TECHNOLOGY-NEUTRAL NUCLEAR POWER PLANT REGULATION: IMPLICATIONS OF A SAFETY GOALS-DRIVEN PERFORMANCE-BASED REGULATION

MOHAMMAD MODARRES
Department of Mechanical Engineering
University of Maryland
College Park, MD 20874, USA
E-mail : modarres@umd.edu

Received May 16, 2005

This paper reviews the pivotal phases of the evolution of the current technology-dependent nuclear power safety regulation in the United States. Understanding of this evolution is essential to the development of any future regulatory paradigm, including the technology-neutral regulatory approach that the U.S. Nuclear Regulatory Commission (NRC) has recently embarked on to develop. The paper proposes and examines the implications of a predominately rationalist and best-estimate probabilistic regulatory framework called safety goals-driven performance-based regulation. This framework relies on continuous assessment of performance of a set of time-dependent safety-critical systems, structures and components that assure attainment of a broad set of technology-neutral protective, mitigative, and preventive goals. Finally, the paper discusses the steps needed to develop a corresponding technology-neutral regulatory system from the proposed framework.

KEYWORDS : Risk-Informed, Technology Neutral, Performance-Based, Advanced Reactor Regulation

1. INTRODUCTION

This paper summarizes a study of the implications of a technology-neutral regulation for advanced nuclear power plant designs and proposes a predominately rationalist approach to future nuclear plant regulations. The current body of regulations has been developed and evolved over the past 50 years with consideration of the knowledge and incidents experienced from operation of the Light Water Reactors (LWRs). While the body of the U.S. nuclear regulations has many provisions independent of specific reactor technologies, it also contains many LWR-specific regulations. A respectable set of safety regulations now forms the basis for licensing the LWRs, as well as for certifying the Advanced Boiling Water Reactor (ABWR), System 80^{+} and AP-600 reactor designs. In reviewing or licensing other than LWR designs (e.g., Ft. St. Vrain, Clinch River Breeder Reactor), the NRC staff had to establish the applicability of its regulations to these designs. Often such reviews required case-by-case exemptions and/or additional requirements to address the unique features of these designs. This, however, is not an efficient and effective approach to reactor licensing and could result in undue delays and prohibitive costs in licensing future advanced reactor designs.

Recently, with the renewed interest in future plant licensing, the NRC staff has been working with the vendors and the U.S. Department of Energy (DOE) toward certification of the AP-1000 reactor design, Gas Turbine Modular Helium Reactor (GT-MHR) which is a 600 Mwt High Temperature Gas-Cooled Reactor (HTGR), Advanced CANDU Reactor (ACR-700) and soon DOE's Generation IV reactors.

To avoid "reinventing" the regulations every time a new technology arises some very important questions that need to be addressed have been asked in SECY-02-0139 [1]. Examples of these questions are:

- Should specific defense-in-depth attributes be defined for non-LWRs?
- To what extent PRAs can establish plant licensing basis?
- Can a plant be licensed without a containment building?
- Can emergency planning zones be reduced?

Any change in regulations requires understanding of the history and evolution of the present body of regulations to appreciate the rationale and significance of specific elements and provisions of such regulations. Of particular interest in this paper is to highlight the origin of the defense-in-depth concept in specific, and the basis of the

present predominately structuralist [2] approach to regulating nuclear reactors in the United States in general. The paper examines the emergence and uses of probabilistic methods and applications of risk information in future nuclear plant regulations. Finally, implications of a predominately rationalist approach [2] to regulation will be discussed.

2. ORIGIN OF NUCLEAR SAFETY REGULATION

Nuclear regulation in the United States was the responsibility of the Atomic Energy Commission (AEC), a 5-member Commission which Congress first established as part of the Atomic Energy Act of 1946 to maintain strict control over atomic technology and to exploit it further for military applications. The 1946 law excluded commercial applications of atomic energy and rested the ownership of the nuclear knowledge with the government. The 1954 Act ended the government's monopoly on technical data and made the need for commercial nuclear power an urgent national goal to promote the peaceful uses of atomic energy provided that: " . . . a *reasonable assurance* exists that such uses would not result in undue risks to the health and safety of the public"

As with most histories of nuclear power, the initial consideration of safety issues begins with the Manhattan Project during the World War II. The chemical engineers of the Du Pont Corporation led the effort to build the nuclear reactors at Hanford, Washington. During the construction process, the chemical engineers disagreed with the physicists over safety issues, especially with Eugene Wigner, who had led the design effort for the smaller, prototype reactors built in Oak Ridge. Using their background in chemical processes, the Du Pont engineers divided the reactor design into smaller, relatively independent subsystems, whose design would be frozen early, so any dependent systems could be designed as well [3]. This created the notion of functional independence, and later gave rise to the concept of "defense-in-depth," which promoted layers of independent "barriers" realizing safety functions to *prevent*, *protect* and/or to *mitigate* release of radioactive substances into the environment. Because the Du Pont engineers lacked a track record with the nuclear technology, they incorporated several safety features to overcome the uncertainties in characterizing the performance and effectiveness of these "barriers", including addition of redundancy, large safety margins, and structures and systems to limit the release of radiation to the environment. In later reactor designs and nuclear facilities, this design concept remained as the principal method of assuring safety and led to remarkably safe nuclear plant designs.

