601 (Ascent Flight Control) MODULES DISPATCHED IN MM603 (Entry Flight Control)
Probability Of PASS Error	1 in 10,000 (Order of Magnitude). Problem required a contingency abort scenario where transition was made to Major Mode (MM) 602 with vehicle velocity between 2500 feet per second and 3200 feet per second so that conditions to transition to MM 603 (final approach and landing major mode) is satisfied as soon as entry to MM 602 (designed for early high altitude entry flight control). This would require an extreme under speed (early 3 SSME out) condition.
BFS Engage	BFS engage should be successful provided the vehicle state at BFS engage was recoverable.
Error Introduced	Pre STS-1
Visibility	Relatively minor as extreme contingency scenario was very low probability and during a period of no flights after STS-51L.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

When Found	October 20, 1986 By SMS When Fault Introduced With Required Timing
Missions Flown At Risk	STS-9, STS-41B, STS-41C, STS-41D, STS-41G, STS-51A, STS-51C, STS-51D, STS-51B, STS-51G,STS-51F, STS-51I, STS-51J, STS-61A, STS-61B, STS-61C, STS-51L
Error Title	DR 100775 – Fail To Sync (FTS) DUE TO DISAGREEMENT IN TRANSMITTER STATIJS
Probability Of PASS Error	1 in 18 due to software process if hardware error scenario occurred (A non-universal I/O error must occur on Flight Control string 1, 2 or 3 at an OPS mode recall. The next higher numbered Flight Control string must be changing Commander between two Non-Prime GPCs).
BFS Engage	BFS Would Be Successful
Error Introduced	Problem introduced on OI-2 (STS-9). CURRENT IPV TOOLS & STANDARDS WERE NOT IN PLACE WHEN PROBLEM WAS INTRODUCED. LOW PROBABILITY & COMPLEXITY OF SCENARIO. THIS PROBLEM HAS BEEN IN THE SOFTWARE SINCE PRE-STS1. PRE 0I02 BUS RECONFIGURATION HAD PRIORITY OVER I/O TRANSACTIONS. THIS MADE IT IMPOSSIBLE FOR TOGGLE BUFFER REASSIGNMENT TO RUN WHILE A BUS RECONFIGURATION REQUEST WAS IN THE QUE before OI-2.
Visibility	Extreme scenario found in SMS, successful BFS engage. Generally positive that efforts to uncover errors needing fixed before STS-26 were being successful, along with BFS recovery. OPS mode recall was normally precluded during ascent / entry unless no other option existed to recover necessary hardware redundancy.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

When Found	April 13, 1988 By Desk Check (Code Audit) By McDonnel Douglas (NASA subcontract)
Missions Flown At Risk	STS-1, STS-2, STS-3, STS-4, STS-5, STS-6, STS-8, STS-9, STS-41B, STS-41C, STS-41D, STS-41G, STS-51A, STS-51C, STS-51D, STS-51B, STS-51G,STS-51F, STS-51I, STS-51J, STS-61A, STS-61B, STS-61C, STS-51L
Error Title	DR 100329 - SSME-OUT SAFING TASK NOT CALLED FOR ENGINE-OUT AT LIFTOFF
Probability Of PASS Error	1 in 100,000 (Order of Magnitude). SSME engine status is check prior to SRB ignition. If an SSME is not performing nominally, a Pad Abort is declared, SSME's are shut down, and there is no SRB ignition. It is extremely unlikely for an SSME to fail after performing satisfactorily and the failure to be recognized in the next 40 milliseconds.
BFS Engage	BFS engage possible, but would require identification of PASS abnormal behavior before a critical situation was reach which the BFS could not recover.
Error Introduced	Combination of lack of explicit requirement and failure to previously recognize failure scenario.
Visibility	Visibility was generally positive. Latent PASS LOCV errors were being discovered after loss of STS-51L as all of NASA and NASA contractors focused on identifying issues requiring fixes prior to STS-26.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 63507

INTERCOMNECT NOT PROTECTED AGAINST IITACT-TO-CONTINGENCY MODE TRANSITION

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

SCENARIO TO GET INTO PROBLEM

1. ENABLE OMS/RCS INTERCONNECT VIA ITEM 5 ON THE OVERRIDE DISPLAY
2. DECLARE AN ABORT WHICH REOUIRED OMS PROPELLANT TO BE DUMPED THROUGH AFT RCS JETS (RCS-ASSISTED OMS DUMP)
3. DURING THE FIRST 1.5 SECONDS OF THE INTERCONNECT PROCESSING, LOSS OF A SECOND SSME OCCURS, REQUIRING SINGLE ENGINE ROLL CONTROL

INTENT OF REQUIREMENT

- THE INTACT INTERCONNECT REQUIREMENTS DIFFER FROM THOSE FOR CONTINGENCY INTERCONNECT IN THAT THE ORDER OF VALVE OPENINGS/CLOSINGS IS REARRANGED (THE END VALVE CONFIGURATION IS THE SAME). THE INTENT OF THE REQUIREMENTS FOR THE CONTINGENCY CASE IS THAT PROPELLANT BE MADE CONTINUALLY AVAILABLE TO THE RCS JETS

HOW USER SEES EFFECTS

- THE ABORT CONTROL SEQUENCER COMMANDS JETS TO FIRE, JETS DO NOT FIRE, AND RCS RM WILL DESELECT THE AFFECTED JETS.
- THIS WILL CAUSE (1) LACK OF RCS ASSISTANCE IN DOING AN OMS DUMP AND (2) LOSS OF SINGLE ENGINE ROLL CQNTROL.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

ACTUAL CODE ERROR:

- A KEY PARAMETER IS CHANGED DURING A MULTIPASS SEGMENT OF A SOFTWARE SEQUENCE. AS A RESULT, RCS JETS CAN BE FIRED WITH NO PROPELLANT AVAILABLE AND THE JETS WILL BE LOST (HARDWARE FAILURE).

WHY NOT FOUND ON SYSTEM WHERE INTRODUCED

- THIS CODE HAS BEEN IN PLACE SINCE PRE-STS-1 (PRIOR TO MULTIPASS ANALYSIS PHILOSOPHY).

WHY NOT FOUND BY STS-2 MULTIPASS AUDIT

- SHOULD HAVE BEEN FOUND
- APPARENTLY, OVERLOOKED - HUMAN ERROR. IT IS FELT THAT THE PARTICULAR VARIABLE WAS ANALYZED AND EXPLAINED AWAY DUE TO CONFUSION OVER THE INTACT/CONTINGENCY REQUIREMENTS INTERFACES.

WHY NOT FOUND BY VERIFICATION TESTING

- THE PARTICULAR TIMING SCENARIO REQUIRED WAS NOT TESTED.

HOW THIS PROBLEM FOUND

- CODE REVIEW FOR NEW CHANGE IMPLEMENTED FOR FIRST AP-101S FLIGHT WITH MORE MEMORY AND SPEED (Ultimately be STS-43 first AP-101S flight with application changes)

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

OPS AFFECTED

- OPS 1/6

SIGNIFICANT CHANGES IN MULTIPASS ANALYSIS SINCE STS-2 AUDIT

- MULTPASS CONSIDERATIONS WERE ADDED TO THE DESIGN/CODE INSPECTION PROCESS
- REQUIREMENT INSPECTIONS WERE INSTI ITUTED TO ATTEMPT TO IDENTIFY AND CORRECT INCOMPLETE OR CONFUSING REQUIREMENTS.

ACTUAL ESCAPE IN PROCESS

- NONE. MULTIPASS AUDIT ADDRESSES THIS TIPE OF PROBLEM.

REASONS MISSED IN STS-2 MULTIPASS AUDIT

- THE METHODOLOGY BEHIND THE MULTIPASS AUDIT PROCEDURES ARE ADEQUATE TO POINT OUT THIS TYPE OF PROBLEM; HOWEVER, ANALYSIS IS REQUIRED FROM THAT POINT TO DETERMINE IF THE SCENARIO WHICH PRODUCES THE PROBLEM CAN ACTUALLY OCCUR. IN THIS CASE, THE REQUIREMENTS ASSOCIATED WITH ABORT TRANSITIONS ARE NOT CLEAR, POTENTIALLY ALLOWING THE SCENARIO TO BE REJECTED AS IMPOSSIBLE.

