Mission Assurance and Residual Risk: The Performance Verification Challenge for Technology Infusion

Peter Gage
Neerim Corp, NASA Research Park, Moffett Field CA

Ethiraj Venkatapathy
NASA Ames Research Center, Moffett Field CA

RISK IS INTENTIONAL INTERACTION WITH UNCERTAINTY [1]

EXPLORATION MISSIONS ARE RISKY

- Exploration is venturing into unknown environment
- Unknown is uncertain

- NASA's Policy on Mission Assurance [3]
  - Accept residual risk
    - Remaining risk that exists after all mitigation actions have been implemented or exhausted in accordance with the risk management process

NEW FRONTIERS ANNOUNCEMENT OF OPPORTUNITY [2]

- No target is specified for mission residual risk
- *Limited number of less mature technologies and/or advanced engineering developments are permitted*
  - *Must contain a plan for maturing systems to TRL 6 … by no later than Preliminary Design Review (PDR)*

- Proposers will likely concentrate on technology risk vs mission residual risk

TECHNOLOGY DEVELOPMENT IS RISKY

- Development means creating new behavior
- New is uncertain

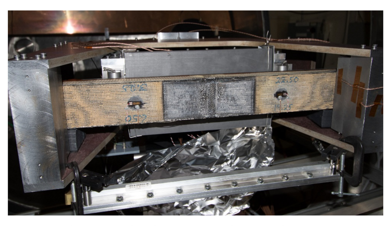
- NASA's Systems Engineering Handbook [4]
  - Technology infusion is
    - Very complex process
    - Ad hoc approaches for different projects have varying degrees of success
    - Failure contributors are related to level of uncertainty at project inception

TRL 6 CAN CORRESPOND TO A WIDE RANGE OF MISSION RISK

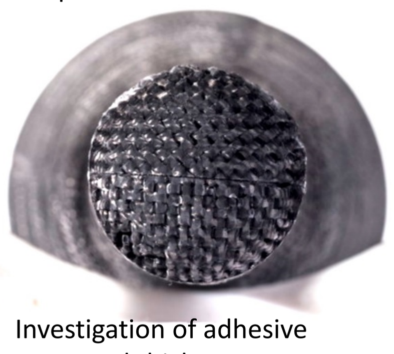
QUALITY OF DEMONSTRATION AND ENVIRONMENT

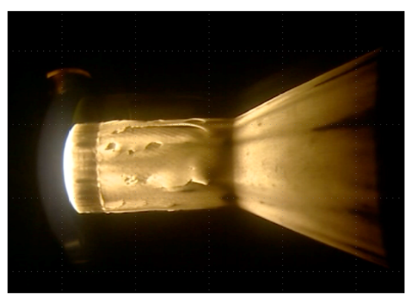
- Nominal vs bounding loads
- Confirming success vs exploring failure
- Individual loads vs combined loading
- Scale of test article
- Gap between demonstration environment and operational environment
  - Thermal Protection System cannot test in fully relevant environment
- Single demonstration vs statistically relevant data set
- Pass/fail vs model correlation
- Attack Unknown and Under-Appreciated Risk [5]
  - Likely a factor of 2-5 higher than estimated risk at start of system operation
  - Affected by
    - Pace of development
    - Prioritization of safety vs cost and schedule