While the "defense-in-depth" concept actually originated in the mid-1940s by the nuclear facility designers, it later played a pivotal role in formulating the body of reactor safety regulations that were crafted by AEC following the 1954 Act. Clearly this concept was an indispensable consequence of inadequate and imprecise knowledge about safety system *design margins* in the early days of the nuclear power industry. In the ensuing years, the defense-in-depth concept adopted by the regulators evolved into a collection of design and operating requirements including:

1. Use of multiple active and/or passive engineered barriers to rule out any single failures.
2. Use of large design margins to overcome lack of precise knowledge about performance of safety barriers under normal or accident conditions.
3. Application of quality assurance in manufacturing and construction.
4. Operation within predetermined safe design limits.
5. Continuous testing, inspections, and maintenance to preserve original design margins.

As defense-in-depth was a means to manage all sorts of uncertainties, the concept took the view that the nuclear regulation must apply it to design, construction and operation to assure that the four uncertain states illustrated in Figure 1 are adequately attained.

This uncertain state approach viewed regulation as a set of detailed prescriptions for how decision making and control (regarding the attainment of these states) can be

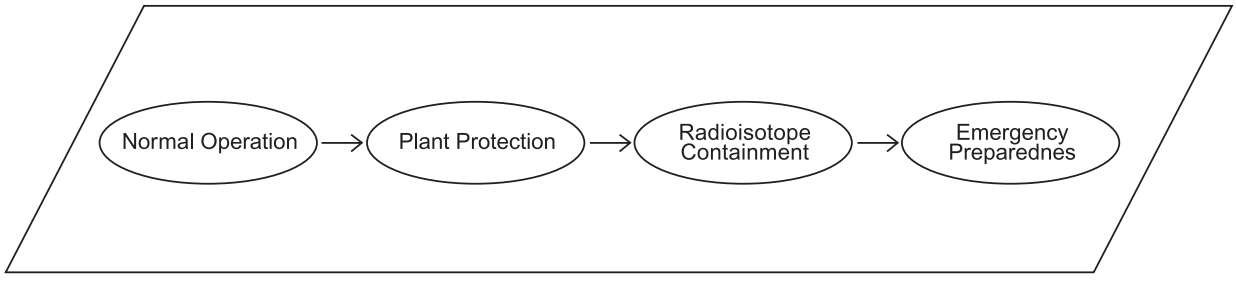

Fig. 1. Defense-in-Depth as "Uncertain States" View of the System

optimally addressed, thus leading to a structuralist approach to regulation. In this approach, the reactor system (design, equipment, procedures, people, etc.) must conform to the defense-in-depth design and safety elements, and to assure that the four key uncertain states can be adequately managed. Since acceptance criteria were needed to measure the extent to which a reactor conformed to the defense-in-depth, AEC considered a reactor system as "safe" if it was able to withstand a fixed set of prescribed accident scenarios *judged* by experts as the most significant adverse events (the so-called Design Basis Accidents or DBAs). Also, the AEC argued that if plants can handle the DBAs, they can also handle any other accidents -- an attempt to eliminate the possibility of plant failure from fundamental design flaws and worst possible accidents. Later, this last claim proved false, when several operational experiences with nuclear plants (e.g., the Three Mile Island accident and other major precursor events to core damage) pointed to the contrary. Nevertheless, the use of DBAs, as well as other prescriptive regulations, led to a body of regulations that were conservative, design-specific, highly prescriptive, and complex.

3. EMERGENCE OF PROBABILISTIC RISK ASSESSMENT

Starting from the mid-1960s, some subsequent events following the establishment and use of the defense-in-depth and DBAs using conservative deterministic methods eventually paved the way to the emergence of Probabilistic Risk Assessment (PRA) methods as an adjunct, prominent force in the nuclear plant regulation. Of special significance was the ability of the PRAs to alleviate the shortcomings of the DBAs, by modeling considerably more realistic accident scenarios. In 1966 Advisory Committee on Reactor Safeguards (ACRS) became concerned that Loss of Coolant Accidents (LOCA) could cause containment breach if Emergency Core Cooling System (ECCS) fails. Subsequently, AEC's focus of safety shifted to *preventing* accidents that threaten containment. In the late-1960s to early-1970s organized opposition to nuclear power grew and characterized AEC's licensing criteria as inadequate and inconsistent. Later, in the early-1970s the Loss of Fluid Tests (LOFT) suggested that the ECCS might not work as DBAs had suggested a steam build-up could prevent injection of water[2]. As a result of these and public pressure, a congressional committee requested that the AEC performs a comprehensive reactor safety study that led to the 1971 – 1974 landmark WASH-1400 Study [4] and the advent of PRA.

