INL/RPT-22-68669

Light Water Reactor Sustainability Program

Risk-Informed Initiating Events and Accident Response

ASSESSMENT OF TIMING PARAMETERS USED IN RISK ASSESSMENTS TO IDENTIFY OPPORTUNITIES FOR SAFETY MARGIN INCREASE

Svetlana Lawrence[1], N. Prasad Kadambi[2]

[1]Idaho National Laboratory, [2] Principal, Kadambi Engineering Consultants

08/30/2022

DOE Office of Nuclear Energy

INL/RPT-22-68669

Light Water Reactor Sustainability Program

Risk-Informed Initiating Events and Accident Response

ASSESSMENT OF TIMING PARAMETERS USED IN RISK ASSESSMENTS TO IDENTIFY OPPORTUNITIES FOR SAFETY MARGIN INCREASE

Svetlana Lawrence[1], N. Prasad Kadambi[2]

[1]Idaho National Laboratory, [2] Principal, Kadambi Engineering Consultants

08/30/2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov/lwrs

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ABSTRACT

Emerging nuclear technologies and advanced reactor developments have brought proposed changes to the regulatory framework which can be leveraged to improve safety implementation and regulatory oversight processes at existing operating nuclear power plants. Specifically, opportunities exist to make plants' regulatory compliance processes more efficient. This can be done by decreasing reliance on purely deterministic and prescriptive approaches and expansion of the use of risk-informed and performance-based approaches to demonstrate reactor safety while achieving economic gains and efficiencies. In this report, we researched possibilities of economic benefits potentially available from the application of concepts associated with a modernized regulatory framework developed for advanced reactors to the existing light water reactors. We used timing factors to demonstrate the complexity of the existing risk assessments and described how these complexities affect regulatory compliance activities at the plants. We also investigated regulatory framework for both existing and new reactors and provided an overview of potential improvements. Lastly, we evaluated various areas of existing plant operations where modernization of compliance activities can offer substantial benefits.

CONTENTS

FIGURES

ACRONYMS

AMP	Aging management plan
ANS	American Nuclear Society
AS	Accident Sequence
ASME	American Society of Mechanical Engineers
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
DBA	Design Basis Accidents
DBE	Design basis events
DI&C	Digital instrumentation and control
DID	Defense-in-depth
DOE	Department of Energy
EDG	Emergency diesel generator
EPRI	Electrical Power Research Institute
FSAR	Final Safety Analysis Report
IE	Initiating Events
INL	Idaho National laboratory
IPA	Integrated Plant Assessment
ITAAC	Inspection, Tests, Analysis and Acceptance Criteria
HEP	Human error probability
HFE	Human failure events
HRA	Human Reliability Analysis
LBE	Licensing Basis Event
LERF	Large Early Release Frequency
LMP	Licensing Modernization Project
LOCA	Loss of coolant accident
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability
MBSE	Model-based systems engineering
MSPI	Mitigating System Performance Index
NASA	National Aeronautics and Space Administration
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Analysis
RAPT	Reasonable Assurance of Protection Time
RCS	Reactor coolant system
RG	Regulatory Guide
RI-ISI	Risk-Informed Inservice Inspection
RIM	Reliability and Integrity Management
RIPB	Risk-informed and performance-based
ROP	Reactor Oversight Process
S&MS	Safety and mission success
SC	Success Criteria
SSCs	Systems structures and components

TEPA	Top Event Prevention Analysis
TH	Thermal-hydraulic

1. INTRODUCTION

Safety is a key aspect to operation of nuclear power plants (NPPs). The United States (U.S.) commercial nuclear industry is facing a strong challenge to maintain regulatory required levels of safety while ensuring economic competitiveness in current and future electricity markets. The fact that other electricity-generating industries do not have a comparable level of expenses dedicated to meeting safety requirements underlines the extreme importance of efficiency in all facets of regulatory compliance. While the need for strong safety regulation is undeniable, the nuclear industry has come to the point where overly conservative regulations threaten the very existence of commercial power plants due to the costs associated with them. As such, dedicated efforts are being made to modernize the regulatory framework with the goal to make safety assurance more cost-effective while maintaining high levels of safety.

To understand the unique challenges posed by the safety assurance framework, it is important to understand its history. The original requirements for nuclear safety were developed decades ago at the onset of commercial nuclear power in the 1950s when the U.S. Congress established the Atomic Energy Act of 1954 and assigned the Atomic Energy Commission to the functions of both encouraging the use of nuclear power and regulating its safety. The Nuclear Regulatory Commission (NRC), established in 1974 to focus solely on safety, developed many of the initial regulations using deterministic strategies that were based on at-that-time state of knowledge, experience, test results, and expert judgement. The regulations were intentionally conservative to ensure that safety margins were sufficient to overcome aleatory and epistemic uncertainties associated with physical phenomena during postulated reactor events. Those scenarios were not expected to occur during the lifetime of a reactor unit but were considered possible in an operating fleet. The conditions associated with such scenarios were called accidents. A subset of such accidents was designated as Design Basis Accidents (DBAs) because the conditions were used to represent challenges that a design is constructed to withstand and do so with satisfactory margin.

Since the early years of commercial nuclear power, significant technological and scientific advances have been made and substantial information has been developed allowing much better understanding of behavior of nuclear reactors and supporting systems during normal and abnormal plant operating conditions. Also, there has been increased use of quantitative methods for assessment of risk (in addition to the mostly qualitative assessments used), which became possible with issuance of the WASH-1400 Reactor Safety Study [1]. This was followed by more advanced developments in Probabilistic Risk Assessment (PRA) as a mature discipline.

These advancements allowed modernization of regulatory processes especially since the issuance of the NRC's Policy Statement, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" in 1995 [2]. Industry efforts made as part of the Delivering Nuclear Promise initiative, which focused on addressing challenges faced by NPPs, demonstrated significant economic benefits to using risk-informed approaches instead of or in addition to prevailing deterministic approaches. While implementation of risk-informed approaches has shown great success, much more can be done to support the goal of making safety implementation as efficient as possible.

This project explores opportunities to benefit economically by optimizing safety implementation practices using the NRC's documented policies to date. A key driver for the project resulted from the simple observation of the complexity associated with a single parameter used in various areas of safety assessments, namely, time. Time is a very important input essential to every aspect of any safety analysis. Risk practitioners can attest that time is one of the most complicated and uncertain input values, which is the reason that it is associated with many assumptions. Most of the timing assumptions are intentionally overly conservative to make the parameters applicable to multiple scenarios so as to make them bounding. The idea was to systematically evaluate areas of risk assessments that rely on timing parameters, consider the assumptions being made, and use the results to identify areas with greatest potential to realize benefits by reducing conservatisms. This research led to significant insights, specifically, that safety implementation practices need to be modernized in order to achieve desirable benefits in terms of efficiencies and economic gains.

The report starts with exploration of the use of timing parameters in risk assessments typically performed for NPPs and progresses to looking into opportunities for improvements, specifically areas that could benefit from reducing conservatisms associated with time inputs. Next, broader opportunities are discussed for improvements of safety margins, gaining flexibility in plant operations, and realizing economic benefits are explored and specific areas with potential cost savings.

2. TIMING PARAMETERS IN RISK ASSESSMENTS

Time is a very important parameter in risk assessments, regardless of what method or tools are used. The following sections discuss ways of timing usage in various types of risk assessment.

2.1 Timing in PRA Models

Each event sequence in PRA involves a timing parameter, such as time to initiate mitigation, time to restore power, time to core damage, time to an early release, time to deploy equipment, etc. Traditional PRA models incorporate timing insights only implicitly via typically overly conservative success criteria, boundary conditions, and assumptions. The conservatism is intentional to generate bounding scenario conditions to simplify risk analyses. Traditional PRAs do not have the capability to explicitly include time as a variable because a PRA is a static representation of a plant configuration with risk metrics informed by historical performance (e.g., equipment failure rates). However, time is a critical parameter and understanding the time implication in models, data, and tools is important to reflect realism and remove conservatisms as appropriate.

PRA models are developed according to a set of requirements outlined in the PRA standard developed in collaboration by the American Society of Mechanical Engineers (ASME) Board on Nuclear Codes and Standards and the American Nuclear Society (ANS) Standards Board, with the latest revision issued in May 2022 [3]. There are eight technical elements:

(a) Initiating Event Analysis (IE)
(b) Accident Sequence Analysis (AS)
(c) Success Criteria (SC)
(d) Systems Analysis (SY)
(e) Human Reliability Analysis (HR)
(f) Data Analysis (DA)
(g) Quantification (QU)
(h) Large Early Release Frequency (LERF) Analysis (LE)

The use of timing parameters in each technical element is discussed in the following subsections.

For brevity, the discussion is focused on internal events for an at-power PRA. The discussion would be much more complex and broader if other PRAs are considered, such as internal flood, fire, seismic, high winds, and external flood PRAs. It should be noted, that while timing parameters are extremely important for the internal events PRA, they are even more significant for external hazard PRAs.

2.1.1 Initiating Events Analysis

The goal of the IE analysis is to identify, quantify, and document events that could lead to reactor core damage. Some IEs are significantly affected by time which is most relevant to external hazards IEs. For example, flooding events, both internal and external, are categorized by how fast a given scenario progresses to understand plant damage that occurs instantaneously or delayed in time, latter providing an opportunity for plant operators to implement mitigating strategies. Other IEs are not categorized by time and typically assumed to occur instantaneously. Examples are loss of coolant accident (LOCA) or loss of offsite power.

The assumptions for time are intentionally conservative for both types of IEs discussed above. For the external events, a time estimate is possible (e.g., a tsunami reaching the plant after a warning is issued), but these estimates are usually considered part of AS or SC analyses. Generally, an IE is assumed to occur instantaneously.

The assumption of an instant IE is valid and justified in most cases. However, in some other instances this assumption is extremely conservative. A prominent example is a large-break LOCA. This IE assumes an instantaneous double-ended break of a pipe in the reactor coolant system (RCS) occurring at the lowest point of the system (i.e., worst location). Such break leads to an instantaneous RCS depressurization and loss of coolant inventory, followed by very quick uncovery of the reactor core with core damage occurring within minutes if not mitigated. The assumption that a pipe can unexpectedly break in half in an instant is extremely unrealistic especially given the rigor of RCS condition monitoring both continuously while in service and periodically via regular inspections. Normally, a pipe failure starts with a small imperfection that grows into a small crack that eventually progresses into a break. An imperfection or a crack would be associated with leakage of the material. The leak in the RCS, even a small one, can be detected by multiple means. First, RCS volume is constantly monitored, and excess leakage is investigated. The RCS contains radioactive water, and the leak would be associated with increased level of radioactivity in the surrounding area which will be picked up by radiation monitoring sensors. Lastly, the condition of RCS pressure boundary components is subject to multiple visual and nondestructive examinations. In summary, the principal assumption for the large-break LOCA IE is unjustifiably conservative.

2.1.2 Accident Sequence Analysis

The objective of the AS analysis is to ensure that the response of the plant's systems and operators to an initiating event is represented in the core damage frequency (CDF) assessment in such a way that any plant-specific scenarios potentially leading to core damage are identified and well-described, and plant system dependencies are represented [3]. The AS analyses use event trees to document accident progression with branches representing success (e.g., safe shutdown) or failure (e.g., core damage) paths with decision points representing plant mitigating strategies. An example of an event tree is shown in Figure 2-1 [4].

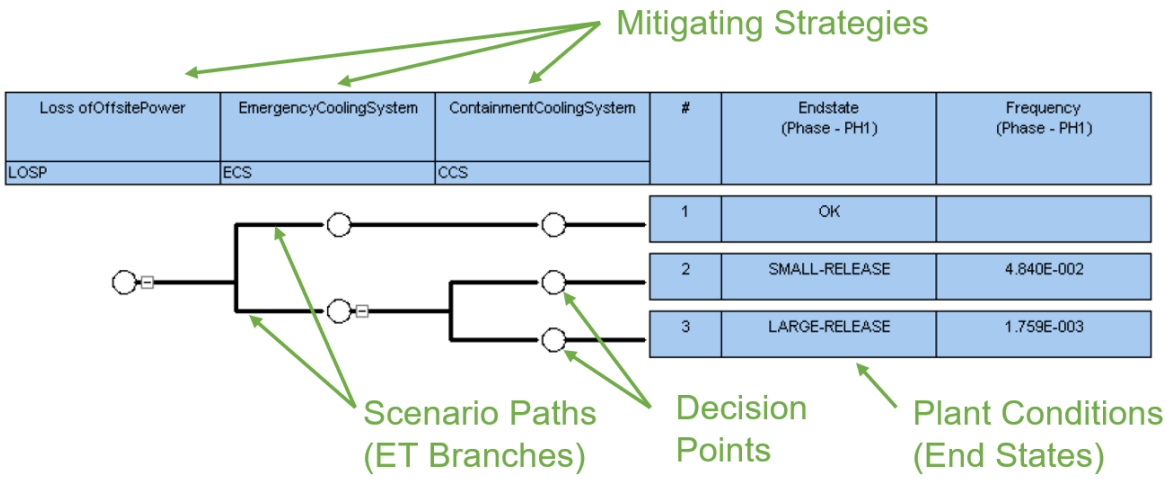

Figure 2-1. Example event tree

Time in AS analyses is considered only in terms of a sequence of events through a scenario progression (i.e., which mitigating strategy is being initiated at what point during the scenario based on other strategies success or failure). As such, there is no time estimation involved in the AS analyses.

2.1.3 Success Criteria Analysis

The success criteria analysis is the most influential technical element of the PRA in terms of the effect on the overall results, such as CDF and LERF. It is also where many assumptions are made. The objective of the success criteria analysis is to define the plant-specific measures of success and failure that support other technical elements of the PRA [3]. The success criteria analysis is performed in such a way that:

1) The success criteria are defined for key safety functions; supporting systems structures and components (SSCs); and operator actions necessary to support accident sequence development

2) The supporting technical bases are realistic; represent the as-built, as-operated plant; and are consistent with the initiating events and accident sequence technical elements of the PRA.

The two high-level requirements for the success criteria analysis are listed below [3] since they are essential to understanding the success criteria objectives and timing parameters that are part of success criteria establishment:

- The overall success criteria for the PRA shall be consistent with the features, procedures, and operating philosophy of the plant. This includes defining core damage, establishing accident sequence mission times, and ensuring that mitigating systems shared between units are addressed.
- The thermal-hydraulic, structural, and other supporting engineering bases shall be capable of providing success criteria and event timing sufficient for quantification of CDF and determination of the relative impact of success criteria on SSCs and human actions.

The success criteria are first developed at the functional level by identifying the key safety functions needed to mitigate an initiating event. The key safety functions for light water reactors (LWRs), also referred to as basic safety functions, are listed below:

- Reactivity control
- Reactor pressure control
- Reactor core inventory control
- Decay heat removal
- Containment integrity protection.

Next, success criteria at the system level are determined for systems required to support the key safety functions. Thermal-hydraulic (TH) analyses are used to determine success criteria for PRA accident scenarios, including success criteria for systems performance and operator actions.

The TH analyses are performed using well-established models representing the behavior of the reactor core and reactor core cooling system under a given accident scenario. The mitigating system physical capabilities (i.e., system design characteristics) are used as an input to TH analyses. For example, in the case of a LOCA, physical performance characteristics for the safety injection system such as pressure, flow rate, time to initiate, etc., are input in the TH model. The system and component performance criteria used as input into TH analyses are defined by system's specifications and verified by routine testing conducted as part of the compliance processes. A couple of examples of performance criteria are shown below:

- Example component performance success criteria: Each pump must be capable of delivering water into the RCS with the *flow rate of 350 gallons per minute (gpm)* at a *pressure of 1250 pounds per square inch (psi)*; the High Pressure Safety Injection (HPSI) pump motor must accelerate the pump to a full speed within *10 seconds* from the motor start.

