

## Incorporating Safety in Early System Architecture Trade Studies

Nicolas Dulac, Nancy Leveson, Ph.D.; Massachusetts Institute of Technology, Cambridge, Massachusetts, USA

Keywords: Design for Safety, Hazard Analysis, Conceptual Design

### Abstract

Evaluating risk early in concept design in order to inform the early trade studies is difficult due to the lack of information available at that early stage. This paper describes the approach used to perform a preliminary risk evaluation to inform the trade studies MIT and the Draper Laboratory are doing as part of the Concept Evaluation and Refinement (CE&R) activities of the new NASA Space Exploration Initiative.

### Introduction

The new Space Exploration Vision outlined by the President involves a return to the moon as a stepping-stone for the future human exploration of Mars. As part of this effort, MIT and the Draper Laboratory are members of a joint team that was awarded a contract to perform a Concept Evaluation and Refinement (CE&R) study for the development of a space exploration architecture that fulfills the needs of the many stakeholders involved in the exploration enterprise. Safety was defined upfront as one of the most critical criteria for a successful space exploration enterprise. It was also recognized that considering safety issues early in the system lifecycle would maximize safety while minimizing negative impacts on the system. In an ideal system safety process, hazard analysis begins at the very start of the system lifecycle. The analyses are continuously revised and refined and are used to design hazards out of the system proactively or, if that is not possible, to mitigate them in the design, instead of adding safety features to a completed design. In this project, we had the opportunity to consider safety at the very beginning of the lifecycle and to influence key architectural decisions that would be impossible to change later.

However, we soon realized that the information available at the very beginning of the project, although broad and plentiful, was so high-level that it would be impractical to perform a full-fledged hazard analysis at this stage. Preliminary Hazard Analyses could be performed and used in the early concept trade studies, but the scope of the system and breadth of information available created some difficult challenges. The methodology presented in this paper describes the approach we developed to perform a structured preliminary hazard analysis while coping with the complexity associated with the large scope of the system. The entire space exploration enterprise was considered in the analysis. In order to limit the scope of this article, however, the methodology is demonstrated using the transportation subset of the exploration architecture. In other words, the scope of the analysis presented in this paper includes bringing humans from earth orbit to mars surface and from moon/mars surface back to earth orbit. Earth launch and re-entry, as well as moon/mars surface operations, are not considered in this paper.

### Task Definition and Key Assumptions

The methodology developed involves an analysis of the hazard mitigation potential of several candidate architectures. A key assumption underlying the risk analysis is that for novel systems with little historical data, it is not possible to accurately predict the likelihood of any particular hazard occurring. The difficulty in predicting hazard likelihood is especially great at the very beginning of conceptual studies, where virtually no design information is available. Inaccurate *a priori* evaluations of hazard likelihood inevitably lead to incorrect risk assessments that can compromise the safety of the system. Accidents in complex systems often happen because some hazards were initially overlooked due to an overoptimistic initial evaluation of likelihood. While hazard likelihood is extremely difficult to evaluate, hazard severity can be evaluated relatively easily by considering the worst-case scenario loss associated with a specific hazard.

The analysis described in this paper takes into account the randomness of some events such as micrometeoroid strikes, solar flares, and some mechanical failures, but it also recognizes that complex aerospace systems usually fail in non-random ways. For example, neither the Challenger nor the Columbia accidents involved unpredictable random failures. Rather, the accidents were caused by a failure to handle well-known and documented risks adequately [1]. Consequently, the number of hazardous activities performed and the time of exposure alone are not good indicators

of risk. In other words, exposure to hazards is not considered as important as the design and operational strategies built into the system to mitigate hazards.

As with any hazard analysis process, the objective of the risk analysis presented in this article is to assist in designing a transportation architecture with an inherently high hazard-mitigation potential. Mitigating hazards at the architecture level improves safety from the very beginning of the system lifecycle, leaving fewer hazards to be mitigated at the system, sub-system, component and procedural levels. Safety is defined broadly in this paper: The analysis is not limited to preventing human losses; it also includes risks associated with mission and equipment losses.

