A CLASSIFICATION OF OPEN-LOOP AND CLOSED-LOOP RISK MANAGEMENT ACTIONS

Brandon D. Owens, Joseph R. Laracy, Margaret Stringfellow Herring, Nancy G. Leveson

Complex Systems Research Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email: owensbd@mit.edu, laracy@mit.edu, sapphire@mit.edu, leveson@mit.edu

ABSTRACT

The management of safety risk in complex systems such as spacecraft and launch vehicles is a task that is mired by uncertainty. Attempts are made in each use of these systems to both solve unprecedented problems and apply unique approaches to traditional problems. Nevertheless, in developing a strategy to mitigate risk, spacecraft and launch vehicle managers, designers, and operators must develop conceptual and quantitative models of these systems. To effectively manage risk, these stakeholders have to be prepared for the many types of hazards in spaceflight that can invalidate their system models. Specifically, the stakeholders must—when cost, schedule, and complexity permit—formulate their risk management efforts to respond to feedback from the system that reveals inadequacies in these models. In this paper, a taxonomy is introduced to assist spacecraft and launch vehicle managers, designers, and operators in identifying risk management approaches that are robust against the perturbations to their systems that could violate their models of risk. This taxonomy applies control theory concepts to the analysis of common risk management practices in spaceflight. Each measure is classified for its tendency to provide *open-loop* or *closed-loop* control of risk over some proposed archetypal cycles of system operation. Additionally, tradeoffs related to *open-loop* or *closed-loop* risk management are presented.

1. INTRODUCTION

Since World War II, engineered systems, including spacecraft and launch vehicles, have increasingly exhibited forms of complexity that have stressed many of the traditional quantitative risk assessment techniques employed in their design and operation [1]. Even probabilistic estimates of system-level responses to stochastic phenomena such as the flux of radioactive particles in spacecraft digital memory can become confounded by human, organization, hardware, and software interactions [2]. Indeed, even a leading researcher in quantitative risk assessment recently acknowledged that the following items are not handled well or at all in quantitative risk estimates [3]:

- human errors,
- software,
- safety culture,
- design errors,
- and manufacturing errors.

Additionally, he acknowledged that for complex systems such as the Space Shuttle, quantitative estimates can vary widely over a period of decades as the organizations or industries that engage in such analyses mature with relevant methodologies [3]. In [4], for example, the variation in Space Shuttle risk assessments before and after each of the two major accidents in that program is summarized. These variations and deficiencies in quantitative risk assessment highlight the need to address the question:

"What should be done if/when the quantitative risk assessments for spacecraft or launch vehicle systems are intractable and/or wrong?"

As spacecraft systems have grown more complex, so too has the uncertainty in predictions of their behaviour. To cope with this increase in system uncertainty, researchers are turning to adapted forms of the feedback control techniques commonly used to manage uncertainty in the operation of electromechanical systems and the metabolism of living organisms. In [5], Leveson introduced a model of accidents (STAMP) in which an accident is viewed not as the result as a chain of random events, but as a failure of the system's socio-technical control structure to enforce system safety constraints. Since then, this model has been applied to root cause analysis of accidents and used as the basis for a new, more powerful hazard analysis technique and to perform various types of risk analysis and risk management tasks [6]. One study, described in [7], performed a risk analysis of NASA's response to a *Columbia* Accident Investigation Board recommendation, while another, described in [8] demonstrated a new approach to risk analysis and risk management in the development of space exploration systems, such as the Ares I launch vehicle and Orion spacecraft. Similarly, over roughly the same time, leading systems engineering researchers have called for systems to be designed for change in order to mitigate the effects of uncertainty [9, 10] and the concept of "Real Options," described in [11], has been suggested for the mitigation of financial risk related to market uncertainties for spacecraft constellations [12, 13].

Each of these approaches and applications uses different terminology to describe the basic concept of using feedback to adapt to unpredictable, potentially hazardous system behaviours. In other words, these approaches and applications are pursued to *control* the effects of difficult-to-quantify behaviours in complex engineering systems that are heavily affected by their social and technical elements (i.e. socio-technical systems). In this paper, the concept of treating safety as a *control* problem is elaborated through the introduction of a taxonomy inspired by control theory and dynamical systems.

