Quantifying ECLSS Robustness for Deep Space Exploration

Christine M. Escobar[1] and Adam C. Escobar[2]
Space Lab Technologies, LLC, Boulder, CO, 80301

and

James A. Nabity[3]
Smead Department of Aerospace Engineering Sciences, University of Colorado, Boulder, Colorado 80309

Human exploration of deep space will require Environmental Control and Life Support Systems of increasing robustness as mission duration and distance from Earth increase. As crews travel to distant unexplored environments, designers will need heightened confidence in life support availability under increasing levels of uncertainty and risk. Variation in system performance, environmental conditions, resource consumption, waste generation, and even mission characteristics will lead to unexpected responses, increased likelihood of failures, and even design obsolescence. The cost of system failures will also rise, due to launch mass and volume constraints, time and cost of resupply, and reduced ability to abort to Earth. If not accounted for early in design, the increased risk and cost of uncertainty might preclude human deep space exploration. This paper is the second in a series addressing the topic of robust ECLSS design. The first paper defined ECLSS robustness and discussed distinctions between robustness, reliability, resilience, and survivability. This prior work defined ECLSS robustness as "the ability to maintain habitable conditions for crew survival and productivity over the mission lifetime under a wide range of conditions." This wide range of conditions includes ordinary usage, temporary environmental disturbances or disruptions (both foreseen and unforeseen), and sustained changes in the system or mission context. ECLSS robustness must be quantifiable for design evaluation, comparison, improvement, and optimization. A robustness metric should address spacecraft habitability, not just crew survival; apply to all levels of system abstraction (component level to system level); apply to all design phases or levels of fidelity (conceptual through detailed design); be practical for use, relevant, and objective; and be compatible with existing assessment tools and all technology types. In this second paper we review several potential methods for quantifying robustness and propose an ECLSS robustness metric for future use in design evaluation and improvement.

Nomenclature

α	=	sensitivity
β	=	slope of dynamic process function
γ_C	=	Cornell's safety index
Δ	=	tolerance range
η	=	signal to noise ratio (Taguchi)
λ	=	constant failure rate
Λ	=	load variable
μ	=	mean of y
ρ_i	=	susceptibility index
σ	=	standard deviation
σ_e^2	=	mean square deviation from target value
ϕ	=	probability density function

[1] Vice President and CBO, Space Lab Technologies, LLC, Boulder, CO 80301
[2] CEO and President, Space Lab Technologies, LLC, Boulder, CO 80301
[3] Associate Professor, Aerospace Engineering Sciences, University of Colorado, Boulder, CO 80309.

ω	=	weighting factor
BVAD	=	Baseline Values and Assumptions Document
C_P	=	process capability index
C_{pk}	=	alternate process capability index
CF	=	Control Factor
D	=	A set of damage states given an exposure
DDT&E	=	Design, Development, Test, and Evaluation
D/T	=	System resistance to degradation
E	=	strength
ECLSS	=	Environmental Control and Life Support System
ESM	=	Equivalent System Mass
$ESM_{Я}$	=	Robustness normalized ESM
Ex	=	a set of hazard exposures
F_i	=	maximal (worst case) value of the system response
$f(t)$	=	failure probability density function
$F(t)$	=	probability unit fails by time t
FMEA	=	Failure Modes and Effects Analysis
FR	=	Functional Requirements
FTA	=	Fault Tree Analysis
H	=	Habitability Index for ECLSS
HIDH	=	Human Integration Design Handbook
H_R	=	ECLSS Robustness Metric
$h(t)$	=	instantaneous rate of failure for survivors at time t (from reliability engineering)
I	=	information content
ISS	=	International Space Station
KPC	=	Key Product Characteristic
$L(y)$	=	Quality loss given system response y
L_H	=	habitability loss
LCC	=	Life Cycle Cost
LEO	=	Low Earth Orbit
m	=	target value of key product characteristic y
M	=	input signal to a dynamic process
MIMO	=	multiple-input and multiple-output
MTBF	=	Mean time between failures
MTTF	=	Mean time to failure
NF	=	Noise Factor
p	=	probability
P_r	=	robustness index based on quality loss and information content
PRA	=	Probabilistic Risk Assessment
Q	=	Average quality loss over all potential values of y
$R(t)$	=	Reliability or survival function
$Я$	=	A robustness metric
$Я_H$	=	ECLSS robustness metric
RDM	=	Robust Design Methodology
S	=	size of white noise disturbance (for ρ_i)
SI	=	Sensitivity Index
SNR	=	Signal-to-Noise Ratio
t	=	Time
tMC	=	time average performance degradation
VMEA	=	Variation and Modes Effects Analysis
VRPN	=	Variation Risk Priority Number
$\boldsymbol{x}$	=	inputs or design parameters controlling or impacting y
y	=	key product or process response, a.k.a. KPC

I. Introduction

THE one common objective of any environmental control and life support system (ECLSS) for human spaceflight is to maintain an environment "suitable for the well-being of men and systems during the mission" in an isolated volume.[1] The ECLSS purpose is to maintain the habitability of the spacecraft. It must provide for the crew's needs, in order to keep them alive (at a minimum) and preferably enable them to be healthy, happy, and productive (to achieve mission objectives).[2] Beyond this commonality however, there is no one-size-fits-all ECLSS for human space exploration. The specific functional, performance, and operational requirements for ECLSS design are derived from mission characteristics (duration, the number of crew, destination environment, and mission objectives). The primary drivers of ECLSS design are the crew's metabolic inputs and outputs (to which the ECLSS provides a counterbalance), environmental conditions (largely determined by mission destination), and mission objectives (dictating the duration, return time to Earth, ability to resupply, and crew activities). The crew consumes resources (food, oxygen, and water) and produces waste (CO_2, humidity, heat, urine, feces, trace contaminants, trash, etc.). In addition to metabolic needs, the crew requires protection from a hazardous space environment characterized by extreme temperatures, high vacuum, micrometeoroids, reduced gravity, and high levels of cosmic or solar radiation. Other mission characteristics that might constrain the ECLSS design include allowable mass and volume, expected frequency of extravehicular activity, expected crew workload, surface operations, and distance from Earth for return or abort.

The ECLSS must first satisfy the physiological needs of the crew by regulating the atmosphere, providing potable water, and removing hazards posed by wastes. The next level of priority is to provide for crew safety, comfort, and well-being with food, safety infrastructure, mental and physical health countermeasures, and other human factors accommodations. The primary ECLSS elements are atmosphere management, water management, waste processing, food supply, safety, and crew accommodations. Though crew accommodations have not typically been included as an ECLSS element we encourage its future integration into ECLSS design and evaluation. Psychological and physiological countermeasures affect crew wellbeing, reduce the risk of illness and injury, and ultimately improve spacecraft habitability. Several NASA references define specific performance requirements, baseline values, and constraints for these elements, including the Human Integration Design Handbook (HIDH),[3] the NASA Spaceflight Human System Standard,[4] and the Life Support Baseline Values and Assumptions Document (BVAD).[5] The variety of technology options available to provide ECLSS functions have evolved significantly since the beginning of human space exploration, especially in the areas of atmosphere revitalization and water recovery. Technology has evolved over the last 50 years towards regenerable or recycling systems that sustain a habitable environment for longer durations, with less resupply mass.

II. The Need for Robust ECLSS Design

A. ECLSS Architecture Development and Optimization

An ECLSS architecture might include many different combinations of technologies that fulfill the functions of atmosphere revitalization, metabolic waste removal, and the provision of food and water. The difficult question facing exploration ECLSS architects is how to optimize for the performance and cost effectiveness necessary for mission success. The best architecture is not necessarily a collection of the most individually efficient components, but a collection of components that work together in an optimal way.[6] Optimization processes attempt to find the best possible design solution amongst all available solutions.[7] Several studies have demonstrated the use of optimization algorithms for ECLSS technology trades, configuration comparisons, and system sizing.[8,9,10,11,12,13,14] When more than one design option meeting all requirements is available, soft constraints, known as objectives, guide architectural comparisons. These objectives, often referred to as '-ilities', reflect the ability of the system to meet the users' needs and expectations (e.g. reliability, maintainability, useability, availability, etc.). Typically, objectives address system effectiveness and its cost, to varying degrees. However, cost and effectiveness criteria usually conflict, requiring multi-objective optimization techniques. For ECLSS evaluation, analysts must first define successful operation as well as cost. ECLSS architecture trades typically compare mass, reliability, and closure. For long missions stored consumables, levels of closure, and spare parts to improve reliability are major drivers of system mass.[15,16] Ref. 17 provides a detailed discussion of the most common ECLSS performance metrics, which include equivalent system mass (ESM), life cycle cost (LCC), closure, stability, and reliability.

B. The Cost of Uncertainty in ECLSS Design

The top technical challenges for human spaceflight beyond low Earth orbit (LEO) are to create safety infrastructure, autonomous operational strategies and systems, highly reliable and maintainable systems, and robust systems to deal with the unexpected.[18,19] As crews travel to distant unexplored environments, mission designers will

need heightened confidence in life support functionality under increasing levels of uncertainty and risk. To meet the demands of long duration life support, ECLSS technology will undoubtedly become more complex and have longer operational life spans. As system complexity and life spans increase, the likelihood of encountering variability (intrinsic or extrinsic) also increases. Uncertainty in things like component reliability, the environment, or crew metabolic loads rises with mission duration and distance from earth, making traditional reliability analysis difficult. In order to develop robust systems, characterization of the unexpected is a necessary first step.

Uncertainty is the result of not having accurate or sufficient knowledge of a situation.[20] Types of uncertainty might include the *probable* (frequent and foreseen, statistically characterized events with relatively low impact); the *possible* (foreseeable events that occur less frequently but have higher impact); or the *plausible* (very infrequent, potentially high impact rare or "black swan" events that may be unforeseeable by subject matter experts). Uncertainty may be aleatory (irreducible randomness) or epistemic (reducible uncertainty due to limited knowledge). Uncertainty, in the natural and engineered environment, is inherent in space exploration, making theoretical reliability analysis difficult.[21] That does not mean however, that designs cannot accommodate the unknown. Designers can bound realistic possible ranges of environmental conditions, or types of rare events to predict their impact on ECLSS performance. Ref. 17 itemized some potential sources of uncertainty to consider in ECLSS design, summarized in Table 1. For example, component failure rates come from limited test data and are themselves stochastic values. Component behavior within the system also may vary, especially for low TRL technologies that have not been well characterized. There may be unanticipated adverse effects of the space environment, like radiation or reduced gravity. Many of these effects can only be observed through long duration flight testing. As exploration missions take spacecraft into less traversed environments, the likelihood of unexpected environmental variability and rare events (such as a solar storm) increases.

Table 1 Sources of uncertainty in ECLSS design.

