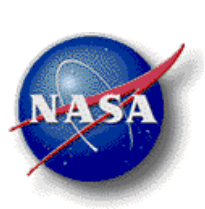
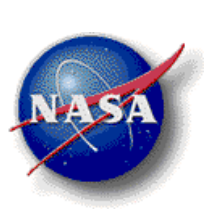


Reliability Analysis and Standardization of Spacecraft Command Generation Processes

Leila Meshkat, Sven Grenander, Ken Evensen
Jet Propulsion Laboratory, California Institute of Technology



Outline

- Problem Addressed
- Command and Control Standardization for Spacecraft Operations
- Probabilistic Risk Analysis for Command Generation
- Hypothetical Example Function & Models
- Summary & Conclusions
- References

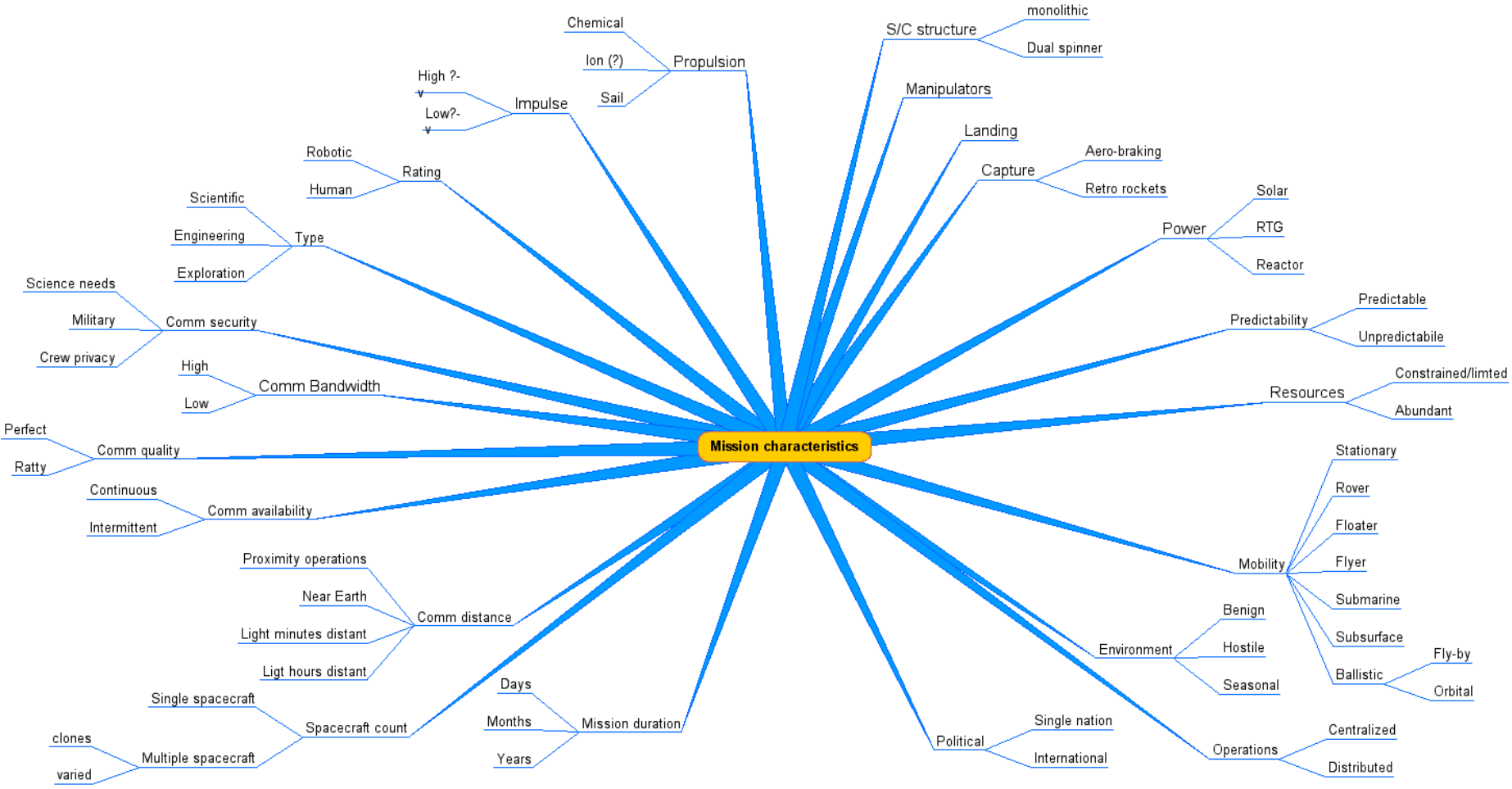
Problem Addressed

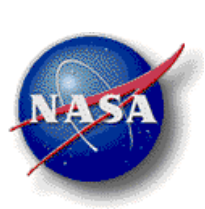
- The problem addressed is reducing the probability of errors in the command generation process and hence commanding errors for spacecraft.
  - These processes involve high levels of human interactions.
- Our approach for addressing this problem is two fold
  - Command and Control Processes for Spacecraft are examined and standardized.
  - A library of process and risk modeling artifacts is built to facilitate the design and/or assurance of command processes.
  - This library utilizes the existing data for Human Reliability Analysis from the Nuclear Industry Data Banks to execute this proposed process.

Command and Control for Spacecraft

- Command and Control (C2) functions for crewed and un-crewed space missions date back over 50 years of robotic and human space exploration.
- The C2 application domain for space exploration represents a huge trade space.
- Traditionally, C2 functions are designed for each mission based on the experience and expertise of designers and their library of available design knowledge.
- The process of generating Command & Control functions has not yet been fully standardized across all mission types.
- C2 functions tackle increasing complexity and performance requirements, and hence bringing order to their design process helps to prevent commanding errors.