1.1. Basic Control Theory Concepts

Four conditions are required for effective control of a system: a goal condition, action condition, model condition, and an observability condition [14,15]. The goal defines the desired outcome of the control, the action affects the system state in a manner that will ideally lead to the goal, the model is used to translate the goal into the action, and the observer ascertains the state of the system. The elements of typical control systems that are used to meet these conditions are described in Table 1.

Table 1. Description of Control System Elements

CONTROL SYSTEM ELEMENT:	DESCRIPTION:
Controller	The controller is the logic of the control system (stored in electronics, human minds, regulations, procedures, etc.) that determines the control actions to be pursued. The controller contains a model of the rest of the system, including the other control elements.
Actuator	The actuator is the physical object or agent that imposes the intent of the controller on the system by executing the control action. The ability of the actuator to impose the intent of the controller on the system is referred to as its *control authority*.
Observer	The observer is the element of the control system (e.g., electromechanical sensor, person, etc.) that ascertains the system state.

There are two basic schemes for control: *open-loop* control and *closed-loop* control.

In *open-loop* control, the *observer*, if one exists, does not feed system state information back to the *controller*. In other words, the *controller* does not take real-time system state information into account when determining the appropriate control actions to command the actuator to perform. Thus, in *open-loop* control, the implicit assumption is that the *controller's* model will accurately predict the state of the system throughout the control action.

In *closed-loop* control, the *observer* feeds system state information back to the *controller*. The *controller* compares this information with its model of the desired system state and then determines a control action to move the system into that state. In some control systems, the *controller* uses the information from the *observer* to update its model and change the manner in which it controls the actuator or even to control a different actuator. For example, in the Apollo 13 crisis, the lunar module, an actuator for achieving lunar landing goals, was used as an actuator for survival goals once it became apparent that the landing was not going to happen. Thus, the implicit assumption made for *closed-loop* control is that the c*ontroller's* model will not be able to accurately predict the state of the system prior to and throughout the control action, but it will be able to drive the system to the desired state as information of its present state becomes available.

2. CYCLES OF COMPLEX SYSTEM OPERATION

One of the most fundamental concepts in control theory is the system's *frequency response* to its inputs. When the system's output is viewed as a function of frequency, the two major attributes of this response, the *phase lag* or *delay* and *magnitude*, can be evaluated against two critical principles in system control. The first principle is that if a response at a given frequency for a *closed-loop* system has sufficient *magnitude* and *delay*, the system will become uncontrollable (i.e., the control system will "over-correct" or drive the system away from the desired goal). The second principle is that the control system will take a longer time to converge on the desired goal than it ideally could if all frequencies associated with acceptable *delays* were not of a significant *magnitude*.

Thus, part of the art of control system design is to determine the appropriate frequencies for the control system to use in responding to system inputs. Unfortunately, while the *frequency response* of linear, time-invariant systems can be mathematically represented on a Bode Diagram, it is currently unclear how to represent the *frequency response* of safety constraint controllers (as defined in STAMP) and "Real Options" in complex, socio-technical systems, which are non-linear and time-variant.

Therefore, we propose the *cycles of complex system operation* as a conceptual tool, similar to the system *frequency response*, for identifying appropriate points of leverage for control of the system. A *cycle of complex system operation* is defined as a qualitatively identifiable iteration of goal-seeking behaviour in a system. Each cycle or iteration represents an opportunity to intervene in the goal-seeking behaviour of that cycle or that of another cycle. For example, if

one wants to reverse a risk management decision in the Space Shuttle Program, that reversal could conceivably occur during a mission, after a mission, during routine maintenance, block upgrades of Space Shuttle elements, or even in the design of the Space Shuttle's successor. Consequently, each iteration or cycle in which an intervention does not occur represents a period of system exposure to the hazards underlying the cycle's goal-seeking behaviour.