In the example above, parameters such as *350 gpm*, *1250 psi*, and *10 seconds*, are used as inputs in TH analyses to determine accident scenario timing parameters (e.g., time to core uncovery, time to core damage). These parameters also become **the requirements** for the system performance assurance. For example, HPSI pumps will be periodically tested and if the flow rate at 1250 psi is 345 gpm instead of required 350 gpm, the pump will be considered failed even though the component is still operable with the performance only marginally degraded.

The timing parameters determined from TH simulations (e.g., time to core damage) are used to define success criteria for the initiation of mitigating strategies. Example success criteria for an inventory control function during a LOCA scenario are presented below:

- Example system functional criteria: To prevent core uncovery during a small LOCA, the HPSI flow must be initiated within 15 minutes from the reactor trip; to prevent core damage, the HPSI flow must be initiated within 30 minutes from the reactor trip.

The time values from the system functional criteria (i.e., *15 and 30 minutes* from the example above), are used as inputs to the HRA discussed later.

The PRA success criteria do not explicitly account for timing parameters. Instead, PRA success criteria are defined in terms of minimum required equipment necessary to perform the function, which is also established using TH analyses, below is an example:

- Example PRA success criterion: To supplement the reactor core inventory lost during a small LOCA, one of three HPSI pumps must inject water from the refueling water storage tank into two of four RCS cold legs.

The set of minimum required equipment is dependent on the postulated accident scenario, meaning that accident sequence and success criteria technical elements of the PRA are highly dependent.

2.1.4 Systems Analysis

The objective of the systems analysis element is to identify the causes of failure for each plant system represented in the IE and AS analyses in such a way that independent failures, system unavailability, and common-cause failures are identified and properly modeled [3]. This element of PRA is very important in terms of proper identification of system internal and external dependencies.

This task includes timing factors in a form of a mission time, which is the parameter describing how long a given system or a component is expected to operate to satisfy a given function. For PRAs, the mission time is usually 24 hours since the onset of an accident scenario. The reason for 24-hour time is because a reactor that has been cooling down for 24 hours presents much lesser danger to public health and the environment compared to an at-power reactor. The 24-hour time window also gives time to enact emergency response such as evacuation of residents and deployment of special external organizations. While in most cases 24-hour mission time is adequate, there are exceptions especially with external hazards such as flooding or seismic events. The Fukushima-Daiichi accident lasted much longer than 24 hours due to various factors. The mission time extension beyond 24 hours should certainly be the consideration in the external hazard PRAs.

In some cases, system- or function-specific mission time is needed. For example, a running emergency diesel generator (EDG) relies on a constant diesel fuel supply. When the fuel supply tank is low, a fuel transfer pump turns on to deliver fuel from the larger fuel storage tank. In this case, the mission time for a fuel transfer pump will be defined both by the number of demands to refill the supply tank and on equipment physical characteristics such as EDG fuel consumption rate, EDG mission time, and volume of the fuel supply tank.

While scenario-specific mission times different from the PRA mission time are usually conservative, they do not significantly alter the overall PRA results and there is no measurable benefit in trying to refine them.

2.1.5 Human Reliability Analysis

The HRA is the technical element of the PRA that is associated more than any other technical element with uncertainties, subjectivities, and assumptions. The objective of HRA is to include impact of plant personnel actions in the assessment of risk. The operator actions in PRAs are called human failure events (HFEs). The actions include pre-initiator HFEs and post-initiator HFEs, with some HFEs being part of the initiating events (e.g., a loss of essential service water is an initiating event and human actions could directly contribute to this initiating event occurrence).

For the pre-initiating events, routine activities that can result in system or SSC unavailability are identified and evaluated using a systematic process. For the post-initiating events, personnel actions are identified based on plant-specific procedures, an HFE is defined for each action, and a systematic process is applied to evaluate each HFE [3].

HRA is closely related to accident sequence, success criteria, and systems analyses discussed in the earlier sections. In the accident sequence analysis, operator actions should be considered along with the system response because many mitigating strategies are reliant on human interference. The success criteria are defined as available time for the necessary operator actions. The systems analysis provides information about specific

personnel actions that could make system unavailable (i.e., pre-initiator HFEs) or actions required to deploy a system to mitigate accident conditions (i.e., post-initiator HFE).

Timing is the key parameter and a structured timeline presented in Figure 2-2 is used for each HFE to capture various aspects of time during the progression of an accident from initiating even until the time at which the action will no longer succeed [5].

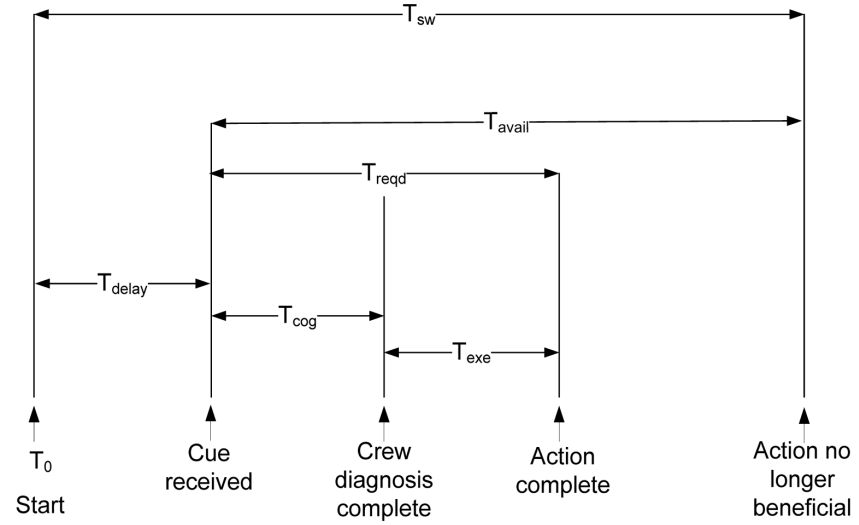

Figure 2-2. HRA timeline illustration diagram

The terms associated with each timing element are described below:

T_0 = start time = start of the event
T_{delay} = time delay = duration of time it takes for an operator to acknowledge the cue
T_{sw} = system time window
T_{avail} = time available = time available for action = ($T_{sw} - T_{delay}$)
T_{cog} = cognition time consisting of detection, diagnosis, and decision-making
T_{exe} = execution time including travel, collection of tools, and manipulation of equipment
T_{reqd} = time required = response time to accomplish the action = ($T_{cog} + T_{exe}$)

The structured timeline allows the analyst to demonstrate, among other things, the feasibility of the action from the perspective of timing [5].

All the timing elements identified above are associated with various assumptions and most often the assumptions are conservative, as discussed below.

The system window time T_{sw} is provided by the success criteria analysis and for many actions, this is the value obtained from TH analyses. From the system functional criteria example discussed in Section 2.1.3, *15 minutes to core uncovery* and *30 minutes to core damage* are the times that can be selected as T_{sw} for an operator action to actuate a standby HPSI pump if the normally aligned pump does not start automatically. While the typical success criteria of prevention of core damage (i.e., *time to core damage*) is sufficient, a shorter *time to core uncovery* is often used for conservatism. The shorter time results in the determination that the operator action is not realistic (i.e., is guaranteed to fail) or it causes a significantly increased human error probability (HEP). In addition, short time windows cause operator actions to fall into the "time-critical operator actions" category which imposes additional requirements like focused oversight, increased frequency of training, requirements for periodic simulation and verification, etc. which require additional personnel or NRC staff time (i.e., increased costs).

The start time T_0 is very straightforward, but it still can vary since it can represent the beginning of the negative event (e.g., RCS pressure boundary failure, which is a LOCA event) or it can be the time when the reactor is tripped following the event initiation (e.g., reactor trips a few seconds after LOCA initiates).

Typically, this parameter does not require assumptions other than a clear definition about what it represents for consistency throughout the entire HRA.

The delay time T_{delay} is usually based on notifications available from various equipment displays, sensors, and alarms that inform operators of a present condition. However, delay time can also be an estimation based on number of steps in procedures that operators would have to go through before arriving to a decision point that directs them to verify a certain condition or perform an action. The delay time based on sensors is the most objective while other estimates can be highly subjective and require expert opinion or other means to estimate. When in doubt, a longer delay time is selected to minimize time available for conservative action.

The cognition time T_{cog}, which consists of detection, diagnosis, and decision-making, is arguably the most subjective timing parameter because it can vary greatly for the same scenario from person to person, crew to crew, and plant to plant. Factors such as clarity of the cues, number of steps in the procedure, memorization of actions, frequency of training, general understanding of the accident in progress, effectiveness of communication between crew members—all directly affect T_{cog} estimates. The above-mentioned factors are highly variable which makes T_{cog} uncertain and subjective. When in doubt, longer amounts of time are used for conservatism to minimize time available for action.

The execution time, T_{exe},is the estimate representing all physical actions that must be performed as part of an HFE. For example, an action to manually close a valve located in a high-radiation zone involves multiple steps, such as command to perform the action issued by a senior reactor operator in the control room communicated to a plant operator, travel time for the plant operator to reach the location of the valve, time to put on personal protection equipment required for the action in the high-radiation zone, time to manually close the valve, and time to confirm with the control room that the action has been completed. The estimate of T_{exe} is typically obtained from a few timed simulations which makes it objective and reasonable. However, analysts may elect to use conservative bounding estimates (i.e., longer amounts of time) instead of measured ones for non-critical scenarios where ample time is available to successfully perform the action.

The available time, T_{avail}, is ultimately the timing element that influences calculations of failure probabilities of operator actions. The available time is often minimized for conservatism by reducing T_{sw} and/or by increasing T_{delay}. Ideally, T_{avail} should be sufficiently longer than the sum of T_{cog} and T_{exe} to allow time for recovery in case the first attempt to perform the action fails. The overly conservative T_{avail}, T_{cog}, and T_{exe} estimates have the same consequences as discussed above for T_{sw} when probabilities of failures are overestimated, and additional oversight requirements are being imposed.

In addition to the estimates of probability of failure for individual operator actions, dependency between multiple actions necessary for mitigation of a given accident is considered part of HRA. The HRA dependency analysis is performed using additional assumptions based on time available, procedures, stress, workload, and crew factors. The basis for the dependency analysis is the idea that the probability of failure of a subsequent operator action is affected by either success or failure of the prior actions. While it may be a valid hypothesis, it has not been fully validated, and associated data are limited. The “dependent HEP” estimate represents a probability of failure of the human-related portion in the mitigating strategy applied to a given accident scenario. There is significant uncertainty associated with a dependency analysis and to overcome this uncertainty a “minimum dependent HEP” is usually imposed in the PRA. The minimum dependent HEP value is typically reasonably small, and its use does not appreciably alter CDF and LERF values. However, the HRA dependency analysis is a very cumbersome, lengthy, process and it significantly complicates PRA model quantification.

The significance of time estimates in the HRA cannot be overstated: the HRA results are often extremely sensitive to event small time variation. The HRA is also one of the highest contributors to the risk results. While it is understandable that plant accident mitigation is very dependent on human actions, something that is characteristic of the design of existing plants, often the estimates of failure to perform highly proceduralized, frequently trained, often memorized actions are overly conservative. The conservatisms in HRA result in overestimation of CDF and LERF which, in turn, limits flexibility in plant operation because regulatory oversight process use CDF and LERF to represent risks associated with a given plant operation. As such, the

switch from a typically conservative to a reasonable HRA is the necessity recognized by the industry, yet it remains unresolved.

2.1.6 Data Analysis

The objective of the data analysis element is to estimate the parameters used to determine the probabilities of the basic events representing equipment failures and unavailabilities modeled in the PRA [3]. Relevant generic industry evidence as well as plant-specific evidence are represented in the parameter estimates, including addressing uncertainties.

Time in the data analysis is the metric associated with data estimates. Specifically, equipment failures are differentiated from demand failures (e.g., pump fails to start) and failure rates (e.g., pump fails to run). However, time may be an implicit factor that affects data estimates. For example, the probability of an EDG to operate is an estimate typically obtained based on EDG testing. The resulting probability of failure is affected not only by the frequency of testing (i.e., how many failures were observed during all the tests performed), but also by the test duration. As such, it is important for the industry to understand the process of how the generic industry estimates are derived since they are typically used as the failure data estimates in the PRA unless plant-specific estimates are significantly different (e.g., specific equipment failures are much more frequent compared to the industry average data). There is an opportunity for the industry to design equipment tests in such a way that they result in more realistic failure estimates.

2.1.7 Quantification

The objective of the quantification element of the PRA is to provide an estimate of CDF based on the plant-specific core damage scenarios for an as-built, as-operated plant, as completed by the PRA technical elements described in the sections above. There are no timing input parameters associated specifically with the quantification element.

2.1.8 Large Early Release Frequency Analysis

The LERF analysis objective is to identify and quantify the contributors to large early releases based on the plant-specific core damage scenarios [3]. The LERF analysis uses the physical characteristics of the Level 1 core damage assessment to define plant damage states and identifies and evaluates plant-specific LERF contributors. The LERF analysis is expected to use realistic assessments of containment failures and containment bypass scenarios.

LERF is defined as the frequency of the accidents leading to rapid and unmitigated release of airborne fission products to the environment before the opportunity to implement offsite emergency response actions. LERF is a surrogate for the early fatality quantitative health objective, and it is used as the quantitative plant risk metric because most of the existing operating reactors do not have Level 3 PRAs. A Level 3 PRA is the comprehensive evaluation of the effects that hypothetical plant accidents may have on humans and the environment.

There are multiple assumptions made in the LERF analysis, and the assumptions are intentionally conservative to simplify PRA modeling and overcome uncertainties associated with the plant system performance. While timing is a key parameter in analyses evaluating health effects from nuclear accidents, it is not explicitly used in LERF analyses because of the simplified approach usually taken. However, in more detailed analyses, time is incorporated via success criteria obtained from modeling of containment performance following core damage.

LERF is currently used for reactor oversight purposes even though it is not the metric supporting reactor licensing. Instead, a release of fission products from the LWR core to the containment atmosphere, also known as “source term,” is the metric used for the purpose of calculating the offsite doses in accordance with 10 CFR Part 100, Reactor Site Criteria [6]. A specific discussion of the use of source term in the regulatory framework applied to the existing LWRs is included in Section 4.1.4 since the topic warrants special attention beyond LERF analysis in the PRA.

2.2 Timing in Deterministic Assessments

After investigating timing parameters used in various aspects of the PRA, it is important to discuss how time is used in some deterministic assessments that are used as a basis for the PRA.

The deterministic analyses usually evaluate physics-based phenomena relevant to nuclear physics, fuel performance, and plant system performance. A representative example of a deterministic analysis is an evaluation of fuel and core performance during postulated design basis accident scenarios given certain mitigating strategies being successful or failed. These are the TH assessments mentioned earlier in the report that provide information such as, for example, time to core damage.

The time to core damage is obtained from well-established models that are verified and validated to reasonably represent physical processes occurring at the reactor core during a postulated accident. The "core damage" state is, however, an assumption on its own. The core damage state is defined as uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core (i.e., sufficient, if released from containment, to have the potential for causing offsite health effects) is anticipated. In the TH analyses supporting PRA, core damage is assumed to occur when:

- Core predicted instantaneous peak clad temperature reaches 2,200°F
- Core predicted sustained (at least 10-minute duration) peak clad temperature reaches 1,800°F.

The above assumptions ensure that both lower temperature sustained heatup of the core and instantaneous short duration extreme heatup of the core are considered when determining core damage.

The conditions postulated as core damage are derived from various experimental tests and based on multiple TH modeling simulations. They have built-in uncertainties and safety margins. This means the instantaneous peak clad temperature when fuel damage is observed could be 2,210°F, for example—10 degrees higher than the postulated benchmark. The additional 10 degrees would result in longer "time to core damage" parameters used throughout the PRA model.

In summary, while deterministic assessments are seen to be based purely on physical phenomena, assumptions and margins that are associated with those deterministic evaluations may have significant effects on risk assessments. As such, attempts should be made to derive "as reasonable as possible" values from the deterministic analyses. This can be accomplished by collecting additional experimental data to refine modeling, by more detailed modeling of the physical phenomena. These models are now possible due to significant advancement of computational technologies, and by scientific advancements applied to better understanding physical phenomena. This will allow removal of assumptions that were necessary to overcome the limitations of not fully understanding of these phenomena.

