FINAL SCIENTIFIC/TECHNICAL REPORT
FOR THE PERIOD March 30, 2005- December 31, 2008
Due Date: March 31, 2009
For
Award Number: DE-FC07-05ID14666

DEVELOPMENT OF RISK-BASED AND TECHNOLOGY-INDEPENDENT SAFETY CRITERIA FOR GENERATION IV SYSTEMS

William E. Kastenberg, Project Director
Department of Nuclear Engineering
University of California
Berkeley, California 94720-1730

Contributors

Edward Blandford
William Kastenberg
Lance Kim

TABLE OF CONTENTS:

CHAPTER 1. DEVELOPMENT OF RISK-BASED AND TECHNOLOGY-INDEPENDENT SAFETY CRITERIA FOR GENERATION IV SYSTEMS

CHAPTER 2. INCORPORATING UNCERTAINTY QUANTIFICATION INTO RISK ASSESSMENT FOR ADVANCED NUCLEAR ENERGY SYSTEMS

CHAPTER 3. A FRAMEWORK FOR ASSESSING AND MANAGING THE RISKS OF ADVANCED NUCLEAR ENERGY SYSTEMS

CHAPTER 4. IMPLEMENTING A ROBUST PROSPECTIVE APPROACH TO RISK ASSESSMENT FOR ADVANCED NUCLEAR ENERGY SYSTEMS

CHAPTER 1. DEVELOPMENT OF RISK-BASED AND TECHNOLOGY-INDEPENDENT SAFETY CRITERIA FOR GENERATION IV SYSTEMS

I. INTRODUCTION

Underlying the Generation IV approach to nuclear energy is an emphasis on the entire fuel cycle. This 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).[1] 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. The main objective of this project is to develop a set of quantitative safety goals representing these "top-level" qualitative goals and a method for their allocation to the various system elements including a framework for quantifying the risk and the associated uncertainty. These quantitative safety goals can then be utilized in both design and in regulation.

We begin our technical approach by considering a generic fuel cycle as a network. The nodes of the network might be enrichment facilities, nuclear reactors, fuel storage facilities, reprocessing facilities, etc. These nodes are related to each other by material, energy and information flows. We envision three types of risk to begin with: 1) the loss of bulk material from the network (e.g. fissile fuel such as plutonium) resulting in proliferation or public welfare risk, 2) the loss of particulate and gaseous material (e.g. fission products and respirable plutonium particles) from the network due to accidents resulting in public health risk, and 3) the planned loss of material from the network (e.g. mill tailings, high-level radioactive waste) resulting in public health and ecological risk.

In this project we have considered a simple system composed of a reactor and some associated processing facilities (transmutation or separation) and storage facilities for both fresh and irradiated fissile fuels and materials. Our approach is conceptual, with little detail regarding the technical design or facility operations.

As will be discussed below, we assume that the U. S. Nuclear Regulatory Commission (NRC) policy on safety goals in terms of quantitative health objectives (QHO) will be applied to Generation IV reactors.[2] However, the subsidiary goals utilized by the NRC in Risk-Informed Regulation, in terms of Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) are specific to today's Light Water Reactors (LWR), and as such, may not be applicable to the various Generation IV candidate systems.[3] Hence the need for risk based criteria that are "technology-neutral" wherever possible, especially during any down-selection process.

II. DEFINITIONS AND PRELIMINARIES

In this section we consider the notion of risk with respect to a nuclear energy system, in order to provide a systematic and logical approach for both delineating design issues and developing risk-based and technology-neutral safety criteria associated with Generation IV energy systems. The intent is to provide some preliminary ideas as a guide to future research. No claim is made regarding completeness in terms of the issues addressed, or in the events considered, as this is a conceptual approach.

II.A. Definitions of Risk

For the purposes of this project, risk is generically defined as the expected value (or frequency) of an undesirable consequence; **i.e. risk is the product of frequency times consequence**. We also recognize the importance of uncertainty in any determination of risk, and that subject will be discussed later in this report. And because we will be dealing with highly uncertain events, **frequency should be interpreted as annual probability of occurrence** for this paper.

In this project we will be dealing with three broad classes of risk: **risk to public health and safety, risk to public welfare** and **risk to the environment (which we term ecological risk)**. These risks are define as follows:

- The risk to public health and safety is a consequence of the movement and release of particulate, gaseous or respirable quantities of radioactive materials from the system to the accessible environment due to accidents. Such movement and release also impacts the environment (ecological risk), and the health and safety of facility and co-located workers.

- The risk to public welfare is a consequence of unauthorized movement of bulk materials (primarily fissile fuel: uranium and plutonium) and unauthorized release of this fuel from the system to the environment, and is a threat to national and international security.

- The risk to the environment (ecological risk) includes accidental releases as well as purposeful releases from any (geological) waste repository to the environment over very long time periods.

These three risks are named separately because the measures used to quantify them will be very different. Moreover, we should also note that routine operations in a nuclear energy system could lead to risk. These risks include radiation exposure to facility workers who are performing activities such as maintenance, emplacement, inspection and surveillance. Considerations such as radiation protection, which are aimed at reducing occupational risks, can also impact the design and should be treated as well.

II.B Movement and Release of Materials.

In order to develop a risk-based approach, it is convenient to define (for the purposes of this report) 4 distinct areas of interest around each facility making up the nuclear energy system, separated by 3 boundaries. For conceptual purposes, consider them concentric circles.

Area 1. This contains one of the facilities such as a nuclear reactor, spent-fuel pool, fissile fuel storage vault, or a separations facility. Release of particulate and/or respirable material into this area can lead to facility worker health and safety risk. Similarly, loss of material verification and surveillance in this area leads to a loss of material accountability, which degrades public welfare.

Boundary 1. This defines the boundary between Area 1 and the remaining facilities and operational areas of the energy system. This boundary may consist of the containment/confinement, the heating, ventilating, and air conditioning (HVAC) system and filters, and the physical security and safeguards systems, all designed for the activities carried out in Area 1.

Area 2. This area is composed of the remainder of the energy system proper. Release of particulate/respirable material can impact facility worker health and safety risk. Release of bulk material into this area is a loss of material control, which also impacts and degrades public welfare.

Boundary 2. This defines the boundary between Area 2 and the remainder of the property upon which other non-nuclear facilities (e.g. the switchyard) are built. This boundary may also have physical walls (or fences), and security and safeguards systems.

Area 3. This area is the remainder of the site property wherein the operator has control either for exclusion or evacuation. Release of particulate/respirable material into this area contributes to co-located worker health and safety risk, and has the potential for environmental degradation. And movement of unauthorized bulk material into this area is also a loss of material control, which further degrades public welfare.

Boundary 3. This separates the nuclear energy system and its environs from the public and the environment. It may also consist of fences, and safeguards and security systems.

Area 4. This is the outside environment. Release of particulate/respirable material into this area contributes to public health and safety risk, and ecological risk. Release of bulk material to this area contributes to public welfare risk.

In this approach, we take the viewpoint that the movement of any material across these three boundaries contributes to risk; and it is in these four areas that the consequences of that movement take place.

It should also be noted that in a strict defense in depth sense, the form of the fissile material (i.e. metal, oxide, etc.) and its state (fresh or irradiated), provide the first area and boundary and contribute to proliferation protection   In this project we focus on the design of the system rather than on the design of the fissile fuel. It is recognized that the design of one certainly impacts the other and should be treated in actuality.

II.C. Measures of Risk

Having defined risk in terms of the movement and release of fissile fuel, and having defined the boundaries and areas associated with the consequences of this movement and release, we can now define the measures of risk. These definitions are not intended to be all-inclusive and may not be precise, but they meet the purposes of the approach presented in this report.

In this approach, we can utilize the standard measures for **public health and safety risk**, and broaden them to include facility and co-located worker health and safety. These standard measures stem from the potential exposure to particulate, gaseous and respirable quantities of fission products and actinides, and include acute and latent fatalities per year, radiation dose (in terms of person-rem) per year, or any other measure of health consequence times frequency (annual probability).

The definition of a measure for **public welfare risk** is more difficult to define because the consequences of unauthorized movement and release of bulk fissile fuel from any facility to the general environment is very difficult to quantify. The consequences associated with loss of accountability and loss of material control are also difficult to quantify, and at a minimum will result in a loss of public confidence. In this case, we define the risk as the frequency (or annual probability) of the event itself. This approach is very much like defining the frequency of core melt (CDF), or the frequency of a large early release (LERF) of fission products from containment, as the risk of interest for nuclear power plants. In this case the consequence is unity; i.e. it is the event itself.

For public welfare risk we define three measures. The risks are measured by the frequency (i.e. annual probability) of:

a) Loss of material accountability: this includes the loss of surveillance, verification and/or monitoring.

b) Loss of material control: this includes the unauthorized movement of bulk fissile material or fuel from a vault, spent fuel pool or from a storage facility to the facility proper.

c) Loss of material: this includes the unauthorized movement or release of bulk fissile fuel to the general environment.

The definition of **ecological risk** is also difficult to derive and is a subject all its own. For the purposes of this project, we will use, as a surrogate, the risks calculated for a geologic repository in terms of dose, such as calculated for the Yucca Mountain Project.

II.D Risk Based Approach to Safety Goals

As an aid in developing a risk-based approach for developing quantitative safety goals, we begin by examining the nature of the initiating events and subsequent failures that can lead to the risks defined above. The general event classes and examples of each (this list is meant to be illustrative and not necessarily complete) are summarized here.

Initiating events include:

1. Random Failures/Internal Initiating Events: These include systems, structures and component (SSC) faults, loss-of-offsite power, etc. Internally generated fires have traditionally been included as an "external" event, but for the purposes of this project, are lumped with random events/internal initiating events. Random failures can lead to both accidents and loss of material accountability.

2. Natural Phenomena/External Initiating Events: These include seismic events, floods, aircraft crashes (accidental), tornados, forest fires, etc. External events can lead to accidents, loss of material accountability, and loss of material control.

3. Human Errors: These may be errors of omission or commission, and are considered unintentional, but can lead to an accident, and/or loss of material accountability and/or material control.

4. Malicious Human Acts: These acts may be due to both insiders or outsiders (or a combination of both), and can lead to accidents, loss of material accountability and/or control, or loss of bulk material. These events are often referred to as acts of sabotage or terrorism.

From a risk and systems viewpoint, our objective is to design an energy system that minimizes the risks to public health and safety, the environment and to public welfare. And by public health and safety, we are including the risk to facility and co-located workers as well. Hence the nuclear energy system should contain features and measures to cope with the four categories of initiating events and any potential subsequent failures.

Subsequent failures include failure of prevention, mitigating and interdiction systems such as the confinement/containment system and any other Engineered Safety Features (ESF) and SSC's. A possible hierarchy of design features and measures is considered, which are intended to reduce the following risks:

1. Features or measures to minimize or eliminate the annual probability of accidents such as core damage, criticality of stored and transported fissile fuel, fires, explosions etc., which will reduce facility worker risk, co-located worker risk, and public health and safety risk. This is sometimes called accident prevention.

2. Features or measures to mitigate accidents should a release of particulate/respirable radioactive material occur, which will reduce co-located worker risk, and public health and safety risk. These features or measures may also be designed to prevent confinement/containment failure and to prevent the release of respirable/particulate material.

3. Features or measures for monitoring and for surveillance, which will eliminate or reduce the annual probability of loss of material accountability.

4. Features or measures to eliminate or reduce the annual probability of material control loss. Together, the features and measures in Categories 3 and 4 make up the "Safeguards" system.

5. Features or measures to eliminate or reduce the likelihood of material loss. These features and measures make up the "Security" system.

Given the initiating events and subsequent failures discussed above, one can then design the features and measures to eliminate or reduce the likelihood of material movement (both respirable/particulate and bulk) from the system facilities to the general environment. In this context, it would be necessary to define the event sequences more precisely as is usually done in a Probabilistic Risk Assessment (PRA). Since this could be a formidable task at present, only a few sequences will be considered in Section III, mainly to illustrate how this approach can be used.

III. DESIGN ISSUES, INITIATING EVENTS AND EVENT SEQUENCES

In this section we discuss some of the design issues in the context of initiating events and event sequences. Event sequences are to be interpreted generically (without respect to any particular design), as is movement of fissile fuel effecting public (and worker) health and safety, and public welfare.

III.A Random Failures/Internal Initiating Events

Random initiating events involve the random failure of structures, systems, and components (SSCs), the random occurrence of internally generated fires, loss of off-site power, internal explosions, as well as other random faults that may occur. Random initiating events may occur with a wide range of frequencies and can affect both public health and public welfare risks.

Public health risk is affected by random failures because these internally generated initiating events can lead to accidents and can also lead to a loss of material accountability.

III.B Natural Phenomena/External Initiating Events

Risk assessments performed for a variety of nuclear power plants indicate that natural phenomena and external initiating events are major contributors to risk. The conventional design approach had been to define design basis events. A design basis for floods, tornados and other natural phenomena are required and are usually specified in both deterministic and probabilistic terms.

Design basis events are also commonly defined for external events that are not related to natural phenomena particularly accidental airplane crashes. The design basis event is defined by consequence, specifying various types of aircraft, impinging the facility at various speeds, and at various angles. More recently, PRA has included external events in a probabilistic fashion, such as in an IPEEE.

III.C Human Errors

Unintentional human errors may occur in conjunction with operations at any nuclear facility. Unintentional human errors may act as an initiating event, or may contribute to the progression of an accident that has been initiated by a random failure or by natural phenomena.

III.D Malicious Human Acts

Safeguards and security (S&S) is the general term given to the protection from theft or diversion of Special Nuclear Material (SNM). As such, it considers insider threats, outsider threats and a combination of both.

In addition to personnel, computer/information and operations security, S&S design is concerned with physical protection systems (PPS) and material, control and accountability (MC&A) systems. In this project we focus on the PPS and MC&A systems, as examples of how S&S is integral to any nuclear energy system.

III.E Accident Sequences

Accidents involving core damage, criticality (of stored fissile material), fires and explosions appear to be the major mechanisms for creating respirable or particulate material. Such accidents may result from any of the initiating events described above.

Fire in any storage facility is potentially a hazardous accident that could take place in terms of the dispersion of particulate/respirable fuel. When heated to its ignition temperature, plutonium for example, reacts at an accelerated oxidation rate that sustains continued oxidation. Plutonium oxide is already in a form suitable for particle dispersion. Dispersibility increases with decreasing particle size. Fire protection usually requires the elimination of combustibles and sources of ignition, and the provision of fire detection capability. Fire protection design is usually based on a design basis fire.

III. F Loss of Containment/Confinement

Several Generation IV design documents speak of a "confinement" system. The design of a reactor without a conventional containment presents a new challenge in that the confinement SSCs may also be part of the physical protection system (PPS), designed as part of the S&S system described above. Thus a loss of confinement can also occur due to malicious acts, in the course of attempts at theft and diversion. Both public health risk and public welfare risk are affected by a loss of confinement.

III.G Loss of Material Accountability and Control

The function of the Safeguards System is to insure that no nuclear materials are inadvertently lost, no unauthorized removals occur, and nuclear materials are accounted for and adequately measured. The accountability portion of the Safeguards System requires a means of physically accounting for fissile fuel on a timely basis, while at the same time reducing employee radiation exposures. The principal radiological concern that occurs with stored Pu arises from the decay of Pu-241 to Am-241, which emits a high yield 60 kev gamma. Since most of the stored Pu is expected to have a relatively low percentage of Pu-241, only a modest amount of shielding may be required. Automated and remote surveillance techniques may be required in order to minimize radiological exposures.

The material control portion of the Safeguards System governs the movement of bulk materials within any storage or transfer facility.

III.H Loss of Material

Theft and sabotage may be prevented using the basic functions of a physical protection system (PPS) that is part of the Security System. Threat characteristics such as actor, motivation, aspirations and capabilities are all important considerations. The PPS has three functions: detection, delay, and response. These three functions are based on the design philosophy that "deterrence" is difficult to prove; the PPS assumes that the postulated act will occur.

The physical protection system will be an integral part of any storage facility. As such, it may share common features with the storage vaults and the facility proper. Its design goals may conflict with those of the confinement system, or they may be compatible, depending on the approach taken. In the next Section, a set of risk based design criteria are formulated, which takes into account the requirements of both.

IV. RISK BASED SAFETY CRITERIA

As noted in the Introduction, one objective of this project was to develop technology-neutral quantitative safety goals using a risk and systems approach. In this Section we employ the approach presented above to develop top-level design criteria called Quantitative Design Objectives (QDOs) based on Public Health Risk and Public Welfare Risk. These QDOs are then utilized to develop functional design criteria for the features and measures necessary to protect against the initiating events and event sequences described in Section III.

IV.A Quantitative Design Objectives (QDOs)

At the present time there is considerable interest in the development of quantitative methods for evaluating the safety of complicated engineered systems. In 1986, the NRC published a set of safety goals and design objectives for the operations at nuclear power plants following a two-year evaluation period.[2] The objective of these goals is to, “establish goals that broadly define an acceptable level of radiological risk.” The NRC established two qualitative safety goals that define the basic philosophy of the approach supported by two quantitative health effects objectives (QHO) for use in regulatory decision-making processes. The Department of Energy adopted these same goals (with only slight modification) for the evaluation of existing DOE nuclear facilities in general.[4] Hence, we assume these goals will still be operative for Generation IV systems.

Quantitative or probabilistic safety criteria to provide guidance to designers have been found to be a useful tool in the United Kingdom (U.K.), and more recently in the U.S., with the advent of Risk-Informed Regulation.[3] There is difficulty, however, in using a public health risk measure as a top-level design criterion because such a measure is an integral quantity involving a mathematical combination of probabilistic (frequencies) and deterministic (consequences) terms, which are not simply additive, are site specific, and add additional uncertainty to a PRA. Hence subordinate top-level criteria have been postulated such as limits to annual probability of core damage (CDF) and limits to annual probability of a large early release (LERF) that are LWR specific.

In those countries where there has been a significant effort on the part of a regulatory agency or a utility to define QDOs for nuclear power plants, there had been a consensus that the annual probability of a large atmospheric release of radioactivity, which we denote by P(lr), should not exceed 10^{-6} per reactor year. "Large release" has rarely been precisely defined, but is usually taken to be 1% or more of the gaseous and volatile isotopes in a reactor core. However, the NRC, in its use of Risk-Informed Regulation uses 10^{-5} as a limit for LERF as a surrogate for meeting the public health objective of one tenth of one percent (0.001) of acute fatalities form all other causes.

There is a subsidiary design objective, usually associated with this objective, to define the maximum acceptable annual probability of accidents causing severe damage of the reactor core, which we will denote by P(a). Values for P(a) range from 10^{-6} per reactor year as adopted by the U.K. utilities, which implies little reliance on containment, to a value of 10^{-4} in the U. S. as a surrogate for meeting the public health objective of one tenth of one percent (0.001) of the background cancer risk (latent fatalities). Today, there is a view in the U. S. that for advanced reactors, a more appropriate value for P(a) should be on the order of 10^{-5} in meeting the NRC's Policy Statement on Advanced Reactors.[5]

Because of the mathematical and conceptual difficulties in using a public health measure as a QDO, and because we wish to illustrate the risk based approach described in Sections II and III above, we begin with values for P(a) and P(lr) that might be appropriate for Generation IV nuclear energy systems. In order to develop a set of QDOs, we will use a set of plausible probabilities based on experience with other nuclear systems. Two sets of QDO are necessary for the issues at hand: one set for protecting public health and one for protecting public welfare.