Before moving into a description of some preliminary archetypes for *cycles of system operation*, several concepts are worth clarifying. The first concept is that each cycle effectively serves as a proxy for frequency in the system response to inputs and will have a frequency associated with it that will be subject to change (this point is of significance because shifts in cycle frequency may present a hazard to the system). The second concept is that though many cycles of system operation will be affected by the phase of the system (i.e., some cycles will end when a specific system lifecycle phase ends), the cycles themselves are not phases. Phases tend to be sequential while *cycles of complex system operation* tend to occur simultaneously but on different timescales (frequencies). The third concept is that each iteration of a specific type of cycle will not necessarily be the same as the iterations proceeding or following it (i.e., the cycles are potentially time-variant). The final concept is that the nature and existence of cycles will be system-specific and thus, it will not be possible to define a universal list. Therefore, the cycles described below are some preliminary examples over a wide range of timescales. The reader is encouraged to identify additional cycles that will be relevant to his or her system of interest.

2.1. Sortie/Loading Cycles

This type of cycle can be thought of as the base unit in the *cycles of complex system operation* taxonomy. If a risk management action for a mission or *sortie* (e.g., Space Shuttle flight) of a system is reversible only in subsequent sorties of that system, it is classified as an *open-loop* action on the Sortie Cycle. For spacecraft and launch vehicle systems, the start of a new Sortie Cycle is most easily defined as the launch because it represents a point of no return for many risk management actions (e.g., most equipment cannot be repaired or replaced if it malfunctions). For a reusable spacecraft, the end of its Sortie Cycle nominally coincides with its return to Earth, while the end of the Sortie Cycle for a spacecraft not returning to Earth coincides with the termination of its functionality.

For certain types of spacecraft and launch vehicle systems (e.g., immovable infrastructure) the concept of a sortie is ambiguous. While a launch pad, for example, may not have a definable sortie per se, it experiences loads (e.g. periods in which the a launch vehicle is at the launch pad, hurricanes, etc.) that limit certain risk management actions and exposes the parts of the overall system to hazards. Informally, the loading of the launch pad can be described as when and to what extent the launch pad is used and/or exposed to certain environmental conditions. Understanding the length and extent of the loadings provides insight into system behaviour, including the identification of periods of heavy use that should be preceded or followed by inspection and maintenance work. Thus, we formally define Loading Cycles as loadings of the system that create hazards for parts of the system and limit risk management alternatives, such as inspections or maintenance that would be available in the absence of the loads.

2.2. Sub-Sortie/Mini-Loading Cycles

With the above definitions of Sortie and Loading Cycles, it is necessary to define Sub-Sortie or Mini-Loading Cycles for cycles that occur on shorter timescales than the standard Sortie or Loading Cycle (cycles that typically occur on longer timescales are defined below). If a Sortie or Loading Cycle is long enough, there will probably be Sub-Sortie and Mini-Loading Cycles where minor inspections, maintenance, software mode transitions, and even upgrades of the system occur. These cycles are not to be confused with the longer timescale inspection, upgrade, and replacement cycles defined below.

2.3. Inspection/Maintenance Cycles

Building upon the concept of Sortie/Loading Cycles, Inspection/Maintenance Cycles provide an opportunity for a risk management intervention between Sortie/Loading Cycles. Inspection/Maintenance can occur after every Sortie/Loading Cycle or after a predetermined or ad hoc series of Sortie/Loading Cycles. Typically, there are multiple Inspection/ Maintenance Cycles occurring simultaneously in a system, each distinguished by type and/or thoroughness of inspection and maintenance. For example, the re-entry system on a reusable vehicle may be inspected thoroughly after every sortie while cracks in structural elements may be inspected after every five sorties.

2.4. Upgrade/Replace Cycles

Opportunities also exist to reverse risk management actions when substantial portions of the system are upgraded or replaced after a single Sortie/Loading or Inspection/Maintenance Cycle or series thereof (e.g., Space Shuttle Main Engine Block Upgrades). Hence we define Upgrade/Replace Cycles to denote the frequency with which major system elements are upgraded or replaced.