### Architectural Design Space and Information Available

As mentioned previously, the task of the safety team was to create a methodology to evaluate the risk associated with different space transportation architectures. The information available at this stage of the lifecycle was in the form of a large number of possible Earth-to-Moon/Mars-and-back (E-M-E) transportation architectures created through a graphical programming language called Object Process Network (OPN). OPN [2] is a domain-neutral meta-language that can be used to represent, generate, and evaluate system models. The OPN architecture generator was used to create 1162 feasible transportation system designs. OPN essentially generates architectures by selecting transportation vehicles and functions based on a set of combination rules and constraints. A large number of these architectures were automatically filtered out based on launch mass constraints and other feasibility criteria. The risk evaluation methodology presented in this article could have been automated and used upfront as one of the architecture-filtering criteria. However, a more practical approach was taken, which involved filtering out highly inefficient architectures from a mass and feasibility perspective, and then performing a risk evaluation on the remaining subset of transportation architectures. A sample OPN-generated architecture visualization is provided in figure 1. A typical OPN transportation architecture includes information such as:

- 1) The number and type of vehicles and modules used
- 2) The role and activities for each vehicle/module, including:
  - a. Dockings and un-dockings
  - b. Assembly of vehicle/modules stacks
  - c. Discarding of vehicles/modules
  - d. Prepositioning of vehicles/modules in orbit and on the planet surface

In addition to the OPN-generated architectures, several Technology/Policy choices were available such as:

1. Propulsion Type: Hydrogen, Methane, Nuclear thermal, Nuclear electric...
2. Orbit Transfer Trajectory: Free-return, Hohmann, Bi-elliptical, Spiral...
3. Orbit Insertion Type: Propulsive, Aerocapture,...

The complete list of parameters and options used in the safety analysis are listed in Appendix 1. The entire architectural space can be theoretically obtained by taking the cross product of all OPN-generated transportation architectures and the possible combination of technology/policy parameters and options. The next section provides a step-by-step description of the methodology developed to evaluate risk for a subset of this architectural trade space.

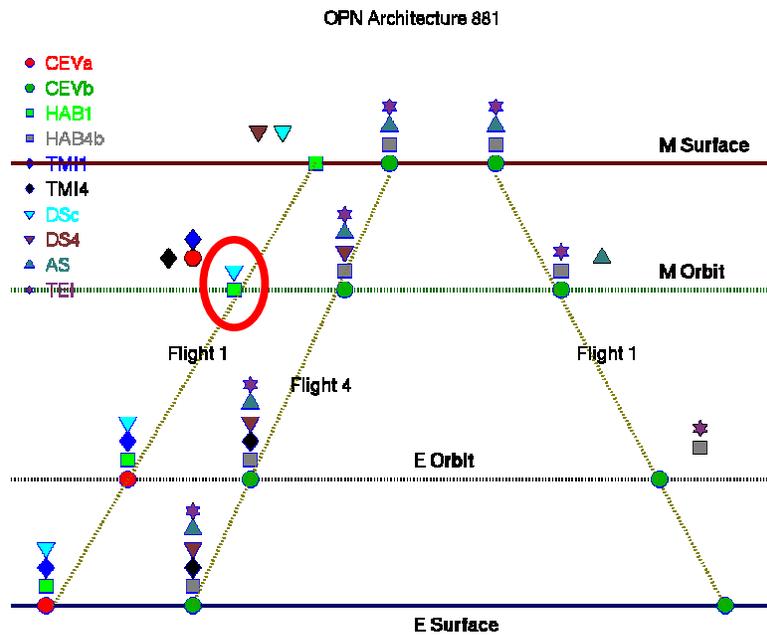
### Hazard-Based Risk Analysis Methodology Overview

The hazard-based safety/risk analysis developed can be described as a three-step process:

1. Identify system-level hazards and associated severities
2. Identify mitigation strategies and associated impact
3. Calculate safety/risk metrics for a given transportation architecture

The first two steps are performed only once, at the beginning of the process. They may have to be repeated if the architectural design space changes and/or if additional hazards are identified. The third step is repeated in order to

evaluate as many transportation architectures and variations as necessary. The following sections discuss each of the three steps in more detail



**Figure 1: Sample Transportation Architecture Visualization**

Step 1: Identify System-Level Hazards and Severities

Just as in typical hazard analyses, the first step in the methodology is to identify the system-level hazards. A Hazard Identification Worksheet (HIW) was created to streamline this process and to ensure proper tracking of the hazards (see figure 2). As with any preliminary hazard analysis activities, identifying system-level hazards involves 10% creativity and 90% experience. Consequently, domain experts were closely involved in identifying hazards for each mission phase.

Once the hazards were identified, the severity of each hazard was evaluated by considering the worst-case loss associated with the hazard. The losses were evaluated for each of three categories: Humans (H), Mission (M), and Equipment (E). A custom severity scale (see figure 3) was defined to account for the losses associated with each category.