For the public health risk based criteria, we assume that two types of event need to be considered:

- Type 1: Severe accidents leading to releases of respirable, gaseous or particulate matter, to the general environment surrounding the system, and sufficient to cause off-site actions such as the interdiction of foodstuffs, or the temporary evacuation of the public.

- Type 2: Severe accidents, even if there is not a significant release of particulate or respirable radioactive material to the general environment. Such an accident would undermine public confidence, both nationally and internationally, in the ability to operate nuclear power plants over long time periods. This would also constitute a very large economic risk.

If we further assume that a Generation IV nuclear energy system should be of comparable public health risk to any other single nuclear facility, either nationally or internationally, such as a single nuclear power reactor, then the annual probability of a Type 1 accident, P(lr), should be limited to 10^{-6} per year. Hence the public in the vicinity of the system would be given the same level of assurance regarding a large release of respirable or particulate matter that they would have for other nuclear facilities worldwide.

With regard to the design target for Type 2 accidents, we can assume that these systems, satisfying the NRC Policy Statement on Advanced Reactors, will seek a goal for P(a) of 10^{-5} per year. Such a level of assurance would be more stringent than the level afforded current nuclear power reactors, from a public confidence viewpoint. However, given the public's concern for nuclear energy, such a level of assurance seems plausible.

For the public welfare risk based criteria, we have already described the three types of event that must be considered:

- Type 1: Loss of material accountability.
- Type 2: Loss of material control.
- Type 3: Loss of material.

In order to establish QDOs based on public welfare risk, we assume that loss of material accountability and control (mac) leads to a loss of public confidence. Over a 100-year period, with 100 GEN IV systems, a 0.1% chance (one chance in a 10000) can be assumed necessary to maintain public confidence, in preventing Type 1and Type 2 events. That is to say, the public might tolerate one event where there is a loss of material accountability and control, but not two events. This assumption translates into a P(mac) on the order of 10^{-4} per year.

Because of the potentially large consequences associated with a loss of material (lm), we suggest a value of P(lm) on the order of 10^{-7} per year as a point of departure for discussion. The limit on P(lm) is an order of magnitude more stringent than the limit assumed for P(lr), which is meant to represent greater significance attached to release of bulk fissile material such as Pu than for respirable or particulate material such as Pu.

The four QDOs can be summarized as follows:

- Limit on the annual probability of a large accident: $P(a)=10^{-5}$/year.
- Limit on the annual probability of a large release: $P(lr)=10^{-6}$/year.

- Limit on the annual probability of a loss of material accountability and control: P(mac)= 10^{-4}/year.
- Limit on the annual probability of a loss of material: P(lm)=10^{-7}/year.

In the next section, we will use these QDOs to develop functional design criteria. The four values for P(a), P(mac), P(lr) and P(lm) can be varied to illustrate the sensitivity of the design to changes in the design targets. In so doing, we can also take into account the major sources of uncertainty in the initiating events, and in the event sequences themselves.

IV.B Functional Design Criteria

The top-level criteria developed above can now be utilized to develop functional design criteria for the features and measures described in Sections II and III. These features and measures fall into 5 categories:

1. Features and measures to reduce or eliminate the annual probability of large accidents, denoted by P(a).
2. Features or measures to mitigate accidents should one occur; these measures effect the annual probability of a large release, P(lr).
3. Features and measures to reduce the annual probability of loss of material accountability, denoted by P(ma).
4. Features and measures to reduce or eliminate the annual probability of loss of material control, denoted by P(c).
5. Features and measures to reduce or eliminate the annual probability of loss of material, denoted by P(lm)

We can express the annual probability of a large accident as:

$$P(a)=P(a{:}he)+ P(a{:}rf)+ P(a{:}np)+ P(a{:}mha). \qquad (1)$$

In Equation 1, P(a:he), P(a:rf), P(a:np) and P(a:mha) are the annual probabilities of an accident initiated by human errors, random failures (internal events), natural phenomena (external events including accidental airplane crashes), and malicious human acts, respectively.

For the sake of illustration, we assume that any containment/confinement system contains all of the features and measures for mitigating accidents, such as sprays, fan coolers, HVAC and HEPA filter systems. Hence we can express the annual probability of a large release as:

$$\begin{aligned} P(lr)= {} & P(a{:}he)P(cf/he)+ P(a{:}rf)P(cf/rf)+ P(a{:}np)P(cf/np) \\ & + P(a{:}mha)P(cf/mha). \qquad (2) \end{aligned}$$

In Equation 2, P(cf/-) is the conditional probability of containment/confinement failure given an accident of the type "-" has occurred.

Equations (1) and (2) can be used to derive numerical values for the functional design criteria. In principle, we can find a large number of combinations that would meet the top-level criteria, and in the absence of a risk assessment or a design, we continue with plausibility arguments and experience with other nuclear facilities. In actuality, a cost/benefit approach could be used in the functional design criteria allocation. We consider two bounding cases as follows:

Case 1 assumes that the containment/confinement system is rather robust, with a conditional probability of failure, given a severe accident, on the order of 10^{-1}similar to today's designs. In this case, the functional design must limit severe accidents for each of the four types of initiating event, to be on the order of 10^{-6}. And since Generation IV systems will have very few active components, we apportion most of the goal to accidents stemming from natural phenomena and external events, and malicious acts, with P(a:np) and P(a:mha) on the order of $5X10^{-6}$.

Case 2 assumes a structurally weak confinement, designed to accommodate a severe accident initiated by a random failure or human error, with its HVAC and HEPA filter systems. In this case, an external event such as an earthquake or plane crash, which causes a severe accident, also fails the confinement. Hence the conditional probability of confinement failure, given natural phenomena or malicious human acts, is 1. Now the functional design must limit the probability of severe accidents for P(a:np) and P(a:mha) to be on the order of 10^{-7}.

The two cases described above can serve to illustrate the designer's options in terms of tradeoffs between features to prevent accidents and features to mitigate accidents, as well as the tradeoffs in protecting against different initiating events. We see that if the designer chooses the option of a structurally weak confinement, but able to accommodate an internally initiated event with its vent-filter system, the frequencies of events such as tornadoes, earthquakes, and plane crashes must be very low. Severe accidents initiated by such external events must then be kept below 10^{-6} /year (total). Given the large uncertainty in characterizing such external events, it is not unreasonable to require a 10^{-7}/year limit for each type of initiating event (i.e. plane crashes, earthquakes).

As an alternative, the designer can choose a very robust containment, and thus alleviate the design constraints on preventing accidents due to external events. Such a requirement might lead to a conventional containment building or an underground facility. In this case the design limits for preventing accidents are on the order of 10^{-5}/year, for both internal and external events.

A similar set of functional design criteria can be derived for the Safeguards and Security System. We can express the annual probability of a loss of material accountability and control as:

$$P(mac)= P(ma)+ P(c) \qquad (3)$$

where:

$$P(ma)= P(ma:he)+ P(ma:rf)+ P(ma:np)+ P(ma:mha) \qquad (4)$$

and:

$$P(c)= P(c:he)+ P(c:rf)+ P(c:np)+ P(c:mha). \qquad (5)$$

In Equations 4 and 5, P(ma:-) and P(c:-) are the annual probabilities of material accountability loss and material control loss, due to the occurrence of "-". Similarly, the annual probability of a loss of material is given by:

$$P(lm)= P(lm:mha)+ P(ma)P(lm/ma) + P(c)P(lm/c). \qquad (6)$$

In Equation 6, P(lm:mha) is the annual probability of a loss of material due to a malicious human act, and P(lm/ma) and P(lm/c) are the conditional probabilities of a loss of material given a loss of material accountability and a loss of material control, respectively.

We can show a possible allocation for the Safeguards and Security System. Considering first the Safeguards System, and as a first assumption, we apportion the goal of 10^{-4}/year, half each to loss of material accountability and to loss of material control. We further assume that the material accountability system may be more susceptible to electronic and mechanical failures, and the material control system to human errors and malicious human acts. These assumptions lead to the allocation among the initiating events, whereby failure of material accountability due to equipment failure is limited to $4X10^{-5}$/year from all causes, and failure of material control due to all human causes is limited to $4X10^{-5}$/year.

It is anticipated that the greatest threat to loss of material is a malicious human act. Hence we allocate a large portion of the QDO for the Security System to this initiating event. We further assume that the conditional probability of a loss of material, given a failure of the Safeguards System is quite small. Hence the limits to loss of Security, stemming from a loss of Safeguards is on the order of 10^{-8}/year.

V. CONCLUSIONS

In this Section, we have provided our preliminary thinking regarding the development of risk-based and technology independent safety criteria (called quantitative safety goals) for Generation IV nuclear energy systems. We considered three types of risk: 1) the loss of bulk material from the network (e.g. fissile fuel such as plutonium) resulting in proliferation or public welfare risk, 2) the loss of particulate and gaseous material from the network (e.g. fission products, respirable plutonium particles) resulting in public health risk, and 3) the planned loss of material from the network (e.g. mill tailings, high-level radioactive waste) resulting in public health and ecological risk.

For simplicity, we considered a simple system composed of a nuclear reactor; some associated processing facilities and storage facilities for both fresh and irradiated fissile fuel. Our approach is conceptual, with little detail regarding the technical design or facility operations. Top-level Quantitative Design Objectives were developed for accidental releases and for unauthorized loss of bulk materials. Subsequently, quantitative functional design criteria were developed for preventing and mitigating accidents, and for preventing the loss of material accountability, control and ultimately, loss of the material itself.

ACKNOWLEDGMENTS

The views expressed in this Chapter are due to the Project Director alone, and do not necessarily reflect the views of neither the granting agency nor any other institution.

We wish to acknowledge a very useful discussion with Dr. Mary Drouin of the U.S. Nuclear Regulatory Commission regarding the Commission's program to develop a technology-neutral regulatory structure for new plant licensing, just as this research was getting under way. The NRC's program status and future plans, as well as stakeholders comments are contained in the proceedings of a March 2005 workshop.[6] These considerations are not reflected in this paper.

REFERENCES

1. NUCLEAR ENERGY RESEARCH ADVISORY COMMITTEE, SUBCOMMITTEE ON GENERATION IV TECHNOLOGY PLANNING "A Technology Roadmap for Generation IV Nuclear Energy Systems," Technical Roadmap Report, submitted to the U.S. Department of Energy, September 23, 2002.
2. TITLE 10, U. S. CODE OF FEDERAL REGULATIONS, PART 50. "Safety Goals for the Operations of Nuclear Power Plants", Policy Statement, November 30, (1988).
3. U.S. NUCLEAR REGULATORY COMISSION, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis", Revision 1, November, (2002).
4. U.S. DEPARTMENT OF ENERGY, Secretary of Energy Notice, Nuclear Safety Policy, SEN-35-91, September 9, (1991).
5. U.S. NUCLEAR REGULATORY COMMISSION, Title 10, U. S. Code of Federal Regulations, Part 50. *Policy Statement on Advanced Reactors.* July 8,1986.
6. U.S. NUCLEAR REGULATORY COMMISSION, "Proceedings of a Public Workshop: Regulatory Structure for New Plant Licensing, Part 1: Technology Neutral Framework," March 14-16, 2005.

CHAPTER 2. INCORPORATING UNCERTAINTY QUANTIFICATION INTO RISK ASSESSMENT FOR ADVANCED NUCLEAR ENERGY SYSTEMS

I. INTRODUCTION

As discussed in the first chapter, risk is generically defined as the expected value of an undesirable consequence. For the purpose of this section, a more complete definition of risk is necessary. Kaplan and Garrick[1] define risk as a set of scenarios, s_i, each with a probability, p_i, and a consequence, x_i. Treating risk as a "set of triplets" provides a fundamental framework for uncertainty quantification (UQ) as conceptually methods for quantifying each member of the triplet are typically different and can be decoupled.

$$R = \{(s_i, p_i, x_i)\},\ x_i = 1, 2, \ldots, N$$

Risk curves, also known as Farmer curves, are typically used to illustrate the risk spectrum associated with a particular system where each scenario, or category of scenarios, is plotted as a function of frequency versus consequence.

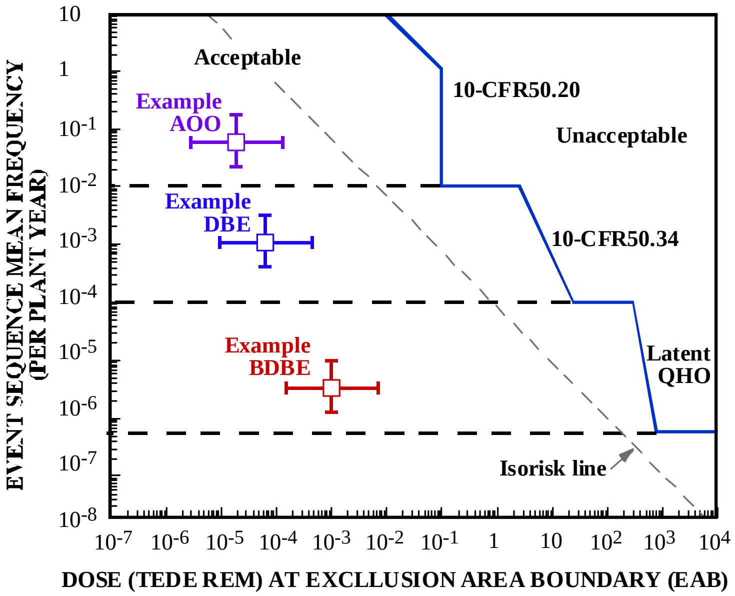


Figure 1 Example risk curve for **a Generation IV reactor design.**[2]

The three distinct risk classes defined in the previous chapter share many commonalities however there are significant differences with respect to methodology development and uncertainty quantification. In this chapter, we will discuss these differences in greater detail as well as offer potential remedial approaches. In each class, the risk measures drive the modeling objective and pose unique challenges when considered innovative nuclear technologies anywhere in the fuel cycle. However, at a fundamental level, the above definition of risk holds true for all risk classes and is very useful in understanding how the uncertainty quantification process varies.

I.A. Background

Before we go through the uncertainty quantification process in detail, we must first define what we actually mean by uncertainty. While the main focus of this work is intended to be practical, it is important to review the overarching philosophical context. Uncertainty is that which disappears when we, the observers, become certain.[3] For the practical engineer or scientist, certainty is achieved through observation, and uncertainty is that which removed by observation. Hence in these contexts uncertainty is concerned with the results of *possible observations*[3]. Immediately one can see that our definition of uncertainty hinges strongly on our ability to observe. In the case of complicated systems, observations are typically a combination of experiments and operational experience. However in the case of complex systems where the sum of the parts doesn't necessarily equate the whole, the level of observation can be quite impressively ambiguous and requires much further discussion which can be found in the following chapters. Ultimately, the level of certainty necessary for uncertainty quantification is a function of social acceptance and is the focus of risk management.

I.A.1 Types of Uncertainties

The polysemus nature of uncertainty leads to several traditional classifications which will be frequently discussed throughout this report. At the most fundamental level, uncertainty that can be reduced by observation is call *epistemic* and uncertainty that arises due to the inherent randomness, or stochastic, nature of the system is called *aleatory*. As pointed out by Winkler[4], both uncertainties are classified by probabilities and distinguishing between the two types can be somewhat arbitrary. For example, the roll of dice at a craps table is classically thought of as a random process where the outcome can be viewed as an aleatory uncertainty. For the reductionist, however, the initial positioning of the dice, motion of the throw, and other physical conditions can in theory be accounted for and used to help quantify the uncertainty. In this case, clearly the uncertainty must be considered epistemic. Ultimately this distinction is made for the purpose of the model being used to assess the risk and is at the discretion of the modeler.

In order to quantify the risk we must develop a mathematical model that best represents the physical situation of interest. This mathematical model, also known as "model of the world", can either be probabilistic or deterministic[5]. If we return to our definition of risk as a set of triplets, the probability of a particular scenario occurring is determined, of course, by using probabilistic models whereas the consequence of that particular scenario is determined using deterministic methods. Uncertainties in the mathematical model can be broadly categorized as *parameter* and *model* uncertainty. Parameter uncertainty is concerned with data inputted into the model whereas model uncertainty is concerned with the overall "truthiness" of the model. As will be shown in the next section, the role of uncertainty quantification can be quite different for the types of mathematical models. A third category of uncertainty is sometimes used to assess the overall completeness of the model and is known as *completeness* uncertainty and is associated with factors not accounted for in the risk analysis by choice or limitations in knowledge (NRC, 2006). Unknown or unanticipated failure mechanisms can contribute to completeness uncertainty for example. The distinction between model and completeness uncertainty can be blurry and for the purpose of this section we will not distinguish between the two.

An overview of the model development and subsequent uncertainty quantification process is illustrated in Figure 2. At the highest level, our physical understanding of what we observe comes directly from our selected metaphysical understanding of the world.