2.5. Project Cycles

We define Project Cycles to coincide with timescales spanning the development and operation of major design platforms. In terms of spacecraft and launch vehicle systems, these design platforms can be thought of as reusable spacecraft, launch vehicles (e.g., Ariane V), spacecraft buses, spacecraft constellations, and single use spacecraft designs. A design platform can be upgraded many times over its Project Cycle and potentially reconfigured for each sortie. Furthermore, individual units of the platform (e.g., satellites in the Global Positioning System constellation) can be replaced throughout the Project Cycle.

2.6. Political/Economic Cycles

Political/Economic Cycles are defined here as cycles in which the market or political importance of the system can change significantly. Often, the system has little direct effect on these cycles, but must nonetheless prepare for the changes created by them (some of which may represent a source of time variance in the system's frequency response). Political Cycles are particularly relevant in government projects and range from annual budget cycles to election cycles and cycles of significant turnover in relevant Congressional committees. Economic Cycles are relevant in private projects and represent a window of opportunity for deploying and profiting from the system. With this definition, it is possible to describe the financial failures of the Iridium and Globelstar constellations as examples of over-correction (or inadequate *frequency response*) in the control of system uncertainty. While in both cases, an Economic Cycle provided an input into the system (a market) that could have been converted into a profit; the delays in system response (the constellation Project Cycles) led to deployment of the system after the market began to disappear. In [12], a "Real Options" approach to staged satellite constellation deployment is proposed to better entrain the system response to what we have defined here as an Economic Cycle.

2.7. Enterprise Cycles

In this paper the term *enterprise* is meant to describe a series of Project Cycles inspired by a specific, open-ended goal. An enterprise can coincide with the lifecycle of a single organization, span the lifecycle of several organizations, or describe one of several vastly different endeavours of a single organization (e.g. aeronautics research and human spaceflight at NASA). Though almost all risk management actions are *closed-loop* over their relevant Enterprise Cycle, the risk management philosophy of institutions performing the actions can change tremendously over the course of the enterprise (e.g., Dan Goldin's [16] faster, better, cheaper approach in NASA's unmanned exploration enterprise), thus altering the context and behaviours associated with higher frequency cycles such as Sortie/Loading cycles.

NASA's human spaceflight enterprise, for instance, has changed significantly since its first decade of existence in which the Mercury, Gemini, and Apollo programs were carried out. In [17], the transition of the culture of NASA's human spaceflight enterprise from its heavy research and "hands on" orientation in the Apollo days to its more bureaucratic ways in 1980s is lamented and implicated as a contributing factor in the *Challenger* Accident. While the author of [17] concludes his argument with hope that such changes will be reversed, another author, in a seminal work on organizational structure, presents another potential future for the culture [18]. While both articles provide a similar description of NASA's Apollo-era culture, [18] suggests that bureaucratization is natural for such a culture as it ages and that this change in structure does not necessarily lead to an overall degradation in competency, but a shift in competencies that could be leveraged if properly identified. In either case, the evolution of the enterprise, while gradual, will set the stage for actions occurring on shorter duration cycles (i.e., the evolution will act as a source of time variance in the *frequency response*).

2.8. Trans-Enterprise Cycles

Finally, Trans-Enterprise Cycles are defined here to span multiple enterprises. While it's possible to imagine an enterprise being controlled by a single organization, it's more difficult to imagine the control of multiple, successive enterprises by a single organization. Yet, over time, the actions of individual enterprises can create hazards in the operation of subsequent enterprises. For example, each space related enterprise could contribute to hazardous material accretion (e.g., orbital debris) and/or valuable resource depletion (e.g. in situ water supplies on the Moon) in the operating environment of future enterprises. Thus, while no individual enterprise can maintain control over a Trans-Enterprise Cycle in most cases, it is possible for each enterprise to control its contribution to these cycles through the imposition and adherence to voluntary or mandatory constraints on its operation.

