THE DEVELOPMENT PROCESS FOR THE SPACE SHUTTLE PRIMARY AVIONICS SOFTWARE SYSTEM

SPACE SHUTTLE PROGRAMS

IBM
Federal Systems Division
3700 Bay Area Boulevard
Houston, Texas 77058/1199

PRESENTATION TO COMMON CONFERENCE
OCTOBER 20, 1987
CHICAGO, ILLINOIS

T. W. KELLER
MANAGER, OBS PROJECT COORDINATION & CONFIGURATION MANAGEMENT
SOFTWARE CRITICAL TO NASA SHUTTLE

CONTENTS

- INTRODUCTION
- PROJECT OVERVIEW
- PRIMARY AVIONICS SOFTWARE SYSTEM DESCRIPTION
- SOFTWARE DEVELOPMENT APPROACH
- USER SUPPORT AND PROBLEM DIAGNOSIS
- SOFTWARE RELEASES AND RECONFIGURATION
- APPENDICES
  A. QUALITY/PRODUCTIVITY PROGRAMS
  B. SOFTWARE DEVELOPMENT/PRODUCTION FACILITIES
  C. ACRONYMS
  D. EXTERNAL EVALUATIONS OF IBM PROCESS
INTRODUCTION
IBM CORPORATE ORGANIZATION

WORLD TRADE

INFORMATION SYSTEMS TECHNOLOGY GROUP
- General Technology Division
- Systems Technology Division

INFORMATION SYSTEMS & COMMUNICATIONS GROUP
- Communications Products Division
- Entry Systems Division
- Industrial Systems
- Telecommunication Products

INFORMATION SYSTEMS & STORAGE GROUP
- Data Systems Division
- General Products Division

INFORMATION SYSTEMS & PRODUCTS GROUP
- Information Products Division
- System Products Division

FEDERAL SYSTEMS DIVISION
- North-Central Marketing Division
- South-West Marketing Division
- National Service Division
- National Distribution Division
PROJECT OVERVIEW
SOFTWARE CRITICAL TO NASA SHUTTLE

PROJECT OVERVIEW

- Software Development Spanned Over 10 Years to the Base System Delivery in 1981
- Now Incorporating New Capabilities Into the Base System
- Current Level of 300-350 Software Developers Per Year
- Releases Tailored to Specific Missions by Data Reconfiguration
- All Work Done in the NASA Software Development and Production Facilities
- On-Line Access to Software Via Terminals
SOFTWARE CRITICAL TO NASA SHUTTLE

SOFTWARE DEVELOPMENT PHILOSOPHY

• Goals:
  - Meet Letter and Intent of Customer Requirements
  - Perform in Accordance with Customer Expectations
  - Error-Free Software

• Project Organization Functions
  - Requirements Analysis, System Architecture
  - Software Development (Design, Code, Test)
  - System Build and Integration
  - Independent Verification
  - Reconfiguration/Certification
  - Customer and Field Support

• Configuration Management
  - Formal Board Structure
  - Documents Requirements and Design Baselines
  - Stored in Configuration Management Data Base
<table>
<thead>
<tr>
<th>SOFTWARE PROJECT</th>
<th>SOURCE LINES OF CODE (X 1000)</th>
<th>NASA CENTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLIGHT SOFTWARE SYSTEM</td>
<td>500K</td>
<td>JSC</td>
</tr>
<tr>
<td>SOFTWARE PRODUCTION FACILITY (SPF) (SIMULATOR AND SUPPORT SOFTWARE)</td>
<td>1,700K</td>
<td>JSC</td>
</tr>
<tr>
<td>MISSION AND PAYLOAD CONTROL CENTERS</td>
<td>4,000K</td>
<td>JSC</td>
</tr>
<tr>
<td>LAUNCH PROCESSING SYSTEM</td>
<td>2,500K</td>
<td>KSC</td>
</tr>
<tr>
<td>SPACELAB</td>
<td>800K</td>
<td>MSFC</td>
</tr>
<tr>
<td>TOTAL</td>
<td>9,500K</td>
<td></td>
</tr>
</tbody>
</table>
PRIMARY AVIONICS SOFTWARE SYSTEM DESCRIPTION
SHUTTLE ONBOARD DATA PROCESSING SYSTEM

• HARDWARE
  — 5 GENERAL PURPOSE FLIGHT COMPUTERS (GPC's)
    • WITH ASSOCIATED DISPLAYS, KEYBOARDS AND MASS STORAGE DEVICES

• SOFTWARE
  — PRIMARY AVIONICS SOFTWARE SYSTEM (PASS)
    • SEPARATED INTO 7 OPERATIONAL PROGRAMS
    • KEYED TO SPECIFIC MISSION PHASES
  — BACKUP FLIGHT SYSTEM (BFS)
    • PROVIDES ADDITIONAL REDUNDANCY DURING CRITICAL FLIGHT PHASES
    • EXECUTES ONLY DURING ASCENT AND ENTRY

• DURING CRITICAL MISSION PHASES (ASCENT, ENTRY, PRE-FLIGHT PREP.)
  — 4 OF 5 GPC's CONTAIN THE PRIMARY AVIONICS SOFTWARE EXECUTING
    REDUNDANTLY
  — THE 5TH COMPUTER CONTAINS THE BACKUP FLIGHT SYSTEM EXECUTING IN
    PARALLEL (WITH OUTPUT COMMANDS INHIBITED)

• IN LESS-CRITICAL MISSION PHASES (ON-ORBIT)
  — MULTIPLE PASS OPERATIONAL PROGRAMS EXECUTE IN 2 OR 3 GPC's
  — REMAINING GPC's ARE POWERED-OFF
REDUNDANT GPC SETS

- Processes within GPCs synchronized.
- Identical input data required. Listen mode used to allow GPC to receive data from bus not under its control.
- Sync points inserted at appropriate locations in software. (~350/sec.).
- Dedicated sync lines interconnect all GPCs. All must send and receive synch discrete at sync window.
- Allows independent strings with simultaneous data access.
EXAMPLE OF REDUNDANT PROCESSING