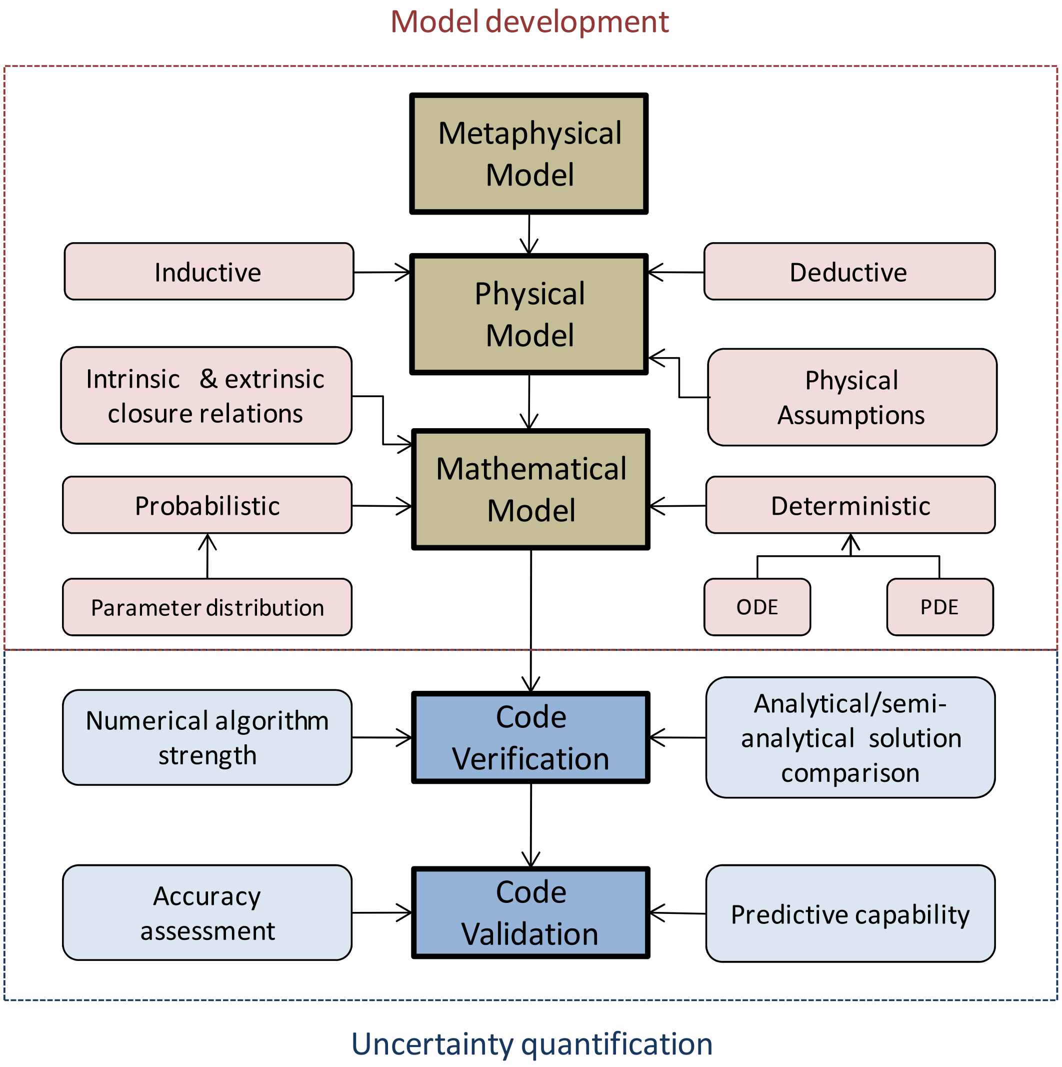


Figure 2 Schematic of the Model Development and Uncertainty Quantification Process

As discussed in the next section, this physical model can be developed using either an inductive or deductive approach but ideally both. Additionally, the physical model is based on a set of physical assumptions where one may have a wide range of previous understanding through observation. The mathematical model is a mathematical representation of the physical model and can be either deterministic (typically in the form of ordinary or partial differential equations for complex systems) or probabilistic. Intrinsic and extrinsic closure relations (i.e. properties of the components and correlations describing the fundamental transport processes such as mass, momentum, and energy in complicated systems respectively) are incorporated into the mathematical model. Code verification focuses on the mathematical basis of the code and ensures the mathematical model has been represented correctly via the appropriate algorithm(s). Once the code has been verified, the overall accuracy of the code must be compared with observation. More on the role of accuracy assessment and comparison with level of observation can be found in the final chapter.

II. HIERARCHIAL STRUCTURE OF COMPLEX SYSTEMS

Much has been written about the role of hierarchical theory in complex systems of great variety[6,7]. As we consider the entire fuel cycle network, implementing a hierarchical approach makes the problem considerably more tractable. In the thermal-hydraulic community, the Hierarchical Two-Tiered Scaling (H2TS) approach was developed by Zuber[8] in order to design scaled facilities that were physically similar to the prototype. In this particular case, the complex system under consideration was limited to the reactor but provides an excellent analogue for consideration of the entire fuel cycle.

The two-tiers in the H2TS approach refer to the top-down (holistic) and bottom-up (reductionistic) scaling approaches used to identify dominant phenomena during a reactor accident. The top-down approach is inductive by nature starting with the system as a whole whereas the bottom-up approach is deductive by nature and starts with the individual components making up the system. The functions and key characteristics of the two approaches are illustrated in Figure 3.

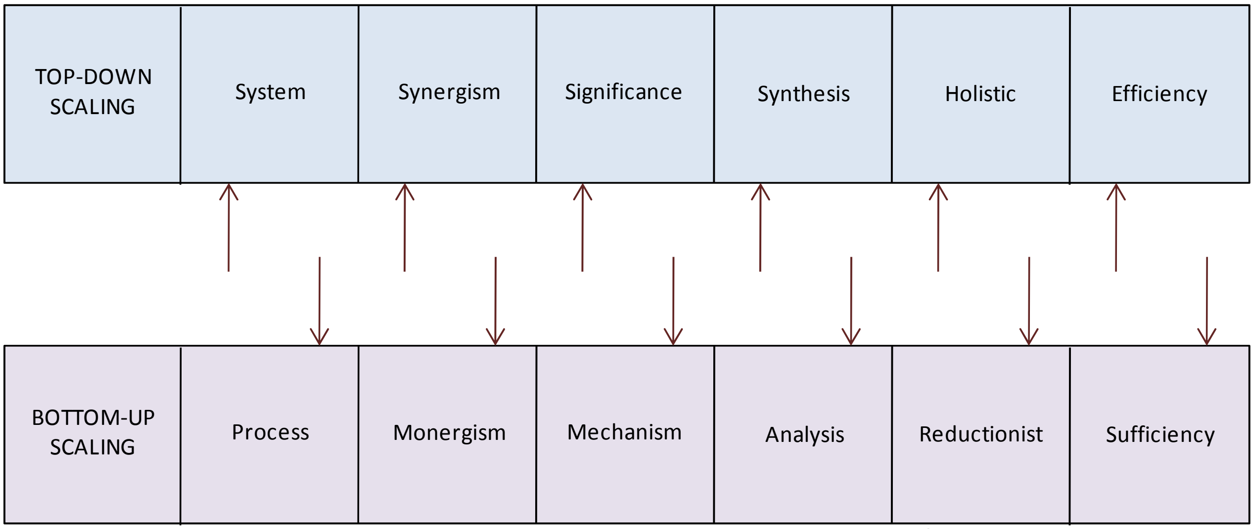


Figure 3 Contents and characteristics of two-tiered scaling[8]

Much like response of the individual reactor system is in fact a series of dynamic interactions between components (i.e. SSC's), the behavior of the entire fuel cycle depends on the interactions of its subsequent components. The holistic, or discovery approach is data-driven where the end goal is inductive inference[8]. The reductionist approach examines the problem at the local level and focuses on isolated interactions. Much like with finite control volume methods, the holistic approach is based on integral methods where the control volume encompasses the entire system. In the case of the reductionist approach, the appropriate analogy is infinitesimal element approach which is solved using differential methods. Since the top-down approach identifies key phenomena (i.e. processes) and affected components, it should be performed prior to the bottom-up approach so as to inform the bottom-up analysis.[8] For the purpose of the work, where this approach is still being developed, it is acceptable to decouple this aspect of the problem and perform each analysis independently.

III. BOTTOM-UP APPROACH TO UNCERTAINTY QUANTIFICATION OF COMPLEX SYSTEMS

Let us now return to the risk curve (Figure 1) in the first section where determining the magnitude of uncertainty bands associated with each scenario (i.e. uncertainty quantification) is the focus of this chapter. Each element of the triplet is determined in a unique fashion and is explored independently. The goal is to not rehash well-established methods in probabilistic risk analysis but rather identify areas of concern in uncertainty quantification for innovative advanced nuclear concepts within the fuel cycle network which is within a series of even larger-scale systems (i.e. geopolitical etc…). As discussed tangentially in the first chapter, uncertainty quantification has significant implications with respect to safety, security, and economics where synergisms often exist. Since we are focusing on the bottom-up approach for this chapter, the monoenergistic effects of the parts of the system are in fact the focus. Therefore, it is acceptable to examine each component of the fuel cycle individually however any emergent properties will be missed. In each of the following sections, we will examine example nodes of the fuel cycle network and see how this process varies.

II.A Scenario Identification

The astute observer notices very quickly that in order to assess the total risk a complex system poses, a complete set of scenarios must first be identified. While several techniques, such as Failure Modes Effects and Analysis (FMEA) and HAZOP exist for identifying unexpected operational modes, these methods were developed primarily for assessing safety risk. Since a risk analysis is limited to a list of scenarios that must be identified by the analyst, how does one cope with the fact that the actual list of scenarios, s_i, is in fact infinite and there exists a fair amount of incompleteness? Kaplan and Garrick[1] attempted to answer this question by introducing an additional scenario, s_{N+1}, to the analyst's list of scenarios and called it 'other'. By definition, this additional category contains all the scenarios that have not been analyzed and we can rewrite the definition of risk as,

$$R = \{(s_i, p_i, x_i)\},\ x_i = 1, 2, ..., N+1$$

Therefore, the list of scenarios is now logically complete however as noted by the author, it appears as if we have just performed a logical trick and not dealt with the fundamental concern.[1] In fact, what was done is allowed the analyst to assign a probability to this additional scenario and proceed in a logical fashion in trying to quantify this value as well as the associated consequence, x_{N+1}.

Since the focus of this work is on advanced reactor technologies and ultimately the entire fuel cycle network, how does one proceed in determining what this probability and consequence are? First, it is important to remember that even though there is a large operational basis for which current PRAs are based, unexpected failure modes such as the core damage at TMI and degradation of the Davis-Besse RPV were not captured effectively (or at all) by probabilistic methods. This concern is why ultimately the NRC relies on a Defense-in-Depth (DiD) approach to safety. Defense-in-depth is applied in safety design to account for the uncertainty in whether all possible scenarios have been identified, and whether the probability and consequences (p_{N+1}, x_{N+1}) have been accurately assessed, given the problem of incomplete knowledge. A "rationalist" approach to DiD (as opposed to a "structuralist" approach) uses PRA methods solely to quantify and reduce system uncertainties as opposed to relying on potentially overly conservative safety margins[9]. In practice, a hybrid rationalist/structuralist risk-informed approach is warranted.

II.A.1Scenario Identification Uncertainty Affecting the Various Risk Cases

When identifying potential scenarios that could lead to consequences affecting public health and safety risk, the methods used for the current fleet of operating reactors serves as an excellent foundation. Unfortunately with limited operational experience, the determination of these scenarios for innovative reactor designs as well as other elements of the fuel cycle network can be very difficult to determine. This problem also creeps up when dealing with the frequency space as will be discussed in the next section.

For each component of the complex system, the most effect way of minimizing the risk (all classes) posed by the previously defined set of scenarios, s_{N+1}, is to introduce a robust strategy for implementing DiD. The approach proposed is based on a framework originally developed by the IAEA[10] and expanded further by the Gen IV Risk and Safety Working Group[11]. The IAEA strategy divides the DiD approach into five levels by which different objectives are established. While this approach was developed for the next generation of nuclear plants, it applies equally to other nodes of the fuel cycle network.

Table 1 Levels of Defense in Depth[10]

Level of Defense	Objective	Essential Means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of beyond design basis events	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Level 1, Prevention of abnormal operation and failures, relates to plant reliability, and thus is of importance to both safety and economics. Ensuring high reliability is congruent with minimizing safety risk and is strongly dependent upon the quality of the programs for predictive maintenance, corrective actions, and human performance.[12]

Level 2 and Level 3 DiD are met through the systematic identification of a set of initiating events and design of safety systems to mitigate the consequences of these events with high reliability.[12]

Level 4, Control of severe plant conditions, and Level 5, Mitigation of radiological consequences, relate to the potential that an unanticipated initiating event, or an unanticipated progression of an initiating event, might occur that could cause degradation of the facility beyond the levels predicted by probabilistic methods.[12]

II.B Frequency Space

The second member of the triplet defining risk is the probability, or likelihood, of the scenario occurring. As noted earlier, frequency should be interpreted as annual probability of occurrence for this paper. In the case of LWRs, there is a strong reliance on active safety systems containing several components required to perform the desired safety function. Here we are concerned primarily with hardware failure as the system is engineered with sufficient safety factors in addition to being designed to ensure diversity and redundancy is maintained.[13] For example, the availability of the ECCS depends on whether the components making up the system are available on demand. For Generation IV nuclear energy systems, there exists a strong preference for performing safety functions passively (i.e. no external power required) where considerable gains in economics and presumably safety can be made through innovative design. However unlike active components, the overall failure of the system is not adequately described using event trees. Event trees are pictorial depictions of the Boolean logic governing the failure mode. Due to the overall simplicity of the safety system, these logical arguments provide little insight into the expected value of the failure rate.

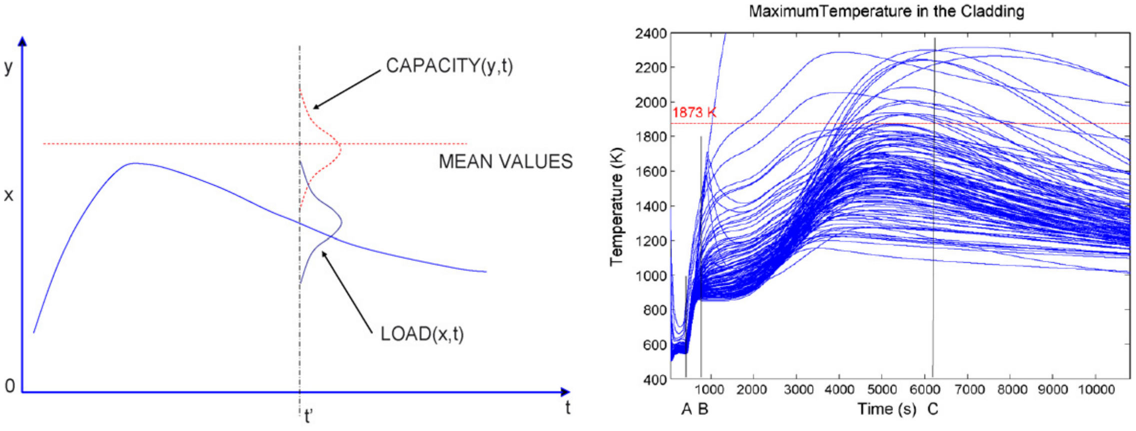
In order to better understand reliability for advanced nuclear systems, the role of a component test facility needs to be introduced. Much like how we build scaled experiments to determine system consequences given a set scenario (will be elaborated on in the following consequence space section), the reliability of SSC's for the system is initially quantified in a component test facility. The main function of the component test facility is to maximize the quantity and quality of reliability-related information available during the licensing process of the particular facility of interest. Component testing includes all safety-related SSCs under prototypical conditions for sufficient time intervals.

II.B.1 Frequency Space Uncertainty Affecting the Various Risk Cases

In addition to the traditional hardware failure rate, we must introduce the concept of functional failure. Burgazzi describes functional failure as the inability of a system to perform its mission due to deviations from its expected behavior (Figure 4)[14]. When we combine hardware failure rates, we typically assume they are binary in nature (e.g. the pump circulates fluid or it does not) whereas with functional failure we are more concerned with when the load on the system exceeds its capacity. The current practice for assessing functional uncertainty is to propagate all the associated uncertainties through the deterministic model for both the load and the capacity and define the failure rate as[14,15],

$$\mathrm{PF}_S \equiv \frac{\sum_{i=1}^{M} A(i)}{M}$$

where A(i) is assumed to be a binary variable representing failure. By performing many realizations using the deterministic model, one is able to quantify the functional uncertainty as a subjective probability.



(a) (b)

Figure 4 a) Example of load and capacity stochastic processes and b) Realizations for maximum cladding temperature where passive decay heat removal is the dominant safety system.[15]

In order to assess and quantify uncertainties associated with the component test facility, a method similar to the Phenomena Identification and Ranking Table (PIRT) process should be used to identify all key dominant phenomena affecting reliability and long-term performance of system equipment. In the case of the PIRT which will be elaborated in the consequence space section, we are typically focused on situations that occur over very short time intervals relative to the temporal scales associated with reliability. This focus on slowly-evolving phenomena as opposed to rapidly occurring phenomena represents a shift in thinking. Due to the slow nature of these degradation mechanisms, a robust strategy towards modern plant health monitoring, and maintenance procedures that can maximize the reliability and availability of the system being studied.

II.C Consequence Space

Finally, the third member of the triplet concerns the consequence or hazard posed by the postulated scenario. Since we are utilizing a bottom-up approach where systems can be decoupled and treated separately, the code, scaling, applicability and uncertainty (CSAU) methods developed for assessing consequences from a particular scenario(s) provides a nice foundation. In the case of current LWRs, a clear distinction exists between the three levels of PRA where uniquely different mechanistic models predict the associated safety consequences for each level (i.e. CDF, LERF, etc..). Innovative nuclear technology may utilize different fuel that behaves fundamentally different than LWR fuel where this delineation of PRA levels may no longer hold appropriate. In this case, new safety risk metrics must be introduced. In the case of physical resistance and protection where strategic actors may be involved, the end consequence (i.e. hostile use of diverted material) is not as useful of a metric as perhaps loss of material or loss of continuity of knowledge (i.e. minimal amount of uncertainty regarding the consequences of an event).

II.C.1 Consequence Space Uncertainty Affecting the Various Risk Cases

Assessing the uncertainties in the consequence space was initially fleshed out in 1988 during the development of the CSAU methodology in response to highly deterministic safety criteria identified in Appendix K of 10 CFR Part 50. While the technology under consideration will be fundamentally different, it is remarkable how flexible and effective these methods are in aiding the designer in best-estimate code development and scaled-experiment design. The PIRT process is an important component of CSAU where the most important and dominant phenomena are first identified and ranked and can apply to any system in the fuel cycle where physical processes take place. A properly scaled experiment provides the system designer a benchmark case for assessing the overall accuracy of the computational model used to predict the system response. It is particularly important to acknowledge that significant uncertainty may exist for particular temporal phases of the scenario under consideration. For example, when assessing the consequences of a large early release of radioactive material from an accident, advanced reactor systems are still concerned with aleatory uncertainties associated with wind patterns, local population distribution, and the associated biological hazards.

REFERENCES

1. KAPLAN, S. AND GARRICK, B. J., "On the Quantitative Definition of Risk", *Risk Analysis*, 1, 11-27, 1981.
2. "US Design Certification: Safety Classification of Structures, Systems and Components for the Pebble Bed Modular Reactor," PBMR Document Number 043553, Rev. 1, August 24, 2006.
3. BEDFORD, T. AND COOKE, R., *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press, Cambridge, 2001.
4. WINKLER, R. L., "Uncertainty in Probabilistic Risk Assessment", *Reliability Engineering and System Safety*, 54, 127-132, 1996.
5. APOSTOLAKIS, G., 1993. A commentary on model uncertainty. In: Mosleh, A., Siu, N., Smidts, C., Lui, C. (Eds.), Proceedings of Workshop on Model Uncertainty: Its Characterization and Quantification, Annapolis, MD, October 20–22, 1993. Center for Reliability Engineering, University of Maryland, College Park, MD, 1993. Also published as Report NUREG/CP-0138, US Nuclear Regulatory Commission,Washington, DC.
6. AUGER, P., *Dynamics and Thermodynamics in Hierarchically Organized Systems*, Pergamon Press, New York, 1989.
7. ALLEN, T. F. H. and Th. B. STARR, *Hierarchy-Perspectives for Ecological Complexity*, University of Chicago Press, Chicago, 1982.
8. ZUBER, N., 1991. Appendix D: a hierarchical, two-tiered scaling analysis, an integrated structure and scaling methodology for severe accident technical issue resolution. US Nuclear Regulatory Commission, Washington, DC 20555, NUREG: CR-5809, November 1991.
9. SORENSEN, J.N., APOSTOLAKIS, G.E., KRESS, T.S., POWERS, D.A., "On the Role of Defense in Depth in Risk-Informed Regulation. In: Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment, Washington, DC, August 22–26, pp. 408–413, American Nuclear Society, La Grange Park, Illinois (1999).
10. IAEA-TECDOC-1366, 2003. Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors
11. Report on the Safety of Generation IV Nuclear Systems, Generation IV International Forum Risk and Safety Working Group.
12. P. BARDET, E. BLANDFORD, M. FRATONI, A. NIQUILLE, E. GREENSPAN, and P. F. PETERSON, "Design, Analysis and Development of the Modular PB-AHTR," 2008 International Congress on Advances in Nuclear Power Plants (ICAPP '08), Anaheim, CA, June 8-12, 2008.