In 1974 the U.S. Nuclear Regulatory Commission was created over the concern that AEC's mission of promoting and regulating nuclear power are in conflict. So, it was the NRC that actually inherited and published the final WASH-1400 report and faced some harsh criticisms and media publicity that ultimately in 1978 prompted the NRC to withdraw its support of the WASH-1400 results, while the Commission recommended that the NRC staff use PRA techniques in general.

In March 1979, the Three Miles Island (TMI) accident happened which among other things underlined the fact that the original assumption by the AEC and later by the NRC that if the plants can handle the DBAs, they can also handle any other accidents, is not true. This gave a new beginning to the use of PRAs, as this approach allowed consideration of more realistic accident scenarios, such as the one in TMI, which are now branded as Beyond Design Basis Accidents (BDBAs).

To deal with a more formal definition of safety and answering the question of "how safe is safe enough?" in 1986 the ACRS, after long deliberations, proposed two safety goals and associated quantitative health objectives to articulate levels of acceptable risk, which later served as the de facto guidelines for using PRA results in regulation [5]. The goals provided indices for the level of "public protection which nuclear plant designers and operators should strive to achieve." The Goals meant to provide additional guidance to the NRC staff for regulatory decision-making. Practical implementation of the Goals proved to be difficult because of the large uncertainties involved in calculation of risk. In 1990, the NRC provided additional guidance on the Safety Goals, endorsing surrogate objectives concerning the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF).

The issuance in1988 of the NRC Generic Letter 88-20 required the industry to beef up its expertise in the uses of risk information in plant operations and interactions with the NRC. Subsequent efforts such as the 1990 NUREG-1150 and the 1995 issuance of the PRA policy statement by the NRC gave further legitimacy to the uses of PRA in regulation.

Another important milestone was adoption of the maintenance rule in 1996. This was the first time that maintenance activities were not prescribed, but rather their effectiveness were measured against some preset rules for a group of important components and systems identified by risk assessment as important. This approach offered flexibility, effectiveness and efficiency in maintenance.

Finally, in 1998 NRC published a series of Regulatory Guides including RG 1.174 for changes to plant licenses, and introduced Reactor Oversight Process, with the seven cornerstones defining the "safety scope" of plants in a probabilistic-deterministic fashion. Many other advances in use of risk information in regulations have also occurred since the turn of the century, including risk-informing of many of the NRC regulations. Today's safety regulation

[2] The LOFT experiments were later shown to have scaling issues that showed the concerns with the ECCS did not translate into full-scale power reactor safety systems.

is therefore a complicated mixture of largely structuralist design-specific approach, augmented by risk-informed and performance-based measures.

The NRC views that the reasonable assurance of adequate protection of public health and safety is, as a general matter, defined by the totality of Commission's health and safety regulations themselves. That is, when the applicant or licensee demonstrates compliance with the NRC's regulations, it follows that there is reasonable assurance of adequate protection of public health and safety.

4. IMPLICATIONS OF THE EVOLUTION OF NUCLEAR PLANT REGULATION ON DEVELOPMENT OF A TECHNOLOGY-NEUTRAL REGULATION

We can learn several important lessons from the evolution of nuclear plant regulations. The first and foremost lesson is that the defense-in-depth came as an intrinsic part of the early nuclear facility designs, and as a means of overcoming uncertainty (i.e., lack of adequate knowledge). That is, it accounted for the uncertainty about the *capacity* of a safety system or barrier (for preventing, protecting and mitigating accidents) to withstand or endure *challenges* imposed by internal or external conditions and events (e.g., due to major accident scenarios or transients). The second key lesson is that the defense-in-depth, its constituent elements, and conservative DBAs, while viewed by the Commission as the embodiment of the reasonable assurance of adequate protection of the health and safety of the public, still may fall short of guaranteeing safety as the TMI accident demonstrated. Other safety assessment techniques, such as PRAs would be needed to augment the traditional deterministic safety assurance methods.

Safety regulation can primarily be characterized as "management of uncertainties" about events, phenomena, processes, etc. that challenge or erode capacity of the safety systems and barriers. Since uncertainty is the predominate force and defense-in-depth is only a means to control it, it follows that uncertainty characterization and reduction should be the most fundamental constituent of any future nuclear regulatory framework. Further, a predominately rationalist approach to regulation should form the basis to principally characterize, reduce, and control uncertainties about the performance of barriers (e.g., capacity and challenges which confront safety barriers) in nuclear facilities. Such safety barriers are there to realize certain protective, preventive and mitigative safety functions. The PRA tools, decision theoretic techniques, and all deterministic calculations are only means to assess and manage uncertainties.

Since uncertainties about the availability, capacity and challenges of safety barriers in nuclear facilities were very high in the dawn of nuclear power, the use of the defense-in-depth and its associated elements made perfect sense, for it was practical and legally defendable. However, after some 50^{+} years of experience in power reactor technologies, access to far more advance computational techniques and codes, PRA technologies and tools, and best estimate decision making techniques, uncertainties can be better characterized, estimated, modeled and managed.

