

## SURETY OF HUMAN ELEMENTS OF HIGH CONSEQUENCE SYSTEMS: AN ORGANIC MODEL

Chris Forsythe and Caren Wenner

Sandia National Laboratories

Albuquerque, New Mexico

[jcforsy@sandia.gov](mailto:jcforsy@sandia.gov), [cawenne@sandia.gov](mailto:cawenne@sandia.gov)

Despite extensive safety analysis and application of safety measures, there is a frequent lament, “Why do we continue to have accidents?” Two breakdowns are prevalent in risk management and prevention. First, accidents result from human actions that engineers, analysts and management never envisioned and second, controls, intended to preclude/mitigate accident sequences, prove inadequate. This paper addresses the first breakdown, the inability to anticipate scenarios involving human action/inaction. The failure of controls has been addressed in a previous publication (Forsythe and Grose, 1998). Specifically, this paper presents an approach referred to as “surety.” The objective of this approach is to provide high levels of assurance in situations where potential system failure paths cannot be fully characterized. With regard to human elements of complex systems, traditional approaches to human reliability are not sufficient to attain surety. Consequently, an Organic Model has been developed to account for the organic properties exhibited by engineered systems that result from human involvement in those systems.

### HISTORY OF SURETY

Surety has its roots in the design of modern-era nuclear weapons. Because of the unacceptable consequences of an accidental nuclear detonation, very high levels of assurance have been mandated. To attain this assurance, a somewhat unique approach to safety design was developed. In particular, a design theme was employed that called for isolation of a weapon’s critical components from unintended sources of energy. This led to designs utilizing an exclusion region barrier that if unintentionally breached, would leave the weapon irreversibly inoperable (i.e., weaklink). This same barrier provided a channel for transmission of intended electrical signals, but only allowed operation in response to a unique signal with a very low probability of natural occurrence (i.e., stronglink).

In subsequent years, the concept of surety has been expanded to address other domains (e.g., transportation, security, critical infrastructures). By definition, surety seeks to go beyond traditional systems engineering. Furthermore, surety seeks a synergy between the safety, security and reliability of engineered systems. Generally stated, surety emphasizes the application of “basic principles” to provide assurance when there is potential for high consequences and it is either impossible, or impractical, to characterize all potential failure paths.

### Traditional Human Factors and Surety

Historically, human error has been a tremendous concern for the Surety community. In fact, these concerns served as a catalyst for the advancement of

Human Reliability Analysis (HRA) (Swain and Guttman, 1983). In HRA, various mechanisms are employed to represent human involvement in an engineered system and identify potential human errors that could lead to system failures. Probabilistic Risk Assessment has utilized HRA for quantitative estimates of human error potentials. However, the preferred use of HRA is to identify measures to lessen the potential for system failures attributable to human error. The resulting contribution to safety should not be underestimated. However, at a fundamental level, HRA is not sufficient to attain surety.

Traditional HRA hinges on the ability to completely specify human actions affecting a system, including human errors. This task exceeds reasonable expectations, but the remedy is to focus on assuring that the HRA has captured the more likely events. Guidance concerning potential unanticipated actions is limited to assurances that measures that improve safety associated with recognized threats should lead to greater safety overall. HRA is a valuable tool and its application should be encouraged; however HRA alone is not sufficient to attain the highest levels of assurance.

### AN ORGANIC MODEL

A system is a regularly interacting or interdependent group of entities forming a unified whole (Merriam-Webster Dictionary, 2000). These entities can be people, procedures, materials, tools, equipment, facilities, or software operating in a specific environment to perform a specific task or to achieve a specific purpose or mission. Traditional systems analysis considers the system as an integrated whole, and uses a

mechanistic, electrical or similar model to represent the operation of each item in the system. However, one difficulty with that approach is that people bring unique capabilities, vulnerabilities and susceptibilities to the system that are difficult to model, understand or predict using the traditional systems engineering approach.

A different approach to understanding the role of people in systems is to recognize that the inclusion of people in the system makes the system itself an organic system. Thus, the system will exhibit the same organic characteristics as all living things. A review of biology textbooks (e.g., Farabee, 2000) identifies the following characteristics of living things: organization, homeostasis, sensitivity, metabolism, reproduction and heredity, growth and development, and adaptation.

Furthermore, living organisms do not exist in isolation. They are part of larger ecosystems, which encompass all of the relationships between groups of organisms with each other and with the environment. The role of people in an engineered system is comparable in that individuals are each entities that interact with various other entities in the system.

Engineered systems are ordered systems that have a range of variability for which the system is tolerant. Beyond that range, the system is intolerant of variability and may be susceptible to failures and accidents. The organic properties suggest sources of variability that is attributable to the inclusion of humans in the system.

Each of the characteristics of living systems and their associated organic properties are described below.

