Resilient Space Habitat Design Using Safety Controls

Robert Kitching[1]; Hunter Mattingly[2]; Dale Williams[3]; and Karen Marais[4]

[1]Graduate Research Assistant, School of Aeronautics and Astronautics, Purdue Univ., West Lafayette, Indiana
[2]Undergraduate Research Assistant, School of Aeronautics and Astronautics, Purdue Univ., West Lafayette, Indiana
[3]Undergraduate Research Assistant, School of Aeronautics and Astronautics, Purdue Univ., West Lafayette, Indiana
[4]Associate Professor, School of Aeronautics and Astronautics, Purdue Univ., West Lafayette, Indiana

ABSTRACT

Space habitats will involve a complex and tightly coupled combination of hardware, software, and humans, while operating in challenging environments that pose many risks, both known and unknown. It will not be possible to design habitats that are immune to failure, nor will it be possible to foresee all possible failures. Rather than aiming for designs where "failure is not an option," habitats must be resilient to disruptions. We propose an approach to resilient design for space habitats based on the concept of safety controls from system safety engineering. We model disruptions using a state-and-trigger approach, where the space habitat is in one of three distinct states at each time instance: nominal, hazardous, or accident. We use safety controls as ways of preventing a system from entering or remaining in a hazardous or accident state. We develop a safety control option space for the habitat, from which designers can select the set of safety controls that best meet resilience, performance, and other system goals. The safety control option space is likely to be large, accordingly, we design a database that links safety controls to the applicable states and triggers. We demonstrate our approach on the early design stage of a Martian space habitat.

INTRODUCTION

Space habitats will involve a complex and tightly-coupled combination of hardware, software, and humans. These habitats will be embedded in challenging environments, whether the microgravity of cislunar space, or the surface of the Moon or Mars. These harsh environments pose many risks, both known and unknown. In an extraterrestrial environment, it is inevitable that things will go wrong. Failures and faults may include component failings, operator or software implementing the wrong actions, or dysfunctional interactions between correctly functioning components. Space habitat systems will be safety-critical, meaning that a "failure might endanger human life, lead to substantial economic loss, or cause extensive environmental damage" (Knight, 2002). It will not be possible to design habitats that are immune to failure, nor will it be possible to foresee all possible failures. Therefore, rather than aiming for designs where "failure is not an option", we must design habitats that are resilient to the inevitable failures that will occur. Resilience is the ability of a system, process or organization to react to, survive, and recover from disruptions (Uday & Marais, 2015). Designing for resilience ensures that a system can *adapt* before or during an encounter with a threat, *prepare for* a threat in advance to enable recovery following an encounter, *withstand* a threat by retaining partial or full functionality following an encounter, or *recover from* a threat by restoring partial or full functionality following an encounter.

Conventional binary and event-based safety and reliability design approaches cannot respond adequately to the level of complexity found and rapid failure responses needed in space habitat systems. Traditional, component-centric approaches to risk identification, assessment, and management, manage risk by preventing failures, or reducing the effects of failures. The weaknesses and limitations of these approaches have been well-documented, and center about their inability to properly address software, human interactions, and accidents that do not involve component failure, but rather arise as a result of dysfunctional interactions. The more complex the system, the less applicable assumptions like independence of failures become. When we include the potential for different environmental conditions, not all of which may be foreseen either in terms of their type (e.g., physical/chemical characteristics of particulates in the atmosphere) or extent (e.g., frequency/intensity of storms), identifying and assessing risk becomes even more challenging. Most approaches to hazard identification (e.g., HAZOP) are essentially sophisticated checklists. In complex unprecedented systems hazard identification is especially difficult because many of the hazards are unprecedented or cannot be foreseen. While failure modes, effects, (and criticality) analysis (FMEA/FMECA) may also help with hazard identification, it requires each failure to be considered individually and independently from other failures. Event Trees and Event Sequence Diagrams are also inductive techniques where a basic initiating event is propagated to its potential consequences. The analyst must know which components or initiating events to consider—in a complex system like a space habitat it is infeasible to analyze all of them (Leveson et al., 2009). Finally, these techniques do not allow consideration of interconnected or otherwise dependent failures.

What is needed for resilient space habitats is an approach that (1) goes beyond the event-centric failure model underlying conventional risk-based design, and (2) helps identify designs that are prepared for both foreseen and unforeseen risks. To address (1), we propose an approach that uses hazardous states and triggers into those states as its basic elements, rather than component and other failures. We then use safety controls to prevent transition to hazardous states, or to exit from hazardous states. To address (2), we propose to develop metrics that assess how well safety controls address their target disruptions or hazardous states, and also their potential to address disruptions or hazardous states for which they were not originally intended.

In this paper, we present our progress on (1): developing a state-based model of a space habitat and identifying potential safety controls. The next section lays out the concept of safety controls and presents an approach for developing safety controls given potential hazardous states and disruptions. The second half of this paper shows how we have applied this approach to developing a set of safety controls for a Martian habitat system. We conclude the paper with a plan for how we will use these resilience design concepts in the design and operation of a space habitat.