Component Performance	Failure rates, process rates, resource requirements, environmental effects
System Definition	Model uncertainty, component interactions, dynamic/transient processes
Metric Uncertainty	Formulation, assumptions, diligence in calculation
Operating Environment	In-flight use, boundary conditions, external environment, disturbance events, operator error
Mission Characteristics	Duration, resupply intervals, crew size, science objectives, etc.

Failures generate costs, and those costs increase the later they occur in the product life cycle. Strategies to reduce failures also come at a cost. Together, the cost of failure plus the cost of failure prevention is known as the *cost of quality.* For space life support, increased uncertainty may result in unanticipated system behavior, increasing the likelihood of component faults, system failure, or even design obsolescence. The cost of safety critical system failures (which may include loss of crew) and the cost of their prevention rise with mission distance and duration, due to launch mass and volume constraints, time and cost of resupply, and reduced ability to abort to Earth.[22] Ref. 23 and Ref. 24 caution that future life support system complexity (large mix of technologies with large variety and numbers of components) will lead to lower reliability and higher maintenance requirements than other systems. However, ECLSS performance to date falls short of the extreme reliability requirements evidenced by actual failure rates as well as on-board maintenance requirements.[25,26,27,28] Due to the increased uncertainty and risk of deep space exploration missions, the ability to maintain function in abnormal, off-nominal conditions as well as nominal conditions is increasingly important.[29,30] A plethora of design objectives (or '-ilities') exist in industry, related to performance under uncertain conditions, most of which suffer from inconsistent or indistinct definition.[31] However, literature reveals four emergent characteristics that best describe *system effectiveness in a dynamic uncertain environment*: *robustness, reliability, resilience, and survivability*. Ref. 17 proposed that *robustness* is an over-arching characteristic that captures reliability, resilience, and survivability. The objective for ECLSS performance should expand beyond reliability, to robustness, in order to reduce the cost and risk of uncertainty for deep space exploration.[17]

III. A Robust Design Methodology for ECLSS

A. Robust Design Definitions and Concepts

In technical literature, definitions of robustness for engineering systems vary widely,[17] but all include the notion of insensitivity of system performance to variation. *Robust products* are less sensitive (in terms of variation of product performance objectives) to environmental effects, deteriorative effects, and manufacturing imperfections.[32] *Robust*

processes make more uniform products despite variation of input variables.[33] A *robust design* "has a smaller deviation from a specified target value than other designs considered"[34] and maintains function against anticipated internal and external perturbations.[35] Since failures are typically caused by variation, robust designs are inherently more reliable by avoiding failure despite the presence of noise.[34] IEEE defines robustness as "the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions."[36] Robustness is particularly important, yet not well understood, in the context of space systems.[37] Ref. 38 suggests that the exploration of space system architectures "through the lens of uncertainty" may change the way designers think about conceptual design and how to select design alternatives to pursue.

> *"Often [spacecraft] systems are forced to operate under conditions which deviate significantly from ideal design conditions. A degree of how well a system performs with no appreciable degradation in performance under such conditions is measured by its robustness."*[39]

Ref. 17 proposed the concept of *robustness* "to characterize and improve ECLSS performance," suggesting that, "ECLSS robustness encompasses all aspects of its mission effectiveness." Given that the purpose of ECLSS is to maintain habitability of the spacecraft environment, Ref. 17 defined ECLSS *robustness* is its *ability to maintain habitable conditions for crew survival and productivity over the mission lifetime under a wide range of conditions.* This wide range of conditions includes ordinary usage, temporary disturbances or disruptions, and longer term, sustained changes in the system or mission context. Ref. 17 discussed definitions of and distinctions between reliability, resilience, robustness, and survivability in detail. The authors proposed that reliability, resilience, and survivability are actually *three separate system characteristics contributing* to ECLSS robustness. Ref. 17 suggested that reliability engineering typically accommodates only expected random failures and conditions (i.e. those that are foreseen and likely to occur); resilience accommodates *foreseen but unexpected* (i.e. less probable) deviations in conditions or disturbance events, and survivability accommodates *unforeseen adverse events (*unknown unknowns*).* Robustness can be achieved or improved by increasing any of these three contributors. Each of these characteristics has varying applicability, effectiveness, and cost depending on the mission circumstances. Figure 1 depicts reliable, resilient, and survivable as three distinct layers of robustness across a continuum of uncertainty.

Figure 1. Characteristics contributing to robustness.[17]

A Quality Characteristic (a.k.a. Key Product Characteristic) is the product or process response (y) that is observed for the purpose of evaluating robustness. Quality loss occurs when y deviates from some nominal target value m. A system's performance (y) can be described as a function of variables (or factors). *Signal factors* are the input variables that specify or control the product or process response; *control factors (CF)* are design parameters set to optimize the product response; and *noise factors (*NF) are variables which impact the product response but cannot be controlled by the designer.[40] Both control and noise factors influence the translation of inputs (or signals) into the intended response. In quality engineering, a parameter diagram (a.k.a. P-diagram), shown in Figure 2, is used to visually depict process signals, control factors, noise factors, and responses. Design margin and safety factors have been historically used to achieve robustness for space systems, however NASA crewed system programs don't have formal margin policies.[39] Worst case tolerancing is also a common method to protect against variation. However, as the number of inputs increases, the degree of over design by worst case tolerancing increases. For example, the likelihood of a part being produced with 20 tolerances all at the edge of tolerance limits is highly unlikely. *Robust design* is recommended as a less costly means of increasing the

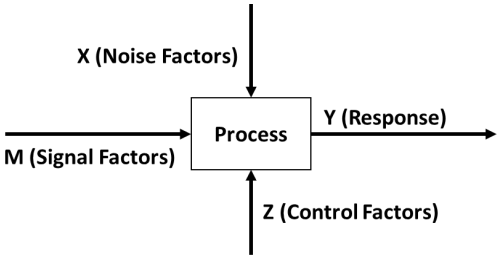

Figure 2. Parameter diagram.

tolerance or ability to operate in a wider range of conditions. Designs with reduced sensitivity to all types of noise avoid the use of "noise reduction/compensation technology" and allow the use of lower grade components and materials.[40] The fundamental principal of robust design is to minimize the effects of variation without eliminating the causes,[34,40] thereby improving product quality. This is depicted graphically in Figure 3. Minimizing sensitivity to noise means minimizing the slope of input variables or design parameters (**x**) versus system response *y*. This is done by selecting designs (or set of design parameters) for which the quality characteristic (*y*) has the least sensitivity to variation sources.[33,34,40] To do so, the designer must understand how input variability propagates through the system resulting in response variability, typically through what is known as a system model or transfer function.[33,34]

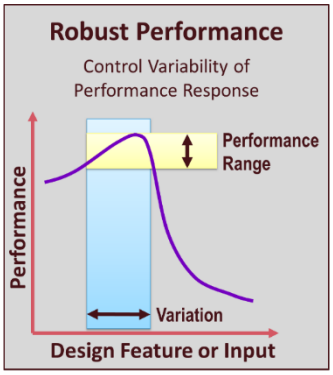

Figure 3. Robust performance.

B. Evolution of Robust Design Practices

Taguchi's Robust Design for Quality Engineering: Taguchi's robust design process is synonymous with robust design in much of the engineering literature. Taguchi breaks up the design process into three phases: 1) System design, during which architectural concepts and technology choices are made; 2) Parameter design, when individual system parameter values are chosen for design components; and 3) Tolerance design, when component tolerances are set to further minimize the effect of noise. Taguchi suggests that *parameter design* is the most important phase for achieving robustness.[32] In this phase, experimental data is used to determine the effects of control factors on quality characteristic, *y*, under expected environmental usage variation (imposed during the experiment).[32,40,41] Optimal control factor levels are then chosen that maximize the signal-to-noise ratio (SNR), a robustness metric pioneered by Mr. Taguchi. In communications, SNR is a measure of a signal strength relative to the noise floor. In quality engineering, it is the ratio between ideal performance (*m*) and deviation from that ideal performance (*y*-*m*). Taguchi pioneered the use of SNR as a robustness metric, since "the higher the ratio, the less harm variations cause to the system."[32] In the Taguchi robust design process, the design is first optimized for SNR, and then control factors are chosen to bring the average system performance closer to the target value *m*. This idea is predicated on the existence of control factors that can affect the mean of *y* with little effect on SNR. Some practitioners reverse this approach by *first* optimizing for maximum expected performance, max(E(*y*)), and *then* optimizing for minimal sensitivity to variation, max(SNR).[35] After design parameters (or control factors) are optimized, such that quality loss cannot be reduced any further, then the designer should consider ways to reduce or control noise factors.[33,40,42,43] This is known as *tolerance design* in manufacturing, and tends to be a much more costly means of reducing variation induced quality loss. Many authors argue that robust design should also be considered during early concept development to identify solutions that avoid noise factors and their associated failure modes all together or reduce their impact.[34] The concept of robust design has evolved over the last 30 years since Taguchi's first publications on the subject, but most approaches are mathematical variations of the same theme, including:

Statistical Process Control: Statistical process control methods involve the measurement and control of production variability relative to the allowable process spread (or tolerance) using process control charts and a process capability index.[44] Essentially, these methods evaluate the likelihood of a product being out of tolerance.

Statistical (or Probabilistic) Robust Design: Many authors[33] view a robust design as one for which system variability is minimized, subject to other performance or design constraints. Similar to the Taguchi method, design parameters are chosen that minimize variation in *y*. In contrast to the Taguchi method, performance variance is often estimated via error propagation through a mathematical system model, instead of being measured experimentally.

Robust Design Optimization: These methods use optimization routines to search a defined design space for solutions that either minimize variance, minimize distance of the mean *y* from target *m*, or some weighted combination of the two (through multi-objective optimization).