To better illustrate this point, consider the following subjectivist view of the categories of uncertainty. Uncertainty arises due to lack of knowledge about a proposition (i.e., it is all epistemic). A further classification of uncertainty, which may prove useful in decision making, is by separating those uncertainties that are characteristically random and impractical to reduce (aleatory), and those that we may treat them as random because of our limited knowledge, but can be reduced (epistemic). Further, the uncertainty is *relative* to the observer's point of view. That is, what the observer "knows" about the state of knowledge (and, hence, uncertainty) is also equally important. Consider Table 1 in which the absolute uncertainty about a proposition (a model, parameter, etc.) and the relative knowledge of the observer about this uncertainty is divided to the dichotomous states of "known" and "unknown".

From Table 1 it is apparent that in an uncertainty management arena, when the observer (e.g., the designer, regulator or operator) completely knows a subject (e.g., capacity or magnitude of challenges imposed on a barrier

Table 1. Categories of Uncertainties and Management Options

	Awareness of Knowledge	
Actual Knowledge	Known	Unknown
Known	No Uncertainty Deterministic Modeling	Reduce/Control Uncertainty by Knowledge Management
Unknown	Reduce/Control Uncertainty by Probabilistic Modeling	Control Uncertainty by Conservatism; Defense-in-Depth

due to a condition or event), then it can be modeled (e.g., modeled deterministically). When the subject is unknown to the observer, but the subject matter itself is known to the literature, then a knowledge management program will be needed to manage this class of uncertainties. This is particularly important for the nuclear industry, as there are no provisions in the nuclear regulations to retain, update and access the whole body of knowledge by both the regulator and the licensee. Another case is when the subject matter is known to the observer, but the literature about the subject is not enough or is even unknown (e.g., does a pipe break by the end of the year?). In this case, it is possible to either reduce the uncertainty (by better tests and developing physics of failure models) or estimate it probabilistically (e.g., from historical occurrences of pipe breaks). This class of uncertainties has been best modeled and characterized by PRAs. Finally, when the subject is unknown both to the observer and to the literature, then means such as conservatism, over-design, defense-in-depth, etc. can be used (e.g., in the cases of terrorism and sabotage).

As discussed earlier, more than half a century of experience in advancing the knowledge about nuclear plant subjects has moved many safety analyses from the lower right quadrant of Table 1 to other quadrants. As such it only makes sense to focus the regulatory process on a rationalist approach to the management of uncertainty and determining the techniques that are best for such management, including the traditional structuralist-based defense-in-depth. This paper proposes a goals-driven performance-based regulation to assess and manage classes of uncertainties discussed in Table 1.

5. PRINCIPLES OF A GOALS-DRIVEN PERFORMANCE-BASED REGULATION

In a prescriptive regulatory approach (also termed structuralist by the ACRS) the collective efforts of the NRC and the nuclear industry are needed to maintain and improve safety. Regulatory oversight of licensee safety is the responsibility of the NRC. Thus, safe performance (but not necessarily safety) reflects the results of the collective efforts of the NRC and the nuclear industry. However, in a prescriptive regulatory regime, the licensee is only required to satisfy the mandated NRC requirements to assure adequate protection of public health and safety. If all actions are taken according to the regulation, but proved inadequate or insufficient to prevent a subsequent accident, one may argue that in the public's eye it would be the regulator's fault. As such, in a deterministic-based regulation, the burden of safety is carried far more on the shoulder of the regulator than the licensee, vendor, or the architect engineer, as they only have to abide by the regulator's requirements. Further, deterministic-based prescriptive regulations tend to be a set of heuristic-based requirements derived from past experiences or unrealistically conservative assumptions. As such, if unsafe situations occur, they prove at best, to be inappropriate. Further, prescriptive approach is contrary to innovation. It is the licensee, vendor, and architect engineers, who should be first and foremost left to innovate, own and ensure the safety of their plant, not the regulator. While safety should be a shared responsibility, the regulator should only set safety goals and be left to rely on its oversight responsibilities to act through a set of careful and forward-looking monitoring of performance monitoring activities to measure attainment of such goals, considering all uncertainties involved.

A goals-driven performance-based regulation [6-8] sets a state to be achieved without mandating a solution. It adds a systematic structure to use the traditional performance-based regulation, in that it guides the regulators and licensee to select and set appropriate goals and means to monitor them. This approach can be applied at any level from the top-level safety goals of the plant downward. It is important to establish clear links between the top-level goals (such as the present NRC safety goals) and critical safety functions, and safety barriers, systems, structures and components. At each level, the regulator may require explicit safety and other *goals*, convincing *methods and arguments* to justify that the goals are met and adequate *evidence* to support the arguments exist. In practice the rigor of the arguments and the amount of evidence will depend on the safety significance of the individual plant safety functions or safety barriers.