A SAFETY-CONTROL APPROACH TO DESIGN FOR RESILIENCE

We consider safety as a control problem, where safety is an emergent property of the system. Rasmussen (1997) pioneered the effort to use control theory in accident modeling: he argued that accidents are often caused not by a coincidence of independent failures but instead reflect a systematic migration of organizational behavior to the boundaries of safe behavior under pressure toward cost-effectiveness in an aggressive, competitive environment. The concept of “boundaries of safe behavior” introduces the conceptualization of regions of safe behavior of the system and regions of unsafe behavior of the system. Rather than assessing faults and failures and reducing their effects, control-theoretic approaches assess risk based on how well the system is kept within safe operating states, or conversely, how well it is kept out of unsafe, or hazardous, states (Leveson et al., 2009). Humans and organizations can adapt to foreseen and unforeseen threats and still maintain safety if they stay within the area bounded by safety constraints (Leveson, 2004). Leveson's (2004) Systems-Theoretic Accident Model and Processes (STAMP) model uses systems theory to show that accidents occur when disturbances, failures, or dysfunctional interactions among system components are inadequately controlled by safety-related constraints on the development, design, and operation of the system. By moving away from the component-centric view of risk, these approaches account for all types of accidents, including those that arise without any components failing.

Our approach considers systems as being in one of three types of states: nominal, hazardous, or accident. A state is a segment of time wherein a system exhibits a particular behavior. A system can be in one and only one state at any given point in time. A nominal state is when the system is within the boundaries of safe behavior. A hazardous state is when the system is in a state that, if left uncontrolled, will result in an accident or loss of life. The system transitions from one state to another via triggers. Triggers occur at instants of time and cause a system to transition between states or remain in the same state (Rao & Marais, 2020). Each state must have at least one entering trigger. Disruptions are a type of trigger that instigates transition to a hazardous or accident state.

We use safety controls to maintain the system in the nominal state(s), or, if it does transition to a hazardous or accident state, return it to a nominal state. A safety control is any aspect of the system design or operation that maintains the system in a nominal state, prevents the system from propagating to a hazardous state, or restores the system from a hazardous or accident state to a nominal state, as shown in Figure 1. In this example, we are concerned with a possible pressure loss inside the habitat due to a micrometeoroid impact. For convenience, we omit the implied entry trigger into the first nominal state. We use safety controls at different points to respond to a disruption. We model the micrometeoroid impact as an initiating disruption that could cause a breach in the habitat structure, triggering a transition to the hazardous state that the *habitat is losing pressure*. We can use safety controls at the time of the disruption to prevent the system from entering a hazardous state, for example in Figure 1 we use *habitat structural protection strong enough to withstand impact*. If no action is taken, the habitat may further deteriorate into a state of *unlivable pressure environment*. We can use safety controls after the time of the disruption to prevent the system from propagating to an accident state, such as in Figure 1 *crew implements oxygen masks,* or regain the system performance to a nominal state (the green arrow). Safety controls appear either as transition (to hazardous or accident state) preventers, or as triggers away from hazardous or accident states. In Figure 1, the safety control *repair breach* is a trigger away from a hazardous state.

Using the state and trigger model as a basis, we propose the approach shown in Figure 2 for identifying safety controls:

Step 1 and 2: Identify Disruptions and Hazardous States (HS): First, we use established techniques from other fields (e.g., HAZOP) and domain expertise (e.g., NASA's lessons-learned database), to create a diverse (but not necessarily complete) set of disruptions and hazardous states from which to begin. We add to this set of disruptions and hazardous states as the design matures and more information is available about the habitat.

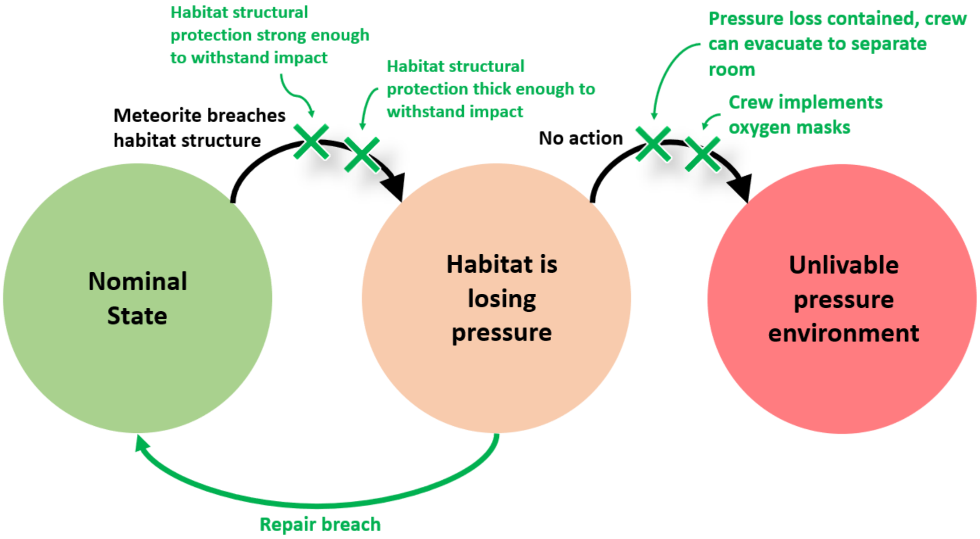
Habitat structural protection strong enough to withstand impact
Habitat structural protection thick enough to withstand impact
Pressure loss contained, crew can evacuate to separate room
Crew implements oxygen masks
Meteorite breaches habitat structure
No action
Nominal State
Habitat is losing pressure
Unlivable pressure environment
Repair breach

