# Space Shuttle Program
# Primary Avionics Software System (PASS)
# Success Legacy – Major Accomplishments and Lessons Learned
# Detail Historical Timeline Analysis

James K. Orr

August 24, 2010

United Space Alliance

# Agenda

- Introduction
- Dedication To Safety
- Space Shuttle Flight Software Period Themes
  - Initial PASS OFT Development Through STS-5 (1978 – 1982)
  - Pre-Challenger Accident Operations (1983 – 1985)
  - Post-Challenger, Return To Flight (1986 to 1988)
  - Process Optimization and Stability Under IBM (1989 to 1993)
  - Transition Period To Loral / Lockheed Martin (1994 to 1997)
  - Transition to United Space Alliance (1998 to 2002)
  - Post-Columbia Accident, Return To Flight (2003 to 2005)
  - Shuttle To End In 2010, OI Development Continuing (2006 – 2008)
  - Shuttle To End Delayed Slightly, Skill Maintenance (2009 – 2011)
- Summary
- Acronyms

# Introduction

- This presentation focuses on the Space Shuttle Primary Avionics Software System (PASS) and the people who developed and maintained this system.
  - One theme is to provide quantitative data on software quality and reliability over a 30 year period
    - Consistent data relates to “code break” discrepancies
      - Requirements were supplied from external sources
        - Requirement inspections and measurements not implemented until later, beginning in 1985
  - Second theme is to focus on the people and organization of PASS
    - Many individuals have supported the PASS project over the entire period while transitioning from company to company and contract to contract
    - Major events and transitions have impacted morale (both positively and negatively) across the life of the project

# Introduction

- Including Approach and Landing Tests, PASS project has run from 1974
  - Process development started at beginning of project
- Detailed metrics on PASS process, quality, and reliability is contained in a separate companion presentation
  - Space Shuttle Program Primary Avionics Software System (PASS) Success Legacy – Quality & Reliability Data
    - This companion presentation presents an "apples to apples" comparison of quality and reliability of PASS from STS-1 to present
- Page 6 shows the number of Product Discrepancy Reports (DRs) flown
  - Vast Majority of Product DRs introduced prior to STS-5
    - 424 PASS Product DRs flew on STS-5 mission
      - DRs unknown at the time of the flight, but discovered over the years since
  - Today there is a 60 % probability that a newly found PASS Product DR was introduced on STS-5 or earlier.

# Introduction

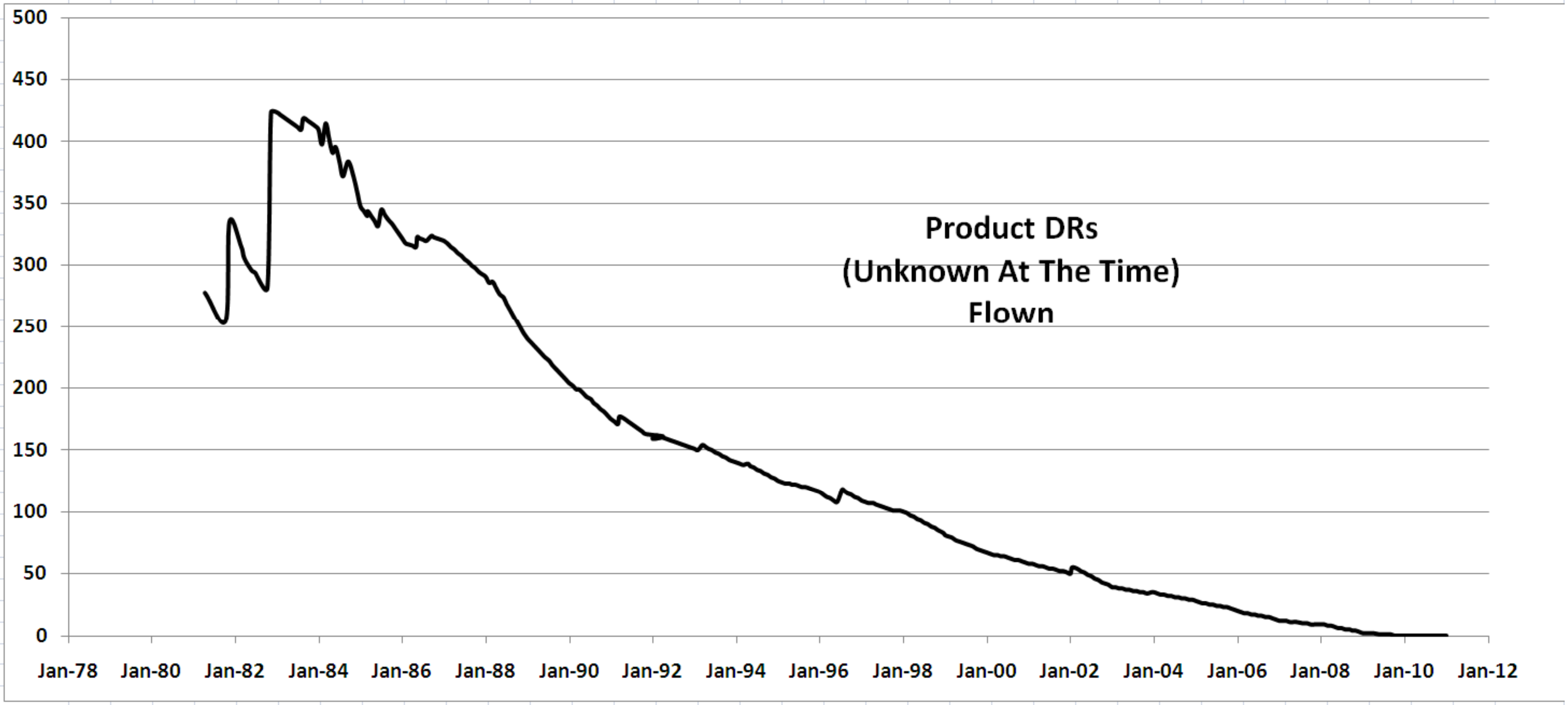
- Quality Measures
  - Errors counted in three periods
    - Errors found by Inspection and Development Test Pre-Build (prior to being placed under project configuration control)
    - Process DRs found Post Build until a milestone called Software Readiness Review (SRR) for the first flight off that increment; typically occurs approximately 4 weeks prior to flight
    - Product DRs found from SRR of first flight until end of program
      - Subset of Product DRs are those which occur in either terminal countdown or in flight, called in-flight DRs
    - Additional special category of DRs are called Released Severity 1 DRs.  These may be process or product DRs.  These are DRs that could cause loss of crew or vehicle that are released to any field site such as the Shuttle Mission Simulator (SMS), the vehicle at KSC, or the Shuttle Avionics Integration Lab (SAIL).

# Introduction

- Quality Measures
  - Pre-build Detection Effectiveness (Inspection Plus Development Test)
    - Errors found by Inspection and Development Test Pre-Build (prior to being placed under project configuration control) divided by total errors
  - Verification Effectiveness
    - Process DRs divided by (Process DRs plus Product DRs)
  - Product Error Rate
    - Product DRs divided by new, changed, deleted source lines of code. Includes only non-comment source lines of code.

# Number Of Latent Unknown Product DRs Flown

| 1978 1979 1980 1981 1982 | 1983 1984 1985 | 1986 1987 1988 | 1989 1990 1991 1992 1993 | 1994 1995 1996 1997 | 1998 1999 2000 2001 2002 | 2003 2004 2005 | 2006 2007 2008 | 2009 2010 2011 |
|---|---|---|---|---|---|---|---|---|
| Initial System Development Supports Incrementally STS-1, STS-2, and STS-5 With Major Capabilities | Pre-Challenger Operations With Incremental Development | Post-Challenger Revalidation Return-To-Flight | GPC Memory/Speed Upgrade CMM Level 5 Optimized Process Skill, Stable Workforce | Workforce Instability OI-25 PTI DR Escapes Process Change GPS Upgrade | Restore Workforce Stability Influx Of New Personnel | Cockpit Avionics Upgrade Post-Columbia Return-To-Flight | Shuttle Ending OI-32, OI-33, OI-34 | Shuttle Ending Skill Maintenance Reductions-In-Workforce |
| 1978 1979 1980 1981 1982 | 1983 1984 1985 | 1986 1987 1988 | 1989 1990 1991 1992 1993 | 1994 1995 1996 1997 | 1998 1999 2000 2001 2002 | 2003 2004 2005 | 2006 2007 2008 | 2009 2010 2011 |




**Product DRs that existed on a flown system, but were unknown at the time of the flight . Discovered up to 25 years later.**

# Introduction

- Common themes running through lifecycle periods
  - Improvements through process enhancements
  - Improvements through automation
  - Defect removal following identification of significant process escapes
  - Impact of workforce instability
  - Early evaluator, adopter, and adapter of state-of-the-art software engineering innovations
- A significant contributor to the success of the PASS FSW organization has been the support of the NASA software customers that have consistently valued quality and supported reasonable implementation schedules. NASA has also supported maintaining critical skill staffing.