13. BURGAZZI, L., “Evaluation of uncertainties related to passive systems performance”,. Nuclear Engineering Design 2004;230:93–106.
14. BURGAZZI, L., “Reliability Evaluation of Passive Systems through Functional Reliability Assessment,” Nucl. Technol.,144, 145 2003.
15. MACKAY, F.J. et al., Incorporating reliability analysis into the design of passive cooling systems with an application to a gas-cooled reactor, Nuclear Eng. Design (2007)

CHAPTER 3. A FRAMEWORK FOR ASSESSING AND MANAGING THE RISKS OF ADVANCED 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 protectio****n* (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.[4] 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.[5] 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.[6]

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.

Klinke and Renn list three challenges for managing the risks of such systems: dealing with complexity, uncertainty and ambiguity, all correlated with one another.[7] Uncertainties may be of four types: aleatory, epistemic, indeterminacy, and ignorance.[8] 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." [9] 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.[10] 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 their 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.[11] 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 H_2O, 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). [12]

Of particular relevance to understanding pattern and structure are the recent advances in Network Theory.[13, 14] 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.[14] 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.[16-19] Of particular interest to this project is the recent work by Carlson and Doyle, and by Fabricant, Koutsoupias, and Papadimitriou which focuses on complexity in **designed** systems.[20-22] 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.[23] 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 socio-political 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.[20, 21] 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.[11] 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.[24] 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.[25] 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.[26] 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.

REFERENCES

1. U. S. NUCLEAR REGULATORY COMISSION. Title 10, U. S. Code of Federal Regulations, Part 50. *Safety Goals for the Operations of Nuclear Power Plants; Policy Statement,* November 30, 1988.
2. U.S. DEPARTMENT OF ENERGY, Nuclear Energy Research Advisory Committee Subcommittee on Generation IV Technology Planning, "A Roadmap to Deploy New Nuclear Power Plants in the United States by 2010", Volume I, Summary Report, October 2001.
3. U.S. DEPARTMENT OF ENERGY, Nuclear Energy Research Advisory Committee Subcommittee on Generation IV Technology Planning, "A Technology Roadmap for Generation IV Nuclear Energy Systems," Technical Roadmap Report, September 23, 2002.
4. U. S. NUCLEAR REGULATORY COMMISSION, , Title 10, U. S. Code of Federal Regulations, Part 50. *Policy Statement on Advanced Reactors,* July 8,1986.
5. U.S. DEPARTMENT OF ENERGY, Nuclear Energy Research Advisory Committee Subcommittee on Generation IV Technology Planning, "A Roadmap to Deploy New Nuclear Power Plants in the United States by 2010", Volume I, Summary Report, October 2001.
6. U.S. DEPARTMENT OF ENERGY, Nuclear Energy Research Advisory Committee Subcommittee on Generation IV Technology Planning, "A Technology Roadmap for Generation IV Nuclear Energy Systems," Technical Roadmap Report, September 23, 2002.
7. A. KLINKE and O. RENN, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based and Discourse-Based Strategies," to appear in *Risk Analysis*.
8. B. WYNNE, "Uncertainty and Environmental Learning: Reconceiving Science and Policy in the Preventive Paradigm," *Global Environmental Change,* pp. 111-127, Vol. 2, June, 1992.
9. A. KLINKE and O. RENN, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based and Discourse-Based Strategies," to appear in *Risk Analysis*.
10. L. von BERTANLAFFY. *General System Theory,* George Braziller, New York, (5th Edition) 1975.
11. S. JOHNSON, *Emergence,* The Penguin Press, London, 2001.
12. F. CAPRA. *The Web of Life,* Doubleday, New York, 1996.

13. A-L BARABASI, “*Linked: The New Science of Networks,*” Perseus Publishing, Cambridge, Massachusetts, 2002.
14. M. BUCHANAN, *NEXUS, Small Worlds and the Groundbreaking Science of Networks*, W. W. Norton and Co., New York and London, 2002.
15. J. HARTE., A. KINZIG and J. GREEN, “Self-Similarity in the Distribution and Abundance of Species”, *Science*, Volume 284, April 9, 1999.
16. C. C. BARTON and P.R. LAPOINTE, *Fractals in the Earth Sciences*, Plemum, New York, 1994.
17. R. LEWIN, *Complexity-Life at the Edge of Chaos*, Macmillen, New York, 1992.
18. B. GOODWIN, *How the Leopard Changed His Spots: The Evolution of Complexity*, Schribner, New York, 1994.
19. L. SMOLIN, *The Life of the Cosmos*, Oxford University Press, New York, 1997.
20. J. M. CARLSON and J. DOYLE, “Highly Optimized Tolerance: A Mechanism for Power Laws in Designed Systems,” *Physical Review E*, Volume 60, No.2 August 1999.
21. J. M. CARLSON and J. DOYLE, “Highly Optimized Tolerance: Robustness and Design in Complex Systems, *Physical Review Letters*, Volume 84, No. 11, March 2000.
22. A. FABRACANT, et. al., “Heuristically Optimized Trade-offs: A New Paradigm for Power Laws in the Internet, Extended Abstract for STOC 02, 2002.
23. A. REKA, et al, “Error and Attack Tolerance of Complex Networks,” *Nature*, 406, pp378-381, 2000.
24. M.E.J. NEWMAN, M. GIRVAN and J. DOYNE Farmer, “Optimal Design, Robustness, and Risk Aversion,” Santa Fe Institute Working Paper No. 0202330 v1, 20 February 2002.
25. L. CAVE and W. E. KASTENBERG, “On the Application of Probabilistic Risk Assessment to Reactors with Inherently Safe Features,” *Nuclear Engineering and Design*, Volume 128, 339-347, 1991.
26. NATIONAL RESEARCH COUNCIL, *Understanding Risk: Informing Decisions in a Democratic Society*, National Academy Press, Washington, DC, 1996.

CHAPTER 4. IMPLEMENTING A ROBUST PROSPECTIVE APPROACH TO RISK ASSESSMENT FOR NUCLEAR ENERGY SYSTEMS

I. INTRODUCTION

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 regulation.

Often missing in discussions of the Generation IV technical roadmap is the need for an overall strategy for the integral fuel cycle based upon assessing and managing consequences and uncertainties with respect to the issues related to sustainability, economics, safety and reliability, and proliferation resistance and physical protection. The requirement of meeting Generation IV goals may result in competing challenges, e.g. satisfying proliferation/protection-oriented goals may be counterproductive to enhancing safety. In this context, challenging the field of risk assessment to be *prospective* raises a number of methodological hurdles when prioritizing engineering design and regulation activities. These challenges can be broadly classified into two principal areas: complex systems modeling and multiobjective decision-making under deep uncertainty.

The nuclear energy system model is technologically complex in the sense that the system features multiple nonlinear interactions between different levels of systems aggregation. In addition to the multi-millennia time scales and the associated intergenerational impacts of nuclear waste, the evolution of nuclear energy systems will take decades to occur given the expected rate of technological development, long facility lifetimes, constraints on the availability of fissile materials, and dispersed decision-making responsibilities.[1,2] The consequences of utilizing these systems are inextricably linked to deployment strategy and depend on the comparative advantages and tradeoffs of these systems measured against a broad set of incommensurable criteria.

Formal decision-making methods enhance the ability to analyze and manage complex systems, but numerous sources of uncertainty, some quantifiable and some not, pervade the long-term planning problem. Multiple incommensurable objectives, changing societal preferences, shocks and surprises, and continuing technology development are all facets of the ever-changing nuclear technology landscape. Commonly used decision-making frameworks utilizing probabilistic descriptions of uncertainty struggle with identifying an overall strategy when confronted with the inherent complexity, uncertainty, and ambiguity of the next generation of nuclear energy systems. The inability to predict hampers the development of prescriptive policies and limits top-down feedback to systems designers. The human tendency to overcome uncertainty through prediction or extrapolation from history faces the hazard of formulating strategies vulnerable to the inevitable shocks and surprises that undermine assumptions.[3]

The overall goal of this framework is to develop long-term nuclear energy planning methods to provide quantitative top-down feedback to policy-makers and to system designers in a manner cognizant of the deep uncertainty in long-term planning. A multidisciplinary and multiobjective robust decision-making framework is proposed to analyze a dynamic nuclear energy system model. Facets of this framework include,

- Sociotechnical Systems and Long-Term Energy Planning
- Robust Decision-Making under Deep Uncertainty
- Multiobjective Optimization with Evolutionary Algorithms
- Nuclear Energy Systems Modeling
- Defining Goals

I.A. Previous Work

Previous nuclear fuel cycle studies have produced insights into system behavior and have established research and development priorities by assessing a limited set of plausible scenarios of future nuclear energy demand.[4,5,6] For instance, principal findings of the Generation IV Fuel Cycle Assessment Report demonstrated the role of transitioning to closed fuel cycles for improving sustainability, managing waste, and fissile material inventories, improving sustainability, and noted the decoupling of economics from other objectives. Research and development recommendations from this study include improving fuel performance and developing new fuels to accommodate plutonium and minor actinides, developing cost effective advanced recycle technologies, the need to manage short-term heat loading, and the proliferation resistance benefits of recycling.

These scenario-based analyses are useful for anticipating the magnitude of the consequences associated with various changes, determining the degree to which consequences can be mitigated, and more completely describes information about the future than point estimate or probabilistic forecasts. Scenario-based planning, however, offers no systematic means to compare alternative strategies. Consequently, policy prescriptions can largely reflect prevailing wisdom and predictions of the future leading to strategies highly vulnerable to shocks and surprises to the underlying assumptions.[7,8] Furthermore, the results from complex models limit accessibility to decision-makers, particularly those more accountable to the public interest that often lack the necessary expertise. Attempts at developing nuclear energy system strategies robust to assumptions and more understandable by decision-makers have largely been qualitative in nature (see Figure).[9]

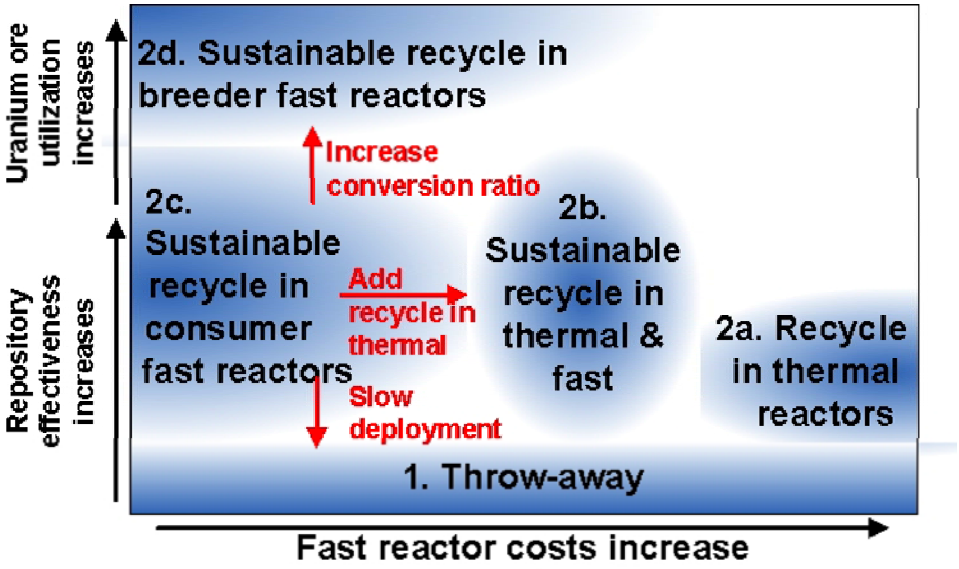

Uranium ore utilization increases
Repository effectiveness increases
2d. Sustainable recycle in breeder fast reactors
Increase conversion ratio
2c. Sustainable recycle in consumer fast reactors
Add recycle in thermal
Slow deployment
2b. Sustainable recycle in thermal & fast
2a. Recycle in thermal reactors
1. Throw-away
Fast reactor costs increase

Figure 1 Qualitative robustness diagram identifying preferred nuclear energy system strategies under varying assumptions and a possible adaptive strategy (red).

II. Sociotechnical Systems and Long-Term Energy Planning

A multidisciplinary sociotechnical systems analysis approach applied to nuclear energy systems incorporates synoptic, reductionistic, and structural points of view. The synoptic overview includes the values of importance to the decision maker i.e. goals. A reductionistic view decomposes the system into smaller isolated components that are then connected structurally.[10] A sociotechnical approach is inherently multiobjective in its outlook by optimizing social and technical factors that influence system behavior. As a subset of sociotechnical systems analysis, long-term energy planning encompasses a broad taxonomy of modeling approaches that typically trade-offs sophistication of economic modeling for lower complexity energy sector models (see Table 1).[11]

Table 1 Long-Term Energy Planning Taxonomy

General Equilibrium (GE) Models		Partial Equilibrium Models		
Multi-Sector GE Models	Optimization Models		Energy Sector Models	Single-Fuel Model
	Economy-Wide Aggregate Optimization Models	Partial Equilibrium Optimization Models		

Utilizing general equilibrium models, scenarios of nuclear energy demand have been developed for a variety of plausible socio-economic and environmental development paths subject to a range of climate stabilization targets. The integrated assessment modeling framework used to generate these scenarios incorporate a variety of sectors that contribute to greenhouse gas emissions including energy, industry, agriculture, and forestry. Each scenario contains a set of assumptions on key uncertainties regarding developmental pathways, vulnerability to climate change, and climate stabilization goals (see Table 2 and Figure 2).[12,13]

Table 2 IIASA Greenhouse Gas Initiative Taxonomy of Scenarios

Uncertainty Type	Factors Affecting Uncertainty	A2r	B2	B1
Emissions	Population size	H	M	L
	Income	L	M	H
	Resource use efficiency	L	M	H
	Technology dynamics (fossil)	M	M	L
	Technology dynamics (non-fossil)	L	M	H
	Emission	H	M	L
Vulnerability	Population size	H	M	L
	Urbanization	H	M	L
	Income	L	M	H
	Vulnerability	H	M	L
Stabilization Target	Exogenous input			
	Scale of required reduction	H	M	L

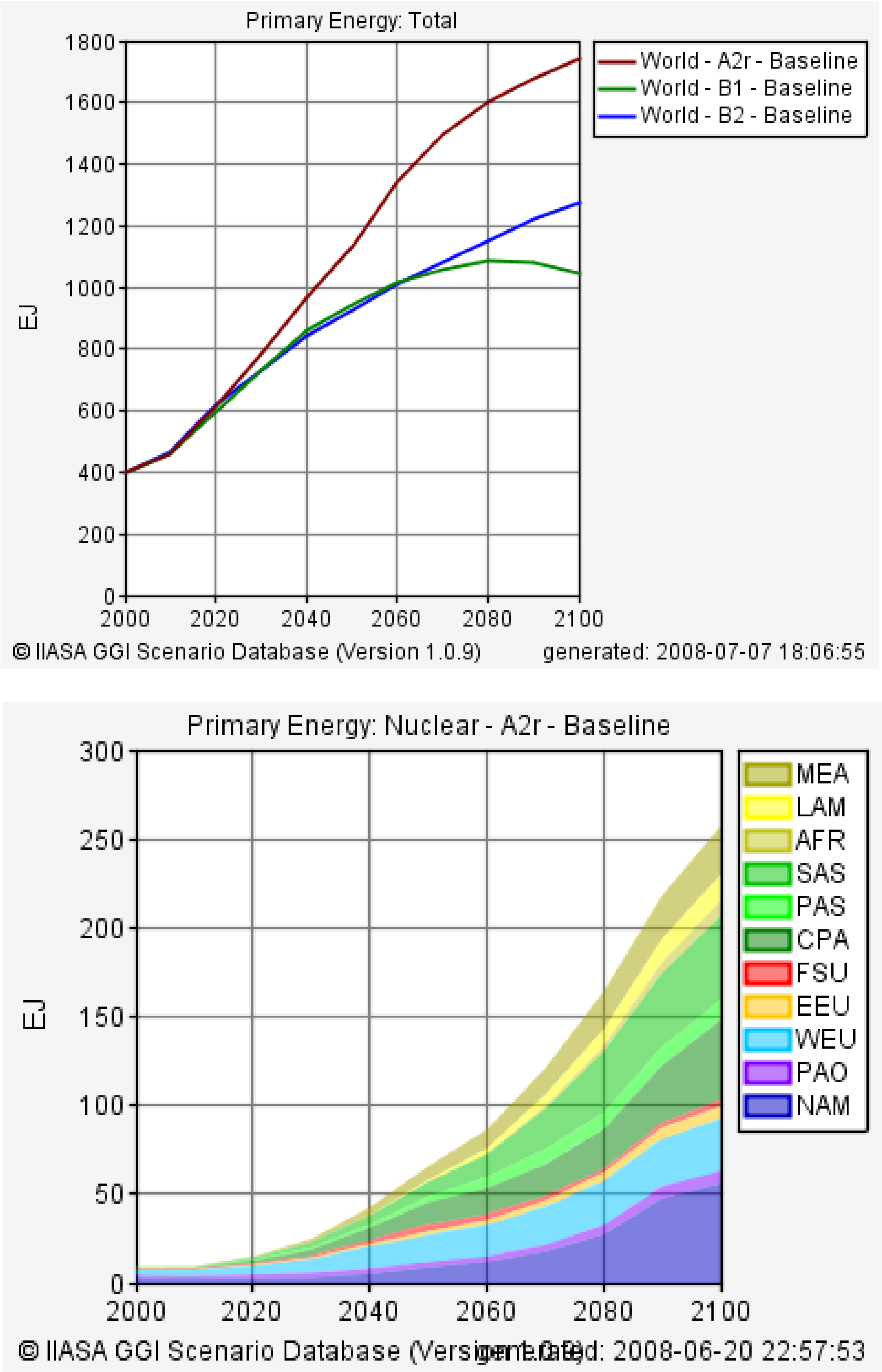


Figure 2 IIASA/GGI primary energy baseline scenarios (top) and A2r regional nuclear energy scenarios (bottom)

In this study, a partial economic equilibrium model of the nuclear energy sector is developed with end-use demands specified exogenously by macroeconomic general equilibrium models. Representative scenarios reflecting low growth, high growth, (IIASA/GGI) and phase out (IIASA/WEC)[14] in the nuclear sector are selected to assess the performance of nuclear energy system across a wide spectrum of plausible futures. The potential distortions from a partial equilibrium model are important to note. The consequences of ignoring the structural connections between the nuclear sector and macroeconomic models depend on the elasticities of substitution between energy technologies[15] and have not been fully evaluated.