Mission Classification Breakdown: Scope of the problem addressed

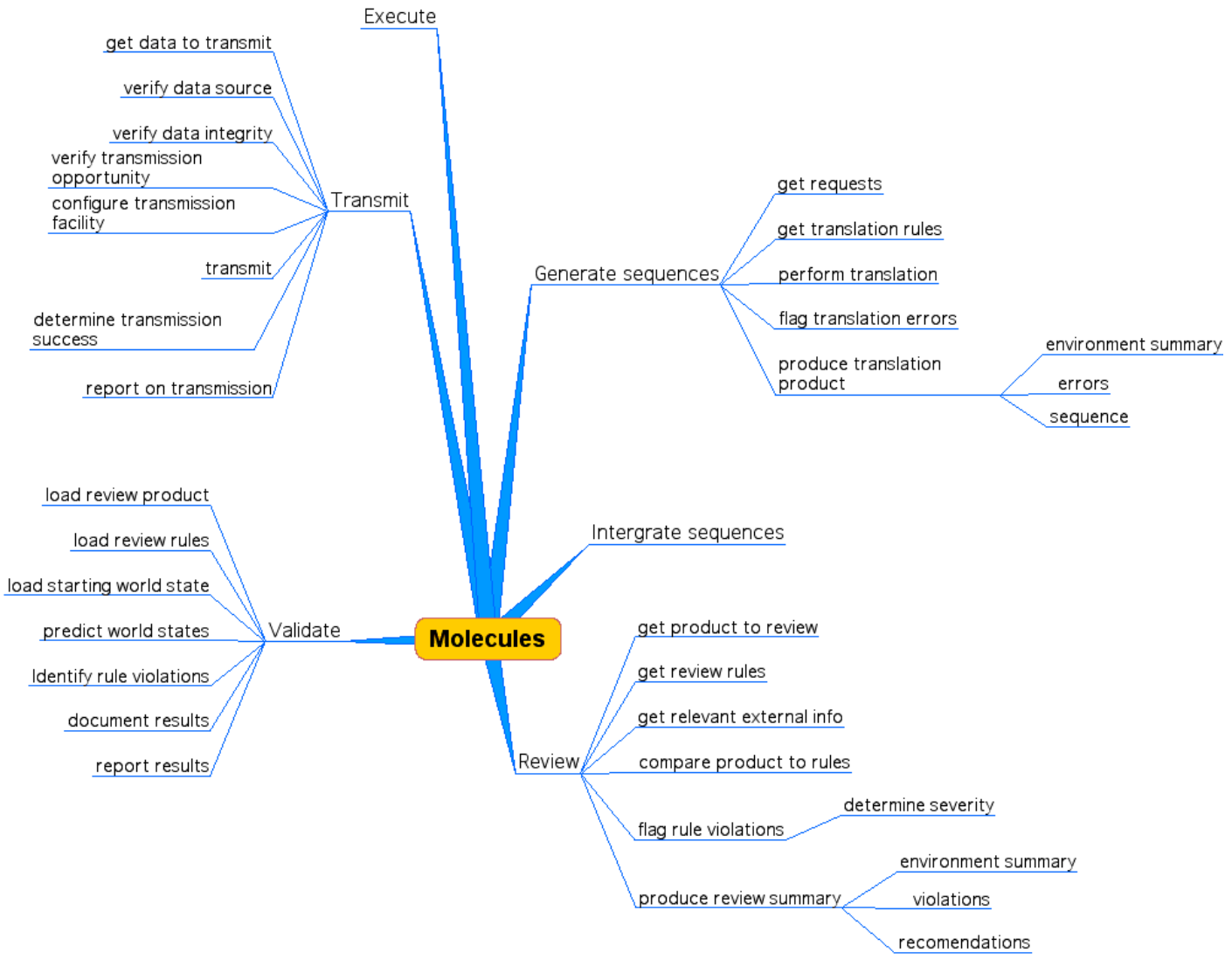




Command and Control for Spacecraft

- A survey of the command generation functions involved in a diverse set of missions, including robotic, human, deep space and Mars missions indicated that:
  - There are only few key atomic level tasks performed in support of these functions.
  - Various combinations of these key atomic level tasks create the main “molecules” used in these functions.
  - Functions represent “composite materials” that are created by the combination of these “molecules”.
  - These composite materials correspond with the mission types.
  - A menu of composite material, and its underlying models therefore facilitates the structured design of C2 functions for an arbitrary mission.