REASONS NOT FOUND IN FSW SHELF LIFE

- CONTINGENCY ABORTS ARE RARELY RUN IN SIMULATORS. IN ADDITION, THIS IS A SMALL WINDOW (ONE TIME ONLY FOR 1.5 SECONDS PER ASCENT) WHICH REDUCES THE CHANCE OF OCCURRENCE.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100329

SSME-OUT SAFING TASK NOT CALLED FOR ENGINE-OUT AT LIFTOFF

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DESCRIPTIQN OF PROBLEM

- REQUIREMENTS STATE THAT THE SSME OUT SAFING TASK I S CALLED WHEN AN SSME FAILS (THIS TASK COMMANDS A TWO-ENGINE POWER LEVEL EQUIVALENT TO THREE ENGINES OR A FULL POWER LEVEL T0 OBTAIN MAXIMUM VEHICLE PERFORMANCE WITHIN FLIGHT CONSTRAINTS). IF AN SSME FALLS WITHIN 40 MILLISECONDS AFTER SRB IGNITION, THE SSME OUT SAFING TASK WILL NOT BE EXECUTED. THE TASK I S NOT CALLED BECAUSE OF THE INCORRECT INITIALIZATIQN OF A PARAMETER USED BY GUIDANCE WHICH INDICATES HOW MANY SSME'S WERE PREVIOUSLY AVAILABLE. INITALIZED TO 0, SHOULD BE 3.

HOW USER SEES EFFECTS

- THE RESULTING TRAJECTORY COULD POTENTIALLY CAUSE STRUCTURAL LOADS AND ALPHA-HEATING PROBLEMS DURING FIRST STAGE. SEVERE PROBLEMS C0ULD ALSO OCCUR DURING AN RTLS ABORT MANEUVER BECAUSE OF ET HEATING.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

PROBLEM HISTORY AND CATEGORIZATION FROM DR ANALYSIS

- THIS PAST VALUE PARAMETER IS NOT EXPLICITLY DEFINED IN THE REQUIREMENTS
- INITIALIZATION STANDARDS ADDRESSING THIS TYPE OF PROBLEM HAVE BEEN IN PLACE SINCE PRE-STS1
- THE LACK OF PROPER INITIALIZATION FOR THIS PAST VALUE PARAMETER IS CONSIDERED TO BE ISOLATED 'ESCAPE' TO ESTABLISHED STANDARDS AND PROCEDURES AND HAS REMAINED UNDETECTED APPARENTLY DUE TO THE EXTREMELY SHORT WINDOW OF VULNERABILITY FOR ITS OCCURRENCE AND THE ACCOMPANYING LOW-PROBABI LITY SCENARIO REQUIRED

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR54961

INCORRECT PROCESSING FOR INVALID PORT ID

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DESCRIPTION OF PROBLEM

- ITEM 8 (BYPASS) AND 9 (RESET) ON THE ENTRY CONTROLS DISPLAY HAVE A TWO DIGIT DATA FIELD FOR THE AEROSURFACE SECONDARY ACTUATOR PORT TO BE RECONFIGURED. THE FIRST DIGIT SIGNIFIES THE DESIRED ACTUATOR AND THE SECOND DIGIT SIGNIFIES THE DESIRED CHANNEL. ENTRY OF THE FIRST DIGIT OTHER THAN 1-6 AND THE SECOND DIGIT OTHER THAN 1 - 4 WILL RESULT IN AN ILLEGAL ENTRY MESSAGE AND SHOULD HALT AN FURTHER PROCESSING. CURRENTLY SOFTWARE WILL ISSUE THE ILLEGAL MESSAGE, HOWEVER, I T WILL ALSO INCORRECTLY ASSIGN INT0 THE OUTPUT BUFFER SET AND RESET PARAMETERS USING THE INVALID PORT ID TO DERIVE THE SUBSCRIPTS.

HOW USER SEES EFFECTS:

- THE USER WILL NOT SEE ANY PORT ID FEEDBACK ON THE DISPLAY BECAUSE THE DEMAND UPDATE FLAG I S NOT SET. HOWEVER, THIS WILL CAUSE THE SOFTWARE TO CLOBBER OTHER SYISTEM SOFTWARE TABLES THAT ARE USED TO SET UP BASE REGISTERS FOR COMP0OLS AND LOCAL DATA, HOLD RETURN ADDRESSES TO CALLS TO LIBRARY FUNCTIONS, POINT TO EVENT VARIABLES , AND OTHER VITAL FUNCTIONS.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

ACTUAL CODE ERROR

- OMISSION OF INTENDED “DO/END” STATEMENTS
- DETAILED DESIGN SPEC FLOW CHART SHOWED INTENDED “DO/END” STATEMENTS; THUS,THE SOURCE CODE DID NOT MATCH THE DESIGN.

WHERE PROBLEM SHOULD HAVE BEEN FOUND

- CODE REVIEW, UNIT TEST

WHY NOT FOUND ON SYSTEM INTRODUCED

- THE PROBLEM WAS MISSED DUE TO ERROR IN THE HUMAN ELEMENT OF THE PROCESS. APPARENTLY, THE LENGTH OF THE "ELSE" PROCESSING (2.5 PAGES), WHICH INCLUDES MULTIPLE, NESTED, "DO/END” GROUPS, MADE THE OMISSION OF THE OUTERMOST "DO/END” MUCH LESS OBVIOUS.

WHY NOT FOUND IN TESTING

- UNIT TEST - CURRENT UNIT TEST PHILOSOPHY REQUIRES THAT PATH ANALYSIS BE DONE ON THE MODIFIED SOFTWARE; ALL DECISION POINTS MUST BE EXERCISED FOR ALL CONDITIONS AND BOTH PATHS. THIS WAS DONE FOR THE CODE IN ERROR; HOWEVER, THE DATA RECORDED FOR ANALYSIS DID NOT SHOW THE ACTUAL PATH TAKEN DUE TO THE FACT THAT ALL ERRONEOUS RESULTS EXISTED OUTSIDE THE SCOPE OF THE MODULE. (SHOULD HAVE BEEN FOUND)
- DETAILED VERIFICATION - TEST APPROACH WAS TO VERIFY CORRECT DISPLAY FEEDBACK AND ACTUATOR STATUS FOR LEGAL AND ILLEGAL VALUES, WHICH WAS OBSERVED TO BE PER REQUIREMENTS. FAILED TO OBSERVE THAT EXTRRNEOUS PROCESSING ALSO OCCURRED.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100775

Fail To Sync (FTS) DUE TO DISAGREEMENT IN TRANSMITTER STATIJS

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

TITLE: FTS DUE TO DISAGREEMENT IN TRANSMITTER STATIJS

- FOUND BY: SMS
- DESCRIPTION OF PROBLEM: IF A GNC DOWNLIST TOGGLE BUFFER RE-ASSIGNMENT OCCURS WHILE A STRING RE-ASSIGNMENT I S QUEUED, TRANSMITTER STATUS WORD A WILL NOT BE UPDATED FOR THE GPC THAT I S CHANGING STRINGS. WORD 6 WILL BE CORRECTLY UPDATED. WORD A AND B WILL NOT MATCH AND DURING I/0 ERROR PROCESSING, THE GPC WITH THE MISMATCH WILL GO TO A WAIT STATE.
- HOW USER SEES EFFECTS: IF THE PRIME CPC FAILS TO SVNC DURING AN OPS TRANSITION OR AN OPS MODE RECALL (OPS 1, 2, 3, 6 OR 8) AND A STRING IS BEING RECONFIGUEED, THERE I S A 2% PROBABILITY (3 MILLISECOND WINDOW OUT OF A 160 MILLSECONDS) THAT THE GPC'S CHANGING THAT STRING WILL GO TO A WAIT STATE (INACTIVE) .

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100775 - DESCRIPTION OF PROBLEM AS SEEN AT THE SMS

- A 3 GPC REDUNDANT SET WAS RUNNING IN GNC OPS 104 WITH THE FOLLOWING STRING ASSIGNMENTS: GPC1 STRINGS 1 & 4, GPC2 STRING 2 & GPC3 STRING 3.
- THE TRANSMITTER & RECEIVER FOR Flight Control String 1 (FC1) WERE FAULTED IN GPC 1 (INDUCED). THIS CAUSED UNIVERSAL I/O ERRORS ON FC1 IN ALL GPCs
- CREW'S RESPONSE WAS TO DO AN OPS MODE RECALL IN MM 104 WITH STRING ASSIGNMENTS AS FOLLOWS: GPC1 IN LISTEN MODE, GPC2 STRINGS 1 & 3, GPC3 STRINGS 2 & 4.
- AT OPS MODE RECALL GPC1 FAILED FROM REDUNDANT & COMMON SET DUE TO NON-UNIVERSAL I/O ERRORS WHICH WERE CAUSED BY THE INDUCED RECEIVER FAILURES.
- GPC1 FAILED TO SYNC (EXPECTED) AND GPCs 2 & 3 UNEXPECTEDLY WENT INTO A WAIT STATE. THE CAUSE WAS TRACED BACK TO A DIFFERENCE IN THE TRANSMITTER STATUS WORDS A & B (EACH GPC KEEPS TWO COPIES).

