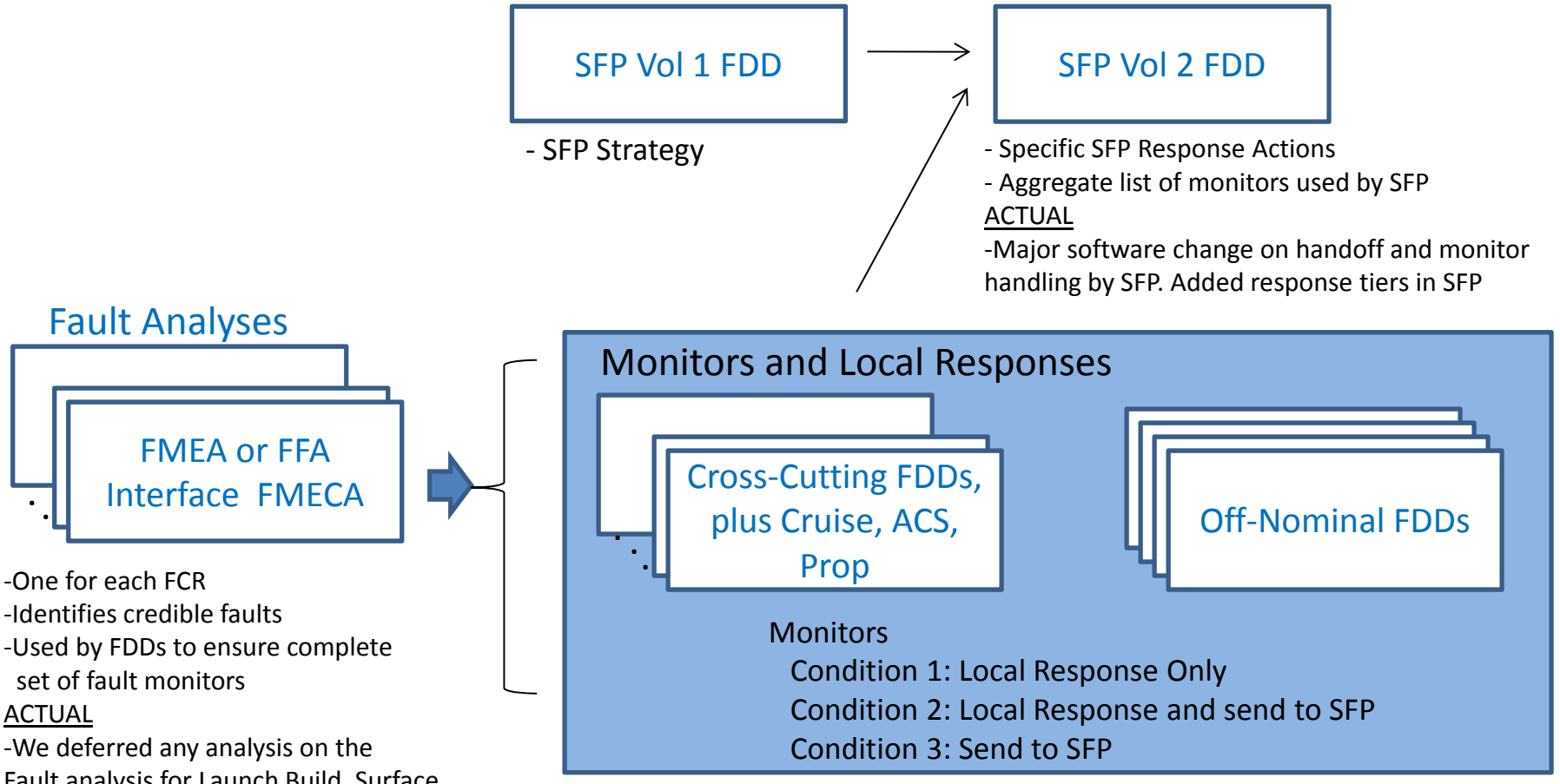
Strategies for Independent V&V of the MSL Fault Protection Software

Shirley Savarino, TASC
Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology
NASA IV&V Workshop
September 11-13, 2012

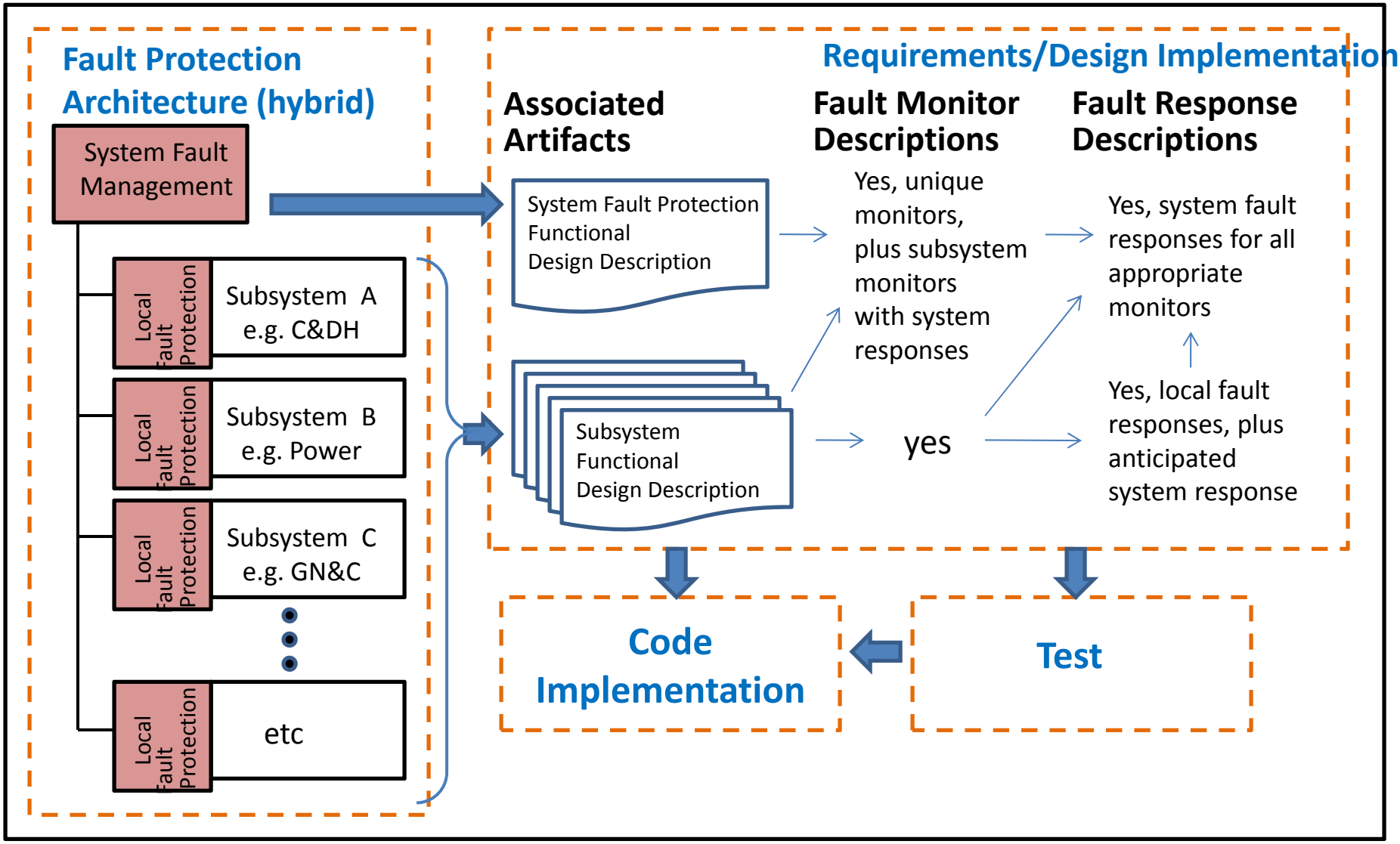
MSL FP/SFP Strategy (Idealized and Actual)



