Systems Engineering When the System is in Pieces: Your Role after CDR and before System Integration

David Everett

GSFC Systems Engineering Seminar

April 8, 2015

Abstract

- After the mission-level Critical Design Review (CDR), the component requirements have been defined and the builders are fabricating all of the system components. The textbook view has the Mission Systems Engineer (MSE) finalizing system-level test and operations planning while others are busy building to the requirements. In reality, numerous issues occur during the building of hardware and coding of software, and the resolution of these problems will determine the ultimate cost, performance, and reliability of the entire system. It is the MSE’s job to ensure anomalies are tracked to root cause with appropriate corrective action, ensure the resolution does not compromise reliability and performance of the system, bring additional engineering expertise to bear when needed, and ensure excessive effort is not expended to resolve a performance shortfall that can be covered elsewhere in the system. This presentation will explore the role of the MSE after CDR and before system integration, with specific examples from LRO and OSIRIS-REx.

Outline

- Project state after CDR
- Textbook view of this period
- Reality
- SE Role
  - Track anomalies to root
  - Ensure technical integrity in anomaly resolution
  - Bring on technical help as needed
  - Look across the system for solutions
  - Maintain vigilance
  - Maintain calm
- SE Processes
- Summary

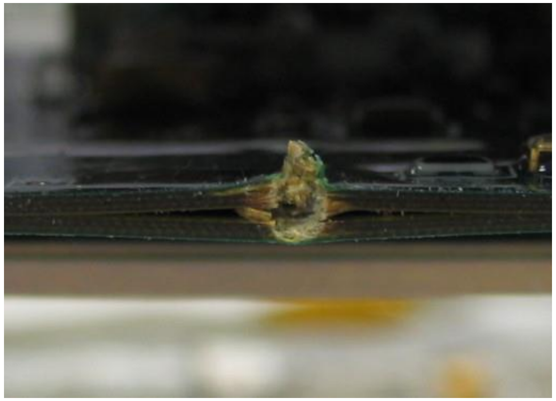
Project State after CDR

- Component requirements are complete
- Component designs are complete, except for some final actions from the CDR’s
- Contracts are in place for out-of-house fabrication
- Plans are in place for in-house fabrication
- Project management is tracking the schedule closely
- The MSE is tracking predicted performance and mass
- A tremendous amount of work is going on in parallel

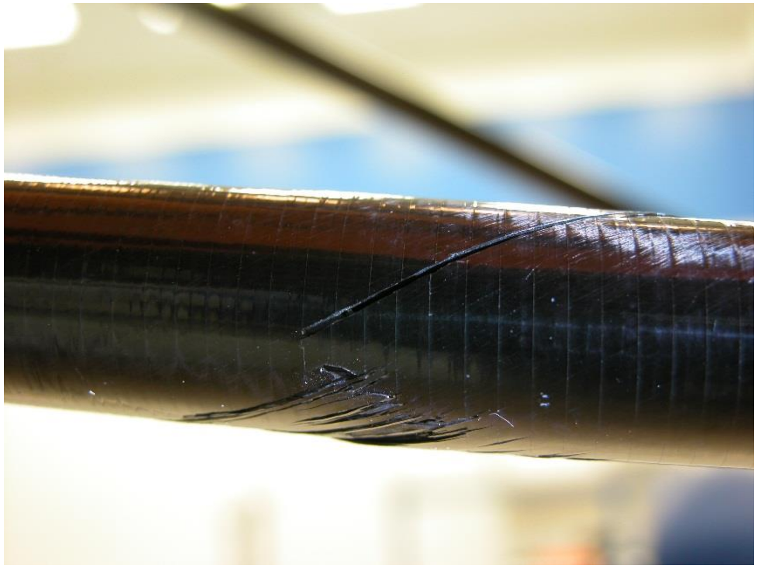
MSE Role: Textbook View

- Track technical performance measures
- Complete plans for system-level testing and operations