Axiomatic Design: Axiomatic design, proposed by Ref. 45, is an excellent robust design method to use during the conceptual design phase,[46,47,48] especially for reliable, cost-effective space life support systems.[49] This design approach consists of two axioms. First, the *independence axiom* is to maintain the independence of design parameters that satisfy functional requirements (FR), making the design controllable and uncoupled. Second, the *information axiom* is to minimize information content of those designs meeting the independence axiom. Information content is $\log_2(1/p)$, where p is the probability of success, or portion of the system performance that overlaps with the desired performance range, shown as the hatched area in Figure 4. To do so, both the bias (mean *y* minus target *m*) and performance variation must be small. To minimize the response variance, sensitivity coefficients can be reduced, increasing stiffness and allowing a larger variance in control factors. Next, design parameters are chosen that minimize

the response bias, similar to the Taguchi 2-step method. The first axiom of Axiomatic design (choosing design parameters to achieve functional independence, or an uncoupled design) is what really differs from Taguchi design.[47] Information content for a system (of multiple functional requirements) is the sum of information content of individual FRs in an uncoupled design. For coupled designs, information content calculation is more difficult, but several methods, such as conditional probability, have been proposed.[47]

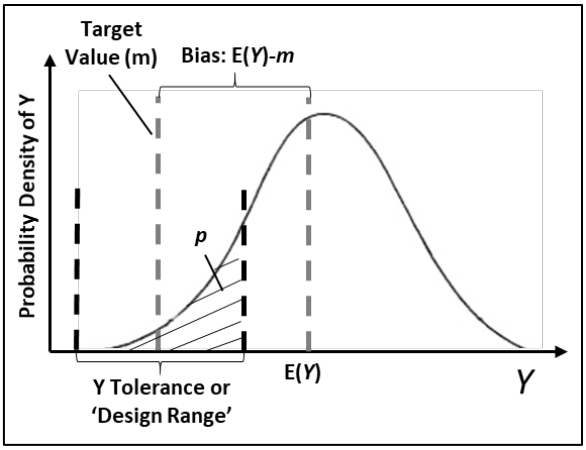

Figure 4. Information content based on probability density function for system performance.[47]

Robust Design Methodology: Many authors advocate an overall *methodology* for robust design rather than a specific procedure or mathematical definition.[34] Ref 50 defines *Robust Design Methodology* as "systematic efforts to achieve insensitivity to noise factors," based on four common principles: awareness of variation, insensitivity to noise factors, application of various methods, and application in all stages of the design process.[51] Similarly, Ref 52 defines robust design as: *a methodology aimed at finding the best possible combination of design parameters, making the product performance as insensitive as possible to the influence of NFs."* Regardless of what defines performance (y) and what optimization objective (i.e. robustness metric) is chosen, the following steps are inherent in robust design, and necessary to practicing Robust Design Methodology (RDM).

1. *Specify key product characteristics (KPC)*
2. *Specify variation*: Identify and characterize variation sources
3. *Specify the system*: Estimate variation effects on system performance y
4. *Quantify robustness*: Calculate a robustness metric, using results of (2) over one or more design alternatives, where the metric quantifies the deviation of y from some defined target or ideal performance.
5. *Select or improve design*: Analyze results of (3) to optimize or improve the design's robustness, by reducing effect of noise factors on KPCs (sensitivity); reducing bias (distance of mean y from target); or reducing noise.

To determine sensitivity to variation, designers must first identify variation sources that may impact system. performance, and if possible characterize their magnitude, spread, and distribution shape. The fidelity of variation characterization will depend on the amount of information available for a particular variation source. While some noise sources may have known probabilistic parameters, other rare extreme events (unknown unknowns) may only be quantifiable on a relative magnitude scale. Next, the designer must understand how potential input variability propagates through the system. If known, the mean, variance, and sensitivity of the response variable across the characterized variation sources can be estimated analytically with a mathematical system model (or transfer function), through simulation with a physical or mathematical system model, or experimentally with test or actual usage data. These values are then used to quantify robustness through a defined metric. Several metrics have been suggested in literature which are described in *Section IV*. Mean and variance estimates of response y can also be used to predict failure rates (for reliability) if a failure threshold is known. Finally, the prior analyses results are used to optimize or improve the system design.

C. A Proposed Robust Design Methodology for ECLSS

ECLSS *robustness* includes the *ability to maintain habitable conditions for crew survival and productivity over the mission lifetime under a wide range of conditions.*[17] In order to apply a Robust Design Methodology to environmental control and life support, we must first define what it means to be 'habitable', what it means to 'maintain' habitability, and what 'wide range of conditions' might occur. We propose the following *Methodology for Robust ECLSS Design.*

1. *Quantify Habitability*: Based on our definition of robust ECLSS, habitability of the spacecraft is the KPC to be optimized. We suggest the establishment of a *Habitability Index (H)* that is a utility function of contributing factors (such as O_2 availability or total pressure). The Habitability Index is discussed further in *Section V*.
2. *Characterize Uncertainty (NFs):* Noise includes potential variation in process inputs and operating conditions, as well as the probabilities of component or subsystem failure (reliability), recovery or repair (resilience), and survival, in the event of a catastrophic failure. This task will require input from subject matter experts within the bioastronautical science and engineering community and should include analysis of historical ECLSS data.

3. *Evaluate Sensitivity to Noise:* This step requires ECLSS definition, in the form of mathematical or physical models, to predict or observe effects of NFs on ECLSS performance, and thus on habitability.
4. *Calculate ECLSS Robustness:* Utilize information from steps 1-3 to calculate an ECLSS Robustness Metric, $Я_H$, defined in *Section V*. $Я_H$ can be used to compare robustness of alternate designs, or to improve an existing design.
5. *Design Improvement:*
   a) Using the results of step 4, identify design features or noise factors contributing most to habitability loss.
   b) Identify potential design improvements targeting those factors, through *axiomatic design* principles, and a *defense-in-depth* type design strategy (discussed in *Section V*), which is a strategy for systematically evaluating or implementing design changes to improve sensitivity, reliability, resilience, and survivability, in that order.
   c) Implement design improvements with the minimum cost of quality (minimum $ESM_Я$, defined in Section V).

This *Methodology for Robust ECLSS Design* embraces and builds upon established engineering approaches to coping with uncertainty including the disciplines of quality, reliability, resilience, and survivability engineering. It should be implemented iteratively throughout the project life cycle (concept development, to detailed design, to real-time, operational use). The methodology can be applied with a level of rigor (with respect to data, mathematical tools, and techniques) that is appropriate for the ECLSS design fidelity (i.e. design phase). It can also be applied at any level of abstraction (component, subsystem, or fully integrated system level). The sections that follow focus on quantification of habitability and of ECLSS robustness (items 1 and 4) and conclude with a brief discussion of the other process steps and future considerations for implementation.

IV. Quantifying ECLSS Robustness

A. Reliability Definitions and Concepts

The objectives of reliability engineering are to prevent or reduce likelihood or frequency of failures, identify and correct causes of failures, determine ways of coping with failures that do occur, and estimate reliability of new designs.[53] *Reliability* is "the probability of a system or system element performing its intended function under stated conditions without failure for a given period of time."[20] Reliability is quantified with a *failure probability density function, f(t)*, representing the probability of failure at time *t*. *Unreliability*, quantified by the cumulative failure distribution function *F(t)*, represents the probability that a component fails before time *t,* calculated as the integral of *f(t)* until time *t.* Conversely, the probability that a non-repairable unit survives past time *t* is known as the *reliability function* (or *survival function*), represented by *R(t)*, equal to 1-*F(t).* A *hazard rate*, *h(t)*, also known as *failure rate*, is the instantaneous probability of the first and only failure at time *t,* given the unit survived to time *t.* The hazard rate is equal to *f(t)/R(t)*. The *mean time to failure (MTTF)* or *mean time between failures (MTBF)* are the average amount of time that a unit is expected to operate before failure for non-repairable and repairable systems, respectively. For units with constant failure rate λ, MTTF and MTBF are equal to 1/λ. Reliability prediction methods include life data analysis (curve fitting of field data), load/strength interference analysis, knowledge of failure mechanisms (physics of failure), systems reliability models (or reliability block diagrams), fault tree analysis (FTA), state space or Markov analysis, or Petri Nets, to name a few.

B. Resilience Definitions and Concepts

The word resilience derives from the Latin verb resilire, meaning "to rebound, jump back, or recoil." The definition of resilience in the context of engineering varies widely in the literature. As a result of the ambiguities, ideas on how to measure, assess, and design for resilience also conflict. The concept of resilience as an emergent system property arose from the field of ecology more than 45 years ago, defined then as "the amount of disturbance that a system can withstand before it shifts into an alternative stable state."[54] Ref. 55 identifies the most common use of the word across a range of disciplines as "the ability of an entity or system to return to normal condition after the occurrence of an event that disrupts its state." Herein, a *disturbance* is defined as an event with the potential to disrupt the system state, such as an external deleterious occurrence (e.g. micrometeoroid impact), or an internal component failure. Resilience includes the following attributes, representing components of a system's response to a disturbance.

1) *Resistance (or Vulnerability):* Degree to which system function degrades as a result of a disturbance
2) *Recoverability*: A combination of 1) ability or degree to which the system performance returns to its pre-disturbance state; and 2) the period of time that it takes to recover to the original state (or better).
3) *Flexibility:* The magnitude of disturbance that the system can tolerate without unrecoverable failure. It represents how far the system performance can degrade without a loss of minimum function.
4) *Adaptability*: The ability or capacity to change or adapt to new circumstances without catastrophic loss of function, in order to mitigate the consequences of future disturbances.

5) *Detection and Avoidance*: Some texts include the abilities to anticipate, detect, and avoid an impending disturbance as a component of resiliency.[56] There may be early warning signals that can predict an imminent disaster so that it can be averted.[57]

Ref. 58 provides an excellent review of articles related to resilience quantification across multiple disciplines. Mathematically, a system's response to a disturbance has several distinct characteristics that can be quantified from a time series of that system's performance, depicted graphically in Figure 5, and described below. Similar to robust design, resilience quantification requires the definition of a key performance characteristic (y).

Survival: The ability to maintain functionality after a disruption can be quantified as the passive survival rate (reliability) plus the proactive survival rate (probability of restoration). The probability of restoration is the joint probability of system failure, failure identification, correct prognosis, and successful recovery.[59]

Vulnerability: Also called system health, vulnerability can be quantified as the total magnitude of function loss or degradation after a disruption.[60] Alternatively, it is calculated as the degradation magnitude as a percentage of the pre-disruption functionality, or the fraction of subsystems damaged after a disturbance.[61,61,62]

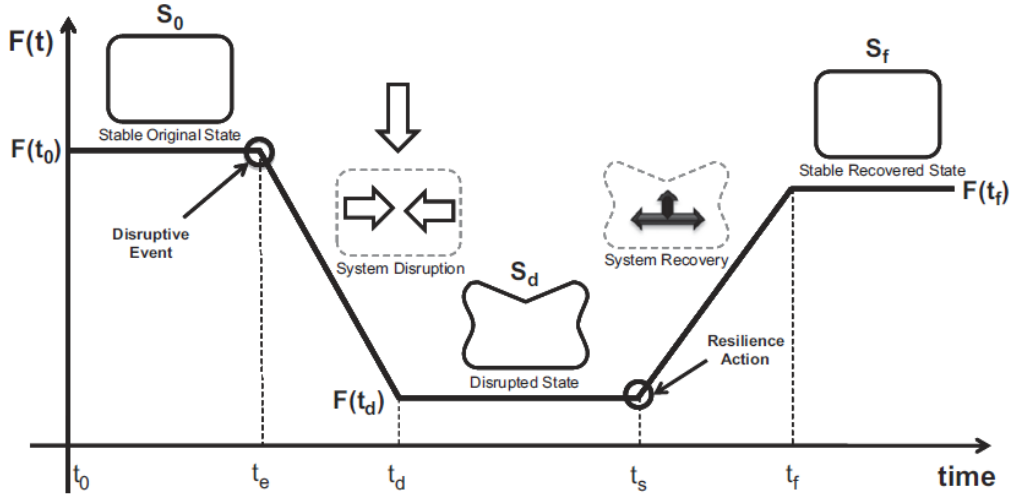

Figure 5. System performance and state transition to describe resilience from Ref. 63.