III. ROBUST DECISION-MAKING UNDER DEEP UNCERTAINTY

Developing prescriptive policies under conditions of deep uncertainty of the future challenge traditional decision-making frameworks that demand more information than available. Decision-making under risk (in contrast to decision-making under certainty) typically seeks optimal solution(s) based on probabilistic descriptions of uncertainty.[16] Under conditions of deep uncertainty, however, all parties to a decision cannot agree upon the model describing the system, the probability distributions characterizing uncertainty about model parameters, or the system of values by which to judge the alternative outcomes.[17]

Robust solutions are often sought under conditions of deep uncertainty. These strategies perform relatively well across a wide range of plausible futures rather than optimizing against certain or probabilistic predictions. A number of methods have been proposed to identify robust solutions, but none are generally accepted. Sensitivity analysis is frequently employed to test a strategy's vulnerability to epistemic and aleatory uncertainties. However, solutions insensitive to assumptions are not necessarily available. Other methods for decision-making under uncertainty include Laplacian indifference, maximax, minmax, satisficing, minimax regret, multiobjective outranking,[18] and information gap robustness and opportunity.[19]

Within the ongoing development of robust decision-making research, efforts at merging scenario-based planning within a quantitative decision analysis framework appear to have promise. Methods for long-term policy analysis, such as RAND's Exogenous-Levers-Response-Measures (XLRM) and Computer Aided Reasoning (CAR) frameworks couple robust decision making with computer-human feedback. The focus of long-term policy analysis under deep uncertainty presents a shift from a framework of prediction driving prescription to a framework assessing the potential long-term consequences of near-term actions. Instead of identifying optimal strategies, robust (possibly adaptive) strategies are sought that satisfice across a broad range of plausible scenarios. Ultimately, long-term policy analysis recognizes the relationships between analyst, model, and data by exploring a broad set of plausible futures. This approach has demonstrated success quantifying and comparing the performance and robustness of various adaptive strategies within the context of developing near-term pollution control strategies to promote long-term economic growth and environmental quality (see Figure 3). [20,21,22]

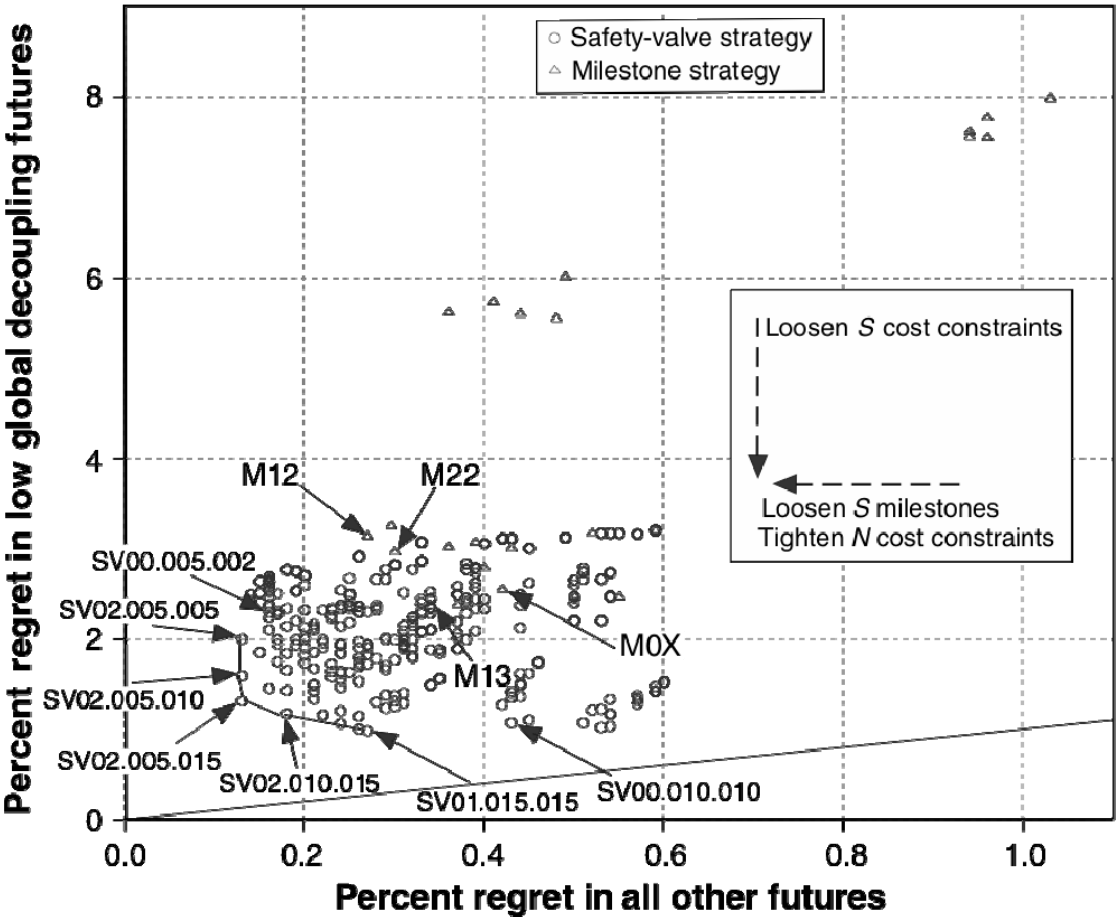


Figure 3. Comparing the robustness of safety-valve and milestone adaptive strategies. Safety-valve emerges as the least regret adaptive strategy.

IV. MULTIOBJECTIVE OPTIMIZATION WITH EVOLUTIONARY ALGORITHMS

Multidisciplinary design optimization permits the utilization of interactions between disciplines. Simultaneous multiobjective optimization is thought to produce superior results in comparison to sequential interdisciplinary efforts, but comes at the expense of greater complexity. Applied to the context of nuclear energy systems, a framework and analytical techniques for integrating multiple objectives into design is sought to identify and maximize synergies and balance conflicts across the possible design configurations and operating modes of a nuclear energy system.[23]

Incommensurable objectives that are not readily incorporated into a single performance measure introduce an element of complexity as decisions are often sensitive to the preferences of the decision-maker and society at large. A multiple objective optimization approach recognizes the importance of all objectives by generating a set of Pareto efficient trade-off solutions. In contrast to multiobjective approaches that optimize against a multiple attribute utility objective, higher level non-technical, qualitative, and experiential factors are applied *post hoc* in a multiobjective approach to select the preferred solution from a set of nondominated solutions.[24]

IV.A Multiobjective Evolutionary Algorithms

Genetic or evolutionary algorithms that mimic Darwinian natural selection offer a robust method for solving complex models. Conventional optimization approaches relying upon gradient-based transition rules are typically limited to smooth continuous surfaces. Multiobjective approaches usually require information on weightings between incommensurable objectives or computationally intensive searches of the decision space. Stochastic decision rules featured in evolutionary algorithms can handle more complex decision spaces including discrete decision variables and discontinuous objective surfaces and search the decision space in an intelligent manner.

Evolutionary algorithms track the evolution of a population of solutions, evaluating their fitness at each generation, and evolving the population through biology inspired reproduction operations that select the most fit individuals for crossover and mutation. In a multiobjective problem, model results are calculated for each individual in the population and ranked by Pareto dominance. The output is a trade off surface between the multiple objectives identifying Pareto efficient solutions and excluding infeasible and inefficient solutions.[25,26] The NSGA-II multiobjective evolutionary algorithm selected for this study incorporates a number of features that speed convergence or provide greater flexibility in problem specification. These features include a fast sorting algorithm, elitism to preserve best solutions from one generation to the next, niching to pressure solutions out of crowded regions to promote solution diversity, and non-penalty-based constraint handling to prevent distortions of the solution space by constraint violation penalties.[27]

A large number of objectives slows convergence of the genetic algorithm to the Pareto efficient front due to 1) more numerous possibilities for nondominated solutions, and 2) greater computational complexity of niching algorithms that maintain diverse solutions on the Pareto front. Dimensionality reduction or preference information can be applied to speed convergence. Structured human-in-the-loop feedback methods may be more appropriate, but “decision-maker in the loop” methods can introduce excessive subjectivity into the results and obviates many of the benefits of multiobjective optimization. Genetic algorithms incorporating multivariate statistical feature extraction provide a computational approach to dimensionality reduction that preserves the benefits of multiobjective optimization. Extracting a lower dimensional space from a high dimensionality space promotes algorithm convergence by eliminating redundant objectives and identifying conflicting objectives that generate tradeoffs. A principal components analysis (PCA) based multiobjective evolutionary algorithm has shown success in eliminating redundant objectives for two or three-dimensional Pareto frontiers amongst as many as thirty initial objectives. (See Figure 4) However, the PCA method is vulnerable to higher dimensionality Pareto fronts.[28] Non-linear dimensionality reduction approaches utilizing maximum variance unfolding have demonstrated the ability to effectively reduce dimensionality by identifying data that occupy a non-linear manifold (See Figure 5).[29]

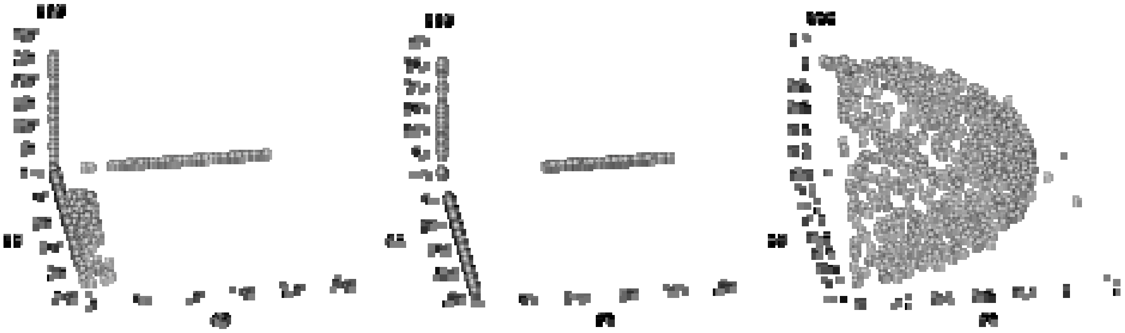


Figure 4. Dimensionality reduction via principal components analysis finding a three dimensional Pareto front from an initial set of ten objectives. Results of PCA-NSGA-II on test problem DTLZ5(3,10) after first (left), second (middle), and third (right) iterations.

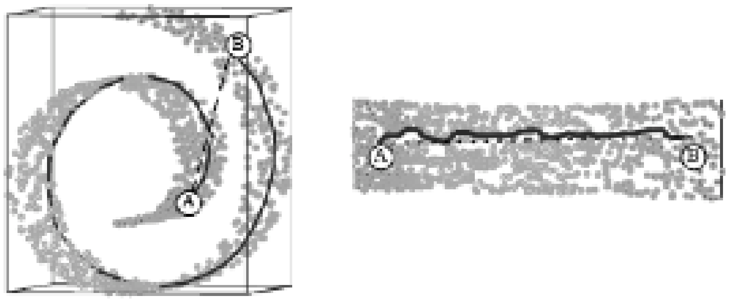


Figure 5. Illustration of submanifold unfolding identifying underlying dimensionality of data.

V. NUCLEAR ENERGY SYSTEM MODELING

The model of the nuclear energy system is composed of representative classes of reactors and fuel cycles (burner, converter, breeder), associated processing facilities (enrichment and reprocessing), and storage facilities for fresh and irradiated fissile fuels and materials. The approach is largely conceptual capturing important details regarding technical design and facility operations, but lacking the higher fidelity neutronics and recycling calculations. This simplified model of the nuclear fuel cycle calculates energy output and materials inventories as a function of reactor deployment decisions and specified reactor performance parameters (e.g. power, fissile loadings, design lifetime, etc). To couple with evolutionary algorithms, the model is designed to model the outcomes of any deployment decision. The model is comprised of several modules that are related by material, energy, and information flows. These modules include 1) population dynamics, 2) materials tracking, 3) energy products, and 4) outcomes.

V.A. Population Dynamics

The population dynamics model tracks the number of reactors in various stages of deployment (licensing, construction, operation, decommissioning) arising from deployment decisions. Reactor operations are tracked for the entire design lifetime irrespective of whether operations extend beyond the 100 year planning horizon. The number of existing reactors and their decommissioning schedules are initial conditions. No additional effort is made to constrain the dynamics of the population within this module. However, these deployment decisions may generate constraint violations or impact other modules. For instance, attempting to deploy a reactor without the necessary fissile material imposes construction costs without generating energy and revenues. Other fuel cycle facilities of interest include enrichment and reprocessing capacity and are assumed to be available as necessary.

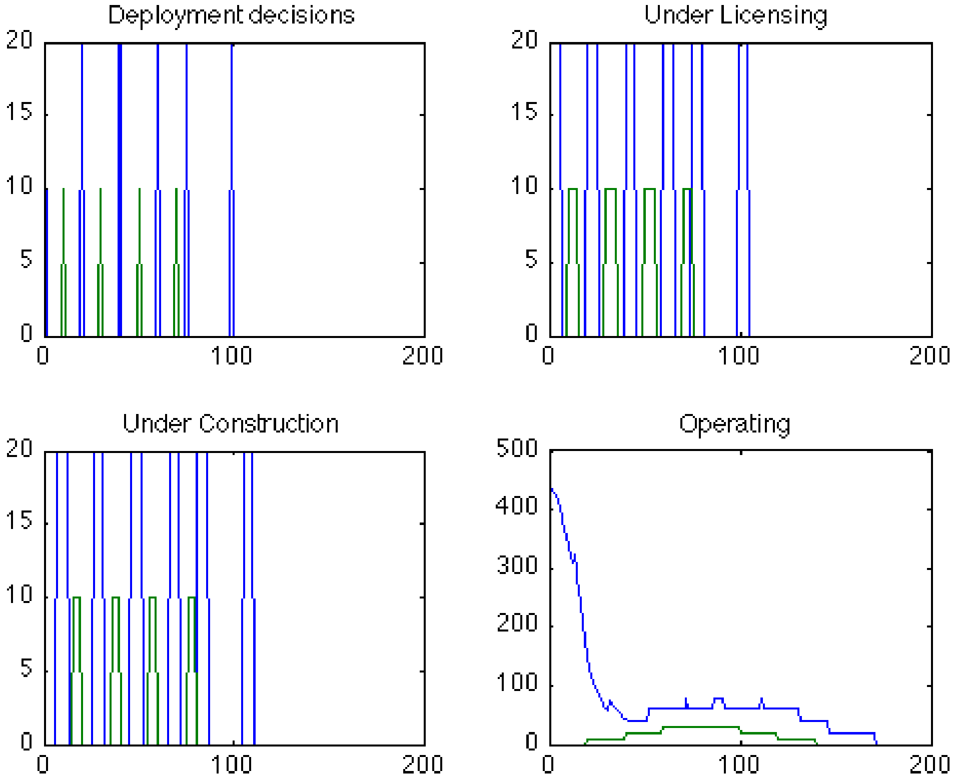


Figure 6. Population dynamics model for arbitrary deployment decisions for two reactor types

V.B. Materials Tracking

Material mass with limited composition information is tracked throughout the nuclear fuel cycle. Multiple fuel bins (unirradiated natural resources, in-core inventories, spent fuel interim storage, repository) track material inventories throughout the fuel cycle from cradle-to-grave. In lieu of detailed radionuclide transport models necessary for a total systems performance assessment of geological repositories, important characteristics of the waste products are tracked.[30] Using ORIGEN to perform depletion and decay calculations for representative nuclear energy systems[32], the mass/volume, short-term decay heat, and long-term radiotoxicity of spent fuel are calculated as they are important determinants of repository performance.

VI. DEFINING GOALS

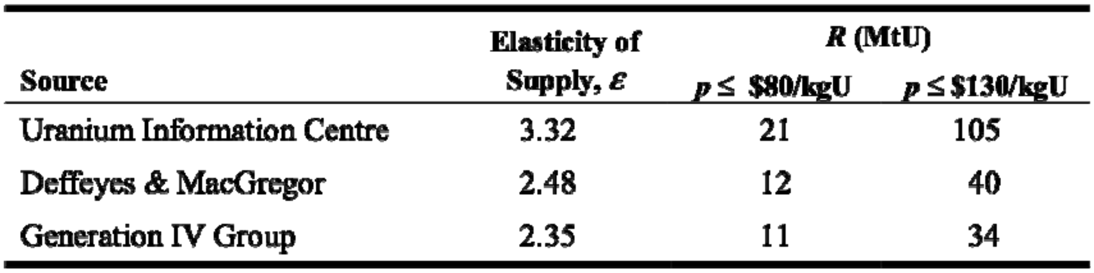
A major objective of this project is to develop a set of technology-neutral quantitative safety goals representing these "top-level" qualitative goals and a method for their allocation to the various system elements including a framework for quantifying the risk and the associated uncertainty. Underlying 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 protectio****n* (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. Here we concern ourselves with defining metrics by which to measure system performance rather than suggesting numerical goals. Decisions as to what combination or combinations of system are acceptable are made by posing a set of Pareto efficient solutions to a decision maker.

VI.A Natural Resource Sustainability

The vagaries of resource estimation preclude firm quantification of total resources available.[32] As such, the proposed natural resource sustainability measure seeks to minimize the cumulative quantity of natural resources consumed by the end of the planning period. Fuel cost escalation with resource consumption is a key linkage between the economics and fuel cycle models that influence decisions on resource utilization. Multiple estimates of price-supply elasticities will be posed when assessing the robustness of fuel cycle strategies. (See Table 3) In the formula below, R, is the total uranium resource recoverable at price p and ε is the long-term price elasticity of supply.[33]

$$R = 2.1\left(\frac{p}{40}\right)^{\varepsilon}$$

Table 3 Uranium supply elasticity estimates



Source	Elasticity of Supply, ε	R (MtU) $p \leq$ \$80/kgU	$p \leq$ \$130/kgU
Uranium Information Centre	3.32	21	105
Deffeyes & MacGregor	2.48	12	40
Generation IV Group	2.35	11	34

VI.B. Waste Management

As noted above, the mass/volume, short-term decay heat, and long-term radiotoxicity of spent fuel are calculated in lieu of detailed radionuclide transport calculations. The simultaneous minimization of all three objectives are sought to improve repository performance. Some effort has been made to calculate the number of Yucca Mountain equivalents with a simplified repository model based on nominal waste mass and short-term heat load constraints to reduce the dimensionality of the waste model. By doing so, economic impacts can be extended beyond the Nuclear Waste Policy Act waste fee that imposes a tax based upon energy generation.[34] However, the short-term and long-term repository impacts may not be commensurable through time discounting.