LISTEN MODE
PRIMARY AVIONICS SOFTWARE SYSTEM FUNCTIONS

• MISSION CRITICAL SOFTWARE SYSTEM

• SUPPORTS ALL FLIGHT PHASES FROM PRE-LAUNCH CHECKOUT THROUGH ROLLOUT
  — COMMANDS OR COMMUNICATES WITH HUNDREDS OF ONBOARD SYSTEMS

• PREFLIGHT
  — VEHICLE SUBSYSTEMS CHECKOUT
  — PAYLOAD CHECKOUT
  — PROPELLANT LOADING
  — TERMINAL COUNTDOWN SEQUENCING (E.G., ENGINE START)

• ASCENT
  — AUTOMATIC AND MANUAL GUIDANCE, NAVIGATION AND FLIGHT CONTROL
  — NOMINAL LAUNCH SEQUENCE (E.G., BOOSTER STAGING)
  — ABORT SEQUENCING (E.G., RTLS, TAL, AOA, ATO)


PRIMARY AVIONICS SOFTWARE SYSTEM FUNCTIONS
(continued)

• ORBIT
  — AUTOMATIC AND MANUAL GUIDANCE, NAVIGATION AND FLIGHT CONTROL
  — VEHICLE SUBSYSTEM MONITORING/FAULT DETECTION/ANNUNCIATION
  — PAYLOAD MONITORING, CONTROL, DEPLOYMENT
  — REMOTE MANIPULATOR ARM CONTROL
  — PAYLOAD BAY DOOR OPERATION
  — COMMUNICATIONS ANTENNA MANAGEMENT
  — ENTRY SYSTEMS CHECKOUT

• ENTRY
  — COMPUTATIONS FOR DEORBIT ENGINE FIRING (TARGETING)
  — AUTOMATIC AND MANUAL GUIDANCE, NAVIGATION AND FLIGHT CONTROL
    (THROUGH ROLLOUT AND BRAKING)
SOFTWARE CRITICAL TO NASA SHUTTLE

SOFTWARE CONFIGURATION FOR A TYPICAL SHUTTLE FLIGHT
There are nine places where on-board primary software developed for the Space Shuttle may be in use:

- Vehicle in Orbit
- Vehicle at Cape Canaveral Preflight (KSC)
- Vehicle at Edwards AFB Postflight
- Shuttle Mission Simulator (SMS)
- Shuttle Avionics Integration Laboratory (SAIL)
- Software Development Facility (SDF)
- Software Production Facility (SPF)
- New Orbiter under Construction at Palmdale
- Vehicle at Vandenberg AFB Preflight (VLS)
SOFTWARE DEVELOPMENT APPROACH
OPERATIONAL INCREMENT DEVELOPMENT MILESTONES

- REQUIREMENTS DEFINITION
- SOFTWARE DEVELOPMENT
- SYSTEM BUILD AND INTEGRATION
- SYSTEM VERIFICATION
- MISSION RECONFIGURATION

TESTING
- LEVEL 1
- LEVEL 2
- LEVEL 3

FACI

CI

FIRST ARTICLE CONFIGURATION INSPECTION

CONFIGURATION INSPECTION

FLIGHT RECONFIGURATIONS

STS: "N"

STS: "N+1"

STS: "N+2"

- LAUNCH DATE
- SOFTWARE RELEASE TO CUSTOMER
- FLIGHT SPECIFIC REQUIREMENTS

IBM SPACE SHUTTLE PROGRAMS
SOFTWARE CRITICAL TO NASA SHUTTLE

SOFTWARE DEVELOPMENT PROCESS
SOFTWARE DEVELOPMENT APPROACH

- MAJOR DEPARTMENT AREAS
  - REQUIREMENTS ANALYSIS & SYSTEM ARCHITECTURE
  - SOFTWARE DEVELOPMENT
  - SYSTEM BUILD AND INTEGRATION
  - INDEPENDENT VERIFICATION
  - CUSTOMER AND FIELD SUPPORT
  - RECONFIGURATION/CERTIFICATION

- CONFIGURATION CONTROL (CONTROL BOARD STRUCTURE)
SHUTTLE ONBOARD SOFTWARE ORGANIZATION

QUALITY PROGRAMS

- AVIONICS SOFTWARE ENGINEERING, DEVELOPMENT & VERIFICATION
  - Requirements Analysis
  - FLT S/W Development
  - Independent Verification

- SOFTWARE SYSTEMS DEVELOPMENT AND ENGINEERING
  - SPF/SDF Software Development & Test
  - Flight Software Reconfiguration and Certification
  - Data Base Applications Development

PROJECT SCHEDULE/BASELINES CONFIGURATION MGT

TEST AND OPERATIONS
PROJECT CONTROL BOARD STRUCTURE

- PROJECT WIDE CONFIGURATION CONTROL MAINTAINED BY 5 CONTROL BOARDS
  - PROJECT SCHEDULING AND OVERALL COORDINATION (BCB)
  - SOFTWARE REQUIREMENTS (RRB)
  - SOFTWARE DISCREPANCIES (DRB)
  - PROGRAMMING STANDARDS AND SYSTEM ARCHITECTURE (SARB)
  - SUPPORT SOFTWARE AND TEST BED (SSRB)

- CHAIRED BY KEY STAFF PERSONNEL

- REPRESENTATION BY ALL PROJECT AREAS (DEVELOPMENT, VERIFICATION, ETC.)
SOFTWARE CRITICAL TO NASA SHUTTLE

ONBOARD SHUTTLE SOFTWARE DEVELOPMENT
REQUIREMENTS ANALYSIS

- DEDICATED REQUIREMENTS ANALYSIS GROUP FORMED TO INTERFACE WITH CUSTOMER AND DEVELOPMENT ORGANIZATION RESPONSIBILITIES INCLUDE:
  - ASSESSMENT OF CUSTOMER SUPPLIED REQUIREMENTS
  - GENERATION OF SOFTWARE REQUIREMENTS

- FUNCTIONS
  - REQUIREMENTS AND DESIGN TRADEOFFS
  - ENSURE REQUIREMENTS MATURITY, COMPLETENESS, CLARITY
  - HARDWARE/FIRMWARE/SOFTWARE COMPATIBILITY
  - CPU AND MEMORY CONSTRAINT CONSIDERATIONS
  - TESTABILITY OF REQUIREMENTS

