From:	Rahn, David
To:	Paige, Jason
Cc:	Waters, Michael; Benner, Eric; Alvarado, Rossnyev; Morton, Wendell; Zhang, Deanna; Salgado, Nancy; Mott, Kenneth; Rebstock, Paul; Thomas, Brian; Govan, Tekia
Subject:	FW: Re: Public Meeting Regarding Updating of BTP 7-19 and Long-term Planning of Future DI&C Modernization Efforts
Date:	Tuesday, April 02, 2019 9:00:04 AM
Attachments:	2018 - Denning and Budnitz, Impact of PRA and SAR in reducing reactor risk Progress in Nuclear Energy 102 pp. 90-102 (2018).pdf Comments on NEI Digital I&C Strategy presentation GLJ 20190401.docx

Hi Jason:

I received the attached email from Gary Johnson (former Lawrence Livermore principal investigator on NRC I&C projects). Please include it with your meeting materials for the April 4th public meeting.

Thanks,

Dave

From: Gary Johnson <kg6un@me.com>
Sent: Monday, April 01, 2019 7:06 PM
To: Rahn, David <David.Rahn@nrc.gov>
Subject: [External_Sender] Re: Public Meeting Regarding Updating of BTP 7-19 and Long-term Planning of Future DI&C Modernization Efforts

Hi Dave

The NEI paper referenced in the invitation looks like Warren Odess Gillette's work. That's good news. I've known Warren for a long time. He's a thoughtful and serious guy. My short version of the paper is "Let's use IEC standards". I'm ok with that.

A few notes on the presentation are attached. You've probably heard most of this before.

What we I&C people want is some way to introduce safety factors like the structural folk. It isn't so easy.

Using a ship analogy we DAS is a kind of double hull. I'm thinking that we need something more like a lifeboat.

I think what we are forgetting a couple of things.

Software CCF in the protection system is only one kind of CCF. CCF come about from Design Errors. We don't know how to predict these and we are probably not through with them. Back in the 60's Eppler concluded that the reliability of protection systems could only be about 10-4 per demand and I have reached the same conclusion during by a different path. One of these days, I'm going to collect all of the I&C related Nuclear Safety articles into one document. Those guys were pretty smart.

We now have additional defense in depth systems that didn't exist or weren't so well understood. To my mind if we take credit for these we might find that the risk from CCF of all kinds is not as scary as we thought in 1993.

Richard Denning and Bob Budnitz (a couple of old NRC troopers) wrote a paper discussing some of the improvements made in that last few decades. Attached.

I know Bob well. He was the staff person responsible for producing the Rogavan report and was for a while the director of research.
During my last years at Livermore he was my Associate Division Leader and I still see him in Berkeley from time to time.

Best Regards
Gary

> On Mar 27, 2019, at 6:15 PM, Rahn, David <David.Rahn@nrc.gov> wrote:
>
> <Meeting Announcement April 4 2019 --Revision of BTP 7-19 and Long-Term (Strategic) Assessment.pdf>

Contents lists available at ScienceDirect

Progress in Nuclear Energy

journal homepage: www.elsevier.com/locate/pnucene

Impact of probabilistic risk assessment and severe accident research in reducing reactor risk

R.S. Denning [a], [*], R.J. Budnitz [b]

[a] Consultant, 2041 Hythe Rd, Columbus, OH, USA
[b] Lawrence Berkeley National Laboratory, University of California, USA

ARTICLE INFO

Article history:
Received 6 March 2017
Received in revised form
11 May 2017
Accepted 23 May 2017
Available online 27 June 2017

Keywords:
Probabilistic risk assessment
Severe accident research
Societal risk
Risk reduction

ABSTRACT

The development of probabilistic risk assessment (PRA) as a safety analysis tool and the implementation of lessons learned from risk studies in the design, operation and regulation of nuclear power plants has resulted in a substantial reduction in reactor risk. The lack of a strong technical basis for realistically assessing severe accident behavior, including the release and transport of radionuclides to the environment, resulted in some conservatism in early risk studies that distorted the true nature of severe accident risk. This paper describes the evolution of PRA over the past four decades, the benefits that have been achieved in the reduction of reactor risk, and the changes in the perspective of the nature of severe accident risk associated with the development of a strong technical basis for assessing severe accident consequences. Based on these developments, we conclude that the probability of early containment failure leading to a large, early release of radioactive material to the environment was over stated in these early risk studies. Although it is not possible to preclude the possibility of offsite early fatalities in a severe accident, the probability is extremely small, perhaps below the level at which it should be a key consideration in regulatory oversight. Conversely, as highlighted by the Fukushima accident, the potential for the societal impacts of land contamination represents an important element of reactor accident risk that has received insufficient consideration in the past. These findings have implications regarding preferred strategies for emergency planning and appropriate metrics for risk-informed regulation.

1. Introduction

In many respects, the nuclear industry grew up too quickly. Initial operation of the Shippingport nuclear plant was followed quickly by the Connecticut Yankee plant, the first true pressurized water reactor (PWR) demonstration plant, and the Dresden plant, the first boiling water reactor (BWR) demonstration plant. Before these 300 MWe demonstration nuclear power plants (NPP) had begun to operate, 600 MWe plants and 800 MWe plants had already been ordered, soon to be followed by plants greater than 1000 MWe. As a result, it was not possible to incorporate significant operating experience into the design basis of subsequent generations of reactor designs. Thus, materials problems, such as steam generator tube degradation, and safety lessons, such as those exposed by the Browns Ferry Unit 3 fire and the Three Mile Island Unit 2 accident, had to be addressed by making expensive backfits to existing plant systems.

The objective of this paper is to assess the impact of two specific developments that have had a major impact on the safe design and operation of existing plants and have laid the groundwork for the improved safety of future plant designs: (1) probabilistic risk assessment (PRA) and (2) severe accident research. These developments have led to both a better understanding of the nature of severe accident risk and to an actual reduction in that risk. This paper only addresses the evolution in safety of light water reactors (LWRs), although an improved understanding of severe accident behavior and the application of risk analysis are playing a key role in the safe design of other advanced reactor concepts.

The nature of the hazard associated with the large inventory of radioactive material in an operating nuclear power plant is significantly different from the safety challenge posed by other forms of electricity generation. This difference was recognized by the designers very early through the development of a Defense-in-Depth (Drouin et al., 2016) approach to assuring adequate public safety (as

[*] Corresponding author.
E-mail address: denningrs.8@gmail.com (R.S. Denning).

http://dx.doi.org/10.1016/j.pnucene.2017.05.021

described in Section 2). However, the plants that are currently operating were largely designed, constructed and operated without an in-depth capability to model the response of the plant to off-normal, low probability events beyond the design basis of the plant.

1.1. Risk

Risk is defined as "the possibility that something bad will happen," (Merriam-Webster Dictionary, 2017). *Risk* always has two elements, a consequence characteristic and a likelihood characteristic. When someone assesses whether an action is "safe" or "unsafe", they are actually assessing what the risk of the action is. Thus, when we describe an improvement in reactor safety, we are implying an improvement in reactor risk, either a reduction in probability, a reduction in consequences or a reduction in both. When we cross a street, there is a potential consequence that we will be struck by a car and die (perhaps the ultimate consequence), but by taking appropriate precautions (staying in the cross walk; looking both ways) we determine that the probability of being struck is sufficiently low that we conclude it is safe to cross. We briefly address "safety adequacy" in this paper within the context of the conformance of plant risk to probabilistic safety goals that have been established by the Nuclear Regulatory Commission (NRC). Nevertheless, the question of safety adequacy underlies basic decisions made by owners, regulators and the public in deciding whether or not to maintain or expand the role of nuclear energy in addressing future energy supply needs.