MSL Fault Protection – Context

- The MSL FP strategy utilizes a two tier approach: local fault protection and system fault protection (SFP)
  - Local fault protection isn't very sophisticated, but 1st tier of defense
  - SFP is fed fault monitors from various parts of the system. All monitors generated locally
  - Based on what monitors are triggered, SFP will take appropriate action
- All FP Documentation goes through the standard validation (completed)
  - New SFP monitor handling and response approach requires IV&V regression (Jan 11)
- Due to the distributed nature and lack of consistency in documentation, IV&V decided to apply monitor mining techniques to arrive at a FP architecture baseline
  - This baseline became the basis for our code and fault analysis IV&V work

Hybrid Fault Protection Architecture Implementation Approach

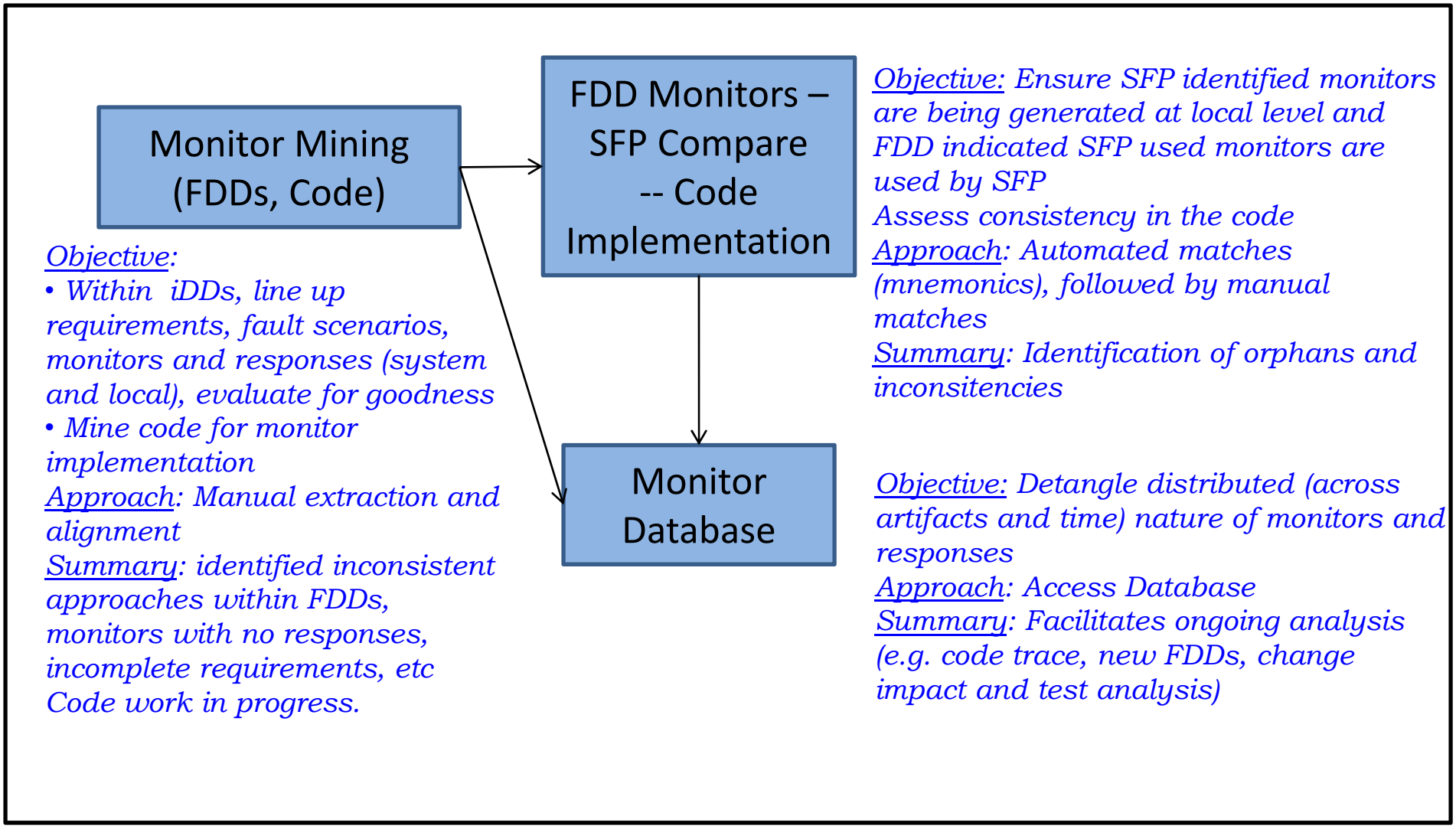


IV&V “Monitor Mining”

Objectives:

- Ensure that each monitor description in an FDD has a requirement and associated fault scenario
- Ensure that each monitor had associated local and/or anticipated system responses described
- Ensure consistency of the monitor requirement, fault scenario and response description
- Ensure that system fault protection identified monitors existed in subsystem FDD descriptions, and vice versa
- Ensure that monitors are implemented in the code
- Ensure consistency of the monitor and associated response implementations between requirements, design and code
- Provide a basis for the IV&V verification analysis

