A FRAMEWORK FOR ASSESSING AND MANAGING THE RISKS OF ADVANCED NUCLEAR ENERGY SYSTEMS

William E. Kastenberg

Nuclear Engineering Department
4103 Etcheverry Hall
University of California at Berkeley, Berkeley, California, 94702-1730
kastenbe@nuc.berkeley.edu

Abstract – This paper is intended to provide some preliminary thinking regarding the foundations and general framework for assessing and managing the risks of Generation IV nuclear energy systems. The keyword here is system, in that an “ecological” approach is required. Formally, ecology is defined as the study of the biological relationships between a living organism and its environment. Our approach is based on recent developments in complexity theory, especially in the area of networks and “scale-free” systems that appear in various fields such as ecology, percolation theory and in nonlinear dissipative systems. We also indicate how these concepts and theories can be applied to nuclear energy systems.

I. INTRODUCTION

Risk assessment to date has been used primarily as a retrospective process. Risk assessment came of age with the publication of the Reactor Safety Study (WASH-1400) in 1975, but only after approximately 75 nuclear power plants already had been designed, built and operated in the U.S. Indeed, the U.S. Nuclear Regulatory Commission’s (NRC) Policy Statement on quantitative safety goals in 1986 could not have been adopted without a robust methodology for assessing the risks of accidents at today’s nuclear power plants.1

We are now challenging the field of risk assessment to be prospective, i.e. to consider the undesirable consequences of a new generation of nuclear power plants before they are fully developed and deployed. It is our belief, however, that risk assessment and risk management as currently conceived and practiced may be lacking in its accuracy and completeness when addressing risk concerns related to the advanced reactors now being considered and developed.2, 3

Underlying the Generation IV approach to nuclear energy is an emphasis on both the entire fuel cycle and the context within which the nuclear fuel cycle will be deployed. This dual emphasis is manifest in the form of “Goals” in four areas: sustainability (in terms of natural resources and nuclear waste), economics (in terms of life-cycle cost and financial risk), safety and reliability (in terms of safe and reliable operation, risk of reactor core damage and offsite emergency response), and proliferation resistance and physical protection (in terms of diversion of nuclear materials and protection against acts of terrorism). Hence we are now confronted with assessing and managing the risks of a complex nuclear energy system, i.e. a nuclear power plant that is embedded in a nuclear fuel cycle, which in turn is embedded in environmental, economic, political and social systems.

This paper is intended to provide some preliminary thinking regarding a newly funded University NERI (Advanced Nuclear Research at Universities Program) project designed to develop the foundations and a framework for a new approach to risk analysis (assessment and management) that is congruent with the complexity, uncertainty and ambiguity inherent in this new generation of nuclear energy systems currently being developed. We present the foundations and general framework for assessing and managing the risks of a nuclear energy system. The keyword here is system, in that an “ecological” approach is required. Formally, ecology is defined as the study of the biological relationships between a living organism and its environment. In our approach, rather than focusing on the elements of the system (e.g. the reactor, the fuel processing plant, etc.) we will consider the fuel cycle as a network, and define risk in terms of overall system behavior and properties as derived from the relationships.
II. THE NEED FOR A NEW RISK ANALYSIS FRAMEWORK

The NRC Policy Statement on Advanced Reactors calls for, among other things, designs that are much simpler than the current generation of nuclear power plants, that rely on passive safety systems to the extent possible, and that minimize operator action in the event of an accident. A summary of “near term” reactors (called Generation III and Generation III+ reactors) that can, in principle, meet the criteria set forth by the NRC is summarized in the so-called “2010 Roadmap” report. Building on this design experience, and laying the foundation for a new and highly innovative approach to nuclear energy is the U. S. Department of Energy (DOE) program for Generation IV nuclear reactors described in the “Technical Roadmap Report for Generation IV Nuclear Energy Systems” that was recently released.

As noted in the technical roadmap report, there are unique risk issues regarding the nuclear reactor power plant itself, and a need for a “simplified” PRA methodology to identify design-basis accidents and transients as well as any highly “hypothetical” sequences. Of particular concern in the technical roadmap is “the failure of passive components” that requires a “complex understanding of physical and human factor ingredients.” The technical roadmap goes on to state: “This poses an issue for PRA methodology because there is less experience in modeling passive systems compared to active systems. Moreover, system-specific operating data are sparse and may not provide statistically useful information.”

What is not mentioned in the technical roadmap is the need for an overall strategy for assessing and managing the risk of the integral fuel cycle, including the issues related to sustainability, economics, safety and reliability, and proliferation/protection. The requirement of meeting the Generation IV goals in each of the four areas may result in competing challenges, e.g. satisfying proliferation/protection-oriented goals may be counterproductive to enhancing safety.