As the result of extensive severe accident research, reactor operating experience, and the application of risk assessment techniques, our technical understanding of reactor accident risk has substantially improved over the past sixty years. The primary value of a risk assessment is generally recognized as the identification of the principal contributors to risk rather than the quantitative (bottom line) results. In fact, risk analysts generally warn against over-emphasis on the calculated risk numbers without consideration of the associated uncertainties. Nevertheless, in this paper we will use the quantitative results from risk assessments to provide a measure of the relative improvement (reduction) in risk that has occurred as a result of changes in plant configuration and plant operations.

The second major topic discussed in this paper is the insight, which has evolved through an extensive body of both experimental and analytical studies, that the likelihood of a major accident that would produce a very early and large release of radioactive material to the environment is much less than had been thought earlier. Conversely, another insight is that the importance of major contamination to off-site property has not received the degree of attention it deserves, either in the regulations or in the considerations of decision-makers at the policy level. The bases for these insights will be discussed in the body of this paper.

The fact that there is an improved technical understanding of NPP risk does not necessarily mean that public *perception* of the risk of NPP accidents has changed. Communicating a technical understanding of risk to the public is extremely difficult. Thus, we will differentiate between a technical understanding of the magnitude of risk, which is the subject of this paper, and public perception of risk.

1.2. Structure of paper

Section 2 of this paper describes the deterministic framework that was developed for the regulation, design and operation of NPPs. Section 3 describes the methodology of PRA, including a description of WASH-1400, the first major application of PRA to address the risk of commercial NPPs (US NRC, 1975). Because of the very limited knowledge of severe accident behavior that existed at the time WASH-1400 was undertaken, before PRA could become a reliable tool for safety regulation it was necessary to undertake sufficient research on severe accident behavior to assure that PRA was not leading to a distorted perspective of the contributors to plant risk. The scope of this research is described in Section 4. Section 5 returns to a discussion of PRA and its broad application to NPPs in the U.S. Section 6 provides our quantitative assessment of the actual reduction in risk of accidents in NPPs currently operating in the U.S. that has resulted from actions taken based on PRA results. This improvement in the understanding of reactor risk has also provided the basis for a future generation of LWRs with even lower risk. Finally, in Section 7 we discuss general misperceptions of the nature of the risk posed by operating plants and provide our own perspective.

2. Development of a regulatory framework, deterministic design criteria, and operating restrictions for U.S. reactors

The regulatory requirements imposed by the U.S. Nuclear Regulatory Commission (NRC) on the safe design, licensing and operation of nuclear power plants are contained in Title 10, Part 50 of the Code of Federal Regulations (US NRC, 2017a). Appendix A to Part 50 identifies General Design Criteria (GDC) that are applicable to all NPPs in the U.S. The GDC codify a safety philosophy built around the use of multiple barriers to the release of radioactive material, a balance of preventive and mitigative safety features, and the use of redundancy and diversity of safety systems. Although the term Defense-in-Depth was not coined until the late 1960s, it is now used as a general description of this underlying approach to NPP safety (Drouin et al., 2016). Some of the key requirements of the GDC are a high level of quality assurance (as detailed in Appendix B of Part 50), protection against natural phenomena hazards, fire protection, leak-tight containment system, emergency core cooling system, negative reactivity feedback, independent reactor shutdown system, and decay heat removal system.

In complying with the GDC and more detailed regulatory guidance documents, *deterministic* design bases are developed by the reactor design organization for safety-related systems. For example, based on a calculation of the increase in pressure that would occur in containment in a major loss of coolant accident of 0.25 MPa, a design basis for the containment might be 0.3 MPa, which includes some safety margin based on established safety codes developed by industry organizations, like the American Concrete Institute. These codes and standards have undergone extensive review by standards committees. The design bases for a nuclear power plant are described in a Safety Analysis Report (SAR) in which compliance with the design bases is demonstrated by the analysis of so-called "design basis accidents." The SAR also includes Technical Specifications that describe the Limiting Conditions of Operation of the plant, such as an identification of the number of safety trains that must be in service for the plant to continue to operate at full power. One of the key design requirements for an NPP is assurance that safety functions can be satisfied even if any single component has failed. This requirement is referred to as the Single Failure Criterion. It is an essential element of the NRC's deterministic approach to safety, in order to provide protection under circumstances in which it is necessary to disable a train of a safety system to perform testing or maintenance while the plant is operating. It also provides protection against a condition in which a safety-related component has failed but its failure has not yet been identified. The Single Failure Criterion is only applied to "active" components, i.e. those components that require some motive force like electricity or a steam turbine or require operator intervention to operate.

The design basis for the strength of the containment structure in currently operating LWRs uses the release of steam to containment for a large loss of coolant accident (LOCA). Because the objective of the leak-tight nature of the containment is to retain the release of radioactive material from the fuel that would occur in a severe accident, this large LOCA design basis assumption acts as a surrogate for containment loads that would occur in a large variety of severe accidents. All BWRs and one class of PWRs (ice-condenser containment design) use pressure suppression devices that condense steam as a means of decreasing the size or strength of the containment for the purpose of reducing cost. Because severe accident loads actually include the production of non-condensable and combustible gases in addition to steam, the likelihood of containment failure has been found to be higher in severe accident scenarios for BWRs than PWRs. This is to a large extent mitigated by the potential for capture of radioactive material in the pressure suppression device (suppression pools in BWRs), which can be substantial as long as the pool is not thermally saturated.

The term "source term" is used in safety analysis to represent the release of radioactive material to the environment. The amount of this release is the source term for assessing environmental dispersion and radiation dose to exposed members of the public. The term is more broadly used to describe the amount of release of radioactive material from fuel and release from the reactor coolant system in addition to the release to the environment. The design basis accident source term used when these plants were originally licensed was developed from a study performed by ORNL and reported in TID-14844 (DiNunno et al., 1962). The "TID source terms" are in many respects inconsistent with current understanding of severe accident source terms. The TID source term assumes a release to containment of 100 percent of the noble gases, 50 percent of the halogens (largely iodine), and 1% of the other fission products in aerosol form. The iodine was primarily assumed to be in the elemental form. Of the iodine released to the containment, 50% was assumed to be captured by removal processes. Based on the TID release to the containment, site dose calculations were performed for each plant to determine exclusion area boundary and low population zone boundary. In this analysis, the containment structure is assumed to leak at its design basis leak rate (in the range of 0.1 vol % per day to 0.25 vol % per day). These boundaries are established to assure that someone standing at the boundary would not receive a dose exceeding 0.25 sievert (Sv) to the whole body or 3 Sv to the thyroid over a 2 h period for the exclusion area or the duration of the release for the low population zone. A very conservative (95th percentile) site-specific meteorology is used in the analysis. The symptoms of radiation sickness occur at approximately 1 Sv. Thus, the siting analysis requirement provides assurance that even for severe accidents, in which the containment remains intact and leaks at its design rate, the consequences to members of the public in the vicinity of the plant will not result in prompt radiation-caused health effects.