# Dedication To Safety

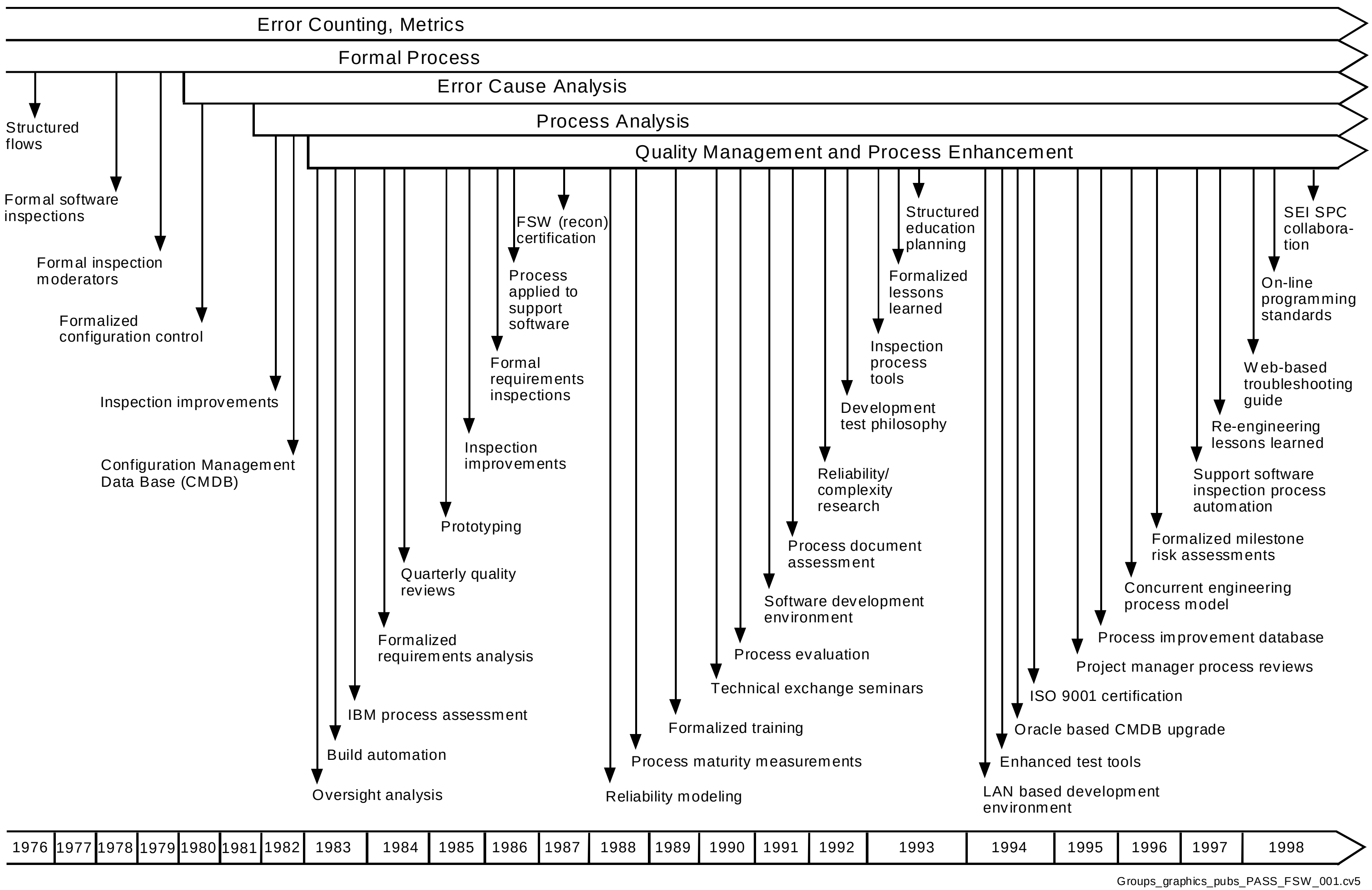
# Dedication To Safety

- Developing complex human-rated flight software is a major technical challenge.
  - Perfection required to achieve the desired level of safety
    - Extremely difficult to accomplish, but can be aggressively pursued
  - Keys to the pursuit of perfection
    - Principles of Providing High Reliability Software
    - Continuous Process Improvement
    - Defect Elimination Process

# Principles of Providing High Reliability Software

- **Safety certification is currently based on process adherence rather than product.**
- **Assumption is that a known, controlled, repeatable process will result in a product of known quality.**
- **Process executed by personnel that are *committed to safety and skilled* relative to processes, system architecture, and specialized software requirements.**
- **Team skills and workload closely monitored by management to prevent over commitment that could result in quality breakdowns.**
- **Use "trusted" tools to develop, build, release and maintain the software.**
- **Use measurements to continuously assess the health of both the process and the product.**
- **Relationship between quality and reliability must be established for each software version and statistically demonstrated for the required operational profiles.**
- **Quality must be *built into* the software, at a *known* level, rather than *adding* the quality after development.**
  - **You cannot *test* quality into software**

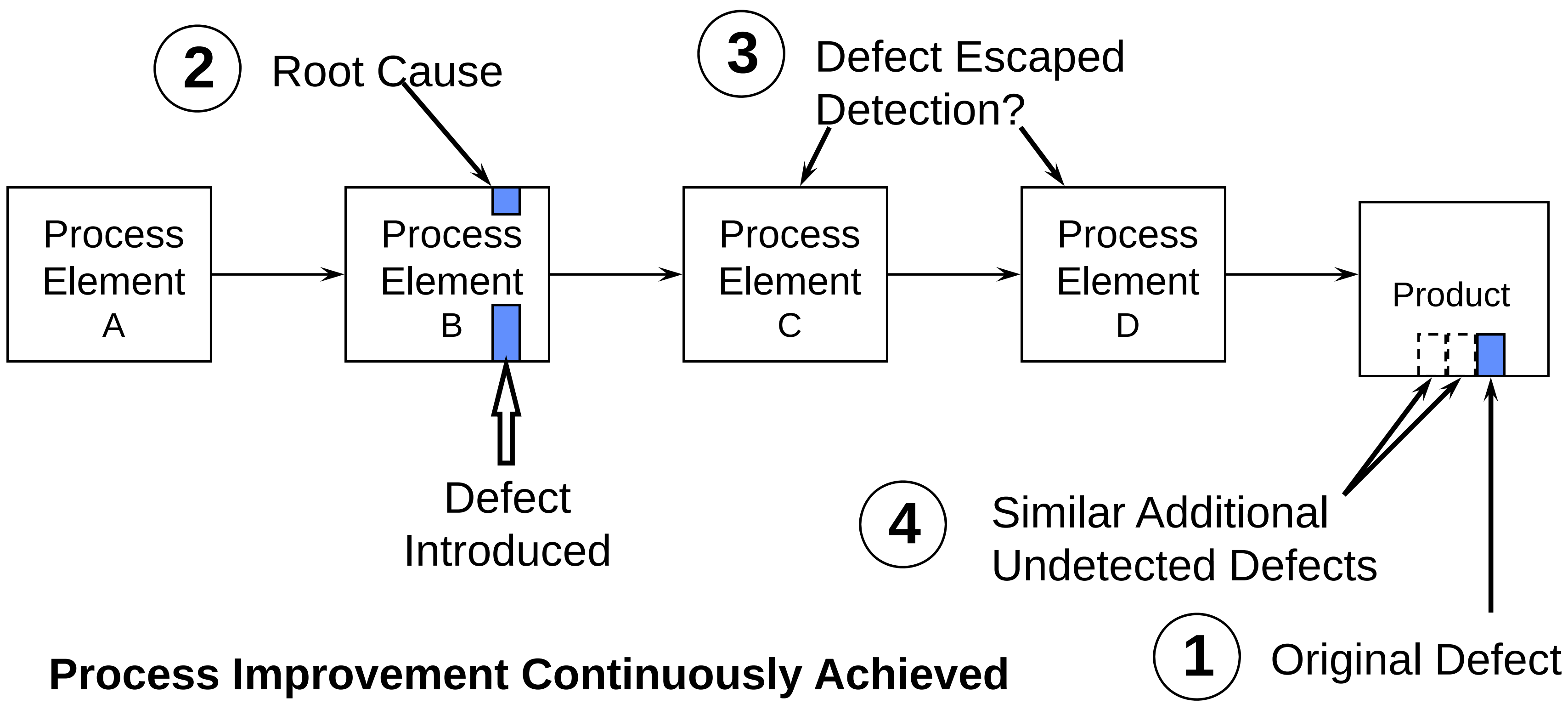
# Examples Of Continuous Process Improvement



# Defect Elimination Process

**Steps performed**

1. **Remove defect**
2. **Remove root cause of defect**
3. **Eliminate process escape deficiency**
4. **Search/analyze product for other, similar escapes**




**Process Improvement Continuously Achieved By Performing Feedback Steps 2 and 3**

# Space Shuttle Flight Software Period Themes

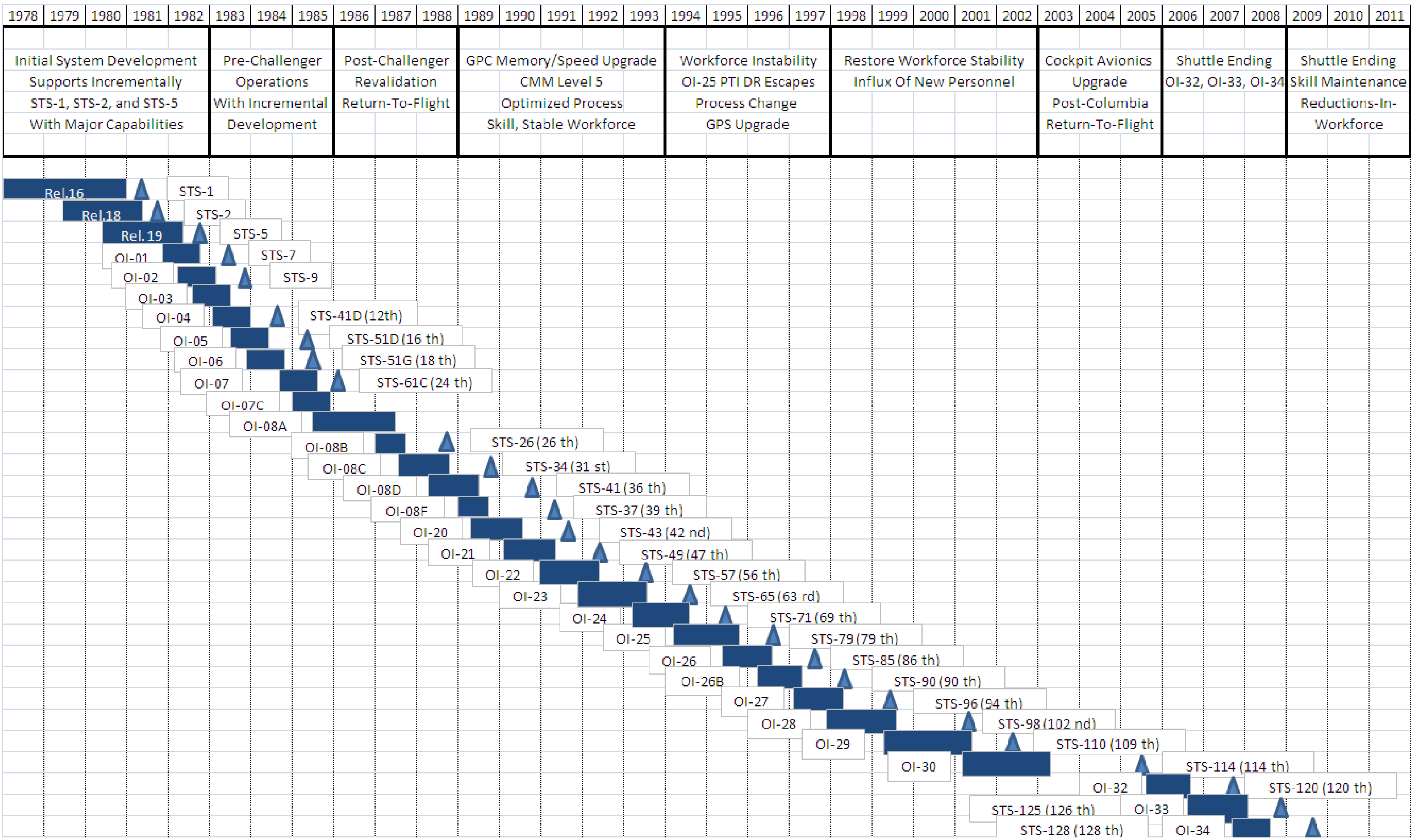
# Quantitative Anchors For Following Discussions