2.3 Timing in Dynamic Risk Assessments

Dynamic PRA or simulation-based risk assessment is a relatively recent advancement in the risk analysis domain. As discussed in Section 2.1, typical PRAs use time only explicitly via multiple assumptions, boundary conditions, and success criteria. This is because typical PRAs are static in nature where plant conditions and relationships are represented as the single-time snapshot. Instead, a dynamic PRA models behavior of the plant system components explicitly over time [7].

Dynamic PRAs are beneficial compared to traditional PRAs because they have the potential to increase realism by explicitly modeling propagation of certain accidents and incorporating mitigating strategies as appropriate during the scenario progression. For example, in traditional PRAs, recovery of failed systems and components typically is not credited because of the assumption that either it is not possible or there is not enough time. However, many scenarios, especially longer ones, most likely offer opportunities for failed equipment restoration.

Siu notes in [8] that dynamic PRA has the capability to improve treatments of potentially important dependent failures. Dynamic PRA can support, for example, a detailed analysis of Flexible Mitigating (FLEX)

strategies. Deployment of FLEX equipment for mitigation of severe accidents requires multiple operator actions performed outside of the control room. Timing associated with these actions includes aleatory variables as well as the conditions under which FLEX may be required. As such, dynamic simulation tools are best-suited to address this problem. Similarly, dynamic PRA has capabilities to address specific challenges associated with external hazards where event progression in time can provide valuable insights of corresponding equipment failures (e.g., a flooding event may fail some equipment instantaneously while it takes time for water to propagate to other areas and fail additional equipment) so that mitigating strategies can be planned accordingly.

2.4 Summary

Timing is without a doubt the key parameter in risk assessment. As discussed in Section 2.1, time is included in essentially every element of the PRA even if only implicitly via multiple typically conservative assumptions and success criteria. Given the significant effect timing parameters have on the risk results, it may be beneficial to refine timing parameters to gain realism in overall risk results.

The risk metrics are important because they directly support safety implementation processes directed at achieving successful regulatory outcomes. More specifically, risk metrics are directly used by the Reactor Oversight Process (ROP), which is the NRC's program to inspect, measure, and assess the safety and security performance of operating commercial NPPs. The ROP is a decision-making framework that ensures that observations at each level of a hierarchical set of performance objectives are satisfied.

This warrants an extension of the discussion beyond timing parameters and how they are used in risk evaluations to the topic of how the regulatory framework affects plant processes, which is offered in the next section.

3. REGULATORY FRAMEWORK FOR U.S. NUCLEAR REACTORS

Safety is a key parameter for all aspects related to operation of NPPs and the regulatory framework plays an essential role in establishing and enforcing rules that provide reasonable assurance of adequate protection of public health and safety. The NRC defines the regulatory framework as follows [9]:

Regulatory Framework: *The interrelated elements that form the basis for the NRC's oversight of the use of radioactive materials, including (1) the NRC's mandate from Congress in the form of enabling legislation, (2) the NRC's licenses, orders, and regulations in Title 10 of the Code of Federal Regulations (10 CFR), (3) regulatory guides, review plans, and other documents that clarify and guide the application of NRC requirements and amplify agency regulations, (4) the licensing and inspection procedures used by NRC employees, and (5) the agency's enforcement guidance.*

All nuclear power plant applications must undergo an NRC safety and environmental review after which the plant is given a license to operate. Once a NPP goes into operation, the framework switches to regulatory oversight, which brings in additional requirements from regulations and regulatory practices. An overview of licensing approaches is presented in the next sections.

3.1 State-Of-Practice – Regulatory Framework Used for Existing Nuclear Reactors

The NRC developed many of the initial regulations using deterministic regulatory requirements that were based on the current state of knowledge, experience, test results, and expert judgement at various times over the past 70 years. The NRC considered a wide range of factors at any given time and in relation to any regulation promulgated. Prominent among such factors are engineering margins and the principle of defense-in-depth (DID). A simplified description of DID assumes that undesirable events can occur and requires plant designers to include multiple layers of safety systems to prevent and/or mitigate consequences of potential accidents. The initial regulations only answered two questions: (1) what can go wrong and (2) what are the consequences without any considerations of likelihood of undesirable events? This was the case until 1975 when the Reactor Safety Study known as WASH-1400 or NUREG/75-014 was published [1]. Since then, the nuclear industry has

significantly advanced its knowledge of risk via implementation of PRA which provides a much more comprehensive understanding of nuclear safety.

Because of these advances, the NRC decided to implement risk-informed, and ultimately performance-based approaches into implementation of the regulations. In 1993, Congress passed a law called the "Government Performance and Results Act" with the objective "*to improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction* [10]." One of the actions taken in response was issuance of the "The PRA Policy Statement" [2], which formalized the NRC's commitment to risk-informed regulation through the expanded use of PRA.

The operating nuclear reactors in the U.S. are licensed under 10 CFR Part 50 [11] which has a two-step licensing process. The licensing process was updated in 2007 when 10 CFR Part 52 [12] was issued. It was perceived to be a more efficient licensing approach, but it used technical requirements drawn from Part 50. Both Part 50 and Part 52 rely almost entirely on deterministic approaches to evaluate the safety of both nuclear reactors and prescriptive approaches to enforce their adequate performance. As a result, many current regulations are still solely based on deterministic and prescriptive approaches even though the NRC has committed to more to risk-informed and performance-based (RIPB) regulations [10].

The same prescriptive approaches were built into the NRC ROP where plant SSCs are required to perform according to a very specific range of operating parameters with any deviation from the prescribed operational range is considered a failure. If a pump flow rate decreases below the prescribed range, the pump is considered failed. However, the pump is in fact still operating and providing flow which could be sufficient to meet some functional requirements.

The prescriptive approach to systems and equipment performance monitoring equates to significant burdens for the plants due to the number of compliance activities. In the late 1990s, the nuclear industry realized that many of such expensive and complex activities resulted in very little gain in overall plant safety. Instead, the focus should be applied to systems and components that are most significant in terms of affecting plant safety. This realization and the fact that plants were equipped with PRAs triggered the advent of risk-informed approaches to plant safety monitoring and maintenance. The earliest risk-informed application was the Risk-Informed Inservice Inspection (RI-ISI) program initiated in 1999 [13]. The program supplemented prescriptive requirements for inservice inspections of NPP components by focusing inspections of piping on highly risk-significant locations and locations at which failures are most likely to occur. This program significantly improved effectiveness of inspections because examination methods were based on the applicable failure modes and configuration of piping systems. At the same time, the program was extremely beneficial in terms of economic efficiencies since it allowed significant scope reduction of the inservice inspections.

Other important risk-informed applications were developed and are currently being adopted by NPPs:

- 10 CFR 50.69 Risk-informed categorization of treatment of structures, systems and components for NPP [14], [15] which allows to reduce prescriptive requirements for SSCs determined to be of low safety significance. This program results in significant cost savings realized through reduced procurement cost by allowing to procure equipment as commercial-grade instead of much more expensive safety-grade dedicated equipment. Also, many monitoring requirements for low safety significance equipment can be either eliminated or simplified.
- Risk-informed technical specification initiative 4b, "Risk-Managed Technical Specifications Guidelines" [16] which allows extension of component unavailability time without entering the Limiting Condition of Operation that necessitates reactor shutdown. This program is very beneficial since maintenance of equipment can be performed for a longer time with reactor still being in operation resulting in significant avoided losses of revenue.
- Risk-informed technical specification initiative 5b, "Risk-Informed Method for Control of Surveillance Frequencies" [17]. This program allows performance of prescribed surveillance activities less frequently (e.g., during every other outage instead of every outage) resulting in significant cost saving on test and maintenance and by reducing duration of outages, which equates to avoided loss of revenue.

While risk-informed approaches gained recognition and demonstrated success in terms of gained efficiencies and improved safety, existing NPPs stopped short of realizing the full potential of the NRC-envisioned strategy of using both risk-informed and performance-based approaches.

3.2 State-Of-The-Art – Transitioning from Deterministic and Prescriptive to Risk-Informed and Performance-Based Approaches

3.2.1 Regulatory Framework for New Reactors

The nuclear industry in the U.S. and around the world could be experiencing revitalization from the many advanced nuclear technologies being developed that promise design, demonstration, and construction of new types of nuclear reactors as early as the next decade. The new technologies brought new challenges and raised questions, many of them related to the existing regulatory framework—are existing regulations applicable, feasible, reasonable, and adequately efficient to be used for licensing and regulation of advanced reactors without placing unnecessary burden that could jeopardize deployment of new technologies?

In the recent few years, both industry and the NRC put significant efforts into expansion and modernization of the U.S. nuclear regulatory framework which primarily targets advanced reactors. The proposed new regulatory framework could permit significant advancements compared to the current regulations by reducing reliance on deterministic and prescriptive approaches and encouraging RIPB approaches. A few proposals for advancements and the progress accomplished so far are outlined below.

The Licensing Modernization Project (LMP) is a major undertaking led by the Southern Company, coordinated by Nuclear Energy Institute (NEI), and cost-shared by the Department of Energy (DOE), with the NRC closely engaged. As the results of these industry-wide efforts, the NRC published Regulatory Guide (RG) 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors. [18]" This regulatory guide endorsed the methodology described in NEI 18–04, Revision 1, "Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development, [19]" as a reasonable approach to support specific aspects of the licensing of non-light water reactors. The NEI 18-04 guideline "*presents a modern, technology-inclusive, risk-informed, and performance-based (TI-RIPB) process for selection of Licensing Basis Events (LBEs); safety classification of structures, systems, and components (SSCs) and associated risk-informed special treatments; and determination of defense-in-depth (DID) adequacy for non-LWRs. This guidance document provides one acceptable means for addressing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection.* [19]"

The LMP is an advancement in the regulatory domain because it introduces risk-informed, performance-based approaches to traditionally deterministic-only areas. One such area is the selection of LBEs. The events used in the licensing process for existing operating reactors were selected based on the experience and expert knowledge of potential and actual hazards observed during accidents (e.g., Three Mile Island nuclear plant accident), as well as significant precursor events such as the vessel-head corrosion at Davis-Besse nuclear plant. The reactors are designed, built, and are now operating under requirements to be able to withstand DBAs regardless of how likely they are, with some exceptions for hazards that were undoubtedly proven to be inapplicable (e.g., tsunami for an in-land plant).

Important progress is also being made in the area of plant performance assurance—the ASME released a code for the Reliability and Integrity Management (RIM) Program known as Section XI, Division 2 [20] which has been endorsed by the NRC in the draft regulatory guide DG-1383 [21] as an acceptable approach for preservice and inservice inspection program for non-LWRs.

ASME Code Section XI, Division 2 outlines a process for developing a RIM program that is similar to the LWR existing programs, but it contains provisions that are well beyond a traditional approach. The Code proposes a risk-informed approach (i.e., use of PRA) to develop reliability targets for SSCs. It also relies on a performance-based approach to monitor SSC performance, with practices such as equipment monitoring and

nondestructive examination, repair, and replacement to maintain the reliability of components based on degradation mechanisms that may occur throughout the life of the plant. This is a very important development for the industry because it represents another traditionally deterministic-only and highly prescriptive area of reactor oversight that shifts to engaging some RIPB approaches.

A potentially major regulatory framework update that is currently in progress is the development of a 10 CFR Part 53 rule "Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors" [22]. The new rule is being developed as an optional regulatory framework for use by applicants for new commercial advanced nuclear reactors. The drafted rule relies on methods of evaluation, including RIPB methods, that are flexible and practical.

While deterministic analyses undeniably remain a very important part of the safety analysis realm, a framework that integrates deterministic, risk-informed, and performance-based approaches is considered appropriate and suitable to support the highest levels of nuclear safety while allowing flexibility for NPP owners and operators to meet those high standards.

3.2.2 Prescriptive Versus Performance-Based Approaches

There are major differences between a prescriptive approach and a performance-based approach to implementing safety requirements and monitoring system performance relative to achieving safety outcomes. A prescriptive approach relies primarily on operational requirements for system and equipment performance (i.e., in which manner a component should operate to be considered acceptable). The prescriptive approach is centered on performance at a component level which is assumed to guarantee the acceptable performance at the system level. Nuclear technology development has traditionally used prescriptive requirements associated with design, construction, and operation. Even before design requirements were considered in terms of NRC regulations, companies unhesitatingly used prescriptive requirements in their proposed designs because it simplified the work of designers and facilitated the procurement process to establish reliable supply chains. Some participants in industry have called such practice "build to print" where manufacture of components occurs to strictly enforced specifications. For example, ASME codes which apply to the manufacture of components are based on such practices.

A performance-based approach initiates at the system level and starts with functional requirements. It relies on a "systems-based" approach in which information related to a design is considered in terms of accomplishing functional purposes in an interdisciplinary and iterative manner. The systems-based approach is a top-down approach that focuses on the system as a whole, and it is capable of tracking and tracing functional performance requirements within the design to assure consistency with multiple considerations such as safety and economics.

The prescriptive approach relies on the presumption that strict compliance with documented specifications is a fully valid solution toward accomplishment of an intended purpose. However, if a connection is not made with the engineering functional objective, there is a possibility for inconsistencies between the system purpose and system performance. A prominent example of this is the requirement that many NPP components meet all criteria in 10 CFR 50, Appendix B regardless of whether meeting these criteria translates into improved safety. Hence, the assumption that documentation is sufficiently complete in relation to an engineering objective may not be valid for activities beyond manufacture of a component. A component that complies with the prescribed requirements may not necessarily be fit for its purpose at the system level. Experience shows that specification of requirements in a prescriptive way tends to be very conservative. This creates the distinctions such as those made between safety-grade and commercial-grade components which are not always necessary. It is in this regard that cost-effectiveness is negatively impacted when conservative requirements are imposed even though they may not be contributing toward fulfillment of the engineering functional objective.

3.2.3 Performance-Based Approach in the Regulatory Framework

The NRC recognized that use of risk information alone may not be sufficient to address the needs of a safe but viable nuclear power industry. The NRC articulated its vision for the future of implementing nuclear safety when it issued SRM-SECY-98-0144, "White Paper on Risk-Informed and Performance-Based Regulation," (hereinafter called the "White Paper"), in March 1999. This vision contains some radical differences with the

regulatory approaches in use during the 1990s. One such difference is the formal recognition of a combination of the risk-informed and performance-based (RIPB) approaches to nuclear safety. The formal aspect arises from the authority of the NRC that the definitions in the White Paper carry in application to nuclear safety regulation. NRC Words used at the NRC level carry policy implications. In this case, the words used by the NRC formally identify the attributes that should characterize a RIPB approach to regulation as follows:

"Stated succinctly, a risk-informed, performance-based regulation is an approach in which risk insights, engineering analysis and judgment including the principle of defense-in-depth and the incorporation of safety margins, and performance history are used, to (1) focus attention on the most important activities, (2) establish objective criteria for evaluating performance, (3) develop measurable or calculable parameters for monitoring system and licensee performance, (4) provide flexibility to determine how to meet the established performance criteria in a way that will encourage and reward improved outcomes, and (5) focus on the results as the primary basis for regulatory decision-making."

The White Paper addresses safety margin by laying down requirements for a decision-making framework that works to avoid safety concerns. Prescriptive specifications on components are unlikely to be the proof of avoiding safety concerns because such concerns invariably occur at the functional or system level. The definition of a performance-based approach also requires that the framework offers flexibility to encourage and reward improved outcomes. The following describes the meaning of each attribute of the performance-based approach outlined in the White Paper.

(1) Measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee, performance…

The expectation outlined in this attribute is that the system performance (explicitly including facility and licensee performance) should be monitored. Monitoring requires that appropriate parameters are identified. The licensee should have the freedom to offer suitable parameters for the NRC to review and approve. There is no prescription related to the nature or scope of the parameters that a licensee may offer to monitor. The only stipulation is that what is monitored must be related to facility and/or licensee performance at the system level.

This attribute of a performance-based approach can be used to facilitate requirements management. A requirement needs to be associated with one or more parameters. Hence, an alternative to a prescriptive requirement is to identify specific parameters that can be monitored.