- TECHNIQUES AND TOOLS
  - CONCEPTUAL DESIGN TEAM CONCEPT TO ADDRESS EACH FUNCTIONAL AREA (CUSTOMER INVOLVEMENT)
  - FORMAL REQUIREMENTS REVIEWS WITH SOFTWARE DEVELOPMENT, VERIFICATION AND FIELD SUPPORT PERSONNEL REPRESENTATION
  - MECHANISM FOR COMMUNICATION OF REQUIREMENT "LETTER" AND "INTENT"
  - ANALYTICAL MODELING OF SOFTWARE SYSTEM

- OTHER RESPONSIBILITIES
  - SYSTEM LEVEL (OPERATIONAL) TEST RESPONSIBILITY
  - CONSULTATION TO ALL PROJECT AREAS (DEVELOPMENT, TEST, CUSTOMER, FIELD SUPPORT)
  - CHANGE CONTROL BOARD MEMBERSHIP
SOFTWARE DEVELOPMENT

- INDEPENDENT ORGANIZATION SEPARATE FROM REQUIREMENTS ANALYSIS, VERIFICATION, AND CUSTOMER SUPPORT GROUPS

- FUNCTIONS
  - PARTICIPATION IN INITIAL REQUIREMENTS BASELINE OR CHANGE ASSESSMENT AND SCHEDULING
  - FUNCTIONAL AND DETAILED DESIGN
  - CODE IMPLEMENTATION
  - MODULE LEVEL UNIT TESTING (LEVEL 1)
  - FUNCTIONAL LEVEL TESTING (MODULE TO MODULE INTERFACES, LEVEL 2)
  - SUBMITTAL TO SYSTEM BUILD
  - DESIGN DOCUMENTATION

- TECHNIQUES AND TOOLS
  - FORMAL, HIGHLY STRUCTURED DESIGN AND CODE INSPECTIONS
    • TRAINED MODERATORS AND PEER PARTICIPATION
    • REPRESENTATIVES FROM REQ'TS ANALYSIS AND VERIFICATION
    • CHECKLISTS WITH FORMAL SIGNOFF
    • CODE AUDITING TOOLS
    • ISSUES FORMALLY TRACKED AND DISPOSITIONED
  - TESTING PERFORMED ON OPERATIONAL HARDWARE
  - INTERIM MILESTONES TRacked AT PROGRAMMER AND MODULE LEVEL AGAINST AUTOMATED DEVELOPMENT PLAN
    • DESIGN START AND COMPLETE, CODE START AND COMPLETE, ETC.
  - RESPONSIBLE FOR IMPLEMENTATION OF ALL DISCREPANCY CORRECTIONS
  - FORMALIZED FEEDBACK AND ANALYSIS OF SOFTWARE DISCREPANCIES
    • ANALYSIS OF INDIVIDUAL DISCREPANCIES TO IDENTIFY WEAKNESSES IN THE PROCESS
    • TREND ANALYSIS
SYSTEM BUILD AND INTEGRATION

• PRIMARY ELEMENTS
  — AUTOMATED SYSTEM BUILD
  — MASS MEMORY INTEGRATION
PASS SYSTEM BUILD

- Online interactive transactions (menus) provide automated build control
- Updated source modules and new modules are placed into permanent system configuration controlled data sets
- A build control list drives the system build process using configuration control information from the configuration management data base
- Consistency between updated source and executable load modules is insured during compilation and link edit steps
- A source dependency scanner automatically identifies other source modules which must be recompiled due to dependencies on source being updated
- A recompile director determines the order in which all source updates must be performed
- Change accounting information (revision level) is added to source language records and identification information is added to load modules
- Build termination processing indicates status of all built items in the configuration management data base
- Numerous analysis reports are output from the system build tools, including a listing tape of all built changes
MASS MEMORY INTEGRATION

• AN AUTOMATED PANEL DRIVEN SYSTEM BY WHICH SOFTWARE ELEMENTS IN ADDITION TO PASS ARE INTEGRATED AND MAPPED INTO THE FORMAT REQUIRED BY THE MASS MEMORY UNITS

• I-LOAD DATA NEEDED TO ALLOW SUCCESSFUL SYSTEM EXECUTION IS APPLIED TO THE MASS MEMORY VIA THE AUTO-I-LOAD PROCESSOR AND THE MASS MEMORY PATCH UTILITY

• SOFTWARE ELEMENTS ARE INTEGRATED ON THE MASS MEMORY UNIT
  — PRIMARY AVIONICS SOFTWARE SUBSYSTEM (PASS)
  — INITIAL PROGRAM LOAD
  — BACKUP FLIGHT SOFTWARE (BFS)
  — SPACE SHUTTLE MAIN ENGINE
  — TFL/DFL
  — TEST CONTROL SEQUENCES
  — TEXT AND GRAPHICS
  — DEU

• PRINTED MASS MEMORY MAPS, PHASE TABLES AND OTHER REPORTS ARE GENERATED

• DELIVERY LOAD TAPES OR DATA SETS ARE CREATED FOR USE BY FACILITIES/VEHICLE
INDEPENDENT VERIFICATION

INDEPENDENT MULTI-LEVEL TEST PROGRAM
• USED ON SHUTTLE ONBOARD SOFTWARE PROJECT
• ASSUMES SOFTWARE IS “UNTESTED”
• ALL TESTING PERFORMED ON OPERATIONAL DPS FLIGHT HARDWARE IN SOFTWARE DEVELOPMENT FACILITY
• TWO LEVELS OF TESTING PERFORMED ON OPERATIONAL HARDWARE BY SEPARATE ORGANIZATIONS
  — DETAILED/FUNCTIONAL TESTING (MODULE/FUNCTIONAL TESTS AGAINST REQ’TS AND DESIGN),
    ALSO CALLED “SPECIFICATION BASED FUNCTIONAL TESTING”
  — SYSTEM LEVEL PERFORMANCE TESTING UNDER OPERATIONAL CONDITIONS
• TEST STANDARDS AND FORMAL TEST CASE REVIEWS TO ASSURE QUALITY
• STATIC CODE ANALYSIS TO AUGMENT TESTING
• RESPONSIBLE FOR REGRESSION TESTING OF ALL CHANGES
• FORMALIZED FEEDBACK AND ANALYSIS OF SOFTWARE DISCREPANCIES
  — ANALYSIS OF INDIVIDUAL DISCREPANCIES TO IDENTIFY WEAKNESSES IN THE PROCESS
  — TREND ANALYSIS
• INTERIM MILESTONES TRACKED AT THE TEST ANALYST, MODULE OR CHANGE LEVEL
  — COMPARISON TO AUTOMATED DEVELOPMENT PLAN
• DOCUMENTATION (TEST SPECIFICATIONS, PROCEDURES, SIMULATION CASES AND REPORTS)
USER SUPPORT
AND
PROBLEM DIAGNOSIS
CUSTOMER SUPPORT AND FIELD OPERATIONS