Some hazards identified, such as fire, explosion, or loss of life-support span multiple (if not all) mission phases. These hazards were grouped under the label “general” hazards to simplify the analysis. However, the mitigation strategies associated with these hazards depend on the mission phase to which they apply. The chart in figure 4 presents a summary of the identified hazards and severities, organized by mission phase.

**Safety and Mission Assurance Hazard Identification Worksheet**

**Hazard Name:** Nuclear reactor overheating

**Mission Phase:** (circle all appropriate)  
 Pre-Launch    To-Space Launch    In-Space Assembly    To M Transfer    To M Descent    **Surface Exploring**    From M Ascent    To E Transfer    In E Orbit Arriving    On E Landing    On E Recovery

**Operation/Event:** Ex: docking, lift-off, etc.  
Power generation for surface exploration activities

**Vehicle(s)/ System(s) Affected:** Ex: CEV, DAV, rover, etc.  
Surface nuclear power generator, and all systems used on M surface. (HAB, DAV, rover(s), powered equipment)

**Subsystem(s) Affected:** Ex: engine, heat shield, etc.  
Nuclear reactor, cooling subsystem

**Severity\*\* (1-4):**  

Human
4

Mission
4

Equipment
3

Environment
1

**Accident Description:** What happened? What unplanned event occurred? What are the worst case scenario effects, given there is no mitigation strategy? What damage was done? Explain the severity ratings provided above.  
Nuclear reactor core meltdown. If abort is unsuccessful, unavoidable, the time the rover would be lost. All surface equipment is lost. No environmental impact on Earth.

**Hazard Description:** What were the circumstances that allowed the hazard to occur? What were the environmental conditions that contributed to the accident?  
Nuclear reactor operating at temperature above design limits.

**Causal Factors / Assumptions:** What conditions allowed the hazard to occur? Why was the system allowed to get into the hazardous state it was in?  
TBD, but possible causes include: thermal control system malfunction, solar radiation protection inadequate, insufficient radiator heat rejection....

**Mitigation Strategy:**

	Cost/ Difficulty (L,M,H)	Mitigation Impact (0-4)
1. Back-up power generation system is available for surface operations	H	1
2. Surface power generation does not rely on nuclear technology	M	4

\*\* SEE ATTACHED SCALES FOR SEVERITY, COST/DIFFICULTY, MITIGATION IMPACT

**Figure 2: Hazard Identification Worksheet**

<b>Severity Scale</b>			
Scale	Human - H	Mission - M	Equipment - Eq
1	Loss of Life	Mission abort or total mission loss	System Loss
2	Severe injury or illness	Major mission objectives incomplete	Major System Damage
3	Minor injury or illness	Minor mission objectives incomplete	Minor System Damage
4	Less than minor injury or illness	Complete Mission Achievement	Less than minor System Damage

**Figure 3: Custom Hazard Severity Scale**

**Step 2: Identify Mitigation Strategies and Associated Impact**

The second step of the methodology involves the identification and assessment of possible mitigation strategies for each hazard. The scope of the analysis was limited to the architectural option space predetermined by the transportation architecture group. However, the architectural space has a tendency to change very rapidly at the beginning of a project when different options are being explored at a rapid pace. Fortunately, the methodology is highly flexible and allows for rapid re-evaluations of architectures when changes occur. The key to this analysis is to determine the impact of each architectural option on each system-level hazard. In order to do so, a 4-level hazard mitigation impact scale was used (see figure 5). This scale is based on typical system safety hazard mitigation priority scales [3] and is used to determine the impact (if any) of a given architecture option on a given hazard. A database of mitigation impact was generated with the help of domain experts and was recorded in a spreadsheet. It contains the mitigation impact (1-4) of each architectural option, for each hazard, for each category (Human, Mission, Equipment).