Degree of Return: After the system has fully recovered (has reached a stable state of functionality) it may not ever reach its original pre-disturbance health. The degree of return is the extent to which functionality is restored after recovery, i.e. post-recovery function divided by pre-event function.[64,65,66] Similarly, Ref. 60 quantifies resilience as the portion of performance recovered from the disrupted state.

Recovery Time: Also known as *return time or restoration time* is the time taken to return to a stable level of functionality after the disturbance event time.[61,64] Since the system may not return to its original state, the return time is *not necessarily* the time to return to pre-event functionality.

Probability of Recovery: The probability of recovering from a disturbance in a single time step.[67]

Integral functional loss, also called *efficiency*[64] is the area above the functional response curve (like that shown in Figure 5) from the beginning of the disruptive event to the time of full recovery (or to the end of some operational period of interest). The *Resilience Triangle* model assumes a linear recovery rate and an immediate performance loss after the event, such that the total functional loss is estimated as a triangle.[68,69] Conversely, many authors propose that a metric of resilience is simply the system performance (as a percentage of nominal or target performance) integrated over time.[70,71,72,73]

Recovery Rate: This is the change in function per time during the recovery phase, also known as return rate.[61,64]

Resistance (Absorbing Capacity): The resistance of the system to degradation after a disturbance (or its absorbing capacity), is the average functional degradation rate over time.[61] The capability to absorb adverse effects given a certain magnitude event or external disturbance can be calculated as:[61]

$$D/T = -10\log_{10}(\text{time averaged performance degradation}/\text{disturbance magnitude}) \quad (1)$$

This concept is very similar to the process capability index utilized in robust design (discussed later in this paper), representing the distance from target performance, normalized by variation in conditions.

C. Metrics of Robustness

Since robust design is concerned with improving product quality and decreasing cost of quality loss, a measure of product quality is needed to evaluate the effect of changing design parameters on the product's performance. Commonly, quality is measured as the fraction of units manufactured that are defective, i.e. falling out of a defined tolerance. However, this implies all products falling in tolerance are equally 'good'.[40] In reality, even if a product is in tolerance, its quality may decrease in the eyes of the user if its value deviates from ideal performance. This performance deviation can create economic loss, such as reduced sales. Several metrics have been proposed to quantify deviation from target performance due to sources of variation, which can be used as objective functions for robust design optimization. These metrics are summarized below.

1. Variance (or Dispersion)

Many authors view a robust design as one for which system variability is minimized, subject to other performance or design constraints.[33] Variance is a key component in *all* potential robustness metrics, and in some cases the only component to be optimized. Therefore, it is necessary to understand how nominal input values and the variability in inputs affect the variability in y, so that var(y) can be minimized. Variance can be estimated from 1) a sample of observations, 2) from a known probability distribution for y, 3) from a system model, f($\boldsymbol{x}$) and known co-variance of $\boldsymbol{x}$, or 4) from system model f($\boldsymbol{x}$) and known joint probability distributions of $\boldsymbol{x}$. The most common method is *Taylor Series Approximation,* based on the method of moments, using a system model and estimates of input variance.

2. Effective Fitness

Conversely, some authors propose that robustness can be achieved by optimizing the system performance (i.e. the expected value of y) subject to a constraint on acceptable output variance. In this case, the typical objective function to be optimized is the expected value of y, or E(y). This metric falls in the more general category of what are called *fitness functions,* commonly used in genetic algorithms, which indicate how close a design solution is to achieving target performance.[74] Just as with variance, E(y) can be estimated from a sample of observations, from a known probability distribution for y, from a system model using Taylor Series Approximation, or from a system model and known probability distributions for inputs $\boldsymbol{x}$.

3. *Robust Counterpart Approach (Worst Case Philosophy)*

Ref. 74 suggest the 'robust counterpart approach' based on 'minimax' optimization concept, used in Chebyshev approximation. This approach is similar to optimizing the expected value of y, but considers local variation in the design parameters in the optimization. The idea is to find design parameters $\boldsymbol{x}$ that minimize F_i, where F_i is the maximal (worst case) value of the system response function $f(\mathbf{x})$ in an interval around design point $\boldsymbol{x}_i$. Similarly, some authors have suggested the difference between the maximum and minimum of response function $f(\mathbf{x})$ as the robustness index.[47]

4. Process Capability Index

The process capability index (C_p) is commonly employed in quality control for manufacturing processes that are normally distributed. It is the ability of a process to perform within stated specification limits,[44] measured as the ratio of allowable process spread to actual process spread. Many authors propose quantifying robustness in terms of C_p.

$$C_P = \frac{\Delta}{6\sigma} \tag{2}$$

where standard deviation (σ) is that of the product or process response function, and tolerance (Δ) is the difference between the upper ($m2$) and lower ($m1$) allowable values of performance objective y, assuming that E(y) is on target (m). Ref. 33 defines an alternative process capability index, called C_{pk}, to use when E(y) is not on target. C_{pk} is the minimum distance to the tolerance limits divided by the spread of the of the output function.[75,76] Ref. 34 suggests the *Cornell reliability index,* γ_C, as a robustness measure that represents the distance to a failure mode, based on load and strength distributions, commonly employed in reliability analysis. Ref. 37 also recommended a load-strength metric for use in space system applications, where "strength" is a quantified measure of the system capacity to accommodate a given "stress". Stress can be any environment or load variable that "infringes on the strength characteristic".[37]

5. Quality Loss

The concept of quality loss, $L(y)$, introduced by Taguchi,[32] represents the financial loss of objective function y deviating from its target value m. Through Taylor Series expansion, $L(y)$ can be represented by Eq. (3):

$$L(y) = k(y\text{-}m)^2 \tag{3}$$

where k is the cost of the defective product (A) divided by the square of tolerance around m (Δ^2). Given Eq. (3), the average quality loss over all values of y, denoted Q, becomes:

$$Q = \mathrm{E}(L) = \mathrm{k}[(\mu - m)^2 + \sigma^2] = k\sigma_e^2 \quad (4)$$

where μ and σ^2 are the mean and variance of response *y*, respectively, and σ_e^2 is the mean square deviation of the product objective function from its target value. Notice that the average quality loss consists of two components: deviation of mean *y* from its target, called bias,[77] and the mean squared deviation of *y* around its own mean. Similarly, Ref. 78 proposed a *worst-case sensitivity* index that is the root mean square difference between *y* at worst case combinations of design variables (y_i) and the target value *m* of response variable *y*.

$$SI = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - m)^2} = \sqrt{Q} \quad (5)$$

Q could also be calculated probabilistically with an event tree, based on potential disturbance events that could disrupt or degrade *y*. The quality loss for an event is the probability of its occurrence times its consequence. For example, given a set of possible disturbance events or 'exposures' (*Ex*), the potential damage states that could result (*D*), and the consequence or quality loss (*L*) incurred as a result of that damage state, then the average quality loss becomes

$$Q = \int_{Ex}\int_{D} L * p(\mathrm{D}|Ex) * p(Ex)dDdEx/\mathrm{n} \quad (6)$$

Where *p* is a probability distribution and *n* is the number of leaves on the event tree (number of exposures times the number of damage states). This method assumes independence of the exposure that causes damage from the failure probability.[79] If the exposure events are not independent, a joint probability distribution could be used instead, i.e. $p(\mathrm{Ex}\cap\mathrm{D})$, which is $p(\mathrm{D}|\mathrm{Ex})*p(\mathrm{Exp})$. Note that this is conceptually similar to probabilistic risk assessment (PRA).

6. Sensitivity

Deterministic sensitivity analysis is a gradient based method to determine the effect of input changes on the system response, typically using 1st order Taylor Series approximation, given a defined system model, ***f(x)***. The goal is *to minimize sensitivity coefficients*, which are the partial derivatives of response function *f* with respect to input noise variables near a reference point.[74] If f(**x**) is non-linear, the designer can then choose values of control factors (controllable design parameters) to minimize the sensitivity coefficients, allowing for wider tolerances, lower grade materials, and a more variable operating environment.[40] A sensitivity measure based on the Jacobian matrix of ***f(x)*** can be used to minimize sensitivity in multiple input multiple output (MIMO) problems.[80,81,82,83,84]

In contrast to deterministic gradient based methods, probabilistic sensitivity analysis employs information from the statistical distribution of the input variables. Three categories of probabilistic sensitivity analysis (PSA) are:[85]

Variance based methods that decompose the total output variance into variation sources. In general, a variance-based sensitivity index is the total variance in *y* due to an input variable x_i ($\mathrm{V_i}$), including main and interaction effects, normalized by total *y* variance (V). Other variance-based methods include Fourier Amplitude Sensitivity Test (FAST) and Sobol indices. Variance-based methods utilize 2nd moment estimates of variance and may not accurately measure dispersion for responses with high skewness or kurtosis.[85] Also, these methods only apply globally, not allowing analysis of performance over a local region of the response distribution.[85]

Probabilistic characteristic methods evaluate the change of output probabilistic characteristics (such as mean, standard deviation or failure probability) as a result of changes in the probabilistic characteristics of inputs (e.g. $\partial\mu_Y/\partial\mu_X$, $\partial\sigma_Y/\partial\sigma_{Xi,}$ or $\partial P_f/\partial P_{Xi}$). These methods also apply to local optimization problems. Ref. 85 describes Wu's sensitivity coefficient, which estimates the impact of input distribution parameters on the probability of failure.

Entropy based methods: Ref. 85 suggests a third type of sensitivity measure, based on K-L (Kullback-Liebler) entropy that can be applied globally or locally. This method defines the most influential inputs as those that create the largest change in the response probability distribution, $p(y)$ when that input is set to a fixed value.