In the safety regulation context, *safety performance* has two core constituents: *Capability* and *Availability*. Capability is the ability of the item or barrier (system, structure or component) to realize its intended function(s) under all possible conditions (normal and accidental). For example to assure that an emergency core cooling system has the capacity (e.g., adequate flow) to overcome all challenges (e.g., transients and LOCAs) and cool the reactor. In a best-estimate approach to measuring capability, the concept of challenge vs. capacity may be used. As there are uncertainties associated with the measures of capacity (strength, endurance, maximum flow capability, etc.) and with the measures of challenge (stress, cumulative damage, minimum flow requirements, etc.), such uncertainties must be estimated and characterized. For example, considering challenge and capacity as uncertain random variables (i.e., the type described in the lower left quadrant of Table 1), then

$$\text{Capability Value} = \Pr(\text{Capacity} > \text{Challenges} \mid \text{all conditions}) \quad (1)$$

Examples of this include:

Capability Value (here probability of meeting a design margin) = Pr (emergency cooling flow either natural or forced > flow needed to prevent fuel or cladding damage |

possible pipe breaks sizes).

Capability Value (here probability of reactor vessel failure) = Pr (Vessel plates and welds fracture toughness > thermally induced stress intensity | possible transients involving high rate of cooling along the vessel wall and high vessel pressure).

Capability Value (here probability of support structure failure) = Pr (yielding point > applied stress | possible seismic loads).

While performance of certain components, systems, and structures can be expressed by their capability values alone, for most active components and systems that undergo maintenance and experience degradation (such as pumps and motor operated valves), availability becomes the prime measure of performance. If we had the exact physics of failure models to estimate the probability of failure of components, systems and structures, then one could just rely on Stress-Strength, Degradation (or Damage)-Endurance and Performance-Requirement models to calculate the probability of failures[9]. However, these models are limited and not available for all components, systems and structures. Therefore, traditionally, historical data on time of failure and time of repair have been used to estimate "availability" or its complement "unavailability" as the measure of performance.

Availability is generally the most appropriate performance measure for repairable items (i.e., active, maintainable systems and components) because it takes into account both failure (measured by reliability) and tests and maintenance downtime data (measured by surveillance, preventive and corrective maintenance). As a quantitative measure, availability is defined as the probability that an item can operate at a specified time, given that it is used under stated conditions in an ideal support environment. If a system operates when in a good condition, availability can be defined as the probability that the safety barrier is in operation at a specified time.

$$\text{Availability} = \Pr(\text{component or system is in good operating condition at time } t \mid \text{component or system capable}) \quad (2)$$

Availability formally is defined as:

Note that availability is the only measure that past PRAs have considered. They assumed perfect capability of all plant components, systems, and structures. In the context of a goals-driven performance-based regulation, however, both capability and availability should be measured and used. Figure 2 illustrates the main elements of performance for items considered in a goals-driven performance-based analysis. In the context of plant operations, the owner/designer often adds another core element to the performance, namely *efficiency*. This element is concerned with the economics and the ease with which the safety barrier and systems are operated and maintained. However, this later element is not a prime concern of the regulator.

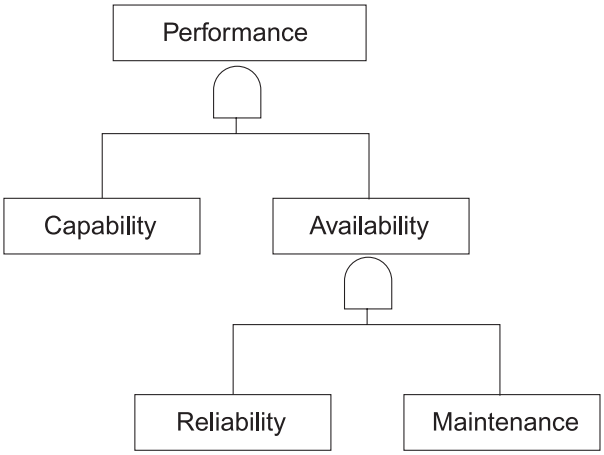

Fig. 2. Elements of Safety Performance

In the safety goals-driven performance-based approach, a goal must be traceable and measurable with unambiguous acceptance criteria. Lessons learned from system complexity theories and modeling is valuable in setting meaningful level of goal-decomposition and setting appropriate performance criteria. Safety goals-driven performance-based regulation is largely a "rationalist" approach in which the purpose of defense-in-depth is to manage uncertainties due to unknown processes, phenomenal, and events and increases the degree of confidence in achievement of safety goals and other conclusions regarding adequate safety. As the ACRS asserts,". . . what distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits."

The proposed goals-driven performance-based regulation uses:

1. safety goals, surrogate objectives, radiation protection, and perhaps additional quantifiable security objectives as measures of acceptable limits and uncertainty;
2. quantitative "scenario, frequency, consequence" approach (primarily the PRA approach) to estimate whether a safety system or technology agrees with these performance goals and objectives and the degree of such agreement;
3. best estimate approach to estimate performance of safety barriers that support or realize safety functions