ID#	Phase	Hazard	Severity		
			H	M	Eq
G1	General	Flamable substance in presence of ignition source (Fire)	4	4	4
G2	General	Flamable substance in presence of ignition source in confined space (Explosion)	4	4	4
G3	General	Loss of life support (includes power, temperature, oxygen, air pressure, CO2, food, water, etc.)	4	4	4
G4	General	Crew injury or illness	4	4	1
G5	General	Solar or nuclear radiation exceeding safe levels	3	3	2
G6	General	Collision (Micrometeoroids, debris, with modules during rendezvous or separation maneuver, etc.)	4	4	4
G7	General	Loss of attitude control	4	4	4
G8	General	Engines do not ignite	4	4	2
PL1	Pre-Launch	Damage to Payload	2	3	3
PL2	Pre-Launch	Launch delay (due to weather, pre-launch test failures, etc.)	1	4	1
L1	Launch	Incorrect propulsion/trajectory/control during ascent	4	4	4
L2	Launch	Loss of structural integrity (due to aerodynamic loads, vibrations, etc)	4	4	4
L3	Launch	Incorrect stage separation	4	4	4
E1	EVA in Space	Lost in space	4	4	1
A1	Assembly	Incorrect propulsion/control during rendezvous	4	4	4
A2	Assembly	Inability to dock	1	4	3
A3	Assembly	Inability to achieve airlock during docking	1	4	3
A4	Assembly	Inability to undock	4	4	3
T1	In-Space Transfer	Incorrect propulsion/trajectory/control during course change burn	4	4	3
D1	Descent	Inability to undock	4	4	3
D2	Descent	Incorrect propulsion/trajectory/control during descent	4	4	4
D3	Descent	Loss of structural integrity (due to inadequate thermal control, aerodynamic loads, vibrations, etc)	4	4	4
A1	Ascent	Incorrect stage separation (including ascent module disconnecting from descent stage)	4	3	3
A2	Ascent	Incorrect propulsion/trajectory/control during ascent	4	3	3
A3	Ascent	Loss of structural integrity (due to aerodynamic loads, vibrations, etc)	4	3	3
S1	Surface Operations	Crew members stranded on M surface during EVA	4	3	3
S2	Surface Operations	Crew members lost on M surface during EVA	4	3	3
S3	Surface Operations	Equipment damage (including related to lunar dust)	2	3	3
NP1	Nuclear Power	Nuclear fuel released on earth surface	4	4	2
NP2	Nuclear Power	Insufficient power generation (reactor doesn't work)	4	3	3
NP3	Nuclear Power	Insufficient reactor cooling (leading to reactor meltdown)	4	3	3
RE1	Re-Entry	Inability to undock	4	3	3
RE2	Re-Entry	Incorrect propulsion/trajectory/control during descent	4	3	3
RE3	Re-Entry	Loss of structural integrity (due to inadequate thermal control, aerodynamic loads, vibrations, etc)	4	3	4
RE4	Re-Entry	Inclement weather	4	2	2

**Figure 4: System-Level Hazards and Associated Severities**

**Mitigation Impact**

<u>Level</u>	<u>General Description</u>	<u>Detailed Description</u>
4	Eliminate	Complete elimination of the hazard from the design
3	Prevent	Reduction of the likelihood that the hazard will occur
2	Control	Reduction of the likelihood that the hazard results in an accident
1	Reduce Damage	Reduction of damage to the system if an accident does occur

**Figure 5: Hazard mitigation Scale and Priority**

Figure 6 provides a snapshot of the tool created to record hazard mitigation information and evaluate architectures. The system-level hazards and their associated severities (human, mission, and equipment) are listed in the top rows. The architectural and technology options are listed in the column on the left. The architectural space is divided into parameters with alternatives (e.g.: the parameter of launch vehicle type has alternatives HLLV, EELV, STS-derived, etc.) The effects of architectural parameters and technology options on each hazard are recorded in the database according to the 1-4 mitigation scale. For example, not performing Rendezvous in Transit and/or Highly Elliptical Orbital Rendezvous reduces the likelihood of being unable to dock (Mitigation Level: 3). Experience has shown that recording the rationale for each mitigation impact is critical as the database size makes it impossible to remember the inputs of every domain expert, which makes future changes very difficult. Once the hazard mitigation database has been populated, it is possible to start evaluating the overall mitigation potential of various transportation architectures.