When currently operating plants were licensed, there was a two-step licensing process (US NRC, 2017a) in which acceptance of a Preliminary SAR was required before construction could begin and acceptance of a Final SAR was required before the plant could be operated. Because design considerations were evolving rapidly, numerous changes would be incorporated into plant designs during the SAR review process to address licensing issues and to satisfy the individual preferences of the utility. As a result, the approximately one hundred (currently 98) nuclear plants operating in the U.S. are each unique in some respect. This has had both safety implications and cost implications associated with the length of time required to obtain an approved license. It has also led to the need for plant-specific risk assessments for virtually every plant. Future plants, like the AP-1000 reactor (Westinghouse, 2017), will be licensed according to a revised process (US NRC, 2017c) in which a reference design is approved by the NRC and a single-step combined construction and operating license is approved, as long as the applicant does not deviate from the approved reference design.

Subsequent to the atomic bomb attacks at the end of World War II, the public became very aware of the potential health effects of exposure to large doses of radiation. Thus, there was fear that a major release of radioactive material from an NPP could have substantial public health implications. If private companies were to design, build and operate nuclear power plants, their liability exposure would be large and considered unacceptable from an investment viewpoint without some federal protection and a means to provide insurance coverage. In 1957 in order to support legislation that would provide a pool of insurance funding, a study was supported by the U.S. Atomic Energy Commission (AEC) and performed by Brookhaven National Laboratory (BNL) to assess the potential consequences of a worst case accident scenario (US AEC, 1957). Lacking the ability to realistically model severe accident scenarios, three possible radioactive material release scenarios were examined for a range of meteorological conditions. Ranges of consequences were calculated for area of land contamination, number of injuries (radiation sickness) and fatalities from a lethal dose of radiation. The estimated frequency of major releases was subjectively assessed as 1E-5 per yr to 1E-9 per yr. The most severe scenario was assumed to result in the release of 50% of the core inventory of noble gases and halogens (iodine) for a 500 MW(thermal) reactor. Up to 3400 early fatalities and up to 43,000 early injuries were estimated depending on meteorology and the conditions of release. The BNL study (typically referenced by its document number WASH-740) also concluded the potential existed for contaminating large areas of land to a level restricting use for crops. The very conservative, non-physical assumptions made in this study resulted in a perspective about the potential consequences of an accident at an NPP that is vastly different from the current technical perspective obtained from the results of more mechanistic studies, as will be discussed in Section 6.

3. Development of probabilistic risk assessment (PRA) as a safety analysis tool

As the nuclear industry began a major expansion in the 1960s, public concerns rose about the safety of nuclear power plants, particularly as the size of the plants began to grow. The potential value of an assessment of the risk of nuclear power was recognized, although with some concern as to whether it would be possible to realistically assess the probability of core damage events with such a limited data base (US NRC, 2016). In 1972, the AEC initiated a planning activity to develop a methodology to be used in a comprehensive assessment of accident risk in NPPs. The methodology that was developed, PRA, relies on reliability tools in use in other disciplines, in particular the aerospace industry. Specifically event trees (ET) are used to characterize the relationships among the success or failure of major systems providing critical safety functions and fault trees (FT) are used to calculate the failure probabilities of systems using basic component failure data. In some respects this FT/ET approach is particularly well-suited for the analysis of accidents in nuclear reactors, whose safety relies on multiple redundant and diverse standby safety systems.

In the PRA process, risk is represented as an ensemble of triplets that address the questions: What can go wrong? How likely is it? What are the consequences? Risk is thus comprised of (1) the identification/definition of scenarios, (2) the associated frequencies (or probabilities) of those scenarios, and (3) the associated consequences of those scenarios. A scenario begins with an initiating event (e.g. loss of offsite power). Depending on the success or failure of safety systems, that initiating event will be coped with without significant consequences or will lead to various levels of consequence depending on which systems succeed or fail. Initiating events typically occur with sufficient frequency that a database exists from which the frequency of occurrence can be determined. Because of the redundancy and diversity of safety systems in a nuclear power plant, in order for an event to result in significant consequences, multiple faults must occur. The overall frequency associated with the combination of the occurrence of an initiating event with the probabilities of multiple failures of systems is small and cannot be quantified directly based on experience. However, the ET/FT methodology decomposes the risk in a manner that uses the database that does exist on component failure probability with Boolean logic to deductively assess the probability of core damage given an initiating event. In combination with the known frequency of initiating events, the overall risk can be quantitatively assessed.

In general, there are limited data on which to base the analysis of the failure probability of full systems, such as the emergency core cooling system, under accident challenge conditions. This is particularly true of redundant systems, for which the loss of function depends on multiple faults. In practice, the most likely source of multiple failures is found not to be the result of the combination of random failures of multiple components but rather due to common cause failures. For example, one type of common cause failure involves maintenance errors, such as an error in the replacement by a technician of a pump seal on the same component in each of three safety trains with the wrong type of seal. Thus, in an accident when the component is called on to operate, not only one component fails but all three redundant components fail. Another type of common cause failure involves the direct impact of the initiating event on redundant components, such as in a fire or a seismic event. Approaches to the quantification of common-cause failure probabilities have been developed that can be effectively implemented within the context of FT/ET methodology (Fleming et al., 1986). Although there are other approaches that can be taken in assessing nuclear power plant risk, the term PRA is usually synonymous with FT/ET methodology. However, using PRA to study reactor safety goes well beyond using FT/ET methods for modeling plant response. For example, probabilistic approaches are also particularly well suited to understanding of containment failure mechanisms and modes, and for modeling the consequences of the release of radioactivity into the containment and later into the environment.

Recognizing the scope of the task to be undertaken in the performance of a major risk study and the ultimate need for acceptance by the technical community, the AEC contracted with Prof. Norman Rasmussen of Massachusetts Institute of Technology to provide technical leadership. Mr. Saul Levine of the AEC staff acted as Project Management Director. The Reactor Safety Study, better known as WASH-1400, was performed over a three year period with a team of over 50 contractors and AEC staff. Much of the work was performed at AEC headquarters with contributions from Boeing Company, Aerojet Nuclear Company, Science Applications, Inc., Lawrence Livermore Laboratory and Sandia National Laboratories (SNL) in the areas of FT/ET analysis. Battelle Columbus Laboratory (BCL) had responsibility for the analysis of severe accident progression and radioactive material release and transport with support from Oak Ridge National Laboratory (ORNL) and Aerojet Nuclear Company. Battelle Pacific Northwest Laboratory had responsibility for offsite radioactive material release and the analysis of offsite consequences. A draft of the final report was issued in 1974. In 1975, the AEC was separated into two separate agencies with the NRC receiving responsibilities for regulatory oversight of NPPs. When the final version of the report was issued in 1975, it was given two report numbers, WASH-1400 (from the old AEC system) and NUREG-75/014 (US NRC, 1975).