7. Signal to Noise Ratio

The signal to noise ratio (SNR), used in communications, is a measure of a signal strength relative to background noise. It serves as a measure of sensitivity to noise and can have different forms, depending on the response variable of interest. For example, in a dynamic process, an input signal *M* is ideally transformed into output *y*, as shown in Eq. (7). In reality, *y* is a function of not only the input signal *M* but also several other uncontrollable noise factors $\{x_1, x_2, \ldots x_n\}$ (Eq. 8). Deviation of *y* from *f(M)* imparts *quality loss,* which can be estimated as the ratio between the ideal function and deviation from the ideal function, as shown in Eq. (9). Ref. 32 defines the signal to noise ratio, η, as a measure of robustness, since "the higher the ratio, the less harm variations cause to the system."

$$y = f(M) \tag{7}$$

$$\hat{y} = f(M,x_1,x_2...,x_n) = f(M) + [f(M,x_1,x_2...,x_n) - f(M)] \tag{8}$$

$$\eta = \frac{\frac{\delta f}{\delta M}^2}{\frac{\delta f}{\delta x1}^2 \sigma_{x1}{}^2 + \frac{\delta f}{\delta x2}^2 \sigma_{x2}{}^2 + \ldots + \frac{\delta f}{\delta xn}^2 \sigma_{xn}{}^2} \tag{9}$$

Ref. 32 notes two problems with the ratio defined in Eq. (9). First, the error approximation in the denominator does not include all variation of the response due to noise (i.e. it is a first order Taylor series approximation of variance). Second, it requires knowledge of the exact function of system behavior. Ref. 32 instead recommends an alternative formula for η, that can be evaluated empirically and, in the case of a dynamic process, simplified to Eq. (10), where σ_e^2 is the mean square error of the process from the ideal function and β can be calculated through a least squares fit.

$$\eta = 10log_{10}\frac{\beta^2}{\sigma_e{}^2} \tag{10}$$

$$\sigma_e{}^2 = \frac{1}{n-1}\sum_i (y_i - \beta M_i)^2 \text{ and } \beta = \frac{\sum_i y_i M_i}{\sum_i M_i{}^2} \tag{11}$$

For static processes, the calculation of η depends on what values of y are considered 'better', shown in Table 2.[40]

Table 2 Alternate signal to noise ratios for static processes.

Smaller the Better (Minimize *y*)	$\eta = -10log_{10}\frac{1}{n}\sum_i y_i{}^2$	(12)
Nominal the Best (Target *m*)	$\eta = 10log_{10}\mu^2/\sigma^2$	(13)
Larger the Better (Maximize *y*)	$\eta = -10log_{10}\frac{1}{n}\sum_i \frac{1}{y_i{}^2}$	(14)
Zero is Best (Target 0)	$\eta = -10log_{10}\sigma^2$	(15)
Fraction Defective (Minimize p)	$\eta = -10log_{10}\frac{p}{1-p}$, where p is the fraction of defective units.	(16)

Similar to minimizing variance, the signal to noise ratio does not allow simultaneous optimization of the mean and variation. It is only effective when factors that influence the mean are separate from those that influence variance.[47] The performance target is reached by scaling design parameters after SNR has been maximized. Also, note that η applies only to a single response variable. Multivariate η functions are still needed.[44]

8. Aggregate Function of Mean and Variance

Since there is typically a trade-off between mean performance of the system response and its variance, many authors recommend multi-objective optimization algorithms. One option is to find Pareto optimal solutions that treat each as a separate optimization objective. Another option, for a smaller the better type problem, is to minimize the expected value and variance of y in an aggregate objective function, incorporating a weight parameter, ω, ranging from 0 to 1.[86]

$$\min (1-\omega)E(y|\boldsymbol{x}) + \omega Var(y|\boldsymbol{x}) \tag{17}$$

9. Variation Risk Priority Number

Variation Modes and Effects Analysis (VMEA) is a tool developed by Ref. 52, as a way to target design improvements that reduce variation risk. It is based on the idea of Failure Modes and Effects Analysis, replacing failure modes with variation sources (as typical causes of failures), and includes the following steps:

1. Identify "Key Product Characteristics" (KPCs), whose variation might adversely affect product function or quality.
2. Decompose KPCs into sub-KPCs (design characteristics) that influence the KPC.
3. Identify noise factors (NFs) that affect each sub-KPC.
4. Assess sensitivity of KPC to sub-KPCs and sensitivity of sub-KPCs to each NF.
5. Assess variation size of NFs.
6. Calculate Variation Risk Priority Number (VRPN), which is the 'variation risk' for each NFs or sub-KPC.

$$VRPN_{NF} = \alpha_i{}^2 \alpha_{ij}{}^2 \sigma_{ij}{}^2 \tag{18}$$

where α_i is the sensitivity of the Key Product Characteristic (KPC) to *i*th sub-KPC, α_{ij} is the sensitivity of *i*th sub-KPC to action of *j*th NF, and σ_{ij} is the NF variation size. VRPN of a sub-KPC is then calculated as the sum of each $VRPN_{NF}$ acting on it. Sub-KPCs and NFs can then be prioritized by their contribution to total variability of the KPC.

This VMEA process can be applied at any design stage. The methods for calculating sensitivity, variation size, and variation risk can change according to the design fidelity and information available. For example, in a *basic* VMEA, sensitivity and variation size give a relative 1-10 score, to quickly learn about potential impacts of variation. In an *enhanced* VMEA, a mathematical model of system performance is available, ***f(x)***, and sensitivity can be estimates from the first derivatives of *f*. Variation magnitude can be estimated as the (max(**x**)-min(**x**))/6. For higher fidelity designs, VRPN can be calculated *probabilistically* with the method of moments:

$$\alpha_i = \delta Y/\delta x_i|_{\mu}, \text{ and } \alpha_{ij} = \delta X_i/\delta NF_{ij}|_0 \tag{19}$$

$$\sigma_Y{}^2 = \sum_{i=1}^{m} \alpha_i{}^2 (\sum_{j=1}^{n_i} \alpha_{ij}{}^2 \sigma_{ij}{}^2) \tag{20}$$

Through Taylor Series approximation, it can be shown that the sum of VRPN for each noise factor and each sub-KPC is equivalent to the system variance.[34]

10. Information Content of Axiomatic Design (i.e. Reliability)

Information content of a design, used in axiomatic design (described in *Section IIIB*), has been suggested as a robustness metric to be minimized. It is defined mathematically as *I* shown in Eq. (21), where *p* is the probability of success, known as *R(t)* in reliability engineering. Information content represents the amount of information gained when a random variable is sampled. The occurance of less surprising events (with higher *p*) provides less information than the occurrence of more rare events (low *p*). If the functional requirements of the system are uncoupled, then the total information content is the sum of *I* for each function.[47]

$$I = \log_2(1/p) \tag{21}$$

The axiomatic design approach allows the use of a design range that is not considered with Taguchi signal to noise ratios but is the basis of reliability prediction. However, a design range by itself does not penalize for quality loss due to performance variation from a target. This can be illustrated in Figure 6. Based on information content alone, the design that performs completely within the design range would be chosen over the one that does not, even though there may be more significant quality loss for the 100% 'reliable' design. Ref. 87 suggests that *"the optimum robust design is the one that has the highest probability of success and the smallest variance."* The authors propose a new robustness index that simultaneously considers information content *and* the loss due to performance variation (i.e. Taguchi's quality loss). It combines the probability of success principle used in axiomatic design with the concept of Taguchi's loss function, in one index, P_r.

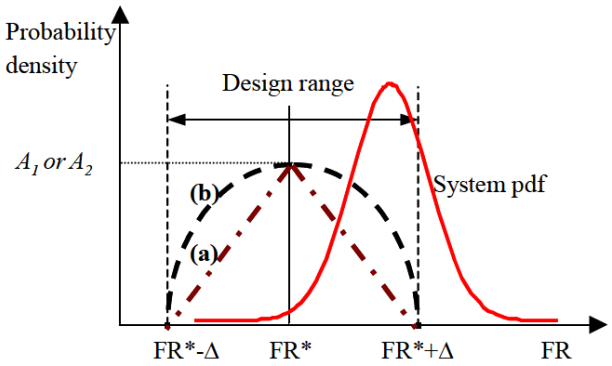

Figure 6. System probability density function and robustness weight function (a. linear; b. quadratic).[87]

$$P_r = \int_{m-\Delta}^{m+\Delta} \omega(FR)\emptyset(FR)dFR \tag{22}$$

where *m* is the target performance value, Δ is half of the acceptable performance range (outside of which would constitute system failure), ϕ(FR) is the probability density function for system performance, and ω(FR) is a weighting function. ω(FR) is defined only within the boundary of the design range, has a maximum at *m*, and can take on any shape that reflects the relative quality loss of moving away from *m*. For example, ω(FR) might be linear, or quadratic. Maximizing P_r selects the design that has the highest probability of success *and* the smallest variance.[89] Note that that information content and quality loss will provide the same answer if the designs meet the independence axiom.[47]

A unified, standardized method for robust design and quantification has not yet been agreed upon and robust design has rarely been applied to large scale problems.[47] Many case studies are still needed to develop a consensus.[47]

D. Habitability Index – A Key Performance Characteristic for ECLSS

The first step in robust design is to determine what key product characteristic should be optimized. The most useful KPCs are a direct outcome of the process or product (i.e. are controllable by the system) and are a monotonic continuous variable.[33,40] A KPC should be easy to measure, complete (covering all dimensions of the system process), and have a known target value (or acceptance limits).[33,40] Based on our definition of robust ECLSS, habitability of the spacecraft is the Key Product Characteristic to be optimized. We suggest a *Habitability Index (H)* that is a utility function of all contributing environmental factors controlled by the ECLSS. A utility function measures "how desirable it is for a response to take on a particular value within the acceptance region for the requirement,"[33] and is often defined on a scale of 0 to 1. The shape of a utility function could be linear or nonlinear, depending on what emphasis is placed on values that are closer to or further away from the target value. When there are multiple system responses that are important, a weighted vector of response variables can be combined into a single utility function.

The ECLSS habitability index, H, defined on a scale of 0 to 1, represents the productive capacity of the crew provided by the ECLSS. H is monotonic and continuous. An H of 0 represents fatal conditions, while a value of 1 indicates no health effects and a crew productive capacity of 100%. Values in between 0 and 1 represent degradation in crew's capacity to perform, as a result of the degradation of the spacecraft habitability. For example, H<0.25 might indicate conditions in which the crew is alive but incapacitated (e.g. unconscious); H<0.5 might indicate conditions in which the crew are ill or injured, with significantly reduced productive capacity; and H<0.75 might indicate conditions causing deleterious symptoms with reduced productive capacity. Table 3 contains a list of suggested contributors to habitability, which include environmental characteristics under ECLSS control. Variation of these characteristics away from their nominal values imparts habitability loss (i.e. quality loss). *Marginal habitability,* $H_i(y_i)$, is a marginal utility function, also defined from 0 to 1, representing the spacecraft habitability with respect to environmental factor y_i. Each contributor can be thought of as a single dimension of the total habitability space, if they are independent. This is graphically depicted in Figure 7 for two dimensions. In this example, deviation of total pressure or O_2 partial pressure away from nominal values *m1* or *m2* (up or down) results in a linear reduction in habitability. On the other hand, H_{CO2} could be an exponential function as shown in Figure 8 (as a theoretical example). Since human exposure limits for noxious substances are often time dependent, marginal habitability may even be auto-regressive, meaning that $H_i(t) = f(H_i(t\text{-}1))$. The marginal habitability functions $H_i(y_i)$ must be standardized in order for robust ECLSS design to be applied equitably. As shown in Figure 7, marginal habitability may not always be monotonic, but rather a 'nominal-is-best' type of function, where positive or negative deviation from some target m imparts habitability loss. The definition of meaningful and consistent utility functions for each contributor to habitability, as well as the mapping of H to crew performance capacity will be challenging. This will require research and data analysis by subject matter experts within the ECLSS and human health and performance communities.

