

NASA Advisory Council Exploration Committee

Constellation LOC/LOM Status

Capt Rick Hauck
NASA Headquarters
April 16, 2009

Cx LOC/LOM Status

- ▶ Exploration Committee fact-finding:
 - Discussions with Carlos Noriega, Cx SR&QA – Hauck Visit to JSC March 4, 2009
 - Briefing by Lauri Hansen, Director of Cx Systems Engineering & Integration (SE&I) – NAC Meeting April 14, 2009
 - Briefing by John Turner, Robert Cross, and Carlos Noriega – NAC Meeting April 15, 2009

www.nasa.gov/mission_pages/station/science/nlab/nlab_proposal.html

Cx LOC/LOM Status

New Human Rating Requirements (NPR 8705.2B Para 3.2.2)

IS: Minimum of 1 failure tolerant to catastrophic events with the specific level of failure tolerance (1,2, or more) derived from an integrated design and safety analysis

WAS: No two failures result in crew or passenger fatality or permanent disability.

Invokes Risk Informed Design (RID)

Rationale for change:

- ▶ Emphasize rigorous engineering and defense of design(s)
- ▶ Apply failure tolerance based on application/need/benefit rather than on an arbitrary requirement
 - Maintain consistency with the inadvertent action requirements

Risk-Informed Design (RID)

- ▶ RID is based on the principle that risk is a design commodity like mass or power.
- ▶ Both Qualitative and Quantitative risk analyses used to expose dominant risk contributors and trade design and planning alternatives in the context of assigning critical design commodities such as mass, volume, power, and cost.
- ▶ Risk analysis includes all significant failure types, including: functional, phenomenological, software, human reliability, common cause, and external or environmental events.

Risk-Informed Design (RID)

- ▶ The intent of RID is to make informed design trades in consciously buying down risk
 - Establishing the relative importance of risk drivers so that design and operations decisions can be made early
 - Better balancing risk against other design commodities in the iterative design and planning process

RID Process

- ▶ **The RID process generally follows a three phase process.**

1. Early design concepts are defined with minimally required functionality to perform the mission and no redundancy.

- **Initial focus on implementing “Key Driving Requirements” vs. establishing a fully functional, acceptably safe, or highly reliable design.**
- **Risk analyses are performed during this phase to understand the risk vulnerabilities of this “zero based design” (ZBD).**

RID Process (Step 2)

2. Once a ZBD baseline has been established design enhancements are evaluated with a focus on enhanced functionality and LOC risk.
 - Focus: “Make the design work” and “Make the design safe”.
 - Design is evaluated to determine the best ways to mitigate risk.
 - Methods may include adding a function (e.g., an abort capability), looking at a diverse method for performing the critical function, increased testing to improve reliability, selecting more reliable components, adding margin to the system or adding redundancy.

RID Process (Step 2)

- Major Premise: Simple redundancy is one option to improve safety and reliability. It is not the only option. It is not always the safest or most cost effective option.
- Many different investment portfolios are compared using FOMs derived from key risk commodities, including LOC risk in order to develop a more functional and safe design within available resources.
- Goal: Spend scarce risk mitigation resources (mass, power, volume, cost) most effectively to maximally address risk

RID Process (Step 3)

3. Finally, additional enhancements are considered which more fully address functional requirements and focus on reliability and loss of mission (LOM) risk.
 - A portfolio approach to comparing investments is again used.
 - Increases the likelihood that the final design iteration produces a vehicle that more optimally meets functional requirements, safely, reliably, and within budget.

Probability Risk Analysis (PRA)

▶ Maturation of Risk Analysis

○ Formulation

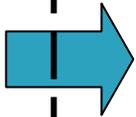
- Early Maturity: *Support Early Concept Development; Select Architecture*
- During this phase Identify and characterize key risk drivers and support the development and comparison of early mission concepts; Simpler high level models focused on risk driver prioritization, fault trees, MEL analysis, heritage based assessment, point estimates, establish preliminary requirements

○ Preliminary Design

- Moderate Maturity: *Provide design guidance, Establish LOC and LOM Requirements,*
- During this phase support design trades and set priorities for preliminary design; Also evaluate potential achievability of LOC and LOM requirements to determine “challenge” requirements; Model environments, integrated effects and phenomenological events in more detail; Retain focus on point estimates where uncertainty is difficult to characterize, evaluate achievability of requirements

○ Verification

- Highest Maturity; *Finalize design assessments, Perform verification of achievement for LOC LOM requirements*
- During this phase refine models to reflect evolving design; Reflect “as designed” systems, accurate environmental models, and mature operations concepts; Develop integrated event tree/fault tree models with uncertainty analysis; Perform Independent Peer Review of Verification models



ISS Integrated Mission Model Status

- ▶ **Several early maturity iterations of Integrated ISS and LS Mission LOC LOM Analysis have been completed**
- ▶ **Integrated analysis currently being updated to incorporate latest design cycle results and systems level LOC LOM analysis**
 - PDR level design maturity in Orion and Ares
 - linked Fault Tree / Event Tree Implementation
 - Uncertainty Analysis
- ▶ **Will provide a basis for the LOC LOM Achievability Assessment in June**

LOC LOM Plan Forward - Summary

- ▶ Continue to refine systems model to reflect latest PDR design iterations for Orion and Ares
- ▶ Update to reflect post LDAC-3 Altair design (LOM Buyback)
- ▶ Integrate systems models into mission model and scenario analysis
- ▶ Provide PDR fidelity analysis at Program PDR LOC-LOM Achievability Assessment decision forum
 - Evaluate achievability of current LOC LOM requirements
 - Identify additional mitigations or requirements changes for action

Summary and Conclusions

- ▶ Risk Informed Design, incorporating PRA, is a new discipline to the design application
- ▶ Early focus is to use LOC LOM analysis to establish relative risk priorities and drive design decisions
 - Significant progress in using LOC LOM to drive Ares, Orion, and Lander design
- ▶ Later focus is to gain fidelity and perform verification analysis
 - Fidelity approaching PDR level
- ▶ Challenge requirements will be finalized at Program PDR
 - Program may update ISS mission LOC and LOM requirements prior to Achievability Review
- ▶ The CxP exploration mission represents a much higher level of complexity than traditional PRA applications
 - Dynamic environments
 - Tight design margins
 - Performance critical
- ▶ CxP is defining new practices, methodologies and models for collaboration in order to meet these challenges
- ▶ Risk analysis is performed with greater consistency on the CxP than previous HSF applications, and is making a profound impact on design and operations planning