Figure 1: Example State and Trigger Model.

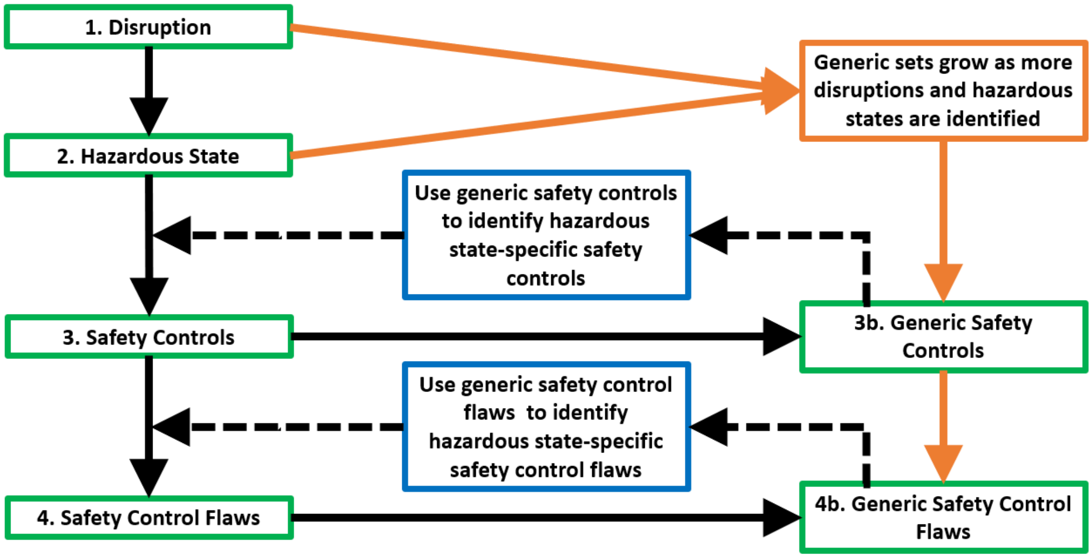
1. Disruption
2. Hazardous State
3. Safety Controls
4. Safety Control Flaws
Generic sets grow as more disruptions and hazardous states are identified
Use generic safety controls to identify hazardous state-specific safety controls
3b. Generic Safety Controls
Use generic safety control flaws to identify hazardous state-specific safety control flaws
4b. Generic Safety Control Flaws

Figure 2: Approach for Identifying Safety Controls

Step 3: Develop safety controls for the Hazardous State: Next, we use our knowledge in systems engineering, system safety, and of past accidents and incidents to develop safety controls that are designed to address these hazardous states. As safety controls are identified throughout the design process, we identify the underlying principle of each safety control and generate a corresponding generic safety control. Generic controls are groupings of safety controls based on their method or principle of control. We use these generic safety controls to develop more safety controls for different kinds of disruptions and hazardous states, identifying and using principles from system safety engineering to categorize controls and expand their applicability. We term the resulting set of potential safety controls the *safety control option space*.

Step 4: Identify control flaws: Next, we identify how controls may be or become ineffective. Identifying control flaws allows for improvement of the controls as the design progresses.

The process is necessarily iterative—we expect to continuously identify additional disruptions and hazardous states, which, in turn will require safety controls. Further, we will also apply it at different levels of abstraction, by flowing system-level states and triggers through to lower levels. The result of this process will be a large set of hazardous and accident states, initiating disruptions, triggers, and safety controls.

In the next section, we discuss the design and development of a database to record and manage such a set.

APPLICATION TO RESILIENT SPACE HABITATS

In this section we discuss our progress to date in identifying, linking, and recording disruptions, states, triggers, and safety controls for a space habitat and storing them in a database.

We consider for our case study a conceptual Mars surface habitat. The habitat consists of a group of connected domes in which the crew lives and performs day to day activities. The habitat has radiation and thermal protection, a photovoltaic power unit, an Environmental Control and Life Support System (ECLSS), and some autonomous and robotic capabilities. A further breakdown of the habitat systems is shown in Figure 3. The crew spend months at a time in the habitat due to mission constraints on getting to and from Mars, and limited ground control support is available. The habitat must be designed to adapt to the harsh environment, and resilient against possible disruptions. Here we demonstrate Steps 1 to 3 of our approach. We leave Step 4 as an item for future work.