(2) Objective criteria to assess performance are established based on risk insights, deterministic analyses and/or performance history…

The licensee is free to use criteria that are traditionally deterministic (i.e., as provided in NUREG-0800 [23]) or risk-informed (i.e., based on PRA insights), each in combination with information supported by performance history. The only stipulation is that the criteria must be objective in nature (in contrast with subjective judgement). Quantification is frequently seen as the ultimate level of objectivity that could be achieved. However, alternatives to quantification may exist that could be sufficiently objective. For example, safety margins may be expressed in terms of time available to correct the deficiency serving as the objective criteria.

(3) Licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes…

This represents one of the major potential payoffs for licensees to incorporate a performance-based approach. Each licensee is free to establish performance criteria and determine how to meet them. There can be a significant scope for innovation by licensees to use their intimate familiarity with their plants to propose specific ways to formulate this attribute. However, the notion of flexibility implies that the domains for the involved variables are relatively continuous and not characterized by cliff-edge effects. There cannot be flexibility without margins, and conversely, greater the margin, the more opportunities exist for flexibility. It is noteworthy that this attribute includes the concept of rewarding superior performance. The investments that a licensee makes in monitoring safety performance appropriately can be used to realize greater cost-effectiveness of various plant activities such as maintenance.

The current ROP framework includes the concept of rewarding adequate performance in the form of limiting ROP activities to the baseline inspection program which "*is considered the minimum inspection effort needed to ensure that plants meet the "safety cornerstone" objectives.* [24]" The plants that do not meet the safety performance objectives receive significantly increased level of oversight as well as potentially stronger actions up to a suspension of the operating license. This structure represents the reward being expressed in terms of avoided penalties instead of a positive reward such as permitting increased flexibility.

Instead, the "reward" should emerge from the way a licensee implements a performance-based approach to take advantage of robust margins that exist on account of the conservative design practices characteristic of operating reactors. Evidence of superior performance could be documented by identifying parameters and criteria for the level of performance objectives supporting the ROP cornerstones of safety. The licensee could identify criteria associated with such objectives in such a way that the NRC can have no reason to consider intrusive actions that could penalize licensee operations unnecessarily. Hence, a licensee can create "rewards" by setting up NRC-approved observations and criteria so that the data monitored provide an alert to have the licensee take appropriate actions well ahead of a level at which NRC might express a concern. The licensee can propose and implement such a process using the ROP framework.

(4) A framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern.

The framework mentioned in the attribute (4) can be established and demonstrated using the safety margin concept. As discussed in NUREG/BR-0303 [25], the safety margin is a quantity that expresses the difference between the expected performance (i.e., within the limits of a corresponding criterion) and performance that is representative of a concern (i.e., undesirable performance). Each performance criterion must be established so that there is a sufficient margin remaining between the "undesirable performance" and "safety concern" metrics. In addition, the word "immediate" in the attribute (4) requires consideration of a time element. A safety margin expressed in time is also an adequate framework based on the notion that upon failure to meet the performance objective, sufficient time will be available to take corrective action to avoid a more serious condition associated with a safety concern. This is confirmed by guidelines provided in SECY-00-0191 that indicates the framework can be confirmed if: *"(1) an adequate safety margin exists, (2) time is available for taking corrective action to avoid the safety concern., and (3) the licensee is capable of detecting and correcting performance degradation.* [26]"

NUREG/BR-0303 "Guidance for Performance-Based Regulation" [25] offers directions on a process for developing a performance-based alternative to support regulatory decision-making. While the guidance was originally developed to support the NRC staff, it is very valuable for use by the industry who consider implementation of risk-informed and performance-based approaches to support regulatory compliance activities.

3.3 Reimagining Requirements Management Structure

As discussed in Section 3.1, the regulatory framework for the existing reactor is based on the set of prescriptive requirements and the adequacy of plant safety performance is assessed in terms of meeting those prescribed requirements. However, the NRC reactor oversight framework is structured as a risk-informed, tiered approach shown in Figure 3-1 [24].

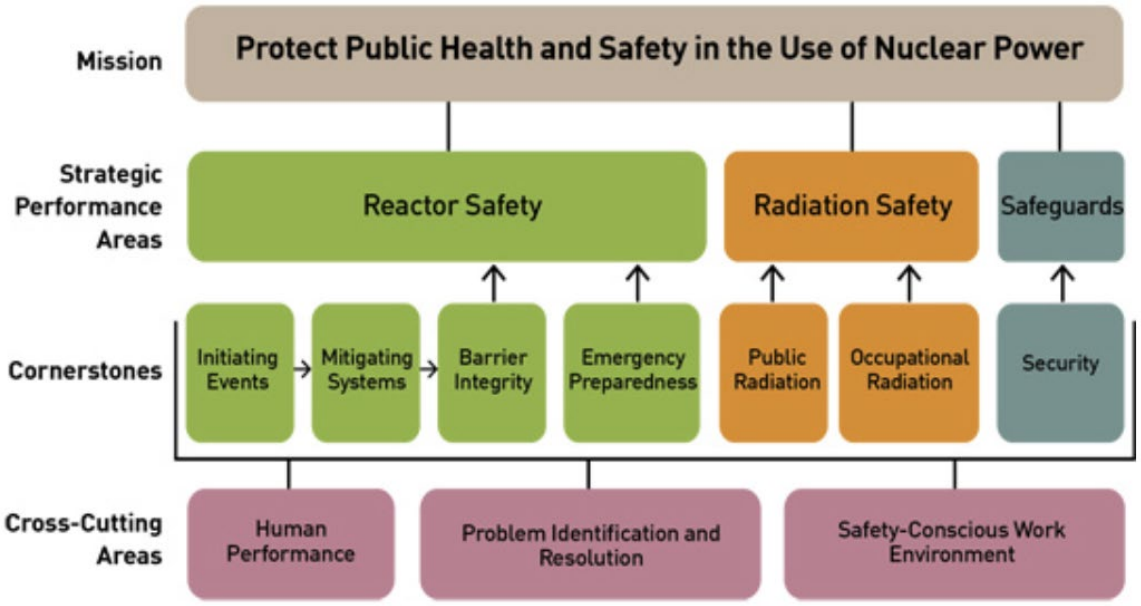

Figure 3-1. NRC Reactor Oversight Framework

The "tiered approach" represents a logical hierarchy where the highest level is the overall mission to "*protect public health and safety in the use of nuclear power*." This represents a goal which is ensured by meeting performance objectives in each Strategic Performance Area. These objectives are in turn supported by each cornerstone's adequate performance with considerations of Cross-Cutting Areas. The tiered approach of the reactor oversight framework correlates well with the concept of Objectives Hierarchy introduced in NUREG/BR-0303 presented in Figure 3-2 [25]. NUREG/BR-0303 makes an argument that it is advantageous to transition from prescriptive to performance-based approaches for decision-making applied to the ROP. This is because [emphasis added] "*A performance-based regulatory action achieves defined objectives and* ***focuses on results****. It differs significantly from a prescriptive action in which licensees are provided* ***detailed direction on how those results are to be obtained****.* [25]"

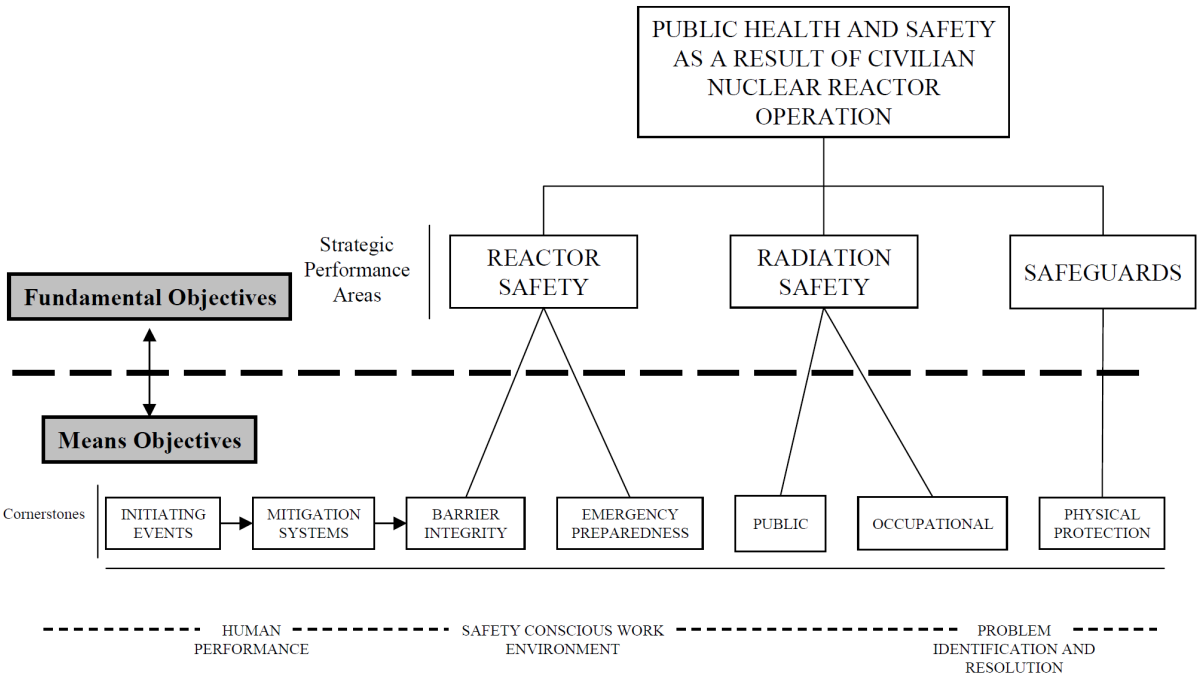

Figure 3-2. Reactor Oversight Process Objectives Hierarchy

The hierarchical decomposition of performance objectives is a similar concept to a "systems-based" approach focused on the system as a whole, where the overall system performance is emphasized over the performance of a system's individual parts. Like a logic tree, each level of objectives is derived from the level above so Fundamental Objectives are supported by Means Objectives, which effectively represents the cornerstones of the reactor oversight framework shown in Figure 3-1.

The benefits from implementation of the systems-based approach are attributed to the allowed flexibility for licensees to select cost-effective strategies at the Means Objectives level that ensure adequate performance at the Fundamental Objectives level. This is a radically different strategy from the currently employed approach where a prescriptive requirement is placed for each of the Means Objectives and for many levels underneath. The prescriptive requirements are associated with built-in conservatisms (intentionally), and offer essentially no flexibility, and as the result causes significant cost burdens for the licensees.

A more detailed discussion about systems-based framework is included in Appendix A-1.

The systems-based hierarchical approach is currently being implemented at other industries, specifically in space applications. An objectives-driven, case-based safety and mission success (S&MS) assurance framework being developed by the National Aeronautics and Space Administration (NASA) Office of Safety and Mission Assurance is discussed in [27]. A need to modernize an S&MS assurance network has emerged in recent years due to inefficiencies of the current approaches and emergence of new engineering methods and tools.

An objective-driven approach is selected for the S&MS assurance framework because it explicitly focuses on meeting ***fundamental objectives*** such as mission technical objectives and safety, along with other objectives important to stakeholders, such as cost. Objectives such as failure tolerance, compliance with quality standards, or implementation of corrective action processes, are only meaningful to the extent that they support the fundamental objectives. In other words, they are ***means objectives*** that indicate ***strategies*** for meeting the fundamental objectives [27]. This definition of the objective-driven approach in the S&MS domain is equivalent to the reactor process Objectives Hierarchy presented in Figure 3-2.

The needs that warranted NASA's transition from a prescriptive to a systems-based approach are strikingly similar to the issues experienced by the nuclear power industry as discussed in more detail below.

The need for a new acquisition strategy: NASA has significantly increased reliance on independent commercial contactors which is different from previous practices where NASA used to oversee the design, development, and testing of the systems provided by the governmental contractors. Acquisition from commercial contractors requires a strategy with a much lesser degree of NASA's involvement in the interim processes but still providing high-level of assurance in the received service or products. The new S&MS assurance framework offers such strategy where (1) NASA specifies the expectations for the high-level system performance and (2) vendor assures NASA that these expectations have been met in the manner of vendor's choosing, consistent with the vendor's means of achieving them given that NASA accepts the assurance mechanisms (i.e., ways to objectively demonstrate that expectations are met).

This is a very similar situation to NPPs updating or upgrading plant systems and relying on commercial vendors to supply a new system. The current approach is to rely on prescriptive specifications for a new system written by the plant staff. These specifications are usually just a repeat of the old system specifications which is, in most cases, a flawed approach because new systems are usually much more capable and significantly different compared from the outdated system they are replacing. Yet, NPPs are still forcing the old specifications to new systems even though it may not assure satisfactory performance on the system level and it forces vendors to make unnecessary and costly modifications just to meet the specification requirements. Obviously, the modifications are causing delays and the increased costs are being passed to the plant. Instead, the system requirements must be developed following systems engineering practices: the plant should clearly specify functional and in some cases performance requirements and allow the vendor to select the best (i.e., most efficient and cost-effective) *means* to meet the specified requirements.

The need to accommodate evolving systems engineering practices. The discipline of systems engineering has been undergoing dramatic changes in recent years which is driven by the increased reliance on digital

technologies. NASA and many other industries (e.g., automotive, commercial airplanes, Department of Defense) move toward a model-based systems engineering (MBSE) where the model is used as the single reference source for all the activities, both internal and external, associated with the system. As noted by Everett et al., the role of modeling and simulation in the analysis of potential mishaps and/or accidents has been increasing to the point where they replace some traditional risk assessment methods such as PRA. Modeling and simulation are being used both as alternatives to traditional PRA and as an addition to traditional PRA to provide hybrid approaches for assessing system performance [27].

A NPP is a "system of systems," comprised of complex systems. Each system is associated with very large network of interconnections with other systems, human operators, operation requirements, regulatory requirements, etc. Yes, plants continue relying on document-based strategies to monitor system performance and for decision-making. Each plant system is accompanied by dozens of documents (e.g., system operating manual, PRA system manual, plant technical specifications, plant normal, abnormal, and emergency operating procedures, system specifications, system maintenance documents, etc.). In addition, documents are owned and maintained by different disciplines (e.g., operations, engineering, licensing, PRA, maintenance, management) who often do not communicate with each other. This amount of information is not only hard to maintain, but is also essentially impossible for a system engineer who is responsible for monitoring system adequate performance to fully understand and trace. As a result, the decision-making is done based on only a subset of information or by using conservative assumptions which leads to unnecessary expenditures (e.g., system maintenance). An MBSE system model considers the system "as a whole" with all the internal and external relationships and dependencies properly accounted for, and all the stakeholders (i.e., disciplines) connected to a single reference source, which is a significantly improved decision-making approach.

The need to stipulate acceptable levels of S&MS risk. Everett et al. point out, "*NASA began actively implementing a philosophy of risk leadership within an established risk posture that can and should extend all the way to the initial selection of mission proposals, especially recognizing and factoring in the various classes of missions, where each class can accept a different level of risk*. [27]" The use of risk metrics in a safety assessment of nuclear power plants is a well-established process. The concept of "acceptable levels of risk" can be correlated to various metrics used in nuclear industry (e.g., acceptable CDF and LERF, acceptable radiation dose limit), and the more recent concept of reliability target use in NEI 18-04 [19] and ASME Section XI, Division 2 [20] guidance.

In short, the systems-based (or objectives-based) approach is the pathway to gain the flexibility in power plant operations while maintaining the highest levels of safety.

As discussed earlier in the report, the NRC has realized and appreciated the benefits of transitioning from deterministic and prescriptive approaches that were used at the initial stages of commercial nuclear power plant operation to risk-informed and performance-based approaches supported by deterministic evaluations. This realization is not new; the transformation process started 20 years ago and is continuing today. The regulatory framework for advanced reactors experiences more rapid modernization as compared to the framework that is in place for existing operating LWRs. However, there are no technical limitations on leveraging the same modernized strategies for the existing fleet. The limitations are only due to the licensing commitments that are already in place, which could be resolved via typical licensing amendment avenues.