WASH-1400 analyzed the risk of two representative reactors, Surry Unit 1, a Westinghouse three-loop, subatmospheric containment PWR in Virginia, and Peach Bottom Unit 2, a General Electric BWR with a Mark I containment design with a toroidal pressure suppression chamber in Pennsylvania. These two reactors were taken as representative of the anticipated population of 100 light water reactors (LWR). Depending on the objectives of the PRA, the scope can be limited to identifying and determining the frequency of severe accident scenarios (Level 1), can include the analysis of severe accident progression, containment failure and release of radioactive material to the environment (Level 2), or can include the calculation of offsite consequences (Level 3) (US NRC, 1983). WASH-1400 was performed as a Level 3 PRA to enable a comparison to be made of the relative risk to the public of a population of nuclear reactors versus other sources of risk to which the public is exposed.

In 1973, the existing capability to model core meltdown behavior was primitive. Some out-of-pile experiments of irradiated uranium dioxide fuel in Zircaloy cladding had been performed by ORNL, some transient experiments had been undertaken in the TREAT facility (Deitrich et al., 1998), and some modeling of core meltdown behavior had been performed at BCL. It was well established that there would be effectively 100% release of noble gases from melting fuel. There was also evidence that there would be substantial release of iodine, cesium and tellurium radionuclides but the associated chemistry was unclear. Thermodynamic analyses indicated that CsI would be the dominant chemical form of iodine relative to the elemental form I_2. However, because there was no experimental evidence of CsI in irradiated fuel rods, “the possibility of CsI being a major chemical form is not sufficiently established to justify consideration in this work (US NRC, 1975).” Although HI was also recognized as a potential chemical form of iodine, the underlying assumption was that iodine would primarily be released in elemental form and that some of this iodine would be converted to an organic iodide in the containment. Organic iodide was of particular concern because it is not effectively removed by deposition processes, such as by the containment spray system. Release fractions were divided into three phases: gap release, meltdown release and vaporization release (associated with gas sparging of the melt during the period when the molten core material is attacking the concrete basemat). Ranges of uncertainty for release fractions in these phases of the accident were developed collaboratively among researchers from BCL, ORNL and Argonne National Laboratory (US NRC, 1975).

In contrast with current modeling capabilities, the characterization of the core, reactor coolant system and containment were coarse: the core region was divided into 5 radial zones (associated with the radial power profile of the core) and 24 axial zones, the water level in the core was tracked as a balance between boiling and makeup, and the rate of hydrogen production from the steam-zirconium reaction was predicted (Baker and Just, 1962). However, the melting temperature of fuel was assumed to occur at the melting temperature of uranium dioxide. The potential for formation of U-Zr-O mixtures with lower melting temperatures and candling down the exterior surface of the cladding was not recognized at the time. There was no assessment made of circulating flow patterns within the core region.

Containment event trees were developed in WASH-1400 to describe the probability of containment failure by different modes: failure to isolate the containment, an in-vessel steam explosion leading to generation of the reactor head as a missile, containment over-pressurization from hydrogen combustion, containment over-pressurization from loss of containment heat removal and non-condensable gas production, and melt-through of the concrete basemat of the containment. In the BWR design, the potential also was assumed to exist for molten core debris to contact and fail the wall of the drywell. In the WASH-1400 analyses, the likelihood of early failure of containment in a severe accident was assessed to be substantial and the associated release of radioactive material to the environment was a large fraction of the core inventory of the more volatile radionuclides.

One of the principal conclusions highlighted in the WASH-1400 Executive Summary was that the risk to the U.S. public from accidents in the anticipated population of 100 NPPs is very small in comparison to other sources of accident risk associated with natural hazards, such as earthquakes and hurricanes, and from man-made hazards, such as aircraft crashes (see Section 6). At a high level, WASH-1400 provided both justification to the public regarding the acceptability of the risk imposed by NPPs and a measure for the NRC to assess the adequacy of regulation. More fundamentally, however, PRA was found to be effective in identifying safety vulnerabilities at NPPs that existed despite what had been considered to be a very conservative deterministic approach to safety assessment. Human error was found to be a major contributor to risk. Some of the plant-specific severe accident vulnerabilities that were identified included the importance of station blackout events (loss of offsite power accompanied by on-site failure of emergency diesel generators), failure of heat rejection in transient accidents, small loss of coolant accidents and the failure of isolation valves separating high pressure from low pressure systems. The latter events, referred to as interfacing system loss of coolant accidents, were of high concern not only because of the potential to result in severe core damage but also for the released radioactive material to bypass the containment building. WASH-1400 also identified some potential threats to containment failure, such as combustible gas explosions.

As a first step in risk analysis, WASH-1400 had a number of limitations. Although the uncertainties in the estimation of core damage frequency and severe accident consequences were recognized as being large, they were treated simplistically (and very subjectively). The study also failed to address fire risk and seismic risk meaningfully, both of which have significant potential for common cause failure. Following release of WASH-1400, the study was subjected to independent peer review (US NRC, 1978). The conclusions of the review were favorable regarding the potential of PRA but identified areas in which the WASH-1400 methodology should be improved. The NRC Commissioners subsequently directed the staff to continue to develop the methodology but, at the current state of methodology, concluded that PRA should not be relied on as the basis for regulatory decisions. Section 4 of this paper describes the severe accident research program undertaken to improve the ability to model severe accident consequences.

In the late 1970s two accidents occurred at U.S. nuclear plants that have had major impacts on plant design (including backfitting of existing plants), plant operations, and regulation. On March 22, 1975, a fire occurred in cabling systems at Browns Ferry Unit 3 in Alabama, which was difficult to extinguish and resulted in the loss of critical safety systems (US NRC, 1976). This event led to major changes in fire safety programs at NPPs including improvements in the separation and protection of safety trains.

On March 28, 1979 an accident occurred at the Three Mile Island Unit 2 (TMI-2) reactor in Pennsylvania that resulted in severe core damage (Rogovin, 1979). Although WASH-1400 had indicated that severe core damage events were credible, the TMI-2 accident not only demonstrated that fact but also displayed many of the WASH-1400 lessons learned, such as the importance of human factors (and human error), transient events leading to core uncovery, and potential challenges to containment integrity (a hydrogen deflagration occurred in the TMI-2 accident with an over-pressure of 0.1 MPa). In the aftermath of TMI-2 two major initiatives were undertaken by the NRC: a research program to better understand severe accident behavior including radionuclide source terms, and research activities to improve PRA methodology. Parallel activities were undertaken by the U.S. nuclear industry and by other countries with NPPs.

In Germany, the WASH-1400 methodology was applied to the Biblis B plant (Verlag Tuev Rheinland, 1980), a German-design of a PWR with a large dry containment. In Reference, (Keller and Modarres, 2005) provide a review of developmental PRA activities that occurred in the U.S. following the completion of WASH-1400. From 1979 to 1984 the NRC undertook the Reactor Safety Study Methodology Applications Program to extend WASH-1400 methodology to additional plant designs and the Interim Reliability Evaluation Program to develop and standardize methods of reliability assessment. Over a similar time period five full-scope PRAs were also performed for U.S. nuclear utilities by the company Pickard, Lowe and Garrick (2008). Sandia National Laboratories (SNL) undertook the Accident Sequence Evaluation Program that included the development of the THERP method for the performance of human reliability analysis (Swain, 1987). These studies made a number of advances in the methodology, particularly in the treatment of uncertainty and in the analysis of accidents initiated by earthquakes and fires.