Step 1: Identify Disruptions

We generated a preliminary list of disruptions by identifying the kinds of threats the habitat may encounter on Mars. Table 1 shows an excerpt of this list. For example, some of the more obvious disruptions we consider are a micrometeoroid impact to the habitat, ionizing radiation, or seismic activity in the area of the habitat. We also consider events like material outgassing, large variations of external temperature, and dust accumulation on the habitat.

Table 1: Preliminary List of Disruptions to Martian Habitat

Disruptions to Martian Habitat
High winds cause dust and debris to impact habitat
Ionizing radiation (including Galactic Cosmic Radiation)
Rapid rise in external temperature
Rapid decrease in external temperature
Extreme high external temperature
Extreme low external temperature
Outgassing of materials
Cold welding causes mechanical parts to fuse
Micrometeoroids impact habitat
Impact of ejecta
Seismic activity within/near habitat
Non-ionizing radiation
Dense dust surrounds habitat

Step 2: Identify Hazardous States

Next, we generate an initial list of possible hazardous states. To determine how disruptions affect the habitat and how the different functions of the habitat will respond to these disruptions, we break the habitat down into its constituent systems, as shown in Figure 3. For example, the structural system is composed of the parts of the habitat that contribute to the physical integrity of the habitat. The radiation protection system may include subsystems like multi-layered insulation or a regolith layer. Many of these systems are interconnected, such as the water recovery and management system providing water for the oxygen generation system through electrolysis, or more obviously the control system, which receives inputs from the sensor management system on habitat setpoints and works to distribute power to many of the other systems to maintain habitat functionality.

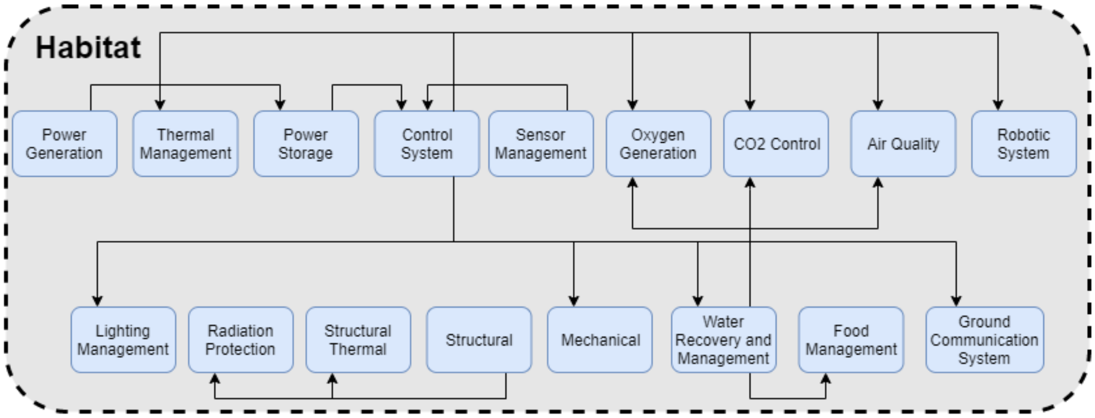

Figure 3: Habitat Systems and Resource Dependencies

This decomposition facilitates identifying and tracking how an initial disruption may propagate through the habitat. For example, Figure 4 shows how the effects of an initial micrometeoroid impact cascade through the habitat. The three hazardous states resulting from a micrometeoroid impact are of immediate concern and should be addressed through human or automated intervention. However, a performance loss in the habitat sensor management system could have more impactful habitat performance implications because of the number of systems that take inputs from the control system, which relies on the sensor management system. We use these system dependencies to record how a single disruption can cause multiple hazardous states in the system it directly impacts, and further cause hazardous states in systems that are dependent on other disrupted systems.

Step 3: Develop safety controls

Table 2 shows how we use the disruptions and hazardous states from Figure 1 to identify safety controls.

The disruption may also propagate through the habitat, creating additional hazardous states and triggers to those states, as illustrated in Figure 4. These triggers and hazardous states, in turn, may be addressed with safety controls. The disruptions and their propagation quickly result in a large space of states, triggers, and potential safety controls. In the example, the initial list of 19 disruptions resulted in 180 interconnected hazardous states. Although the final set of selected safety controls will not necessarily directly address each hazardous state or disruption, the total number of states and disruptions (199) provides a reasonable initial estimate of the potential size of the safety control option space. We use a relational database and network representation to record and archive the resulting large data set, as discussed next.

