Fishbone Status

- The fishbone analysis has been an effective tool used to focus the attention of the team on the most likely causes
- Two major branches have been designated as not credible causes
  - Held two telecons with Fred Huegel to discuss potential hardware causes and how they could be eliminated
    - Included hardware component failures and environmentally induced failures
  - The result of these meetings was that the best description for these two classes of failures was “not credible”
    - As examples, these categories would require parallel failures in 5 boxes, would require marginal performance that was not affected by the environmental test sequence, or would require some other condition that was considered not credible
- The abbreviated fishbone charts attached present the possible and unlikely items, with non credible items removed.

Abbreviated Fishbone

Cause	Discussion/Rationale	Status
1. Hardware failure induces reboot	Identical pre-existing, intermittent or environmentally induced failure of isolated part or board in 5 independent processors is not a credible cause for reboots	Not Credible
2. Software induced reboot		Possible
2.1. Operating system flaw		
2.1.1. Priority inversion	Code has been designed to avoid this issue	Unlikely
2.1.2.OS does not provide memory protection	Code analysis performed to eliminate potential memory overwrite errors, but see 2.2.1	Very Unlikely
2.2. Application software bug		Possible
2.2.1. Memory overwrite		Very Unlikely.
2.2.1.1. Generic overwrite	Potential for overwrite documented in FSW-823, FSW-831. Static code analysis tools utilized by IVV to check for unprotected memory writes. Issues found in JIRAs xxx, xxx and resolved.	Very Unlikely.
2.2.2. Interrupt locks	Code has been designed to avoid this issue	Unlikely
2.2.3. Task exception	Could not cause watchdog timeouts, since the CPU takes an exception first. Task exceptions are handled in the exception vector. System designed to collect information on the task that attempted to execute illegally. This data is captured preserved. These resets, when they occur are captured and provide good insight into what's happened.	Possible
2.2.4.Race Conditions	Where race conditions are a potential, system designed to sequence events thru use of semaphores	Unlikely

Abbreviated Fishbone (Continued)

Cause	Discussion/Rationale	Status
3. Operations/environment	Not a credible cause – environmental testing was successfully completed with no change to reboot rate during any environment	Not Credible
4. LAT software interacts with computer firmware/operating system feature		Possible
4.1. Feature documented in vendor errata sheets	General note: examined errata from vendor, including newly disclosed features.	Unlikely.
4.1.1. Errata 15	LAT is susceptible, documented in FSW-820, FSW-821. Recommended work-around implemented in Build 0.8.x, so now considered unlikely. Will not rule out yet.	Unlikely.
4.1.2. Errata 24	LAT is susceptible, documented in FSW-822, FSW-824. Recommended work-around implemented in Build 0.8.x, so now considered unlikely. Will not rule out yet.	Unlikely.
4.2. Undocumented and previously unknown errata		Possible
5. EPU/SIU hardware design flaw		Possible
5.1. LCB FPGA error		Possible
5.1.1. LCB incorrectly writes memory	Writes to random areas in memory could cause an exception reboot, but very unlikely to cause a watchdog timer reboot since corrupted memory would be more likely to cause computation errors or exceptions rather than causing a process to hang.	Possible