	A	B	C	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR
1		<b>Hazard ID --&gt;</b>												
2		<b>Hazard Name --&gt;</b>												
3		<b>Design/Architecture Parameter</b>	970	2	1	4	1	2	4	3	4	4	3	4
14		Nuclear Surface Power - Yes												
15		Nuclear Surface Power - No	1											
16		Level of Autonomy - High												
17		Level of Autonomy - Low	1											
18		Highly Elliptical Orbital Rendezvous - Yes												
19		Highly Elliptical Orbital Rendezvous - No	1					3	3	3				
20		Rendezvous in transit - Yes												
21		Rendezvous in transit - No	1					3	3	3				
22		Artificial gravity - Yes												
23		Artificial gravity - No	1											
24		High-closure ECLSS (H2O, O2) - Yes												
25		High-closure ECLSS (H2O, O2) - No	1											
26		Low boil-off propellant storage - Yes												
27		Low boil-off propellant storage - No	1	3										
28		In-space propellant transfer - Yes												
29		In-space propellant transfer - No	1	3										
30	<b>Policy / Operational</b>	HLLV - Yes			3	3			3	3				
31		HLLV - No	1		1	1								
32		Nuclear - Yes												
33		Nuclear - No	1											
62		Anything Prepositioned on M	1		1	1	1							
63		Nothing Prepositioned on M												
64		Prepositioning modules at Earth orbit - Yes												
65		Prepositioning modules at Earth Orbit - No	1											
66	<b>Docking/Undocking</b>	Need to Dock at Earth Orbit upon Return - NO	1					3	3	3				3
67		Need to Dock at M Orbit Inbound- NO	1					3	3	3				3
68		Need to Dock at M Orbit Outbound- NO						3	3	3				
69		Need to Undock at Earth Orbit upon Return- NO		2							3	3	3	
70		Need to Undock at M Orbit - NO		3							3	3	3	
71	<b>Human/Cargo Couple</b>	Transfer Together												

**Figure 6: Hazard Mitigation Database/Tool**

Step 3: Evaluate Architectures and Calculate Safety/Risk Metrics

A complete transportation architecture is defined as the union of an OPN-architecture with a set of technology/policy parameter options. In order to evaluate the risk associated with a specific architecture, an architecture vector is created that includes all of the parameter for that architecture. This vector is in the form of a large string of binary numbers. Looking at Figure 6, the architecture vector can be found in column C of the spreadsheet. The “1” values in the vector indicate that the corresponding option is selected. In this example, the vector shows that the selected architecture includes:

1. No Nuclear Surface Power
2. Low Level of Autonomy
3. No Highly Elliptical Orbital Rendezvous
4. No Rendezvous in Transit
5. No Artificial Gravity
6. And so on...

An architecture vector has to be created for each architecture evaluation. The architecture vector generation process can easily be automated if a large number of evaluations have to be performed. Once an architecture vector has been defined, the risk evaluation and metrics computation proceeds as follows:

- 1) For each hazard, and each hazard category (human, mission, equipment), that is, for each column of the spreadsheet, the tool searches for the option that provides the maximum hazard mitigation for each architectural parameter. These maximum hazard mitigations are added to obtain the total maximum hazard mitigation factor for each hazard and each category (H,M,E). These *Maximum Mitigation Factors* are architecture-independent. They only depend on the architectural option space and the hazards identified. The process of searching for maximum mitigation factors must be automated to provide the flexibility necessary to modify the architectural

space or to make the tool evolvable. The maximum mitigation factors obtained in this step is almost never achievable in real-life because it would either be impractical or too expensive, or simply because some architecture options conflict with others in terms of hazard mitigation potential. Nevertheless, the maximum hazard mitigation factor is important because it provides an architecture-independent theoretical absolute upon which all the other architectures can be compared.

- 2) To evaluate a specific architecture, the analysis tool matches the selected options with their respective hazard mitigation impact and computes a sum of the mitigation factors obtained for the options selected in the architecture under evaluation. This process is repeated for each hazard and category (H, M, E). The result is a set of *Hazard Mitigation Indices* obtained for a particular architecture.
- 3) A *Relative Hazard Mitigation Index* is calculated for each hazard and each category using the following formula:  $Relative\ Hazard\ Mitigation\ Index\ (i) = 1 - (Hazard\ Mitigation\ Index\ (i) / Maximum\ Mitigation\ Factor\ (i))$
- 4) If a hazard is completely eliminated (Mitigation Level = 4) by a selected architectural option, the *Relative Hazard Mitigation Index* for this hazard is automatically set at zero.
- 5) A *Relative Severity Index* for each hazard and category is then calculated as follows:  $Relative\ Severity\ Index\ (i) = Relative\ Hazard\ Mitigation\ Index\ (i) * Original\ Hazard\ Severity\ (i) ^2$ . The “squared” severity is used to provide heavier weighting on the higher severity indices.
- 6) Three Safety/Risk Metrics (Human, Mission, Equipment) are obtained by aggregating the *Relative Severity Indices* for each category (H, M, E) across all hazards.
- 7) As needed, an Overall Safety/Risk Metric (OSRM) for an architecture can be obtained using a weighted average. In this project, the weighting factors selected were: Human: 9, Mission: 3, Equipment: 1.