- The following pages shows the succession of releases that implemented major capabilities into the PASS FSW along with key quality / reliability measures.
  - Space Shuttle Flight Software Period Themes (page 15)
    - PASS FSW History divided into periods with consistent environments
  - PASS FSW Releases (page 16)
    - Note: No flights using releases OI-3, OI-7C, and OI-8A
  - Space Shuttle Flight Rate and Key Flights (page 17)
  - Number of Known PASS FSW Product DRs Flown (page 6)
    - Peak of 425 Product DRs (unknown at the time) flown on STS-5
    - No Product DRs discovered since 11/14/2008
  - Reliability of PASS FSW During Missions (page 18)
    - From MTBF of 7 Flight Days between in-flight DRs on STS-1
    - To MTBF of 294 Flight Days between in-flight DRs on STS-134

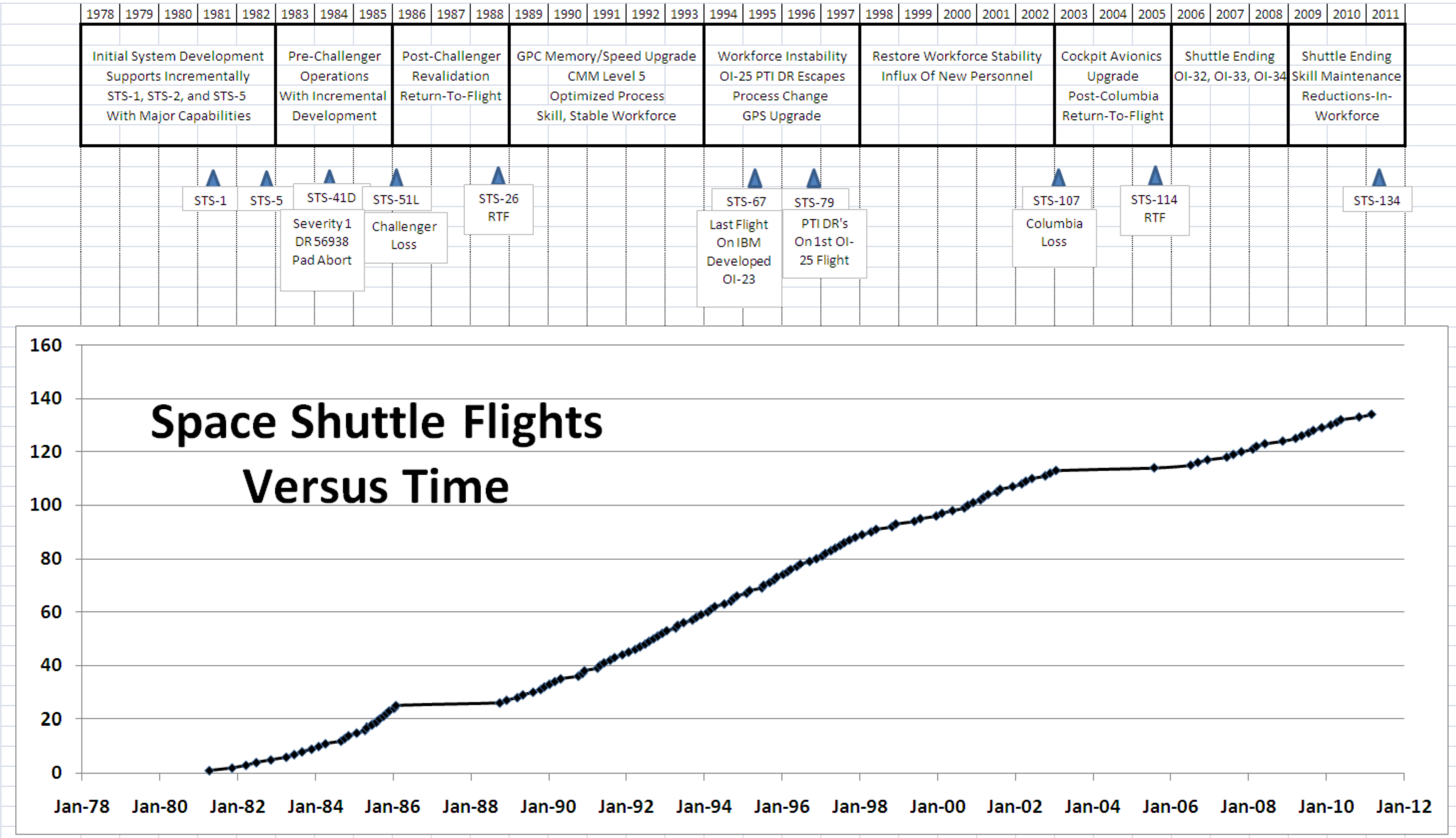
# Space Shuttle Flight Software Period Themes

| Years | Theme | Events |
|---|---|---|
| 1978-1982 | Initial System Development | Supports Incrementally / STS-1 to STS-5<br>Many Major Capabilities |
| 1983-1985 | Pre-Challenger Operations | Incremental Development / Reductions in Staff during 1985 |
| 1986-1988 | Post-Challenger, Return to Flight | Challenger Accident / PASS FSW Revalidation / Return to Flight |
| 1989-1993 | Process Optimization and Stability | CMM Level 5 / GPC Memory/Speed Upgrade<br>Skilled, Stable Workforce |
| 1994-1997 | Transition To Loral / Lockheed Martin | Workforce Instability / OI-25 PTI DR Escapes<br>Process Change / GPS Upgrade |
| 1998-2002 | Transition to United Space Alliance | Restore Workforce Stability / Influx Of New Personnel |
| 2003-2005 | Post-Columbia / Return-To-Flight | Cockpit Avionics Upgrade / Columbia Accident / Return to Flight |
| 2006-2008 | Shuttle Ending, OI Development | OI-32, OI-33, OI-34 / Display Upgrades evolved From CAU / CMMI Level 5 November 2006 |
| 2009-2011 | Shuttle Ending, Skills Maintenance | Skills Maintenance / Reductions-In-Workforce<br>CMMI Level 5 in September 2009 |

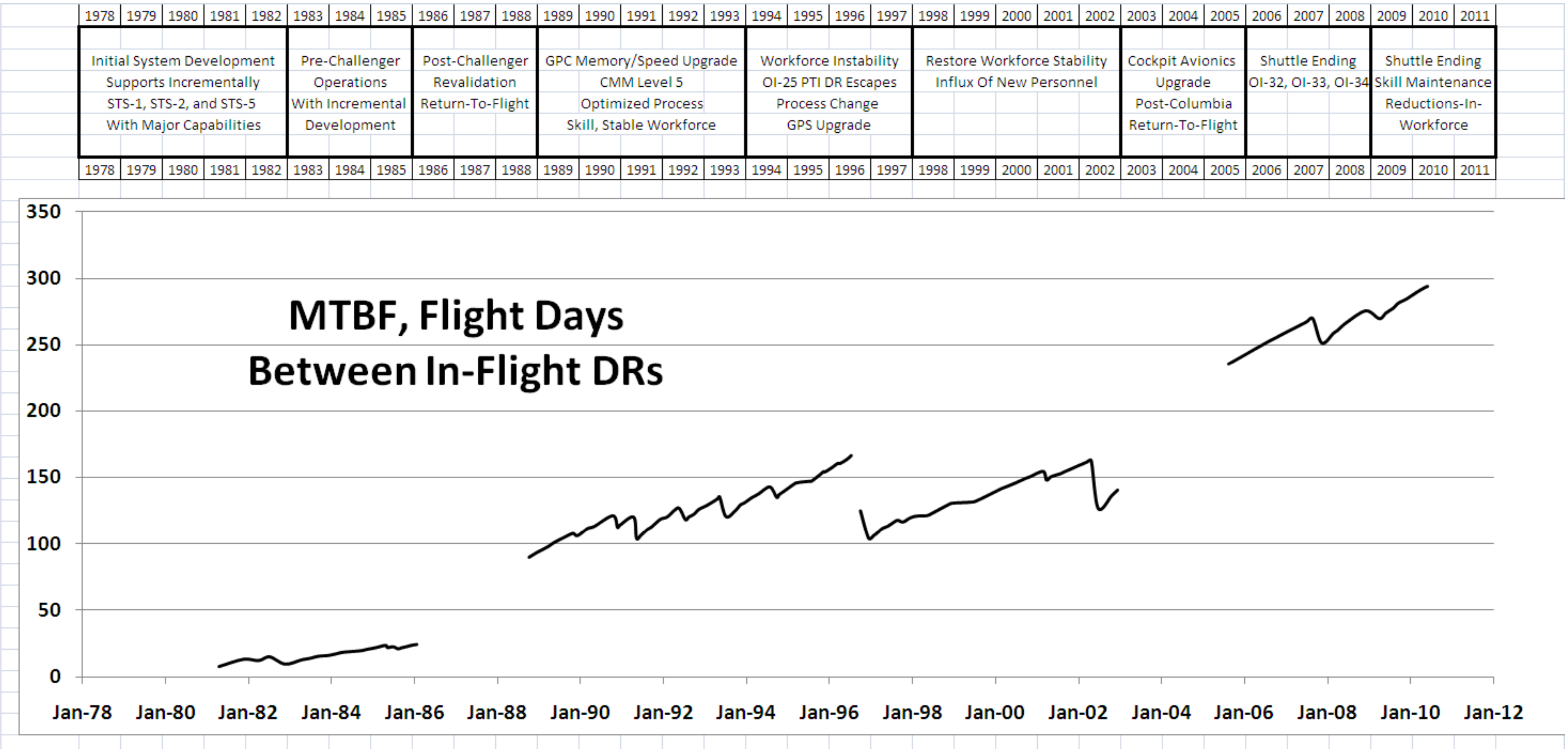
# PASS FSW Development History



# Key Space Shuttle Flight(s) ?



# MTBF, Flight Days Between In-Flight DRs






USA United Space Alliance

# Initial PASS OFT Development Through STS-5 (1978 – 1982)

# Characteristics Of Period (1978 – 1982)

- It is not possible to do this period justice given the significance of the accomplishment (developing software for STS-1 through STS-5) and the challenges faced and overcame.
- PASS history has been extensively documented in other reports and articles
    - Reference:
        - http://history.nasa.gov/computers/Ch4-5.html
            - Computers in Spaceflight: The NASA Experience, - Chapter Four - Computers in the Space Shuttle Avionics System - Developing software for the space shuttle
        - http://history.nasa.gov/computers/Source4.html
            - Sources for the above references

# Characteristics Of Period (1978 – 1982)

- Major technical challenges in terms of infrastructure, programming languages, and requirements definition.
- Major challenges in terms of memory and CPU speed limitations of AP-101B
- Design/Code inspection conducted by Development Organization including Developer, Requirements Analyst, and Peer Programmer.
  - No measurements on inspections available
- Rigorous testing program
  - 7 levels of testing prior to Configuration Inspection (CI)
  - Integrated Avionics Verification in SAIL after each release
- 24 Interim releases provided to field users prior to STS-1 over a 2 year period
- 2764 Process DRs found prior to Software Readiness Review (SRR) for STS-1