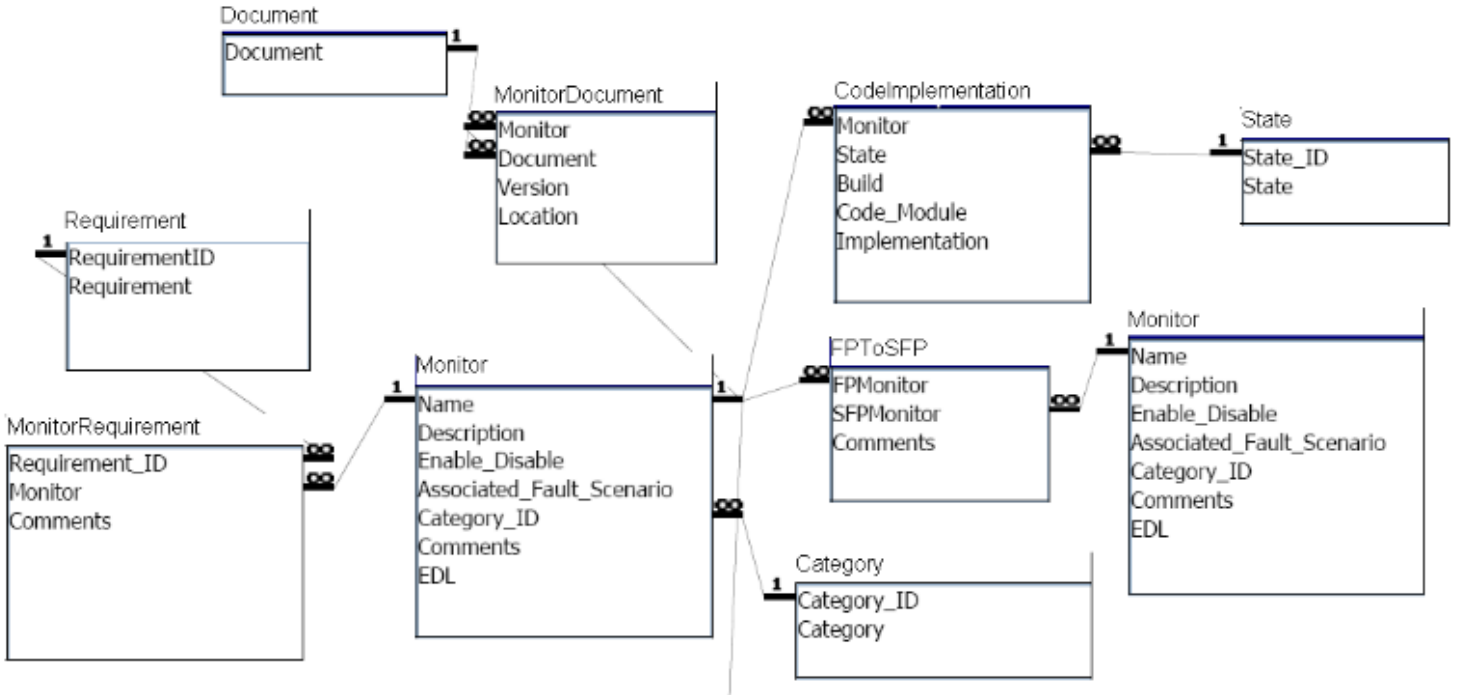
IV&V Monitor Mining Tasks - Approaches



IV&V Monitor Mining Process, Results

Category	Description
IV&V Monitor Mining Work Instructions	• Search the entire FDD for keywords - fault, monitor, response • Review diagrams for fault monitors and responses • Document fault monitors and applicable information • Document fault management requirements with no monitor
IV&V Monitor Mining Result Types	• Missing fault management requirements and/or responses • Incomplete requirements in describing fault scenarios • Requirements with no fault monitor/response • Unclear response descriptions - local or system response • Occasionally, pre-existing requirement map to fault monitor is incorrect
Observations resulting from the IV&V Monitor Mining	• Lexicon: SFP FDD and code uses mnemonics, but subsystem FDDs do not in any consistent fashion. In some cases, monitors are not explicitly named (though fault conditions and responses are provided) – Lack of a consistent lexicon across documentation meant that judgment needed to be applied as to 1) whether a response was truly a fault response or just defensive programming, and 2) uncertainty in the results (though we reviewed and reviewed our work to reduce errors to extent possible) • Different approaches to FP were applied across the FDDs. Faults and associated response descriptions varied across the project. The tables and spreadsheets had the most logical presentations. In some cases faults were only provided in PDF pictures. In other cases, we inferred faults due to telemetry provided

Monitor Mining Database Entity Relationship Diagram



<u>Entity Relationship Diagram (ERD)</u>

-Boxes are tables in the dbase

-Lines are relationships

- infinity indicates many
- 1 indicates 1
- -Many to many come from concatenations