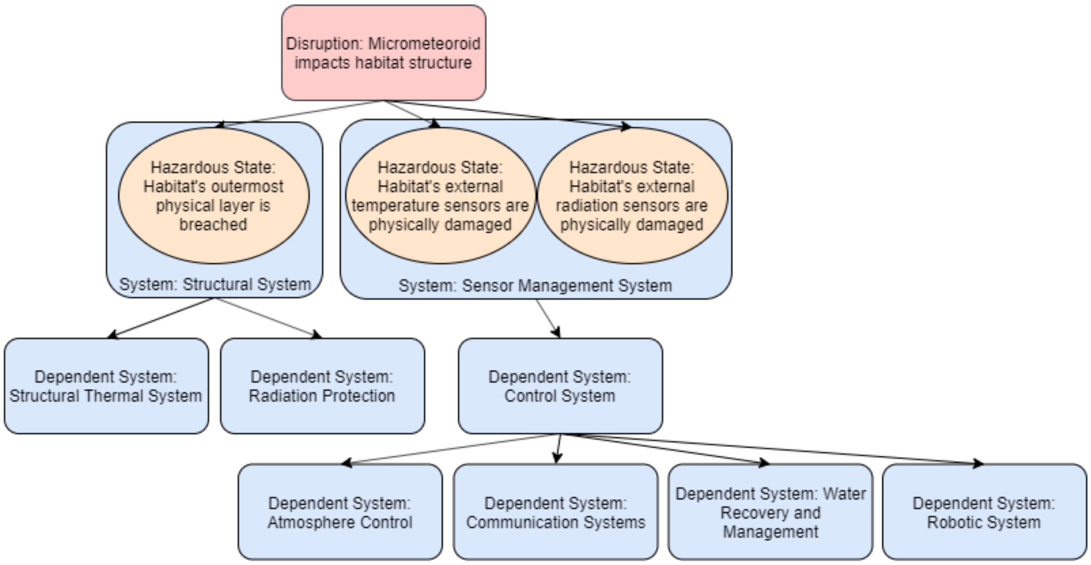
Disruption: Micrometeoroid impacts habitat structure
Hazardous State: Habitat's outermost physical layer is breached
System: Structural System
Hazardous State: Habitat's external temperature sensors are physically damaged
Hazardous State: Habitat's external radiation sensors are physically damaged
System: Sensor Management System
Dependent System: Structural Thermal System
Dependent System: Radiation Protection
Dependent System: Control System
Dependent System: Atmosphere Control
Dependent System: Communication Systems
Dependent System: Water Recovery and Management
Dependent System: Robotic System

Figure 4: Disruption propagation through the habitat systems

Table 2: Identification of Safety Controls for Example Disruptions, Hazardous States, and Triggers

Disruption, Hazardous State, or Trigger	**Safety Control**
Disruption: Micrometeoroid breaches habitat structure	Habitat structural protection strong enough to withstand impact
Disruption: Dust storm impacts habitat	Ability to remove dust contaminants with humans or robot repair agents
Hazardous state: Weakened habitat thermal protection	Ability to increase heat output to meet temperature demand
Hazardous state: Power unit damaged, degraded functionality	Ability to use backup power source

Disruptions, Hazardous States, and Safety Control Network

We use Microsoft Access to store the data in tables that are organized in a way that allows us to link relationships between cells where appropriate. The data is formatted for export to Matlab, where we use the data to create a directed network, linking the cells based on their relationships. Figure 5 shows the resulting failure network. The network is formatted in a layered orientation to illustrate the propagation from the nominal state (blue node), to the disruptions (magenta nodes), to the hazardous states (red nodes). To simplify the diagram, where two hazardous states are connected by the No Action trigger, we connect them directly.

The network contains 200 nodes (1 nominal state, 180 hazardous states and 19 triggers) and 728 edges. Hazardous states are organized in three levels: subsystem level, system level, and habitat level. Habitat level hazardous states include states that directly affect the living conditions in the habitat, such as *Hazardous chemicals present in habitat*, *Internal temperature above livable condition*, and *Habitat has no electrical power*. Referring to the failure network, we create layers of safety controls at the subsystem and system level to prevent transition to the habitat level hazardous states. Next, we illustrate this process using an example disruption.

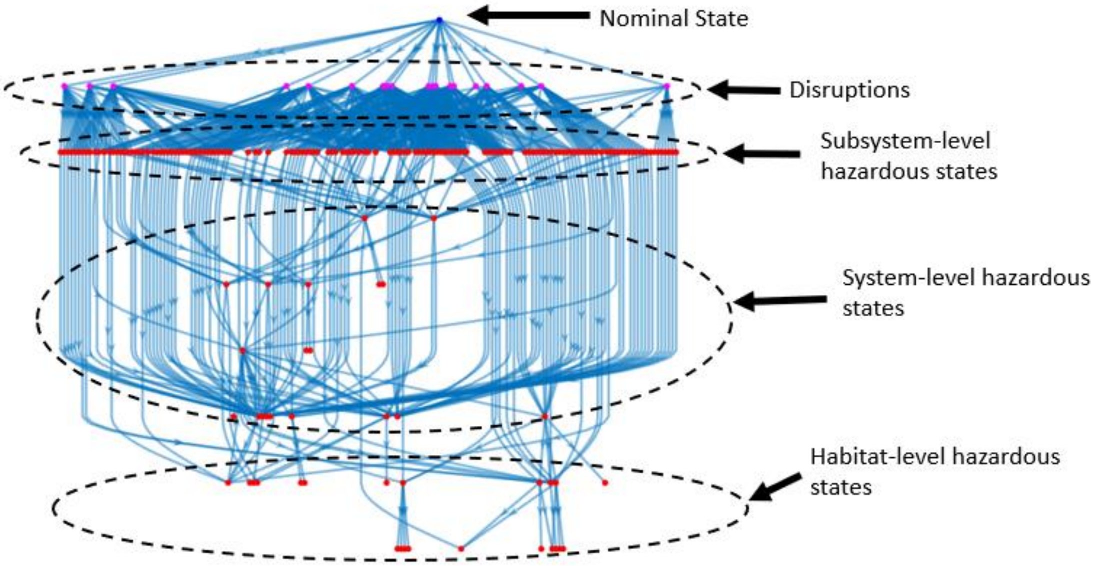
Nominal State
Disruptions
Subsystem-level hazardous states
System-level hazardous states
Habitat-level hazardous states