# Space Events (1978 – 1982)

- Voyagers 1 & 2 Flybys of Jupiter & Saturn
- Skylab Deorbited
- Interim Upper Stage (IUS) approved for Shuttle and later renamed to Inertial Upper Stage (IUS)
- First Space Shuttle Launch (STS-1)
- OFT-1 through OFT-4 Shuttle test flights
- Salyut-6 Space Station Deorbited
- Salyut-7 Space Station Launched
- First satellite deploys (STS-5)

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Transition from ALT work to OFT development<br>• Expansion of orbit FSW capability post STS-1<br>• First Flight Capabilities<br>• Schedule driven, heavy change request traffic<br>• Early Systems Management / Payload Management Software |

| Category | Observation / Characteristics |
|---|---|
| Quality | • Release 16 (STS-1) Product Error Rate = 0.8 DRs/KSLOC<br>• Release 18, 19 (STS-2, STS-5) Product Error Rate = 1.1 DRs/KSLOC<br>• Verification Effectiveness defined as Process DRs / (Process DRs plus Product DRs)<br>    • Release 16 (STS-1) at 91 % of DRs found by SRR<br>    • Release 19 (STS-5) at 77 % of DRs found by SRR<br>• Early reliance on testing |

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| Reliability | • Mean Time Between Failure (MTBF) values based on reliability modeling<br>• Three MTBF measures presented here.<br>- Calendar Days Between Any Product DR<br>• STS-1, 5.8 Calendar Days<br>• STS-5, 7.3 Calendar Days<br>- Flight Days Between Any In-flight DR<br>• STS-1, 7.3 Flight Days<br>• STS-5, 9.1 Flight Days<br>- Shuttle Flights Between Severity 1 PASS DR[1] (Estimated)<br>• STS-1, 327 Flights<br>• STS-5, 409 Flights |

**(1) Severity 1 DR is a DR that results in loss of crew and/or vehicle. Reference: Shuttle Flights Between Severity 1 PASS DR (Estimated) at risk level of 1 in approximately 1000 for STS-51L as a return-to-flight action for STS-26.**

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • 523 Product DRs remaining at SRR for these systems<br><br>• STS-5 flew with 424 Product DRs (unknown at the time)[1] present<br>    • In-flight DRs for STS-1 to STS-5:<br>        • 29 Total Flight Days<br>        • Two DRs during terminal countdown<br>        • One DR during flight<br><br>    • Released Severity 1 DRs<br>        • STS-1 flew with 4 Severity 1 DRs<br>            • One removed prior to STS-2<br>            • Scenarios typically involved multiple SSME failures and contingency aborts |

**(1) Product DRs that existed on a flown system, but were unknown at the time of the flight; discovered up to 25 years later.**

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • Valid models in software test environment are critical<br>    • Timing related hardware models need to include random variation similar to hardware characteristics<br>• Collect appropriate data during integrated hardware tests<br>• Multiple "apparently unrelated" changes can collectively produce unexpected erroneous consequences<br>• Manual processes require continuous management oversight to insure rigorous analysis<br>• All possible scenarios must be identified, accommodated via design, and tested.<br>    • Many scenarios-related problems have extremely small timing windows. Very unlikely to detect during testing only. Requires "Multi-Pass" analysis methods to insure identification.<br>    • Proper initialization under all scenarios required. |

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • Verification analyst participation in the pre-build inspection process significantly adds quality<br>  • Prior to mid part of Release 19 (STS-5), the Verification analysts did not participate in design/code inspections. However, they did participate in inspections of patches implemented on STS-1 due to the increased risk of patch implementation over source change.<br>  • Assessment of the quality of the STS-1 patches versus the STS-2 source changes for the same DR and CR implementation resulted in the observation that the STS-1 patches were of higher quality.<br>  • Following this conclusion, the pre-build design/code inspection process was modified to require participation of the Verification analyst. |

# SAMPLE PASS SEVERITY 1 DR CAUSAL MECHANISM

| Mechanism: | Description: | Application To Future |
|---|---|---|
| Multi-Pass Scenario | A Multi-Pass function is one which requires code segment(s) to be executed multiple times before a function is completed where code logic paths are a function of multiple input variables which may change while the function execution is in progress. | • One defense is to force the function to complete before the code accepts a change to the input variables<br>• If input variables are allowed to change, then the requirements may not allow for correct functioning if the scenario was not well analyzed.<br>• Insure Proper Design/Code Initialization for all input variable state transitions. |
| | **Example:**<br>• Command interconnect between Space Shuttle OMS fuel tanks and RCS jets during an abort to allow propellant dump to reduce weight.<br>• Additional failures occur, and the abort mode is changed.<br>• Command a "return to normal" interconnect (RCS jets supplied from RCS fuel tanks) prior to completion of prior interconnect. | **Example Problems:**<br>• Fuel system valves may be incorrectly configured such that no fuel can reach the RCS jets, resulting in loss of control due to lack of control authority.<br>• Coding construct (such as "Do-Case") may not be initialized properly. In PASS in the 1980's, this resulted in a "random" incorrect branch due to case number exceeding maximum case. |

# Initial Development (1978 – 1982)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Initial staffing in 1978 was a mix of new hires and experienced staff from Apollo<br>• Schedule pressure, significant overtime<br>• STS-1 launch was delayed several times due to technical challenges (TPS, MPS).<br>• By the time of STS-1, the staffing was very experienced<br>• Morale was very high.<br>    • Program was cutting edge technology<br>    • IBM was a premier company in computer programming industry |

# Shuttle/FSW Reconfiguration

- ALT
  - FSW definition of the Downlist and I-Load reconfigurable data and tables/code were coded by hand
- STS-1
  - Recon data now defined in Level C cards from Rockwell/Downey
  - FSW definition of the SM and I-Load reconfigurable data and tables/code were generated by the SM preprocessor with workarounds coded by hand
  - SM reconfigurable table layout somewhat simple and straight forward in some cases
  - Errors caused by inconsistent data and coding errors
  - Downlist generated by a preprocessor (not sure if it was STS-1 or shortly thereafter)
- STS-2 – STS-4
  - Progression of SM Preprocessor/I-Load tools to automate table generation/coding
  - Errors due to immaturity of tools/consistency checking
  - Work in progress to categorize I-Loads for reconfiguration

# Pre-Challenger Accident Operations (1983 – 1985)

# Characteristics Of Period (1983 – 1985)

- Major challenges in terms of adding functions and maintaining system in the face of memory and CPU speed limitations of AP-101B
  - Issue with CPU speed resulted in the introduction of Severity 1 DR 56938
  - SM/PL Software redesigned on STS-5 due to both memory and CPU issues adding payload support
- Pre-Build Design/Code inspection conducted by FSW Organization including Developer, Requirements Analyst, Verification Analyst, and Peer Programmer.
  - Measurements on inspections available, process effectiveness rapidly rising.
- In transition from manually generated vehicle and payload flight specific code to code generated by automated pre-processors from reconfiguration databases
  - However, several errors introduced due to manual final load reconfiguration changes
- Staffing Transition from development to operations
  - De-staffing by IBM in 1985 via placement on other projects

# Characteristics Of Period (1983 – 1985)

- **Transitioned from long development time for releases into frequent Operational Increments with delta time between Configuration Inspections (CI) on the order of four months. Net effect was reduced verification time per release**
- **Significant number of Product DR's introduced in this period which are discovered in flight**
- **Product DR's (newly introduced and latent from 1978 – 1982 period) affect mission objectives, three Product DRs patched during flight**
- **Additional Released Severity 1 DRs are discovered, creating concerns to (a) avoid future introduction and (b) find any remaining existing Severity 1 DRs**
- **Continued high demand for software CR changes with some risk of over-commitment.**
  - **Increasing late change traffic on OI's (Over 50 % of the OI-7C content baselined post FACI)**

# Space Events (1983 – 1985)

- First satellite retrieval (STS-41C)
- First Spacelab flight (STS-9)
- Centaur Upper Stage Funded for Shuttle Use
- First DOD flight (STS-51C)
- Challenger, Discovery and Atlantis Debuts
- 9 Shuttle flights in CY1985
- Salyut-7 is extensively repaired after full breakdown
- Enterprise Fit-Tests at Vandenberg
- Spacelab
- Main Engine Control redesign
- Payload manifesting flexibility
- Crew enhancements
- Enhanced ground checkout
- Western Test Range (Vandenberg)

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Rendezvous<br>• Full Redesigned SM/PL Capabilities<br>• RMS Deploy and Retrieval<br>• Centaur Development<br>• Spacelab<br>• Main Engine Control redesign<br>• Payload manifesting flexibility<br>• Crew enhancements<br>• Enhanced ground checkout<br>• Western Test Range (Vandenberg)<br>• Reconfiguration tool planning / development<br>• Tools and procedures planning / development for DOD flights |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| Quality | • Product Error Rate spikes to 2.8 DRs/KSLOC on OI-1 (STS-7)<br>• Product Error Rate declines to 1.1 DRs/KSLOC by OI-7 (STS-61C) similar to Release 19 (STS-5)<br>• Verification Effectiveness in the range of 70 % to 80 % DRs found by SRR<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) increasing from 40 % to 65 %<br>    • Percent of error present in the inspection materials found by the inspection |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| Reliability | • Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 9.9 Calendar Days to 19.2 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 12.3 Flight Days to 23.9 Flight Days<br><br>•Shuttle Flights Between Severity 1 PASS DR (Estimated)<br>• From 552 Flights to 1072 Flights |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
| --- | --- |
| Product DRs | • Additional 109 Product DRs introduced on OI-1 to OI-7<br>• Product DRs (unknown at the time) flown down to 322 remaining at end of 1985 (24 % improvement over STS-5)<br>• In-flight DRs for STS-6 to STS-51L<br>  • 147 Total Flight Days<br>  • 8 DRs during flight (3 patched in-flight)<br>• Released Severity 1 DRs<br>  • STS-6 to STS-51L flew with 6 Severity 1 DRs<br>  • STS-41D aborted at T-6 seconds when GPC detected anomaly in orbiter's number three main engine.<br>    • Otherwise, would have flown with a 1 in 6 chance of DR 56938, Data Homogeneity Issue, causing loss of crew and vehicle |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • Manual processes require continuous management oversight to insure rigorous analysis<br>• All possible scenarios must be identified, accommodated via design, and tested.<br>    • Many scenarios related problems have extremely small timing windows.  Very unlikely to detect during testing only.  Requires "Multi-Pass" analysis methods to insure identification.<br>    • Proper initialization under all scenarios required.<br>• Valid models in software test environment are critical<br>    • Timing related hardware models need to include random variation similar to hardware characteristics<br>• Collect appropriate data during integrated hardware tests<br>• Multiple "apparently unrelated" software changes can collectively produce unexpected erroneous consequences |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • All possible scenarios must be identified, accommodated via design, and tested.<br>  • Failed hardware handling must be included in requirements<br>  • Scenario analysis must include maximum ranges for parameters and variable precision must match<br>• Software Interface Control Document requirements must be verified in an end-to-end manner<br>  • Two in-flight DRs due to failure to verify PASS SM to Spacelab ICD.  Both required in-flight patches when effect on experiments was observed. |