Kline and Renn list three challenges for managing the risks of such systems: dealing with complexity, uncertainty and ambiguity, all correlated with one another. Uncertainties may be of four types: aleatory, epistemic, indeterminacy, and ignorance. Ambiguity refers to the, “variability of (legitimate) interpretation based on identical observation or data assessments. Ambiguity may come from differences in interpreting factual statements about the world or from differences in applying normative rules to evaluate the state of the world.” It is not at all clear that our current reductionist approach to risk analysis is adequate for dealing with the complexity, uncertainty and ambiguity of the proposed Generation IV nuclear energy systems being considered. Moreover, the traditional Utilitarian or “consequentialist” approach, as manifested in risk/cost/benefit analysis, may also be inadequate because of the uncertainty and ambiguity in risk (a subject for a subsequent research project).

The risk analysis framework which has been developed and employed to-date works well when the system under consideration has historical or actuarial data on initiating events and failure rates, and empirical data on public health and environmental impact. Moreover, the system must be fairly well defined, has (assumed) fixed or rigid boundaries and where second order effects are (assumed) small. As such, it is amenable to decomposition in terms of fault and event trees, containment trees and dose-response models.

III. A SHIFT FROM COMPLICATED TO COMPLEX

Because we believe that the newest advances in nuclear energy systems require a new paradigm for risk analysis, it is useful to reiterate here some of the basic differences between the old and the new. The key distinction we draw is between systems that are "complicated" and systems that are "complex".

As noted above, the context within which the current generation of nuclear power plants is understood is based on a reductionistic or linear worldview. This worldview is atomistic, deterministic and dualistic. In other words, the behavior of these complicated systems can be: (1) understood by studying the behavior of their component parts, (2) deduced from cause and effect (a search for causal links or chains), and (3) determined independent of the observer, that is, only deduced from "objective" empirical observations.

The context within which the proposed Generation IV nuclear energy systems, we believe, should be understood is based on a nonlinear worldview. This worldview gives rise to complex systems that are characterized by at least one of the following: (1) holistic/emergent—the system has properties that are exhibited only by the whole and hence cannot be described in terms of its parts, (2) chaotic—small changes in input often lead to large changes in output and/or there may be many possible outputs for a given input, and (3) subjective—some aspects of the system may only be described subjectively. Hence there may be system properties not exhibited by the parts alone, there may not be a causal relationship between input and output or the output may be path dependent, and there may not exist an analytic description for the system.

It should be noted that the impacts of nuclear energy on both society and the environment (from developing nuclear power plants to deploying nuclear weapons) have always been complex. In the past, however, the only undesirable consequences of a nuclear power plant considered in a PRA were geographically local (public health effects out to one mile or 25 miles) or they were
observable in “real” time (the unfolding events at Three-Mile Island). This gave the impression that the current risk paradigm is accurate because locality and observability were two characteristics of the impact. This lens has changed in modern times and yet our practices are still based on the same paradigm. That is, a core melt accident has “global” impacts (a severe accident at one plant affects all plants) and manifests very quickly (e.g., loss of public confidence worldwide). In the case of disposal of radioactive waste, the undesirable consequences are almost imperceptible (e.g., the migration of high-level radioactive waste). Moreover, these impacts may be temporally persistent and/or irreversible (e.g., the degradation of public welfare due to nuclear proliferation).

IV. A POSSIBLE NEW APPROACH TO RISK ANALYSIS

We begin this exploration of a new approach to risk analysis by considering a complex system as: a set of elements, the attributes of these elements, and the relationships among the elements and among the attributes. A “set” implies a boundary, which may be physical or conceptual, and the attributes are expressed as measures or qualities of the elements (e.g., mass, temperature, concentration, on/off, etc). General System Theory and its handmaiden, cybernetics, provide useful concepts for understanding the nonlinear processes by which a general system is stabilized and organizes itself, as well as the processes by which information is received, exchanged and used to adjust to changes in the external environment. A cybernetic event is one in which the output of a system (its behavior) is measured and “fed back” to the system’s sensors so that the system’s performance, with respect to a set of pre-established goals, can be determined. Hence a general system is “goal seeking” and its goal is to search for equilibrium or balance (homeostasis). We say that such a system is “self-organizing” or “adaptive.”

The main characteristics of a general system are as follows:

- The system cannot be reduced to its parts without altering its relationships.
- The system is not only a whole, but also a part within a larger whole. Hence, it is a subsystem within a larger system, the character and functioning of which is integral and co-determinative.
- The system has permeable boundaries and is continually in a process of exchanging mass, energy and information with its environment.
- The system stabilizes itself through negative feedback; i.e., it will adjust its output to produce and sustain a match between the input it receives and its programming.