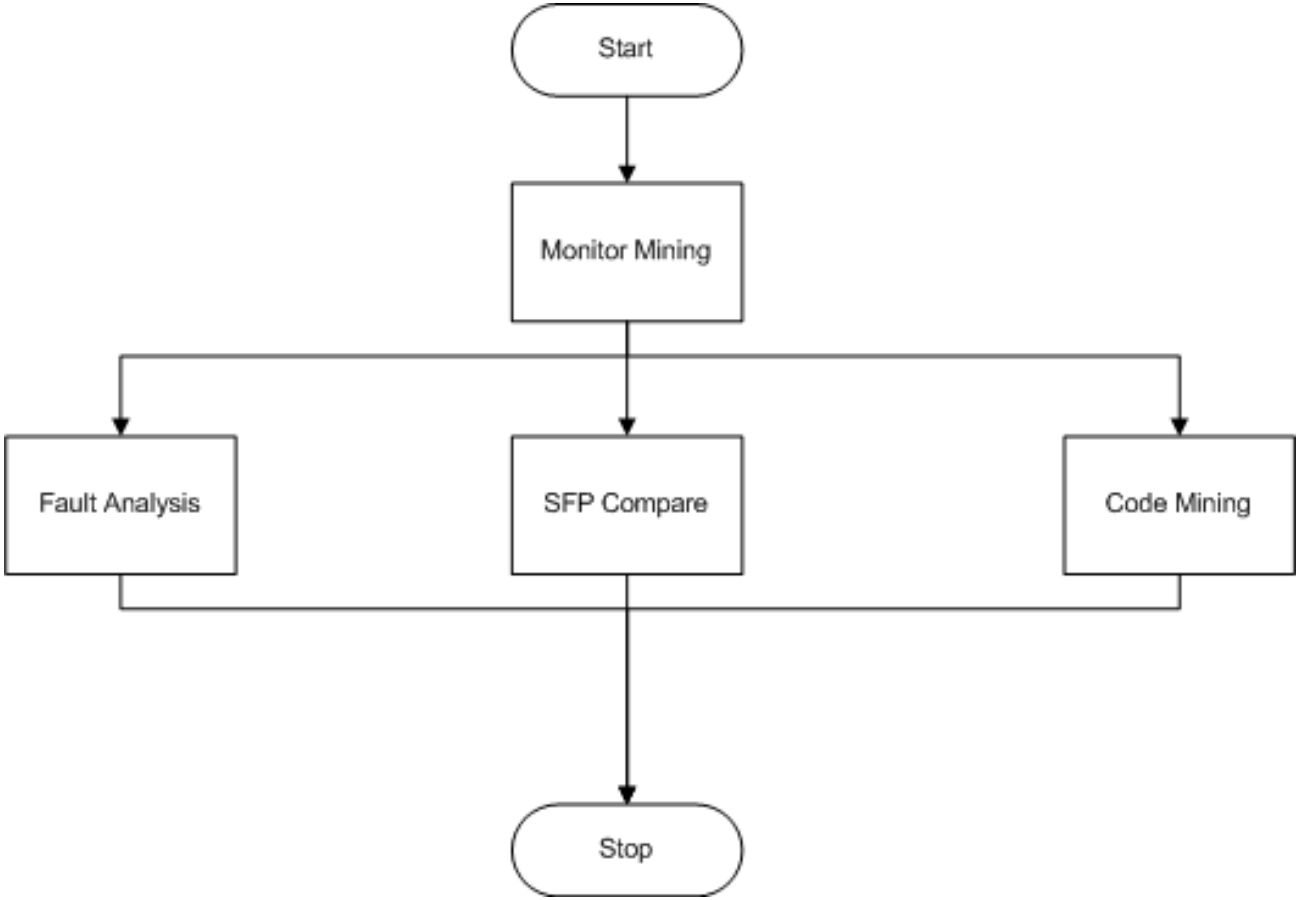
-Monitor Table is the center of the database

-Dbase differentiates SFP required vs. FDD generated monitors but it is all in the same table

Monitor Mining Database Benefits

Description	Benefit
Consistency	• Database structure ensures capturing data in a consistent manner
Queries	• Rather than using Excel sorts and filters, database queries can be employed, with results provided in a report
Reports, Input Forms	• Reports capture data in any manner desired • Different reports/input forms can be employed by different analysts as long as the same data is captured
Agility and speed of manipulating data	• Greatly improved over spreadsheet approach - this was perhaps the most important and quickly realized benefit once the monitor mining database was operational • Database allows IV&V to capture analysis and provide reports of remaining efforts. • During analysis, identification of exceptions (issues) are facilitated by database queries • Database enables IV&V to focus on the analysis tasks vs. the data manipulation efforts

IV&V Fault Protection Analysis



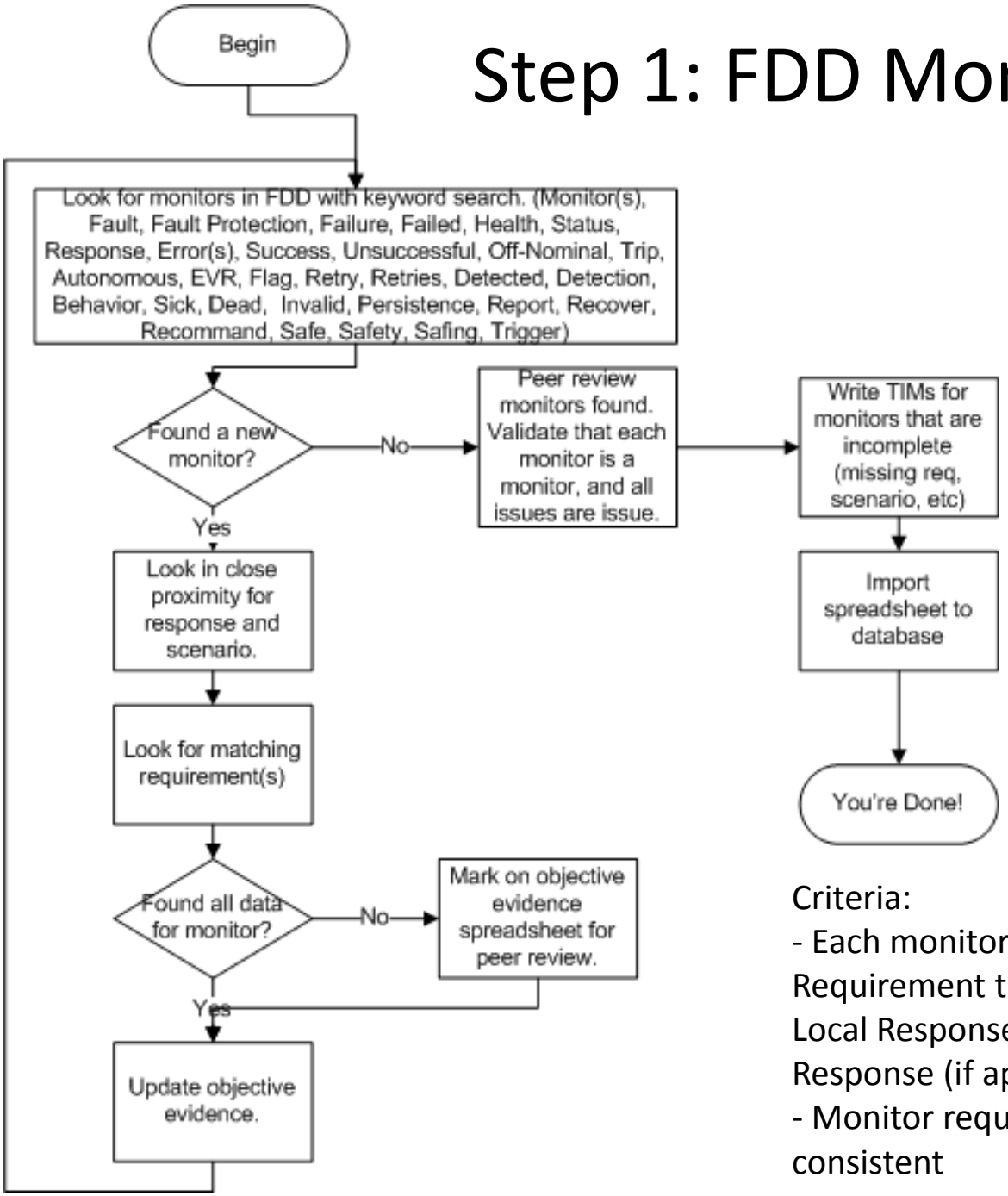
Step 1: Perform Monitor Mining to attain a FP baseline
Must be performed first