4. Severe accident research

In 1980 the NRC issued notice of intent (45 FR40101, 1980) to undertake a Degraded Core Rulemaking process to determine whether nuclear power plants “should be designed to deal effectively with degraded core and core melt accidents.” With the support of NRC funding, experimental programs (simulant materials, prototypic materials, in-pile, out-of-pile, separate effects, integral experiments) were performed in the areas of:

- Fuel degradation, cladding oxidation, corium formation (mixtures of U-Zr-O), fuel melting and slumping
- Radionuclide chemical forms and release from over-heated fuel
- Radioactive material retention associated with natural deposition processes and the effects of engineered safety features such as sprays and pools
- Hydrogen combustion including limits of deflagration and flame acceleration
- Steam explosions associated with corium/water interactions
- Molten fuel/reactor vessel interaction and failure
- Molten core-concrete interaction
- Over-pressurization failure modes of steel and concrete containments
- Pressure loads on containment associated with the rapid transfer of heat to the containment atmosphere from the dispersal of fragmented molten core debris in the event of lower head failure while the primary system is at high pressure.

Prior to WASH-1400, severe accident behavior was not explicitly considered in the licensing and regulation of nuclear power plants, other than through the use of TID-14844 source terms for the analysis of design basis accidents. In the early stages of the NRC's severe accident research program, the Source Term Code Package (STCP) (Gieseke et al., 1986) was developed by BCL, which pieced together separate effects models for source term analysis. The STCP was used to explore a range of accident scenarios for a variety of plant designs. A study was also undertaken by the NRC using the tools available in the 1980 timeframe, primarily the STCP, to assess how severe accident behavior could be more realistically included in the regulatory process (U.S. NRC, 1982). The Sandia Siting Study developed five categories of fission product source terms to be used in determining site acceptability (Aldrich et al., 1982). The most severe of these categories included source terms as large as those obtained in the WASH-1400 study. Based on the results of expert elicitations and uncertainty analyses, the NRC also developed a set of conservative but more physically realistic source terms, NUREG-1465, to be used for regulatory applications as an “alternative” to the source term prescription in TID-14844 (US NRC, 1995a).

In this time period, severe accident process-specific computer codes were under development by a number of DOE laboratories in conjunction with major severe accident experimental programs. As a replacement for the STCP, development of a severe accident integrated effects code was undertaken by SNL as the MELCOR (U.S. NRC, 2005) code. The NRC philosophy at the time was to develop a two-tiered analysis approach in which high fidelity models would be developed to address specific severe accident processes, such as hydrogen deflagration, containment behavior, radionuclide chemistry and transport, and core melt progression. An integrated effects code would be developed to support PRA applications. The integrated effects code would have simpler, fast-running models that could be benchmarked against the high fidelity codes. This led to a proliferation of computer codes that would require validation and updating. In practice, as MELCOR development progressed the best features of the high fidelity models were incorporated into the MELCOR code. At Idaho National Laboratory (INL), a parallel development effort was undertaken for the SCDAP computer code. SCDAP had two advantages relative to MELCOR: a more phenomenological modeling of fuel degradation and slumping and a more mechanistic treatment of two-phase flow through coupling with the RELAP code (Siefken et al., 2001). Ultimately, the financial burden of supporting parallel code development activities by the NRC led to the elimination of support at INL. Some development work on RELAP5/SCDAP was continued by INL and separately by a private contractor, Innovative Systems Software, as RELAP5/SCAP-SIM package (Allison and Hohorst, 2010).

Although MELCOR has modeling capability for PWR and BWR plant designs, the initial application studies at SNL focused on PWR scenarios. In this time frame, in the late 1980s, ORNL undertook the modeling of BWR accident scenarios and the evaluation of the effectiveness of BWR safety systems under severe accident conditions with the BWRSAR code (Hodge and Ott, 1990).

In the U.S. the nuclear industry undertook its own degraded core cooling research, under the acronym IDCOR (Buhl et al., 1987). This program focused on a number of areas in which the industry felt that the WASH-1400 models were too conservative and could potentially distort perspective on the magnitude and nature of severe accident risk. The NRC and IDCOR scientists undertook collaborative workshops to discuss such issues as the credibility of the hypothetical containment failure mode (referred to as α-mode) associated with an in-vessel steam explosion that would convert the vessel head into a missile and the magnitude of containment loads associated with high pressure ejection of molten fuel, if bottom head failure were to occur at high primary system pressure. The principal conclusions of the IDCOR project were (Buhl et al., 1987):

- Probabilities of severe accident scenarios are extremely low
- Fission product source terms are likely to be much less than previous studies
- The risks and consequences to the public of severe accidents are much smaller than previous studies and much smaller than the NRC's safety goals
- Major design or operational changes in reactors are not warranted.

In August 1985, the NRC issued a policy statement on severe accidents (US NRC, 1985) in which they withdrew their intent to undertake a Degraded Core Rulemaking, concluding that “existing plants pose no undue risk to the public health and safety.” In 1986 the NRC published a “Reassessment of the Technical Bases for Estimating Source Terms”, NUREG-0956 (Silberberg et al., 1986) describing improvements in the understanding of severe accident phenomena and their impacts on source term magnitude. Following closure of the IDCOR program, the Electric Power Research Institute became the focus of industry-sponsored severe accident research. Just as MELCOR 2 (Humphries et al., 2017) has become the state-of-the-art NRC computer code for the analysis of severe accident behavior, the MAAP5 (EPRI, 2013) code has become the industry's state-of-the-art integrated severe accident analysis computer code. MAAP5 has the advantage of being relatively fast running and of providing consistent, reproducible results for severe accident outcomes obtained by different code users. MELCOR 2 has the advantage of flexible modeling to allow consideration of the effects of severe accident modeling uncertainties.

In addition to the U.S. severe accident research effort, research programs in other countries have also made major contributions to the understanding of severe accident behavior. Experimental research in Germany on fuel pin melting and slumping behavior provided a very important early contribution to improving severe accident modeling capability. France, Japan, Korea, Sweden and a number of other countries have also contributed particularly in large international cooperative programs, such as the Phebus program in France (Clement and Zeyen, 2005). The ASTEC code (Van Dorsselaere et al., 2009), developed with French and German support has capabilities comparable to MELCOR and MAAP. In Reference, (Sehgal, 2012) has provided a comprehensive summary of severe accident research world-wide.

5. Extension of PRA as a tool to support plant design, operations, and regulatory oversight

In order to determine the impact of the results of severe accident research on the assessed risk of nuclear power plant accidents, the NRC initiated a follow-on study to WASH-1400, which involved an analysis of five plants, the two WASH-1400 plants, Surry (PWR, with subatmospheric, large-dry containment design), Peach Bottom (BWR, Mark I containment design), plus Zion (PWR, large-dry containment design), Sequoyah (PWR, ice-condenser containment design), and Grand Gulf (BWR, Mark III containment design). The resulting report NUREG-1150, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Plants,” (US NRC, 1990) also undertook an extensive treatment of uncertainties involving expert elicitation to characterize the ranges of uncertainties. Although a version of the MELCOR code was available to provide some integrated results for accident scenarios, the factors entering into the source term, such as magnitude of release from fuel, retention in the primary and retention in the containment were based on STCP analyses and expert elicitation from panels of experts on ranges of associated uncertainty. A first draft of this report was issued in 1987. However, it received a large number of review comments and underwent extensive revision. The final version was issued in 1990 (US NRC, 1990). A noteworthy feature of the NUREG-1150 effort was the extensive use of numerous topic-specific expert elicitation panels, which was very resource-intensive. The level of effort was so great for this study that it is unlikely a similar approach for the treatment of uncertainty will be used for any PRA in the future.