Modernization of the regulatory framework for the existing operating NPPs offers various benefits, with the main one being greater flexibility in plant operations while maintaining the same high levels of safety. The flexibility translates into more efficient and effective plant operations via reduction of unnecessary burdens imposed by the current regulatory framework. While the goal of encouraging the regulatory framework modernization is to assist sustainability of the existing NPP fleet, this initiative would also be welcomed by NRC staff since it will directly support their goal of *Becoming a Modern, Risk-Informed Regulator* [28].

4. COST SAVING OPPORTUNITIES FROM MODERNIZATION OF LWR REGULATORY FRAMEWORK

To continue the discussion from the previous section, subsections below investigate specific areas where the transition to a modernized regulatory framework offers measurable benefits.

4.1 Regulatory Process Opportunities

4.1.1 Selection of Design Basis Events and Corresponding SSC Categorization

Section 3.2.1 discussed the LMP approach presented in NEI 18-04 [19] and endorsed by the NRC in RG 1.233 [18] which introduced risk-informed and performance-based approach to the selection of design basis events (DBEs) which is a fundamentally different practice as compared to the DBAs selected prescriptively for the operating reactors. If the same approach would have been applied to the existing LWRs, the set of DBEs could be different which would dramatically affect the set of safety-related equipment. In the LMP approach, SSCs classified as safety-related perform one or more safety functions that are required to either [19]:

1) Mitigate DBEs and design-bases accidents within prescribed frequency-consequence target

2) Prevent any high-consequence beyond DBEs from exceeding the frequency of $1x10^{-4}$/plant-year.

The safety-related SSCs for operating LWRs are defined in 10 CFR Part 50.2 [29] as:

"*Structures, systems and components that are relied upon to remain functional during and following design basis events to assure:*

(1) The integrity of the reactor coolant pressure boundary
(2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable."

The change in the set of DBEs will directly affect the set of safety-related SSCs, which is important because this equipment is subject to special treatment requirements. Some of the DBEs selected for LWRs would belong to the category of beyond DBEs if the LMP approach is used. An example is the large-break LOCA briefly discussed earlier in this report.

Significant benefits can be expected by simply revising the definition of LWR safety-related SSCs. The LMP approach defines safety-related SSCs based on their capabilities to prevent overall consequences (i.e., radiological release) while for existing LWRs, safety-related SSCs are defined based on their capability to support one of three safety functions. The significance is in the perceived independence for DID assessment of the three safety functions which leads to an unnecessarily large set of safety-related SSCs.

The SSCs are working together in a complementary way to prevent and/or mitigate the ultimate consequence (i.e., release of radiological material to the environment). Since each plant has multiple options to prevent and mitigate consequences from DBEs, the set of "necessary and sufficient SSCs" (i.e., the minimal subset of SSCs) to achieve the function of "prevention and/or mitigation of radiologic release" is expected to be significantly smaller than the current set of safety-related SSCs at a given LWR.

The recent study performed by the NRC and INL researchers evaluated application of the LMP approach to operating reactors [30]. The study concluded that (emphasis added), "*The LMP methodology is a useful tool that can be applied* ***beyond the original intended application*** *of the methodology. These types of results* ***can support integrated risk-informed decision-making*** *by highlighting areas where* ***safety margins*** *exist and* ***can be used to show the impact of DID design features***."

Additional research in this area is warranted such as:

- Investigating the possibilities for a correlation between the risk metrics employed for LWR safety evaluations (i.e., CDF and LERF) and the LMP risk metric expressed as 30-day total effective dose equivalents. Such a correlation would avoid the need for plant-specific Level 3 PRAs.
- Finding potential options for simplified Level 3 PRA modeling where radiological material propagation after its release from the containment is assessed using intentionally conservative but simple models which would allow significant reduction of efforts required for a full-scale Level 3 PRA model development.

The efforts to introduce risk-informed, performance-based approaches into reactor design are also being made in the LWR domain. The ANS just recently published standard ANS 30.3-2022, "Light Water Reactor Risk- Informed, Performance-Based Design," which provides requirements for the incorporation of risk-informed, performance-based principles and methods into the nuclear safety design of commercial light water reactors [31]. The standard gives plant designers the flexibility of selection of specific metrics to be used to define safety and then identify SSCs necessary to meet the risk criteria for the selected metric(s).

During the development of the ANS 30.3-2022 standard, a PRA from an operating plant was used as the case study that investigated what would have been classified as safety-related SSCs if this ANS standard was applied. The case study employed a method known as Top Event Prevention Analysis (TEPA) [32] which demonstrates that the logic models of PRAs can be used to support the selection of safety-related SSCs [33].

The TEPA method merits a dedicated discussion. If a flexibility is allowed to select any combination of SSCs to achieve necessary performance, it makes sense to accomplish this in the most efficient way. TEPA is a tool that systematically solves this selection problem by deciding where to best allocate resources to ensure the system performance. PRA provides input into TEPA in the form of cut sets and the output is the list of prevention sets, each with a selection of elements that satisfy safety objectives in joint reliability performance (achieved through prevention of failures) [32]. The TEPA method is a practical approach to select SSCs that are necessary and sufficient to assure the success of the fundamental objective instead of a prescriptive method applied for the selection of safety-related SSCs. In [32], Youngblood discusses an example of applying TEPA to generate prevention sets that specify intermediate levels of seismic hardening, as opposed to simply settling for either "no hardening" or a single preselected value. However, TEPA methodology can be extended to any initiating events and successfully used to inform selection of safety-related SSCs for operating NPPs, as demonstrated by the case study performed to support ANS 30.3-2022 standard development [33].

4.1.2 Equipment Qualification

In continuing the topic discussed in Section 4.1.1, equipment qualification can significantly benefit from performance-based approaches as compared to the prescriptive specifications, especially for the safety-related equipment that are obligated to be procured and maintained under the ASME Quality Assurance Requirements for Nuclear Facility Applications (NQA-1) [34]. The NQA-1 standard imposes numerous requirements associated with equipment manufacturing, testing, and maintenance during operation. The requirements are usually extremely strict which causes equipment costs to increase, in some cases, by several orders of magnitude. The same exact equipment, often by the same manufacturer, may cost 10–20 times more, simply because it went through the NQA-1 qualification process rather than being procured as a commercial, off-the-shelf (i.e., COTS) component.

The performance-based approach would allow for an alternative to the specification-type thinking traditionally applied to equipment qualification. Instead, equipment must be demonstrated to reliably perform functions assigned to it. The strategies must then be put in place to monitor the performance of the equipment while it operates to ensure that the equipment is functioning as expected with sufficient safety margins built in to ensure inadequate performance is corrected before it causes any events that may be significant to plant safety.

4.1.3 Physical Security

The physical security staffing accounts for nearly 20% of the entire NPP workforce [35]. This expenditure is unsettling given that out of all commercial power generation industries only nuclear is subject to this expense which contributes to the fact that existing operating plants struggle to compete economically with other power

sources. The physical security consists of a variety of measures to protect NPPs against malicious acts. The NRC and licensees currently use a graded approach for physical protection based on several considerations: threat assessment, physical protection areas, intrusion detection and alarms, and armed response. The graded approach uses intentionally conservative deterministic evaluations to find how much protection is enough which, in turn, determines the scope of the protection measures.

The current approach to physical security considers risk factors—the target set (i.e., what SSCs at the plant must be protected) is determined based on the insights from the plant-specific PRA model. However, this is the only risk-informed aspect of the entire physical security domain. The rest of the evaluations use conservative assumptions and boundary conditions.

For example, the evaluation starts with an assumption that an attack is imminent (i.e., probability of an attack is 1.0). Then, adversaries are assumed to be successful in breaching the secure perimeter of the plant and access the plant protected area. From there, physical barriers positioned throughout the plant provide DID to delay adversary progression and allow plant security personnel to take actions. The DID measures are designed based on assumptions that the adversary is highly skilled, trained, and motivated to be successful in breaching multiple levels of defense, then reaching and compromising several SSCs simultaneously to initiate an accident.

While the deterministic and prescriptive approaches are highly dominant, the regulatory framework 10 CFR Part 53 [22] that is currently being developed has dedicated significant efforts to transition the physical security domain to relying on performance-based approaches. While Part 53 is being developed with the focus on new reactors, the concepts being developed are technology-inclusive and many of them can be leveraged to gain benefits for existing reactors.

Recent research demonstrated success of using risk-informed, performance-based approaches to support physical security evaluations. The research conducted by INL demonstrated how plant safety metrics such as time to core damage can be used to demonstrate that reactor safety will be successfully maintained during many postulated security events [36]. The research is based on the idea that physical security strategies adequacy should be measured based on the consequence, such as core damage, and not by the binary measure (i.e., success or failure) of ability of adversary to complete the task. Figure 4-1 demonstrates the difference between the current and consequence-based (or performance-based) approaches.

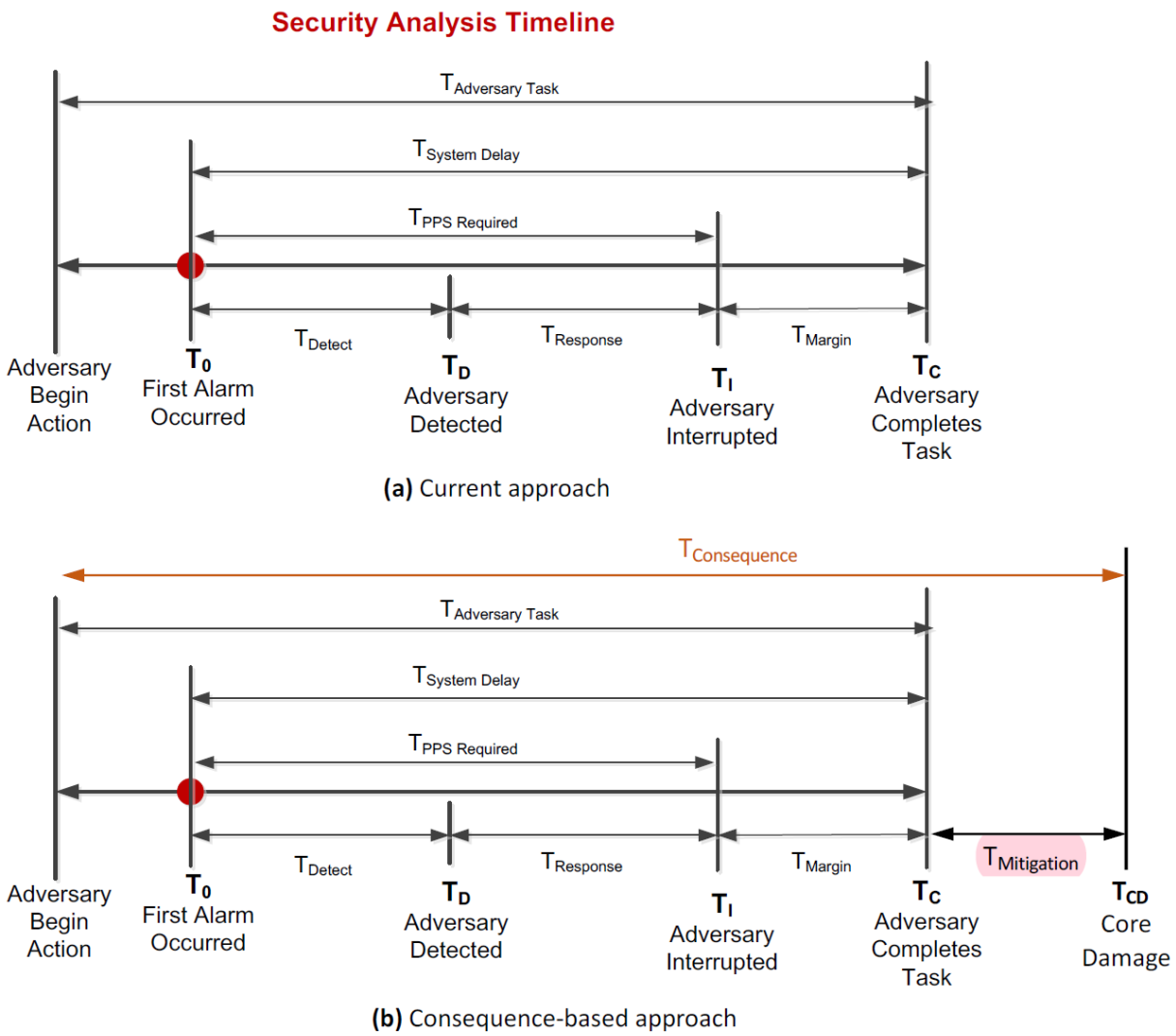

Figure 4-1. Comparison between Current and Consequence-Based Approaches to Security Timeline Analysis

The newly introduced $T_{mitigation}$ is the key parameter to implementing mitigating strategies that bring the plant to a safe state, even after the adversary task is completed successfully. Every plant has capabilities and means to mitigate beyond DBEs (i.e., events that are out-of-the-ordinary and not of the expected nature). These mitigating capabilities are mostly attributed to FLEX systems, but many plants have additional equipment and means. Plant personnel are trained on implementing FLEX, and deploying equipment is covered in procedures. As such, plants should be able to take advantage of these capabilities, and deploying FLEX to respond to a physical security event is one of the applications where such credit is extremely beneficial. The demonstration of plant safety expressed in terms of prevented consequences serves as the basis for relaxation of some prescriptive requirements, such as reduction of security forces (e.g., security guards) and better utilization of security equipment.

The risk-informed and performance-based approaches to physical security assessments offer even larger benefits to the new reactors that are still being developed. The new reactors have an opportunity to incorporate physical security measures in the facility design (e.g., minimal number of entry points). The risk-informed approach allows screening many postulated security events based on the consequence argument. Some security events can be demonstrated not to result in a release of radiological material to environment; thus, they can be screened from further consideration. Other security events can be demonstrated to require longer times to accomplish (i.e., to reach the Adversary Completes Task point) than Reasonable Assurance of Protection Time (RAPT), the point at which any security event is reasonably assured to be mitigated (e.g., by use of both in-site

and external security forces). In this case, plants rely on a performance-based approach where plant-specific physical barriers are demonstrated as capable of stopping or delaying the adversary while providing necessary advantages to security forces.

4.1.4 Radiological Release and Emergency Response

Controlling and limiting the release of radioactive materials from NPPs is one of the fundamental safety functions nuclear reactors and the NRC use in many aspects of regulatory policies and regulations. The operating reactors were licensed under 10 CFR Part 100 [6]. This requires evaluation of an event where there is an accidental fission product release resulting from substantial meltdown from the core into the containment. Its potential radiological consequences are to be evaluated assuming that the containment remains intact, but leaks at its maximum allowed leak rate [37]. There are two terms associated with radioactive material—material released from the containment is referred to as "radiological release to the environment," and radioactive inventory within the containment is called "in-containment source term," or simply "source term."

The early-day licenses postulated release that consisted of 100% of the core inventory of noble gasses and 50% of iodines based on experiments conducted in the late 1950s based on documentation in the TID-14844 report [38]. The regulatory guidance presumed that the source terms within the containments were instantaneously available for release with iodine chemicals at their most hazardous states. These assumptions significantly affected the design of engineered safety features, including containment isolation valve closure times.

The next progression in the analysis came with the WASH-1400 [1] study that introduced severe accident releases that were mechanistically determined best-estimate values and included estimates of containment failures. Although severe accident source terms have not been used in individual plant licensing safety evaluations, they have had significant regulatory applications such as partial basis for the sizes of emergency planning zones, basis for staff assessment of severe accident risk in the environmental statement, part of the basis for staff prioritization and resolution of generic safety issues, and other regulatory analyses [37]. Substantial information developed over 30 years following the issuance of the WASH-1400 study significantly increased knowledge about severe accidents at LWRs and the behavior of resulting fission products. As a result, NUREG-1465 was issued in 1995 [37] to provide realistic estimates for postulated fission product source term released into containment which has been used by most NPPs as the basis to change regulatory requirements. The approach in NUREG-1465 was a performance-based and physics-based approach to realistically estimate source terms released into containment considering fuel performance and in-containment removal mechanisms.