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100775 - DESCRIPTION OF THE SOFTWARE PROBLEM

- TWO IDENTICAL TRANSMITTER STATUS WORDS (A & B) ARE KEPT IN EACH GPC. THEY INDICATE WHICH FLIGHT CRITICAL BUSES THE GPC IS COMMANDING.
- AS PART OF I/O ERROR PROCESSING THESE STATUS WORDS ARE COMPARED TO EACH OTHER. IF THEY DIFFER THE GPC GOES TO THE WAIT STATE.
- THE TWO TRANSMITTER WORDS ARE SUPPOSED TO BE ALWAYS EQUAL UNLESS HARDWARE ERRORS OCCUR. HOWEVER, A SOFTWARE SCENARIO EXISTS THAT WILL INCORRECTLY RESULT IN TWO DIFFERENT TRANSMITTER STATUS WORDS.
  - BACKGROUND INFORMATION
- STRINGS ARE REASSIGNED BY FCOS ONE AT A TIME IN ASCENDING NUMBER ORDER.
- EACH STRING IS REASSIGNED IN TWO STAGES:
  - STAGE 1 - REQUEST - BUS RECONFIGURATION IS REQUESTED & QUEUED IF THE BUSES ARE BUSY. TWO MASKS ARE SAVED FROM THE SAME SOURCE AND LATER USED TO GENERATE TRANSMITTER STATUS WORDS "A" & "B"
  - STAGE 2 - SERVICING - THE QUEUED BUS RECONFIG REQUEST IS SERVICED WHEN THE BUSES ARE FREE. AS PART OF THE PROCESS THE TWO MASKS SAVED IN STAGE 1 ARE USED TO GENERATE THE TWO TRANSMITTER WORDS.
- THE MASK USED TO GENERATE TRANSMITTER STATUS WORD “A" IS ALSO USED BY OTHER FCOS PROCESSES THAT DEAL WITH BUS TRANSACTIONS. THIS IS NOT A PROBLEM.
- ANY PROCESS USING THE MASK WHILE A BUS TRANSACTION IS QUEUED IS SUPPOSED TO SAVE IT & RESTORE THE MASK AFTER USE.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100775 - DESCRIPTION OF THE SOETWARE PROBLEM (CONTINUED)

- THIS RULE IS VIOLATED BY THE GNC DOWNLIST TOGGLE BUFFER REASSIGNMENT FUNCTION IN ALL FLIGHT OPS. GNC DL DOES NOT RESTORE THE MASK AFTER USE. GNC DL LEAVES A ZERO MASK AFTER IT USES IT. THIS IS THE SOFTWARE PROBLEM.
- THIS MEANS THAT IF THE TOGGLE BUFFERS ARE REASSIGNED WHILE A FC BUS RECONFIGURATION REQUEST IS QUEUED, THEN THE TRANSMITTER STATUS WD "A" WON'T BE UPDATED (DUE TO A ZEROED MASK) WHILE TRANSMITTER STATUS WD "B" WILL BE CORRECTLY UPDATED.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 100775 HISTORY OF THE PROBLEM

- THIS PROBLEM HAS BEEN IN THE SOFTWARE SINCE PRE-STS1.
- PRE 0I02 BUS RECONFIGURATION HAD PRIORITY OVER I/O TRANSACTIONS. THIS MADE IT IMPOSSIBLE FOR TOGGLE BUFFER REASSIGNMENT TO RUN WHILE A BUS RECONFIGURATION REQUEST WAS IN THE QUE.
- THE OBJECT OF THE 0I-02 CHANGES WAS TO PREVENT HFE I/O JITTER.
- ON 0I-09 (AP-101S Upgrade GPC Prototype SSW system) TOGGLE BUFFER REASSIGNMENT IS DONE BY A COMMON FCOS FUNCTION THAT DOES ALL BUS REASSIGNMENTS. THEREFORE, THE PROBLEM DOES NOT EXIST ON AP-101S Systems.
- Problem corrected on AP-101B flights starting with STS-51L

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

DR 65325

MM601 (Ascent Flight Control) MODULES DISPATCHED IN MM603 (Entry Flight Control)

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

PROBLEM DESCRIPTION

- FSW DESIGN FOR TRANSITION FROM ASCENT SOFTWARE (MM 601) TO ENTRY SOFTWARE (MM602,MM603) DURING RTLS REQUIRES 480 MILLISECONDS IN MM602.
  - MFE MUST RUN 3 TIMES BEFORE UPDATING AN HFE DISPATCHER TABLE POINTER TO INVOKE 12.5 Hz ENTRY MODULES AS OPPOSED TO 12.5 Hz ASCENT MODULES
  - THREE MFE PASSES ARE REOUIRED IN MM602 TO INSURE CONVERSION OF DATA FROM M50 TO EARTH-FIXED"COORDINATE SYSTEM PRIOR TO USE BY MM602, MM603 MODULES .
- AUTOMATIC MM601 TO MM602 TRANSITION OCCURS AFTER -Z TRANSLATION: AUTOMATIC MM602 TO MM603 TRANSITION OCCURS WHEN VELOCITY IS BETWEEN 2500 AND 3200 FPS
- IF A MANUAL OR AUTOMATIC MM601-TO-602 TRANSITION OCCURS WHILE 2500 < VEL < 3200 THEN THE 602-TO-603 TRANSITION OCCURS BEFORE THREE MFE PASSES HAVE BEEN COMPLETED IN MM602
- END RESULT IS A MIXED BAG OF 25 Hz HFE ENTRY MODULES RUNNING WITH 12.5 Hz HFE ASCENT MODULES, CAUSING (SUSPECTED) SERIOUS CONTROL PROBLEMS
- ERROR WAS INTRODUCED IN THE SOFTWARE PRIOR TO STS-1 (LATENT PROBLEM)

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

PROBLEM SCENARIO

- ONE SCENARIO HAS BEEN IDENTIFIED BY IBM WHICH COULD MEET THE CRITERIA FOR MANIFESTATION OF THIS PROBLEM:
  - TWO ENGINE OUT RTLS
  - VEHICLE HEADED BACK TO LAUNCH SITE (POST-FLY BACK)
  - MECO WITH VELOCITY IN THE SPECIFIED RANGE (POSSIBLY CAUSED EARLY DUE TO A DATA PATH ERROR)
- ATTEMPTS TO SIMULATE THIS FAILURE IN THE SDF HAVE BEEN UNSUCCESSFUL
  - VEHICLE CONTROL IS HARD TO PREDICT DURING RTLS SCENARIOS
    - DUE PARTLY TO IMPRECISE AERODYNAMIC MODELS FOR THAT REGIME (ALL SIMULATORS)
    - DUE TO SDF/SPF LACK OF "PAPER PILOT" TO SIMULATE CREW MANUAL INPUTS
  - OUR SIMULATIONS LOSE CONTROL PRIOR TO 602/603 TRANSITION (DUE TO SDF/SFP LIMITATIONS ABOVE) DURING THE PARTICULAR SCENARIOS TESTED
- IF THE VEHICLE CAN FLY TO THE DESCRIBED POINT, THE SOFTWARE ERROR WILL PROBABLY RESULT IN LOSS OF CONTROL PRIOR TO DITCH

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

HOW PROBLEM FOUND

- DETAILED VERIFICATION
  - FOUND PROBLEM IN AP-101S SYSTEM TEST CASE
  - MANUAL PRO TO MM602 WHILE SSME'S STILL BURNING
    - THE TEST SCENARIO GENERATED IS CATASTROPHIC, BUT WAS DONE TO SAVE VERIFICATION TESTING RESOURCES

No valid, realistic demonstration of problem believed possible.