In 1986, the NRC adopted a set of probabilistic safety goals for the risk to members of the public from severe accidents in NPPs (US NRC, 1986). The Commissi8on stated that it “has established two qualitative safety goals which are supported by two quantitative objectives." The qualitative goals are:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant risk to life and health; and
- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The two supporting objectives are based on the principle that nuclear risks should not be a significant addition to other societal risks. The safety goals address two types of radiologically-induced health effects: early fatalities from radiation sickness and radiation-induced cancer fatalities. In developing quantitative health objectives, the NRC interpreted "not significant" to imply less than 0.1% of other comparable health risks. Within one mile of a nuclear plant, the prompt fatality risk should be less than 0.1% of other accident risks and within ten miles of the plant the increment in latent cancer fatalities due to radiation exposure should be less than 0.1% of an individual's cancer fatality risk. A principal finding of NUREG-1150 was that the risk associated with NPP accidents is very small relative to other risks, even for people living in the close proximity of NPPs (see Section 6 below).

In November 1988, the NRC imposed a requirement for an Individual Plant Examination (IPE) at each U.S. NPP (US NRC, 1988) based on favorable NRC and industry experience with probabilistic analysis indicating "that systematic examinations are beneficial in identifying plant-specific vulnerabilities to severe accidents that could be fixed with low cost improvements." While the IPE analyses emphasized searches for vulnerabilities, another outcome was that the technical staffs at many more U.S. operating plants became aware of the value of PRA methods, severe-accident analysis, and how to apply these ideas at their plants. This cultural shift, still under way, has had a positive impact on reactor safety.

In addressing the NRC requirement for a systematic IPE, the utilities were given the option of performing a PRA or undertaking a less-expensive alternative. Although some utilities chose an alternative to PRA to satisfy this requirement, today every nuclear plant has at least a Level 1 PRA. In addition, the NRC also has a plant-specific PRA for each plant, referred to as a SPAR model (US NRC, 2017d), which has been validated against the utility's PRA model. Utilities use these PRA models on a daily basis to alert operators of potentially vulnerable conditions. For example, if a plant has two trains available to provide a particular safety function and Train A is out of service for testing or maintenance, the plant's on-line risk monitor warns the operator not to take components out of service from Train B. The NRC uses its plant-specific SPAR models for activities such as determining the risk-significance of operational events as potential severe accident precursors (Johnson and Rasmuson, 1996). Because of the success of the IPE program in the identification of plant-specific vulnerabilities for internally initiated events, the NRC extended the IPE requirement for each plant to perform external event analyses (e.g. analysis of accidents initiated by earthquakes or external flooding) in the IPEEE program (US NRC, 2002).

In 1995 the Commissioners issued a policy statement strongly supporting the use of PRA within the regulatory process. The policy statement said in part "*The use of PRA technology should be increased in all regulatory matters to the extent* supported *by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.* " (US NRC, 1995b). Recognizing that ineffective regulatory requirements can divert plant personnel from performing activities that can significantly improve reactor safety, the NRC undertook a comprehensive review to identify regulations that could be more "risk-informed." For example, integrated leak-rate tests of containment integrity before plant restart are very time consuming and directly impact plant capacity factor. In cooperation with the industry, the NRC developed less-time consuming requirements that are focused on the areas of highest potential leakage. Similarly, when changes are made in equipment or testing procedures that would require a change in the plant's operating license, the plant can expedite the regulatory review by demonstrating that the effect of the changes satisfy limits on changes in core damage frequency and large early release frequency, as described in Regulatory Guide 1.174 (US NRC, 2011a).

Within the time period of these changes in the role of risk assessment in reactor regulation, a major accident occurred at the Chernobyl Unit 4 reactor in Ukraine within the former Soviet Union. The lessons learned from this accident had very limited impact on improving the safety of U.S. commercial nuclear power plants. The design-related issues that led to and exacerbated the event were specific to the unique Soviet-designed RBMK reactors (Petrangeli, 2006). The design features of the Fukushima Dai-ichi reactors damaged in an accident in Japan in 2011 were similar to some older U.S. NPPs. However, the specific event leading to severe core damage was very site-specific. The height of the tsunami that destroyed the ability to power systems required to provide adequate heat removal far exceeded the design basis for the plant. In retrospect, it is clear that the process used to establish the design basis for tsunami protection was inadequate. There was sufficient empirical evidence in the Fukushima region of historical tsunamis of equal or greater magnitude that it should have been recognized that the design basis was inconsistent with generally accepted safety principles. A level of protection is required for NPP safety that goes beyond industrial standards for the design of typical safety-related structures like bridges. One of the lessons from the Fukushima accident is the need to risk-inform the design bases of external event threats. Had the design basis for the tsunami barrier been risk-informed, for example to withstand a 10,000 year event, there would have been no core damage. Failure to protect the plant's emergency diesel generators from flooding also reflected a failure of defense-in-depth and safety culture. At the neighboring Dai-ini plant site an emergency diesel generator had been provided with protection against flooding, which was used as a source of emergency power to that site protecting those reactors from the degraded conditions at the Dai-ichi site (National Research Council, 2014). Shortly following the Fukushima accident, the NRC's Near Term Task Force made some recommendations that would significantly expand NRC's oversight into the area of beyond design basis events (US NRC, 2011b). However, the NRC Commissioners have concluded that major changes in regulatory oversight will not be required. Severe accident management guidelines will remain an industry initiative. Hardened vents will be required for each of the Mark I and II BWRs (US NRC, 2015). All U.S. plants have reviewed their ability to respond to a range of natural phenomena hazards including seismic events and external floods. Other than the seismic design basis where reconsideration of the seismic hazard at all U.S. NPP sites was already in progress at the time of the Fukushima accident, the need for design changes at U.S. plants has been limited.

One of the significant post-Fukushima initiatives that has been undertaken involves upgrades to severe accident management guidelines and more extensive training on these guidelines at the plants. The industry has also initiated a program, referred to as the FLEX program, to provide an additional layer of defense-in-depth to address unanticipated safety threats. In this program, mobile equipment is being provided both at each plant site and at regional centers that could be rapidly deployed to provide an additional source of cooling water or electric power for extended scenarios associated with loss of long term cooling or ac power as encountered at Fukushima (Nuclear Energy Institute, 2012). The methods for incorporating FLEX-type safety improvements at the plants into their PRA analyses are still under development at this time.