Steps 2, 3, 4: Ensure

a) Monitors have underlying fault analysis
b) Handoffs to SFP occur correctly
c) Implementation in code is correct

Can be performed in parallel

Step 1: FDD Monitor Mining



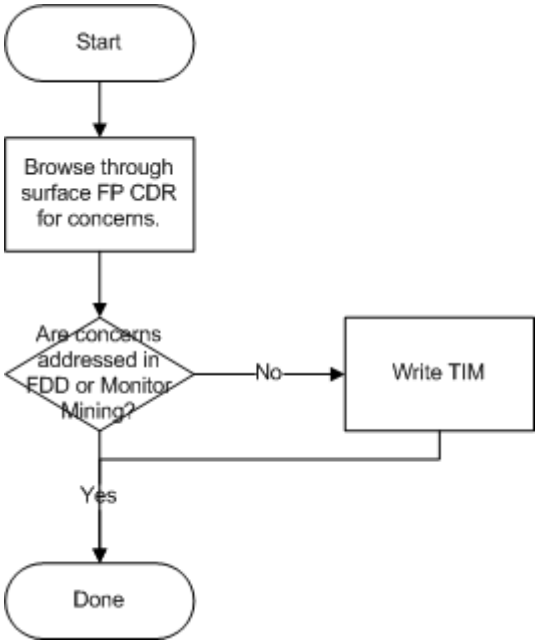
Criteria:

- Each monitor needs to have an associated Requirement that includes Fault Scenario, Local Response (if applicable) and System Response (if applicable)
- Monitor requirement and design must be consistent

Monitor Mining Best Practices, Lessons Learned

- Monitor mining was the trickiest part – this defined the baseline for the rest of the analysis
  - We heard that the FP domain lead kept a copy of the IVV monitor list with her since we had integrated the architecture
  - MSL project didn't use consistent lexicon or organization – announce vs. declare fault .. No mneumonics .. Ancillary worksheets, commands, separate sections, pdf pictures
- The good
  - The monitor mining required a detailed eye. Analysts were selected with this skill.
  - Having a good understanding of the fault protection architecture enabled us to correctly set this analysis up – we asked the project if they had a single list of all the monitors and they acknowledged this weakness (due to distributed nature of FP implementation)
  - Peer reviews were essential to gain understanding of the fault protection schema. A strong systems engineer in the peer review was beneficial
- Lessons Learned
  - We tried to use different reviewers ← this ended up being inefficient and ultimately we had to redo the reviews with the same people
  - We ended up having to do this a couple times on the launch monitors – in the end, it might have been useful to run the fault protection monitors with subsystem owners to make sure we got it right
  - Reuse of fault protection is tricky since it is a system activity. MSL used MER FP for cruise and had criticality of cruise been higher, we would have done a separate task here.

Step 2: Fault Analysis



Criteria:
-The subsystem fault analysis needs to be consistent with the FP monitors and associated responses described in FDDs and implemented in code

Methods
-Two way trace between monitors and CDR charts

Thoughts
-Skill set requires sufficient SE skills to understand the Fault analysis and correlation to FDD. This is to filter false positives when discrepancies identified

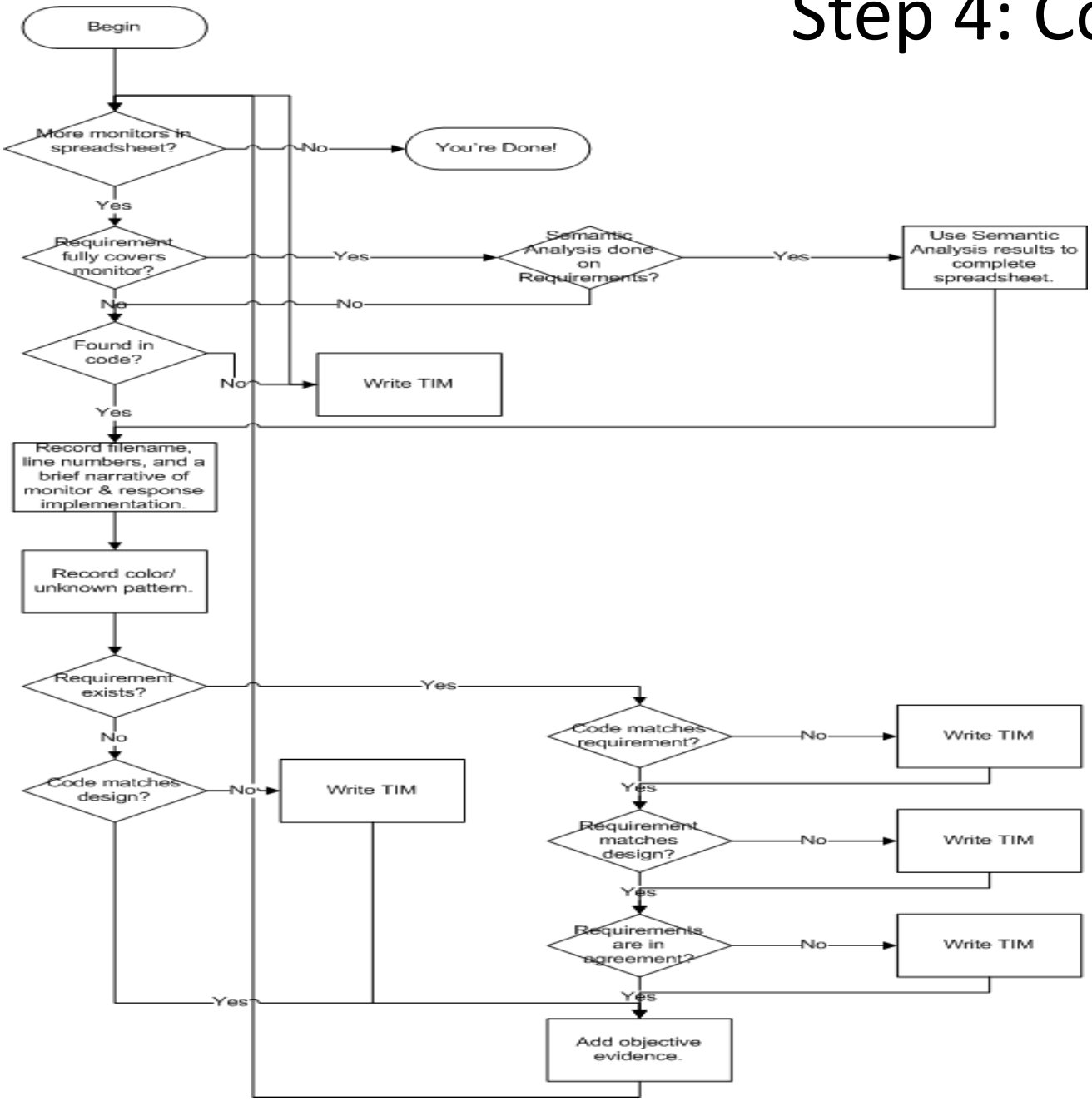
Step 3: Monitor Compare with SFP– Engineering Approach