- With positive feedback a mismatch between input and programming occurs, and the system either searches for a new equilibrium state within more inclusive negative feedback loops, or it collapses.
- The system’s behavior may be stochastic or chaotic, achieving equilibrium through a “trial and error” process.

It is often said that for these complex general systems, “the whole is greater than the sum of the parts.” This statement means that there is an emergent property (or emergent quality) that cannot be exhibited by the parts alone. A classic example of an emergent property has to do with the chemical compound we call water. While the atomic weights of two atoms of hydrogen and one atom of oxygen are the same as $\text{H}_2\text{O}$, and while hydrogen and oxygen are a gas at ordinary room temperature, water has the emergent property of wetness. In the same manner, living organisms can be dissociated into their component organs, tissues, cells, etc. Quantitatively, nothing is lost, but qualitatively, life is lost; the organism is no longer living.

In developing a new operational definition of risk, we will rely heavily on recent advances in Network Theory and on a model, which reflects the new understanding of living (biological/ecological) systems. Summarizing Capra, living systems possess three criteria:

- Pattern of organization: (the configuration of relationships that determines the system’s essential characteristics),
- Structure: (the physical embodiment of the system’s pattern of organization), and
- Life process: (the activity involved in the continual embodiment of the system’s pattern of organization).

Of particular relevance to understanding pattern and structure are the recent advances in Network Theory. A network, like a general system, can be described by a set of nodes (elements) and links (connections which describe a set of relationships between the nodes). The links can convey mass, energy and information between the nodes. Until recently, networks such as electric power grids, river drainage systems, and the Internet were thought to be either ordered (a set of nodes in which each one is linked to a specific number of nearest neighbors) or random (the set of nodes are connected in a haphazard way). It is now understood that many of these systems are of a third kind called “small world” networks. A simple example of a small work network is an ordered network with a few random links connecting distant nodes. The ordered connections or links are called “strong” links, while the few random connections are called “weak” links.

Small world networks can be divided into two types called egalitarian and aristocratic. Egalitarian networks have roughly the same number of links per node, which appears to be typical for electric power grids, and the neural networks of the brain. On the other hand,
aristocratic networks such as the Internet, airline networks, certain social networks and certain economic networks have a great disparity in the number of links per node. The latter are said to be an example of “the rich getting richer” as the network grows. Such “rich” nodes are called hubs.

According to this new theory of networks, when consistent patterns emerge at every level of complexity, we have what are called scale-free, and which follow the same “power-law” distribution (a straight line on a log-log plot) as the “self-similar” rules that have been discovered recently in ecological systems. A number of investigators have developed theories that shed light on why such natural systems (from geophysical to astrophysical, and from biological to ecological and social) exhibit self-similarity, power laws, universality classes, and other signatures of criticality as an emergent quality. Of particular interest to this project is the recent work by Carlson and Doyle, and by Fabricant, Koutsoupia, and Papadimitriou which focuses on complexity in designed systems. Carlson and Doyle introduce a mechanism for generating power law distributions for complex systems that are optimized, either through natural selection or engineering design, to provide robust performance despite uncertain environments. They suggest that power laws in these systems are due to tradeoffs between yield, cost of resources and, tolerance to risks. These tradeoffs lead to highly optimized designs that allow for occasional large events. Fabricant and colleagues suggest that the scale free topology of the Internet is a result of complex multi-objective optimization.

Of particular interest to this proposed project is the robustness of these scale free systems or networks when they are threatened, i.e. are under attack. Numerical simulation appears to indicate that small world networks are more robust (fail gracefully) than either ordered or random networks, when various nodes or links are removed. In a comparison between an aristocratic small world network and a random network, the aristocratic network was more robust with respect to random failures and the random network more resistant to a coordinated attack against the hubs. It is the random failure of the unimportant nodes (connected by the “strong” or ordered links) that make the small world networks robust with regard to random failures; and it is the reliance on the hubs that make them susceptible to a coordinated attack. Hence, both redundancy and diversity are important to the robustness of a network, a lesson already learned in the design of engineered systems such as a nuclear power plant.

We can then conjecture that once a complex system such as a network is characterized as being ordered, random or small world, it is possible to ascertain how mass, energy and information is exchanged within that network, and based on that, to determine how prone or not that network is to failure. In other words, it is possible to assess the risk associated with that network.