Although the range of consequences of severe accidents as analyzed in NUREG-1150 reflected the contemporary modeling capability, the range was in large part driven by two aspects of the assessment: 1). The large uncertainties assessed by the technical experts who participated in the expert elicitation process and 2). Simplifications made in the separation of radionuclide release and transport into separable factors (release from fuel, retention in the primary system, release from core-concrete interaction, retention in water pools, retention in containment). This process led to very large overall source term uncertainties, to some extent reflecting the contemporary level of epistemic uncertainty but in part associated with the uncertainty propagation process used in the study. Over the intervening twenty years, considerable additional severe accident research has been performed beyond the status represented by the "Reassessment of the Technical Bases for Estimating Source Terms" (Silberberg et al., 1986) (see Section 4), which has substantially further reduced the uncertainties associated with the phenomena that potentially threaten containment integrity and the release and transport of radioactive material from the core. The MELCOR 2.1 and MAAP 5 codes have matured and been validated against integral effects experiments, like the PHEBUS experiments (Clement and Zeyen, 2005). In order to obtain a contemporary understanding of the impact of these methodological improvements on severe accident source terms, the NRC recently undertook a major project, with support from SNL, called the State of the Art Reactor Consequence Analyses (SOARCA) study (SNL, 2012). Using the best available models, the SOARCA study re-examined the best-estimate consequences of dominant accident scenarios for the Surry and Peach Bottom plants using MELCOR 2.0 to determine the physical response and release of radioactive materials from the plant and the MACCS computer code (US NRC, 1998) to assess off-site consequences. Subsequent to the World Trade Center and Pentagon terrorist attack, the NRC established additional requirements for mitigating the consequences of terrorist attacks on nuclear power plants (US NRC, 2017b). Much of that focus was related to the potential for the draining of water from the spent fuel storage pool as the result of an aircraft crash. Equipment and procedures, called Extensive Damage Mitigation Guidelines, were provided to plant sites to reduce the associated risk. Historically, PRA studies have limited the consideration of recovery and mitigative actions. However, because some of these additional safety measures provided to address risk from terrorist acts would affect the likelihood and consequences of key accident sequences, the SOARCA study also examined the impact of this equipment on the reduction of the risk from key accident scenarios.

The SOARCA analyses indicate that the fractions of the core inventory of key radionuclides released to the environment in risk-dominant scenarios are substantially smaller than those obtained in earlier risk studies and used in regulatory analyses, such as the Sandia Siting Source Terms (Aldrich et al., 1982). In contrast to WASH-1400, in which the probability of early failure of the containment was assessed to be high in some scenarios, more realistic assessments of containment loads and containment strength in the SOARCA analyses indicate that, if containment failure were to occur, it was generally much later in the accident scenario providing substantial time for radionuclide retention mechanisms to be effective. Similarly, in containment bypass scenarios, such as the interfacing LOCA scenario, which has a delayed release but bypasses containment, the effects of deposition in primary and secondary system piping as well as in the auxiliary building were found to substantially reduce the release. In those scenarios involving containment failure, the release of radioactive iodine and cesium isotopes was found not to be dominated by the quantity airborne at the time of failure, as in earlier studies, but by the delayed revaporization of radionuclides from reactor coolant system surfaces into the containment volume after it had previously failed.

In 2012, the results of an NRC task force were released, that had been charged with the development of a more comprehensive, risk-informed, performance-based regulatory approach broadly across all aspects of the regulatory oversight of reactors, materials, waste, fuel cycle and transportation (Apostolakis et al., 2012). However, to date changes to use risk information in NRC regulation in areas beyond nuclear power plant safety have been implemented in only a few cases, in part because if the potential consequences of events are small, the added cost of risk assessment may not be warranted, and in part because in some areas PRA-type methods have not been developed or used.

6. Assessment of changes in reactor risk

As stated in Section 1, the objective of this paper is to discuss and assess the impact of two specific developments that have had a major impact on the safe design and operation of existing plants and have laid the groundwork for the improved safety of future plant designs: (1) the probabilistic risk assessment (PRA) methodology for assessing the risk of reactor accidents and (2) the capability to analyze severe accident progression with the potential for the release of significant amounts of radioactivity to the environment. Reactor safety has also been improved as the result of actions taken to address lessons learned from a few important accidents, in particular the Browns Ferry fire, the TMI-2 accident and the Fukushima accident. The research that has been performed over the past 40 years has resulted in an improved technical understanding of the magnitude and the nature of reactor risk. Improved understanding does not necessarily assure a reduction in risk, however. In order to achieve a reduction in risk actions have to be taken.

A number of major insights into reactor safety arose from the earliest PRAs and the earliest severe-accident analyses. In the intervening decades a steady stream of additional insights have arisen and have been assimilated into the safety philosophy of reactor-safety analysts, owners, operators and regulators. The reactors are much safer as a result. Among the most important were the findings in WASH-1400 that sequences starting with small LOCAs and transients, rather than large-LOCA sequences, were the dominant contributor to overall core-damage frequency (CDF). Similarly the importance of the contributions to CDF of human errors and of common-caused failures were other vital insights arising from WASH-1400. Shortly thereafter, the first industry-sponsored PRAs identified that accidents initiated by earthquakes and internal fires were among the most important contributors to CDF at many plants. This led in turn to major improvements in safety in those areas.

The results of WASH-1400 not only showed the importance of severe core damage to accident risk but highlighted the various potential threats that arise to containment integrity, such as failure to isolate the containment, steam explosions, hydrogen explosions and bypass scenarios. As severe accident research led to improved understanding of these threats, some of the hypothesized threats were found to be of such low probability that they have been dismissed from further consideration. A prime example was the use of a process called Risk Oriented Accident Analysis Methodology

(ROAAM) (Theofanous and Yuen, 1995) to dismiss the α-mode failure of containment described in Section 4. Although α-mode failure had been assessed to have very low probability in WASH-1400, the level of consequences associated with a very large and very early release of radioactive material was quite high and distorted the perspective of consequences potentially anticipated in a core melt accident. The ROOAM approach was also used to address the probability of liner melt-through following lower head failure in a Mark I BWR design. Similarly, more mechanistic models of containment pressurization, hydrogen combustion, direct containment heating if molten core material were to be dispersed in the containment atmosphere if the reactor vessel failed while still at high pressure, and ability of the containment to withstand pressures well beyond design resulted in reduction in the associated probabilities of containment failure and increased delay in the release of radioactive material. These analyses also identified the effectiveness of site-specific offsite protective measures in mitigating impacts on nearby populations.

The initial PRAs considered accidents initiated while the reactor was at full power. During plant outages when the vessel head has been removed, the level of decay heat removal required to cool the core is lower and the inventories of short-lived radionuclides are smaller than when the plant is operating. However, some of the standby safety systems available when the plant is operating are no longer available in a shutdown condition, the containment barrier is no longer closed, and maintenance operations, like welding, represent potential accident initiators. In recent years, utilities have been undertaking risk assessments for plants for accident initiators associated with a shutdown plant. These risk assessments have enabled the plants to better manage the threats associated with the shutdown condition.

All of these PRA insights led to changes in the design and operation of the plants that have substantially improved overall safety. Another major impact of the plant-specific PRAs was identifying which categories of equipment and which operator actions generally suffered from compromises in reliability or efficacy; this led the plants to concentrate resources on those categories, thereby substantially improving their reliability and efficacy. Those improvements, in turn, have played a major role in the huge increase in the plants' on-line availability; the plants now produce electricity about 90% of the time or more, compared to about 50–55% that was typical in the years before the advent of PRA.