- Work Instructions
  1. Extract monitors from IV&V monitor mining that were conditions 2 or 3 (send to SFP)
  2. Compare to SFP Annex which showed monitors expected for SFP operation
  3. Criteria: handoff must occur – looked for orphans on both sides. If subsystem FDD had anticipated SFP response (vs. SFP handoff only) ensured that response was correct
  4. Peer Review and Write TIMs
- Analysis Facilitation
  - Wrote a script to extract full compares of monitors (required mnemonic) – only 4 exact matches
  - SFP used Mnemonics, FDDs often didn't. SFP used specific cases of monitors, FDDs often used general cases (resulting in many to one relationships)
  - Manual matches became difficult because of narrative nature of the monitor descriptions, we didn't want to inadvertently pass something.
  - Spreadsheet was "messy"

SFP Compares: Best Practices and Lessons Learned

- In general, we've received feedback that IVV analysis associated with interactions between subsystems yields high value – biggest concern from SFP folks was that they might have missed an intended fault requiring a system response
- Best practice
  - SFP FDDs had lists of monitor names using mnemonics with system fault responses. That facilitated our analysis greatly and we liked this
  - We did about 4 iterations of this analysis until everything lined up – results written up in group TIMs
  - Automation and database facilitated analysis – matches between same monitor instantiated as "local monitor" in FDD and "system monitor" in SFP vol2
- Lessons Learned
  - One-many matches (e.g. thermal too-hot zones was a single monitor in Thermal FDD but had dozens of counterparts in system FP). Subsystem FDDs often didn't have mneumonics to match

Step 4: Code Analysis



Criteria:
-Code should match requirement, if it exists.

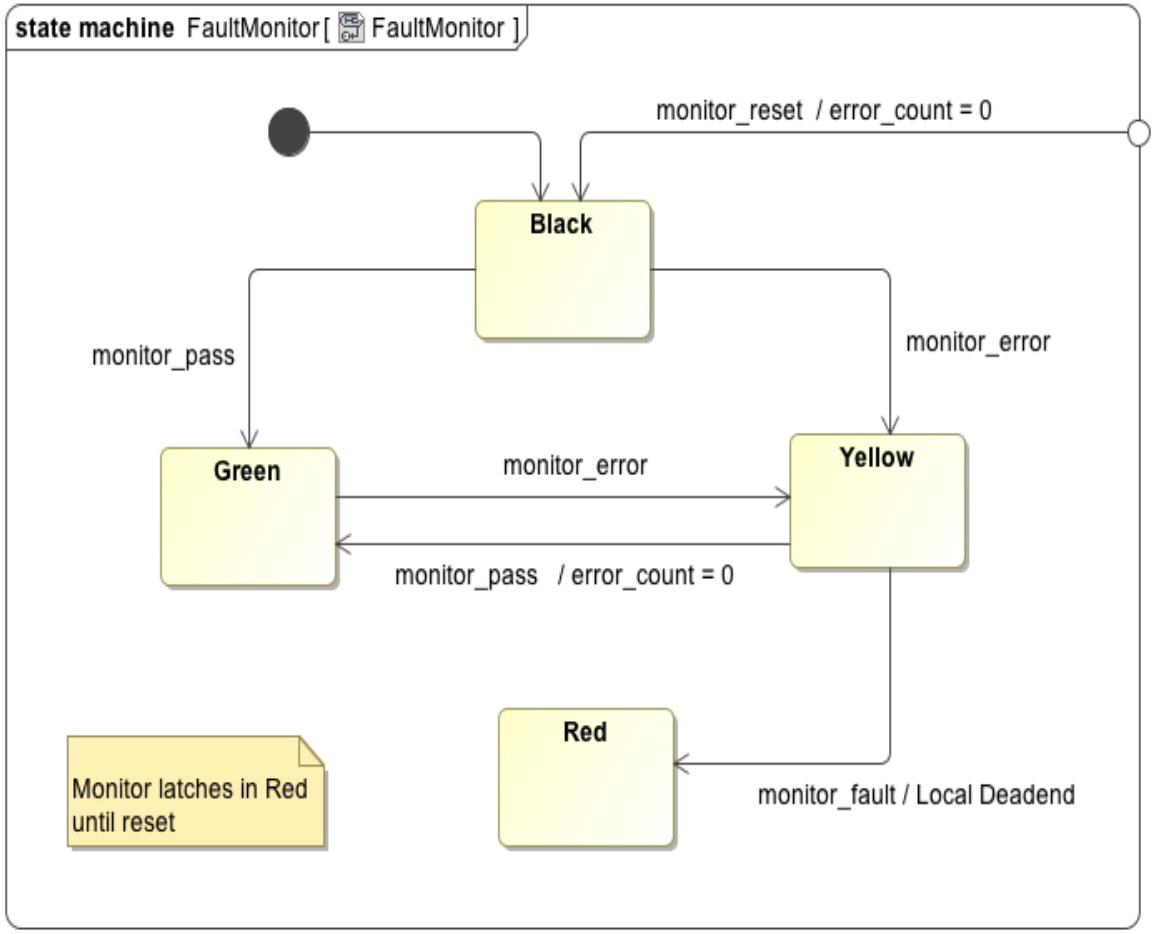
- Requirements should match design.

- Requirements should agree. (often monitor had multiple associated requirements)

- If there's no requirement, code must match design.