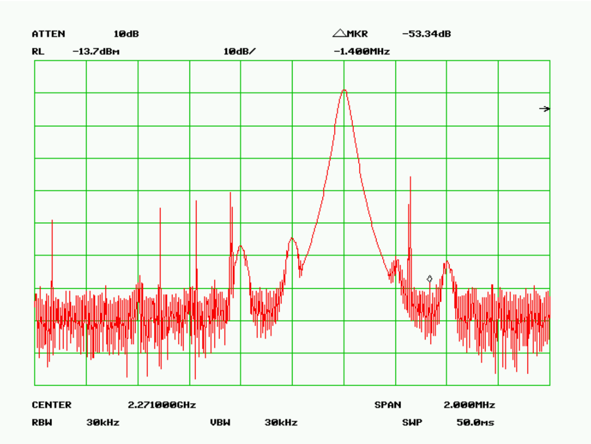
Reality



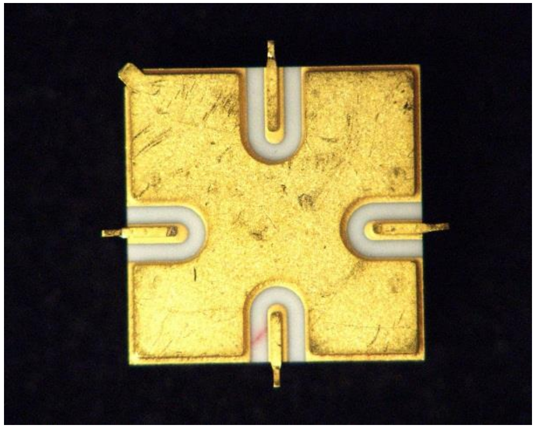
Mistakes (LAMP Circuit Board)



Design Failures (Mini-RF Strut)



Unexpected Performance (Transmitter)



Part Failures (Cougar Amp Cracks)

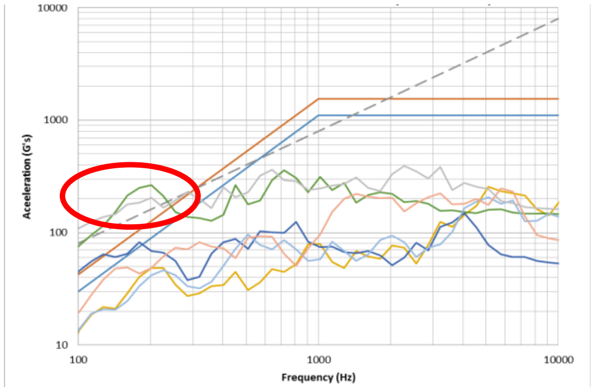
LRO had over 50 Issues after CDR!

- Nearly every component had some sort of problem during the build phase:
  - C&DH:
    - Assembly issues—rework
    - SBC noise problem—rearrange spacewire ports
    - Power supply parts delays—build extra unit
  - Comm
    - Transponder Software design flaw—change ground stations
    - Transponder Hardware design flaw—replace part, jumpers
    - Modulator assembly problems—bring in-house
    - Modulator performance at cold—modify circuit
    - TWTA design error in ground protection circuit—fly as-is
  - GN&C
    - Wheel board layout problem—redo
    - Star Tracker resets—change part
    - MIMU part failure—replace part

LRO had over 50 Issues after CDR (cont.)!