Table 3. Potential Habitability contributors.

i	**Contributor to Habitability (y_i)**
1	O_2 availability in the cabin air (partial pressure)
2	CO_2 partial pressure in the cabin air
3	Total cabin pressure
4	Wet bulb temperature (a combination of absolute temperature and relative humidity)
5	Food quality (measured in days of available food per crew member, meeting minimum quality standards)
6	Water quality (measured in days of available water per crew member, meeting minimum quality standards)
7	Presence of noxious substances (including toxins, pathogens, etc.)

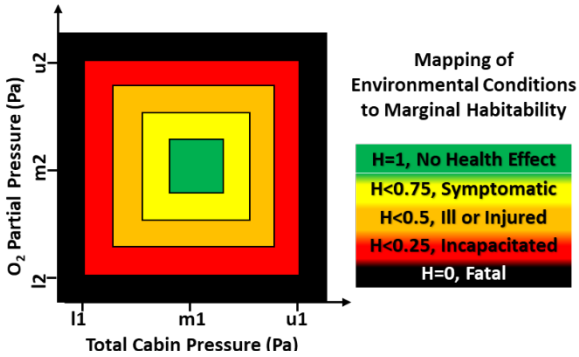

Figure 7. Mapping of environmental conditions to habitability.

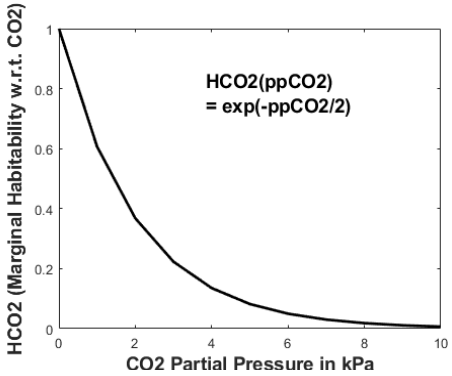

Figure 8. H_{CO2}, marginal utility.

Next, the marginal habitability indices, H_i, are combined to estimate the total habitability of the spacecraft (H). There are many possible aggregate functions, such as the mean, geometric mean, product, minimum, or a distance metric (like Euclidean distance). For example, Ref. 33 suggests taking the geometric mean of H_i, so that any unacceptable value makes the entire solution unacceptable. We considered the following criteria in defining H:

1. H must be 1 when the crew's performance capacity is full, i.e. when all H_i are equal to 1.
2. H must be 0 under any fatal conditions, i.e. when any $H_i = 0$.
3. H must be no better than any individual H_i, i.e. $H \leq \min(H_i)$
4. The impact of H_i on H is not independent. A reduction in one H_i increases the impact of another H_i. For example, if CO_2 levels are high and available food supply is low, but each of these conditions are not enough to cause failure, the combination of the two may be multiplicative, making the spacecraft uninhabitable.

Criteria 2 rules out the mean. Criteria 3 rules out the geometric mean and Euclidean distance. Criteria 4 rules out the use of $\min(H_i)$. The product of H_i appears to meet all criteria for our habitability index. H is thus defined as:

$$H = \prod_i H_i, \text{ for } i = 1,....,n \text{ and } H_i \in [0,1] \tag{23}$$

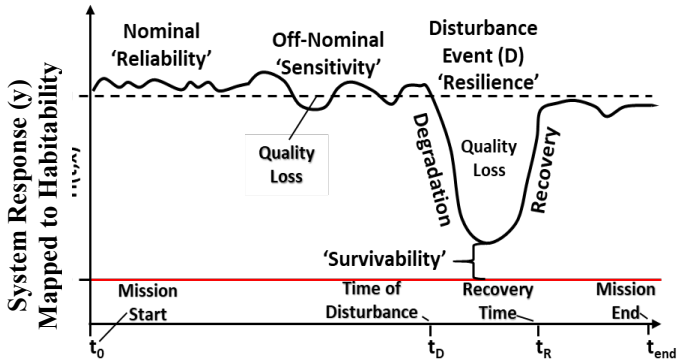

Figure 9. Habitability over time for mission of duration t_{end} minus t_0.

where n = number of contributing factors. H will change over time, particular due to changes in process inputs ($\boldsymbol{x}$), the occurrence of disturbance events, and the system's previous state, $H(t\text{-}1)$, depicted graphically in Figure 9. Therefore, at any moment, $H = H(t,\boldsymbol{x})$. H_i can also be calculated to compare single subsystems, such as a thermal control system, or even for a single component by assuming all other factors are nominal and scaling the marginal habitability function $H_i(y_i)$ by the maximum expected capability of that subsystem or component. For a single component j, multiply its output, y_{ij} by a scaling factor, n, where n is the number of components it would take to provide H_i of 1.

E. A Proposed Metric for ECLSS Robustness, $Я_H$

Ref. 17 discussed several important features for a meaningful and usable ECLSS robustness metric. A robustness metric must quantify the system's ability to maintain consistent performance (i.e. conditions necessary for crew productivity) in time, under perturbation of state, and in the event of system disturbance (failure or other shock).[17] This accounts for the contributing factors of reliability, resilience, and survivability, as an extension beyond the traditional notion of sensitivity to noise. In addition, a robustness metric should address spacecraft habitability, not just crew survival; apply to all levels of system abstractions (components, to subsystems, to integrated system); apply to all levels of design fidelity; be practical for use, relevant, and objective; and be compatible with existing assessment tools and all technology types.[17] Our proposed approach applies conventional robustness metrics, while expanding them to include not only input variation but the potential for failure or other disturbance events. These events may or may not be recoverable or repairable. After review of all of the robustness, resilience, and reliability metrics suggested in engineering literature (and summarized in *Sections IVA-IVC)*, a metric based on *average quality loss,* defined by Eq (5) and Eq (6), appears best suited for this application. Given habitability index H, defined from 0 to 1, we herein define habitability loss (L_H), expected value of habitability loss, $E(L_H)$, and subsequent ECLSS robustness, $Я_H$, as

$$L_H = (H\text{-}1)^2 \tag{24}$$

$$E(L_H) = E[(H\text{-}1)^2] = [1\text{-}E(H)]^2 + Var(H) \tag{25}$$

$$Я_H = 1 - \sqrt{E(L_H)} = 1 - \sqrt{[(1 - E(H))^2 + Var(H)]} \tag{26}$$

This definition also builds on the concept of integral functional loss, often used to quantify resilience,[64,70,71,72,73] where $Я_H$ is equivalent to the realized system performance, as a percentage of target performance, integrated over time. This metric has several advantages over other possible metrics considered.

1. $Я_H$ is defined on a scale of 0 to 1. When E(H) is 0, var(H) is also 0, such that $Я_H$ is equal to 0, the minimum possible value. Similarly, when E(H) is 1, var(H) = 0, such that $Я_H$ is equal to 1, the maximum possible value. A bounded scale allows specification of robustness requirements across various subsystem technologies.
2. $Я_H$ is reduced by variance of system performance from the mean, as well as by deviation of the mean from target performance (bias), incorporating both components of quality loss in one measure.
3. The $Я_H$ components (mean and variance in habitability, H) make the metric intuitive and simple to calculate.
4. The $Я_H$ components can be estimated throughout design, with different levels of fidelity, and can include meaningful detailed information about system function.
5. Habitability index H will be impacted by process sensitivity to variation (conventional Taguchi notion of robustness) but also by disturbance events (incorporating reliability, resilience, and survivability).
6. Because H is defined for components, subsystems, or integrated systems, $Я_H$ can be quantified at any level of system abstraction.
7. Finally, the cost of deviation from the mean is represented by mapping system response y into a utility function (similar to the k term in Eqs. (5) and (6)).

V. Evaluating and Improving ECLSS Robustness

A. Evaluating ECLSS Robustness, $Я_H$

With $Я_H$ defined, the designer can apply the metric throughout the design process. This requires the characterization of uncertainty (or noise factors) and evaluation of the effects of uncertainty on habitability index H (steps 2 and 3 in the *Methodology for Robust ECLSS Design*). Noise includes potential variation in process inputs and operating conditions, as well as the probabilities of component or subsystem failure (reliability), recovery or repair (resilience), and survival, in the event of a catastrophic failure. Recall that at any given moment in time, habitability is a function of time t and $\mathbf{x}$, which is a multivariate state space for inputs and external conditions with a joint probability distribution. This can include continuous inputs as well as a binary vector of discrete event occurrences. Variation sources could be identified and quantified from historical operational ECLSS data or from subject matter experts. There are a wealth of modeling tools for predicting the effects of noise factors $\mathbf{x}$ on outcome H, which can be categorized as deterministic, stochastic, or physical. Given a deterministic model of system performance, f($\mathbf{x}$), and given mean and variance of inputs $\mathbf{x}$, $E(H)$ and $Var(H)$ can be solved analytically, through approximation (e.g. Taylor series approximation) or Monte Carlo simulation. If the joint probability distribution, $p(\mathbf{x})$ is known,, then E(H) can be estimated stochastically as the integral $H_i * p(\mathbf{x})$. This approach is similar to Probabilistic Risk Assessment (PRA). If the system is too complex to model mathematically, a physical model (or prototype) can be built and tested, to measure the variation in y_i across the range of $\mathbf{x}$. At lower design fidelity, a simple scoring method can even be used to calculate a rough estimate of $Var(H)$, such as the Variation Risk Priority Number, as shown in Eq. (18). Finally, given an estimate of $E(H)$ and $Var(H)$, the designer can calculate ECLSS robustness $Я_H$, with Eq. (26). This is step 4 of the *Methodology for Robust ECLSS Design*.

B. Improving ECLSS Robustness Through a Defense-in-Depth Type Strategy

Once we know how to calculate $Я_H$ for a given system design, how do we then identify the best ways to improve robustness? A metric alone does not tell *how* to achieve robustness. Following step 6 of the *Methodology for Robust ECLSS Design,* the designer should first identify design features or noise factors contributing most to habitability loss. Many of the robustness metrics described in *Section IV C* are excellent tools for doing so, such as sensitivity analysis, variation modes and effects analysis, signal to noise ratios, or information content from axiomatic design. Next the designer might explore potential design improvements that target the most influential noise factors or contributors to habitability loss. There is a plethora of tools in reliability engineering, resilience engineering, survivability engineering and robust design that can be employed. For example, reliability improvement might be achieved by adding redundancy, increasing material strength or margin, decreasing tolerances, decreasing complexity (i.e. information content), or decreasing coupling (functional independence). Sensitivity might be improved by choosing design parameters with less influence on y (Taguchi methods). Resilience might be improved by adding fault detection and isolation, repair mechanisms, noise reduction through shielding, while survivability might be improved by adding failure contingency capability.[88] There are generally three ways to increase ECLSS robustness:

1) Increase the overall system performance capacity, by increasing the expected value of Habitability, $E(H)$. This is equivalent to bringing the mean on target in Taguchi's robust design process.
2) Decrease variability by decreasing the sensitivity of H to variation in $\mathbf{x}$. This is related to the concept of parameter design in Taguchi's robust design process.