Function Decomposition From Project Architectures



Functional breakdown from project documentation study

Probabilistic Risk Analysis (PRA) for Command Generation

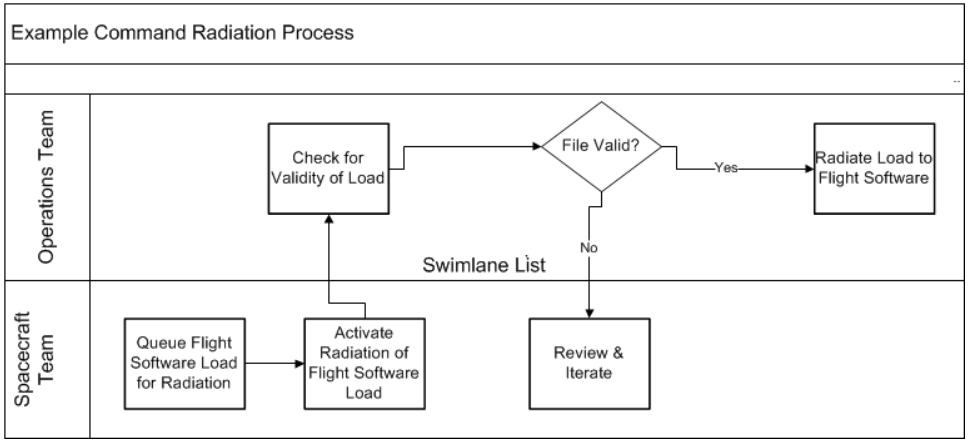
- The focus of this study is to manage the risks associated with human errors during the command generation process.
- These models are applicable for:
  - Risk-based design of C2 functions
  - Mission Assurance of C2 functions
- There are several approaches for Human Reliability Analysis
  - THERP
  - Time Reliability Curves
  - SLIM/FLIM Methodology
  - HEART Approach
  - Cause-Based Decision Tree (CBDT) method
  - Holistic Decision Tree (HDT) Method
- For the purposes of this study, we use a combined THERP and BPMN approach.
  - Data available is based on the THERP approach.
  - BPMN models facilitate the development of PRA models.