Figure 5: Martian Habitat Failure Network

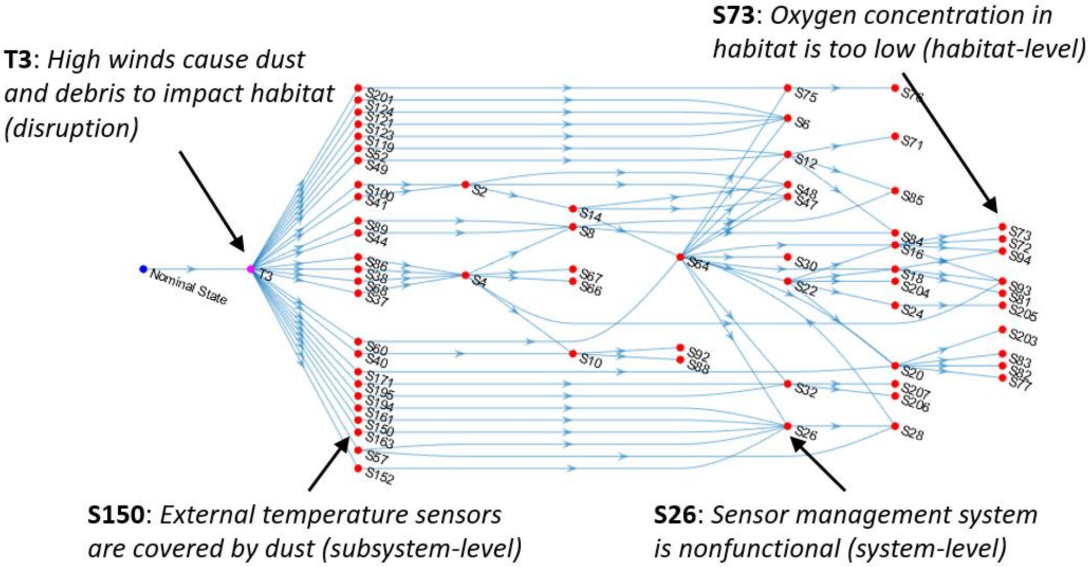
T3: *High winds cause dust and debris to impact habitat (disruption)*
S73: *Oxygen concentration in habitat is too low (habitat-level)*
S150: *External temperature sensors are covered by dust (subsystem-level)*
S26: *Sensor management system is nonfunctional (system-level)*
Nominal State
T3
S201
S124
S121
S123
S119
S52
S49
S100
S41
S89
S44
S86
S38
S68
S37
S60
S40
S171
S195
S194
S161
S150
S163
S57
S152
S2
S4
S14
S8
S67
S66
S10
S92
S88
S64
S75
S6
S12
S48
S47
S30
S22
S32
S26
S7
S71
S85
S84
S16
S18
S204
S24
S20
S207
S206
S28
S73
S72
S94
S93
S81
S205
S203
S83
S82
S77

Figure 6: Propagation of the "High winds cause dust and debris to impact the habitat" disruption through the Martian Habitat Failure Network

Figure 6 shows the 66 identified hazardous states that may result from the disruption "High winds cause dust and debris to impact the habitat" (**T3**). We model **T3** as directly leading to 25 potential hazardous subsystem states. Allowing these subsystems to remain in hazardous states may result in the disruption propagating to one or more of 15 system level hazardous states. Further, failure to control a system-level hazardous state could lead to one of 26 habitat level hazardous states. Figure 7 shows one path that may result when the **T3** disruption occurs to the habitat starting in a nominal state. The disruption begins by covering the external temperature sensors in dust. These sensors are a subsystem of the Sensor Management System. The sensors are therefore in hazardous state **S150**: *external temperature sensors are covered by dust*. If the sensors are covered in dust, they cannot give proper readings, rendering the Sensor Management System nonfunctional (**S26**). Tracking system dependencies, we identify an additional 32 hazardous states either at the system level or at the habitat level that may cascade from **S150**. Of these states, we identify one at the habitat level—**S73**: *Oxygen concentration in habitat is too low*.