Copyright James K. Orr 2015

Flown LOCV DR's Found After STS-51L and Prior to STS-26

Future actions taken:

- INCREASED EMPHASIS ON OFF-NOMINAL TEST SCENARIOS
  - POSSIBLE SCENARIOS ARE UNLIMITED; ONLY A LIMITED NUMBER OF SCENARIOS CAN BE SIMULATED
- REQUESTED NASA INPUT ON THE SELECTION OF OFF-NOMINAL SCENARIOS TO BE TESTED
  - COST/BENEFIT TRADE-OFF

For Future Development Systems, a subset of Performance Verification cases was allocated to “Off-Nominal” test scenarios with input from NASA

Copyright James K. Orr 2015

Flown LOCV DR's Found Prior To STS-51L

Flown LOCV DR’s

Found On Or After STS-26

NONE

Copyright James K. Orr 2015

Never Flown

LOCV DR's Found After Verification Complete (Including SAIL Verification)

NONE

Copyright James K. Orr 2015

Never Flown

LOCV DR's Found Prior To Verification Complete

(Including flight specific SAIL Verification)

Copyright James K. Orr 2015

Never Flown LOCV DR's Found After Verification Complete

When Found	October 7, 1982 - CREW SMS TRAINING; October 8, 1982 – SAIL Test
Missions Flown At Risk	None
Error Title	DR 50788 - OMS TO RCS INTERCONNECT AND 20 NULL RCS JETS FIRING NOT TERMINATED DURING A CONTINGENCY DUMP WHEN Nz > 0.05 G's
Probability Of PASS Error	100 % For CONTINGENCY DUMP IN MM602
BFS Engage	BFS engage would not result in recovery. PASS error results in no fuel path to RCS jets for vehicle control or propellant dump.
Error Introduced	Changed for STS- 5. WHILE PERFORMING A CONTINGENCY DUMP IN MM602, THE 20 NULL RCS JET FIRING AND THE ASSOCIATED OMS TO RCS INTERCONNECT DID NOT TERMINATE AS EXPECTED WHEN THE NORMAL ACCELERATION (Nz) EXCEEDED 0.05 g's, INVESTIGATION SHOWED THAT THE Nz LIMIT I-LOAD HAS THE VALUE OF 1.61 G's INSTEAD OF THE REQUIRED 0.05 G's VALUE. Error introduced when a constant (0.05) was converted to a mission reconfigurable value. Value supplied for mission needed to be converted from units of feet per second (requirement units) to 0.05 g's (FSW implementation units).
Visibility	Very High. Ultra simple change was incorrectly implemented. Released with only code inspection (no testing).

Copyright James K. Orr 2015

Never Flown LOCV DR's Found After Verification Complete

When Found	March 22, 1983 – Found By SMS In Doing Flight Software Integration Prior To Crew Training Start
Missions Flown At Risk	None
Error Title	DR 51057 - INCORRECT GUIDANCE PAIUMETERS PASSED TO THE BFS
Probability Of PASS Error	100 %
BFS Engage	PASS would have performed correctly. Following BFS engage, BFS guidance would not work correctly in OPS 1.
Error Introduced	STS- 8 Recon 1 system. Within the 13th set of data output by the PASS to the backup computer during the one-shot transfer in G9, pitch bias slopes (2 parameters) and pitch bias intercepts (2 parameters) are in reverse order from the sequence expected by the backup flight system. This parameters were sent to PASS during G9 (Ground Operations at KSC) as late mission specific updates to address day of launch winds.
Visibility	Relative minor. PASS change made. Error made in order of terms. Discovered immediately in first integrated verification of PASS to BFS interface during flight system integration for SMS training. Released without verification of interface on BFS side by PASS verification. Would also have been found in SAIL testing of PASS and BFS together.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found Prior To Verification Complete

When Found	April 19, 1985 by PASS Verification After Early Release (before Verification Complete) to SAIL and SMS.
Missions Flown At Risk	None
Error Title	DR 61229 – Yaw Filter Switch Not Performed Properly
Probability Of PASS Error	Nearly 100 %. CR 79167A (for filament wound case SRBs) added a yaw filter "switch" to First Stage (SRBs burning). The check was placed in a location that would not be cyclically executed. Needed to execute cyclically to switch on required velocity cue.
BFS Engage	BFS Engage would be successful if PASS incorrect behavior detected.
Error Introduced	Late on OI-7 just prior to early release to SAIL and SMS for additional verification time and additional crew training time.
Visibility	Minimum. Found by verification. Only listed due to found after an extraordinary early release to maximize SAIL verification and SMS crew training due to extremely late change implementation relative to normal OI development/verification template.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found Prior To Verification Complete

When Found	December 15, 1985 by PASS Verification After Early Release (before Verification Complete) to SAIL and SMS.
Missions Flown At Risk	None
Error Title	DR 58906 – OMS Engine Redundancy Management Not Running For OMS Dump In Major Mode 304
Probability Of PASS Error	100 %
BFS Engage	BFS engage would be successful if abnormal PASS behavior recognized.
Error Introduced	Immediately Prior To Release For OI-7C (changes to support Centaur upper stage on Space Shuttle). PASS would not alert the crew to an OMS engine failure following commanding an OMS propellant dump in MM 304. Part of software changes to allow ascent abort with Centaur upper stage.
Visibility	Minimum. Found by verification. Only listed due to found after an extraordinary early release to maximize SAIL verification and SMS crew training due to extremely late change implementation relative to normal OI development/verification template.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found After Verification Complete

When Found	March 4, 1987 during Crew SMS Training Following Flight Specific I-Load Changes
Missions Flown At Risk	None
Error Title	DR 100781 - Guidance Failure On 3 Engine TAL Pre Press To MECO
Probability Of PASS Error	100 %
BFS Engage	BFS Engage Successful
Error Introduced	Coding Error Introduced With TAL for STS-5. However, first exposure on STS-28 Recon 1 system when Mission Specific I-Load values first allowed incorrect code to execute.
Visibility	Very High. Latent code error protected by specific mission dependent I-Load discovered by crew training in SMS. THIS PROBLEM WAS INTRODUCED IN RELEASE 19.07 (STS-5) WITH THE IMPLEMENTATION OF THE ORIGINAL TAL CR (39401A). • THE TEST FOR TFAIL WAS PART OF A BLOCK OF CODE CORRESPONDING TO THE GUIDANCE PARAMETER RE-INIT TASK. THIS WAS DONE FOR EFFICIENCY PURPOSES AND WAS CORRECT PRE 19.07 (prior to STS-5 flight). • IMPLEMENTATION OF THE TAL CR MADE THE RE-INIT TASK EXECUTABLE ONLY IF NO TAL WAS DECLARED. THE TEST FOR TFAIL WAS INCORRECTLY LEFT IN WITH THE RE-INIT TASK. CONDITIONS FOR EXECUTING RE-INIT TASK WERE CHANGED AGAIN TO EQUIVALENT CONDITIONS (WITH RESPECT TO TAL ABORTS) BY CR 69555 (TAL WEATHER ALTERNATE) ON 0I7.03. THE PROBLEM COULD HAVE BEEN FOUND THEN BUT THE BLOCK OF CODE REMAINED UNCHANGED.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found After Verification Complete

When Found	August 1, 1987 Found By Code Review By Assigned Developer
Missions Flown At Risk	None
Error Title	DR 110419 – GPS Commfault Status Indicator Missing In Flight Control Operating System
Probability Of PASS Error	100 % for scenario of 3 string GPS flight and multiple errors in both an I/O error on the Flight Forward MDM 2 (FF2) GPS Read and an inability to communicate information on that error across the GNC Redundant Set.
BFS Engage	BFS Engage Successful
Error Introduced	Error introduced on Operational Increment OI-8B supporting STS-26. However, the code could not be executed until 3 string GPS hardware was installed. Error was found by PASS development prior to any flight with 3 string GPS hardware installed.
Visibility	Generally positive. Another latent code error was identified between STS-51L and STS-26. Discovery of error lead to development of an audit of I/O tables in the operating system, and identification of process improvements to avoid similar problems in the future.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found After Verification Complete