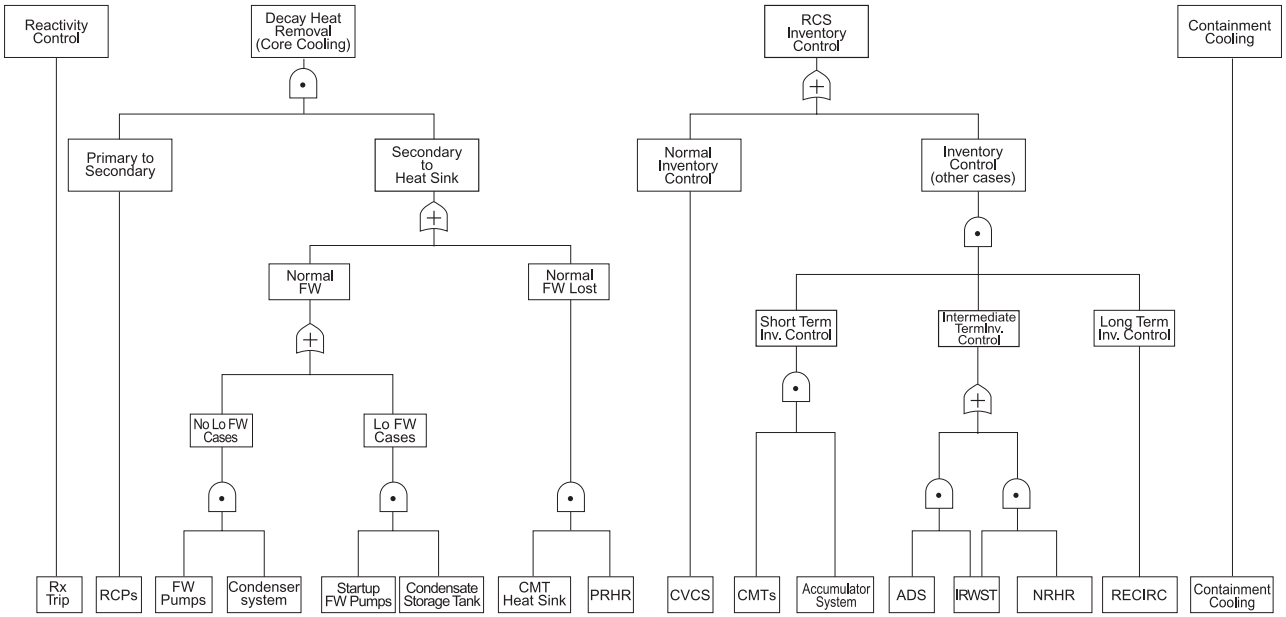

Fig. 3. Decomposition of AP-600 Reactor Safety to Safety Functions and Systems

and ultimately the high-level safety goals, including characterization of epistemic and aleatory uncertainties;

4. traditional conservative approach (defense-in-depth concept and single failure criteria) as a structuralist adjunct for cases where there are substantial lack of knowledge (uncertainties);
5. continuous monitoring of safety and security-critical elements and periodic reassessment of risk and security and its trend to maintain agreement with safety and security goals and objective.

To illustrate the points raised above, consider decomposition of a safety goal such as the risk limits for an individual in the vicinity of a nuclear power plant due to fatalities resulting from reactor accidents, that should not exceed 0.1% of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed; the associated limit on the overall mean frequency of a large release of radioactive materials to the environment which is 1 in 1,000,000 per reactor-year; and the frequency of a core damage frequency limit of 1 in 10,000 per reactor-year. These are high-level goals that can be used to apportion and set performance requirements consistent with these goals at the lower level sub-goals, safety functions, and safety barriers (safety systems, physical barriers, human actions, etc.). Figure 3, shows decomposition of functions critical to safety (functions critical to core damage prevention and containment integrity) in the AP-600 reactor design. Consistent with the high level goals (say set by the regulator such as the current safety goals) some limits or performance level of the sub-goals, functions and systems (safety barriers) described in this figure can be assigned.

The performance limits of goals, functions, structures, systems (safety barriers) can be categorized into frequency (or probability) limits and physical requirements (minimum flow or maximum cladding oxidation). Frequency limits are usually applied to occurrence of events and conditions (e.g., frequency or probability of a pipe break), while physical limits are applied to measurable physical properties (e.g., strength or endurance of a pipe in a corrosive environment).

Demonstration of the attainment of the goals, sub-goals, safety functions and safety barriers over the life of the plant would be the responsibility of the licensee. Such a demonstration may rely on the traditional PRA techniques, deterministic analyses, and actual demonstration tests to verify safety goals, frequency levels, physical requirements, and other performance limits.