FIELD SITE RESIDENT PERSONNEL WITH RESPONSIBILITIES AS FOLLOWS:

- SOFTWARE INSTALLATION AND MAINTENANCE
- USER TRAINING
- USER LIAISON
- CUSTOMER TEST SUPPORT
- OPERATIONS SUPPORT
IBM PROBLEM DIAGNOSIS

SIMULATIONS AND TRAINING

0 VERBAL DESCRIPTIONS
0 VEHICLE DYNAMICS
0 LOG OF KEYBOARD INPUTS
0 MEMORY DUMPS
0 TELEMETRY DOWNLIST
0 CONSOLE LOGS
0 TABULAR PARAMETRIC DATA

IN FLIGHT

INITIAL CLUES
- DISPLAYS (Photos)
- VERBAL DESCRIPTIONS
- VEHICLE DYNAMICS
- LOG OF KEYBOARD INPUTS
- MEMORY DUMPS
- TELEMETRY DOWNLIST
- CONSOLE LOGS
- TABULAR PARAMETRIC DATA

VERIFICATION AND TESTING

PROBLEM

IBM FLIGHT SOFTWARE SUPPORT

DIAGNOSIS

RESOLUTION

GROUND SUPPORT

MATRIX OF EXPERTISE

IBM SPACE SHUTTLE PROGRAMS
FACT FINDING

1. QUESTION THE WITNESS
   - WHAT DID HE OBSERVE

2. DETERMINE FLIGHT SCENARIO
   SURROUNDING PROBLEM
   MEMORY CONFIGURATION
   MANEUVERS EXECUTED
   KEYSTROKES ENTERED
   FAILURES EXPERIENCED

3. SEARCH FOR USERS WITH
   SIMILAR SYMPTOMS
INVESTIGATION TECHNIQUES

- USE APPROPRIATE DIAGNOSTIC TECHNIQUES
  - PROGRAM CROSS REFERENCE
  - MAGNIFIED TIMELINES
  - CAUSE AND EFFECT GRAPHS
  - CYCLIC/MULTIPASS EVALUATIONS
  - TRAP PATCHES/TRACES
  - PROCESS DESENSITIZATION
  - COMMON DENOMINATOR DETERMINATION

- EVALUATE FSW RESPONSE TO HYPOTHESIZED INPUTS
  - CODE WALK-THROUGH/MENTAL INSPECTION
  - EXECUTION TEST
  - REVISE HYPOTHESIS
  - CHALLENGE ASSUMPTIONS
Problem Isolation

Initially Suspected "Unit" of Software

A. Hardware Sensor Input

B. Sensor Interface (Process X)

C. Sensor Fault Detection (Process Y)

D. Annunciation Routine (Process Z)

Errors (annunciates system failure)

Immediate Symptom

Raw Sensor Output Telemetry (indicates no sensor failure)

Sensor Status Telemetry (indicates a sensor failure)

Successive Iterations

Move upstream in process flow

"Reported Symptom"

IBM Space Shuttle Programs
THE GN&C FSW PROBLEM ANALYSIS PROCESS

DEFINITION OF PROBLEM
EVALUATION:
- "WHAT IS THE PROBLEM" (DIRECTLY CONTACT WITNESS)
- THE SCENARIO WHICH LED TO THE PROBLEM AND THE ENVIRONMENT, SYSTEM, AND FSW CONFIGURATIONS
  - FAULTS, FAILURES ENCOUNTERED
  - EXTERNAL STIMULI
  - SOFTWARE VERSION
  - SOFTWARE ALTERATIONS APPLIED
- WHETHER OTHER USERS EXPERIENCED SIMILAR SYMPTOMS
- THE "CORRECT" SOFTWARE RESPONSE TO THE CONDITIONS ENCOUNTERED (REVIEW REQUIREMENTS)