When Found	September 18, 1987 By SAIL
Missions Flown At Risk	None
Error Title	DR 100762 -OMS/RCS INTERCONNECT INITIATED AT MECO
Probability Of PASS Error	100 % For The Scenarios Of The DR.
BFS Engage	BFS Engage Not Successful. Orbiter hardware affected (no propellant to RCS jets in Ops 1/6 and electrical system overload in OPS 3).
Error Introduced	Error introduced on OI-8A (part of accelerated development for STS-26). A REQUIREMENTS PROBLEM WAS IDENTIFIED FOR A CONTINGENCY INTERCONNECT REQUESTED WHILE AN INTACT INTERCONNECT IS IN PROGRESS OR COMPLETED. CR 89185A WAS WRITTEN TO RESOLVE THIS ISSUE. ABORT SEQUENCER TASK FORCE MET TO DISCUSS "AS IMPLEMENTED OI8A" SOFTWARE AND PLANNED OI-8B (flown on STS-26) IMPLEMENTATION. THE LETTER OF CR 89185A DID NOT SATISFY THE INTENT TO SOLVE THE REQUIREMENTS ISSUE. AN AGREEMENT ON INTENT WAS RESOLVED AND WORDING WAS RESOLVED TO DOCUMENT INTENT (CR 89237). THE DESIGN FOR CR's 89185 AND 89237 IMPLEMENTED THE INTENT AS UNDERSTOOD BY THE COMMUNITY (ABORT SEQUENCER TASK FORCE). THIS PROBLEM SCENARIO WAS NOT RECOGNIZED WHEN WRITING REQUIREMENTS OR DESIGN. SPECIAL CODE INITIALIZATION TO COVER THE SCENARIO WAS NOT MADE (ALL LOGIC CHANGES WERE CORRECT).
Visibility	Very High. Error reflected continuing difficulty to address all OMS/RCS Scenarios for all software permitted scenarios, including contingency aborts.

Copyright James K. Orr 2015

Never Flown LOCV DR's Found Prior To Verification Complete

When Found	April 29, 1988 By PASS Inter-Process Variable audit. System released early to SAIL and SMS prior to verification complete.
Missions Flown At Risk	None
Error Title	DR 102466 – OMS/RCS Interconnect Sequence Ignores Commfault
Probability Of PASS Error	100 % for unlikely scenario requiring multiple failures.
BFS Engage	BFS Engage Successful
Error Introduced	Error introduced on OI-8A (part of accelerated development for STS-26).
Visibility	Relatively Minor. Change had significantly added protection for OMS/RCS Interconnect by monitoring actual state of propellant interconnect valves. Requirements addressed the case of inability to determine the state of the value due to no input (commfaulted data). For one input, an incorrect variable was used for commfault status. This exposed the possibility of divergent processing within the Redundant Set leading to a probable Fail-To-Sync. Error detected by Inter-Process Variable audit which verified that correct Commfault variable was used.

Copyright James K. Orr 2015

Alternate View
PASS LOCV Released Errors

Copyright James K. Orr 2015

PASS FSW FMEA SEVERITY ASSESSMENTS

- SEVERITY #1 - SEVERE VEHICLE OR CREW PERFORMANCE IMPLICATIONS
  - INCLUDES LOSS OF VEHICLE OR CONTROL (MUST BE FIXED - MAINTAINED ON CRITICAL ITEMS LIST UNTIL FIX COMPLETED AND VERIFIED)
- SEVERITY #2 - AFFECTS ABILITY TO COMPLETE MISSION OBJECTIVES
  - NOT A SAFETY ISSUE
  - MUST BE FIXED
- SEVERITY #3 - VISIBLE TO USER (NOT SEVERITY 1 OR 2) MINIMAL EFFECTS ON PROCEDURES OR WORKAROUND AVAILABLE
  - USUALLY OPS NOTED AND WAIVED
  - NCLUDES 1N & 2N FOR QUALITY STATISTICS

(NOT VISIBLE TO USER)

- SEVERITY #4 - INSIGNIFICANT VIOLATION OF REQUIREMENTS
  - INCLUDES DOCUMENTATION AND PAPERWORK ERRORS
  - INCLUDES INTENT OF REQUIREMENTS MET
  - INCLUDES INSIGNIFICANT WAIVERS (WITHOUT OPS NOTES)
- SEVERITY #5 - NOT A FLIGHT, TRAINING, SIMULATION, OR GROUND CHECKOUT ISSUE
  - MAINTENANCE ISSUES
  - PROGRAMMING STANDARDS VIOLATION

Copyright James K. Orr 2015

PASS FSW FMEA SEVERITY ASSESSMENTS

DISCRIMINATORS:

- SEV 1 - REGARDLESS OF PROBABILITY OF OCCURRENCE OF CODE PROBLEM FOR ALLOWED "OPERATIONAL SCENARIO", THE CODE PROBLEM CAN CAUSE LOSS OF CONTROL, EXPLOSION, OR OTHER HAZARDOUS EFFECT.
- SEV 1N - A PROBLEM IS SEVERITY 1N IF ESTABLISHED/REASONABLE PROCEDURES PRECLUDE ANY OPERATIONAL SCENARIOS FOR WHICH PROBLEMS EXISTS.
  - IF UNUSUAL/UNREASONABLE ACTION IS REQUIRED TO AVOID THE PROBLEM OR EFFECT, THEN THE PROBLEM IS SEVERITY 1.

    OR
  - NUMBER OF FAILURES REQUIRED TO EXECUTE CODE PROBLEMS EXCEEDS DESIGN REQUIREMENTS FOR SOFTWARE OR SYSTEM (NOTE: NUMBER OF FAILURES REQUIRED WILL BE SPECIFIED ON DR ANALYSIS AND DR MANAGEMENT FORMS)