VI.C. Economics

An economics model consistent with the Generation IV Economics Modeling Working Group's draft report is under development. This approach calculates the present value of profit streams and capital at risk to a single present day decision-maker given a deployment strategy, the operational timeline of the reactor, plant cost structure, and various parameters describing energy and finance market conditions. The decision-maker is assumed to maximize profits and minimize capital-at-risk such that capital-at-risk counterbalances cost efficiency achieved through economies of scale.[35,36] Uncertainties in economic performance will be a key element when assessing robustness as the history of nuclear energy to date reflects significant variation in economic performance and high cost surprises.[37,38]

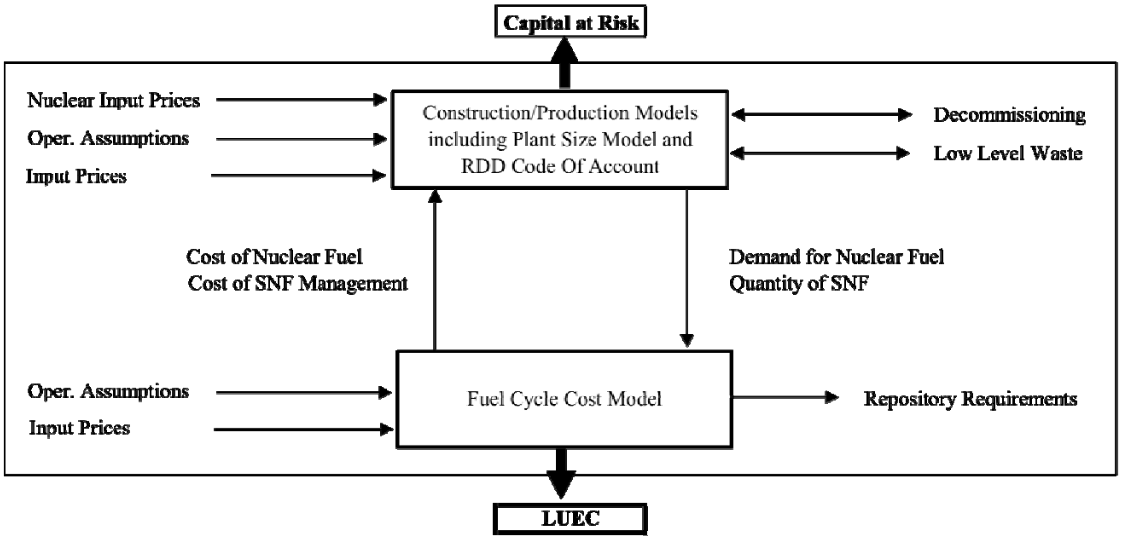


Figure 7. Generation IV Economics Modeling Working Group's proposed integrated nuclear energy economic model (GIF/EMWG, 2006)

Table 4 Economics Parameters

Category	**Parameters**
Timeline	Licensing Construction Operation Decommissioning
Market	Electricity demand Real price of electricity
Finance	Debt-to-Equity ratio General inflation rate
Plant Cost Structure	Overnight cost Construction cost profile Operations and maintenance (fixed and variable)

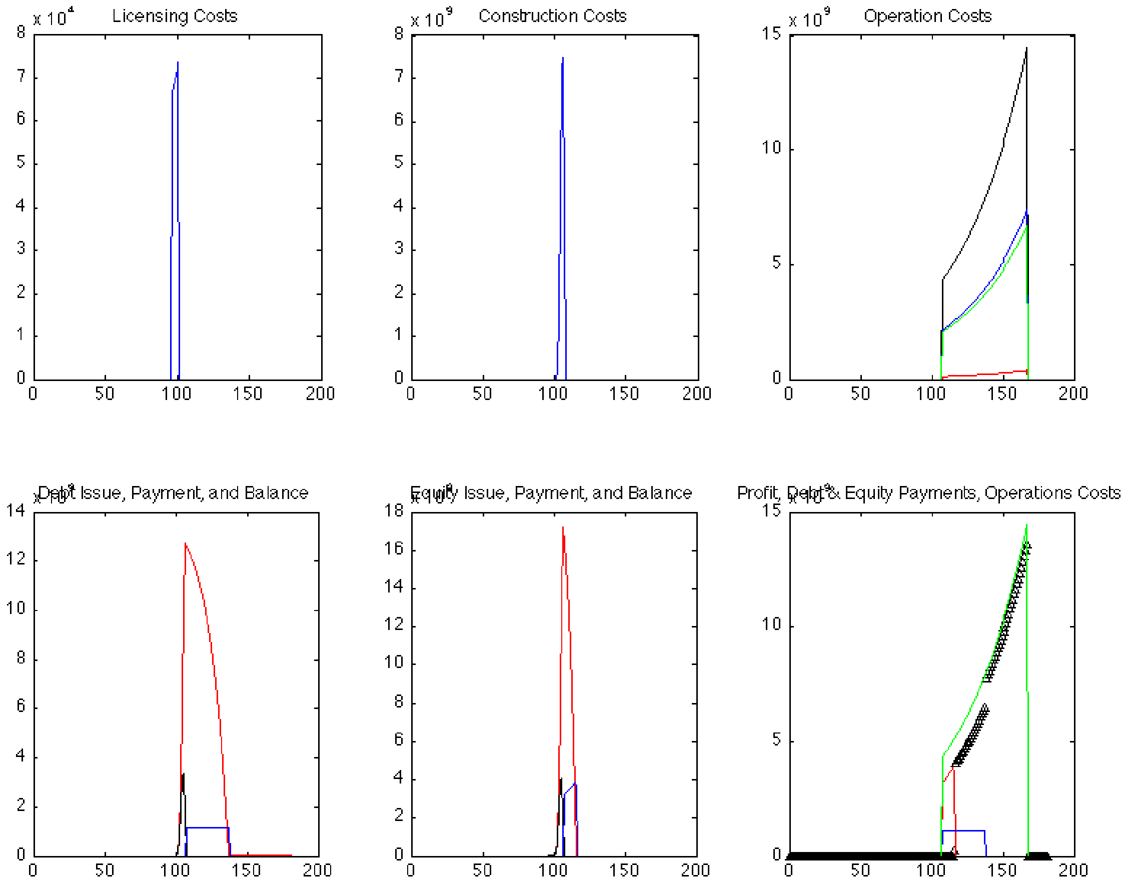


Figure 8. Economic calculation for a single reactor over its lifetime demonstrating impact of various costs, debt/equity financing, revenues, and inflation on profits.

VI.D Safeguards and Security

Safeguards and security (S&S) is the general term given to the protection from theft or diversion of Special Nuclear Material (SNM) as a result of human malicious acts, sometimes in combination with random non-human events. As such, it considers insider threats, outsider threats and a combination of both that can lead to accidents, loss of material accountability and/or control, or loss of bulk material. In addition to personnel, computer/information and operations security, S&S design is concerned with physical protection systems (PPS) and material, control and accountability (MC&A) systems. In this project we focus on the PPS and MC&A systems as examples of how S&S is integral to any nuclear energy system and the interaction between physical and human factor ingredients.

VI.D.1 Security

While quantitative risk analysis techniques have been successfully applied to manage safety risks at nuclear power plants, applying a similar risk minimization framework to security has limited value due to severe uncertainties in adversary behavior and neglects the strategic nature of malicious human acts. The application of game theory methods to security provides a framework by which to better understand the strategic interaction between defender and adversary. The security problem is modeled as a resource allocation problem at the level of an individual facility (e.g. a nuclear power plant) and across multiple types of critical infrastructure (e.g. nuclear and non-nuclear).

The current framework for managing security risk is based on demonstrating adequate protection against a Design Basis Threat (DBT) and is thought to incompletely characterize risk, ineffectively identify cost-effective risk management options, and lead to escalating physical protection costs. The management of security risk based on prioritization by conditional risk (i.e. probability of adversary success given that the specified threat occurs) poses problems with ranking threat scenarios and resource allocation. Conditional risk measures typically reflect inadequate knowledge of attack frequency and/or unacceptably high consequences where frequency of attack is considered unimportant.[39] Conditioned on the DBT occurring, the effectiveness of the system considers the likelihood of sensing, assessing, detecting, interrupting, and neutralizing the adversary by the timely response of a protective force.[40] However, focusing on the highest ranked scenario on a conditional risk basis may not represent the most cost effective approach to risk reduction.[41]

In place of current policy, a risk-informed, threat-likelihood-consequence approach[42] has been proposed to better assess security risk while limiting cost escalation. This principally consists of a more complete, probability-weighted DBT as an input to a vulnerability analysis. A more complete range of threats may identify risk significant vulnerabilities, some of which may be initiated by low capability-high frequency threats, presumably while discounting high capability-low frequency threats. While risk-informed approach has the benefit of assessing risk more completely, principal limitations include the certainty of estimating the likelihoods of threats and the strategic response of the adversary to defensive actions.

While a more complete probabilistic DBT confers a number of advantages, the principles of assessing the frequency of a random event such as a hurricane or a terrorist attack are not well suited to describing the intelligent nature of a human adversary that optimizes and adapts. Numerous sources cite the drawbacks of probabilistic descriptions of human behavior and their use in risk analysis.[43.43,45] One such criticism comes from the seminal moments of game theory,

> “Every participant can determine the variables which describe his own actions, but not those of the others. Nevertheless those ‘alien’ variables

> cannot, from his point of view, be described by statistical assumptions. This is because the others are guided, just as he himself, by rational principles – whatever that may mean – and no *modus procedendi* can be correct which does not attempt to understand those principles and the interactions of the conflicting interests of all participants.”[46]

To better model the strategic interaction between defender and adversary, game theorists have identified a defensive strategy that minimizes the adversary’s maximum expected gain as a Nash equilibrium solution to a simultaneous, two-person, zero-sum game where no actors can do better by unilaterally changing strategy.[47] If such a model is appropriate, this minimax objective represents a departure from risk management methods based on adversary intentions to a method based on adversary capabilities.[48]

<u>Single Infrastructure</u>: For a facility like a nuclear power plant, redundant and diverse subsystems give rise to dependencies between sets of targets that an adversary can choose to attack. (See Figure 9)

Random events, r, and malicious human acts, mha, contribute to the frequency of a top event such as a large release of radiation, lr, that is preceded by the generation of a source term and the failure of containment, cf.[49] Severe uncertainties of the attack frequency, λ_{mha} and conditional probabilities, α_i, of attack sequences, a_i, limit the value of a risk minimization framework.

$$\lambda(\mathrm{lr}) = \lambda_{\mathrm{r}}\mathrm{P}(\mathrm{a}\,|\,\mathrm{r})\mathrm{P}(\mathrm{cf}\,|\,\mathrm{r}) + \lambda_{\mathrm{mha}}\left\lfloor \sum_{\forall \mathrm{i}} \alpha_{\mathrm{i}}\mathrm{P}(\mathrm{a}_{\mathrm{i}}\,|\,\mathrm{mha}) \right\rfloor \mathrm{P}(\mathrm{cf}\,|\,\mathrm{mha})$$

A mathematical program is defined that allocates limited safety resources, R_{safety}, amongst safety-related targets to minimize risk against a set of initiating events, IE, that occur with known frequency, λ. The set of safety-related sets of targets are the sets of targets that must be disabled to generate a source term and fail containment. The rare event approximation is applied to find the probability of the top event.

$$\min_{\bar{\mathrm{r}}} \mathrm{C} \sum_{\mathrm{k}\in \mathrm{IE}} \lambda_{\mathrm{IE}_{\mathrm{k}}} \Pr\left(\mathrm{TE}\,|\,\mathrm{IE}_{\mathrm{k}}\right)\left(\bar{r}\right)$$

$$\text{s.t.}$$

$$\sum_{\mathrm{i}\in \mathrm{T}_{\mathrm{safety}}} \mathrm{r}_{\mathrm{i}} \le \mathrm{R}_{\mathrm{safety}}$$

$$\mathrm{r}_{\mathrm{i}} \ge 0, \forall \mathrm{i} \in \mathrm{T}_{\mathrm{safety}}$$

The conditional probability of failure of a target given a specified initiating event is assumed to be a decreasing convex function of resources expended on that target.

$$\Pr_{\mathrm{i,k}}(\mathrm{failure}\,|\,\mathrm{IE}_{\mathrm{k}}) = \Pr_{\mathrm{i,k,0}} e^{-\mathrm{h}_{\mathrm{i,k}}\mathrm{r}_{\mathrm{saf,i,k}}}$$

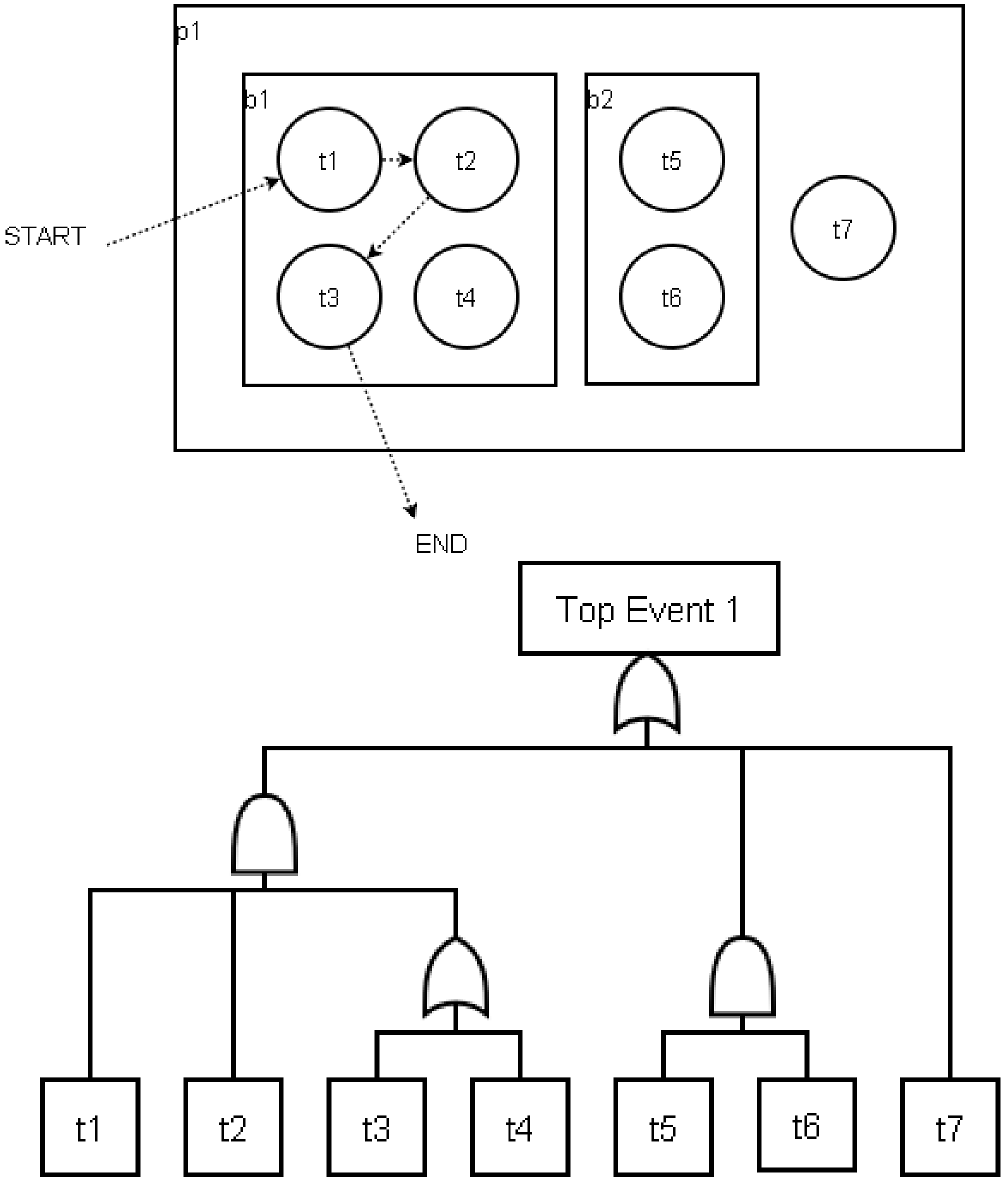


Figure 9. System model with adversary pathway (top) and fault tree (bottom).

Security is assessed with risk minimization and minimax objectives utilizing a pathway-based assessment of physical protection system performance.[50,51] Likely pathways are identified for a well-defined single adversary intent on effecting a large release where exiting the system is unimportant. The performance of the system relies entirely on the intrinsic vulnerability of the targets and pathways. The vulnerability of each target is a decreasing convex function and is conditioned on adversary capabilities. Security-related targetsets, TS, are sets of components that must be disabled and pathways that must be traversed for the adversary to effect a large release. The vulnerability of each targetset, V_{TSi}, is calculated with the rare-event approximation.

The risk minimization approach allocates security resources, $R_{security}$, by assuming an adversary attack strategy, α, representing the conditional probability that an adversary will choose a targetset. A minimax security model allocates resources to minimize an adversary's maximum gain.

$$\begin{aligned}&\min_{\vec{r}} C \sum_{\forall TS_i} \alpha_{TS_i} V_{TS_i}(\vec{r})\\ &\text{s.t.}\\ &\sum_{i \in T_{security}} r_i \le R_{security}\\ &r_i \ge 0, \forall i \in T_{security}\end{aligned}$$

$$\begin{aligned}&\min_{\vec{r}} z = w\\ &\text{s.t.}\\ &w \ge C\, V_{TSi}, \forall TS_i\\ &\sum_{i \in T_{security}} r_i \le R_{security}\\ &r_i \ge 0, \forall i \in T_{security}\end{aligned}$$

Comparing the reductions in risk with expanding resources, a risk minimization approach to security can underestimate risk in comparison to the minimax solution. In the former approach, assumptions of an adversary's intentions create uncertainties in risk reduction. A minimax approach based on adversary capabilities is a risk adverse strategy that introduces the arguably reasonable assumption that the adversary will choose to attack the targets with the highest expected payoff.

Error! Not a valid link.

Figure 10. Risk reduction profiles for risk minimization and minimax models.

Error! Not a valid link. **Error! Not a valid link.**

Figure 11. Minimax allocation (left) and balanced protection (right)

In the absence of information on the frequency of attack, the Pareto efficiency criterion identifies nondominated combinations of safety and security given available resources and technological possibilities. The preferred solution is identified by maximizing a multi-attribute utility model of individual choice describing preferences for safety, security, and opportunity cost with assumed constants and weighting factors.

$$U(s,\psi,R_{total}) = w_s e^{-k_s s} + w_\psi e^{-k_\psi \psi} - w_{oc} R_{total}$$

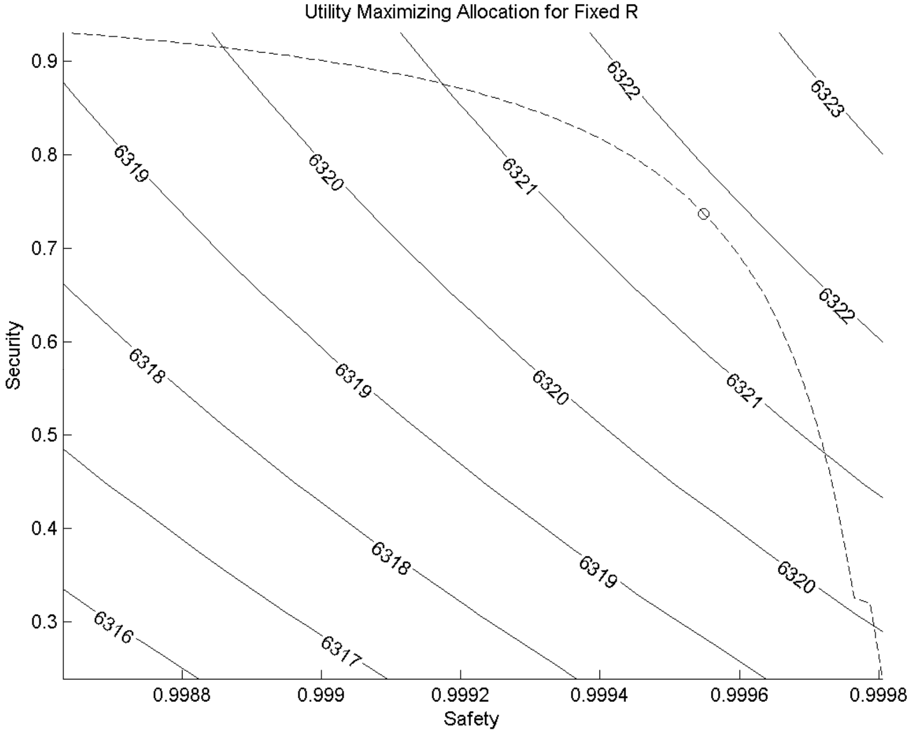


Figure 12. Efficient frontier at a fixed level of resources and lines of isoutility.