3) Decrease the size of the uncertainty space (covariance of $\boldsymbol{x}$), by reducing exposure (e.g. shielding) to noise, tightening tolerances, or removing threats all together. This is typically the most difficult and expensive means of improving $Я_H$.

We propose a 'defense-in-depth'[89,90] type design strategy that systematically identifies and evaluates added design features to improve quality (sensitivity), reliability, resilience, and survivability, in that order, as shown in Figure 10. Quality engineers have found that the most cost-effective improvements are likely those that reduce sensitivity to noise. Therefore, this is the first line of defense. The second line of defense is to improve reliability, by using stronger components, remove failure modes, or adding fault tolerance (through redundancy). The third line of defense is to increase the ability to avoid, absorb, or recover from disturbances and failures (resilience engineering). And finally, the last defense is to improve the chances of survival in the event of a catastrophic (unrecoverable) system failure.

Figure 10. Defense-in-depth strategy for robust ECLSS design.

Given a set of design solutions, the best option is the one that minimizes the cost of quality, i.e. the solution for which the cost of design change (ΔC) is less than the value of loss prevention (ΔP). For ECLSS, the cost of a design change could potentially be estimated by the change in ESM, while the value of loss prevention is quantified by increased robustness, $Я_H$. Ref. 91 states that, "the lowest ESM option is thus the best choice, provided the options have the same function, reliability, safety and interfaces or are adjusted suitably." The problem is that most architectural comparisons based on ESM do *not* account for reliability (or robustness for that matter). Therefore, we propose a normalized Equivalent System Mass, $\text{ESM}_Я$ that is the equivalent system mass as defined by Ref. 91, divided by $Я_H$, as shown in Eq. (27).

$$\text{ESM}_Я = \frac{\text{ESM}}{Я_H} \tag{27}$$

$\text{ESM}_Я$ theoretically represents the total mass of the systems that would be required to achieve an equivalent level of robustness. Given that H accounts for functional capacity *and* variance, the normalized ESM accounts for the overall functional capacity, reliability, resilience, and survivability of the ECLSS. The optimal ECLSS architecture can now be defined as one in the feasible design space (meeting minimal functional requirements or constraints) that has the minimum cost of quality, or $\text{ESM}_Я$.

VI. Conclusion

Many studies and reports on ECLSS performance cite the need for robust systems. There has been much progress in the definitions, assessment tools, and design practices for ECLSS reliability. However there has been little attention given to the definition, tools, and practices for robust ECLSS design. Sometimes the word robust is used interchangeably with reliable, resilient, and survivable. We propose that robust encompasses the other three distinct and equally important aspects of system performance. ECLSS robustness is its ability to maintain habitable conditions for crew survival and productivity over the mission lifetime under a wide range of conditions. This wide range of conditions includes ordinary usage, temporary disturbances or disruptions, and longer term, sustained changes in the system or mission context. In order to apply a *Robust Design Methodology* to environmental control and life support, we must first define what it means to be 'habitable', what it means to 'maintain' habitability, and what 'wide range of conditions' might occur. A *Methodology for Robust ECLSS Design* is proposed herein, that incorporates variation sources into calculation of a habitability index. *Habitability Index (H)* is a utility function of all environmental quality factors that are controlled by the ECLSS. We next propose an ECLSS robustness metric, $Я_H$ which is a function of the mean and variance of H. This metric can be used to compare alternate ECLSS designs and to evaluate the merit of potential design improvements. Finally, we suggest a 'defense-in-depth' type design strategy that systematically evaluates added design features to improve quality, reliability, resilience, and survivability, in that order. The ECLSS robustness metric $Я_H$ can then be used in combination with ESM estimates to calculate a normalized ESM, representing the cost of quality for the design change under consideration. The optimal ECLSS architecture can now be defined as one in the feasible design space with the minimum cost of quality.

The Methodology for Robust ECLSS Design defined herein is generalized and flexible, such that it can be applied to any system, subsystem, or component, at any stage of design. However, standardization requires the development of marginal habitability functions (i.e. utility functions) for each ECLSS function. This can only be achieved through cooperative research and data analysis by subject matter experts within the ECLSS and human health and performance communities. Once this is accomplished, the next step is to demonstrate robustness quantification through analysis of historical ECLSS performance data and to demonstrate the robust design methodology through specific examples. Though reaching consensus on utility functions may be challenging, it will be instrumental in the provision of robust ECLSS, enabling long duration human exploration of deep space.

References

[1] Eckart, P., *Spaceflight Life Support and Biospherics*, Vol. 5, Springer, Netherlands, 1996.

[2] Klaus, D. M., "Functional Integration of Humans and Spacecraft through Physics, Physiology, Safety and Operability," *2017 IEEE Aerospace Conference*, 2017 (submitted for publication).

[3] "Human Integration Design Handbook," NASA/SP-2010-3407, January 27, 2010, pp. 337-9.

[4] "NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health," NASA-STD-3001, Volume 2, Revision A, February 10, 2015, p. 26.

[5] Anderson, M. S., Ewert, M. K., Keener, J. F., and Wagner, S. A., "Life Support Baseline Values and Assumptions Document," NASA/TP-2015–218570, 2015.

[6] Czupalla, M., Dirlich, T., and Bartsev, S. I., "An Approach to LSS Optimization Based on Equivalent System Mass, System Stability and Mission Success," *SAE Technical Paper* No. 2007-01-3222, 2007.

[7] Burke, E. K., and Kendall, G., *Search methodologies*, Springer Science Business Media, Inc., 2005.

[8] Bartsev, S. I., "Life Support System Power Supply Optimization," *SAE Technical Paper* No. 972299, 1997.

[9] Bartsev, S. I., "Optimum Control of Closed Ecological Systems: Mathematical Aspects," *Life Support & Biosphere Science: International Journal of Earth Space,* Vol. 6, No. 2, 1998, pp. 123-131.

[10] Bartsev, S. I., Mezhevikin, V. V., and Okhonin, V. A., "Evaluation of Optimal Configuration of Hybrid Life Support System for Space," *Advances in Space Research*, Vol. 26, No. 2, 2000, pp. 323-326.

[11] Lin, K.-P., Luo, Y.-Z., and Tang, G.-J., "Optimization of Logistics Strategies for Long-Duration Space-Station Operation," *Journal of Spacecraft and Rockets*, Vol. 51, No. 5, 2014, pp. 1709–1720.

[12] Miyajima, H., "Parametric Analysis of Logistics and Life Support Systems for Deep Space Mission Design," *45th International Conference on Environmental Systems*, 2015.

[13] Nagendra, N. P., Schubert, D., Zabel, P., "System Analysis and Evaluation of Greenhouse Modules within Moon / Mars Habitats Supervisors," *9th COSPAR Scientific Assembly*, Mysore, India, July 2012, p.1318.

[14] Shaw, M. M., and de Weck, O. L., "An Analysis of Hybrid Life Support Systems for Sustainable Habitats," *44th International Conference on Environmental Systems,* July 2014.

[15] Anderson, M. S., and Stambaugh, I. C., "Exploring Life Support Architectures for Evolution of Deep Space Human Exploration," *45th International Conference on Environmental Systems*, 2015.

[16] Do, S., Owens, A., and de Weck, O., "HabNet–An Integrated Habitation and Supportability Architecting and Analysis Environment." *45th International Conference on Environmental Systems,* 2015.

[17] Escobar, C., Nabity, J., and Klaus, D., "Defining ECLSS Robustness for Deep Space Exploration," *47th International Conference on Environmental Systems*, 2017.

[18] Perry, J. L., Sargusingh, M. J., and Toomarian, N., "Guiding Requirements for Designing Life Support System Architectures for Crewed Exploration Missions Beyond Low-Earth Orbit," *AIAA SPACE,* 2016, pp. 5461.

[19] Larson, W. J., and Pranke, L. K., *Human Spaceflight: Mission Analysis and Design*, McGraw-Hill Companies, 1999.

[20] Adcock, R. D. (Ed.), "*Guide to the Systems Engineering Body of Knowledge (SEBoK)*," October 27, 2016, Retrieved February 16, 2017, from http://sebokwiki.org/.

[21] Holubnyak, Y., and Rygalov, V., "Theoretical Analysis for Long-Term Space Life Support Reliability," *International Conference on Environmental Systems,* 2009.

[22] Owens, A., and De Weck, O., "Limitations of Reliability for Long-Endurance Human Spaceflight," *AIAA SPACE*, 2016.

[23] Averner, M., and Blackwell, C., "The Development and Operation of Life Support Systems for Long Term Space Exploration Missions," *SAE Technical Paper* No. 961494, 1996.

[24] Jennings, H. A., "Maintainability and Reliability of Environmental Control Life Support Systems," *Aeronautic and Space Engineering and Manufacturing Meeting*, 1968.

[25] Burnett, J. R., and King, C. D., "Reliability and Maintainability Problems Confronting Environmental Control Life Support Systems for Long Duration Space Flight," *SAE Technical Paper* No. 680744, 1968.

[26] Hodgson, E. W., Converse, D., Duggan, M., and Gentry, G. J., "Flexible Path Environmental Control and Life Support Technology-An Updated Look at Next Steps," *43rd International Conference on Environmental Systems*, 2013, p. 3409.

[27] Russell, J. F., and Klaus, D. M., "Maintenance, Reliability and Policies for Orbital Space Station Life Support Systems," *Reliability Engineering and System Safety*, Vol. 92, No. 6, 2007 pp. 808-820.

[28] Likens, W. C., "A Preliminary Investigation of Life Support Processor Reliabilities," *International Conference on Life Support and Biospherics*, Huntsville, Alabama, Feb. 18-20, 1992.

[29] Levri, J. A., and Vaccari, D. A., "Model Implementation for Dynamic Computation of System Cost for Advanced Life Support," *Advances in Space Research*, Vol. 34, No. 7, 2004, pp. 1539–1545.

[30] Jones, H. W., Hodgson, E. W., and Kliss, M. H., "Life Support for Deep Space and Mars," *44th International Conference on Environmental Systems,* 2014.

[31] Mekdeci, B., Ross, A. M., Rhodes, D. H., and Hastings, D. E., "Pliability and Viable Systems: Maintaining Value under Changing Conditions," *IEEE Systems Journal*, Vol. 9, No. 4, 2015, pp. 1173–1184.