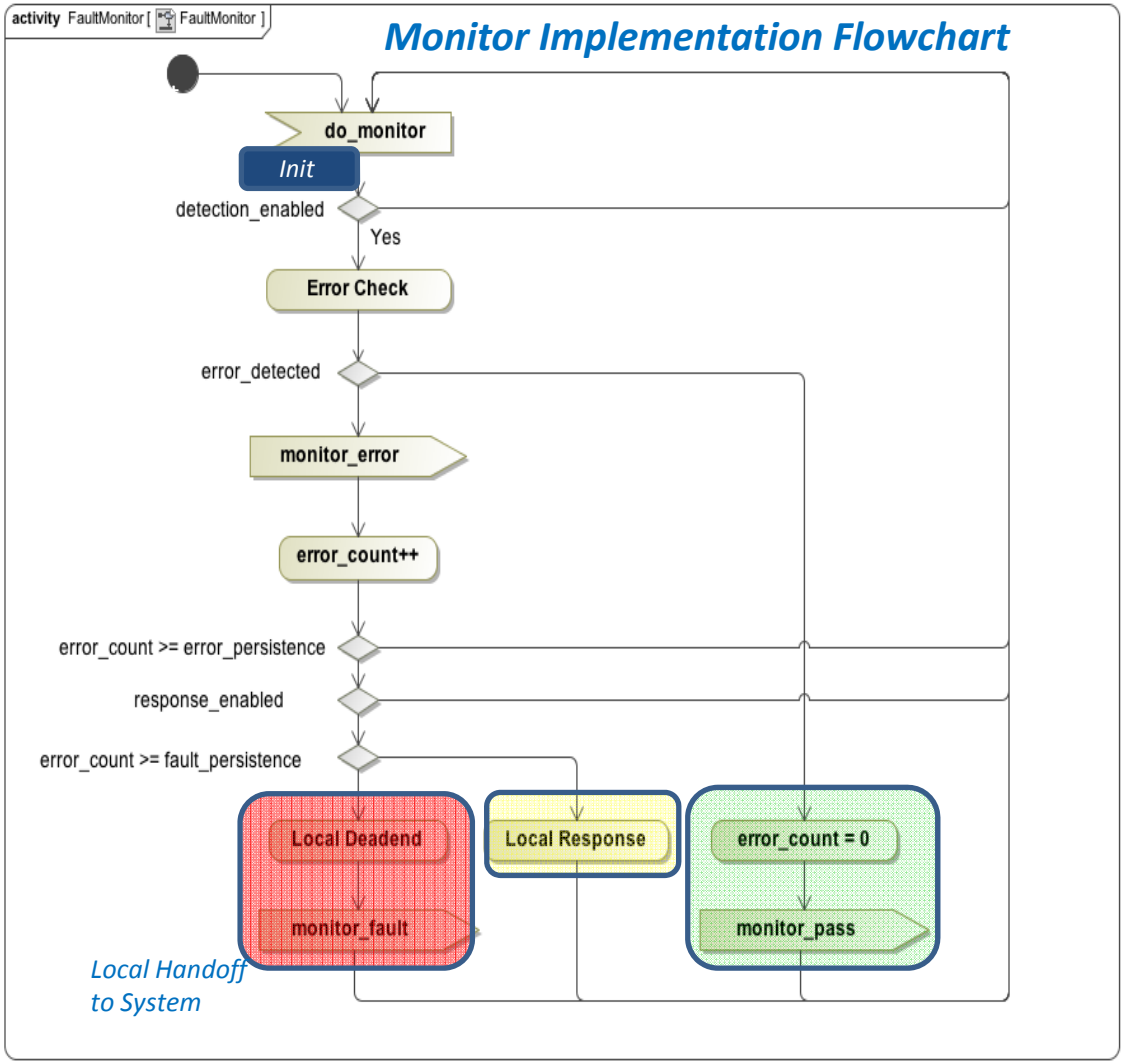
MSL Monitor Pattern

- In Oct 2010, MSL project updated their SFP handoff from a "push" (function call) to a "pull" (polling) strategy. The code needed to be retroactively updated (~1200 monitors)
- All monitor code is supposed to implement the color pattern shown on the right
  - Black – initial state
  - Yellow – error persistence exceeded
  - Red – fault persistence exceeded
  - Green – nominal
- Along with monitor colors, a standard code pattern was implemented

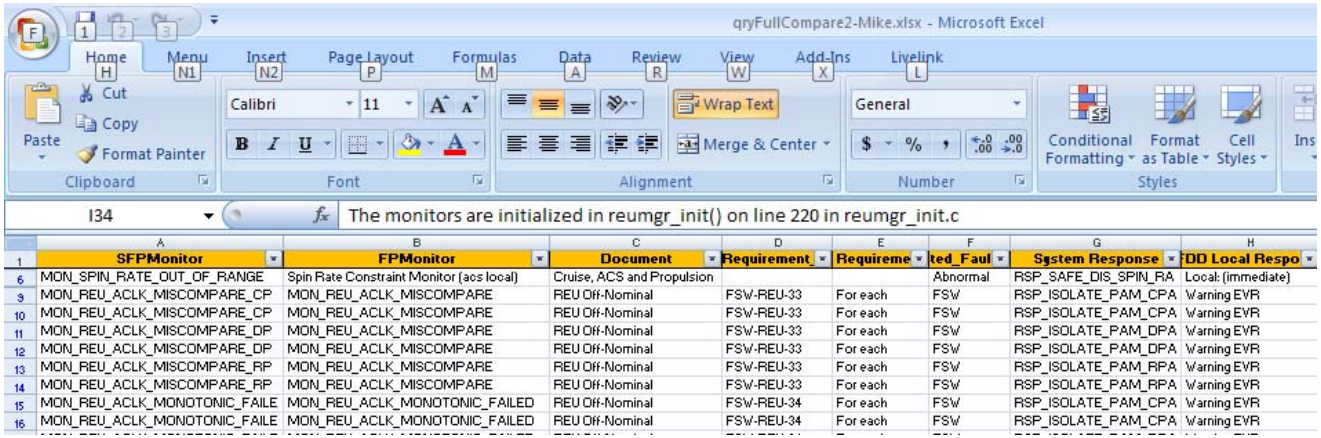


Fault Monitor Code Analysis Overview

- Used monitor mining and MSL code pattern (on right) as a basis for our code analysis.
- Compared code to requirements, design and implementation of code pattern
  - "monitor-centric" analysis (reqts + design), vs. reqt only
  - Used IV&V Monitor Database
- Grabbed additional metadata location that wasn't always available in the requirements/design
  - Enables
  - Persistence



Code Analysis Worksheets (p1 of 2)