In summary, a method for managing safety and security risk is explored for a system that achieves high reliability through redundancy and diversity. The minimax objective represents a shift from risk management based on assumptions of an adversary's intentions to one based on an adversary's capabilities. Such an approach is consistent with the Generation IV Proliferation Resistance and Physical Protection methodology that advocates risk assessment conditioned on a reference threat occurring. A risk management approach based on adversary intentions converges with a capabilities approach if the adversary is assumed to attack the most vulnerable set of targets. In the absence of information on the frequency of an attack, the efficient frontier identifies efficient combinations of safety and security. Though the Pareto efficiency criterion is agnostic on the preferred allocation between safety and security, it excludes inefficient and infeasible solutions that a decision-maker should avoid. The multiattribute utility function that identifies the preferred allocation largely reflects perceptions of the frequency of an attack.

A number of extensions can be envisioned to the method described. An integrated model may better assess the effects of synergistic or antagonistic interactions between safety and security. Passive safety systems could be better treated with capacity-demand models describing functional failures. A security performance metric based on a timely detection better captures detection, delay, and response elements of a physical protection system. Information gap decision theory may identify a maximally robust allocation against uncertainty in attack frequency. In all cases, heuristic optimization algorithms may better accommodate more complex models.

Multiple Infrastructure: Defending multiple types of critical infrastructure poses the additional challenges of modeling multiple consequences. Not only do the type and scale of consequences vary by target, the adversary and defender may weigh these outcomes differently in their overall measure of utility. Three approaches to managing security risk are assessed and compared: 1) design basis threat, 2) risk informed, and 3) game theoretic. In all approaches, the defender and adversary control the distribution of limited resources amongst two types of critical infrastructure, nominally nuclear and non-nuclear. The adversary chooses how to allocate his resources amongst multiple targets and amongst multiple attack capabilities. The defender can allocate her limited resources to mitigate consequences at a site, increase the cost to adversary of conducting an attack, and/or decrease the vulnerability of the targets. Each actor is represented by a genetic algorithm that attempts to find a global maximum under resource constraints.

The Design Basis Threat approach ensures that system effectiveness is below an acceptable level for one threat of interest. Security standards based on conditional probability of success are necessary when the frequency of the initiating event is unknown and/or the consequences are sufficiently high to demand protection regardless of attack frequency. System effectiveness is measured based on the likelihood of sensing, assessing, detecting, interrupting, and neutralizing the adversary by the timely response of a protective force conditioned on the specified threat occurring. To limit the number of variables, these factors are reduced to a target vulnerability function. In the model below, the defender can effect changes in the vulnerability of a target by allocating limited resources to each target. The vulnerability of the two sites is based on the maximum vulnerability of all four targets for a single adversary capability. Neither the frequency of attack nor the consequences of the attack are considered. An acceptable performance criteria constraint can be imposed such that additional resources are not expended beyond the acceptable limits.

$$\begin{aligned}
&\min_{\vec{r}_d}\left(\max_i\left\{P_{e,i}(\vec{r}_d)\right\}\right)\\
&s.t.\\
&P_{e,i} \le P_{e,acceptable}\,\forall i\\
&\sum_i r_{d,i} \le R_d\\
&r_{d,i} \ge 0\,\forall i
\end{aligned}$$

In the risk informed approach, an attack pathway (capability and target) is assumed to occur with some frequency. Based on this probabilistic design basis threat, the defender allocates resources to minimize risk. The defender has site-specific and target-specific defensive options - resources can be allocated amongst the four targets to reduce vulnerability and/or resources can be allocated amongst the two sites (e.g. nuclear and non-nuclear) to mitigate consequences.

$$
\begin{aligned}
&\min_{\vec{r}_d}\left(\sum_i f_i C_i(\vec{r}_d) v_i(\vec{r}_d)\right)\\
&s.t.\\
&\sum_i r_{d,i} \le R_d\\
&r_{d,i} \ge 0 \forall i
\end{aligned}
$$

The game theory approach is modeled as a two-tier defender-adversary hierarchical optimization problem.[52] In this sequential game, the defender, in full view of the adversary, allocates resources and the adversary responds to maximize gain. The defender then selects the lowest risk allocation. As before, the defender has target-specific and site-specific defensive options. In addition, the defender can increase the cost to the adversary of attacking. The adversary allocates resources to each attack strategy (combination of capability and target) to affect the frequency of attack and maximize his utility given the defenders actions. The frequency of attack is related to by the cost of conducting the attack, the annual budget the adversary allocates, and the defender's spending on efforts to increase the cost of attacking. While the adversary and defender share information sets on resource allocations, frequency of attack, consequences, and vulnerability, they place different weights on the consequences.

$$
\begin{aligned}
&\min_{r_d}\left(\max_{r_a}\left\{\begin{array}{l}\sum_i f_i(r_d,r_a) w_d(C_i) C_i(r_d) v_i(r_d) \text{ for defender}\\ \sum_i f_i(r_d,r_a) w_a(C_i) C_i(r_d) v_i(r_d) \text{ for adversary}\end{array}\right\}\right)\\
&s.t.\\
&f_i = \frac{r_{a,i}}{C_3(r_{d,i})} \forall i\\
&\sum_i r_{d,i} \le R_d\\
&\sum_i r_{a,i} \le R_a\\
&r_{d,i} \ge 0 \forall i\\
&r_{a,i} \ge 0 \forall i
\end{aligned}
$$

A direct comparison of the results is complicated by differing objective functions e.g. comparing vulnerability to a risk measure. To compare results, defender and adversary (where applicable) resource allocations are presented along with a risk profile. The results demonstrate significant variation in defensive resource allocation between Design Basis Threat, risk-informed, and game theoretic approaches given the same quantity of resources. For instance, no resources are allocated to consequence mitigation under the Design Basis Threat as the system effectiveness measure only considers vulnerability (see Figure 13).

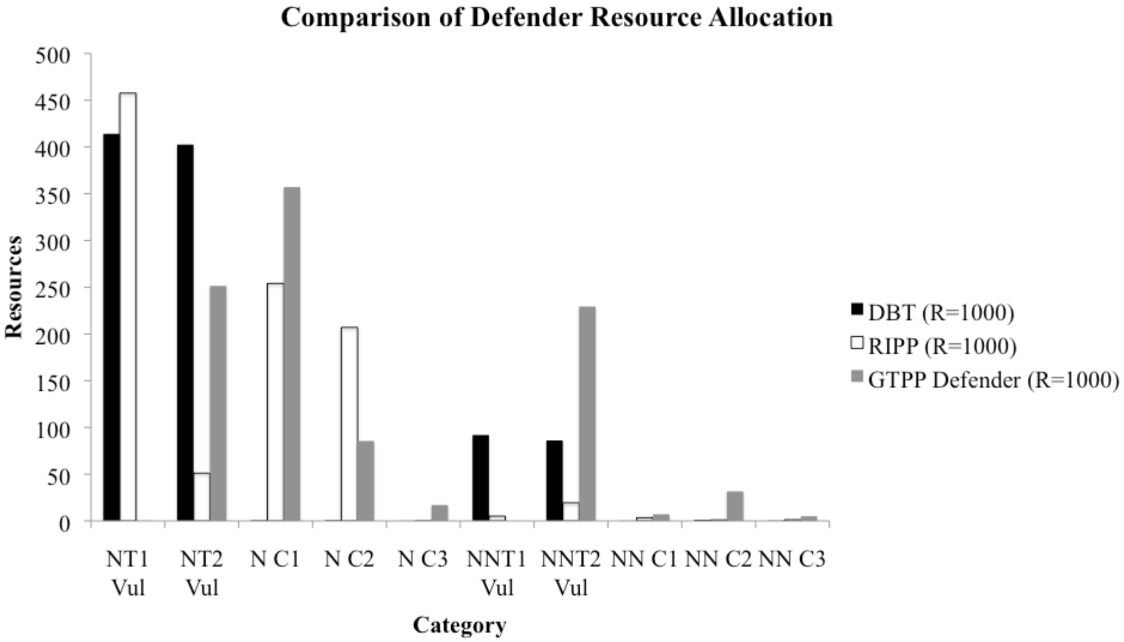
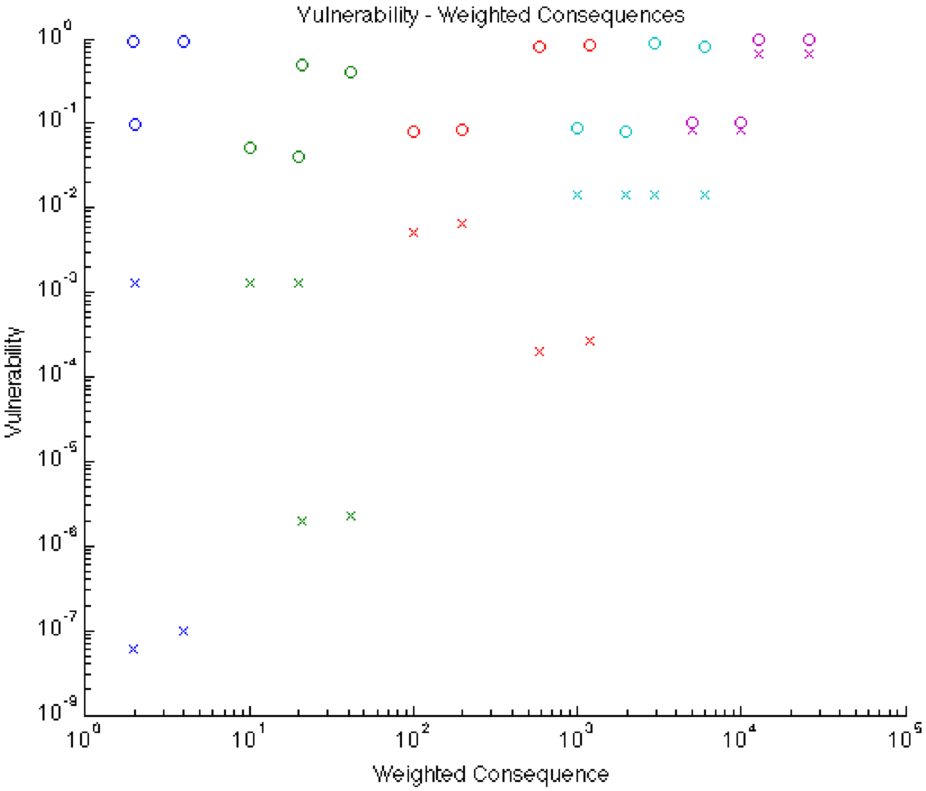


Figure 13. Comparison of defensive resource allocations between design basis threat, risk informed, and game theoretic frameworks

Vulnerabilty-consequence profiles before and after resource allocation also differ markedly. For the DBT approach, comparing the vulnerability-consequence profile before and after defensive spending shows that vulnerability decreases for all sequences with no changes in consequences. This result reflects a modeling assumption that spending to harden a target against the DBT results in additional protection against all threats. In contrast, the game theoretic approach results in shifts in both vulnerability and consequence dimensions more finely tailored to the full range of threat capabilities. (Figure 14) And in marked contrast to the risk-informed model, the frequency of attack is endogenous to the model specification i.e. frequencies of attack is an output rather than an input as in the risk informed approach. (Figure 15)



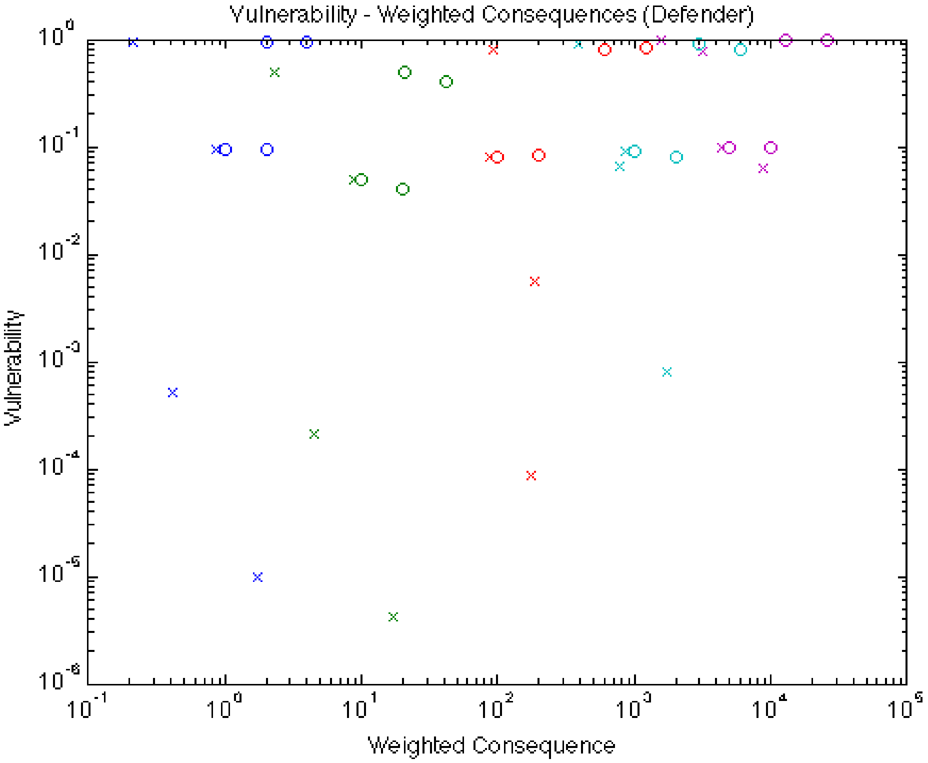


Figure 14. Vulnerability-consequence profiles form the defender's perspective between a DBT (top) and game theoretic (bottom) approaches before (o) and after (x) resource allocation

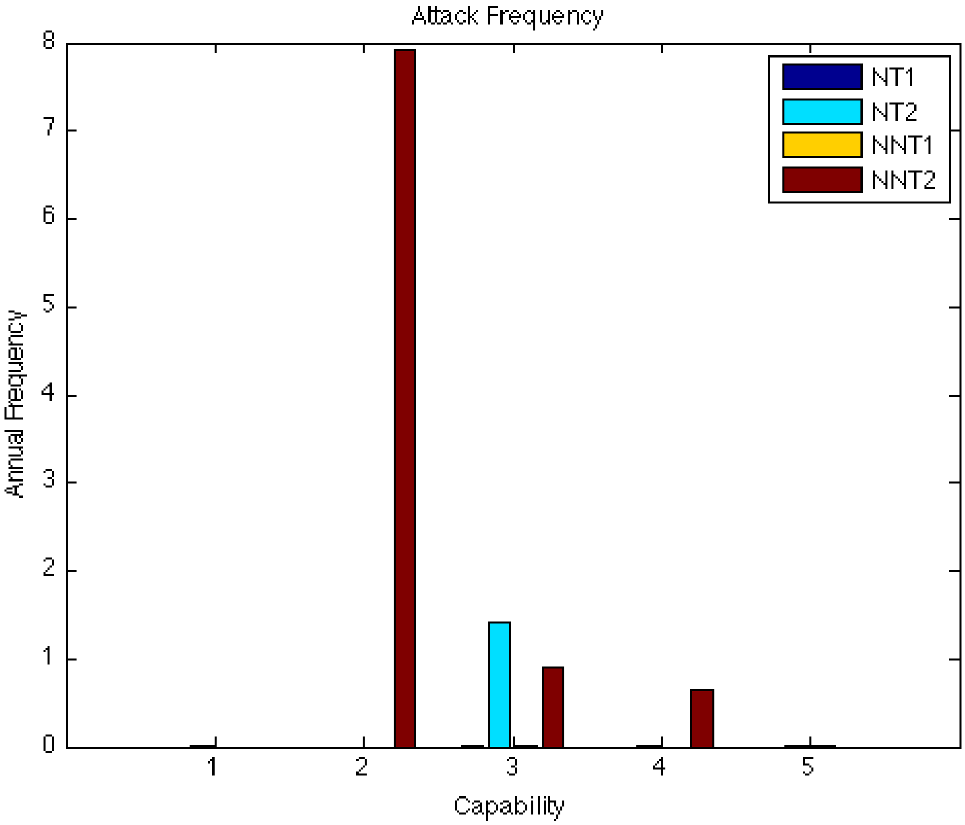


Figure 15. Attack frequency against nuclear (NTx) and non-nuclear (NNTx) targets output from the game theory model. The adversary most frequently attacks the second non-nuclear target (NNT2) with a lower capability threat (C2).

VI.D.2 Proliferation Risk

Under the strains of a global expansion of nuclear energy, nonproliferation efforts based on materials accountancy and technology control may be insufficient, particularly when faced with determined and sophisticated states. That a single uncooperative state can constitute a threat to international security suggests that the number of cooperative states and similar "glass half full" metrics are incomplete measures of the efficacy of the nonproliferation regime - a nonproliferation strategy must also be resilient to the inevitable failures of the regime.

Should materials accountancy and technology control fail to prevent a state from acquiring sensitive nuclear technologies, the nonproliferation regime does not adequately expose the intentions of the state. The question of whether the existence of nuclear infrastructure is indicative of a weapons program is difficult to answer conclusively. This ambiguity of a state's intent limits the ability to draw noncompliance judgments and forge an international consensus to respond effectively. As evidenced by the ongoing dispute with Iran, a Light Water Reactor (LWR) justifies sensitive fuel cycle facilities under various pretexts including energy security, economics, and the inalienable right to peaceful nuclear technology. While much of this rhetoric is readily discounted, Non-

Nuclear Weapons States (NNWSs), some with commercial nuclear fuel cycle aspirations, have expressed a reluctance to act in part to protect their Nonproliferation Treaty (NPT) Article IV rights to peaceful nuclear technology. Confronted with other priorities, Nuclear Weapons States (NWSs) have also been reluctant to act without being confronted with incontrovertible evidence of weapons activity.