Figure 7 provides a summary of the weighting factors used in the calculation of the OSRM for the MIT/Draper CE&R project.

		Human	Mission	Equipment
<b>Hazard Severity</b>	<b>Weight</b>	<b>9</b>	<b>3</b>	<b>1</b>
<b>4.Catastrophic</b>	<b>16</b>			
<b>3.Critical</b>	<b>9</b>			
<b>2.Major</b>	<b>4</b>			
<b>1.Marginal</b>	<b>1</b>			

**Figure 7: Weighting Factors used in Calculating OSRM**

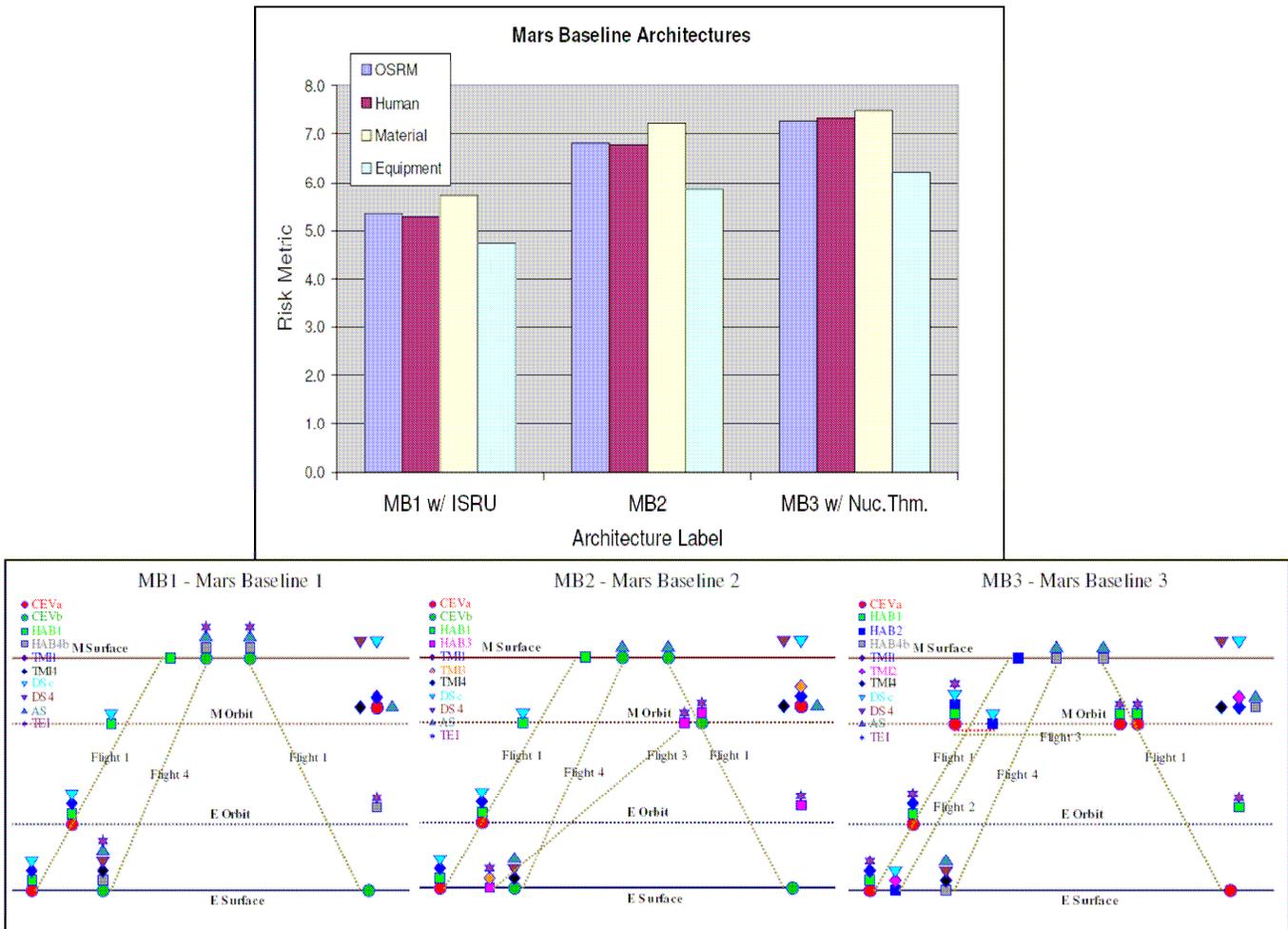
The Safety/Risk metrics are used to evaluate and rank potential transportation architectures. By systematically selecting and deselecting options in the architecture description, it is possible to perform a first-order assessment of the relative importance of each architectural option in determining the Overall Safety/Risk Metric.