FACT FINDING

DO REQUIREMENTS COVER THESE CONDITIONS

SOFTWARE RESPONSE CORRECT

ASSIGN TO REQUIREMENT REVIEW TEAM

EDUCATE THE USER

PROBLEM RECONSTRUCTION

SEARCH FOR SUSPECT UNIT OF CODE

IS OUTPUT SYMPTOM AN EFFECT OF A SYMPTOMATIC INPUT TO THAT CODE

REITERATE

YES

NO

IS ROOT PROBLEM RECOGNIZABLE

YES

NO

APPLY SPECIAL TECHNIQUES

HAS SYMPTOM-CAUSING SCENARIO BEEN RECONSTRUCTED

RE-EVALUATION OF PROBLEM HYPOTHESES

RE-EVALUATION OF PROBLEM HYPOTHESES

INTERPRET RESULTS OF DIAGNOSTIC TESTS

APPLICATION OF DIAGNOSTIC TECHNIQUES

- RESULTS OF APPLICATION OF DIAGNOSTIC TECHNIQUES REVIEWED
  - FOR NEW SYMPTOMS
  - FOR INTERMEDIATE SYMPTOMS

SHORTENED TIMESLINES

CAUSE AND EFFECT GRAPHS

CYCLIC OR MULTI-PASS EVALUATIONS

"TRAP" PATCHES OR TRACES

PROCESS DESENSITIZATION TO SELECTED INPUTS

COMMON DENOMINATOR DETERMINATION

EVALUATE CODE UNIT RESPONSE TO INPUTS

INVESTIGATION

INTERPRETATION OF CLUES

RE-EVALUATION OF THEORIES

SOLUTION

MAKE RECOMMENDATION FOR SOLUTION
- MODIFY
- DOCUMENT PROBLEM AND WORKAROUNDS

IBM SPACE SHUTTLE PROGRAMS
MAGNIFIED TIMELINE EXAMPLE

IBM SPACE SHUTTLE PROGRAMS
CAUSE AND EFFECT GRAPHING **EXAMPLE**

- **SIMULATED ENVIRONMENT**
  - MODELED IMU ACCELERATION

  **INSTRUMENT MEASUREMENT UNIT INPUT INTERFACE**

  **IMU-SENSED ACCELERATION**

  **ATTITUDE PROCESSOR**

  **NAVIGATION USER PARAMETER PROCESSOR**

  **CLOSED-LOOP PITCH AXIS CONTROL**

  **NAVIGATION DERIVED AIR DATA EQUIVALENT PROCESSOR**

  **ENTRY GUIDANCE PROCESSOR**

  **FLIGHT CONTROL PROCESSOR**

  **NORMAL ACCELERATION COMMAND**

  **ELEVON COMMAND**

  **SENSIZED ALTITUDE RATE**

  **TACAN △**

  **ALTIMETER**

  **DYNAMIC PRESSURE**

  **SENSE DROG**

  **TIME**

IBM SPACE SHUTTLE PROGRAMS
SOFTWARE RELEASES AND RECONFIGURATION
SOFTWARE CRITICAL TO NASA SHUTTLE

SOFTWARE RELEASES AND RECONFIGURATION

Months

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

New Capabilities Development

2 3 4

FACI

FACI

FACI

Independent Verification

2 3 4

CI

Flight Reconfiguration

X STS "N"

Flight Reconfiguration

X STS "N+1"

Flight Reconfiguration

X STS "N+2"

X - Launch Date

FACI - First Article Configuration Inspection

CI - Configuration Inspection
RECONFIGURATION/CERTIFICATION

- INDEPENDENT ORGANIZATION RESPONSIBLE FOR "TAILORING" FLIGHT SOFTWARE SYSTEMS TO SPECIFIC FLIGHTS
- HIGHLY AUTOMATED PROCESS
- FUNCTIONS
  - RECEIVE ELECTRONIC REQUIREMENTS FROM NASA (WITHIN THE SPF)
    - MISSION PROFILE DATA (CALLED I-LOADS)
    - PAYLOAD AND VEHICLE SYSTEMS DATA (CALLED LEVEL-C DATA)
    - TELEMETRY CONFIGURATION DATA (CALLED DOWNLIST)
  - REQUIREMENTS READIED FOR APPLICATION TO BASE FLIGHT SOFTWARE SYSTEMS USING AUTOMATED PRE-PROCESSOR SYSTEMS
  - PROCESSED REQUIREMENT APPLIED TO BASE FLIGHT SOFTWARE SYSTEMS USING AUTOMATED BUILD AND
  - RECONFIGURED SYSTEM TESTING
    - AUTO SCORERS
    - DETAILED TESTING IN SPF
    - FLIGHT SIMULATIONS IN SPF
  - GENERATION AND QA OF DELIVERABLES (TAPES, DOCUMENTATION, ETC.)
- CURRENTLY PARALLEL RECONFIGURATION IS PERFORMED BY THE STS OPERATIONS CONTRACTOR AND BY IBM (CALLED CERTIFICATION)
NOMINAL (IDEAL) PASS DEVELOPMENT AND RECONFIGURATION ACTIVITY

"OPERATIONAL INCREMENT PLAN/FLT-TO-FLT RECONFIGURATION PLAN"

LEGEND
- NEW CAPABILITIES
- ERROR CORRECTION (REQMTS & CODE)
- MISSION UNIQUE ONLY
- RECONFIGURATION ONLY
" FSW RELEASE

IBM SPACE SHUTTLE PROGRAMS
ACTUAL PASS DEVELOPMENT AND RECONFIGURATION ACTIVITY

LEGEND
- NEW CAPABILITIES
- ERROR CORRECTION (REQMTS & CODE)
- MISSION UNIQUE
- RECONFIGURATION ONLY
- FSW RELEASE

IBM SPACE SHUTTLE PROGRAMS
APPENDIX A

QUALITY/PRODUCTIVITY PROGRAMS
IBM QUALITY AND PRODUCTIVITY IMPROVEMENT PROGRAM

DEFECT CAUSE ANALYSIS AND REMOVAL

- Inspections of Work Products Across the Process
  - Requirements
  - Design
  - Code
  - Test

- Categorization of Defects
  - Data Collection and Retention
  - Analysis

- Defect Trend Studies
  - Escape Error Analysis
  - Process Studies Conducted By Those Involved
IBM QUALITY AND PRODUCTIVITY IMPROVEMENT PROGRAM

DEFECT REMOVAL CYCLE

Input → Work Activity → Output → Measurements

Input → Work Activity → Output → Measurements

Input → Work Activity → Output → Measurements

Test Evaluate Implement

Defect Identification Categorize Set Priorities

Defect Cause Removal

Develop Corrective Action Solution New Objectives

Defect Cause

Defect Cause Analysis Collect Relevant Data Diagnose for Cause
DISCREPANCY ANALYSIS PROCESS

• EVERY DISCREPANCY IS FORMALLY REVIEWED TO DETERMINE WHETHER IT WAS MISSED BY ("ESCAPED") ANY "UPSTREAM" STEP IN THE DEVELOPMENT/VERIFICATION PROCESS
  — EACH AREA CONDUCTS INVESTIGATION FOR EACH OF ITS OWN "ESCAPES"
    • WHY PROBLEM MISSED
      — IF HUMAN ERROR, HOW TO DETECT/CORRECT
      — IF PROCESS ERROR, HOW TO CHANGE PROCESS
    • COULD OTHER OCCURRENCES OF SAME "ESCAPE" EXIST
      — IF SO, DEFINE SCOPE OF EXPOSURE
      — IF SO, DEFINE "AUDIT" TO IDENTIFY OTHER OCCURRENCE
  — QUALITY DATA RECORDED FOR FUTURE REFERENCE (CONFIGURATION MGMT DATA BASE)
    • CHANGE BEING MADE WHEN ERROR INTRODUCED
    • TYPE OF ERROR MADE
    • REASONS MISSED
    • SEVERITY OF ERROR IN FLIGHT IF NOT FIXED
  — DISCREPANCY HISTORY STUDIED FOR TRENDS/PATTERNS/COMMON TYPES