To better cope with this deficiency, a nonproliferation strategy is proposed that minimizes the ambiguity of intent that emerges from a state's technology choices. Specifically, technological demands for dual-use nuclear fuel cycle technologies capable of producing pure streams of fissile material are minimized. The discovery of these technologies and materials in a state then provides a clearer indicator of a weapons program. The improved responsiveness of the international community that results improves resiliency to the failures of other elements of the nonproliferation regime. The advanced fuel cycles that present lower ambiguity of intent also enable a more sustainable and nondiscriminatory approach to nuclear energy. The implications of this strategy on nuclear energy research priorities contradict efforts to delay the development of advanced nuclear energy systems.

To arrive at these conclusions, the performance of the nonproliferation regime is considered under a challenging scenario of the future describing a global expansion of nuclear energy necessitating a transition to closed fuel cycles and the increasing sophistication of states. The failure of technological and institutional controls on nuclear technology and material is considered within the context of this scenario. While the likelihood of this scenario cannot be estimated with high confidence, its plausibility suggests a need for strategies that are more resilient to failure.

The global expansion of nuclear energy and the transition to closed fuel cycles will expose the limitations of the existing nonproliferation regime. At the institutional level, export control regimes and Multilateral Nuclear Arrangements (MNAs) limit the number of states with access to nuclear technology.[53] More technologically oriented measures provide timely detection of the theft and diversion of material to increase the proliferation resistance of nuclear energy systems.[54,55]

Nonproliferation strategies dependent on the success of technology control and materials accountancy will be ineffective against sophisticated states determined to acquire nuclear weapons. From the beginning of the Atomic Age, many have recognized that nuclear technology will not remain the exclusive domain of the NWSs. This trend will continue. Illicit nuclear trafficking networks have already reduced barriers to uranium enrichment. And despite efforts to shut down these networks, sensitive fuel cycle technologies will only become more accessible to states—information on various methods of enrichment and fissile material separation is available and can be developed indigenously.

Renewed efforts to implement MNAs to rein in the diffusion of sensitive nuclear technology may not succeed. The feasibility of MNAs are questionable given perceptions of discrimination and difficulties with siting facilities with the necessary economic, political, and technological diversity to provide assurances of supply. Should these obstacles be overcome, the sustainability of MNAs is threatened by shifts in political relationships that can occur on timescales shorter than the lifetimes of nuclear infrastructure. While many states may nonetheless choose to participate in such arrangements, MNAs do not fully address a state's "inalienable right" to peaceful nuclear technology. Iran's rejection of a proposal for multinational control of an enrichment facility located in Russia is an example of such a failure that limits the resiliency of this approach.

Turning to controls more technological in nature, increasing the proliferation resistance of nuclear energy systems such that they are, "the least desirable route" to acquire fissile material decreases the coupling between commercial nuclear technologies and nuclear weapons. To this end, various intrinsic and extrinsic measures to guard against the theft and diversion of fissile have been evaluated. In particular, a greater reliance on intrinsic features to enhance proliferation resistance has been pursued to better tolerate failure of extrinsic controls such as international safeguards.[56] Consequently, various strategies are available to provide timely warning of the theft and diversion of fissile material from nuclear energy systems such that,

> "…the diversion risks encountered in the various stages of the [Fast Breeder Reactor] FBR fuel cycle present no greater difficulties than in the case of the LWR with the U-Pu cycle or even in the case of the once-through cycle…"[57]

These measures, however, do little against the threat of clandestine programs nor do they mitigate the consequences of breakout, particularly when faced with determined and sophisticated states. Knowledge and experience gained from operating a nuclear system, including "proliferation resistant" reprocessing technologies relying on intrinsic barriers (e.g. isotopics, radiation, decay heat), can be applied to a clandestine effort to produce fissile material. In addition to the theft or diversion of material, the possibility of breakout will remain regardless of reactor option or fuel-supplier arrangement. A state with a nuclear reactor will possess enough fissile material for nuclear weapons.

Ultimately, a clearly superior nuclear energy system is difficult to identify in terms of proliferation resistance. While methods for evaluating proliferation resistance are necessary to consistently evaluate nuclear energy systems, the inherent subjectivity of these assessments limits the ability to select a nuclear technology. The International Nuclear Fuel Cycle Evaluation recognizes the subjectivity of proliferation resistance assessments by noting,

> "The extent to which the possibility of misuse vary between fuel cycles is not easy to judge. Taking into account the qualitative nature of the evaluation, the different stages of development of the various fuel cycles, the extent to which complete fuel cycles are present within individual countries and the evolutionary nature of the technical safeguards and institutional improvements that may be implemented, no single judgment

> about the risk of diversion from the different fuel cycles can be made that is valid both now and for the future."

Increasing the responsiveness of the international community may better cope with failures of the nonproliferation regime and offer an additional criterion for technology decisions. In their report to the Director General of the International Atomic Energy Agency (IAEA), the expert panel on MNAs notes that,

> "…enhanced safeguards, MNAs, or new undertakings by States will not serve their full purpose if the international community does not respond with determination to serious cases of non-compliance…."

While a number of institutional enhancements may improve the responsiveness of the international community to proliferation threats, technological measures have received less attention.

To enhance responsiveness, lower ambiguity nuclear energy systems are defined as technologies that better differentiate a state's intent based on the state's observable technology choices. More concretely, low ambiguity nuclear energy systems limit a state's ability to justify sensitive fuel cycle technologies capable of producing pure streams of weapons-usable fissile material (uranium enrichment and plutonium/U233 separation) to support a commercial nuclear power program under the pretext of economics, energy security, Nonproliferation Treaty Article IV rights, etc. Uranium enrichment and plutonium separation is of particular concern as they are essential for the production of fissile material usable in weapons and have been demonstrated by empirical social science research to be the most significant contributors to the acquisition of nuclear weapons.[58]

Against this definition, LWRs are an example of a higher ambiguity nuclear energy system. These reactors enable states to justify sensitive nuclear fuel cycle technologies under the guise of a commercial program. The presence of uranium enrichment or plutonium separation is an ambiguous indicator of a weapons program as these facilities can conceivably produce fissile material for a commercial nuclear reactor or for a nuclear weapon. Uranium enrichment can be justified to secure access to enrichment services for a reactor requiring frequent refueling. Plutonium separation can also be justified to increase sustainability by reducing waste and increasing resource utilization.

In contrast, a Fast Breeder Reactor (FBR) coupled to Proliferation Resistant Reprocessing (PRR), pyroprocessing in particular, is an example of a lower ambiguity system. By eliminating technological requirements for enriched uranium or separated plutonium, evidence of enrichment or plutonium separation activities becomes clearer indicators of the intent to pursue nuclear weapons. To avoid uranium enrichment, an initial supply of fissile material, possibly provided by another state, would form the basis for a sustainable commercial nuclear enterprise. By breeding fissile material from this initial supply, a FBR with PRR can operate without enriching uranium or separating plutonium.

On the back end of the cycle, PRR is the enabling technology whose key feature is the absence of a pure stream of fissile material directly usable in a nuclear weapon. Modifications to these systems to separate fissile material should be readily observable via safeguards and present a clear signal of intent. Some PRR systems, such as pyroprocessing, pose less ambiguity than others given inherent technological barriers that largely preclude reconfiguring the systems for fissile material separation - aqueous separation processes are more readily reconfigured. While a state could separate fissile material from the output of PRR, the chemical separation of fissile material is a common threat across all fuel cycle options.

On the front end, uranium enrichment is unnecessary provided that a sufficient inventory of fissile material is available to support refueling and capacity expansion. However, additional supplies of fissile material will be necessary if the demand for nuclear energy increases at a rate that outstrips the ability to breed. Should this be the case, plutonium produced in Heavy Water Reactors (HWRs) fueled with natural uranium is a source of fissile material that avoids uranium enrichment.

Such a system does not entirely eliminate ambiguity of intent. The economic argument is one of the few remaining sources of ambiguity that presents a pretext for possessing sensitive fuel cycle technologies. For instance, plutonium separation may be substituted for PRR at lower cost and enriching uranium may be more favorable in comparison to plutonium production in a HWR. In any event, closed fuel cycles may not be economically competitive with once-through strategies until uranium prices increase.

Technological measures enhancing the responsiveness of the international community present largely unexplored opportunities to manage proliferation risk. Should the nonproliferation regime fail to prevent a state from acquiring sensitive nuclear technologies, the viability of lower ambiguity nuclear energy systems enable the international community to draw more conclusive judgments of the intent of a state’s nuclear program. To this end, a fuel cycle composed of Fast Breeder Reactors, Heavy Water Reactors, and Proliferation Resistant Reprocessing (FBR-HWR-PRR) is just one example of a nuclear energy system that reduces ambiguity of intent by eliminating technological requirements for uranium enrichment and fissile material separation. A low ambiguity approach, however, does not obviate the need for existing nonproliferation efforts. Materials accountancy and technology control will be desirable elements of a comprehensive nonproliferation strategy. Increasing responsiveness rounds out the strategy by offering a mechanism to cope with the inevitable failures brought about by a global expansion of nuclear energy and the increasing technological sophistication of states.

A nonproliferation objective that minimizes the likelihood of theft and diversion of fissile material appears unlikely to conclusively differentiate between nuclear energy systems. Various combinations of intrinsic and extrinsic features can be expected to provide similar levels of protection against theft and diversion across most nuclear energy systems. A nonproliferation objective that increases the responsiveness of the international community by minimizing demand for sensitive nuclear fuel cycle facilities (i.e. uranium enrichment and plutonium separation, particularly aqueous processes) has been proposed to assess its impacts on the efficient solutions.

VII. CONCLUSIONS

In this Section, we have described a robust decision-making framework that aims to provide quantitative top-down feedback to decision-makers and system designers. A multidisciplinary and multiobjective robust decision-making framework is proposed to analyze a dynamic, but simplified nuclear energy system model with respect to the Generation IV criteria. Multiobjective evolutionary algorithms are assessed with respect to their ability to solve complex models featuring many degrees of freedom that challenge gradient-based solvers. Methods for assessing physical protection are assessed, including game theoretic approaches that incorporate the strategic behavior of adversaries. With respect to proliferation resistance, demand-side strategies that permit a more resilient response to proliferation challenges is proposed that account for limitations in technical assessments of proliferation resistance and institutional controls on technology.

REFERENCES

1. NUCLEAR ENERGY RESEARCH ADVISORY COMMITTEE, "Generation IV Roadmap Fuel Cycle Assessment Report," Technical Roadmap Report, sumitted to the Generation IV International Forum, Demember, 2002.
2. S. PIET, et al, “Fuel Cycle Scenario Definition, Evaluation, and Trade-offs,” INL/EXT-06-11683, August 2006.
3. R. LEMPERT, S. POPPER and S. BANKES, “Confronting Surprise,” *Social Science Computer Review*, 2002.
4. NUCLEAR ENERGY RESEARCH ADVISORY COMMITTEE.
5. S. PIET
6. MIT. *The Future of Nuclear Power*. Cambridge, MA: Massachusetts Institute of Technology, 2003
7. R. LEMPERT, S. POPPER and S. BANKES, “Confronting Surprise.”
8. R. LEMPERT, S. POPPER and S. BANKES, “A General, Analytic Method for Generating Robust Strategies and Narrative Scenarios,” *Management Science*, April 2006.
9. S. PIET
10. S. J. KLINE, “Conceptual Foundation for Multidisciplinary Thinking,” Stanford University Press, Stanford, 1995.
11. KYDES, SHAW, and MCDONALD, “Beyond the Horizon: Recent Directions in Long-Term Energy Modeling,” *Energy*, 1995
12. K. RIAHI, A. GRUBLER and N. NAKICENOVIC. "Scenarios of Long-Term Socio-Economics and Environmental Development Under Climate Stabilization." *Technological Forecasting and Social Change*, 2007.
13. IIASA, *Greenhouse Gas Initiative Database*, 2006, http://www.iiasa.ac.at/web-apps/ggi/GgiDb/ (accessed February 2008).

14. IIASA/WEC. *IIASA/WEC Global Energy Perspectives.* 1998. http://www.iiasa.ac.at/cgi-bin/ecs/book_dyn/bookcnt.py (accessed February 2008).
15. KYDES, SHAW, and MCDONALD
16. R. D. LUCE and H. RAIFFA, *Games and Decisions: Introduction and Critical Survey*. Dover Publications, Inc., New York, 1957.
17. R. LEMPERT, S. POPPER and S. BANKES, “A General, Analytic Method for Generating Robust Strategies and Narrative Scenarios.”
18. J. ROSENHEAD, M. ELTON and S. GUPTA, "Robustness and Optimality as Criteria for Strategic Decisions," *Operational Research Quarterly*, 1972.
19. Y. BEN-HAIM, *Information Gap Decision Theory: Decisions Under Severe Uncertainty*, Elsevier Ltd., San Francisco, (2nd Edition) 2006.
20. R. LEMPERT, S. POPPER and S. BANKES, *Shaping the Next 100 Years: New Methods for Quantitative, Long-Term Policy Analysis*, RAND, Santa Monica, RAND, 2003.
21. S. POPPER, “Robust Decision Methodology for Reasoning Under Deep Uncertainty,” *World Future Society Professional Forum*, Chicago, August 2005.
22. R. LEMPERT, S. POPPER and S. BANKES, “A General, Analytic Method for Generating Robust Strategies and Narrative Scenarios.”
23. H. KHALIL, et al., “Integration of Safety and Reliability with Proliferation Resistance and Physical Protection for Generation IV Nuclear Energy Systems,” to appear in *Proceedings of Global 2009*, Paris, France, 2009.
24. D. BELL, R. KEENEY and H. RAIFFA, *Conflicting Objectives in Decisions,* International Institute for Applied Systems Analysis, 1977.
25. K. DEB, *Multi-Objective Optimization Using Evolutionary Algorithms*, John Wiley and Sons, Ltd., New York, 2001.
26. K. C. TAN, E. F. KHOR, and T. H. LEE, *Multiobjective Evolutionary Algorithms and Applications,”* Springer-Verlag London Limited, London, 2005.
27. K. DEB, et al. “A Fast Elitist Multiobjective Genetic Algorithm: NSGA-II,” *IEEE Transactions on Evolutionary Computation,* April 2002.
28. K. DEB and D. K. SAXENA, “On Finding Pareto Optimal Solutions Through Dimensionality Reduction for Certain Large-Dimensional Multi-Objective Optimization Problems,” Kanpur Genetic Algorithms Laboratory, 2005
29. D. K. SAXENA and K. DEB, “Non-linear Dimensionality Reduction Procedures for Certain Large-Dimensional Multi-Objective Optimization Problems: Employing Correntropy and a Novel Maximum Variance Unfolding,” Kanpur Genetic Algorithms Laboratory, 2007.
30. J. AHN, “Deterministic Assessment for Environmental Impact of Yucca Mountain Repository Measures by Radiotoxicity,” *Journal of Nuclear Science and Technology*, 2007.
31. E. BOUVIER, *Environmental Impact Assessment of Nuclear Fuel Cycles*, Diss. University of California, Berkeley, 2007.
32. OECD NUCLEAR ENERGY AGENCY AND THE INTERNATIONAL ATOMIC ENERGY AGENCY, *Uranium 2005: Resources, Production, and Demand*, 2005.
33. M. BUNN, S. FETTER, J. HOLDREN, and B. VAN DER ZWAAN, *The Economics of Reprocessing vs. Direct Disposal of Spent Nuclear Fuel*, Harvard University, December 2003.

34. OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT, "Nuclear Waste Fund Fee Adequcy: An Assessment," sumitted to the U.S. Department of Energy, Demember, May 2001.
35. ECONOMICS MODELING WORKING GROUP, "Cost Estimating Guidelines for Generation IV Nuclear Energy Systems," submitted to the Generation IV International Forum, November 2006.
36. CONGRESSIONAL BUDGET OFFICE, “Nuclear Power’s Role in Generating Electricity,” 2008.
37. N. HULTMAN, J. KOOMEY, and D. KAMMEN, “What History Can Teach Us About the Future Costs of U.S. Nuclear Power,” *Environmental Science and Technology*, April 2007.
38. L. KIM AND P. PETERSON, “Future Roles for Nuclear Energy,” *Physics of Sustainable Energy, Using Energy Efficiently and Producing it Renewably*, American Institute of Physics, 2008.
39. B. BIRINGER, R. MATALUCCI, and S. O’CONNOR, *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*, John Wiley and Sons, 2007.
40. M. GARCIA, *The Design and Evaluation of Physical Protection Systems,* Butterworth-Heinemann, 2001.
41. L. COX, “Some Limitations of ‘Risk=Threat x Vulnerability x Consequence’ for Risk Analysis of Terrorist Attacks,” *Risk Analysis*, 2008.
42. B. GARRICK, et al, “Confronting the Risks of Terrorism: Making the Right Decisions,” *Reliability Engineering and System Safety*, 86 (2004): 129-176.
43. R. POWELL, “Defending Against Terrorist Attacks with Limited Resources,” *American Political Science Review*, August 2007.
44. V. BIER, A. NAGRAJ, and V. ABHICHANDANI, “Protection of Simple Series and Parallel Systems with Components of Different Values,” *Reliability Engineering and System Safety*, 2005.
45. L. COX
46. J. VON NEUMANN AND O. MORGENSTERN, *Theory of Games and Economics Behavior*, Princeton University Press, Princeton, 1944.
47. R. POWELL
48. R. D. LUCE and H. RAIFFA
49. W. E. KASTENBERG, “Development of Risk-Based and Technology-Independent Safety Criteria for Generation IV Systems,” *Proceedings of the International Topical Meeting on Probabilistic Safety Assessment*, San Francisco, CA, 11-15 Sep, 2005.
50. M. GARCIA
51. PROLIFERATION RESISTANCE AND PHYSICAL PROTECTION EVALUATION METHODOLOGY EXPERT GROUP. *Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy* Systems *Revision 5.* Submitted to the Generation IV International Forum, September 30, 2006.
52. G. BROWN, M. CARLYLE, J. SALMERON, and K. WOOD, “Defending Critical Infrastructure,” *Interfaces*, November-December 2006, pp. 530-544.
53. INTERNATIONAL ATOMIC ENERGY AGENCY, *Multilateral Approaches to the Nuclear Fuel Cycle: Expert Group Report Submitted to the Director General of the*

International Atomic Energy Agency, International Atomic Energy Agency, Vienna, 2005.

54. PROLIFERATION RESISTANCE AND PHYSICAL PROTECTION EVALUATION METHODOLOGY EXPERT GROUP
55. NUCLEAR ENERGY RESEARCH ADVISORY COMMITTEE
56. H. FEIVESON, *The Search for Proliferation-Resistant Nuclear Power,* Federation of American Scientists, October 2001. http://www.fas.org/faspir/2001/v54n5/nuclear.htm (accessed March 13, 2008).
57. INTERNATIONAL ATOMIC ENERGY AGENCY, *International Nuclear Fuel Cycle Evaluation.* International Atomic Energy Agency, Vienna, 1980.
58. M. KROENIG *Importing the Bomb: Sensitive Nuclear Assistance and Nuclear Proliferation,* Cambridge: Harvard University, 2008.