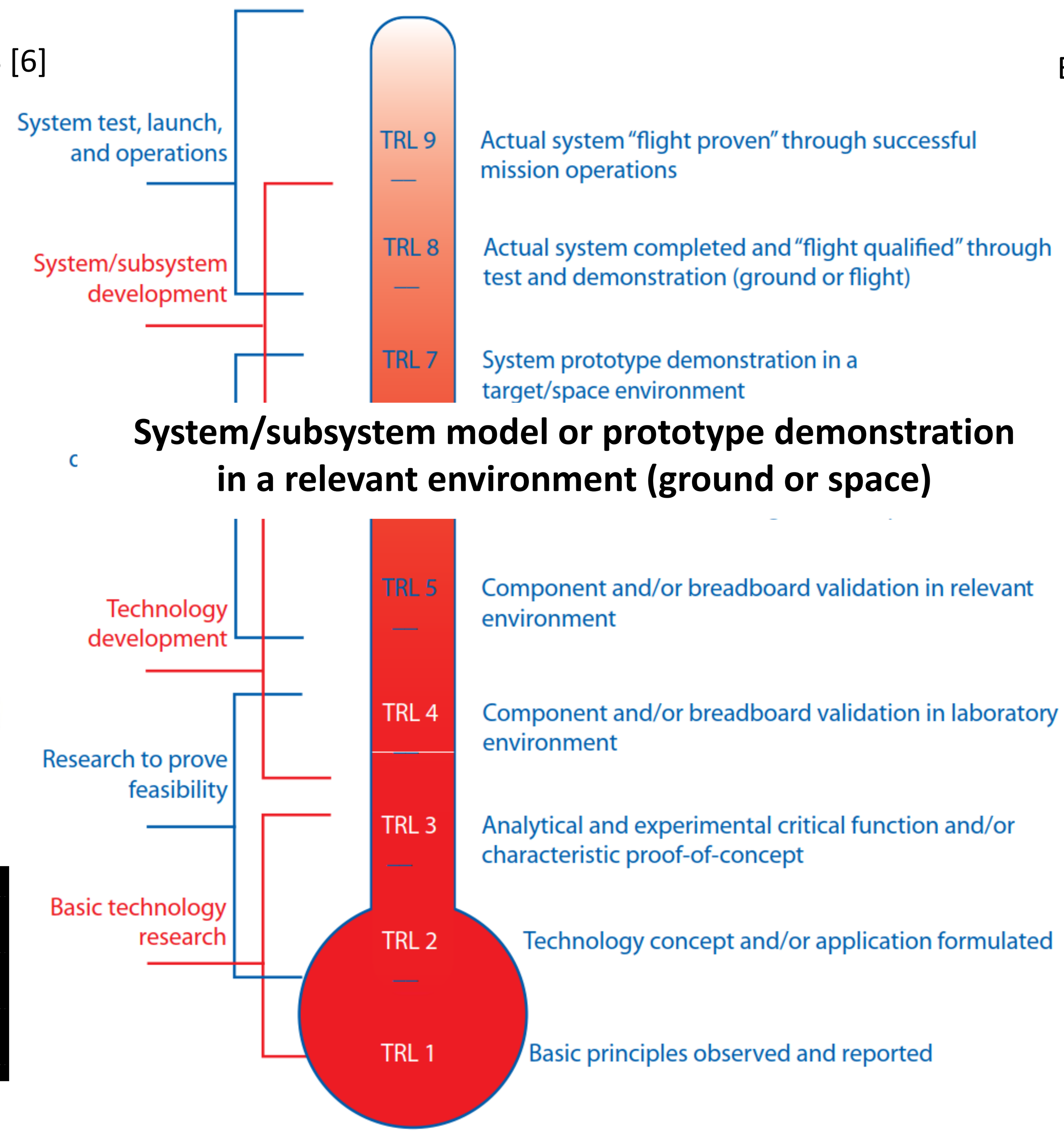
Example: HEEET TPS [6]


Combined thermal and mechanical loading of seams

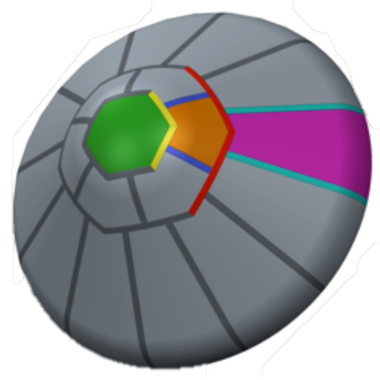

High shear testing of complete seam


Investigation of adhesive types and thicknesses


Extreme environment testing of acreage material

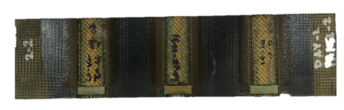


Example: HEEET TPS [6]