More recent analysis conducted by Sandia National Laboratory in 2010 [39] demonstrated that the retention of fission products within the vessel and the RCS are greater than contemplated in the NUREG-1465 prescription. The overall release fractions to the containment were determined lower by about a factor of two with longer release durations than those suggested in NUREG-1465. The research determined that the NUREG-1465 formula appeared to be significantly more conservative compared to the best-estimate analyses employed in the Sandia study. While there are benefits for the operating reactors to refine the licensing bases from NUREG-1465 to use less conservative analyses, operating reactors did not attempt to do so because of the complexity and expenses associated with the License Amendment Request process required for such a change. This means that there are significant safety margins available that would allow relaxing some of the regulatory requirements associated with the source terms prescribed by NUREG-1465.

As discussed above, the existing protection measures for LWRs against the DBAs reflect the traditional approach for multiple barriers providing DID to limit releases of radiological material. These barriers include fuel cladding, RCS pressure boundary, and containment. As mentioned earlier, the LWR containments are designed to control the leakage of radioactive material following the DBAs and their performance criteria are defined as an allowable leakage rate. The same protection measures and performance criteria may not be applicable or adequate for non-LWR technologies since they have different design, fuel, coolant, and operating conditions. These differences prompted the necessity for different approaches to meeting the fundamental safety function of limiting the release of radioactive material. In response to this need, a "functional containment"

concept was developed and approved after extensive collaboration between the NRC and industry stakeholders by SECY-18-0096 [40].

The NRC proposed a methodology for functional containment performance criteria that is based on the NRC's objective to use risk-informed, performance-based approaches in regulatory decision-making. A "Bow Tie" analysis technique [41] presented in Figure 4-2. Figure 2-1 was selected as the method for functional containment performance criteria selection.

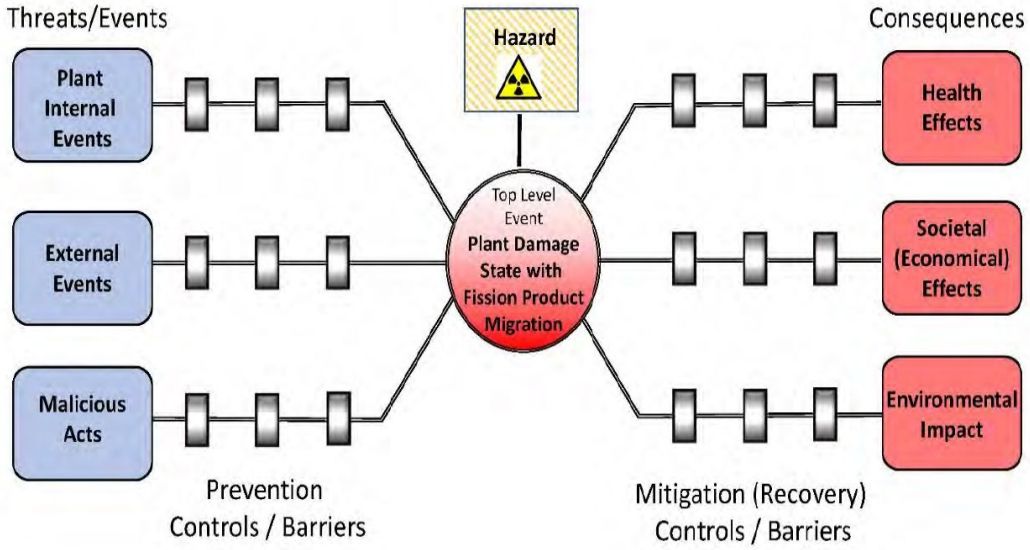

Figure 4-2. Risk Management – Barrier Assessment (Bow Tie) Method

The approach for functional containment performance criteria is defined as technology-inclusive, risk-informed, and performance-based. Considered simultaneously are potential consequences associated with a given technology (threats/events in Figure 4-2.) and plant SSCs intended to prevent or mitigate a plant damage state that could result in the unplanned release of radioactive material (mitigation controls / barriers in Figure 4-2.). This approach provides an opportunity to the reactor designers to assess the benefits and related costs of the plant SSCs that are designed to fulfill control and mitigation functions. The number and specific design of SSCs is informed by the identified events, associated hazards (i.e., the amount and form of radioactive materials), and the uncertainties associated with capabilities and availability of other controls and SSCs [40].

The functional containment concept can be leveraged to extract benefits for operating reactors by using the same risk-informed and performance-based approach where containment performance criteria could be defined in the same manner as proposed by SECY-18-0096 instead of a leak rate. To achieve this, realistic mechanistic source terms must be determined considering performance of fuel and RCS pressure boundary based on improved scientific knowledge in fission product release and propagation using modern modeling techniques. The implementation of Accident Tolerant Fuels with more robust properties to retain fission products during postulated accidents potentially expands the benefits that can be realized. The demonstrated safety margins will provide bases for relaxing various regulatory requirements prescribed for accident mitigation and emergency response actions, not to mention potential reduction in requirements for containment leakage testing.

4.1.5 Subsequent License Renewal

The current regulation for SLR is 10 CFR Part 54 [42] where applicants must perform and Integrated Plant Assessment (IPA) which, in short, consists of the following steps [43]:

1. Identify SSCs that are in-scope of Part 54 which are:
    - Safety-related SSCs
    - Non-safety-related SSCs whose failure could prevent accomplishment of safety-related functions

- SSCs relied on for compliance with certain NRC regulations (e.g., fire protection, shutdown operations).

The safety-related functions mentioned above are 1) integrity of RCS pressure boundary; 2) shutdown the reactor and maintain it in a safe shutdown; and 3) prevent and mitigate the consequences of accidents which could result in offsite exposures.

2. For the "in-scope" SSC, identify structures and components that require aging management review which are structures and components that are both passive and long-lived
    - Passive = perform their intended functions without moving parts or without a change in configuration or properties
    - Long-Lived = not subject to replacement based on a qualified life or specified time period.
3. For each structure and component identified in (2), demonstrate that the effects of aging will be adequately managed so that the intended function(s) will be maintained

    - Identify aging effects that could prevent intended functions (e.g., cracking)
    - Identify aging management programs to manage the effects of aging.

The entire process of Part 54 is deterministic-only, as pointed out by the NRC staff during a public meeting on risk-informing the SLR process in August 2022 [43]:

- Scoping is deterministic – *all SSCs* that meet the scoping criteria based on the intended functions must be included
- Screening is deterministic – *all structures and components* that are passive and long-lived must be included
- Aging management review is deterministic – for *each* structure and component, demonstrate that the effect of aging will be adequately managed so that *intended functions* will be maintained.

The NRC staff maintains the position that PRA (i.e., risk-informed approach) can be used "as a **supplemental tool** in the renewal applicant's Integrated Plant Assessment, and as a supplement **to the primarily deterministic methods for the screening methods and aging management approaches** [43]." The reason for PRA being only a supplemental approach is that the aging data and models are not yet developed for many SSCs and there are no established criteria to evaluate the PRA results. Therefore, in the NRC's opinion, PRA alone is not an acceptable basis for the exclusion of SSCs from the scope of Part 54.

The important capability that PRA models possess is the representation of relationships and dependencies between SSCs and their individual and combined effectiveness to prevent or mitigate undesired events, specifically those that could lead to a release of radioactive material. As such, PRA is a very capable tool to identify SSCs that are the most influential to the risk metrics (i.e., risk-significant SSCs). This capability is the basis for the proposed industry initiative to risk-inform some of the SLR processes. As shown in Figure 4-3 [44], the industry position presented by NEI at the RIC-2022 conference [45] is that scoping, screening, and aging management review tasks can leverage risk insights (i.e., provided by PRA) which would allow to focus the aging management plan (AMP) and associated resources on the "key issues". Other risk-informed applications already approved by the NRC—specifically 10 CFR 50.69 for categorization of SSCs [14]—could be used as the basis to allow risk-informing SLR tasks/processes. The NRC and industry are engaged in the collaborative discussions to identify a path forward.

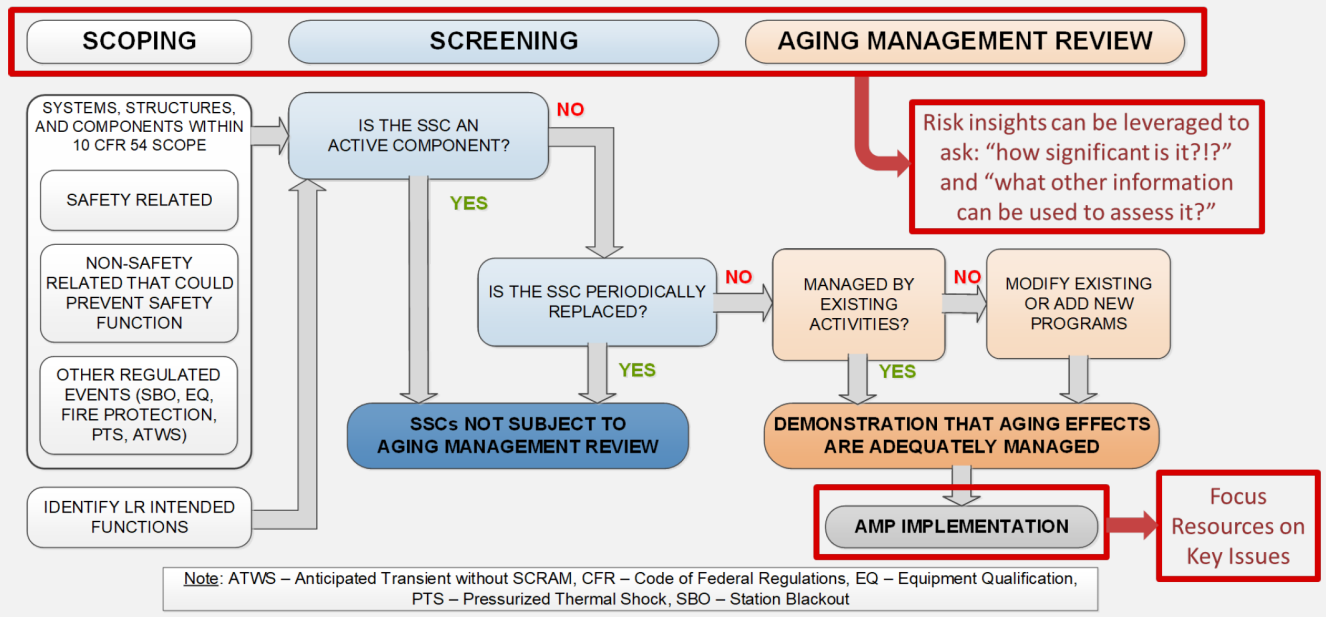

Figure 4-3. Current License Renewal Aging Management Review Process and Proposed Modifications [44]

There is an opportunity to lower SLR-associated burdens for operating power plants if the "in-scope" number of SSCs is reduced. As discussed earlier, NRC does not consider PRA alone an acceptable basis for the exclusion of SSCs to be evaluated as part of the IPA. However, the systems-based approach discussed in Section 3.3 may offer the path forward.

Clearly, a rule change for the "in-scope" SSCs would have a dramatic effect, allowing reduction of the number of systems and components that a plant is committing to for implementation of various AMPs. A systems-based approach Section 3.3 may be the path forward. The SLR process in this approach would focus on satisfying the fundamental objectives (i.e., meeting safety objectives of the Strategic Performance Areas) while allowing licensees a flexibility in the means objectives (i.e., cornerstone areas). Instead of a prescriptive rule defining a list of SSCs that must be included in the scope of SLR, the functional objective can be stated as, for example, "prevention of radiological consequences," which encompasses all three safety functions for safety-related SSC discussed in Section 4.1.1 (i.e., integrity of RCS pressure boundary, ability to shut down reactor and maintain it in safe shutdown, and prevention or mitigation of accidents with a potential of offsite exposures). It will be up to the licensees to identify strategies to meet the functional objective and demonstrate sufficient safety margins.

The strategies to meet safety objectives could be different compared to a simple inclusion of all the safety-related SSCs. Instead, a set of SSCs that are "necessary and sufficient" (i.e., minimal subset of SSCs) to satisfy the functional objective could be identified which potentially can include both safety-related and non-safety-related SSCs. Additional SSCs that have this capability would provide DID to the minimum subset. PRA is a powerful tool to support the selection process since it models relationships and dependencies between SSCs and their effect on the "top event," which can be defined as CDF, LERF, or any other undesired condition or state. A TEPA methodology discussed in Section 4.1.1 could be employed to solve the selection problem along with other methods such as optimization techniques (e.g., discussed in [46] and [47]).

4.2 Plant Analysis and Engineering Opportunities

4.2.1 Equipment Maintenance

To reduce operation and maintenance costs, NPPs are moving from corrective and periodic maintenance to predictive maintenance strategies. Corrective maintenance is performed only when a component fails and is associated with high costs due to component replacement and unexpected system and plant unavailability (e.g.,

loss of generation). Periodic maintenance is performed at specific time intervals based on reliability factors and past operational experience, which is also associated with high costs due to continuous maintenance operations that may not be warranted. The solution lies in predictive maintenance strategies that are designed in such a way that maintenance occurs only when the component requires it (e.g., before its imminent failure). This approach guarantees that component availability is maximized while maintenance costs are minimized [48].

Currently, the NRC ROP uses Performance Indicators which are defined as "*a quantitative measure of a particular attribute of licensee performance that shows how well a plant is performing when measured against established thresholds*" to monitor plant performance in each cornerstone area [24]. The mitigating systems cornerstone employs the Mitigating System Performance Index (MSPI) to monitor the performance of selected systems based on their ability to perform risk-significant functions. The MSPI is comprised of three elements – system unavailability, system unreliability, and system component performance limits, and it is used to determine the cumulative significance of failures and unavailability over the monitored time period [49]. The MSPI is defined as the sum of changes in a simplified CDF resulting from differences in unavailability and unreliability relative to industry standard baseline values. Simply put, the MSPI measures plant system performance by comparing plant-specific unreliability and unavailability values to the industry average values.

The MSPI approach was adopted to use a more objective process for assessing plant safety performance by relying on risk-informed approaches that enable focusing on safety-significant aspects. While the approach serves its purpose, it has some drawbacks. First, the MSPI provides backward-looking information, meaning that index is calculated based on the recent (i.e., quarterly), but still past data. Secondly, MSPI generation is heavy on manual processes to collect and process data which is the constant complaint from the industry. Lastly, the MSPI metric is ultimately a simple comparison of the plant performance to the rest of the industry with negative performance being penalized via various regulatory penalties while "above-normal" performance is not being rewarded.

A better approach would be to use current system health information as the performance measure supported by prognostic information. The system health can be compared to the performance objectives and available safety margin can be used to gain significant economic measures such as switching from prescriptive periodic maintenance to performance-based maintenance of equipment. This approach would ensure that safety is maintained while allowing plants to eliminate maintenance that is not warranted.

4.2.2 Specifications Management

As briefly discussed in Section 3.3, NPPs rely on a greatly outdated specification management process that does not fully address the present-day needs for acquisition of new plant systems. This may negatively affect the ongoing plant modernization activities. For example, many NPPs are currently pursuing modernization of digital instrumentation and control (DI&C) systems. Many non-safety-related systems have been already transitioned from analog to digital technology, but safety-related DI&C systems are lagging due to extensive safety requirements. The current approach for a new system acquisition is to rely on prescriptive specifications for a new system written by the plant staff. These specifications are usually just a repeat of the old system specifications which in the case of analog to digital transformation is a flawed strategy because underlying technologies are completely different.

A different strategy would be to follow an objectives-based approach proposed for NASA's S&MS assurance framework [27]. In this approach, an NPP would specify system functional requirements and potentially some of the performance requirements instead of providing a full-scope specification for the new system. The system vendor will be required to provide assurance to the NPP that all the requirements are met. The assurance can be in form of completed testing and verification, adherence to appropriate design standards, or via alternative strategies. The system acquirer (i.e., NPP) and system provider (i.e., vendor) must establish and agree on both the requirements and assurance strategies to demonstrate that requirements have been met.