### Sample Results

The results from the risk/safety analysis provide a ranking of the selected transportation architectures based on the hazard mitigation potential of each. According to the analysis, Mars Baseline Architecture 1 (MB1) (see Figure 1) is the architecture that has the most inherent hazard mitigation potential. Hundreds of parameters are considered in the Safety/Risk analysis, but some major contributors to the hazard mitigation potential of MB1 include the use of heavy module repositioning on the surface of Mars and the need for rendezvous and docking maneuvers. Repositioning modules allows for pre-testing and mitigates the hazards associated with loss of life support, equipment damage, and so on. On the other hand, repositioning modules increases the reliance on precision landing to ensure that all

landed modules are within range of each other. Consequently, using heavy prepositioning may require additional mitigation strategies to reduce the risk associated with landing in the wrong location. As another example, the transportation architecture MB1 requires no docking at Mars orbit or upon return, which mitigates the risk of collision or failed rendezvous and docking maneuvers.

Figure 8 provides sample results obtained for the three Mars baseline architectures. In this analysis, MB1 was evaluated with the in-situ resource utilization turned on because a direct return from the Martian surface is not possible in MB1 unless propellant is extracted from local resources. MB3 was evaluated with Nuclear Thermal Rockets propulsion, which shortens the transit time but requires additional mitigation for hazards associated with the use of nuclear power (radiation, contamination, overheating, inadequate propulsion/control, high structural loads, etc.) Low OSRM scores are associated with low residual risk, so the lower the OSRM, the better.



**Figure 8: Sample Evaluation Results for Mars Baseline Architectures 1, 2, and 3 and associated Visual Representations**

An automated tool was created to perform multiple evaluations based on the needs of the team responsible for designing the transportation architecture. Hundreds of different architecture evaluations have been performed with little maintenance and data input efforts. The analysis started at the very beginning of the conceptual design phase. However, by the end of the first midterm review (4 months into the project), the information available was very different than at the very beginning. The methodology proved flexible and extensible enough to carry us from day 1 to the beginning of the detailed design phase, at which point, a more detailed hazard analysis methodology such as STPA [4,5] will be necessary.

## Conclusion

The methodology presented in this paper was developed in order to perform a structured preliminary hazard analysis to inform the early system architecture trade studies of the MIT/Draper CE&R project. The need for such a methodology emerged early in the project because of the highly complex, broad-scoped, multi-vehicle, time-dependent nature of the exploration enterprise. The methodology was developed with the specific purpose of evaluating transportation architectures generated by the MIT/Draper team. However, care was taken to make the methodology flexible, extensible, and adaptable to other complex systems. This paper focused on describing the methodology by using a very structured transportation architecture generation scheme as an example. However, the methodology has been applied with equal success to perform a structured preliminary hazard analysis of the surface operations mission architecture of the same project. The information available for the surface architecture evaluation had very different format and content, but the safety analysis was similar. Our experience with the early system architecture trade studies for the MIT/Draper CE&R project convinced us that a highly structured preliminary hazard analysis process is required to incorporate safety early in a project of this size and complexity. The methodology described in this paper provides the structure necessary to perform preliminary hazard analysis early in the development of complex engineering projects.

## Acknowledgements

This work was partially supported by a NASA CE&R contract to MIT and Draper Labs and by a grant (NAG2-1543) from the NASA Engineering for Complex Systems Program.

## References

- [1] Nancy Leveson, Nicolas Dulac, "Safety and Risk-Driven Design in Complex Systems-of-Systems. 1st Space Exploration Conference, Orlando, January 2005.
- [2] Benjamin Koo, "A Meta-Language for System Architecting". Ph.D. Thesis, 2004. Engineering Systems Division (ESD), Massachusetts Institute of Technology.
- [3] Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley Publishers, 1995.
- [4] Nancy Leveson, "A New Approach to Hazard Analysis for Complex Systems." International Conference of the System Safety Society. 2003.
- [5] Nicolas Dulac, Nancy Leveson, "An Approach to Design for Safety in Complex Systems". INCOSE04, Toulouse, France, June 2004.

## Biography

Nicolas Dulac, Ph.D. Candidate, Dept. of Aeronautics and Astronautics, MIT, 77 Mass. Ave., Bldg. 33-407, Cambridge 02139, phone – (617) 253-3045. fax – (617) 253-7397, email – [ndulac@mit.edu](mailto:ndulac@mit.edu).