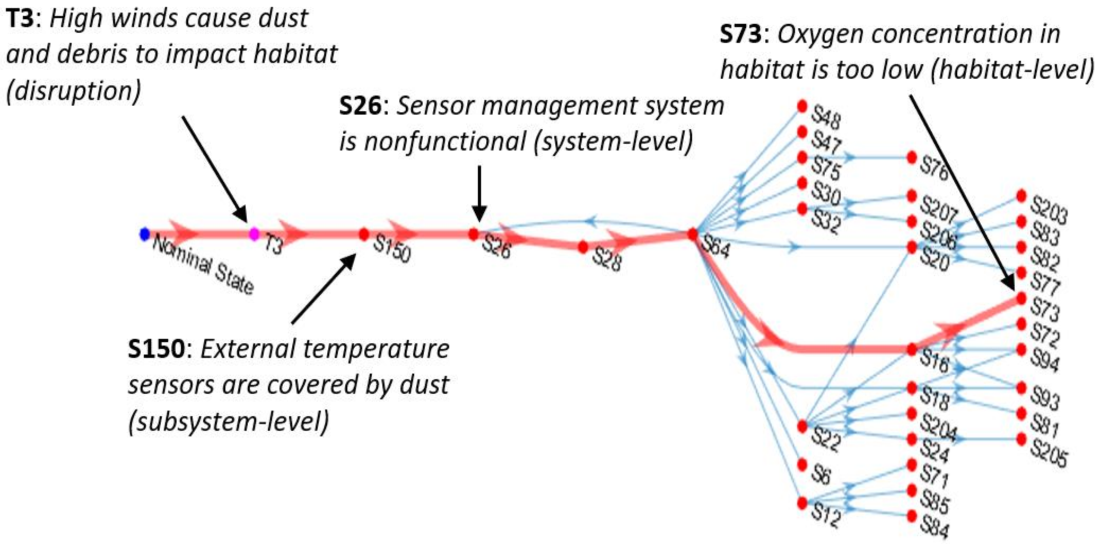
T3: *High winds cause dust and debris to impact habitat (disruption)*
S26: *Sensor management system is nonfunctional (system-level)*
S73: *Oxygen concentration in habitat is too low (habitat-level)*
S150: *External temperature sensors are covered by dust (subsystem-level)*
Nominal State
T3
S150
S26
S28
S64
S48
S47
S75
S30
S32
S76
S207
S206
S20
S203
S83
S82
S77
S73
S72
S94
S16
S18
S204
S24
S71
S85
S84
S93
S81
S205
S22
S6
S12

Figure 7: Path from Nominal State, through hazardous state S150, to habitat level hazardous state S73: *Oxygen concentration in habitat is too low*

Considering Figure 7, there are therefore several points in the network where intervention can prevent the eventual occurrence of **S73**. Table 3 shows examples of safety controls along this path. We chose one hazardous state from each level (subsystem: **S150**, system: **S26**, and habitat: **S73**) and designed three safety controls for each hazardous state.

Figure 8 shows the safety controls (green) applied to the failure path in Figure 7. We apply **SC1-S150** and **SC2-S150** to return the habitat to the nominal state. The remainder of the safety controls in this case study prevent the habitat from propagating to a habitat-level hazardous state.

We design safety controls for disruptions and at all levels of hazardous states. At the subsystem level, we aim to withstand a specific disruption, at the system level we ensure the habitat systems can prepare for a threat in advance and adapt during an encounter, and at the habitat level we ensure the safety of the crew while taking measures to mitigate the threat. Unlike Event Sequence Diagrams which track failures of basic components, safety controls create layers of defense against disruptions at each level of the habitat.

Table 3: Hazardous States and their Safety Controls

Hazardous State ID	Hazardous State Description	Hazardous State Level
S150	External temperature sensors covered by dust	Subsystem

Safety Control ID	Safety Control Description	General Safety Control	Return to Nominal State?
SC1 – S150	Ability to remove dust from temperature sensors	REMOVE SOURCE	Yes
SC2 – S150	Ability to sense temperature despite dust	WITHSTAND SOURCE	Yes
SC3 – S150	Ability to switch to backup temperature sensors	PHYSICAL REDUNDANCY	No

Hazardous State ID	Hazardous State Description	Hazardous State Level
S64	Power distribution system is nonfunctional	System

Safety Control ID	Safety Control Description	General Safety Control	Return to Nominal State?
SC1 – S64	Ability to repair power distribution system	REPAIR CONTROL	No
SC2 – S64	Ability to isolate power distribution failure	CONTAIN FAILURE	No
SC3 – S64	Ability to switch to backup power distribution system	PHYSICAL REDUNDANCY	No

Hazardous State ID	Hazardous State Description	Hazardous State Level
S73	Oxygen concentration in habitat is too low	Habitat