It is in terms of this general system model for living systems (pattern, structure and process) and with particular emphasis on scale free networks that we wish to base our new approach to risk assessment. Working from holism rather than reductionism, we intend to develop the hypothesis that in order to evaluate the impact of complex nuclear energy systems on the ecology of life, we must expand from only considering the elements themselves (failures of pumps, valves, etc) to include both the relationships among the elements and any emergent qualities of the system being assessed. In these systems, the relationships among the elements (sometimes called “lower level” or “local” relationships) are not dictated by some central processor or authority, but rather are integral to the pattern, structure, and process of the system. Moreover, these lower level relationships give rise to emergent qualities in much the same way that the “one-on-one” simple relationship between any two insects in a colony give rise to the global properties of the insect colony. In a sense, the integrity of the colony’s emergent properties is a global measure of the health of this nonlinear system in the same way that the value of risk is a summative measure for a linear system. Hence, we wish to begin our exploration of risk for these complex systems with the potentials for degradation of emergent property integrity as well as the degradation in the relationships that contribute to the emergent property.

V. RESEARCH AGENDA

We propose to carry out this project in three phases. The first phase will focus on the development of a new framework for assessing the risk of complex nuclear energy systems. Beginning with the basic principles of General System Theory, a generic nuclear fuel cycle embedded in an environmental, economic and sociopolitical system would be constructed. The fuel cycle network would include the resource (mining) and the waste (final disposal), as well as aspects of the sociopolitical system (in terms of nuclear weapons).

Constructing, qualitatively analyzing and eventually quantifying an updated fuel cycle network for Generation IV nuclear energy systems will be the prime focus of this first phase. In carrying out this phase of the work, we will rely heavily on the work of Carlson and Doyle. In their seminal paper they state: “The specific models we introduce are not intended as realistic representations of designed systems...Our goal is to take the first step toward more complicated structure in the context of familiar models to illustrate how even a small amount of design leads to significant changes in the nature of an interconnected system.” Our approach then, is to extrapolate from these simple models to the complexity of a nuclear fuel cycle.
The second phase will focus on the application of Phase 1 results to a Generation IV nuclear energy system. Candidate instrumental definitions of risk would be considered for a fuel cycle network such as shown in Figure 1 and a methodology for qualitatively or quantitatively assessing risk would be developed. This approach would focus on the pattern of organization as well as its structure and any emergent qualities of the nuclear energy system. Object oriented computer codes such as STELLA and computing languages such as C++ are especially amenable for quantifying such complex networks. Our new understanding of emergence considers that in complex systems, order arrives from the “bottom up” and not from the “top down.” Such systems display emergent behavior: the movement from low-level rules to higher-level complexity. For example, the single failure criterion utilized in the design of a nuclear power plant leads to the concepts of redundancy and diversity. These concepts in turn, lead to the sophisticated logic of multiple trains at the system level (e.g. the auxiliary feedwater system in a PWR) and multiple systems at the functional level (e.g. high and low head injection and core spray in a BWR).

The third phase of the research will consider an approach to risk management in terms of safety goals and cost/benefit considerations.

As noted above, complex systems that exhibit power law distributions (scale free or self-similar patterns) are robust with respect to random failures and are prone to large catastrophic events. As suggested by Newman and co-workers, a degree of risk aversion can be incorporated into highly optimized systems in order to protect against catastrophic events. The net effect is to truncate the tails of a power law so that the probability of disastrously large events is dramatically lowered, giving the system more robustness. We will explore this approach as means of managing the risks of an advanced nuclear energy system. Beginning with the NRC Safety Goals (two qualitative and two quantitative) for existing nuclear power plant operations, appropriate qualitative or quantitative lower-level or subsequent goals would be developed paralleling the Generation IV design goals, as well as an overall safety target. This aspect of the research would also be applied to a Generation IV nuclear energy system as well as the results of the Phase 1 and 2.

V. SUMMARY AND CONCLUSIONS

In this paper we have outlined the development and the foundations for a new framework for risk analysis that can be used for Generation IV nuclear energy systems. As noted by the National Research Council, risk characterization should be a decision driven activity, directed at informing choices and solving problems. Given the present state of development of these systems, risk analysis can be used as a design tool, assessing options for reducing risk as well as ensuring compliance with NRC regulations. Our ultimate objective then, is to develop an approach for assessing and managing the risks of Generation IV nuclear energy systems that can be used in both design and the regulation.

ACKNOWLEDGMENTS

This work was supported in part by the U.S. Department of Energy under Grant No. DE-FC07-051D14666. The views expressed in this paper are due to the author alone, and do not necessarily reflect the views of neither the granting agency nor any other institution.

REFERENCES