## Organization

Living systems are very complex. Single cells are organized into tissues, tissues are organized into organs, and organs are structured into organ systems. These systems, such as the musculoskeletal, respiratory and circulatory systems, ensure that the living organism is able to maintain homeostasis. However, each of these organ systems has limitations on its functions. Beyond individual organisms, there are complex, multi-layer, relationships that exist between different living organisms within larger-scale systems.

*Organic Property 1: Biological Limitations.* This property encompasses limitations that are a consequence of the physical capacities of the body, such as limits in performing mechanical work and adjusting to extreme temperature conditions. Additionally, since information processing limitations may be attributed to the functional capabilities of the brain and sensory organs, these are also considered biological limitations. Where engineered systems can tolerate little variability in human performance, situations that impose undue

physical and information processing demands may create conditions outside acceptable bounds.

*Organic Property 2: Meta-Systems.* Organic systems exhibit emergent properties. When individuals of a species regularly co-exist, culture emerges. In humans, this is reflected in the commonality of values and beliefs that exists within different groups. The design of engineered systems typically reflects the values and beliefs of the designers, managers, owners, rulers or some other group with sufficient influence. Theoretically, a system may be engineered to be independent of values and beliefs, but it may be argued that this is an unrealistic expectation in practice. Variability may arise when individuals bring values and beliefs that are contrary to those that guided the engineered system design.

## Homeostasis

All living systems aim to maintain a stable internal environment, though this environment is never static. The system must continuously adjust to changes in its internal state.

*Organic Property 3: Constant Fluctuations.* Metabolism is essential to living organisms. However, precise control of metabolic processes is not possible through neural-hormonal mechanisms. This results in cyclical patterns of activity as the endocrine system overreacts to food intake and subsequently, undergoes a series of corrective responses. This pattern is typical of feedback-controlled processes in organic systems. Furthermore, it may also be observed with feedback-controlled processes at individual and organizational levels.

In addition to the fluctuations that result from imprecise feedback control, organic systems also exhibit fluctuations that are chronologically driven. The biological clock, with its 24-hour circadian and constituent ultradian cycles, is one example. Physiological processes such as brain activity and body temperature, with behavioral corollaries (e.g., alertness and vigilance), fluctuate on a daily basis. However, there is often an implicit assumption in engineering design that human performance is constant, immune to these cyclical fluctuations.

*Organic Property 4: Susceptible to Perturbations.* The sustained function of an organic system often requires that a balance be maintained between competing forces. Events may disrupt this balance leading to shifts in emotional state manifested through variability in behavior, or abnormal behavior. The same perturbations may also be exhibited at an organizational level. One example would be the organizational instability that

sometimes results when an influential individual departs leaving no clear successor.

*Organic Property 5: Non-Linear Behavior.* In organic systems, it is not uncommon to observe non-linear behavior. With these phenomena, a gradually shifting or steady state is punctuated by a period of rapid change. Non-linearity is observed in state transitions. Here, after exceeding some critical threshold, a system undergoes a massive transformation as it moves into a distinctly different state. Punctuated equilibrium also occurs. In these cases, prolonged periods of quiescence are interrupted by brief periods of profound upheaval.

Engineered systems are susceptible to the same phenomena. The human counterpart can be observed in panic or mob behavior. Similarly, the dissemination of information (e.g., rumors) or behavior (e.g., fads) may exhibit exponential properties. Engineered systems tend to favor linear representations of human activities. Consequently, the variability resulting from non-linear behavior may exceed the tolerances of the engineered system.

### Sensitivity

Living systems are able to detect and respond to stimuli in their environment. Some of these responses (behavior) are innate, while others are learned.

*Organic Property 6: Basic Instincts.* Whether truly instinctual, or the product of either learning or epigenetic mechanisms, certain human behavioral tendencies appear to be universal. Often these behavioral tendencies lead to actions that are contrary to one's wellbeing. For example, a scuba diver may panic and rapidly ascend to the surface despite knowledge of the associated safety risks. The fight or flight reflex illustrates a behavioral phenomenon considered to be instinctual. Concern arises because these tendencies may prompt behavior outside the bounds of an engineered system.

*Organic Property 7: Affordances.* Whereas instincts address the inherent tendency for situations to induce certain patterns of behavior, affordances represent an innate propensity to recognize meaningful aspects of the environment. Certain smells may have a quality that makes them universally repulsive. Certain sounds may connote specific sensations (e.g., urgency, danger). Affordances may be effectively utilized to reduce variability by directing activity in accordance with desired pathways. However, violations may be a source of confusion and in general, it will be more difficult to curtail variability where engineering design is in opposition to basic affordances.

### Metabolism

Living systems require energy to function, and this energy is often obtained from the environment. Also, energy is released to the environment. This energy exchange is performed in living systems through chemical reactions, and is illustrated by ingestion, secretion and excretion.

*Organic Property 8: Energy Exchange.* Energy, in the form of information, supplies and other resources, is constantly flowing through an engineered system and is needed for the system to sustain normal operations. Living organisms are non-equilibrium ordered systems (Kauffman, 1995) that require energy to sustain an ordered state. Similarly, engineered systems need energy to maintain an ordered state. For example, an organization must provide training to ensure the competency of its workforce.