3. TRADE-OFFS BETWEEN OPEN-LOOP AND CLOSED-LOOP CONTROL

Because o*pen-loop* control of hazards relies on models of the system that do not take system performance feedback into account, it is vulnerable to poor estimation of the hazards. *Closed-loop* control, on the other hand, does take system feedback performance into account and includes capabilities that can be thought of as "insurance" against poor hazard estimation. However, a *closed-loop* control action is not necessarily

appropriate simply because it is *closed-loop*. Much like insurance, its value is related to the level of uncertainty in the hazard estimation. Furthermore, as mentioned above in the discussion of *frequency response*, there are two potential weaknesses in *closed-loop* control: under-correction and over-correction. Under-correction occurs when the capability for *closed-loop* control exists in a system and is not utilized when it should be. It represents a "double whammy" of sorts because the undesired effect occurs even after the expense necessary to introduce the *control authority* in the system has been incurred. Alternatively, over-correction occurs when the responses of the control system can be more dangerous or disruptive than non-responses. For instance, Wally Schirra's decision not to use the crew escape system during the launch pad abort of Gemini VI is widely regarded as a prudent choice that saved his mission and perhaps his and Tom Stafford's lives [19, 20].

Not all *closed-loop* control actions are created equal and thus, consideration should be given not only to multiple approaches to *closed-loop* control, but also to whether or not *open-loop* control may be appropriate over a given cycle in a given set of circumstances. On Gravity Probe B, for example, there was a safemode that would reboot the main flight computer if an unacceptable number of Multiple Bit Upsets (MBUs) occurred in a set time interval, regardless of whether or not the corrupted data would ever be accessed [21]. At times, this rebooting of the computer interrupted the mission more than the anomalies. In this situation, an *open-loop* action such as the selection of a memory device with a different physical arrangement of bits would have been more appropriate [2, 21]. Similarly, a better conceived *closed-loop* approach, such as the implementation of an error detection and correction routine capable of automatically correcting MBUs would have effectively eliminated the risks associated with the execution of MBUs without seriously interrupting the mission [2, 21].

It has been shown repeatedly that projects, in the aerospace industry and elsewhere often try to save money in the beginning of the Project Cycle and end up over budget because of cost cutting measures. *Closed-loop* control in operations should not be used as a tactic to delay critical thinking about hazard control. The early design decisions for a system dramatically affect the options for hazard controllability in the later stages of design as well as in operations. If a tough decision looms large early in the design phase, *closed-loop* control should not be viewed as a panacea.

4. APPLICATION OF THE CYCLES OF COMPLES SYSTEM OPERATION CLASSIFICATION SYSTEM TO SELECTED RISK MANAGEMENT ACTIONS

The *cycles of complex system operation* are a qualitative construct for cataloguing the loops that are closed by specific risk management actions. With knowledge of when and how a control loop is closed, one can understand the potential exposure of the system to complications resulting from poor hazard estimation and identify the potential for under-correction and over-correction in trade analyses of these actions. In this section, we describe the application of the *cycles of complex system operation* to commonly used risk management actions. While the list of actions provided here is not exhaustive, it illustrates ways in which designers and operators either build confidence in *open-loop* control over select cycles or utilize performance information over cycles to renew or reverse risk management decisions (i.e., *close-the-loop* on the uncertainty of those decisions).

4.1. Fault Tolerance and Over-design

The **selection of materials and equipment** for spacecraft structures and functions is perhaps one of the most critical processes in spaceflight risk management. Each type of material and piece of equipment has vulnerabilities that place limitations on what the spacecraft can safely do and where it can go safely. In almost all cases, the selection of materials and equipment for a spacecraft is an *open-loop* risk management action over its Sortie Cycle. For single-use spacecraft designs, it is also an *open-loop* action over the Project Cycle of the design. There are, however, limited opportunities for reusable spacecraft, spacecraft buses, and spacecraft constellations to *close-the-loop* on material and equipment selection through ad hoc or pre-planned Upgrade/Replace Cycles.

Because the selection of materials and equipment inevitably involves the tolerance of specific hazards over at least one Sortie Cycle, spacecraft designers often look to build confidence in the system by including safety margins in structural elements and using "high-reliability" components for spacecraft functions. This approach, however, is highly vulnerable to poor estimation of the component reliability and emergent phenomena on the system-level due to the selection of the component. On the Gravity Probe B mission, for example, the on-board digital memory's resistance to MBUs was overestimated by orders of magnitude when the memory device was selected [21]. Though the mission met its data collection requirements, three percent of its data collection opportunities were lost and thousands of employee hours were spent on

investigative and recovery work resulting from the system-level responses to the MBUs [21].