• PROCESS AND PROCEDURES ARE THEN AUGMENTED TO DEFENSE AGAINST FUTURE "ESCAPES" OF KNOWN PROBLEMS (AREA BY AREA)

• RESULTS OF ALL DISCREPANCY OVERSIGHT ANALYSES REVIEWED QUARTERLY WITH CONTRACTOR AND NASA MANAGEMENT
  — DISCREPANCY "ESCAPE/DETECTION" HISTORY PRESENTED (ANALYZED)
IBM OBS QUALITY MEASUREMENT DEFINITIONS

EARLY DETECTION % = \( \frac{\text{NUMBER OF MAJOR INSPECTION ERRORS}}{\text{NUMBER OF MAJOR INSPECTION ERRORS} + \text{VALID DRs}} \times 100 \)

PROCESS ERROR RATE = \( \frac{\text{NUMBER OF VALID DRs DURING DEVELOPMENT CYCLE THROUGH SRR (OR CI*)}}{\text{THOUSAND NEW, CHANGED, OR DELETED SOURCE LINES OF CODE}} \)

PRODUCT ERROR RATE = \( \frac{\text{NUMBER OF VALID DRs POST COMPLETION (SRR OR CI*)}}{\text{THOUSAND NEW, CHANGED, OR DELETED SOURCE LINES OF CODE}} \)

RELEASED PRODUCT ERRORS = \( \text{NUMBER OF VALID DRs AGAINST NEW OR CHANGED CODE WHICH WERE FOUND AFTER RELEASE AND ARE PRECEIVABLE BY USERS (SEV 1-3)} \)
EARLY DETECTION

-- WHAT PERCENT OF ALL ERRORS MADE WERE FOUND AND ELIMINATED BEFORE BEING IMPLEMENTED INTO THE FSW?
PROCESS ERROR RATE

   -- HOW MANY ERRORS WERE MADE IN THE FSW BUT WERE FOUND BEFORE FLIGHT?
PROCESS ERROR RATE

0 1.4 2.8 4.2 5.6 7.0 8.4 9.8 12.6 14.0

ERRORS/KSLOC

0101 0103 0105 0107 0109 0111 0118B

0102 0104 0106 0107C 0110 0118A

ONBOARD FLIGHT SOFTWARE RELEASES

LEGEND
-
ACTUAL
-
GOAL

6/22/87 CMDB
TOTAL CLASS 1 RELEASED PRODUCT ERRORS
AS OF 7/7/87
Not Including 2 New DRs Found Against Pre-013 FSW Since 3/87

Software System Released
F_n Denotes Class 1 DRs in Frontroom for O1n Specified to Left.
TOTAL CLASS 1 RELEASED PRODUCT ERRORS
AS OF 7/7/87
SEVERITY DISTRIBUTION
Not Including 2 New DRs Found Against Pre-O13 FSW Since 3/87

Software System Released
Fn Denotes Class 1 DRs in Frontroom for Oln Specified to Left.
SOFTWARE QUALITY AND PRODUCTIVITY MEASUREMENTS

AUTOMATED SOFTWARE TOOLS AND PROCESS IMPROVEMENTS IN THE RECONFIGURATION PROCESS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4 Flights</td>
<td>5 Flights</td>
<td>10 Flights</td>
<td>15 Flights Planned</td>
</tr>
</tbody>
</table>

- Reconfiguration Data Processors
- Operator Standardization (On-Line, Menu Driven)
- Automated Requirements Generation and Data Collection
- Automated Test and Quality Assurance Systems (Autoscorers)
- Automated System Build and Integration
- Workstation Improvements
SOFTWARE QUALITY AND PRODUCTIVITY MEASUREMENTS

ONBOARD SHUTTLE SOFTWARE RECONFIGURATION
PRODUCTIVITY IMPROVEMENTS

![Bar graph showing improvements in software reconfiguration productivity from 1982 to 1985.]

- Number of Shuttle Missions Per Year
- Elapsed Time to Reconfigure Software in Weeks
- Effort Expended Per Flight In Person Years
SOFTWARE QUALITY AND PRODUCTIVITY MEASUREMENTS

SHUTTLE SOFTWARE RELATIVE QUALITY IMPROVEMENTS

NORMALIZED ERROR RATE

Support (Ground)
Onboard
Reconfigured

70% IMPROVEMENT

1/84  1/85  1/86
SOFTWARE QUALITY AND PRODUCTIVITY MEASUREMENTS

SOFTWARE QUALITY IS AN IBM FSD STRENGTH

<table>
<thead>
<tr>
<th>INTERNAL</th>
<th>CUSTOMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>Code</td>
</tr>
</tbody>
</table>

**Total Inserted Errors**

<table>
<thead>
<tr>
<th>Industry</th>
<th>IBM FSD Houston</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 - 10</td>
<td>9 - 15</td>
</tr>
</tbody>
</table>

**Product Errors**

| 40 - 85  | <1              |
SOFTWARE QUALITY AND PRODUCTIVITY MEASUREMENTS

- Onboard Shuttle Software Quality Measurements Show Significant Improvement
- Onboard Shuttle Software Quality Among Highest in the Industry
- Shuttle Software Reconfiguration Productivity Increased Over 50%
- Onboard Shuttle Software Achievements Result From Commitment to **Zero** Errors
APPENDIX B

SOFTWARE DEVELOPMENT/PRODUCTION FACILITIES
SOFTWARE CRITICAL TO NASA SHUTTLE

SOFTWARE DEVELOPMENT AND PRODUCTION FACILITY

- Mainframe Host Computers, Extensive Direct Access Disk Storage, Shuttle General Purpose Computers And Interfaces Necessary for Testing
- Access Via Terminals for Software Developers and NASA Community
- Software Consists of All Tools Necessary to Develop And Reconfigure the Software
  - Application Tools
  - Shuttle Simulator
  - Flight Software
  - Configuration Management Data Base
- Configuration Management Data Base is the Repository for All Project Control and Descriptive Information
SOFTWARE CRITICAL TO NASA SHUTTLE

