NASA Hazard Analysis Process

George Deckert
Johnson Space Center
Safety, Reliability and Mission Assurance Directorate
Subsystem Safety Engineering Through the Project Life Cycle

Work Authorization
- Kick off
- Reviews

Pre Phase A & Phase A
- Formulation

Phase B
- Definition

Phase C
- Design

Phase D – Development

Phase E – Operations

Retirement/Disposal
- Retirement Plan
- System Closeout Report
- Materials Disposition Report
- Lessons Learned

Operation & Maintenance
- Change Requests
- Problem Resolution
- Training
- Flight Rules & Procedures
- CoFR
- Mission Operations
- SPIT

Deployment & Acceptance
- Change Requests
- Problem Resolution
- Training
- Flight Rules & Procedures
- CoFR
- Mission Operations
- SPIT

Integration & System Test
- Configuration Items
- Acceptance Data Packages
- GIDEP ALERTS
- Lessons Learned
- MCRs
- QA Audit
- PRACA
- RIDs

Fabrication
- System Test Report
- Certification Data Package
- Final Safety Data Package
- FMEA/CIL
- Verification & Validation
- QA Audit
- PRACA
- GIDEP ALERTS

Risk Management
- Preliminary Hazard Analysis
- Integrated Hazards Analysis
- Subsystems Hazards Analysis
- Element Hazards Analysis
- Human Factor Analysis
- S/W Hazards Analysis
- Hazard Report Development

Hazards Report Maintenance/ Risk Analysis
The Risk Informed Design Process

- The process is a continuous process throughout the lifecycle of the Project
- At each design and verification cycle, work to reduce the risk drivers
  - Focus on the Top Drivers to maximize impact
- When new drivers emerge (new cycles) as Top Drivers, work those drivers
- Key decision points emerge at various program milestones (e.g. Achievability)

NASA Risk informed Design Process

- Use of PRA, Hazard Analysis, and FMEA
- Use of engineering judgment and analysis
- Use of Operational judgment and analysis

Start with a Baseline Design

Initial Analyses

Review/Validate Analyses (Includes all stakeholders)

Update analyses

Update the Design (using the RID to influence design/test/Operational decisions)

Identify set of Risk Drivers for the vehicle based on analyses
Types of NASA Hazard Analysis

- Preliminary Hazard Analysis
- Subsystem Hazard Analysis
- Element Hazard Analysis
- Operating and Support Hazard Analysis
- Software Hazard Analysis
- Integrated Hazard Analysis
- Functional Hazard Analysis
Preliminary Hazard Analysis (PHA)

- The PHA is the initial effort in hazard analysis during the early design phases that identifies top level hazards and controls, provides a first look at the system risk, and provides the foundation for future analyses. It is based on the best available data. Sources for data include but are not limited to: system description documents, system diagrams, mission descriptions, operational concepts, functional analysis/architecture documents, Functional Flow Block Diagrams (FFBDs), mishap data from similar systems, and lessons learned from other projects. The PHA identifies and evaluates the hazards and hazardous events associated with the proposed design or functions for potential hazard severity, probability, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented.
Hazard Analysis Process

- Identify hazardous conditions, events or states
- Identify the effect of the hazardous state
- Identify severity of the effect
- Identify all potential causes of the hazardous states
- Identify controls for each of the hazard causes
- Identify likelihood of each cause
- Identify verification strategies for the controls
- Track verification to closure
Identify Hazardous Conditions

• Basically this is a brainstorming exercise!
• What is inherently dangerous about the operation of your system?
  – Standard hazard lists
  – Historical experience/documentation from legacy systems
  – Your engineering training and experience
Consider all Interfaces

My Subsystem

Other Sub-systems
Example

• ISS Crew Transport Mission
  – Launch a crew to the International Space Station
  – Stay docked to the Space Station for 6 months
  – Return the crew to Earth and land in the water
Work a Preliminary Hazard List

• Identify the hazards for this mission.
**NASA Generic Hazards List**

- Collision or Impacts
- Loss of Control
- Contamination
- Corrosion
- Electrical Discharge/Shock
- Environmental/Weather
- Temperature Extremes
- Gravitational Forces
- Electromagnetic Interference
- Radiation
- Explosion
- Fire/Overheat
- Flight Termination Systems

- Implosion/Loss of Pressure
- High Pressure Sources
- Loss of Structural Integrity
- Mechanical
- Loss of Critical Function
- Loss of Safe Return Capability
- Loss of Habitable Environment
- Pathological/Physiological/Psychological
- Inadequate HF Engineering
- Lasers
- Utility Outages
- Common Cause Failures
• Hazard analysis results in the identification of risks and the means of controlling or eliminating them. Hazard analysis also quantifies the risk for the Program/Project Manager.
Final Thoughts

• Hazard analysis is structured process to
  – Identify risk
  – Classify risk
  – Manage risk

• Hazard analysis is not an exact science
  – Relies on engineering expertise and engineering judgment
  – Requires rationale to justify hazard classification

• Hazard analysis is an important tool in
  – Design Process
  – Requirements Validation
  – Risk Management