# Pre-Challenger Accident (1983 – 1985)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • The staffing was very experienced<br>• One occasion when a task deemed "very easy", a Co-op was assigned to source ILOAD values. Co-op failed to realize units conversion was required. Released Severity 1 DR resulted (DR 50788) but found in first run in SAIL.<br>• Morale was very high.<br>    • Flying Space Shuttle was exciting<br>    • IBM was de-staffing the Space Shuttle project, but providing employment opportunities to all affected employees to projects either in Houston or other IBM facilities.<br>    • Challenge to find and remove latent defects introduced earlier<br>    • Challenge to correct processes to avoid the introduction of additional Severity 1 DRs |

# Shuttle/FSW Reconfiguration

- STS-5 – STS-51L
  - SM/PL tables redesigned to support payloads and to conserve space in order for there to be room in the GPC to fit the payload support
  - Some of the SM/PL table layout now more complex and difficult to patch
  - SM/PL Preprocessor was also redesigned for the new tables
  - Auto I-Load processor
  - Errors due to immaturity of tools and coding errors for late changes that didn't go through preprocessor

Note (from 1986 NASA Excellence Award):

- Elapsed time (and man hours) to reconfigure FSW was reduced to half (11 weeks to 5 weeks) by 1985

# Post-Challenger, Return To Flight (1986 to 1988)

# Characteristics Of Period (1986 – 1988)

- Space Shuttle Challenger was lost with its crew on 01/28/1986.
- The next flight, STS-26, was 09/28/1988
- This time period focuses on the actions taken to achieve the return-to-flight on STS-26.
  - Rigorous review of software requirements; numerous safety changes were identified and implemented on OI-8A and OI-8B
  - Action assigned to compute the probability of the loss of a shuttle and crew due to a PASS FSW error
    - PASS reliability calculations ignore the potential for the Backup Flight System (BFS) to safely engage
  - While executing tasks to safely return the shuttle to flight, eight PASS Severity 1 DRs were discovered during this period in addition to two found in 1985.

# Characteristics Of Period (1986 – 1988)

- This was a very, very busy period, especially in 1988
  - Completing special studies under the label "Revalidation"
  - Preparing for STS-26 flight including expanded Flight Readiness Review (FRR) Process
  - Completing verification of OI-8C and development of OI-8D
  - Preparing to resume transition to the AP-101S upgraded computer
    - Transition to the AP-101S upgrade flight computer started prior to the Challenger accident (AP-101S required operating system changes)
      - Development work was abandoned (OI-9, OI-10, OI-11)
      - Return-to-flight DRs were implemented on AP-101B systems (OI-8A, OI-8B, OI-8C, and OI-8D)
      - AP-101S system software changes only were implemented on OI-8F (started at the end of this period)

# Characteristics Of Period (1986 – 1988)

- Infrastructure upgrades
  - Significant changes to the ability to execute test in the Software Development Lab (SDF) / Software Production Lab (SPF)
    - At the start of this period, there was one Flight Electronics Interface Device (FEID) that could run multi-computer runs by itself, and three FEIDs that could run single computer runs or be combined to run multi-computer runs
    - At the end of this period, there were six FEIDs that could each run multi-computer runs
      - Capacity to run test cases in the SDF and SPF increased by at least a factor of 3
        - This is a significant contributor to a reduction in in-flight DRs compared to product DRs found on the ground in later periods

# Space Events (1986 to 1988)

- Voyager 2 Flyby of Uranus
- Challenger Accident (STS-51L)
- Mir Launched
- Shuttle / Centaur canceled
- Shuttle Vandenberg Launch Site canceled
- Shuttle Return to Flight (STS-26)
- Only Buran Flight (Two Orbits)

# Post Challenger Accident (1986 – 1988)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Post-51L Safety Changes<br>• Bailout Capability<br>• Abort Enhancements |

| Category | Observation / Characteristics |
|---|---|
| Quality | • Product Error Rate declines 0.7 DRs/KSLOC on OI-8B (STS-26)<br>• Product Error Rate continues to decline to 0.2 DRs/KSLOC on OI-8C (STS-34)<br>• Verification Effectiveness in the range of 60 % to 70 % DRs found by SRR (very few changes in highly critical areas)<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) increasing to near 80 % |

# Post Challenger Accident (1986 – 1988)

| Category | Observation / Characteristics |
|---|---|
| Reliability | • There were no flights in this period. Data address comparison from STS-51L in early 1986 to STS-26 in late 1988<br>• Three Mean Time Between Failure (MTBF) measures presented here.<br>- Calendar Days Between Any Product DR<br>• From 19.2 Calendar Days to 28.6 Calendar Days<br>- Flight Days Between Any In-flight DR<br>• From 23.9 Flight Days to 89.6 Flight Days<br>- Shuttle Flights Between Severity 1 PASS DR<br>• From 1072 Flights to 1599 Flights |

# Post Challenger Accident (1986 – 1988)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • Additional 16 Product DRs introduced on OI-7C/8A/8B/8C<br>  • OI-7C/8A product DRs normally shown as from CI<br>  • This data counts from STS-26 SRR (1st off OI-8B)<br><br>• Product DRs (unknown at the time) flown down to 240 remaining at end of 1988<br>  • 43 % improvement over STS-5<br>  • 24 % improvement over prior time period<br><br>• Released Severity 1 DRs<br>  • 8 Severity 1 DRs identified and removed in this period<br>  • No known Severity 1 DRs flown on STS-26 or any later flight |

# Post Challenger Accident (1986 – 1988)

| Category | Observation / Characteristics |
| --- | --- |
| Lessons Re-learned | • Changes can have unintended consequences. Delta Test approach may miss. Inspections best opportunity to detect.<br>• All possible scenarios must be identified, accommodated via design, and tested.<br>    • Proper initialization under all scenarios required.<br>    • Failed hardware handling must be included in requirements |

| Category | Observation / Characteristics |
| --- | --- |
| New Lessons Learned | • Implement more vigorous scenario testing<br>• Need to audit requirements to code mapping<br>• Failed hardware handling must be included in requirements |

# Post Challenger Accident (1986 – 1988)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • De-staffing from early development levels completed in late 1985 just prior to Challenger accident<br>• Slight re-staffing occurred starting in mid 1986<br>• Improving morale with the low point the accident and the high point as of the STS-26 flight<br>• Staff very focused on flight software due to safety enhancements on STS-26 and other Revalidation tasks to improve flight safety<br>• Staff energized at the future opportunity to add functionality once development of OI-20 begins in1989 to take advantage of the increase memory and speed of the AP-101S GPC<br>    • Large backlog of new capabilities waiting to be implemented |

# Shuttle/FSW Reconfiguration

- **STS-26**
  - **STAR/MAST System development began around 1983, implemented/released post STS-51L (1986), and used in line to STS-26**
  - **Recon data now defined by inputs to the STAR/MAST systems**
  - **STAR generates Level C for SM/PL and I-Loads**
  - **MAST generates TFL/DFL/FPL**
  - **Ensures consistency across not only FSW but also ground facilities**
  - **Better consistency checking for all users**
  - **Any issues have better chance of identification earlier**
  - **STAR/MAST tools targeted to a "mature" vehicle fleet but an enormous number of modifications to the fleet resulted from the Challenger accident which in turn affected the tools' audits.**
  - **Reduced staffing, resulting from the "improved" toolset, handicapped ability to provide timely software release updates.**
    - **Resulted in numerous reworks early (STS-26 through STS-29)**
    - **Offline tools were developed to augment the STAR/MAST tools (many of which are still in production today).**

# Process Optimization and Stability Under IBM (1989 to 1993)

# Characteristics Of Period (1989 – 1993)

- This period is bounded by the STS-26 return-to-flight launch on 09/28/1988 at the beginning and ending with the sale of IBM Federal Systems Division to Loral Corp. effective January 1, 1994
  - Also at the end of this period, the IBM Federal Systems Division Houston contract on Space Station Freedom software was terminated.
- Quality of new development is maintained over this entire period at record low levels approaching 0.1 DR/KSLOC Product Error Rate.
- Available AP-101S memory and CPU speed result in major capability additions.
- Achievements in quality recognized in 1989 when NASA uses the PASS project for a "practice" CMM assessment
  - Concludes organization assessed at CMM Level 5 (Highest possible, first ever)
  - Starts an on-going collaboration with the Software Engineering Institute

# 1989 CMM Level 5 Assessment

During the week of November 13, 1989, a team of Software Capability Evaluators visited the National Space Transportation System (Space Shuttle) Onboard Flight Software Project at IBM-Houston. The team was part of a larger Safety, Reliability, Maintainability, and Quality Assurance (SRM&QA) Site Survey Team visiting Johnson Space Center (JSC) from NASA Headquarters. The Software Capability Evaluation Team consisted of the following software professionals:

Donald Sova, Team Leader
NASA Headquarters

Alice Robinson
NASA Headquarters

Larry Hyatt
Goddard Space Flight Center

Paul Hurst
Marshall Space Flight Center

Marilyn Bush
Jet Propulsion Laboratory

Richard Fairley
George Mason University

Al Pietrasanta
Consultant

# 1989 CMM Level 5 Assessment

Based on our examination of the IBM National Space Transportation System Flight Software Project, the NASA Headquarters SRM&QA Survey Team has determined that the Flight Software Project is at Level 5 (highest level) of the Software Engineering Institute Contractor Evaluation scale. Project strengths in the areas of formal inspections, error feedback and process improvement, configuration management, and subcontractor management are to be commended. Areas that should be examined for possible improvements include inspections, quality assurance and testing, and entry level training.