ONBOARD SHUTTLE SOFTWARE DEVELOPMENT

Diagram showing the relationship between the Configuration Management Database, Flight Software, Shuttle Simulator, and Application Tools, with interaction between Requirements Analyst, Software Development Programmer, Software Verifier, and Software Build/Integration.
ACRONYMS
### ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCLMAKER</td>
<td>BUILD CONTROL LIST MANAGER</td>
</tr>
<tr>
<td>BFS</td>
<td>BACKUP FLIGHT SYSTEM</td>
</tr>
<tr>
<td>BFSPLP</td>
<td>BFS PAYLOAD PREPROCESSOR</td>
</tr>
<tr>
<td>CCB</td>
<td>CONFIGURATION CONTROL BOARD</td>
</tr>
<tr>
<td>CI</td>
<td>CONFIGURATION INSPECTION</td>
</tr>
<tr>
<td>CIP</td>
<td>CLASS 1 INTEGRATION PLAN</td>
</tr>
<tr>
<td>CITE</td>
<td>CARGO INTEGRATION TEST EQUIPMENT</td>
</tr>
<tr>
<td>CLASS 1</td>
<td>FSW CAPABILITY UPDATE</td>
</tr>
<tr>
<td>CMC</td>
<td>CONFIGURATION MANAGEMENT &amp; CONTROL</td>
</tr>
<tr>
<td>CMDB</td>
<td>CONFIGURATION MANAGEMENT DATA BASE</td>
</tr>
<tr>
<td>CPU</td>
<td>CENTRAL PROCESSING UNIT</td>
</tr>
<tr>
<td>CR</td>
<td>CHANGE REQUEST (Used Interchangeably With SCR)</td>
</tr>
<tr>
<td>CSECT</td>
<td>CONTROL SECTION</td>
</tr>
<tr>
<td>DBA</td>
<td>DATA BASE ADMINISTRATOR</td>
</tr>
<tr>
<td>DCCB</td>
<td>DATA CONFIGURATION CONTROL BOARD</td>
</tr>
<tr>
<td>DCR</td>
<td>DATA CHANGE REQUESTS</td>
</tr>
<tr>
<td>DDRB</td>
<td>DEVELOPMENT DISCREPANCY REVIEW BOARD</td>
</tr>
<tr>
<td>DL OR D/L</td>
<td>DOWNLIST</td>
</tr>
<tr>
<td>DLP</td>
<td>DOWNLIST PREPROCESSOR</td>
</tr>
<tr>
<td>DPSD</td>
<td>DATA PROCESSING SYSTEM DIVISION</td>
</tr>
<tr>
<td>DR</td>
<td>DISCREPANCY REPORT FOR FSW</td>
</tr>
<tr>
<td>DSN</td>
<td>DATA SET NAME</td>
</tr>
<tr>
<td>FACI</td>
<td>FIRST ARTICLE CONFIGURATION INSPECTION</td>
</tr>
<tr>
<td>FCCB</td>
<td>FACILITIES CHANGE CONTROL BOARD</td>
</tr>
<tr>
<td>FEID</td>
<td>FLIGHT EQUIPMENT INTERFACE DEVICE</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>-</td>
</tr>
<tr>
<td>FLP</td>
<td>FLIGHT LOAD \ PREPARATION SYSTEM</td>
</tr>
<tr>
<td>FRR</td>
<td>FLIGHT \ READINESS FIREING</td>
</tr>
<tr>
<td>FSW</td>
<td>FLIGHT SOFTWARE</td>
</tr>
<tr>
<td>GFE</td>
<td>GOVERNMENT FURNISHED EQUIPMENT/INFORMATION</td>
</tr>
<tr>
<td>GMEM</td>
<td>GENERAL MEMORY READ/WRITE \ PROCEDURE</td>
</tr>
<tr>
<td>GTL</td>
<td>GENERIC TRAINING LOAD</td>
</tr>
<tr>
<td>HDW</td>
<td>HARDWARE</td>
</tr>
<tr>
<td>HSM</td>
<td>HIERARCHICAL \ STORAGE \ MANAGEMENT</td>
</tr>
<tr>
<td>IBCB</td>
<td>INTEGRATED BASELINE CONTROL BOARD</td>
</tr>
<tr>
<td>IBM</td>
<td>INTERNATIONAL BUSINESS MACHINES</td>
</tr>
<tr>
<td>IDRBB</td>
<td>INTEGRATED DISCREPANCY REVIEW BOARD</td>
</tr>
<tr>
<td>IDS</td>
<td>ILOAD DATA \ SET</td>
</tr>
<tr>
<td>IL OR I/L</td>
<td>INITIALIZATION LOAD</td>
</tr>
<tr>
<td>IMRB</td>
<td>INTERIM \ MASTER \ RECONFIGURATION BASE</td>
</tr>
<tr>
<td>IMS</td>
<td>INFORMATION \ MANAGEMENT \ SYSTEM</td>
</tr>
<tr>
<td>JES</td>
<td>JOB ENTRY SUBSYSTEM</td>
</tr>
<tr>
<td>JSC</td>
<td>JOHNSON \ SPACE \ CENTER</td>
</tr>
<tr>
<td>KSC</td>
<td>KENNEDY \ SPACE \ CENTER</td>
</tr>
<tr>
<td>L6</td>
<td>LEVEL 6 DETAIL FUNCTIONAL TESTING</td>
</tr>
<tr>
<td>L7</td>
<td>LEVEL 7 \ CAPABILITIES \ PERFORMANCE TESTING</td>
</tr>
<tr>
<td>L8</td>
<td>LEVEL 8 \ RECONFIGURATION \ PERFORMANCE TEST</td>
</tr>
<tr>
<td>MAST</td>
<td>MEASUREMENT \ AND \ STIMULUS \ DATA \ BASE</td>
</tr>
<tr>
<td>MCC</td>
<td>MISSION CONTROL CENTER</td>
</tr>
<tr>
<td>MDBINIT</td>
<td>MEMBER DATABASE INITIALIZATION</td>
</tr>
<tr>
<td>MIP</td>
<td>MASS MEMORY \ INTEGRATION PLAN</td>
</tr>
<tr>
<td>MM</td>
<td>MASS MEMORY</td>
</tr>
<tr>
<td>MMI</td>
<td>MASS MEMORY \ IMAGE</td>
</tr>
</tbody>
</table>