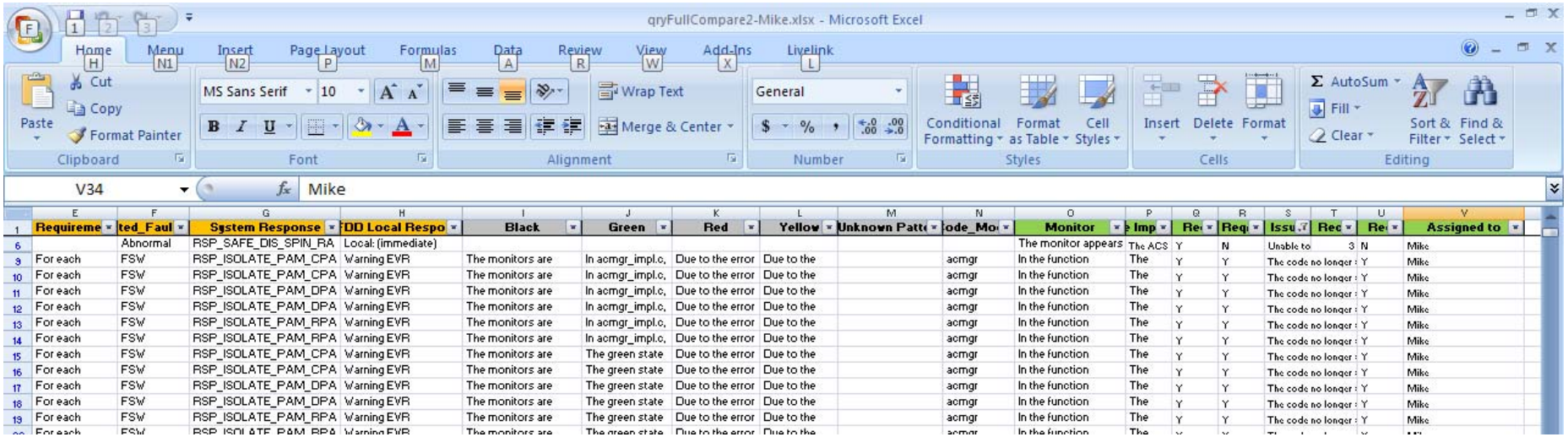


	A	B	C	D	E	F	G	H
1	SFPMonitor	FPMonitor	Document	Requirement_	Requireme	ted_Faul	System Response	DD Local Respo
6	MON_SPIN_RATE_OUT_OF_RANGE	Spin Rate Constraint Monitor (acs local)	Cruise, ACS and Propulsion			Abnormal	RSP_SAFE_DIS_SPIN_RA	Local: (immediate)
9	MON_REU_ACLK_MISCOMPARE_CP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_CPA	Warning EVR
10	MON_REU_ACLK_MISCOMPARE_CP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_CPA	Warning EVR
11	MON_REU_ACLK_MISCOMPARE_DP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_DPA	Warning EVR
12	MON_REU_ACLK_MISCOMPARE_DP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_DPA	Warning EVR
13	MON_REU_ACLK_MISCOMPARE_RP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_RPA	Warning EVR
14	MON_REU_ACLK_MISCOMPARE_RP	MON_REU_ACLK_MISCOMPARE	REU Off-Nominal	FSW-REU-33	For each	FSW	RSP_ISOLATE_PAM_RPA	Warning EVR
15	MON_REU_ACLK_MONOTONIC_FAILE	MON_REU_ACLK_MONOTONIC_FAILED	REU Off-Nominal	FSW-REU-34	For each	FSW	RSP_ISOLATE_PAM_CPA	Warning EVR
16	MON_REU_ACLK_MONOTONIC_FAILE	MON_REU_ACLK_MONOTONIC_FAILED	REU Off-Nominal	FSW-REU-34	For each	FSW	RSP_ISOLATE_PAM_CPA	Warning EVR

Associated Monitor Mining Data

- Monitor name from SFP FDD
- Monitor name from Subsystem FDD
- Which subsystem FDD
- Requirement ID and text
- Fault Scenario
- System Response
- Local Response

Code Mining Tracking Sheet part 2 of 2



Associated code color patterns captured during code analysis

IV&V Assessment Fields

Monitor Implementation	Response Implementation	Req consistent with each other? (TIM)	Req/Design consistent with code? (TIM)	Issue description (TIM)	Recommended Severity (TIM)	Req fully verified? (Y/N/Partial) (Randall)	Assigned to

Code Analysis Challenges, Best Practices

- System Response: Look for color pattern first
  - Great for finding everything about monitor.
  - If there's no pattern, use similar keywords as monitor mining, or monitor name if applicable (e.g. fault, monitor, trip, announce)
- Local Responses harder to find, since the pattern wasn't required for implementation.
  - We used EVRs to identify potential faults
- Does a local deadend qualify as a local response? ← we never quite converged and just called it orange in the end ☺

Other FP design/code analysis tasks performed by MSL IV&V team

- Understand SFP Fault Protection engine and trace to code
- Monitor response collisions – system to system; system to local and local to local
  - Make sure that if you were doing one response, that another one didn't come in and mess the system up
- System response implementation in code
- "Fatal" EVRs
- EDL Second Chance

Monitor Database – Pulling it all together

- Objective: Detangle distributed nature of monitors and responses – project and IV&V activities (to date and anticipated). Additions to IV&V analysis will be easier in database

- Approach: Access Database, with philosophy to "Keep it Simple". Database tables include
  - FP Monitor
  - Requirements
  - FDD
  - SFP FDD
  - Monitor Category
  - Code Implementation

- Database Facilitation
  - With many to many relationships, it was useful to incrementally dump data from each of the spreadsheets to refine actual organization
  - Needed queries straightforward since we had been using mining data frequently

- Database successfully used in launch build fault protection analysis. Portions of the dbase migrating to the SQL dbase for MSL surface analysis

Monitor Mining Database Benefits

Description	Benefit
Consistency	• Database structure ensures capturing data in a consistent manner
Queries	• Rather than using Excel sorts and filters, database queries can be employed, with results provided in a report
Reports, Input Forms	• Reports capture data in any manner desired • Different reports/input forms can be employed by different analysts as long as the same data is captured
Agility and speed of manipulating data	• Greatly improved over spreadsheet approach - this was perhaps the most important and quickly realized benefit once the monitor mining database was operational • Database allows IV&V to capture analysis and provide reports of remaining efforts. • During analysis, identification of exceptions (issues) are facilitated by database queries • Database enables IV&V to focus on the analysis tasks vs. the data manipulation efforts