# Characteristics Of Period (1989 – 1993)

- Workforce stable, includes flight software development subcontract with Loral Corp.
  - Code produced by subcontractor is entered into pre-build Inspection Process the same as code developed by IBM employees
  - Effective with OI-23 (1993), Loral conducts internal peer reviews on code prior to submission to IBM pre-build Inspections
- Processes matured & better documented with ISO9000, regular process team meetings & formalized process change teams
- IBM negotiated a five year sole source extension of the contract to support PASS FSW development and maintenance starting in July, 1993. Contract included provisions for gradually reducing the staffing level over the five years.
- Increasing flight rate with more complex missions
- First flight of upgraded AP-101S Computers

# Space Events (1989 to 1993)

- Voyager 2 Flyby of Neptune
- Magellan Launched to Venus (STS-30)
- Galileo and Ulysses Launched to Jupiter (STS-34 & STS-41)
- Hubble Space Telescope Launched (STS-31)
- Gamma Ray Observatory Launched (STS-37)
- Endeavour First Flight (STS-49)
- First Hubble Repair Mission (STS-61)
- Last Dedicated Shuttle DOD Flight (STS-53)

# CMM Lvl 5 Process Under IBM (1989 to 1993)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • GPC Upgrade<br>• Extended Landing Site Table<br>• OPS 3 (TAL Code) in upper memory<br>• Redesigned Abort sequencer<br>• 2 Engine Out Auto Contingency Aborts<br>• OV-105 Hardware changes<br>• On-Orbit Changes<br>• MIR Docking<br>• On-Orbit DAP Changes |
| **Category** | **Observation / Characteristics** |
| Quality | • Product Error Rate steady in range of 0.1 to 0.2 DRs/KSLOC<br>• Verification Effectiveness steady in the range of 80 % to 90 % DRs found by SRR<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) steady in the range of 80 % to 90 %. |

# CMM Lvl 5 Process Under IBM (1989 to 1993)

| Category | Observation / Characteristics |
| --- | --- |
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 28.6 Calendar Days to 41.7 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 89.6 Flight Days to 130.8 Flight Days<br><br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 1599 Flights to 2335 Flights |

# CMM Lvl 5 Process Under IBM (1989 to 1993)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • Additional 22 Product DRs introduced on OI- 8F through OI-24<br>• Product DRs (unknown at the time) flown down to 140 remaining at end of 1993<br>  • 67 % improvement over STS-5<br>  • 42 % improvement over prior time period<br>• In-flight DRs for STS-26 to STS-61<br>  • 291 Total Flight Days<br>  • 1 DR during flight (introduced prior to STS-1)<br>• Released Severity 1 DRs<br>  • 1 newly introduced released Severity 1 DR<br>    • Found by IBM Flight Specific testing, no flight exposure<br>  • No known Severity 1 DRs flown during this period |

# CMM Lvl 5 Process Under IBM (1989 to 1993)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • All possible scenarios must be identified, accommodated via design, and tested.<br>  • Proper initialization under all scenarios required.<br>  • Avoid using the same FSW variable for multiple requirements variables |

# CMM Lvl 5 Process Under IBM (1989 to 1993) (cont'd)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • Latent problems can remain in the FSW multiple years until scenario and hardware re-action timing align<br>• Sequential inspections (e.g., development peer review followed by pre-build inspection) are equally effective in removing the same % of errors that exist at the start of the inspection.<br>    • A single inspection removes about 55 % of errors<br>    • Two sequential inspection each remove about 55 % of errors remaining at the start of the inspection.<br>    • Collectively, they remove 80 % of the errors present at the first inspection. |

# CMM Lvl 5 Process Under IBM (1989 to 1993)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Morale very high;<br>• Staff very focused on flight software quality due to experiences during return-to-flight (1986 – 1988)<br>• With the AP-101S GPC upgrade, major new development during this period with large capabilities being implemented<br>• Organization recognized nationally and internationally for processes due to CMM Level 5 appraisal<br>• New contract work on the Space Station Freedom software (although the work would be terminated in late 1993) |

# Transition Period To Loral / Lockheed Martin (1994 to 1997)

# Characteristics Of Period (1994 – 1997)

- This period covers the time from transition from IBM to the time the project transitioned to United Space Alliance
  - IBM Federal Systems Division sold to Loral Corporation as of January 1, 1994
  - On April 22, 1996, Lockheed Martin completed the acquisition of Loral Corporation's defense electronics and system integration businesses including the former IBM Federal Systems Division.
  - USA and NASA signed the Space Flight Operations Contract in September 1996 to become the single prime contractor for the Space Shuttle program.
  - NASA intent was to transfer the PASS FSW contract work to USA at the completion of the five year contract signed in 1993.
    - PASS FSW Contract work transition to USA on July 4, 1998.

# Characteristics Of Period (1994 – 1997)

- Late 1993 was not a good period for IBM Federal Systems in Houston
  - Re-planning / transitioning from Space Station Freedom program to the International Space Station program
    - IBM's contract work on Space Station software would end in 1993
  - IBM commercial divisions were struggling with revenues and profits as the mainframe era came to an end and the PC/server era evolved.
    - To raise cash, IBM made a strategic decision to sell its space and defense businesses
  - IBM Houston personnel were scattered
    - Remaining Space Shuttle work sold to Loral Corporation
    - Many IBM Houston personnel either elected early retirement packages, transfer to other IBM projects and divisions, or voluntarily left for more promising job prospects outside of IBM.

# Characteristics Of Period (1994 – 1997)

- Leadership immediately following the transition to Loral was a morale plus
  - Our initial Loral executive manager was Mike Coats
  - Tom Peterson, as PASS program manager, provided significant stability
- However, it still was a traumatic period as 1993 ended
  - Space Shuttle PASS project lost virtually all personnel with less than four years experience
  - Other experienced personnel left the project
  - One interesting exercise was merging the IBM and former Ford Aerospace subcontractor personnel into one new Loral organization.
- Morale within PASS FSW project began to deteriorate after the loss of Mike Coats in 1996 when Mike Coats become Vice President of Civil Space Programs for Lockheed Martin Missiles and Space in Sunnyvale, California.

# Characteristics Of Period (1994 – 1997)

- **Corporate level process improvement activities affecting the PASS Space Shuttle project became less focused after the Houston organization was re-organized separate from other parts of the former IBM Federal Systems Division.**
- **As contract end approached, and transition to United Space Alliance approached in July, 2008, there was conflict based on the perception of attempts to prevent transition of the Space Shuttle PASS FSW contract to USA in accordance with NASA plans.**
- **Some personnel were extremely distracted throughout this period.**
- **Management attempted various motivational approaches to retain employees.**

# Space Events (1994 to 1997)

- 7 Shuttle Flights in each year from CY1994 to CY1996
- 8 Shuttle Flight in CY1997
- Longest Duration Human Spaceflight Completed (438 Days)
- Shuttle / Mir Crew Exchanges Begin (STS-71)
- Upgrades to Hubble Space Telescope (STS-82)
- Launch of Cassini Mission to Saturn

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Mir Docking Adapter<br>• On-Orbit DAP Changes<br>• 3 Engine Out Auto Contingency Aborts<br>• Ascent Performance Enhancements<br>• Single-String GPS |

| Category | Observation / Characteristics |
|---|---|
| Quality | • Process escape on OI-25, Product Error Rate jump to 0.8 DRs/KSLOC, otherwise Product Error Rate steady in range of 0.1 to 0.2 DRs/KSLOC<br>• Verification Effectiveness steady in the range of 60 % for OI-25, otherwise 85 % to 100 % DRs found by SRR<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) steady in the range of 75 % to 85 %. |

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 41.7 Calendar Days to 54.0 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 130.8 Flight Days to 119.3 Flight Days<br>• Decrease due to In-flight DRs introduced on OI-25 during this period<br><br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 2335 Flights to 3161 Flights |

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • Additional 12 Product DRs introduced on OI- 25 through OI-27<br>• Product DRs (unknown at the time) flown down to 100 remaining at end of 1997<br>  • 76 % improvement over STS-5<br>  • 29 % improvement over prior time period<br>• In-flight DRs for STS-60 to STS-87<br>  • 365 Total Flight Days<br>  • 4 DRs during flight (2 introduced prior to STS-1, 2 introduced on OI-25)<br>• Released Severity 1 DRs<br>  • 1 newly introduced released Severity 1 DR<br>    • Found by FSW Development, no flight exposure<br>  • No known Severity 1 DRs flown during this period |

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • It requires a 100 percent team effort, from executive management to every analyst, to achieve the quality levels that the PASS Space Shuttle project expects of itself.<br>  • Without proper checks, a very few individuals can cause problems to escape that put the crew's life at risk<br>  • Escapes also show up dramatically in quality measurements (such as what happened on OI-25 with Product Error Rate).<br>• All possible scenarios must be identified, accommodated via design, and tested.<br>  • Proper initialization under all scenarios required. |

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • Essential to formalize management and lead analysts responsibility for assessing skills proficiency and work performance history for every individual on every team and evaluate risk based on skills mix with closed loop responsibility to program manager.<br>• Essential to put measurements in place and provide for proactive searches for "in process" symptoms (major actions with low team detection distribution; training pedigree; individual detection effectiveness; effects of multiple inspections).<br>• Essential to have a method for confidentially reporting suspected deficiencies and process to respond to reports. |

# Re-Inspection Criteria For D/C Inspections

- **PASS FSW D/C Re-Inspection Criteria (Maintenance Environment)**
  - The moderator will make a re-inspection decision for each module inspected without considering other modules in the package.
  - For Design Inspections, re-inspection of a module is required if three or more major errors are found in the design. If fewer than three major design errors are found, it is up to the moderator to decide if the module should be re-inspected.
  - For Code Inspections, re-inspection of a module is required if 10% or more non-comment lines have to be reworked, provided there are at least five lines to be reworked. If less than 10% non-comment lines have to be reworked, it is up to the moderator to decide if the module will be re-inspected.
  - A re-inspection is also required if a comparison between inspected and final pool elements (or one of the other comparisons defined in Section 5.3.4, "Pool Elements") cannot be generated.
  - For Design or Code Inspections, re-inspect if 50% or more of the major actions were found by one inspector only OR only one major action was found and only one inspector found it.

# Loral / Lockheed Martin (1994 to 1997)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Morale was shattered repeatedly in this period.<br>• Repeated staffing loses at each transition<br>• IBM to Loral<br>• Loral to Lockheed Martin<br>• Lockheed Martin to USA in July 1998<br>• Organization was caught up in the massive consolidation in the defense industry during this period<br>• Internal to the PASS FSW Project, the OI-25 PTI DR's served as a call to action to renew our commitment to quality and safety.<br>• There is a uniformly accepted belief in the PASS project that the severity of a code error is independent of the particular error<br>• The same type of error in one situation can have very benign effects and yet in another case result in loss of crew/vehicle<br>• Consequences of the OI-25 PTI DRs could have been much worst. |

# Transition to United Space Alliance (1998 to 2002)

# Characteristics Of Period (1998 - 2002)

- **This period focuses from transition of contract work to United Space Alliance on July 4, 1998 until the second shuttle accident involving loss of crew and vehicle (STS-107) on February 1, 2003**
- **Early 1998 was difficult as the time to transition to USA approached.**
  - **NASA and United Space Alliance did everything in their power to make the transition smooth and as seamless as possible to employees.**
- **Once the contract transition was completed, and employees were part of USA, there was a vast improvement in morale. Employees were well treated by USA.**
  - **For some employees, there were significant advantages in that service under United Space Alliance was favorably treated under the Loral (including IBM earned service) and Lockheed retirement plans. Possible to start retirement payments earned under IBM/Loral/Lockheed Martin while continuing to work for USA.**

# Characteristics Of Period (1998 - 2002)

- NASA was focused on extending the life of the Space Shuttles to 2020
  - Several major upgrades were in the process of being implemented including the Cockpit Avionics Upgrade
  - In 2002, PASS FSW development resources began work on OI-41 which was to support the PASS changes necessary for Cockpit Avionics Upgrade
    - Additional hiring for Cockpit Avionics Upgrade