Prof. Nancy G. Leveson, Dept. of Aeronautics and Astronautics, MIT, 77 Mass. Ave., Bldg. 33-336, Cambridge 02139, phone – (617) 258-0505. fax – (617) 253-7397, email – [leveson@mit.edu](mailto:leveson@mit.edu).

Appendix 1:

Parameters and Options for Transportation Architecture Safety/Risk Analysis

Design / Architecture Parameter	
Technology Choices	ISRU - Yes
	ISRU - No
	Aerocapture - Yes
	Aerocapture - No
	Nuclear Thermal Rockets - Yes
	Nuclear Thermal Rockets - No
	Solar Electric Propulsion - Yes
	Solar Electric Propulsion - No
	Nuclear Electric Propulsion - Yes
	Nuclear Electric Propulsion - No
	Nuclear Surface Power - Yes
	Nuclear Surface Power - No
	Level of Autonomy - High
	Level of Autonomy - Low
	Highly Elliptical Orbital Rendezvous - Yes
	Highly Elliptical Orbital Rendezvous - No
	Rendezvous in transit - Yes
	Rendezvous in transit - No
	Artificial gravity - Yes
	Artificial gravity - No
High-closure ECLSS (H2O, O2) - Yes	
High-closure ECLSS (H2O, O2) - No	
Low boil-off propellant storage - Yes	
Low boil-off propellant storage - No	
In-space propellant transfer - Yes	
In-space propellant transfer - No	
Policy / Operational	HLLV - Yes
	HLLV - No
	Nuclear - Yes
	Nuclear - No
	De-investing in the moon - Yes
	De-investing in the moon - No
	Level of international involvement - High
	Level of international involvement - Low
	Level of commercial involvement - High
	Level of commercial involvement - Low
	Free-return trajectory - Yes
	Free-return trajectory - No
	Initial Mars mission duration - Long
Initial Mars mission duration - Short	
Level of abort options - High	
Level of abort options - Moderate	
Level of abort options - Low	
Others	Crew size - 0
	Crew size - 1+
	Mars landing sites - Single
	Mars landing sites - Diverse
	Mars landing sites - Chain
	Surface elements reusability - Yes
	Surface elements reusability - No
Transportation elements reusability - Yes	
Transportation elements reusability - No	

Design / Architecture Parameter (cont)	
Prepositioning	Prepositioning HAB at M (surface or orbit) - Yes
	Prepositioning HAB at M (surface or orbit) - No
	Prepositioning Power Generator at M (surface or orbit) - Yes
	Prepositioning Power Generator at M (surface or orbit) - No
	Prepositioning Ascent Vehicle at M (surface or orbit) - Yes
	Prepositioning Ascent Vehicle at M (surface or orbit) - No
	Anything Prepositioned on M
	Nothing Prepositioned on M
Docking/Undocking	Prepositioning modules at Earth orbit - Yes
	Prepositioning modules at Earth Orbit - No
	Need to Dock at Earth Orbit upon Return - NO
	Need to Dock at M Orbit Inbound- NO
	Need to Dock at M Orbit Outbound- NO
	Need to Undock at Earth Orbit upon Return- NO
	Need to Undock at M Orbit - NO
Human/Cargo Couple	Transfer Together
	Transfer Separately
Number of Habitable Modules during TMI	1
Number surface habitats	2+
	1
	2+
Propulsion (to Mars)	H2 / LOX (Isp ~ 440)
	CH4 / LOX (Isp ~ 390)
	Hypergolic (Isp ~290)
	Nuc. Thm. (Isp ~ 850)
	Low Thr. (Isp O(1e3))
Propulsion (descent and ascent)	H2 / LOX (Isp ~ 440)
	CH4 / LOX (Isp ~ 390)
	Hypergolic (Isp ~290)
	Nuc. Thm. (Isp ~ 850)
	Low Thr. (Isp O(1e3))
Propulsion (Mars arriva)	H2 / LOX (Isp ~ 440)
	CH4 / LOX (Isp ~ 390)
	Hypergolic (Isp ~ 290)
	Nuc. Thm. (Isp ~ 850)
	Aero Capture
Propulsion (Return Flight)	H2 / LOX (Isp ~ 440)
	CH4 / LOX (Isp ~ 390)
	Hypergolic (Isp ~ 290)
	Nuc. Thm. (Isp ~ 850)
	Low Thr. (Isp O(1e3))