Complete heatshield


Assembly


Seam interfaces


Seam assembly

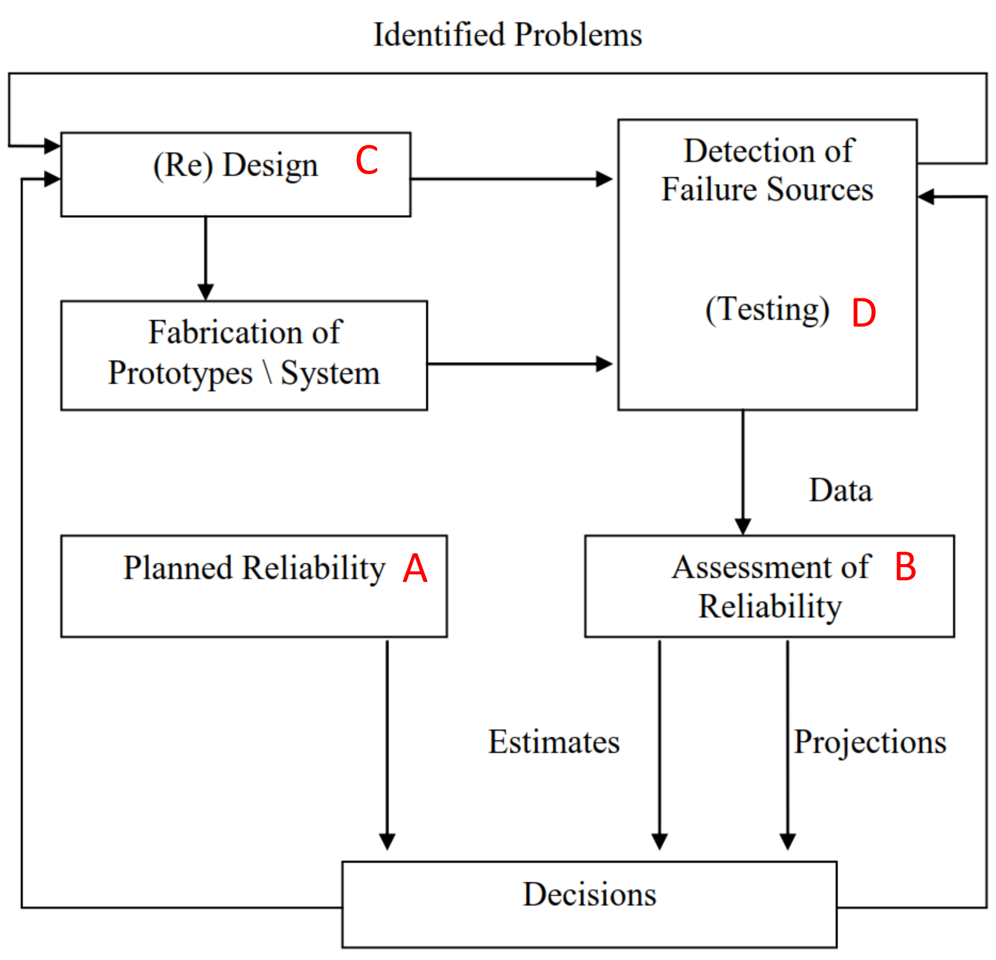

Component

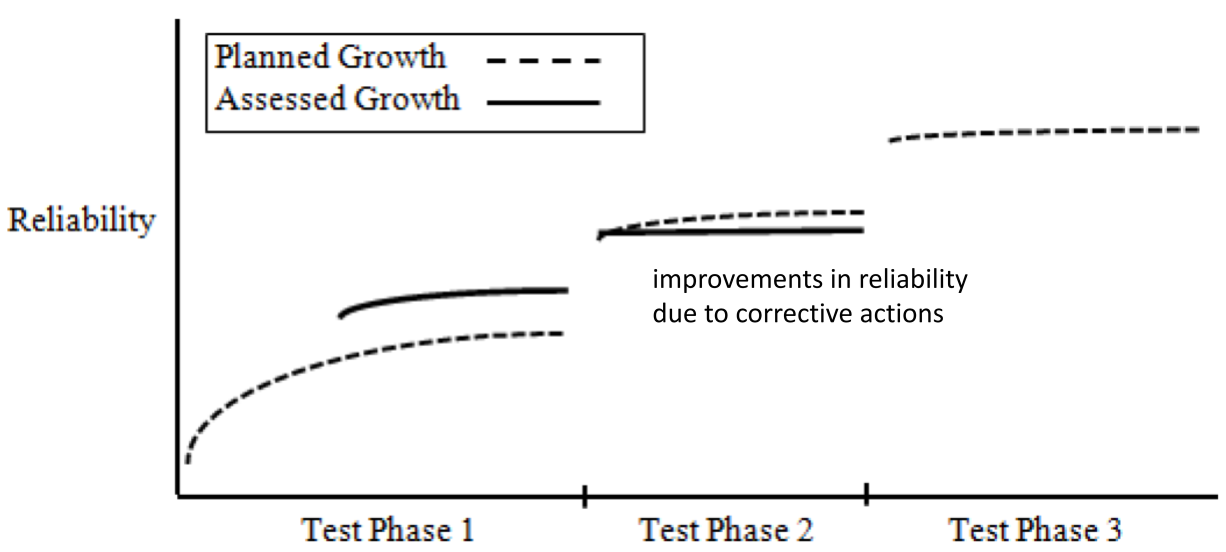
QUALITY OF PROTOTYPE

- Who built it?
  - Technologist vs industry
  - Experienced personnel available for flight build?
  - Same manufacturing infrastructure for flight build?
- When was it built?
  - Obsolescence of components or processes [7]
- Are the processes mature and repeatable?
  - Verification and acceptance criteria
- Are there raw material procurement issues?
- Is the supply chain complex?
- Sole source or intellectual property issues?
- Any scale changes required for flight?

RECOMMENDATIONS FOR MISSION RESIDUAL RISK REDUCTION

Reliability growth [8] is improvement in reliability over time due to corrective actions to system design, operation… or the associated manufacturing process





A. Assign reliability goal for system in Announcement of Opportunity [9]
   - Facilitates comparison of Expected Value from competing mission proposals
   - Proposers can allocate reliability requirements to subsystems
     - Balance new technology reliability against capability of other subsystems
B. Assess reliability of subsystems and integrated system
   - Avoid costly reliability improvement for subsystems that do not drive integrated mission risk [10]
   - Search for unanticipated failure modes
     - Drive down Unknown Risks [5]
   - Concentrate on failure modes that dominate risk [11]
   - Monitor remaining opportunity for reliability growth
C. Provide flexibility for TRL advances in mission development schedule
   - Different technologies have different design cycle duration
     - Short cycle time permits later design freeze in mission development timeline