Probabilistic Risk Analysis

- Probabilistic Risk Analysis (PRA) models for functions identified in the C2 standardization effort are built.
  - Models are executable.
  - They provide the possible end states for each function and its associated probability.
  - Data from human reliability handbooks are being used for running these models.
  - Models provide the possible end states for each function, and its associated probability.

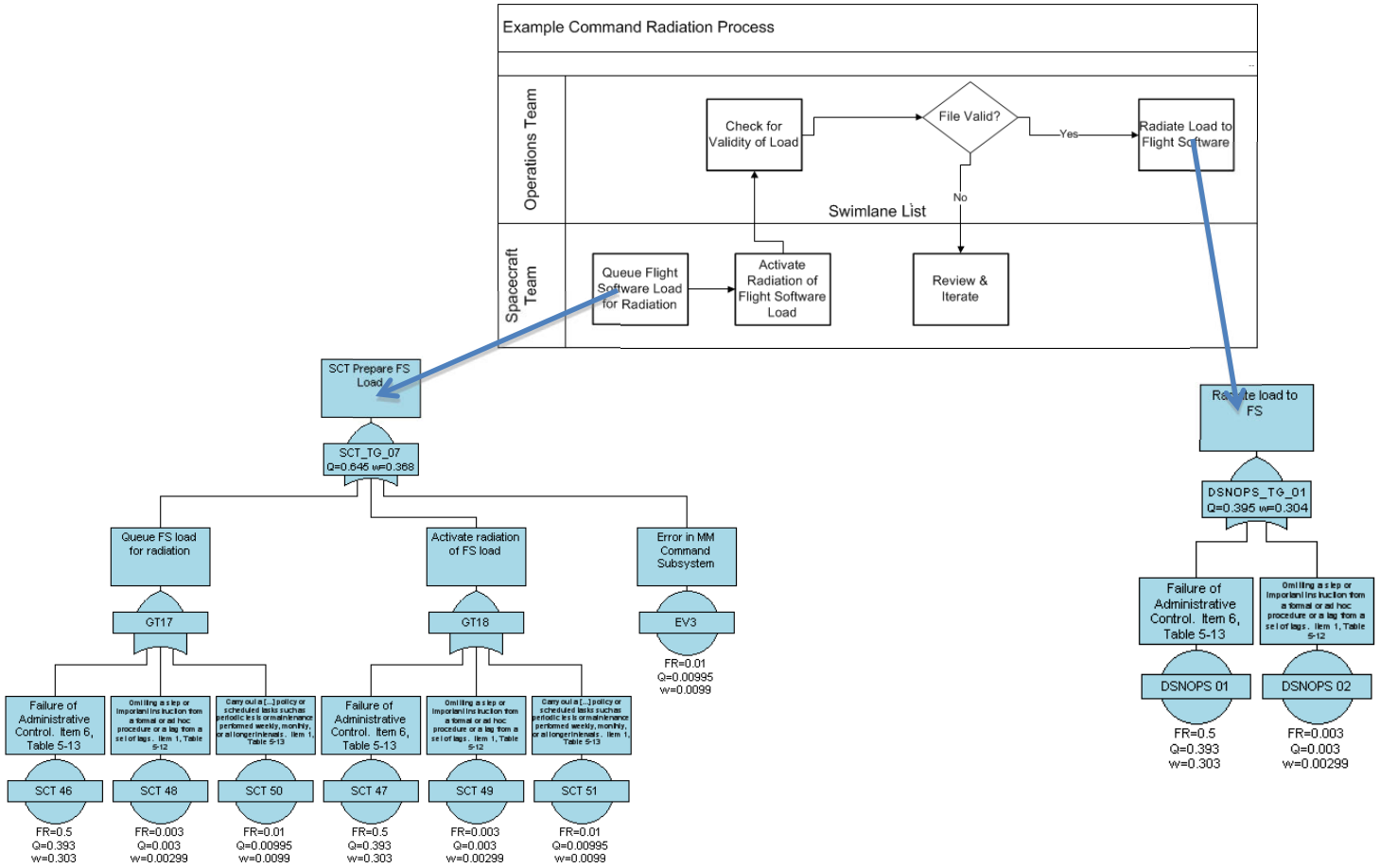
Hypothetical Example BPMN Model

- The Business Process Modeling Notation is used for building the activity flow diagrams.
