NASA’s Software Architecture Review Board’s (SARB) Findings from the Review of GSFC’s “core Flight Executive/Core Flight Software” (cFE/CFS)

Lorraine Fesq and Dan Dvorak
Jet Propulsion Laboratory, California Institute of Technology
NASA Software Architecture Review Board

Flight Software Workshop
November 7-9, 2012
Southwest Research Institute
San Antonio, Texas

Copyright 2012 California Institute of Technology. Government sponsorship acknowledged. The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
Background

Software Architecture Review Board

- SARB established in 2009 based on recommendation from FSW Complexity study to Office of Chief Engineer
- Funded as a NESC technical discipline team by Michael Aguilar
- Several reviews conducted, varying in duration and depth
- SARB Reviewed GSFC’s cFE/CFS in October 2011
  - Reviewers: Michael Aguilar (NESC, NASA Software Tech Fellow), Dan Dvorak (JPL, SARB Lead), Lorraine Fesq (JPL, review chair), Robyn Lutz (Iowa State University) – Product Line expert, Michael Madden (LaRC), Pedro Martinez (JSC), Alex Murray (JPL), John Weir (MSFC), Steve Williams (APL)
SARB’s website is a sub-Community of the Software Engineering Community of Practice

https://nen.nasa.gov/web/software/sarb
cFE/CFS Background

- Developed by GSFC Flight Software Systems Branch in response to growing costs and schedule for SW development due to increasing system complexity
- Project-independent FSW provides run-time environment and services for hosting applications
- Targeted for Class B FSW for Robotic s/c and instruments
- Domain: C&DH, GN&C, thermal, power, instrument control
- Users: ARC/LADEE, JSC/Morpheus, APL/RBSP
“Lollipop” Diagram shows cFE core applications and software bus (green), plus CFS applications that plug into the bus (blue and purple).
Review Objectives & Focus

- **Objectives:**
  - Help project identify architectural issues that may have been overlooked
  - Recommend actions to minimize downstream problems

- **Focus on software architecture**
  - not detailed design, not code, not avionics

- **Engineering peer review**
  - Tabletop review style, not primarily presentations to board

- **Report:**
  - Board report finalized January 2012
  - Report restricted to GSFC 582 management unless they permit broader release
Findings

- Well thought-out, perhaps partly due to systems engineers and FSW engineers in same organization, promoting collaboration

- Four categories of findings
  - Governance
  - Use on Projects
  - Architecture
  - Documentation
Findings: Governance

Meets a need across NASA, used by several projects at multiple Centers

• Has potential to become a dominant architecture framework for NASA FSW

• Lacks a business model - requires formal support for full benefit of product line to be realized
Findings: Use on Projects

Users at Multiple Centers were interviewed

- Technology viewed as mature – easy to build and test
- Promotes collaboration across Centers
- Code violates some standards
- Applications outside of original scope likely will require enhancements
- Could provide valuable training for pipelineing students – open-source availability
Findings: Architecture

Highly regarded by the Board

- Development guidelines for app layer exert a positive influence on architecture
- Use of pub/sub SW bus
  - allows for distributed development and easy integration
  - Well-encapsulated apps improve abstraction, flexibility, reuse, division of concerns
  - Could result in non-deterministic/non-repeatable execution
Findings: Architecture – cont.

- Modular components, well-defined I/Fs
- cFE shields apps from data structure formats
- OSAL allows easy use of different Operating Systems
- cFE can be used Stand-alone
- Message queue overflow handling
  - Drops newer messages
  - Subscriber not notified
- Seconds and sub-seconds derived from different sources, which could lead to timing issues
Findings: Documentation

SARB often find that the documentation doesn’t describe all the key aspects that future users ought to know. Utility/longevity limited by quality, depth, maintenance of architectural description

- ADD incomplete
- ADD uses ad-hoc graphical notation
- Discrepancies in representation and terminology
- Document what has been used on projects
- ADD does not identify required vs optional cFE components
Findings: Documentation – cont.

- Distinction between cFE and CFS components not clear in ADD
- Need view of connections between publishers and subscribers
- Need description of dependencies among source packages
- Need rationales for design decision and underlying assumptions
- Need testing guidelines
- Conceived to meet GSFC’s Earth-orbiter needs; no insight into architectural influences/limitations
Findings: Documentation – cont.

- QoS attributes not well documented
- Need guidance for complex, FT, autonomous control systems
- Need definition of FM philosophy – Limit Checker meets EO needs
- Need start-up procedures
- Need expanded time-services description
- Provide info to configure, execute, analyze performance data
- Document/analyze flight/ground division
Conclusions/Summary

- cFE/CFS Architecture highly regarded by the SARB
- Well-thought out – much potential
- Needs improved documentation
- Needs Governance and support to reach full potential
- Users outside of EO community should proceed with caution
Epilogue

- GSFC division management views the SARB review as value added and is executing a plan to address the SARB findings.
- cFE/CFS use outside of EO has expanded after the SARB review – JSC Class A effort, APL use on DoD missions, GRC, KSC, KARI Lunar Lander.
- cFE/CFS support for multicore, distributed, and partitioned systems in development.
  - Prototyping has shown that these systems can be supported by the architecture.
- Governance model remains undefined, but is currently being addressed.
- For more information, contact Jonathan Wilmot -- 301-286-2623, Jonathan.J.Wilmot@NASA.gov.