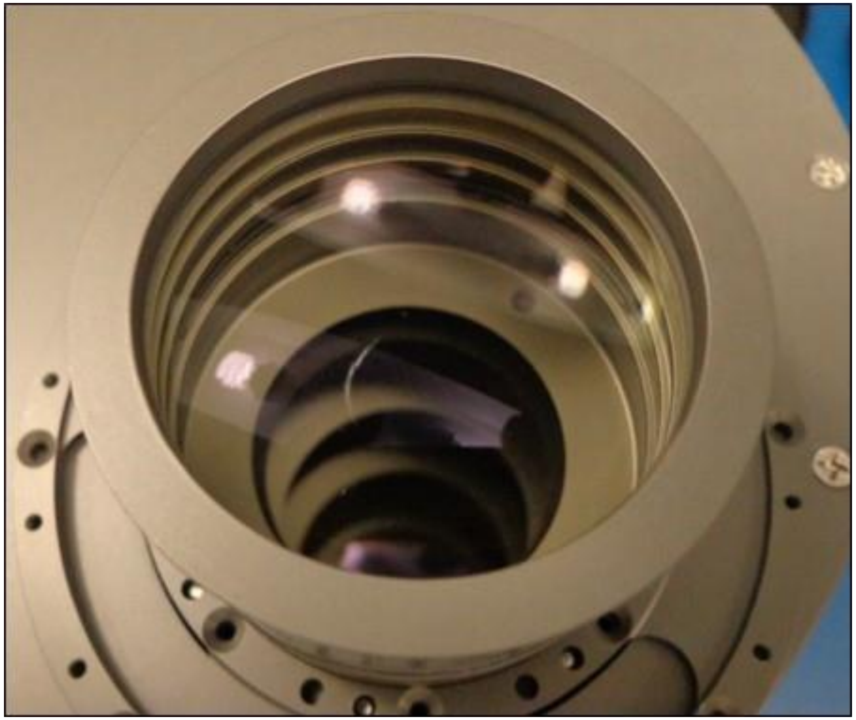
- Nearly every component had some sort of problem during the build phase:
  - Software performance problems—update code
  - Power: PSE frequency shift during vibe—tighten and retest
  - Payloads
    - CRaTER ETU part failure—flight parts OK
    - Diviner actuator damaged during test by long screw—re-work
    - LAMP board damaged by long screw—replace board
    - LEND power surge during thermal vacuum—replace unit (flight spare)
    - LOLA housing corrosion—fly as is
    - LOLA overtest during sine burst—no damage
    - LOLA corona during thermal vacuum—no damage
    - LROC NAC vibration failure—redesign mount for secondary
    - Mini-RF strut failure during thermal vac—redesign strut

OSIRIS-REx is having its Share



Unexpected Environments (SRC shock)

Unexpected Events (OVIRS fire)



Mistakes (MapCam scratch)

Heritage Hardware is not Immune

- Flaws in heritage hardware discovered by OSIRIS-REx testing
  – SRC shock environment
  – Parachute deployment cord cut
  – CPS-J power supply start up
  – CPS-J noise issue

Don’t Panic!

- Anomalies and failures are NORMAL in this phase
  - All components and instruments built and tested in parallel
  - Parts failures, performance shortfalls, unexpected behavior, and handling mistakes are inevitable
- Role of project systems
  - Ensure anomalies are tracked to root cause, with appropriate corrective action
  - Ensure resolution does not compromise reliability and performance of the system
  - Bring additional engineering expertise to bear when needed
  - Ensure excessive effort is not expended to resolve a performance shortfall that can be covered elsewhere in the system
  - Maintain Constant Vigilance for misunderstandings and disconnects
  - Provide a calm presence to reassure the team and management

24-hour Rule

- Expect notification shortly after the discovery of a serious anomaly or mistake
  - Set the expectation through verbal and contractual means
  - Encourage the notification by not over-reacting to bad news
  - Keep project management informed
- Do not ask for data or possible solutions within 24 hours of the discovery of an anomaly
  - The engineers working on the problem need time to digest the situation
  - The problem almost always looks less dire after those closest to it have had some time to gather data and think
- These steps encourage open communication, which builds trust—trust is essential to optimal problem solving!

Ensure Anomalies are Tracked to Root Cause

- Root cause is within the process that led to the error that led to the failure or flaw
- Don’t fixate too early on a possible root cause to the exclusion of other possibilities; be rigorous in determining all possible root causes and then focus on the most credible (might be more than one).
- Don’t stop at the error—figure out why the error was made, and fix the process!
- Example:
  - OCAMS fastener length—3 similar cameras, one needed slightly shorter screws. Procedure was copied—needed to re-review all procedure to look for places where things should be different.
  - DTCI problem on MAVEN not fully corrected (root was a signal integrity issue)—needed to re-layout board for OSIRIS-REx
  - Honeywell had a bad batch of bearings on wheels—did an excellent job working with experts, customers to understand cause and update process
  - Taurus XL launch of OCO failed, then the very next launch, Glory, also failed; although root cause was not determined by either mishap board due to lack of telemetry and hardware, the Glory mishap board discovered potential root causes that were missed by the previous mishap board

Ensure Resolution does NOT Compromise System

- There are tremendous cost and schedule pressures at this phase
- Understand the contractor motivations, and make sure the contract does not cause a bad decision
- Make sure you hear the minority opinions
- Make sure the builders are providing a balanced perspective—ask questions!
- Choose risky options with your eyes open and project management aware—document the risk
- The SE is the advocate of the system and needs to consider the system ramifications of any proposed solution
- Example:
  - MAVEN spares pushed aside by other contracts
  - LCROSS star tracker noise perturbed attitude control and used excessive fuel
  - OCAMS concerns raised by quality engineer who was concerned that the team was going too fast; project stepped in and made sure issues were properly addressed
  - Diviner mechanism damaged by long fasteners; project opted for longer disassembly and clean-out of debris, rather than attempt to vacuum through holes