     - Technology already transferred to industry can have shorter delivery schedule
   - New technologies are likely early in the reliability growth curve
     - Expect significant reliability improvement from an additional design cycle
D. Test hard
   - Develop insight into technology capability limits
   - Vary test environments to assess sensitivity of response
   - Collect data to validate predictive models
   - Study failure phenomenology, including precursors [12]

REFERENCES

1. Cline, Preston B. (3 March 2015). "The Merging of Risk Analysis and Adventure Education" (PDF). Wilderness Risk Management. **5** (1): 43–45.
2. NASA Announcement of Opportunity New Frontiers 4, NNH16ZDA011O, (2016)
3. NASA Policy for Safety and Mission Success NPD 8700.1E, Revalidated (2013)
4. NASA Systems Engineering Handbook NASA SP-2007-6105 Rev 1 (2007)
5. Benjamin, A., Dezfuli, H., Everett, C., "Developing Probabilistic Safety Performance Margins for Unnown and Underappreciated Risks"
6. Venkatapathy, E., Ellerby D., Gasch, M., "Heat-shield for Extreme Entry Environment Technology (HEEET): Development Status", IPPW June 2017
7. Valerdi, C., Kohl, R., "An Approach to Technology Risk Management", ESD Symposium, Cambridge MA, March 2004
8. Department of Defense Handbook: Reliability Growth Management, MIL-HDBK-189C, June 2011
9. NASA System Safety Handbook, Vol 1. "System Safety Framework and Concepts for Implementation", NASA SP-2010-580, November 2011
10. NASA Risk Management Handbook, NASA SP-2011-3422
11. Vander Kam, J., Gage, P., "Estimating Orion Heat Shield Failure Risk Due To Ablator Cracking During the EFT-1 Mission", June 2016
12. Groen, F., Stamatelatos, M., Dezfuli, H., Maggio, G., "An Accident Precursor Analysis Process Tailored for NASA Space Systems", STI 10-027