Redundancy provides a limited form of *closed-loop* risk control in system Sortie Cycles in instances where the sortie can effectively be descoped and/or terminated early and repeated at a later time. Specifically, redundancy can give operators and/or automation an alternative means to perform a safety critical function when the primary means (e.g. component) for completing the function degrades or fails. This opportunity to rely on an alternative means to perform the critical function allows operators to *close-the-loop* on the hazard by safely terminating the sortie or changing the manner in which it is carried out. For example, there have been two Space Shuttle missions, STS-2 and STS-83, in which a fuel cell has failed or degraded to an unacceptable level and the crew has been forced to return to Earth utilizing the redundant fuel cells [22]. In both cases, the objectives of those missions were ultimately accomplished in subsequent Space Shuttle missions.

Unfortunately, redundancy usually provides *open-loop* risk control for hazards in the Sortie Cycles of systems. Essentially, while redundancy can be effective at mitigating risks for wear and tear hazards (i.e. hazards that are instantiated after excessive use of a system component) and random quality-related hazards (i.e. hazards that are instantiated by errors in system manufacture, maintenance, and operation), it is largely ineffective when there are flaws in the design of the redundant components and/or the approach used to operate them. It is possible for both the primary and redundant components to fail to perform their assigned function within a short time span, especially if they are identical (e.g., the O-rings on the Space Shuttle Solid Rocket Booster joints for *Challenger's* last mission [23]). Such situations prevent a graceful termination of the sortie. This is especially true in highly dynamic Sortie Sub-Cycles (such as the launch cycle of a spacecraft) and in systems in which only one sortie is possible (e.g. deep space probes).

4.2. Safing Systems

Crew escape systems are used in human spaceflight to safely separate the crew from malfunctioning boosters during launch and from re-entry vehicles incapable of landing during the crew's return to Earth. As was the case for the early Soviet human spaceflight missions, crew escape systems can be used as part of nominal system operations [24], however, they are most frequently used as a source of *closed-loop* control of launch/landing vehicle hazards on the Sortie Cycle. During the Soyuz T-10-1 mission, for example, the crew escape system was successfully used to separate the crew capsule from the booster as it exploded on the launch pad [25]. Because crew escape systems tend to have a significant impact on the architecture of the spacecraft, designers sometimes opt to exclude them from the design. The Space Shuttle initially had no crew escape system; however, after the *Challenger* accident limited crew escape capability was added [26]. This risk management decision with respect to the crew escape capability now available represents *closed-loop* control on the Project Cycle and *open-loop* control over the Upgrade Cycle (i.e., a reversal of this decision was only possible through an upgrade). There still are, however, significant portions of the launch phase where the crew escape capability will be ineffective and thus, the ability to add that capability for those portions of the launch will have to wait for the next Project Cycle of NASA's human spaceflight enterprise.

Safemodes allow the system upon detection of a problem to move into a state from which an operator can safely diagnose the problem and bring the spacecraft back online. For the most part, safemodes represent the *closed-loop* risk management over the Sortie Cycle. Certain aspects of them, however, can be subject to *open-loop* control over Inspection/ Maintenance, Upgrade, and even Project Cycles. Each safemode relies on instrumentation to detect the anomalous situations. This instrumentation requires hardware and software and appropriate settings for sampling rate and the safemode threshold. Sampling rates and thresholds can be controlled in a *closed-loop* manner over the Sortie Cycle if they are adjustable throughout the sortie. Instrumentation hardware, however, can fail or degrade over the course of a sortie and will not be replaceable until a subsequent Sortie Cycle. Furthermore, certain problems require specific hardware for detection and thus, if it is discovered during a Sortie Cycle that new hardware is needed, it may not be possible add that hardware without an upgrade or new vehicle design.