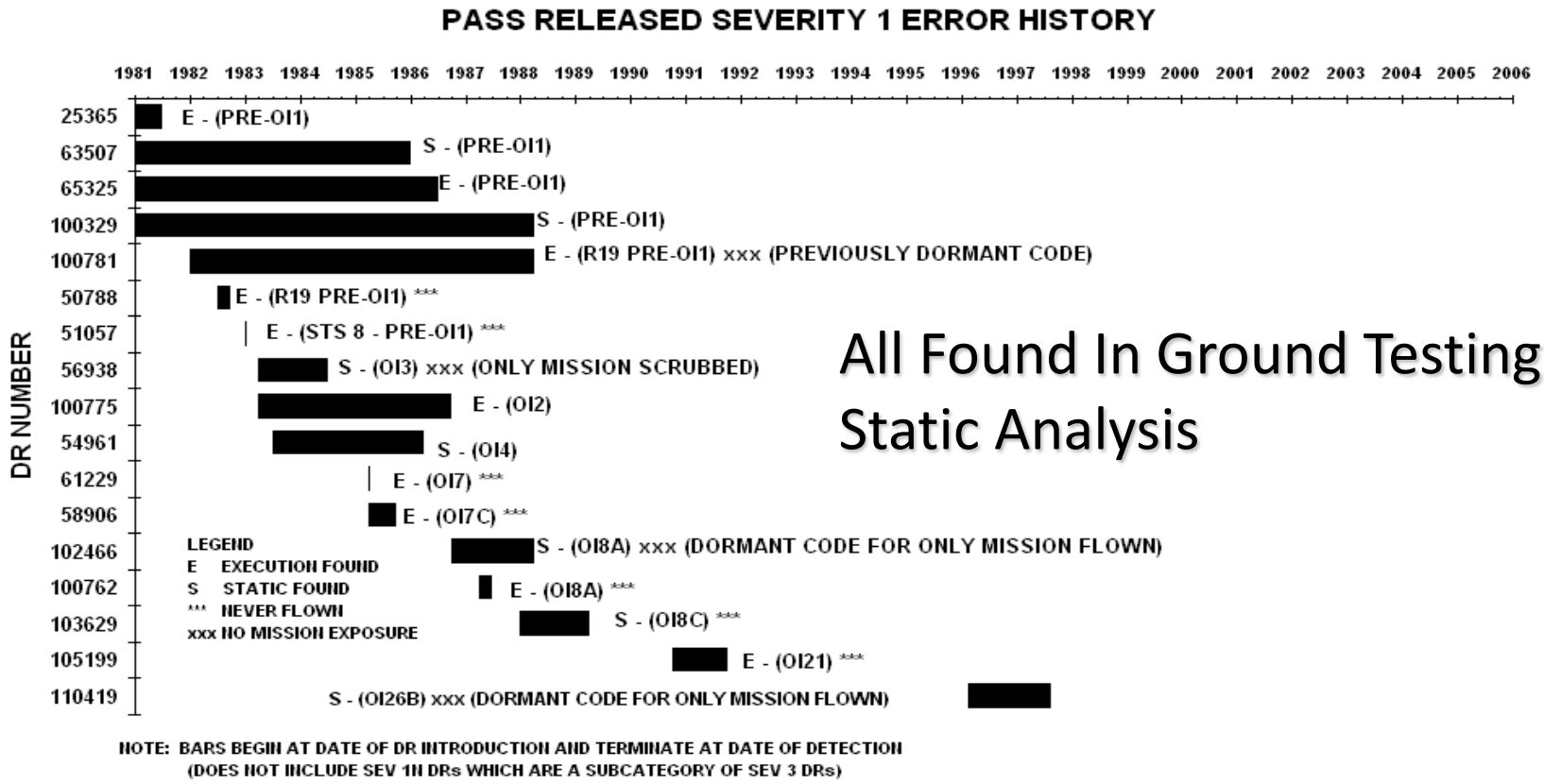
Copyright James K. Orr 2015

PASS FSW FMEA SEVERITY ASSESSMENTS

- ILLUSTRATIVE EXAMPLES FOR SEV 1 AND SEV 1N:
  - TIME DELAY IN VALVE PROCESSING IS ZERO CAUSING POTENTIAL FOR EXPLOSION IN FUEL LINES (SEV 1)
  - EXECUTION OF LATE SSME CHECK DURING IGNITION (SEV 1N)
  - RE-ENABLE OF INTERCONNECT CAUSES 'HARD LOOP' IN CODE EXECUTION RESULTING IN PASS LOSS (SEV 1)
  - FLYING - 90 DEGREES PITCH RESULTS IN LOSS OF CONTROL DURING MM305 (SEV 1N)
  - EXECUTION OF VENT DOOR SEQUENCER IN OPS1 CAUSES UNPREDICTABLE INDEXING (SEV 1)
  - FOUR FAILURE SCENARIO LEADS TO LOSS OF CONTROL (SEV 1N)

Copyright James K. Orr 2015

PASS Released Severity 1 Error History



All Found In Ground Testing or Static Analysis

Copyright James K. Orr 2015

PASS SEVERITY 1 DR BREAKDOWN

ALL SEVERITY 1 DR's (1981 - PRESENT)

- CLASS 1 (CODE BREAK)
  - • 17 CODE ERRORS RELEASED *
    - 15 PERTAIN TO ASCENT ONLY
      - 4 FOUND BY SMS
      - 2 FOUND BY SAIL
      - 8 FOUND BY PASS FSW
      - 0 FOUND BY KSC
      - 1 FOUND BY MDAC (SUB TO NASA)
      - 0 FOUND IN FLIGHT 3
    - 1 PERTAINS TO ENTRY ONLY
      - FOUND BY PASS FSW
    - 1 PERTAINS TO ASCENT & ENTRY
      - FOUND BY PASS FSW
- MOST RECENT LATENT SEV 1 CODE ERROR FLEW IN 1986 (DR100775 FOUND 10/22/86)
- RELIABILITY STATISTICS
  - 10 FOUND IN EXECUTION
  - 7 FOUND BY STATIC FMEA

Copyright James K. Orr 2015

PASS SEVERITY 1 DR BREAKDOWN

ALL SEVERITY 1 DR's (1981 - PRESENT)

- 7 FOUND AND FIXED BEFORE FLIGHT (NEVER FLOWN)
  - 1 FOUND AND FIXED BEFORE FLIGHT, ALTHOUGH PRESENT ON EARLIER SCRUBBED MISSION
- 3 PRESENT IN SOFTWARE FLOWN, BUT IN DORMANT CODE
- 11 OF THE TOTAL 17 TO WHICH CREW WAS NOT SUBJECTED