A-3
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMU</td>
<td>MASS MEMORY UNIT</td>
</tr>
<tr>
<td>MOCRB</td>
<td>MISSION OPERATIONS CHANGE REVIEW BOARD</td>
</tr>
<tr>
<td>MOD</td>
<td>MISSION OPERATIONS DIRECTORATE</td>
</tr>
<tr>
<td>MODRB</td>
<td>MISSION OPERATIONS DISCREPANCY REVIEW BOARD</td>
</tr>
<tr>
<td>MRAS</td>
<td>MAINTENANCE RELEASE AUTHORIZATION</td>
</tr>
<tr>
<td>MRB</td>
<td>MASTER RECONFIGURATION BASE</td>
</tr>
<tr>
<td>MSFC</td>
<td>MARSHALL SPACE FLIGHT CENTER</td>
</tr>
<tr>
<td>MVS</td>
<td>MULTIPLE VIRTUAL STORAGE</td>
</tr>
<tr>
<td>OASCB</td>
<td>ORBITER AVIONICS SOFTWARE CONTROL BOARD</td>
</tr>
<tr>
<td>OI</td>
<td>OPERATIONAL INCREMENT (BASE FSW SYSTEM)</td>
</tr>
<tr>
<td>ORG</td>
<td>ORGANIZATION</td>
</tr>
<tr>
<td>OSDR</td>
<td>OPERATION SHUTTLE DATA RECONFIGURATION</td>
</tr>
<tr>
<td>PASS</td>
<td>PRIMARY AVIONICS SOFTWARE SUBSYSTEM</td>
</tr>
<tr>
<td>PCO</td>
<td>PATCH CUT-OFF</td>
</tr>
<tr>
<td>PCR</td>
<td>PROGRAM CHANGE REQUEST</td>
</tr>
<tr>
<td>PRCB</td>
<td>PROGRAM REQUIREMENTS CONTROL BOARD</td>
</tr>
<tr>
<td>PRN</td>
<td>PROGRAM RELEASE NOTICE</td>
</tr>
<tr>
<td>PSCR</td>
<td>PRODUCTION SOFTWARE CHANGE REQUEST</td>
</tr>
<tr>
<td>PSDR</td>
<td>PRODUCTION SOFTWARE DISCREPANCY REPORT</td>
</tr>
<tr>
<td>PSF</td>
<td>PARAMETER SPECIFICATION FILE</td>
</tr>
<tr>
<td>R &amp; E</td>
<td>RESEARCH AND ENGINEERING</td>
</tr>
<tr>
<td>RASS</td>
<td>RELEASE AUTHORIZATION SIGNATURE SHEET</td>
</tr>
<tr>
<td>RCV</td>
<td>RECEIVING</td>
</tr>
<tr>
<td>RECON</td>
<td>RECONFIGURATION (FLIGHT-TO-FLIGHT)</td>
</tr>
<tr>
<td>RELAUTH</td>
<td>RELEASE AUTHORIZATION</td>
</tr>
<tr>
<td>RI/D</td>
<td>ROCKWELL INTERNATIONAL/DOWNEY</td>
</tr>
<tr>
<td>RM</td>
<td>ROOM (AS IN FRONTRoom OR BACKROOM)</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>RSD</td>
<td>RECONFIGURATION SYSTEMS DEVELOPMENT</td>
</tr>
<tr>
<td>RSOC</td>
<td>ROCKWELL SHUTTLE OPERATION COMPANY</td>
</tr>
<tr>
<td>RT &amp; O</td>
<td>RECON TEST &amp; OPERATIONS CONTROL BOARD</td>
</tr>
<tr>
<td>SAS</td>
<td>SOFTWARE APPROVAL SHEET</td>
</tr>
<tr>
<td>SCCB</td>
<td>SOFTWARE CONFIGURATION CONTROL BOARD</td>
</tr>
<tr>
<td>SCR</td>
<td>SOFTWARE (CAPABILITY) CHANGE REQUEST</td>
</tr>
<tr>
<td>SDF</td>
<td>SOFTWARE DEVELOPMENT FACILITY</td>
</tr>
</tbody>
</table>
| SM      | 1. SYSTEM MANAGEMENT AS IN "SIM: FSW:"
|         | 2. SUBMIT TRANSACTION AS IN "SUBMIT TOOL: ELEMENT VIA SM TRANSACTIONS: SIM:"
| SMP     | SYSTEMS MANAGEMENT PREPROCESSOR |
| SPF     | SOFTWARE PRODUCTION FACILITY |
| SPIF    | SHUTTLE PAYLOAD INTEGRATION FACILITY |
| SPT     | SUPPORT |
| SRC     | SOURCE |
| SRR     | SOFTWARE READINESS REVIEW |
| SSD     | SPACECRAFT SOFTWARE DIVISION |
| SSDR    | SUPPORT SOFTWARE DISCREPANCY REPORT |
| STAR    | SPACE TRANSPORTATION AUTOMATED RECONFIGURATION |
| STS     | SPACE TRANSPORTATION SYSTEM |
| STSOC   | SPACE TRANSPORTATION SYSTEM OPERATIONS CONTRACT |
| SW OR SW| SOFTWARE |
| SYNVAT  | SYSTEM NAME VALIDATION TABLES FOR SMDB |
| T & O   | TEST & OPERATIONS |
| TCT     | TEST COORDINATION TEAM |
| TR      | TRANSMITTAL RELEASE |
| UAT     | USER ACCEPTANCE TEST |
ACRONYMS

UPF: UNIVERSAL PATCH FORMAT
VCS: VEHICLE/CARGO SYSTEMS
VLS: VAN DENBERG LAUNCH SITE
APPENDIX D
EXTERNAL EVALUATIONS OF IBM PROCESS
EXTERNAL EVALUATIONS OF IBM PROCESS

- NASA EXCELLENCE AWARD FOR QUALITY AND PRODUCTIVITY RECIPIENT
  1986
  IBM Federal Systems Division
  Houston, Texas

- "To summarize then, the computer software checking system and attitude is of highest quality."

  Dr. Richard Feynman
  Report of the Presidential Commission on the Space Shuttle Challenger Accident