Immersive simulations of contingencies—not to be confused with computer simulations used for design or research—create a virtual environment (e.g. spacecraft mock-up, simulated data piped into the actual operation facilities, etc.) for system operators to rehearse contingency procedures. In spaceflight operations such simulations are used most frequently to train operators (i.e. refine their mental model of system behaviour). Additionally, high fidelity simulations are used to work out bugs in both standard and ad hoc procedures. Thus, immersive simulations are used for both short-term confidence building in controller mental models and long-term procedural evolution. Therefore, they provide *open-loop* control of human operator performance over specific Sub-Sortie Cycles or even entire Sortie Cycles (if they are not performed by the controllers during the sortie) and *closed-loop* control

over procedural evolution throughout longer timescale cycles.

5. FUTURE WORK

Future work will probe further into the design principles and heuristics that can be derived from a notion of *frequency response* in complex socio-technical systems. Delays in *closed-loop* control actions for socio-technical systems can lead to over- and under-corrections, just as they do in linear, time-invariant systems. Such delays are inherent in the selection of both the *cycle of complex system operation* to control over and the type of *control authority* used for the control. The cycles defined in this paper will be used as a qualitative construct to categorize control actions and *control authority* types pursued in past accidents/incidents and current operations. The cycle definitions themselves may be expanded and/or iterated to better address system boundary definition issues and emerging "micro-theories" of cycle coupling. Additionally, tools, analogous to the Bode Diagram, for visualizing cycle characteristics will be examined for their usefulness in the design process.

6. CONCLUSIONS

The taxonomy laid out in this paper provides a vocabulary to characterize specific risk management actions in terms of the basic control theory concepts of *open-loop* and *closed-loop* control. Though the flight controllers for Apollo 13, for example, may not describe their actions this way, they were in fact controllers of Sortie Cycle uncertainties that recognized that a portion of their *control authority* (the Lunar Module) could be used to drive their system to a safe state. Describing their actions in these terms helps to elucidate how they and others have treated safety as a control problem.

Though this taxonomy for hazard controllability is in its early stages and much analysis remains to identify many of the key spacecraft system design and operation heuristics and principles to follow from it, the taxonomy provides a language to discuss today the tradeoffs between *open-loop* and *closed-loop* control. At times, commonly used *open-loop* techniques to reduce risk, such as material selection, and techniques to *close-the-loop* on an uncertainty will seem at odds due to resource constraints and/or the tendency of *open-loop* solutions to occasionally inhibit the flexibility necessary in loop-closing actions. It is in these situations, perhaps more than in any other, that the authors hope that the taxonomy provided here will be invoked to enlighten the discussion of the appropriate course of action.

7. ACKNOWLEDGEMENTS

The authors would like to thank our system safety research colleagues (Dr. Betty Barrett, Prof. John Carroll, Prof. Joel Cutcher-Gershenfeld, Dr. Nicolas Dulac, and Prof. Jeffrey Hoffman), for their constructive comments on the subject matter of this paper.

This research was supported by USRA Cooperative Agreements 05115-C1P2-01 and NSF Grant SES-0527660.

8. REFERENCES

1. Leveson, N. G., *Safeware: System Safety and Computers*, Addison-Wesley Publishing Company, 1995.
2. Owens, Brandon D. and Nancy G. Leveson, "A Comparative Look at MBU Hazard Analysis Techniques," *Proceedings of the 9th Annual Military and Aerospace Programmable Logic Devices International Conference (MAPLD),* Washington, D. C., Sept. 26-28, 2006.
3. Apostolakis, George E., "How Useful is Quantitative Risk Assessment?" *Risk Analysis*, Vol. 24, No. 3, 515-520, 2004.
4. Laracy, Joseph R., "Addressing System Boundary Issues in Complex Socio-Technical Systems," *Proceedings of the 5th Annual Conference on Systems Engineering Research (CSER)*, paper 63, Hoboken, NJ, March 14-16, 2007.
5. Leveson, Nancy G., "A New Accident Model for Engineering Safer Systems," *Safety Science*, Vol. 42, No. 4, pp. 237-270, April 2004.
6. Leveson, Nancy G., *System Safety Engineering: Back to the Future*, Cambridge, MA, 2006. Available online at: http://sunnyday.mit.edu/book2.html
7. Dulac, Nicolas; Nancy Leveson; David Zipkin; Stephen Friedenthal; Joel Cutcher-Gershenfeld; John Carroll; and Betty Barrett, "Using System Dynamics for Safety and Risk Management in Complex Engineering Systems," *Proceedings of the 2005 Winter Simulation Conference*, Florida, December 4-7, 2005.
8. Dulac, Nicolas; Brandon D. Owens; and Nancy G. Leveson, "Modelling Risk Management in the Development of Space Exploration Systems," *Proceedings of the 2nd Annual International Association for the Advancement of Space Safety (IAASS) Conference*, May 14-16, Chicago, IL, 2007.
9. McManus, Hugh and Daniel Hastings, "A Framework for Understanding Uncertainty and its Mitigation and Exploitation in Complex Systems," *IEEE Engineering Management Review*, Vol. 34, No. 3, pp. 81-94, 2006.
10. Fricke, Ernst and Armin P. Schulz, "Design for Changeability (DfC): Principles To Enable Changes in Systems Throughout Their Entire Lifecycle," *Systems Engineering*, Vol. 8, No. 4, pp. 342-359, 2005.