Variability may result when there is insufficient energy available to sustain essential order, or when energy is misdirected and is not applied at the necessary points within the system (e.g., throwing good money after bad).

### Adaptation

Living systems are continuously adjusting to changes in the environment.

*Organic Property 9: Adaptation.* To survive, organisms must possess an ability to adapt to changes in their environment. Learning is a prominent means of adaptation that allows organisms to supersede innate limitations. Adaptation may be beneficial to an engineered system and it is the associated capacity to respond to unanticipated events that is often the justification for employing human-in-the-loop designs. In fact, human adaptation will often sustain poorly engineered systems. However, as illustrated by situations involving excessive workload, in adapting to ongoing environmental conditions, humans sometimes introduce behavior that is contrary to the wellbeing of the engineered system (e.g., attentional fixation).

*Organic Property 10: Self-Organizing.* Despite rare counterexamples, humans generally desire social contact. There exists a compulsion to form and sustain social affiliations. By design, engineered systems specify that communication should follow certain channels. Due to the human tendency for affiliation, as well as pre-existing social affiliations that humans bring to an engineered system, social entities emerge that overlay the engineered system. This can be adaptive in that within an organization, often, there are numerous informal channels of communication that are essential to the ongoing functioning of the organization. However,

informal affiliations also increase the degree of coupling between elements of an engineered system increasing the complexity of the system and the potential for fatal interactions (Perrow, 1999).

### **Reproduction and Heredity**

Living systems are characterized by their ability to reproduce, and to pass along traits to their offspring.

*Organic Property 11: Propagation.* For successful adaptations to endure, there must be some means of propagation. Organic systems exhibit various mechanisms for accomplishing propagation. In intelligent organisms, observational learning and cultural transmissions provide mechanisms for behavior transference. With engineered systems, when adaptations arise that deviate from the design intent of the engineered system, such deviations cannot be assumed to be isolated events. For example, if an experienced technician takes an unadvised short cut and there are no immediate repercussions, seeing the resulting efficacy of the short cut, the technician's apprentices and co-workers may adopt the same behavior. As this pattern is repeated, there is diffusion. Consequently, this variation in the engineered system propagates.

*Organic Property 12: Individual Differences.* Genetic variability is essential to the adaptation and perpetuation of species. Furthermore, epigenetic processes provide a second mechanism that creates enduring variability in certain skills and traits. To the extent that an engineered system aims to be inclusive, it must tolerate individual differences in physical, sensory and cognitive capabilities.

### **Growth and Development**

Living systems continue to grow and develop throughout their life cycle. This process brings about both biological and psychological changes.

*Organic Property 13: Maturation.* Over the life span of a living organism, there is predictable variation in physical capabilities and behavioral drives. In larger scale organic systems, maturation may also be observed (e.g., transformations that accompany climate change or significant extinction). It may be anticipated that an engineered system will similarly mature exhibiting discernable life cycles. Maturation is a source of variability and may profoundly affect processes essential to sustainment of an engineered system.

## **APPLICATIONS**

There are three major applications that are envisioned for the Organic Model. First, the model can be used to develop assessment tools for gauging vulnerabilities associated with personnel, and developing and assessing associated controls.

A second application of the Organic Model uses the model as a framework to guide post-incident investigations.

Finally, the Organic Model may also be used as a basis for a realistic agent-based representation of human behavior.

## **CONCLUSION**

The organic model provides a new framework for considering human variability in engineered systems. It recognizes that these systems take on organic properties when humans are introduced, and that human involvement is present at all levels of the system. Understanding the variability in the system, which may lead to errors, necessitates a better understanding of the root of that variability. The Organic Model offers an alternative perspective that provides insight into the sources of human variability.

## **ACKNOWLEDGMENTS**

This work was supported by the United States Department of Energy under Contract DE-AC04-99/AL85000.

## **REFERENCES**

- Farabee, M. (2000). **The On-Line Biology Book.** <http://gened.emc.maricopa.edu/bio/bio181/BIOBK/>
- Forsythe, C. and Wenner, C. (1999). **Flawed Assumptions, Models and Decision Making: Misconceptions Concerning Human Elements in Complex Systems.** Paper presented at the High Consequence Systems Surety Conference, Albuquerque.
- Forsythe, C. and Grose, E. (1998). Human Factors in High Consequence Manufacturing Systems. **SME Technical Paper MM98-105**, Paper presented at AUTOFACT '97, Detroit.
- Kauffman, S. (1995). **At Home in the Universe: The Search for Laws of Self-Organization and Complexity.** Oxford: Oxford University Press.
- Merriam-Webster Dictionary** (2000). <http://www.m-w.com>
- Perrow, C. (1999). **Normal Accidents: Living with High-Risk Technologies.** Princeton: Princeton University Press.
- Swain, A. and Guttman, H. (1983). **A Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.** NUREG/CR-1278. Washington D.C.: USNRC.