For example, consider Figure 4. In order to demonstrate the integrity of a safety barrier (a system or structure), the licensee may estimate the spectrum of loads imposed on the barrier (and uncertainties associated with such estimates), as well as the capacity (e.g., strength and endurance) of the barrier at the given time of interest. The convolution integral of the two probability distribution functions gives the probability of failure (as in equation 1) due to the overlap area. If the probability exceeds the limit set for this barrier (e.g., the apportioned or preset probability or confidence limits), then the goal is not

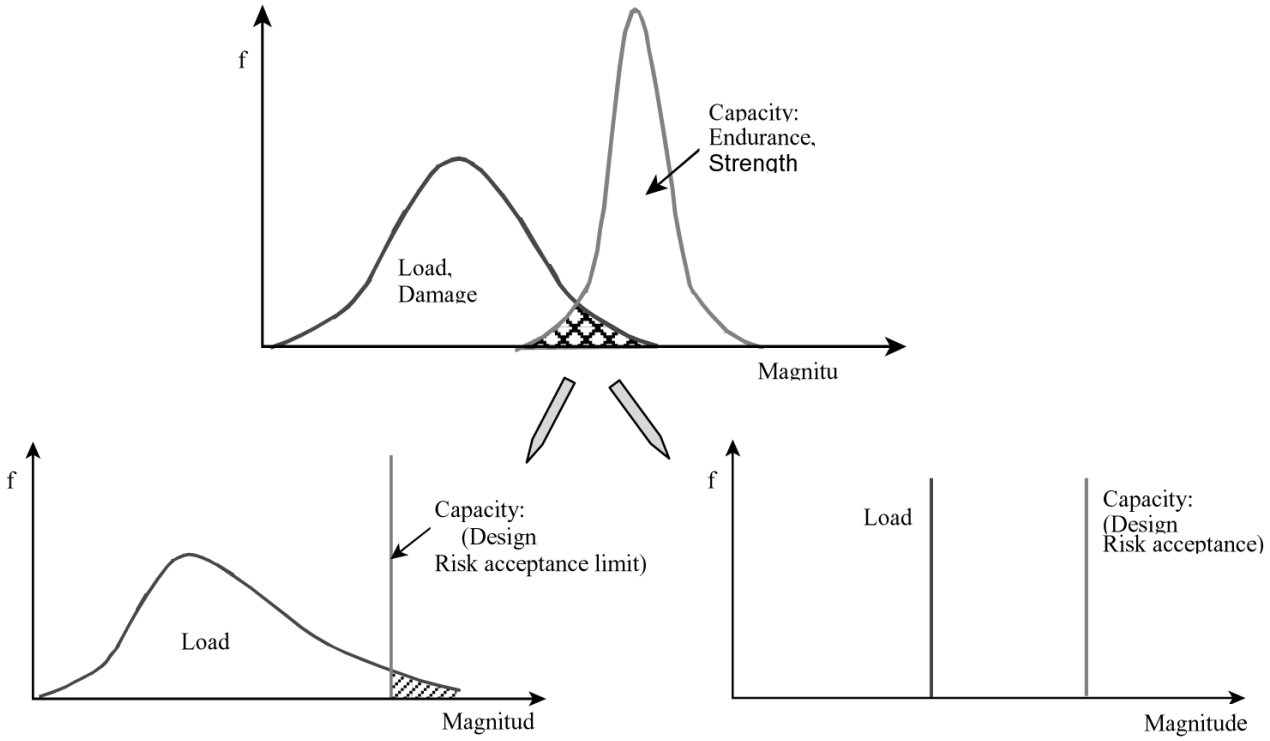

Fig. 4. Representations of Performance Criteria

attained. It is also possible that the challenge and capacity can be measured, estimated, demonstrated, or calculated with no uncertainty in which case the acceptance of the goal would be more objective. In fact, in the traditional conservative calculations, instead of a best estimate calculation, conservative limits (often unrealistic values) were set for both the capacity and challenge to avoid measuring the uncertainties. Many years of experience in characterizing and estimating uncertainties allow us to model and quantify uncertainties and perform best-estimate calculations. For example recent efforts by the University of Maryland to quantify uncertainties associated with safety systems capabilities and phenomena in large scale thermal-hydraulic calculations using standard systems code (e.g., RELAP5 and TRACE) and uncertainty analysis of the recent Pressurized Thermal Shock studies have been extremely successful.

The safety goal directed performance-based approach to nuclear power plant regulation should, as a minimum, monitor the performance of the plant in all phases of operation during the entire life of the plant from the perspective of the immediate sub-goals, functions and safety barriers associated with:

1. Core Integrity (Goal: No radiation will be released from the core; No more than a fixed number of events per year identified as a significant precursor of a nuclear accident; No statistically significant adverse trends in performance of specific components, systems or structures)
2. Containment or Confinement Integrity (Goal: No radiation will be release to the environment)
3. Plant Security (Goal: No intentional harm can be inflicted; No breakdown of physical security that significantly weakens the protection against radiological sabotage or theft or diversion of special nuclear materials in accordance with abnormal occurrence criteria)
4. Radiation Protection (Goal: Radiation exposure standards are met, No radiation overexposures from nuclear reactors accidents that exceed applicable regulatory limits; No more than a fixed number of radiation releases per year to the environment that exceed the regulatory limits)
5. Organizational Safety (Goal: Programs, processes and safety culture that support all safety needs)
6. Emergency Preparedness (Goal: Plans, drills assure adequate response to emergency situations)

Understanding common properties of complex systems would be helpful in setting meaningful goals.