# Space Events (1998 – 2002)

- Final Shuttle / Mir Mission (STS-91)
- Final Spacelab Mission (STS-90)
- Beginning of ISS Construction (STS-88)
- Mir Deorbited
- ISS Crew Increments Begin
- ISS U.S. Laboratory Destiny Added (STS-98)
- Chandra X-Ray Observatory Launch (STS-93)
- First MEDS flight (STS-101)
- First ISS Truss Element – S0 Added (STS-110)

# United Space Alliance (1998 to 2002)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • 3-String GPS<br>• East Coast Abort Landing (ECAL) Automation<br>• Automatic Reboost<br>• GPC Payload Command Filter (GPCF)<br>• Increased data to MEDS<br>• Start of Cockpit Avionics Upgrade (CAU) builds |

| Category | Observation / Characteristics |
|---|---|
| Quality | • Product Error Rate steady in range of 0.1 to 0.2 DRs/KSLOC<br>• Verification Effectiveness steady in the range of 85 % to 95 % DRs found by SRR<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) steady in the range of 85 % to 90 %. |

# United Space Alliance (1998 to 2002)

| Category | Observation / Characteristics |
|---|---|
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 54.0 Calendar Days to 60.7 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 119.3 Flight Days to 140.4 Flight Days<br><br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 3161 Flights to 3491 Flights |

# United Space Alliance (1998 to 2002)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • Additional 8 Product DRs introduced on OI- 28 through OI-30<br>• Product DRs (unknown at the time) flown down to 39 remaining at end of 2002<br>  • 92 % improvement over STS-5<br>  • 61 % improvement over prior time period<br>• In-flight DRs for STS-89 to STS-107<br>  • 675 Total Flight Days<br>  • 2 DRs during flight (1 introduced prior to STS-1, 1 introduced on OI-28)<br>• Released Severity 1 DRs<br>  • No newly introduced released Severity 1 DRs<br>  • No known Severity 1 DRs flown during this period |

# United Space Alliance (1998 to 2002)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • All possible scenarios must be identified, accommodated via design, and tested.<br>  • Failed hardware handling must be included in requirements<br>  • Scenario analysis must include maximum ranges for parameters and variable precision must match<br>• Conservative planning for new capabilities is important. Even if the capability is "really cool".<br>  • Recurrence of over committing relative to the skill capability of the team. Strong desire to see the capability implemented was a significant contributor (e.g., "really cool").<br>  • Detected early and corrective actions put in place<br>• Separation of duties can enhance overall quality.<br>  • Requirements/development, development/project management, etc.<br>• USA / SEI Collaboration used multiple inspector data to assess the effectiveness of our re-inspection criteria compared to elaborate statistical methods. |

# United Space Alliance (1998 to 2002)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Significantly better.<br>• People no longer concerned with whether they would be at the same company next year.<br>•Excellent Senior Management<br>• Many senior managers were former astronauts or former flight directors<br>• People felt appreciated for skills and potential to contribute to United Space Alliance into the future<br>• Shuttle program to continue to 2020<br>• Pride in producing safe, high quality products |

# Post-Columbia Accident, Return To Flight (2003 to 2005)

# Characteristics Of Period (2003 – 2005)

- **Cockpit Avionics Upgrade began in 2002. Continued until canceled late in 2004. Very large, major development activity with USA as prime for the development of hardware, software and integration.**
  - **Major SAIL facility modifications required**
  - **Major PASS FSW changes required**
  - **Major support software (Application Tools) changes required**
  - **Major FEID modifications required**
- **Space Shuttle Columbia and crew lost on February 1, 2003.**
- **OI development in this period limited to CAU which was large**
  - **Non-CAU work limited to additional flight changes to OI-30 for return to flight**
  - **No OI Development going on that would lead into a flight system.**

# Characteristics Of Period (2003 – 2005)

- For Cockpit Avionics Upgrade software, a new “upgrades” organization was formed.
  - Staffed in part by part time PASS personnel and by additional personnel hired specifically for CAU
- Cockpit Avionics Upgrade making meaningful progress.
- CAU requirements definition phase extended somewhat, with impact to development schedule
- President Bush changed space policy as a result of the Columbia accident on January 14, 2004
  - Space Shuttle would end by 2010
  - New exploration program which became Constellation
- CAU development terminated very late in 2004 after three years of effort.

# Space Events (2003 to 2005)

- Loss of Columbia (STS-107)
- 2-Man ISS Increments
- Messenger Launch to Mercury
- Mars Rovers Spirit / Opportunity Launched
- First Chinese Manned Spaceflight
- Shuttle Return to Flight (STS-114)

# Post-Columbia, Return To Flight (2003 to 2005)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Last of CAU builds<br>• Enhanced ADI / HSI capability |
| **Category** | **Observation / Characteristics** |
| Quality | • No active development for production Operational Increments<br>• Some activity changes on flight systems but no separate quality measures (included into OI-30 measurements).<br>• No objective data on CAU quality due to termination of program prior to verification start<br>• Focus on CAU and other return-to-flight activities continued to identify and remove latent errors in the PASS system<br>    • Nearly 50 % of remaining latent product DRs were discovered during this period between flight.<br>    • Significant increases in PASS software reliability |

# Post-Columbia, Return To Flight (2003 to 2005)

| Category | Observation / Characteristics |
|---|---|
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 60.7 Calendar Days to 75.2 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 140.4 Flight Days to 235.3 Flight Days<br><br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 3491 Flights to 4212 Flights |

# Post-Columbia, Return To Flight (2003 to 2005)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • No Product DRs introduced during this period<br>  • Development effort was focused on changes in support of the Cockpit Avionics Upgrade project, which was canceled<br><br>• Product DRs (unknown at the time) flown down to 20 remaining at end of 2005<br>  • 95 % improvement over STS-5<br>  • 49 % improvement over prior time period<br><br>• Released Severity 1 DRs<br>  • No newly introduced released Severity 1 DRs |

# Post-Columbia, Return To Flight (2003 to 2005)

| Category | Observation / Characteristics |
| --- | --- |
| Lessons Re-learned | • CAU re-taught us that new projects (which it really was) are not the same as maintenance projects<br>  • Challenge to teach this lesson to new persons or new project managers based on prior projects rather than learning it fresh on each project. |

| Category | Observation / Characteristics |
| --- | --- |
| New Lessons Learned | • None |

# Post-Columbia, Return To Flight (2003 to 2005)

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Expected morale hit following the Columbia accident<br>• Morale recovered as work continued on CAU and return-to-flight changes for STS-114<br>• Moral slightly impacted by new space policy including end of shuttle in 2010<br>    • Offset by opportunity for new work on Constellation<br>• Overall, moral relatively good with focus on return-to-flight |

# Shuttle To End In 2010, OI Development Continuing (2006 – 2008)

# Characteristics Of Period (2006 - 2008)

- Focus on flying shuttle missions and maintaining the critical skills to provide mission support and to resolve any issues in a timely manner
- Three OI's developed in this period (OI-32, OI-33, and OI-34)
  - OI content driven in differing directions by different forces
    - Large content desired from a skill maintenance perspective
    - Selected customer constituents advocating specific changes
    - Flight Operations and others wanting to minimize content so as to minimize the cost of stepping up to an OI in a declining budget environment
- Orion (CEV) contract awarded to Lockheed Martin on August 31, 2006.
- Moderately small, but significant flight software, simulation software, and CAIL (CEV Avionics Integration Laboratory) subcontract awarded to USA for support by the USA Flight Software Element.

# Characteristics Of Period (2006 - 2008)

- **To insure continued process quality and efficiency, complete a CMMI appraisal in November 2006; assessed at CMMI Level 5**
- **Generally, content size getting small and getting smaller. OI implementation of change instruments sometime assigned across multiple teams just to spread the exposure to code and process.**
- **After return-to-flight, there were a number of space shuttle program level technical issues that constraint the flight rate during this entire period as solutions were found to the technical issues**

# Space Events (2006 – 2008)

- Launch of New Horizons to Pluto
- Completion of ISS U.S. Segment (STS-120)
- Completion of ISS Truss Segments (STS-119)

# OI Development Continuing (2006 – 2008)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • Lambert Guidance Improvements<br>• 6x Traj display redesign<br>• Entry and Ascent Bearing Display additions<br>• RTLS ET Sep improvements<br>• Entry Remote Controlled Orbiter (RCO) Capability<br>• Elimination of old user notes and DRs<br>• Reduction in Horizontal Sit display code size<br>• Year End Roll Over (YERO) |

| Category | Observation / Characteristics |
|---|---|
| Quality | • Product Error Rate steady in range of 0.0 to 0.1 DRs/KSLOC<br>• Verification Effectiveness steady in the range of 95% to 100% DRs found by SRR<br>• Pre-build Detection Effectiveness (Inspection Plus Development Test) steady in the range of 80% to 100%. |

# OI Development Continuing (2006 – 2008)

| Category | Observation / Characteristics |
|---|---|
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br><br>•Calendar Days Between Any Product DR<br>• From 75.2 Calendar Days to 88.1 Calendar Days<br><br>• Flight Days Between Any In-flight DR<br>• From 235.3 Flight Days to 275.5 Flight Days<br><br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 4212 Flights to 4930 Flights |

# OI Development Continuing (2006 – 2008)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • Additional 1 Product DRs introduced on OI- 32 through OI-34.<br><br>• Product DRs (unknown at the time) flown down to 2 remaining at end of 2005<br>  • 99 % improvement over STS-5<br>  • 90 % improvement over prior time period<br><br>• In-flight DRs for STS-114 to STS-126<br>  • 162 Total Flight Days<br>  • 1 DR during flight (1 introduced on OI-33)<br><br>• Released Severity 1 DRs<br>  • No newly introduced released Severity 1 DRs<br>  • No known Severity 1 DRs flown during this period |

# OI Development Continuing (2006 – 2008)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • Ever present risk to "stumble" into maintenance traps once the maintenance trap is introduced into the software<br>  • Hardware constraint required data for output transactions to be located on "full word" (32 bit) boundary<br>  • Programming Standard put in place to require HAL/S compiler technique to always rigorously enforce "full word" boundary<br>  • Standard exception coded in one software module which required manual validation<br>    • Comments in code module described the exception<br>  • Due to series of events, the comments and code locations were separated<br>  • Unrelated change made on OI-33 which shifted data, resulting in a break in an existing capability<br>  • Model fidelity in simulations, lab anomalies, and failure to execute scenarios resulted in error escaping to flight.<br>  • Automated PASS software capabilities did not work in flight; required ground controllers to perform manual workarounds. |

# OI Development Continuing (2006 – 2008)

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • None |

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Negatively impacts morale<br>• Decision to cancel CAU<br>• Count down to the end of shuttle program puts future employment at risk<br>• Quite a bit of uncertainty<br>• Positively impacts morale<br>• CEV (Orion) subcontract provides hope for continued employment at the end of shuttle program<br>• Steady space shuttle missions provide sense of accomplishment |

# Shuttle To End Delayed Slightly, Skill Maintenance (2009 – 2011)

# Characteristics Of Period (2009 - 2011)

- Space Shuttle end targeted for October, 2010
- 8 shuttle flights in 14 months provide a focus which distracts from the approaching end of shuttle through STS-132 (May 2010)
- Focus on executing training activities to maintain critical skills in place of production OI work in prior period
- President Obama administration announced new space policy on January 27, 2010 which would extend International Space Station operations through at least 2020 but abandon NASA's current plans to return U.S. astronauts to the moon.
- Payload issues and ISS traffic constraints result in slipping last space shuttle flight ending in March 2011
  - Leaves large gaps between flights
    - May 2010 to Nov 2010, Nov 2010 to Feb 2011

# Characteristics Of Period (2009 - 2011)

- To insure continued process quality and efficiency, complete a second CMMI appraisal in September 2009; assessed at CMMI Level 5
- Uncertainty of fate of Constellation projects such as CEV (Orion)
- Uncertainty over the NASA authorization language that will be law for 2011

# Space Events (2009 – 2011)

- Six Person ISS Resident Crew Capability
- Completion of Primary ISS Construction (STS-130)
- ATV / HTV first flights
- Last Hubble Space Telescope Repair Mission (STS-125)
- End of Shuttle Program – 2011? (STS-135?)