- A simple example command radiation process is shown below.
- This model is executed in the Process Simulator to yield performance metrics (such as time to perform and availability of each resource.)
- It is also transformed into a risk model for Probabilistic Risk Analysis



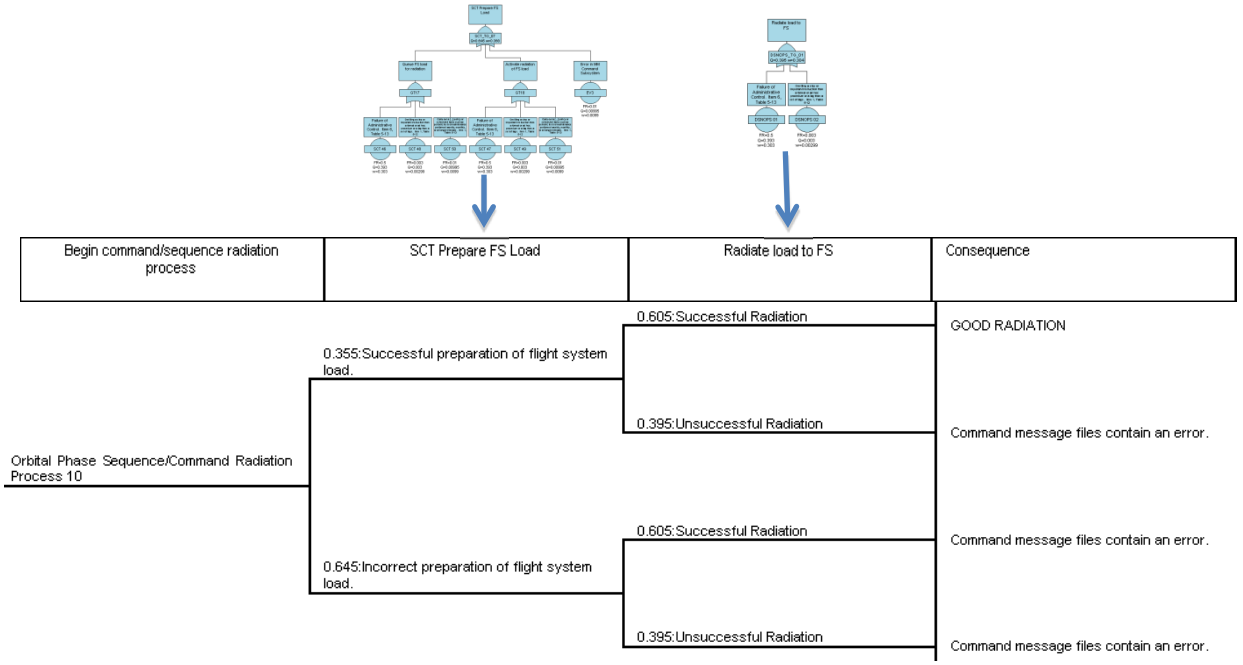
Probabilistic Risk Assessment: Fault Trees

- Each sub-activity in an activity flow is modeled in a fault tree.
- These activities are further broken down into atomic level tasks that correspond to data in human reliability data banks.