11. De Neufville, Richard, "Real Options: Dealing with Uncertainty in Systems Planning and Design," *Integrated Assessment*, Vol. 4, No. 1, pp. 26-34, 2003.
12. De Weck, Olivier L.; Richard De Neufville; and Mathieu Chaize, "Staged Deployment of Communications Satellite Constellations in Low Earth Orbit," *AIAA Journal of Aerospace Computing, Information, and Communication*, Vol. 1, No. 3, pp. 119-136, 2004.
13. Hassan, Rania; Richard De Neufville; Olivier De Weck; Daniel Hastings; and Daniel McKinnon, "Value-at-Risk Analysis for Real Options in Complex Engineered Systems," *2005 IEEE International Conference on Systems, Man and Cybernetics*, Vol. 4, pp. 3697-3704, Hawaii, Oct. 10-12, 2005.
14. Ashby, W. R., *An Introduction to Cybernetics*, Chapman and Hall, London, UK, 1956.
15. Conant, R. C. and W. R. Ashby, "Every Good Regulator of a System Must Be a Model of that System," *International Journal of System Science*, Vol. 1, No. 2, pp. 89-97, 1970.
16. Lambright, W. Henry, "Leading change at NASA: The case of Dan Goldin," *Space Policy*, Vol. 23, No. 1, pp. 33-43, 2007.
17. McCurdy, Howard E., "The decay of NASA's technical culture," *Space Policy*, Vol. 5, No. 4, pp. 301-310, 1989.
18. Mintzberg, Henry, "Organization design: fashion or fit?" *Harvard Business Review*, Vol. 59, No. 1, pp. 103-116, 1981.
19. Kranz, Gene, *Failure is Not an Option: Mission Control from Mercury to Apollo 13 and Beyond*, Berkeley Books, New York, New York, 2000.
20. Kraft, Christopher C., *Flight: My Life in Mission Control,* Penguin Putnum Inc., New York, New York, 2001.
21. Owens, Brandon D.; Mike E. Adams; William J. Bencze; Gaylord Green; and Paul Shestople, "The Effects of Radiation Events on Gravity Probe B," *Proceedings of the 9th Annual Military and Aerospace Programmable Logic Devices International Conference (MAPLD),* Washington, D. C., Sept. 26-28, 2006.
22. Jenkins, Dennis, *Space Shuttle: The History of the National Space Transportation System-The First 100 Missions*, Midland Publishing, Hinckley, UK, 2002.
23. Rogers, William P. (Chair), *Report of the Presidential Commission on the Space Shuttle Challenger Accident.* Government Accounting Office, June 1986.
24. Ravnitzky, M. J.; S. N. Patel; and R. A. Lawrence, "To fall from space – Parachutes and the space program," *Proceedings of the 10th AIAA Aerodynamic Decelerator Systems Technology Conference*, pp. 222-232, Cocoa Beach, FL, April 18-20, 1989.
25. Hall, Rex D. and David J. Shayler, *Soyuz: A Universal Spacecraft*, Springer-Praxis, 2003.
26. National Aeronautics and Space Administration, *Implementation of the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident*, Report to the President of the United States of America, Washington, D.C., June 1987.