# Skill Maintenance (2009 – 2011)

| Category | Observation / Characteristics |
|---|---|
| Scope Of Development | • No active development for production Operational Increments; minor flight systems changes |

| Category | Observation / Characteristics |
|---|---|
| Quality | • No active development for production Operational Increments<br>• Minor flight systems changes, inadequate size of changes to establish meaningful metrics. |

| Category | Observation / Characteristics |
|---|---|
| Reliability | •Three Mean Time Between Failure (MTBF) measures presented here.<br>•Calendar Days Between Any Product DR<br>• From 88.1 Calendar Days to 94.0 Calendar Days<br>• Flight Days Between Any In-flight DR<br>• From 275.5 Flight Days to 293.9 Flight Days<br>•Shuttle Flights Between Severity 1 PASS DR<br>• From 4930 Flights to 6260 Flights |

# Skill Maintenance (2009 – 2011)

| Category | Observation / Characteristics |
|---|---|
| Product DRs | • No additional Product DRs introduced during this period<br><br>• Product DRs (unknown at the time) flown down to 0 remaining as of July, 2010<br><br>• In-flight DRs for STS-119 to STS-132 (as of 05/2010)<br>    • 114 Total Flight Days<br>    • 0 DRs during flight<br><br>• Released Severity 1 DRs<br>    • No newly introduced released Severity 1 DRs<br>    • No known Severity 1 DRs flown during this period |

# Skill Maintenance (2009 – 2011)

| Category | Observation / Characteristics |
|---|---|
| Lessons Re-learned | • None |

| Category | Observation / Characteristics |
|---|---|
| New Lessons Learned | • None |

| Category | Observation / Characteristics |
|---|---|
| Staffing / Morale | • Positive effect on morale<br>• High flight rate to May 2010, sense of accomplishment<br>• Personnel engaged in value add skill development projects<br>• Shuttle continuing to fly slightly longer<br>• Potential that CEV Orion project will continue to be funded<br>• Negative effect on morale<br>• Unemployment rapidly approaching |

# Summary

# Contributors To PASS FSW High Quality

| Contributor To PASS FSW High Quality | Context |
|---|---|
| Multiple releases and multiple iterations of testing prior to STS-1. | Delays in launch date due to TPS and SSME issues provided more testing time and more opportunities to fix identified problems. |
| Fully automated Flight-to-Flight Reconfiguration Process and Tools | Early flights had a number of System Management in flight failures due to late manual updates. |
| Structured "PASS Revalidation" activities between Challenger accident and STS-26 | Direct contributor to eliminating Severity 1 (Loss of crew/vehicle) DRs from PASS |
| Continual enhancements of the Requirements/Design/Code/Test Inspection Processes | • Have appropriate participation in each type of inspection including external community participation<br>• Having appropriate re-inspection criteria |
| Adequate test facility functionality and capacity (equipment to execute cases on flight equivalent hardware) | Significant improvement in in-flight reliability between STS-51L and STS-26 during a period when test facility capacity increased by a factor of 3. |
| Defined criteria for selection of personnel for teams; define how to resist over commitment of critical skills. | Critical skills management has always been a priority. Re-enforced by action From OI-25 PTI DRs where team skill and over commitment were contributing factors. |
| Rigorous configuration management of all products including requirements, design, code, and tests. | Basic necessary condition |

# Space Shuttle Flight Software Periods

| Years | Theme | Summary |
|---|---|---|
| 1978-1982 | Initial System Development | Tremendous accomplishment with quality level of about 1 product error / KSLOC. Excellent in flight software reliability in this period. However, still resulted in 424 DRs flown (unknown at the time) on STS-5 including 3 Severity 1 DRs (loss of crew/vehicle) in contingency abort scenarios. |
| 1983-1985 | Pre-Challenger Operations | Product error/KSLOC increased for early OI releases. Flight to flight reconfiguration late updates were manual, resulting in several in flight DRs. Additional DRs due to failure to test PASS to Spacelab interface. Abort due to SSME failure on STS-41D prevented launch with Severity 1 DR with probability of occurring of 1 in 6. |
| 1986-1988 | Post-Challenger, Return to Flight | Very productive period with an emphasis on safety and quality. Product error rate reduced to 0.2 errors/KSLOC. STS-26 flew with only 240 DRs (unknown at the time), a significant reduction from STS-5. All Severity 1 DRs identified and removed prior to STS-26. In flight software reliability increased by a factor of 10 over STS-5. Preparation in work to step up to upgraded General Purpose Computer AP-101S. |
| 1989-1993 | Process Optimization and Stability | Recognized as CMM Level 5. Implemented GPC Memory/Speed Upgrade and added major new capabilities. Product error rate reduced to 0.2 errors/KSLOC. Skilled, Stable Workforce. STS-61 flew with 140 DRs (unknown at the time). Only one in flight DR over 291 flight days. |
| 1994-1997 | Transition To Loral / Lockheed Martin | Significant work force distractions during acquisitions affecting the PASS project . Notable process escape on OI-25. Excluding OI-25, continued to achieve Product error rate of 0.2 errors/KSLOC. Continued reduction in latent DRs being flown to 100 DRs (unknown at the time). |
| 1998-2002 | Transition to United Space Alliance | Restore Workforce Stability / Influx Of New Personnel. Product error rate of 0.2 errors/KSLOC. Continued reduction in latent DRs being flown to 39 DRs (unknown at the time). In flight software reliability increased by a factor of 15 over STS-5. |

# Space Shuttle Flight Software Periods

| Years | Theme | Summary |
|---|---|---|
| 2003-2005 | Post-Columbia / Return-To-Flight | Activities included Cockpit Avionics Upgrade (later canceled), Columbia Accident , and Return to Flight. No OI development in this period that went to flight systems. Continued reduction in latent DRs being flown to 20 DRs (unknown at the time). |
| 2006-2008 | Shuttle Ending, OI Development | Continued development of OI-32, OI-33, and OI-34. Assessed as CMMI Level 5 November 2006. Product error rate of 0 to 0.1 errors/KSLOC. Continued reduction in latent DRs being flown to 2 DRs (unknown at the time). |
| 2009-2011 | Shuttle Ending, Skill Maintenance | Continued training activities for Skill Maintenance. SAIL to one shift operations and other Reductions-In-Workforce. As of this presentation, there had been no DRs discovered, including latent DRs, since the first flight of OI-34. |

# Wrap-up

- This presentation has shown the accomplishments of the PASS project over three decades and highlighted the lessons learned.
- Over the entire time, our goal has been to
  - Continuously improve our process
  - Implement automation for both quality and increased productivity
  - Identify and remove all defects due to prior execution of a flawed process in addition to improving our processes following identification of significant process escapes
- Morale and workforce instability have been issues, most significantly during 1993 to 1998 (period of consolidation in aerospace industry)
- The PASS project has also consulted with others, including the Software Engineering Institute, so as to be an early evaluator, adopter, and adapter of state-of-the-art software engineering innovations

# Acronyms

# Acronyms

| | Acronym |
|---|---|
| ADI | Attitude Direction Indicator |
| ALT | Approach and Landing Test |
| AP-101B | Initial flight computer for Space Shuttle; 104 K 32-bit full works of Memory |
| AP-101S | Upgrade flight computer for Space Shuttle; 256 K 32-bit full words of Memory (256K 32-bit FWs = 1MB 8-bit bytes). |
| ATV | Automated Transfer Vehicle |
| CAIL | CEV Avionics Integration Lab |
| CAU | Cockpit Avionics Upgrade |
| CEV | Crew Exploration Vehicle |
| CI | Configuration Inspection |
| CM | Configuration Management |
| CMM | Capability Maturity Model |
| CMMI | Capability Maturity Model Integrated |

# Acronyms

| | Acronym |
|---|---|
| CPU | Central Processing Unit |
| DAP | Digital Auto Pilot |
| DOD | Department of Defense |
| DR, DRs | Discrepancy Report(s) |
| ECAL | East Coast Abort Landing |
| ET | External Tank |
| FSW | Flight Software |
| GPC | General Purpose Computer |
| GPCF | GPC Payload Command Filter |
| GPS | Global Positioning System |
| HIS | Horizontal Situation Indicator |
| HTV | H-II Transfer Vehicle |
| ICD | Interface Control Document |
| KSC | Kennedy Space Center |

# Acronyms

| | Acronym |
|---|---|
| KLSOC | 1000 Non-Comment Source Lines of Code (new, changed, and deleted) |
| MEDS | Multifunction Electronic Display System |
| MIR | Name of the Russian Space Station |
| MTBF | Mean Time Between Failures |
| NASA | National Aeronautics and Space Administration |
| OFT | Orbital Flight Test |
| OI | Operational Increment |
| OPS | Operational Sequences |
| OV | Orbiter Vehicle |
| PTI | Program Test Input |
| RCO | Remotely Controlled Orbiter |
| RMS | Remote Manipulator System |
| RTLS | Return-To-Launch-Site |

# Acronyms

| | Acronym |
|---|---|
| RTLS | Return-To-Launch-Site |
| SAIL | Shuttle Avionics Integration Laboratory |
| SASCB | Shuttle Avionics Software Control Board |
| SEI | Software Engineering Institute |
| SM | Systems Management |
| SM/PL | Systems Management/Payload |
| SMS | Shuttle Mission Simulator |
| SRR | Software Readiness Review, typically 4 weeks prior to flight |
| SSME | Space Shuttle Main Engine |
| STS | Space Transportation System |
| TAL | Transoceanic Abort Landing |
| TPS | Thermal Protection System |
| Traj | Trajectory |
| YERO | Year End Roll Over |