Bring on Help

- Don’t be afraid to bring on additional expertise to resolve questions
- Unanswered questions will haunt you for the rest of the mission, and follow-on missions.
- Minimal cost associated with resolving questions will easily pay for itself.
  - No additional effort to respond to reviewers’ questions
  - No time spent later chasing down a different symptom of the same problem
  - Better future relationship with customers
- Examples:
  - OSIRIS-REx Lidar procured by LM, laser life-test unit experienced premature failure, GSFC expert worked with contractor to solve issues
  - LRO Narrow Angle Camera structure failed during vibration testing, provided additional analysis support

Look Across the System

- Some problems can be handled by margin elsewhere in the system
- Look for “soft” requirements—places where choices were made early on without significant analysis
  - Sometimes expected performance becomes the requirement, then the component under-performs
  - These soft requirements can over-constrain a mission if the rationale is not captured (you can’t remember why you have a requirement, so you are reluctant to change it)—this is a lesson back to formulation!
- Example:
  - LRO transponder had trouble locking to “1010” pattern; problem understood, but required PROM change to fix; changed ground station idle pattern to “1100”
  - Move of battery to fix cg problem on OSIRIS-REx
  - OSIRIS-REx natural feature tracking accuracy requirement is tighter than baseline lidar—driving shape model requirements

Constant Vigilance

- Warning signs
  - Conflict
    - Understand the cause and cure it at the root; do not simply ask folks to "get along"
    - Someone's focus is not on the mission, someone is leading poorly, and/or someone is making poor decisions
  - Disconnects
    - Different interpretations by different individuals with different perspectives
    - Gaps in the requirements
  - Anomalous behavior
    - Never assume—make sure the source is clearly identified
- Strategies
  - Maintain personal contact across the team
    - Feel the stress level of team members, sense their priorities, hear their concerns
    - Develop the technical credibility and rapport with the out-of-house engineers—you want them to work with you toward mission success, not jump at the lowest-cost solution
  - Use risk management process to open dialog and empower builders
  - Encourage social interaction (picnic, happy hour, etc.)—team spirit
- Examples:
  - LRO parts issue with C&DH
  - Conflict between WIRE project manager at GSFC and Instrument Manager at JPL was a symptom not adequately pursued by GSFC and JPL management—may have led to missed peer review

Maintain Calm

- Enforce the 24-hour rule
- Express realistic optimism about success
  - It is hard to do something which you think cannot be done
- Calm flows down to the team, and stress also flows down to the team
- Example:
  - Design protection circuit error in LRO TWTA—Glenn Research Center Chief Engineer involved
  - LRO project manager’s calm, optimistic approach encouraged solutions and kept the project on schedule
  - OSIRIS-REx PI’s intensity can create stress and over-reaction; I have established a relationship where we can talk through concerns without spinning up the team

Engineering Management Processes

- Requirements Management
  - Make sure the plan is coming together for system-level verification
  - Start checking off requirements (analysis)
- Interface Management
  - Interface tests (early and often)
- Technical resource budget tracking
  - Ensure builders are providing updates: no update means they haven't looked
  - Watch center of mass, software performance, and other areas that don't change much before CDR—data is NOW available, so you should see changes
- Configuration Management
  - Make sure waiver process is working
- Risk Management—CRITICAL in this phase!
- Team with Mission Assurance—process is closely tied with working, reliable product during this phase
- Communication
  - Element and subsystem teams tend to disconnect while each is focused on internal problems
  - Systems engineering must keep the communication paths open

Summary

- The period between CDR and System Integration is where design meets reality
- Anomalies, failures, misunderstandings, and mistakes are inevitable during this period when so much work is going on in parallel
- The actions of the systems engineer during this period will:
  - determine the ultimate reliability and performance of the system
  - have a big impact on the final cost of integration
- Be vigilant and calm, anticipate problems where you can, and work through them where you can't
- Be the technical conscience of the mission