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
25365	1	PASS System Hung Up in MM602	With all induced failures described on the Scenarios to Produce Error section, at T+11:25 the PASS GPC's started showing instruction minitor errors in the GPC error log and then all CRT's were X'ed out. About 10 secs later BFS was engaed. There was no CAM lights on, Talkbacks remained in Run and GPC's did not respond to engaged, i.e. did not go to Wait.	System-wide Audit to identify the problem that could happen during the Multipass scenario and corrected code.	Problem existed Pre STS-1	Found on 9/30/81 by SMS	Simulation of contingency abort that the flight had been flown into Second Stage (After SRB SEP). Induced failures to cause all three main engines to shut down prematurely. The timing of fault was such that the crew was forced to select a contingency abort to ROTA, Spain.	The error was missed because the problem was scenrio dependent and occurred in small timing window ---- * Recommended to develop system audit procedure and checklist procedure; Complete search for "DO case". Train system audit personnel. Identify modules with exposure.	The FSW modules in question were intended to be running during this abort case. There were test cases performed for many contingency abort scenarios but not the specific scenrio that occurred during crew training session. There has been no similar Abort case ever happened to Shuttle Program.
50788	1	Deleted I-Load for RTLS NZ-Limit Has Wrong Source Value	While performing a contingency Dump in MM602, the 20 NULL RCS jets and the associated OMS to RCS interconnect were not terminated as expected when the nomal acceleration exceed 0.05 G's. Investigation showed that Nz_LIMIT has the value of 1.61 G's instead of the required 0.05 G's. This problem was caused by implementing CR 29551B to delete 23 I-loads and made them constants or initialization parameters. One of these parameters was in a derived equation to obtain the proper units.	Patch to Mass Memory for flight.	Introduced to FSW on 7/1/1982 by CR29551B	Found on 10/07/82 by SAIL	Ran SAIL testing in RTLS abort case	The error occurred in part because the change was felt to be virtually risk free. The error was missed because the problem was scenrio dependent -- Recommended to review other I-Loads Conversion to constant by the same CR. Re-inforced the culture than any change to PASS FSW has the potential to be Severity 1.	Obvious error caught during SAIL Integrated Avionics Verification. The error was caught and corrected before the software was ever flown on any real flight.
51057	1	BFS One-Shot Xfer Param Reversed	The 13th set of data output by PASS during the one-shot transferwas in the wrong order such as: P_SLP (1) & (2), P_INT (1) & (2), DEL_CST (1) & (2), V_EO_SW, and TREF_ADJUST. BFS expects P_INT to be transferred before P_SLP (the rest of the data is in the correct order).	Patch to Mass Memory for flight.	Introduced STS-8 RC1 (2/83)	Found on 3/22/83 by SMS (Not Flown)	Ran in SMS and checked for interfaced data between PASS/BFS.	Error was missed because PASS/BFS interface not sufficiently tested -- Recommended to improve testing and re-audit BFS one shot transfer parameter order.	Obvious error caught during crew training in the SMS. The error was caught and corrected before the software was ever flown on any real flight.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
54961	1	Process Out of Range Port IDs Incorrect	Illegal entry on the Entry Control Display (ECD) panel created a warning message and assigned data to output buffer but also reset parameters using the invalid port ID. User would not see any port ID because the port ID parameter was reset. This will clobber other system software.	Released Note on OI7 & OI7C for possible workaround and fixed code on OI8A to add a 'DO/END" case statement around the bypass and reset case processing.	Error was introduced in software built OI04.04 on 8/83 by CR 29444C.	4/30/1986 by IBM Developers	Performed an illegal entry on the ECD pad.	The error was missed because the display response was correct even though the port ID was invalid internally to software. --- Recommended a re-review of CR implementation. Audited the coding of the indexing and illegal entry.	These entry activities on the ECD panel are mostly done while On-orbit or on the ground. The chance for error to be occurred and caused LOV/LOC is probably none due to the frequency of usage of key entry during Ascent and Entry and the severity of the error's impact.
56938	1	Data Homogeneity Violation	IBM identified insufficient "data homogeneity margins" for FSW commands to the Master Events Controller (MEC) which trigger SRB SEP and ET SEP. If all 3 commands from MEC SOP are not output for the same computation cycle (40 ms rate) then SRB SEP or ET SEP may not occur.	Patch to allow MEC SOP to finish on the same computation cycle.	Introduced to FSW OI3.04 built on 4/83.	Found by IBM Verifier (System Analysis) on 7/23/84 (Not Flown – Original flight scrubbed on PAD)	Code Analysis.	The error was missed because the problem was scenrio dependent and occurred in small timing window -- Recommended a complete system training study and audit of all data homogeneity measurements made.	This DR was not exposed to any mission due to an Pad Abort after SSMEs started. Problem corrected prior to next launch attempt. .
58906	1	OMS FDIR Not Running in MM304	Upon executing an "OMS Dump Enable" in MM304 (Entry mode), OMS engine RM was not activated as required because the two flags necessary to activate the OMS Engine FDI module were not 'Phased" correctly. The problem was introduced with the implementation of CR79134E OMS Dump in MM304. The user will not be alerted to OMS engine failures since OMS engine RM (Redundancy Management) is not being performed.	Source code fixed for flights.	Introduced to OI-7C.12 software built on 6/85.	Found by IBM verifier on 12/15/85.	Performed OMS Dump Enable in MM304 scenario.	The error was missed because the problem was scenrio dependent --- Recommended to add "Modules Running" analysis t selected test cases.	The error was fixed before flights either in patch or source code correction.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
61229	1	Yaw Filter Switch Not Performed Properly	CR 79167A (for filament wound case SRBs) added a "switch" yaw filter to First Stage in the Ascent DAP. However, the check for when to switch was placed under a test for First Stage that will NOT be cyclically executed. It will be executed only when external events (such as Engine Failures) occurs. This is unacceptable since the yaw filter will therefore NOT switch on the required velocity cue.	Review CR implementation	Introduced in OI-7.07 on 4/85 when implementing CR 79167A.	Found on 4/19/85 by IBM Level 7 Testing	Not presented due to DR found by Verification prior to release (CI).	The error was missed because there were oversight on code review and Unit Test. --- Recommended to review CR implementation.	DR was discovered during the verification cycle prior to release (CI). However, due to requirements for an early release, the DR was released on initial SAIL test system. The problem was discovered and corrected before any real flight was flown on the software.
63507	1	I-Connect Not Protected Against Intact-to-cont Transition	If an Intact-To-Contingency abort mode transition occurs during the first 1.5 secs. of an OMS/RCS interconnect or Return-To-Normal (ICNCT/RTN), the processing of the interconnect or Return-To-Normal will erroneously indicate Complete. While no propellant is available to the RCS jets, subsequent use of the jets prior to acutal completion of the ICNCT/RTN will result in jet failures. This is not a problem if the mode transition occurs before the first pass of CSI or after the 1.5 secs window.	Abort Sequence Audit, Indexing Audit, Multi-Pass Audit, Illegal Entry Audit.	Introduced since the beginning Pre- ST51	Found by IBM Level 7 Testing on 3/11/86	Intact-To-Contingency abort mode transition occurs during the first 1.5 secs. of an OMS/RCS interconnect or Return-To-Normal (ICNCT/RTN)	Oversight in Multi-pass analysis; Scenario dependant. --	Multiple flights were flown with this ascent exposure. Exposure was mitigated by the Contingency Abort scenario as well as small timing exposure during which the Intact to Contingency abort downmode had to occur. There has been no similar Abort case ever happened to Shuttle Program.
65325	1	MM601 Modules Dispatched in MM603	Upon Transition from RTLS abort case MM601 (Ascent) to MM602/603 (Entry) The PASS FSW executed 480 ms delay in MM601 to ensure all Ascent SW data conversion modules were completed prior to allowing Entry SW modules to run. However, if the velocity was between 2500 to 3200 fps (I-load value) or a Manual transition was initiated then a mixed bag of Ascent SW modules were running with Entry SW modules causing suspected serious control problem.	Fixed source code to add another condition for automatic transition to MM603.	Introduced Pre-ST51	Found by IBM Verification testing in 7/86	Manual or automatic MM601 to MM602 transition while vehicle velocity is in the range of 2500 fps (ft / sec) to 3200 fps	The error was missed due to multiple passes of a module require to accomphish a function and off-nominal flight scenarios -- - * Recommended to Involve tracking which modules are running at any give time and flags deviation from the expected. * Increased emphasis on Off-Nominal test scenarios.	The problem existed since the beginning and 25 missions were exposed prior to discovering of this error. The FSW modules in question were intended to be running during RTLS abort case. There were test cases performed for many contingency abort scenarios and also there was no Abort case ever happened to Shuttle Program therefore there was no chance to know how the FSW would behave during abort in real life.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
100329	1	SSME Out Safe Task, Not Perform For Engine Out at Lift-off	When an SSME fails within 40 ms after SRB ignition, the SSME out safing task was not executed as called out by the requirement. The task was not called because of the incorrect initialization of a parameter used by Guidance which indicates how many SSME's were previously available. This could potentially result in structural loads and alpha-heating problems during First Stage (MM102). The depressed trajectory would also pose significant problems during RTLS abort maneuver due to ET-heating and P-total exceedances.	Patched for STS 26, 27, and 28. Code fixed for flights STS 29 and 30 to properly initialize Past Value Parameters.	Introduced Pre-STS1	Found on 4/21/88 by IBM during requirements to code mapping analysis.	Desk Analysis	Error was due to requirements which did not explitcitly define Past Value Parameters.. ---- Recommended to consider the need for audits to detect any additional oversights of this nature.	No SSME failure right after ignition was ever happened in real flights so the SW error was not manifested even though the described problem existed since Pre-STS1.
100762	1	OMS/RCS Intercon Seq Problem	Due to incorrect initialization, if the OMS/RCS interconnect sequence is called for the first time with a return to normal request, then the sequence will incorrectly initiate an "Interconnect" followed by a return to normal sequence. This results in an unexpected 4.5 sec. interval without a fuel path to the Aft RCS jets. In OPS 3, the erroneous interconnect is done using a 0.16 sec interval between sequence steps (nominally 1.6 sec). This will cause electrical system overload.	Code change on OI8A and OI8B to prevent the OMS/RCS Interconnect Seq from being activated with a request for a Return-to-Normal without having previously performed an Interconnect. On OI8C, additional changes to the OMS/RCS Interconnect Seq to cause termination of the sequence if it is called with a request to perform a Return-to-Normal when the current state is already a normal configuration.	Introduced to OI8A.9 on 4/87.	Found by SAIL on 9/17/87.	The problem would occur whenever an OMS/RCS Return-to-Normal request is made without frist performing an Interconnect such as (1) Interconnect Inhibited; Abort declared (RTLS, ATO, TAL) (2) OMS-only (non-interconnect) dumpt in OPS 3.	Error was blamed on rush schedule and piecemeal requirement that leaded to a "narrow" focus on new capability. -- More aggressive testing scenario is recommended such as considering other OMS/RCS Interconnect scenarios.	Obvious error caught during SAIL Integrated Avionics Verification. The error was caught and corrected before the software was ever flown on any real flight.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
100775	1	GPCs Go To Wait State Due To Disagreement in Xmitter Status	If the prime GPC fails to sync (due to a hard failure) from a three or more GPC redundant set during an OPS mode recall request with restringing of multiple flight critical data buses, it is possible that two good GPCs may also fail to sync by entering the software halt. This is due to disagreements between these good GPCs in the two software copies of the flight critical transmitter status mask.	Fixed source code to correctly saved and restored the transmiter mask after used for any process that was using the mask while a bus transaction is queued.	The problem has been in the software since OI-2.	Found by SMS on 10/22/86	* A non-universal I/O error must occur in a prime GPC on FC string 1, 2, or 3 at an OPS mode recall. * The next higher numbered FC string from the one with error must be changing Commander between two Non-Prime GPCs. * The reconfiguration for the string in error must occur in close proximity to the HFE timer which preceded on MFE cycle.	Error was missed because IPV tools and standards were not in place when problem was introduced. Complex scenarios needed to catch the problem. ---- * Audit is recommended on all FCOS process that are performed in two or more states (queue and Service). * Audit all "Mutually Exclusive Process" IPV Alibies. * Repeat a study of All "Latent" found DRs to aid in the definition of required audits.	There were no GPC's fail as described in the scenario in any real flight therefore the error was not manifested during any previous flights.
100781	1	Guidance Failure for 3 Eng TAL	If a 3 engine TAL abort is declared prior to TFAIL (Failed Time) from I-Load, PASS Guidance software directs the vehicle straight up or down and a loss of vehicle control would occur. This problem is caused by Second Stage Guidance getting stuck in the thrust Phase 1. TFAIL is uesd to transition from Second Stage Guidance to Thrust Phase 2. The check for TFAIL was put into the wrong section of the code.	Source code was fixed with logic to test for TFAIL at the appropriate code location.	Introduced in Release 19.07 on 1/82.	Found by SMS on 3/4/87 (dormant where flown)	* Declared a 3 engine TAL with PRE Press to MECO to cause a PASS Guidance failure.	Error was missed due to oversight on Design & Code Inspection and testing ---- More vigerous test scenarios should be implemented. More efficiency in code documentation and audit in requirement to code mapping.	Flight Design dependent. Code in error was dormant in all flight exposures due to flight specific ILOAD values which precluded the error. Error was found during crew training on the first system with flight specific exposure.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
102466	1	OMS/RCS Intercom Seq Ignores COMMfault	Module GSI (Abort OMS/RCS Interconnect) monitors the RCS Tank Isolation Valves Closed status and terminates the sequence after three consecutive passes of False status. However, the referenced valve position status data is being processed without the validity check via the COMMFault status. When the input data is COMMFaulted, there is no guarantee that all redundant GPC's will have the same inputs. There is a potential for divergent processing leading to a probable Fail-To-Sync situation within the Redundant Set and the firing of jets from isolated manifolds.	Waiver and OPS notes for STS-26 due to non- use of OMS/RCS Interconnect on the flight and problem only occur during Interconnect. Patches for STS 27, 28, 29 and 30. Source code was fixed to correct the described problem for the rest of the STS flights that used OI-8B.	Introduced in OI-8A.07 on 10/86	Found by IBM IPV Audit on 4/29/88	Code analysis; Problem only occurs during intact interconnect. Multiple failures are required for problem to occur.	The error was missed because Code review and Unit Test oversight. --- More audit on code, clean up ambiguous requirements and more tests in the presence of CommFaults.	Error was detected during audits prior to STS-26. There was no exposure on STS-26 due to the specific mission design. Error was fixed on all future flights.
103629	1	Incomplete OPS Overlay	Program overlays for Phase OPS transition (OPS G1, G2, or G3) require two phases to be retrieved from Mass Memory Unit. If a Dual/Split Phase OPS overlay is attempted and at least one but not all of the GPC's in the target set receive errors on the alternate bus while acquiring the first phase of the overlay, then the non-erring GPC's will indicate a successful program overlay although they contain incomplete program overlays.	* Patch for STS-31, 32, 34, 36 final loads. (OI-8C) * Source fix for STS-35, 37, 38, 39 40 RECON 1 (OI-8D). * Source fix on RECON 1 for all OI8F Flights. * Source fix on OI20 to correct the described problem.	Introduced in OI8C on 01/88 because of DR 100792 (MMU Transaction Error Recorvery)	Found by IBM during Dev. Testing on 6/26/89 (Not Flown)	Created a target OPS set of a Split/Dual Phase Program Overlay (G1, G2, G3) with two or more GPCs. Create a failure on the alternate MMU Bus with at least one, but not all GPCs receive errors on the alternate bus while reading the first phase of the program overlay.	An oversight in the coding failed to terminate Mass Memory Switching logic once a a switch between buses had already occurred and also on Non-Universal Single Bus errors. --- Recommended the community to approved test plan included universal Dual Bus and Non-Univeral Sing Bus errors.	Patches were done to all STS flights that were using OI-8C and OI-8D software releases to correct the described problem. Source code was fixed for later STS flights so basically the problems were fixed before the software was flown.