Probabilistic Risk Assessment: Event Trees

- Top gates from fault tree become successive steps in the event tree
- “Consequences” are used to capture end result of each branch in the event tree with the corresponding probability, and therefore, the output of the modeled activity

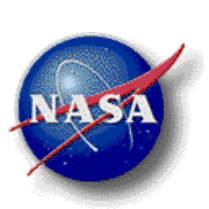


Fault Links

- The correspondence between the “Periodic Table” that is built for standardizing C2 functions and the PRA models that are built for Risk Management is made via the “fault links”
- Each C2 function is the “composite material” built from “molecules” that are combinations of the “atoms” in the table.
- Each function or “composite material”, in turn, corresponds with a BPMN/Event Sequence Diagram.
- Each activity or “molecule” corresponds with a fault tree
- Each basic event in the fault tree corresponds with an “atom”.

Representation of hypothetical model as Fault Links

Function (Composite Material)	Molecule (Sub-activity)	Atom (Event)	MTTF
Example Command Radiation Process	Begin command/sequence radiation process	Begin command/sequence radiation process	1.0
Example Command Radiation Process	SCT Prepare FS Load	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	SCT Prepare FS Load	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	SCT Prepare FS Load	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030
Example Command Radiation Process	SCT Prepare FS Load	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030
Example Command Radiation Process	SCT Prepare FS Load	"Carry out a [...] policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals. Item 1, Table 5-13"	0.01
Example Command Radiation Process	SCT Prepare FS Load	"Carry out a [...] policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals. Item 1, Table 5-13"	0.01
Example Command Radiation Process	SCT Prepare FS Load	Error in MM Command Subsystem	0.01
Example Command Radiation Process	Radiate load to FS	"Failure of Administrative Control. Item 6, Table 5-13"	0.5
Example Command Radiation Process	Radiate load to FS	"Omitting a step or important instruction from a formal or ad hoc procedure or a tag from a set of tags. Item 1, Table 5-12"	0.0030



Conclusions

- In order to reduce commanding errors that are caused by humans, we create an approach and corresponding artifacts for standardizing the command generation process and conducting risk management during the design and assurance of such processes.
- The literature review conducted during the standardization process revealed that very few atomic level human activities are associated with even a broad set of missions.
- Applicable human reliability metrics for performing these atomic level tasks are available.
- The process for building a “Periodic Table” of Command and Control Functions as well as Probabilistic Risk Assessment (PRA) models is demonstrated.
- The PRA models are executed using data from human reliability data banks.
- The Periodic Table is related to the PRA models via Fault Links.

References

- David I. Gertman, Harold S. Blackman, " Human Reliability & Safety Analysis Handbook", John Wiley & Sons, Inc. 1993.
- Anthony Spurgin, " HRA Concepts and Applications", Series of workshops given at Tsinghua University, Beijing, China May 10th through 12th , 2005
- Grant Faris, " Proposed Institutional Command File Error Definition, Categories, and Metrics". 3 April 2008.
- Michael Jones, “Juno Project Functional Description Document”.
- Shamas P. Smith and Michael D. Harrison, “ Blending Descriptive and Numeric Analysis in Human Reliability Design”. The Dependability Interdisciplinary Research Collaboration, Department of Computer Science, The University of York, United Kingdom.
- P. Trucco, E. Cagno & O. Grande, “ A Bayesian Belief Network Approach for Integrating Human and Organizational Factors in Risk Analysis: A Case Study for the Maritime Industry.
- “Summary of Some Recurring Software-Related Mission Anomalies, “Laboratory for Reliable Software 28 June 2009.
- Grant Faris, January 2010, “Mars Program Office Command File Errors”,