For example a complex system shares the following common characteristics including any nuclear plant technology:

1. *Evolving* : Evolution leads to hierarchy (both functional and structural) and thus any stable system is necessarily hierarchical. They also retain memories of the past. This means that the upper safety goals are very generic and can be broken down to sub-goals. Setting such requirements at high level goals guarantees that system specific features do not enter the regulatory requirements, as these appear at the lowest level of the hierarchy. This feature of complex systems obviates the natural use of PRA techniques that efficiently model complex system hierarchy.
2. *Integrated* : All systems are coupled tightly and diversely and at times are uncertain. This means that the goals, functions and structures may be related and the performance limits must be selected such that they measure adequacy of diverse elements, and such that the non attainment of such goals does not quickly (due to system tightness) lead to loss of major goals (e.g., core or containment integrity). Further, uncertain events and relationships are the inherent property of any complex system and should be characterized, and when possible measured.
3. *Large* : System elements participate in diverse processes and geographically wide structures and utilized over long time. This means that goals may be set on processes that are widespread and should be observed over long periods of time. For example the management organization may be physically distributed. Goals for processes such as communications, learning, and knowledge management are, therefore, important to safety.
4. *Intelligent* : Plants may have capabilities of self-organization (random and intended perturbations could lead to known patterns in space and time) and have learning abilities (complex intelligent systems learn new ways to achieve their goals in the face of obstructions). Again appropriate goals for the degree of learning and ability to self organizes are also issues to consider in setting goals and performance requirements.

Like any other change, a sweeping change in a regulatory system such as the one discussed in this paper faces strong opposition from within, and it is natural that accepting this proposal to make a drastic paradigm shift from a predominately structuralist approach to nuclear plant regulation to a predominately rationalist approach would encounter resistance, as it is contrary to the well-established culture and norms. However, considering realities of complex systems and our abilities to model and characterize their underlying processes and phenomena, limited resources available, and abilities to innovate, the only practical and efficient approach to regulation appears to be a predominately rationalist approach.

6. CONCLUSIONS

This paper summarizes the implications of a safety goals-driven performance-based approach to regulation. This approach is similar to the maintenance rule in that it advocates setting goals on a set of high-level safety goals concerning common safety functions and safety barriers (systems and structures) that assured: Core Integrity; Containment or Confinement Integrity; Plant Security; Occupational and Routine Radiation Exposure; Organizational Safety Commitment and Integrity; Emergency Preparedness; Other Radiological Source Protection. In turn it is proposed to decompose each of these safety functions to more detailed generic functions and safety barriers and requiring that the licensee proposes convincing limits that assure attainment of such goals. The role of the regulators would be to manage uncertainties. For example to assure that such goals are attained (with high confidence or probability) at all times through the use of performance monitoring. Performance of each item in the plant is composed of its capability and availability, both of which will be quantified using probability. Further, the regulator should require that the licensee institutes a well-defined knowledge management program to reduce uncertainties that arise from lack of knowledge driven by lost or unknown, but existing information. This approach provides a reasonable balance among accident prevention, radiation exposure prevention, and consequence mitigation in assuring safety.

A review of the history of the safety regulation in the nuclear power industry reveals that many of the required features such as the defense-in-depth continue to appear as the means to control uncertainties about performance of the systems and structures, but should not be a required feature of a plant design. Rather it should be a means for protecting against unknowns. Further, this paper examined the emergence of the use of probabilistic approach and risk information in regulation and shows that such methods are powerful tools for measuring attainment of goals and uncertainties associated with performance measures.

It is believed that a safety goals-driven performance-based regulation promotes creativity and shifts the safety burden more toward the plant owners. Further case studies for applications to specific advanced reactor designs would be necessary to demonstrate the feasibility of this regulatory approach.

Acknowledgement

This paper is prepared as part of the cooperative research agreement NRC0498056 between the University of Maryland, Center for Technology Risk Studies and the U.S. Nuclear Regulatory Commission.

REFERENCES

[1] SECY-02-0139, “Plan for Resolving Policy Issues Related

to Licensing Non-Light Water Reactor Designs July 22, 02"
[2] Sorensen J., Apostolakis, G., Kress T., and Powers D. On The Role of Defense In Depth in Risk-Informed Regulation, Proceedings of PSA'99, Washington, DC, August 22-26, 1999.
[3] Rhodes R, the Making of the Atomic Bomb, New York, Simon & Schuster, 1986.
[4] U.S. Nuclear Regulatory Commission, WASH-1400: Reactor Safety Study (NUREG-75/014), Oct. 1975.
[5] U.S. Nuclear Regulatory Commission, Safety Goal Policy Statement, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," USNRC, *Federal Register*, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986.
[6] Pavey, D., et al., Cost Effective Modernisation of Systems Important to Safety, Post FISA-2003 Workshop Report, 2003.
[7] Lord Robens, Safety and Health at Work. Report of the Committee 1970 - 72. HMSO Cmnd 5034, 1972.
[8] Lord Cullen, The public inquiry into the piper alpha disaster, HMSO Cm 1310, 1990.
[9] Modarres, M. Krivtsov, V, Kaminskiy, K., Reliability Engineering and Risk Analysis: A Practical Guide, Marcel Dekker, 1999