An objectives-driven approach places increased responsibility on the vendor to validate adequacy of the system especially in a case of a novel system, such as safety-related DI&C systems. This is a different compared to a prescriptive approach where a system is presumed adequate with respect to acceptable performance by

virtue of compliance. An objectives-driven approach also places new responsibilities on the NPP staff and/or independent technical reviewers to evaluate the vendor's solution. The assurance case can be defined as "*a compelling, comprehensible, and valid argument supported by evidence that a vendor has met the specified objectives.* [27]"

Everett et al. [27] offer a comparison of an objectives-driven approach vs. a prescriptive approach. Traditionally, documentation of compliance with prescriptive requirements is the accepted way to provide the assurance of adequate system performance given that the requirements are complete and valid. The benefit of this approach is the simplicity (i.e., system is either "in compliance" or not). However, there are numerous disadvantages in reliance on prescriptive requirements [27]:

- This reliance places the burden and ownership of system "completeness and validity" on the drafters of the requirements instead of on the system developers
- It promotes a culture of compliance instead of ownership of the system performance
- Prescriptive requirements often place unnecessary burden on the system developers which could result in costly system modifications; without a specific requirement in place, the same performance objective(s) could be potentially achieved by the existing design
- It is difficult to formulate a comprehensive set of prescriptive requirements for novel technologies.

An objectives-driven approach initiates with the system's future owner (NPP) specifying the fundamental system objectives. Then, the system vendor develops a set of "means" objectives which collectively satisfy the fundamental objectives. The assurance process includes verification that the "means" objectives provide reasonable assurance of satisfaction of the fundamental objectives as supported by evidence.

The proposed objectives-driven approach to managing requirements for new systems offers a great opportunity to reduce cost of new systems and potentially shorten the schedule for the system development, verification, and testing which, again, contributes to the system overall costs.

5. CONCLUSION

This report presents findings of the research that investigated opportunities to gain efficiencies and associated economic benefits from modernizing the way regulatory safety assurance is conducted by existing NPPs. The recent advancements in the regulatory framework being developed for advanced nuclear reactors can be successfully leveraged and even expanded to gain such efficiencies.

The investigation conducted as part of this research suggests a regulatory framework that integrates deterministic, risk-informed, and performance-based approaches would allow flexibility for NPP owners and operators in meeting nuclear safety goals. This flexibility, in turn, is expected to reduce any unnecessary burden associated with the current safety assurance processes which would result in cost savings. Multiple areas are identified where the potential for economic benefits exist, as discussed in Section 4.

Additional research via case studies applied in areas with expected benefits is needed. The future work in this area will be based on the feedback from industry stakeholders identifying the areas with the most urgent and/or highest importance needs that can be addressed by application of modernized strategies to the management of NPP safety assurance.

A case study has been already suggested by the industry collaborator for investigation of application of a systems-based approach to management of NPP systems.

6. REFERENCES

[1] NRC WASH-1400, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Comission, NUREG-75/014, 1975.

[2] NRC Policy Statement, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," U.S. Nuclear Regulatory Commission, 60 FR 42622, 1995.

[3] ASME/ANS RA-S-1.1-2022, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," American Sociewty of Mechanical Engineers (ASME) and American Nuclear Society (ANS), 2022.

[4] INL SAPHIRE User Manual, "An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software," Idaho National Laboratorym, SAPHIRE 8 Basic, 2020.

[5] EPRI/NRC NUREG-1921, "Fire Human Reliability Analysis Guidelines," Electric Power Research Institute (EPRI) and U.S. Nuclear Regulatory Commission, 2012.

[6] NRC 10 CFR Part 100, "Reactor Site Criteria," U.S. Nuclear Regulatory Commission, Title 10, Code of Federal Regulations (CFR), Part 100.

[7] N. Siu, "Risk assessment for dynamic systems: an overview," *Reliability Engineering and System Safety,* vol. 43, pp. 43-73, 1994.

[8] N. Siu, *Dynamic PRA for Nuclear Power Plants: Not If But When?,* Technical Opinion Paper, ML19066A390: U.S. Nuclear Regulatory Commission, 2019.

[9] NRC NUREG-1614, "Strategic Plan Fiscal Tears 2022-2026," U.S. Nuclear Regulatory Commission, ML22067A170, Vol. 8.

[10] NRC, "History of the NRC's Risk-Informed Regulatory Programs," [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/history.html. [Accessed July 2022].

[11] NRC 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Title 10, Code of Federal Regulations (CFR), Part 50.

[12] NRC 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Title 10, Code of Federal Regulations (CFR), Part 52.

[13] EPRI RI-ISI, "Revised Risk-Informed Inservice Inspection Evaluation Procedure," Electrical Power Research Institute, 1999.

[14] NRC 10 CFR 50.69, "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors," U.S. Nuclear Regulatory Commission, 2004.

[15] NEI 16-09, "Risk-Informed Engineering Programs (10 CFR 50.69) Implementation Guidance," Nuclear Energy Institute, 2020.

[16] NEI 06-09, "Risk-Managed Technical Specifications (RMTS) Guidelines," Nuclear Energy Institute, 2006.

[17] NEI 04-10, "Risk-Informed Technical Specifications IInitiative 5b, Risk-Informed Method for Control of Surveullance Frequencies," Nuclear Energy Institute, 2007.

[18] NRC RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors," U.S. Nuclear Regulatory Commission, Revision 0, ML20091L698, 2020.

[19] NEI 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," Revision 1, Nuclear Energy Institute, 2019.

[20] ASME Section XI, Division 2, "Requirements for Reliability and Integrity Management (RIM) Programs for Nuclear Power Plants," American Society of Mechanical Engineers, 2019 ASME Boiler & Pressure Vessel Code, Section XI: Rules for Inservice Inspection of Nuclear Power Plant Components, Division 2, 2019.

[21] NRC DG-1383, "Draft Regulatory Guide DG-1383: Acceptability Of ASME Code, Section XI, Division 2, Requirements for Reliability and Integrity Management (RIM) Programs for Nuclear Power Plants, for Non-Light Water Reactors," U.S. Nuclear Regulatory Comission, ML21120A185, 2021.

[22] NRC 10 CFR Part 53, "Part 53 – Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," U.S. Nuclear Regulatory Commission, Title 10, Code of Federal Regulations (CFR), Part 53.

[23] NRC NUREG-0800, "Standard Review Plan for the Review of SafetyAnalysis Reports for Nuclear Power Plants: LWR Edition," U.S. Nuclear Regulatory Commission, ML052340534, 1987.

[24] NRC ROP, "Reactor Oversight Process," U.S. Nuclear Regulatory Commission, [Online]. Available: https://www.nrc.gov/reactors/operating/oversight.html. [Accessed July 2022].

[25] NRC NUREG/BR-0303, "Guidance for Performance-Based Regulation," U.S. Nuclear Regulatory Commission, 2002.

[26] NRC SECY-00-0191, "High-Level Guidelines for Performance-Based Activities," U.S. Nuclear Regulatory Commission, 2000.

[27] C. Everett, R. Youngblood, H. Dezfuli and C. Everline, "Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices," Office of Safety and Mission Assurance National Aeronautics and Space Administration (NASA), 2021.

[28] NRC RI Regulator, "Becoming a Modern, Risk-Informed Regulator," U.S. Nuclear Regulatory Commission, [Online]. Available: https://www.nrc.gov/about-nrc/plans-performance/modern-risk-informed-reg.html. [Accessed July 2022].

[29] NRC 10 CFR Part 50.2, "Part 50.2, Definitions," U.S. Nuclear Regulatory Commission.

[30] M. Humberstone, A. Hathaway, K. Compton and K. Vedros, "Licensing Modenization Project for Operating Reactor," in *ANS 2021 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2021)*, 2021.

[31] ANSI/ANS-30.3-2022, "Light Water Reactor Risk-Informed, Perfromance-Based Design," American Nuclear Society (ANS), 2022.

[32] R. Youngblood, "Multi-State Top Event Prevention Analysis," in *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, 2020.

[33] D. Blanchard, "Categorization and Classification of SSCs for a Current Generation Nuclear Power Plant Using a RIPB Advanced Reactor Standard," in *Probabilistic Safety and Management (PSAM) 16*, Honolulu, 2022.

[34] ASME NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications," The American Society of Mechanical Engineers (ASME), ISBN: 9780791874783, 2022.

[35] V. Yadav and P. H. Burli, "Economic Analysis of Physical Security at Nuclear Power Plants," INL/EXT-20-59737, Light Water Reactor Sustainability (LWRS) Program, 2020.

[36] V. Yadav, R. Christian, S. Prescott and S. S. Germain, "Risk-informed Physical Security Assessment for Nuclear Power Plants," in *Probabilistic Safety Assessment and Management (PSAM)*, Honolulu, Hawaii, 2022.

[37] NRC NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1995.

[38] J. DiNunno and e. al, "Calculation of Distance Factors for Power and test Reactor Sites," U.S. Atomic Energy Commission, Technical Information Document (TID)-14844, 1962.

[39] SAND2008-6664, "Accident Source Terms for Pressurized Water Reactors with High-Burnup Cores Calculated Using MELCOR 1.8.5," Sandia national Laboratories, 2010.

[40] NRC SECY-18-0096, "Functional Containment Performance Criteria for Non-Light-Water-Reactors," U.S. Nuclear Regulatory Commisiion, ML18115A157, 2018.

[41] ISO-31010, "Risk management — Risk assessment techniques," International Organization for Standardization (ISO), IEC 31010:2019, 2019.

[42] NRC 10 CFR Part 54, "Requirements for Renewal of Operating Licenses for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Title 10, Code of Federal Regulations (CFR), Part 54.

[43] A. Hiser and L. Gibson, "Risk-Informing License Renewal, Current Opportunities and Future Potential," U.S. Nuclear Regulatory Commission, ML22214A096, 2022.

[44] EPRI 2020, "Leveraging Risk Insights for Aging Management Program Implementation," Electrical Power Research Institute (EPRI), https://www.nrc.gov/docs/ML2028/ML20287A126.pdf.

[45] B. Titus, "Leveraging Risk Insights in License Renewal," in *U.S. Nuclear Regulatory Commission 34th Annual Regulatory Information Conference (RIC 2022)*, NEI, 2022.

[46] C. Wang, D. Mandelli, M. Abdo, A. Alfonsi, J. Cogliati, P. Talbot, S. Lawrence, C. Smith, D. Morton, S. H. C. P. I. Popova, J. Miller and S. Ercanbrack, "Development and Release of the Methods and Tools for Risk-Informed Asset Management," Light Waret Reactor Sustainability Program, INL/EXT-21-63255, 2021.

[47] Y.-J. Choi, M. Abdo, D. Mandelli, A. Epiney, J. Valeri, C. Gosdin, C. Frepoli and A. Alfonsi, "Demonstration of the Plant Fuel Reload Process Optimization for an Operating PWR," Light Water Reactor Sustainability Program, INL/EXT-21-64549, 2021.

[48] D. Mandelli, C. Wang, R. Christian, E. Birch and S. Lawrence, "Bridging Equipment Reliability Data and Robust Decisions in a Plant Operation Context," Light Water Reactor Sustainability (LWRS) Program, 2022.

[49] NEI 99-02, "Regulatory Assessment Performance Indicator Guideline," Nuclear Energy Institute (NEI), Revision 7, 2013.

[50] NRC SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulations," U.S. Nuclear Regulatory Commission, ML003753593, 1999.

[51] NRC NUREG-2150, "A Proposed Risk Management Regulatory Framework," U.S. Nuclear Regulatory Commission, ML12109A277, 2012.

[52] NRC General Design Criteria, "Appendix A to Part 50—General Design Criteria for Nuclear Power Plants," [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appa.html. [Accessed July 2022].

[53] NRC RG-1.174, "An Approach for using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to Licensing Basis," U.S. Nuclear Regulatory Commission, 2018.

Appendix A: Framework for Implementation of Performance-Based Approaches by Operating NPPs

A-1. Purpose

This appendix offers a systems-based conceptual framework that promotes safe operation while enabling economic success of an operating nuclear power plant. The framework is construed hierarchically so that the higher levels represent more aggregated performance goals and objectives. An example of a high-level performance goal is the protection of public health and safety. Elements at lower levels of the hierarchy represent more granular elements characterized by inclusion of greater detail down to properties at the component level. The hierarchical arrangement enables a logical and formal decomposition of the higher level goals and objectives into lower-level elements in a way that enables consideration of factors from both safety and economic aspects.

The framework as described above can be distinguished from the modeling involved within the PRA construct. The PRA and the proposed framework can both capture performance at a plant level. However, the systems-based framework represents the accomplishment of functional objectives and enables defining performance factors that could be considered necessary and sufficient for decision-making. Also, a systems-based framework relies on the observations of the parameters associated with the established performance objectives. This leads to a different type of decision-making as compared with what has been extensively described and documented in the technical literature as risk-informed decision-making based on a PRA. However, it is important to note that at the highest levels of the hierarchy, the goals of risk-informed and systems-based framework decision-making processes are completely consistent with each other. The systems-based framework enables validation and verification of system performance in a way that supports greater confidence in the predictability of plant-wide performance-based on a logical combination of systems that perform according to established requirements.

A-2. Systems-Based Requirements Management

In a systems-based framework, management of the requirements associated with each objective constitutes the key consideration for success. Performance requirements carry different implications at each of the levels in the hierarchy. At any level and for any performance objective, a particular requirement would be associated with one or more specific parameters based on an acceptance criterion. A requirement is fulfilled if the observations of a particular parameter demonstrate that the associated acceptance criterion has been met. At higher levels in the systems-based framework, performance goals and objectives are more complex which requires establishment of performance monitoring parameters that represent a collection of functions that together offer evidence for adequate system level performance supporting decision-making.

The high-level goals can be decomposed into functions whose successful performance contribute directly to achieving them. Functional performance objectives could be further decomposed into system, sub-system, and component level performance elements each associated with requirements represented by parameters and acceptance criteria.

A-2.1 NRC Example

NUREG/BR-0303 offers an example based on the NRC's ROP for operating plants currently in place to make safety decisions supporting adequate protection of public health and safety. However (as is appropriate in the regulatory context), cost-effectiveness of the requirements is not included as a consideration.

In the ROP, the highest level of the performance objective is termed as the "Mission" and described as "Protect Public Health and Safety in the Use of Nuclear Power." The performance objective under "Mission" is decomposed into "Strategic Performance Areas," which are identified as "Reactor Safety," Radiation Safety," and "Safeguards" [24]. The "Strategic Performance Areas" are further decomposed into seven "Cornerstones."

As applied to the concept of objectives' hierarchies presented in NUREG/BR-0303 [25], the key upshot is that the ROP is a hierarchical decision-making framework in which fulfillment of the performance objectives of the seven "Cornerstones" assures fulfillment of the "Mission." Generalization of this example as a conceptual framework leads to the conclusion that an objectives' hierarchy is a decision-making framework composed of performance objectives that cover the whole range of decision-making involving safety at each operating nuclear power plant. This framework is applied within the operating fleet every day by the NRC's inspection and oversight function. However, consistent with NRC's mission, the process does not include addressing cost-effectiveness of the application of the framework. The responsibility to consider cost-effectiveness falls to the licensee. This becomes eminently possible because the ROP is transparent in the way it is applied. Hence, licensees have considerable flexibility in how the "Cornerstones" are implemented at lower levels in the hierarchy.

Further characterization of the framework leads to the following observation: elements of goals and objectives at the higher levels would entail decision-making through processes that employ highly concentrated information that have the potential for large impacts on significant portions of the scope of the framework. At the level of the "Cornerstones" and below, the performance objectives become more focused on SSCs of specific functional objectives. The value proposition of the "Cornerstones" is that the performance objectives can be related to the evidence gathered in the operating field for decision-making. The evidence thus gathered can be used to validate and verify successful performance at the lower levels in the hierarchy to substantiate assurance that higher level goals and objectives are being accomplished.