Copyright James K. Orr 2015

Details On RELEASED PASS SEVERITY 1 DR's

DR #	Sev. Lvl	General Description	Detailed Error Description	How Error Was Corrected	When Err Introduced to FSW	Date Found and by Whom	Scenario(s) to Produce the Error	Reason that the Error was missed ---- Lesson Learned.	Why the SW error did not cause Real Life catastrophic event?
105199	1	Multiple Flt CNTL Modes Active in Ascent Abort	Both First Stage and Second Stage Flight Control Subphases were active at SRB SEP because there was a flag, which indicated that a new attitude Quaternion is ready for the DAP, was set for 160 ms at SRB ignition and at powered pitch down. The Ascent Dispatcher Table Update (DTU) used this flag to determine when to attach or detach the appropriace D/C steer module. If this flag is ON during a 160ms window immediately following SRB ignition then the connection between guidance and flight control will be effectively severed at SRB separation resulting in loss of control. This problem was introduced by CR89990E on OI21.	* Patches were done for flights STS 49, 50, 46 and source code was fixed for the rest of the flights to correct the effect that the same FSW variable was used for multiple requirement parameters. Instead created new parameter definition for different portion of requirement.	Introduced in OI-21.21 on 10/90.	Found by IBM Certification for STS-50 Engineering Cycle Certifi8catio n FEID testing on 10/31/91	* Perfrom a Contigency Abort on STS-49 recon-1 from T-5 min. to ET SEP +10 seconds with SSME's 1 and 2 failed at T+4 min via PUSH BUTTON.	Error was missed due to Timing scenario dependent --- Recommendations included emphasis on analyst not to use the same FSW variable multiple requirement parameters. Also increase efficiency on analysis tasks such as Requirements Evaluation, More Guideline in Development Process Document, Design/Code Inspection, and Level 6 and 7 Testings.	The error was caught and corrected in patches or code fixed before the software was ever flown on any real flight.
110419	1	GPS COMMfault Status Indicator Missing in FIOCBLKs	If multiple failures occur resulting in Both an I/O error on the FF2 GPS Read AND an inability to communicate information on that error across the GNC Redundant Set (40 msec max window for second failure - fail to sync situation), all PASS GNC GPCs may enter an infinite loop in FCOS I/O completion processing with interrupts disabled.	* STS-90 was flown with an I-Loads set that would cause the FSW to bypass the affected code in GPS I/O so it could never be invoked * Code was fixed for the remaining OI26B flights (STS-91, 88, 95) by adding a data entry for GPS into the I/O Problem Report Fail CommFaulted Table.	Error introduced by CR 91077B implemented on OI26B (2/13/96)	Found by PASS FSW developer during desk analysis on 8/1/97 (Dormant due to planned uninstall HW)	Requires 3 string GPS configuration plus an I/O error on GPS receiver on FF2, plus additional failures.	Design oversight because I/O Problem Report failure was not considered because the logic was very specialized and has not changed over 15 years. --- Recommendations were to audit I/O table and to identify process improvement and implemented them as appropriate.	Logic was associated with 3 string GPS configured vehicles. First exposure would have been in 2007. STS-90 flight used I-Loads for single string GPS to bypass the execution of GPS I/O code portion and was declared to be "Requirement Intent Met disposition for this flight only." Since the affected code was not being executed therefore no catastrophic event was happenned. The code was fixed for other flights.

Copyright James K. Orr 2015

References

1. Hamlin, Teri L., *Shuttle Risk Progression: Use of the Shuttle Probabilistic Risk Assessment (PRA) to Show Reliability Growth*, Jan 01, 2011, NASA JSC-CN-22748, JSC-CN-24359. Also AIAA 2011-7353, AIAA Space 2011; 26-29 Sep. 2011; Long Beach, CA; United States. Copy available for free at http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110004917.pdf
2. Christopher J. Hickey, Andrew L. Klausman, James B. Loveall, and James K. Orr, *The Legacy of Space Shuttle Flight Software*, August, 2011, NASA JSC-CN-24428, JSC-CN-24683. Also AIAA 2011-7307, AIAA Space 2011; 26-29 Sep. 2011; Long Beach, CA; United States. Copy available for free at http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110014946.pdf
3. *Reports and Articles, Communications of the ACM*, September 1984 Volume 27 Number 9.
4. Jim Asher, *Shuttle Problem Fixed Countdown Resumes*, *The Houston Post*, Thursday August 30, 1984. This was a page 1 article.
5. *Space Shuttle abort modes*, Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Space_Shuttle_abort_modes
6. James K. Orr, Daryl Peltier, *Space Shuttle Program Primary Avionics Software System (PASS) Success Legacy – Quality & Reliability Data*, August 24, 2010, NASA JSC-CN-21317, presented at NASA-Contractors Chief Engineers Council 3-day meeting August 24-26, 2010, in Montreal, Canada. Copy available for free at http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100029536.pdf
7. James K. Orr, Daryl Peltier, *Space Shuttle Program Primary Avionics Software System (PASS) Success Legacy - Major Accomplishments and Lessons Learned Detail Historical Timeline Analysis*, August 24, 2010, NASA JSC-CN-21350, presented at NASA-Contractors Chief Engineers Council 3-day meeting August 24-26, 2010, in Montreal, Canada. Copy available for free at http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100028293.pdf

Copyright James K. Orr 2015