Safety Control ID	Safety Control Description	General Safety Control	Return to Nominal State?
SC1 – S73	Ability for crew to use oxygen masks	REMOVE HUMANS FROM SOURCE	No
SC2 – S73	Ability for crew to evacuate until oxygen concentration is restored	REMOVE HUMANS FROM SOURCE	No
SC3 – S73	Ability to use backup oxygen generators (oxygen candles)	PHYSICAL REDUNDANCY	No

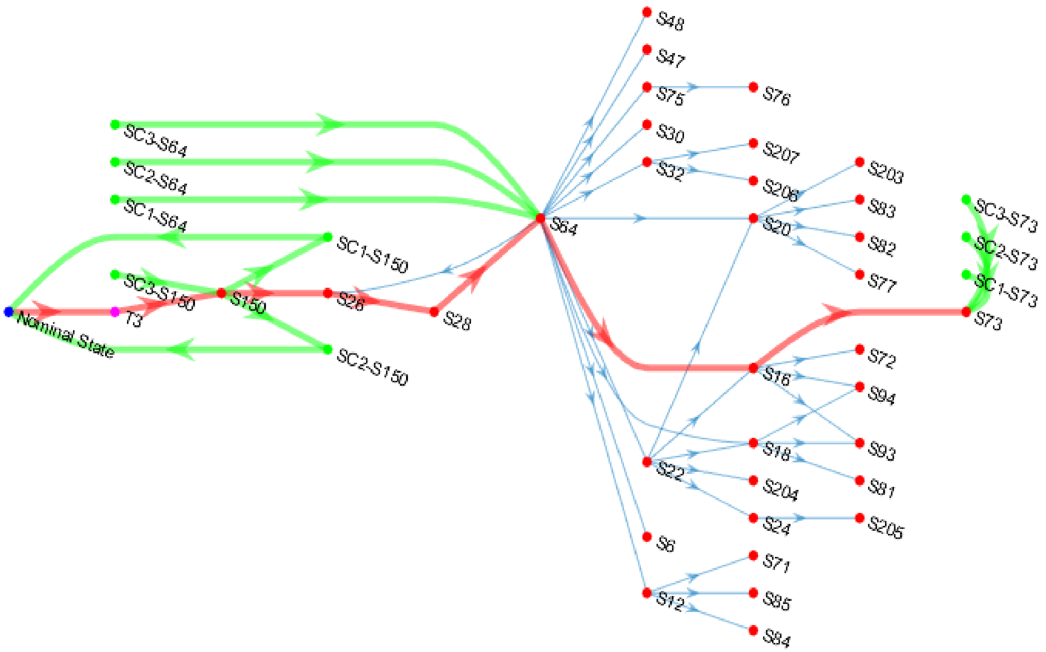

Figure 8: Application of Safety Controls to the case of high winds causing dust to impact the habitat, damaging the sensor management system

CONCLUSION

To help develop resilient space habitat systems, we proposed a way to systematically develop a database of disruptions, hazardous states, and potential safety controls. We use a state and trigger model to model the habitat's states and transitions between these states, and a network model to illustrate the interdependencies between the aspects of our database. Using these dependencies, we determined how a disruption would propagate through the habitat systems and trigger subsequent hazardous states, which we mitigate by implementing safety controls. The result is a large safety control option space.

In current work, we are developing a control-effectiveness metric, which indicates how well a control addresses the hazardous state or set of hazardous states it was designed for. We will also develop a resilience power metric, which indicates how well a control contributes to the overall resilience of the habitat. These metrics can then be used as part of the overall system design process to select safety controls that contribute to a design with the desired performance, resilience, and other system level properties, addressing the second objective of our research approach.

ACKNOWLEDGEMENT

This material is based upon work supported in part by NASA under grant or cooperative agreement award number 80NSSC19K1076. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Aeronautics and Space Administration (NASA).

REFERENCES

Kaplan, S., and Garrick, J., 1981. On the quantitative definition of risk. *Risk Analysis*, 1(1), pp. 11-28.

Knight, J. C., 2002. *Safety critical systems: Challenges and directions.* Orlando, ICSE, pp. 547-550.

Leveson, N., 2004. A new accident model for engineering safer systems. Safety Science, pp. Vol. 42, No. 4, pp. 237-270.

Leveson, N., Dulac, N., Marais, K., and Carroll, J., 2009. Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Organization Studies*, pp. 227-249.

Patriarca, R., Bergstrom, J., Di Gravio, G., and Constantino, F., 2018. Resilience engineering: Current status of the research and future challenges. *Safety Science*, pp. Vol. 102, pp. 79-100.

Rao, A., and Marais, K., 2020. A state-based approach to modeling general aviation accidents. *Reliability Engineering and System Safety*.

Rasmussen, J., 1997. Risk management in a dynamic society: A modelling problem. *Safety Science*, pp. Vol. 27, 183-213.

Uday, P., and Marais, K., 2015. Designing resilient systems-of-systems: A survey of metrics, methods, and challenges. *Systems Engineering*, pp. 18 (5), 491-510.