A-3. High-Level Performance-Based Guidelines

The feasibility of considering temporal factors for assessing reactor safety was evaluated more than 20 years ago as part of NRC's efforts to implement risk-informed and performance-based regulations. NUREG/BR-0303 documents a process for achieving the outcome objectives of the NRC's definition of a performance-based approach as presented in the NRC's "White Paper on Risk-Informed and Performance-Based Regulation" [50] which includes consideration of temporal factors. The process developed for NUREG/BR-0303 was presented by NRC staff to the NRC in SECY-00-0191, "High-Level Guidelines for Performance-Based Activities" [26].

Appendix A of NUREG/BR-0303 provides the high-level guidelines in a way that facilitates developing performance-based alternatives to issues that were previously treated either prescriptively or by what was termed risk-informed decision-making. Risk information relied on information drawn from a plant's PRA. The high-level performance-based guidelines are sub-divided into three sets of more detailed guidelines called "Viability Guidelines," "Assessment Guidelines" and "Guidelines for Consistency with Regulatory Principles." These sets of guidelines are not hierarchical but sequential in a manner that supports safety decision-making. For the purpose of determining the feasibility of considering temporal factors for assessing reactor safety, the "Viability Guidelines" are the most relevant.

The "Viability Guidelines" offer a step-by-step process to reach an answer to the question, "Can a performance-based alternative which formally conforms with the terms of the NRC's definition of a performance-based approach be developed for the issue at hand?" The implication of posing this question relative to any issue is that a binary choice becomes available to the decision maker: If the answer is "No," then the process has concluded that pursuing an alternative to a prescriptive or PRA-based approach is not worthwhile. If the answer is "Yes," the implication is that the terms of the NRC's definition of a performance-based approach can be met and may be pursued to gain benefits of a performance-based approach including use of temporal factors.

Why would a licensee want to pursue a PB approach? The premise of a PB approach is that a licensee can exercise far greater control over the management of risk at an operating plant and thereby exercise greater control over operating costs. This sets up the basic contrast between a prescriptive approach, which has characterized the way NRC staff has conducted reviews for the operating fleet, and what the NRC has directed that the staff pursue in the future as part of the modernization of the regulatory practice. Hence, a licensee has an option to invoke the NRC's guidance presented in SRM-SECY-98-0144 and formally implement the process

described in NUREG/BR-0303. Any submittal for the NRC review of operating procedures using this basis would have NRC-directed policy as the justification expediting NRC reviews and approvals.

The specific step in the process for implementing the "Viability Guidelines" which brings in temporal factors is the one related to margins. The concept of margins is intimately related to identifying what it takes to formally meet the NRC's definition of a performance-based approach. The safety margin for the purpose of this report is defined as follows:

"Safety Margin: Safety margin is represented as the difference, expressed in consistent terms, between a capacity function (a representation of a system state in a mathematical sense) and a challenge function within the context of a particular scenario. The capacity function is associated with a structure, system or component (or a set of such elements) to represent its time-dependent capability to perform a safety function successfully in a conservatively or a realistically evaluated analysis. The capacity function could be expressed probabilistically in terms of likelihood of successful performance when challenged as specified. The challenge function is defined within the context of the design basis or licensing basis scenario as the limiting or time-dependent conditions imposed on a structure, system, or component (or a set of such elements) due to challenging events. The challenge function could incorporate time-dependent physical parameters expressed in natural or calculated measures (see NUREG/BR-0303) or qualitatively with constructed or proxy measures. A probabilistic representation of the challenge function could be employed provided a suitable basis for comparison with the capacity function is defined in context and in consistent terms."

The definition of safety margin involves identification and characterization of specific system states that would be associated with scenarios important to safety decisions. The first system state that needs to be identified is the limiting condition of the system which lies at the boundary between an acceptable system state and an unacceptable one. This represents the capacity function. The characterization of this state would be represented by a function in which acceptance criteria for parameters are specified. An example of such an expression of a system state can be found in 10 CFR Part 52.47(b)(1) in which an essential part of an application for a design certification called ITAAC (Inspection, Tests, Analysis and Acceptance Criteria) is to be found. An ITAAC is an example of a capacity function as it occurs in the definition of "safety margin." The significance of the ITAAC concept lies in the regulatory application that sets up the outcome of a license application and the safety review in a mathematical form involving a necessary and sufficient set of performance factors which are determinative of "adequate protection." This is stated in the regulation as, "The proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the NRC's rules and regulations. [12]" Hence, the term "adequate protection" represents an acceptance criterion that is an abbreviated form of the phrase from the regulation stating, "…has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. [12]"

The other part of the definition of "safety margin" is a "challenge function," which is a generalized way of representing approaches to safety implementation that could be conventional (based on DBAs), risk-informed (based on probabilistically based scenarios), or performance-based (based on accomplishment of defined performance objectives). These options are usually dealt with separately. A decision-making process would use these options to develop choices to be made by a decision maker.

A-4. Decision-Making Process Options

Operating power plants employ mature decision-making processes and procedures to cater to the needs of regulatory conformance, plant asset management, and cost controls. Details may differ significantly among individual plants, but, generally, best practices are well known and can be observed at most operating power plants. However, as operating licenses were issued 35–50 years ago, the decision-making processes are likely rooted in deterministic and prescriptive frameworks. As part of the movement toward modernization of regulatory processes, in 2012 NRC issued NUREG-2150, "A Proposed Risk Management Regulatory

Framework" [51] to help incorporation of new concepts into regulatory processes. Although NUREG-2150 was not officially adopted into the NRC's procedures, many concepts from it have been gradually incorporated into regulatory practices. Consideration of temporal factors in reactor operations would be facilitated by including NUREG-2150 along with NUREG/BR-0303 for adapting existing decision-making processes to include performance-based methods.

NUREG/BR-0303 offers four process options for decision-making. These are:

1. The Traditional Method
2. The Risk-Informed (RI) Method
3. The Performance-Based (PB) Method
4. The Risk-Informed and Performance-Based (RIPB) Method.

Among these methods, there is robust documentation for best practices in the Traditional Method and the RI Method. Guidance in NUREG-2150 would be useful for pursuing the PB Method or the RIPB Method which involves integrated decision-making. The essential feature of a systems-based framework is the implementation of integrated decision-making processes within the existing decision-making structures by a panel of experts. Most operating plants have some form of such a panel to make choices that have broad impacts throughout the plant.

A-4.1 The Traditional Method:

The traditional licensing process for operating plants employed provisions of 10 CFR Part 50 in two steps to go from design to operating phases. Plants generally went through the construction permit phase by submitting a Preliminary Safety Analysis Report prior to obtaining an operating license based on a Final Safety Analysis Report (FSAR). The FSAR was generally based on requirements spelled out in 10 CFR Part 50.34(a) especially with regard to principal design criteria. 10 CFR Part 50.34(a) refers to 10 CFR Part 50, Appendix A (General Design Criteria) for acceptance criteria related to the principal design criteria [52]. The General Design Criteria were interpreted deterministically and applied prescriptively based on a set of DBAs.

In relation to the "safety margin" definition, a DBA is a postulated event that represents the challenge function against which the capabilities of specific structures, systems and components are compared to assess margins. The postulation of the DBA may be initiated at any of the various modes of operation of the reactor. The time-dependent variation of the parameters associated with the challenge function as applied to any given structure, system or component would depend on the initial conditions, the transient that is postulated and the requirements for the analysis such as consideration of the worst single active failure. The traditional way of dealing with such a complex set of conditions has been to simplify the analysis to make it as conservative as possible. For example, the challenge function for LWR cladding during a postulated LOCA is applied in a "hot channel" at a "hot spot" under a flow transient that is stylized and recognized to be unrealistic. An additional factor that can become significant is the regulatory constraint that such an analysis cannot consider cost impacts by definition of the way "adequate protection" is applied.

Similar considerations could apply to the capacity function in the "safety margin" definition. To maintain conservatism, the capacity function is minimized. In the LWR LOCA example, strength of the cladding to withstand the challenge imposed by the postulated event is minimized by limiting the "hot spot" temperature to 2200°F for Zircalloy fuel cladding including the maximum allowable oxidation. The intent of minimizing strength while maximizing the challenge is to conservatively estimate the safety margin as required by 10 CFR Part 50.34(a).

A-4.2 The Risk-Informed Method:

Promulgation of 10 CFR Part 52 [12] and 10 CFR Part 50.69 [14] gave rise to opportunities to mitigate some of the difficulties of 10 CFR Part 50. Part 52 required preparation of a PRA and offered separate processes

for licenses that covered, among other things, just design or combined design with operation. Additionally, each process permitted by Part 52 relied on Part 50 for its technical requirements. However, Part 52 had several significant differences from Part 50 that offered more flexibility to applicants and licensees. Several of the differences offered alternatives to the strictly conservative ways to specify safety margins. For example, a policy change has made it possible to exclude the single-failure criterion from some safety analyses if risk-informed criteria are shown to apply.

By definition, a PRA is constructed from models that represent SSCs by means of best-estimate parameters applied to their capabilities. Although this is a significant improvement over the Part 50 construct, Part 52 imposes the requirement to include consideration of uncertainty. In practice, this is done in such a formal way that use of PRA becomes prescriptive. Considerations of uncertainty in probabilistic parameters associated with PRA models introduces significant adverse regulatory impacts on predictability of NRC staff reviews. Even though a PRA model may have been developed on the basis of best-estimate parameters, considerations at the event sequence levels employ significant conservatism toward arriving at the end state of the sequence. This conflation of best-estimate and conservatism concepts appears to reduce the effectiveness of using PRA as a tool to mitigate the adverse impacts of the traditional methods. Experience has shown that when cost-effectiveness is considered, conservative estimates in the Traditional Method may offer benefits over the best-estimate plus uncertainty approach because meeting terms of NRC staff review may become too onerous.

Resolving the difficulties with consistently using best-estimate parameters requires a reconsideration of specific parameters at the event sequence level. As an option for a decision-making process, the “safety margin” definition permits characterizing the capacity and challenge functions in terms of best-estimate parameters with uncertainty. A formal approach requires that the comparisons be based on probability distributions rather than point estimates of specific parameters.

A-4.3 The Performance-Based Method:

This method is based on implementing NUREG/BR-0303 in a formal manner to take advantage of the opportunities for flexibility, incentives for improved outcomes, and consideration of temporal factors in the margin estimates. The framework that formally meets NUREG/BR-0303 would offer flexibility with incentives for a licensee to voluntarily seek opportunities to be rewarded with reduced cost impacts. Hence, improvement in outcomes includes better cost-effectiveness.

There can be little doubt that absence of flexibility in the Traditional Method increased costs of operating NPPs without commensurate benefits to safety. In fact, this was an important reason for developing the ROP which resulted in beneficial flexibility for licensees as well as NRC inspectors tasked with oversight and enforcement. The flexibility would not have been possible without a conscious change in policy directed from the NRC level (documented in SRM-SECY-98-0144) to distinguish between prescriptive and performance-based regulations. This change in policy clearly identified the drawbacks of a prescriptive approach with undue emphasis on literal compliance which results in wrong incentives for licensees. Experience showed that existing incentives encouraged generating products and outputs such as documents and reports rather than outcomes that improved functional performance of organizations and systems.

A major example of a change from the compliance-based prescription to a performance-based approach was the issuance of SECY-18-0096, “Functional Containment Performance Criteria for Non-Light Water-Reactors” [40]. The change effected by this action is that a leak-tight containment is no longer needed to be considered as a fundamental regulatory requirement for non-LWRs. This feature of operating LWRs was replaced by the concept of a functional containment that has a performance objective targeting retention of radioactive material. Nothing in the staff’s paper or the NRC’s approval excludes application of the basic principle to LWRs. Some developers of small modular LWRs are likely to employ interpretation of functional containment in licensing applications. One of the consequences of such an interpretation could be that the time related to the rate at which radioactivity is released from the fuel (through a cladding breach) or leakage from the reactor coolant pressure boundary could be specifically included in the analysis to estimate radiation doses from accidents. The time over which radioactivity might be released into and out of the containment boundary is

an example of consideration of temporal factors in safety decision-making made possible with the adoption of a performance-based approach.

Among the improved outcomes that could be sought through a performance-based approach using NUREG/BR-0303 is achievement of two recommendations:

- Performance levels and reliability parameters should be set at the highest practical level.
- Guidance should be given on the extent to which multiple performance parameters that provide redundant information should be used to satisfy the DID philosophy.

In the context of a systems-based framework, setting performance levels at the highest practical level implies that different levels are considered within the decision-making process and optimization judgements are applied. Criteria set at higher levels offer greater flexibility at lower levels of performance objectives. Among the cost saving measures that could be considered within the process is the question of whether imposition of the single-failure criterion is necessary. The same considerations could be applied to question whether a prescriptive code such as ASME's NQA-1 is needed in all the aspects where it is currently used.

A-4.4 The Risk-Informed and Performance-Based Method:

The systems-based framework is highly conducive for incorporation within a systems engineering approach which considers all aspects of a complex project over time from the conceptual design through operations to decommissioning. One of the key documents that deals with integrated decision-making in operating reactors is Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis" [53]. Although this document appears from the title to only apply to risk-informed methods, the substance of the guidance is equally applicable to performance-based methods. NUREG-2150 [51] offers details on making these connections.

The systems-based framework, being a hierarchical structure with processes that execute principles and policies toward an outcome, is a safety assurance approach that is based on combining risk and performance information. If the systems-based framework is constructed and used in a manner consistent with NUREG-2150, it captures existing policies and practices while proposing improvements toward an improved risk management framework. The functional objective is to manage radiological risk through appropriate performance-based controls and oversight. Although the framework addressed in NUREG/BR-0303 was developed with regulatory applications in mind, there is no reason that the structure and processes cannot be adopted for use in design and operation of NPPs.

RG-1.174 offers five principles related to integrated decision-making. These principles could be considered as part of a process in which information is fed into decision-making related to a specific issue. The following addresses the five principles related to integrated risk-informed decision-making:

1. **Current Regulations Met:** This takes account of the flexibility in the regulatory framework provided by the NRC's transformational actions to mitigate prescriptive practices. Taking account of temporal factors may merely be more accurate representation of postulated scenarios. Such instances still count as current regulations being met.
2. **Defense-in-Depth Consistency:** Being consistent with the philosophy of DID is a key requirement for reaching an "adequate protection" finding by NRC staff. The most recent updates to Regulatory Guide 1.174 incorporate the performance objectives to meet the consistency criteria.
3. **Maintenance of Safety Margins:** Implementation of the performance-based approach would be a key basis for obtaining information about the most important safety margins relevant to a given decision. The functional analysis that clarifies the purposes to be served by performance objectives determines which safety margins should be focused on to meet this principle.

4. **Risk-Informed Analysis:** An important consideration in exercising this principle may be the distinction that should be made with a risk-based perspective. As pointed out in SRM-SECY-98-0144, the insights from risk analysis should be given greater importance than the numerical result. The risk-informed analysis will be the best source of information for priority setting and resource allocation.

5. **Performance Monitoring:** This is another key aspect of implementing a performance-based approach. The parameters monitored should be associated with outcomes and performance objectives as closely as practicable. Sound technical judgement from appropriate subject matter experts is likely to be the most important source of information for exercising this principle.

A-5. Summary

There have been substantial changes in the regulatory landscape since the time that most operating plants in the U.S, received their operating licenses. Most of these changes have occurred in the context of demonstrably greater levels of safety at the plants in combination with specific actions taken by the NRC to transform itself into a modern regulatory body. One such change that has not been given sufficient attention is that NRC has adopted a policy of less reliance on strict compliance with the literal meaning of specific requirements as documented in a plant's licensing basis to one of accomplishment of specific functional objectives. Inclusion of this consideration within an analysis and establishing acceptance criteria involves concepts of physical and temporal margins as described in NUREG/BR-0303 [25]. The concepts and methods related to consideration of margins were developed and approved based on specific NRC direction. This does not mean that other NRC direction related to traditional methods or more recently developed risk-informed methods are negated. The approaches presented in this Appendix expands the range of choices available to a licensee to incorporate cost considerations while considering changes to the existing prescriptive requirements.