[32] Taguchi, Genichi, and Cariapa, *Taguchi on robust technology development*, 1993.

[33] Dodson, B., Hammett, P., and Klerx, R., *Probabilistic design for optimization and robustness for engineers*, John Wiley and Sons, 2014.

[34] Bergman, B., De Maré, J., Svensson, T., and Loren, S., eds., *Robust design methodology for reliability: Exploring the effects of variation and uncertainty*, John Wiley and Sons, 2009.

[35] Baxter, B., and Malak, R., "Increasing System Robustness Through a Utility-Based Analysis," *ASME 2013 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference,* American Society of Mechanical Engineers, 2013.

[36] SEBoK, "Reliability, Availability, and Maintainability," *Guide to the System Engineering Body of Knowledge,* URL: https://www.sebokwiki.org/w/index.php?title=Reliabiflity,_Availability,_and_Maintainability&oldid=52881 [cited 9/09/2018].

[37] Ryan, R, "Robustness," *NASA Technical Report*, NASA-TP-3336, Mar 01, 1993.

[38] Walton, M. A and Hastings, D., "Applications of Uncertainty Analysis Applied to Architecture Selection of Satellite Systems," *Journal of Spacecraft and Rockets* 41.1, 2004, pp. 75-84.

[39] Miller, J., Leggett, J., and Kramer-White, J, "Design Development Test and Evaluation (DDTE) Considerations for Safe and Reliable Human Rated Spacecraft Systems," NASA/TM-2008-215126/Vol II, 2008.

[40] Phadke, M. S., *Quality engineering using robust design*, Prentice Hall PTR, 1989.

[41] Andersson, P., "A semi-analytic approach to robust design in the conceptual design phase," *Research in Engineering Design,* 8(4), 1996, pp. 229-239.

[42] Taguchi, G., Elsayed, E. A., and Hsiang, T. C., *Quality engineering in production systems, Vol. 173*, New York: McGraw-Hill, 1989.

[43] Arvidsson, M., and Gremyr, I., "Principles of robust design methodology," *Quality and Reliability Engineering International*, 24(1), 2008, pp. 23-35.

[44] Mondal, S. C., P. K. Ray, and J. Maiti, "Modelling robustness for manufacturing processes: a critical review" I*nternational Journal of Production Research* 52.2, 2014, pp. 521-538.

[45] Suh, N. P., *The Principles of Design*, Oxford Univ. Press, New York, 1990.

[46] Hwang, K. H., and G. J. Park, "Development of a robust design process using a new robustness 'index'," *ASME 2005 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, 2005.

[47] Park, G., Lee, T.-H., Lee, K. H., and Hwang, K.-H., "Robust design: an overview," *AIAA Journal*, 44(1), 2006, pp. 181–191.

[48] Suh, N. P., *Axiomatic Design: Advances and Applications*, Oxford Univ. Press, New York, 2001.

[49] Jones, H., "Axiomatic Design of Space Life Support Systems," *47th International Conf. on Environmental System*s, 2017.

[50] Arvidsson, M., and Gremyr, I., "Principles of robust design methodology," *Quality and Reliability Engineering International*, 24(1), 2008, pp. 23-35.

[51] Arvidsson, H and Gremyr, I., "A review of practices for robust design methodology," *Journal of Engineering Design*, 20(6), 2009, pp. 645-657.

[52] Johansson, P., Chakhunashvili, A., Barone, S., and Bergman, B., "Variation mode and effect analysis: a practical tool for quality improvement," *Quality and Reliability Engineering International*, 22(8), 2006, pp. 865-876.

[53] O'Connor, P., and Kleyner, A., *Practical Reliability Engineering*, Wiley, Hoboken, NJ., 2012.

[54] Holling, C. S., "Resilience and stability of ecological systems," *Annual Review Of Ecology And Systematics,* 1973.

[55] Hosseini, S., Barker, K., and Ramirez-Marquez, J. E., "A review of definitions and measures of system resilience," *Reliability Engineering and System Safety*, 145, 2016, pp. 47-61.

[56] Hollnagel, E., Woods, D. D., and Leveson, N., *Resilience engineering: Concepts and precepts*, Ashgate Publishing, 2007.

[57] Scheffer, M., Bascompte, J., Brock, W. A., Brovkin, V., Carpenter, S. R., Dakos, V., ... and Sugihara, G., "Early-warning signals for critical transitions," *Nature*, 461(7260), 2009, p. 53.

[58] Hosseini, S., Barker, K., andRamirez-Marquez, J. E., "A review of definitions and measures of system resilience," *Reliability Engineering and System Safety*, 145, 2016, pp. 47-61.

[59] Youn, B. D., Hu, C., Wang, P., "Resilience-driven system design of complex engineered systems," *Journal of Mechanical Design*, 133:10, 2011.

[60] Balchanos, M., Li, Y., and Mavris, D., "Towards a method for assessing resilience of complex dynamical systems," *Resilient Control Systems (ISRCS), 2012 5th International Symposium* on. IEEE, 2012.

[61] Wang, J. W., Gao, F., and Ip, W. H., "Measurement of resilience and its application to enterprise information systems," *Enterprise Information Systems,* 4(2), 2010, pp. 215–23.

[62] Owin, K. H., and Wardle, D.A., "New indices for quantifying the resistance and resilience of soil biota to exogenous disturbances," *Soil Biol Biochem*, 26, 2004, pp. 1907–12.

[63] Henry, D., and Ramirez-Marquez, J. E., "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering and System Safety* 99, 2012, pp. 114-122.

[64] Todman, L. C., Fraser, F. C., Corstanje, R., Deeks, L. K., Harris, J. A., Pawlett, M., ... and Whitmore, A. P., "Defining and quantifying the resilience of responses to disturbance: a conceptual and modelling approach from soil science," *Scientific Reports*, 6, 2016, p. 28426.

[65] Omer, M., Nilchiani, R., and Mostashari, A., "Measuring the resilience of the trans- oceanic telecommunication cable system," I*EEE Systems Journal*, 3(3), 2009, pp. 295–303.

[66] Chen, L., and Miller-Hooks, E., "Resilience: an indicator of recovery capability in intermodal freight transport," *Transp Sci,* 46(1), 2012, pp. 109–23.

[67] Hashimoto, T., Stedinger, J. R., and Loucks, D. P., "Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation," *Water Resources Research*, 18(1), 1982, pp. 14-20.

[68] Bruneau, M., Chang, S. E., Eguchi, R. T., Lee G. C., O'Rourke, T.D., Reinhorn, A. M., et al., "A framework to quantitatively assess and enhance the science the seismic resilience of communities," *Earthq Spectra* 19(4), 2003, pp. 733–52.

[69] Zobel, C. W., "Representing perceived tradeoffs in defining disaster resilience," *Decision Support Systems,* 50(2), 2011.

[70] Attoh-Okine, N, Cooper, A.T., and Mensah, S.A., "Formulation of resilience index of urban infrastructure using belief functions," *IEEE Systems Journal,* 3(2), 2009, pp. 147–153.

[71] Ayyub, B. M., "Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making," *Risk Analysis*, 34(2), 2014, pp. 340-355.

[72] Dalziell, E., and McManus, S., "Resilience, vulnerability, and adaptive capacity: implications for system performance," 2004.

[73] Ouyang, M., Duenas-Osorio, L., and Min, X., "A three-stage resilience analysis frame- work for urban infrastructure systems," *Structural Safety* 36–37, 2012, pp. 23–31.

[74] Beyer, H., and Sendhoff, B., "Robust optimization–a comprehensive survey," C*omputer Methods In Applied Mechanics And Engineering* 196.33, 2007, 3190-3218.

[75] Kane, V. E., ''Process Capability Indices,'' *Journal of Quality Technology*, 18, No. 1, 1986, pp. 41–52.

[76] Frey, D. D., Otto, K. N., and Wysocki, J. A., "Evaluating Process Capability During the Design of Manufacturing Systems," *Journal of Manufacturing Science and Engineering,* 122, 2000, pp. 513–519.

[77] Abate, M. L., Morrow, M. C., and Kuczek, T., "An application of robust parameter design using an alternative to Taguchi methods," *No. SAND-96-0250C; CONF-9608107-2*. Sandia National Labs., Albuquerque, NM (United States), 1996.

[78] Sundaresan, S., Ishii, K., and Houser, D. R., "A Robust Optimization Procedure with Variations on Design Variables and Constraints," *Engineering Optimization*, Vol. 24, No. 2, 1995, pp. 101–117.

[79] Baker, J. W., Schubert, M., and Faber, M. H., "On the assessment of robustness," *Structural Safety* 30.3, 2008, pp. 253-267.

[80] Al-widyan, K., and Angeles, J., "A model-based framework for robust design," *Recent Advances in Integrated Design and Manufacturing in Mechanical Engineering*, Kluwer Academic Publisher, 2003.

[81] Caro, S., Bennis, F., and Wenger, P., "Tolerance synthesis of mechanisms: a robust design approach," *In ASME 2003 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, 2003, pp. 339-348.

[82] Hu, S. J., Webbink, R., Lee, J., and Long, Y., "Robustness evaluation for compliant assembly systems," *Transactions of the ASME, Journal of Mechanical Design,* Vol.125, June, 2003, pp. 262-267.

[83] Zhu, J., and Ting, K.L., "Performance distribution analysis and robust design," *Transactions of the ASME, Journal of Mechanical Design*, Vol.123, 2001, 11-17.

[84] Lu, X., Li, H. X., and Chen, C. P., "Variable sensitivity-based deterministic robust design for nonlinear system." *Journal of Mechanical Design* 132.6, 2010, p 064502.

[85] Liu, H., Chen, W., and Sudjianto, A., "Probabilistic sensitivity analysis methods for design under uncertainty," *Proceedings of Tenth AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, Albany, NY, Aug. 2004.

[86] Beyer, H., and Sendhoff, B., "Robust optimization–a comprehensive survey," *Computer Methods In Applied Mechanics and Engineering*, 196.33, 2007, pp. 3190-3218.

[87] Hwang, K. H., and Park, G. J., "Development of a robust design process using a new robustness index," *In ASME 2005 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, 2005, pp. 231-241.

[88] Trujillo, A. E., and de Weck, O. L., "Contingency Operations for Failures in a Generalized Mars Transit Architecture," *48th International Conference on Environmental Systems,* 2018.

[89] NSA, "*Defense in depth: A practical strategy for achieving Information Assurance in today's highly networked environments*," 2012.

[90] Drouin, M., Wagner, B. J., Lehner, J., and Mubayi, V. *Historical Review and Observations of Defense-in-depth*. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2016.

[91] Levri, J. A., Vaccari, D. A., and Drysdale, A. E., "Theory and Application of the Equivalent System Mass Metric," S*AE Technical Paper* No. 2000-01-2395, 2000.