6.1. Changes in risk perspective

The principal consequences of concern for severe accidents are:

- Radiological exposures of members of the public at a level of dose sufficiently high, e.g. greater than 4.5 Sv, to result in fatality in the near term, e.g. within thirty days.
- Radiological exposure leading to radiation sickness (early injury), e.g greater than 1 Sv
- Radiation exposure to a population leading, after some latency period, to a stochastic increased likelihood of cancer fatality
- Land contamination sufficient to affect land use, products, commerce, habitability and need for either exclusion or decontamination.

As previously discussed, a high level finding of WASH-1400 was that a population of 100 reactors in the U.S. would represent an extremely small increment to the risks from natural hazards and manmade hazards to which the public is already exposed. Fig. 1 provides a reproduction of the WASH-1400 risk curve (exceedance frequency of an event with consequences equal to or greater than the associated abscissa) of fatalities that would be expected in a population of 100 reactors in the U.S. in comparison with the risk of natural phenomena events (e.g. hurricanes and earthquakes) and man-caused events (e.g. aircraft crashes) to which the U.S. population is exposed but without curves for the individual risk contributors (e.g. hurricane risk). Note that the axes involve logarithmic scales. As indicated in the figure, the additional contribution to fatality risk in the U.S. associated with accidents in

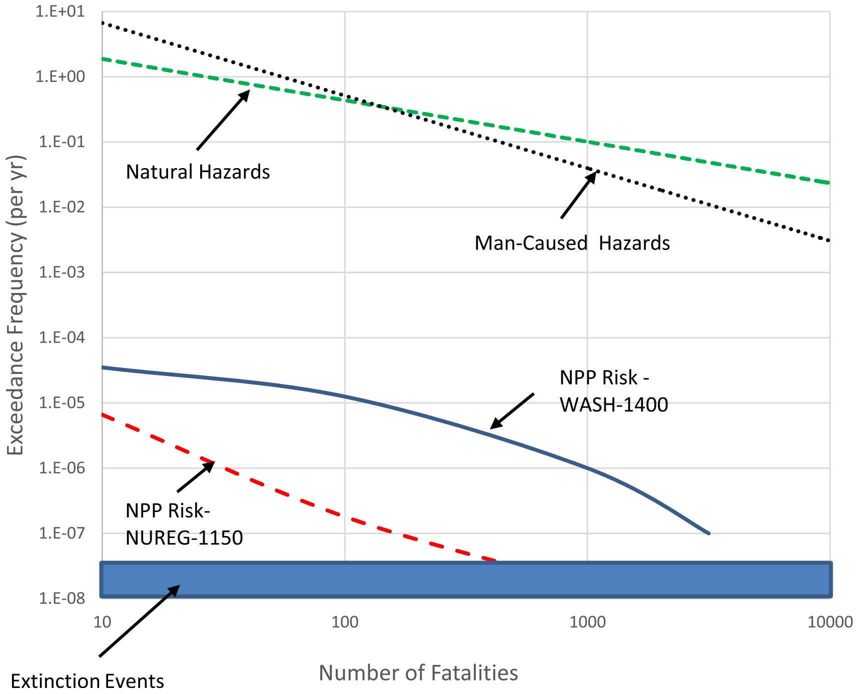

Fig. 1. Comparison between early fatality risk for 100 nuclear power plants and other sources of fatality risk in the United States (Natural Hazards, Man-Caused Hazards, NPP Risk-WASH-1400 are based on Fig. 6.1 and 6.2 in Ref. (US NRC, 1975); NPP Risk-NUREG-1150 is based on Figs. 3.9, 4.9, 5.8, 6.8 and 7.7 of Ref. (US NRC, 1990)).

nuclear power plants was assessed to be less than 1:100,000th (approximately five decades lower) of the background risks.

Although the presentation of risk in NUREG-1150 did not focus on a comparison with other natural and manmade sources of risk as shown in WASH-1400, it is possible to show NUREG-1150 results in this format of an exceedance frequency as illustrated in the bottom curve in Fig. 1. This comparison indicates that the more primitive tools used to assess accident consequences in the WASH-1400 analyses resulted in an over-estimation of the risk by approximately a factor of 10–100 relative to the state-of-the-art at the time of the NUREG-1150 study.

It is important to recognize that the SOARCA study was not a risk study and focused on a few accident scenarios that have tended to dominate risk, such as station blackout scenarios. The results of the SOARCA study are described in terms of latent cancer fatalities because the releases of radionuclides for the scenarios analyzed were too small to produce off-site early fatalities because of their dose threshold nature. The broader implication of the SOARCA study is that the likelihood of early fatalities in a severe accident is at worst extremely small relative to the early fatality risk assessed in NUREG-1150. Because major extinction events (for example precipitated by large meteors) have historically occurred with a frequency of 4E-8 per year, it makes no sense to consider accident frequencies smaller than this value, as indicated by the band at the bottom of Fig. 1. Although it is not possible to completely exclude the possibility of offsite early fatalities in a severe accident based on SOARCA results (Ghosh et al., 2017), we conclude that the likelihood is very small and falls within this band of truly negligible events.

As indicated in Fig. 1, WASH-1400 had demonstrated how small nuclear power plant risks are relative to comparable risks from natural hazards or man-caused events for the average American but had not shown what the risk is for the maximally exposed people living in the near proximity of a plant. The NUREG-1150 report (US NRC, 1990) addresses this risk by comparison with the QHOs. Fig. 2 is reproduced from NUREG-1150. The figure shows that each of the five NUREG-1150 plants easily satisfies the NRC's QHOs by large margin including the associated uncertainties. The smallest margin between the 95th percentile risk for each plant and the safety goal is more than a factor of ten for early fatality risk and approximately a factor of 100 for latent cancer fatality risk. Because the safety goals represent 0.1% of the background risk, the results indicate that people living in the near vicinity of an NPP are exposed to an incremental risk of less than 1:10,000 for early fatality risk and 1:100,000 for latent cancer fatality risk. The SOARCA results further modify this perspective, particularly for early fatality risk, which is assessed to be extremely small relative to the NUREG-1150 mean risk.

In contrast to early fatality risk, the individual latent cancer fatality risks within ten miles for the Surry and Peach Bottom plants are found to be essentially the same between the NUREG-1150 and SOARCA base case (unmitigated) analyses. Nevertheless, there is substantial technical question about the applicability of the linear, no-threshold model used in the calculation of latent cancer fatality risk. The sensitivity of the results has been explored in the SOARCA study. However, the strong support provided to the linear, no-threshold model in the recent BEIR committee report (National Academy of Science, 2006) indicates that obtaining a consensus of technical experts in removing any conservatism in this model will not occur in the near future.

In retrospect, one of the major deficiencies of NUREG-1150 was an insufficient consideration of land contamination as a significant aspect of NPP risk. In the Fukushima accident the radiological exposures of individual members of the public were small (World Health Organization, 2013) but the societal impacts of relocating large numbers of people and of the contamination of land and property have been very high. The NRC's latent cancer fatality QHO is often referred to as a societal risk objective. However, this QHO does not capture the societal impacts associated with relocation of personnel, property loss, interruption of commerce, and decontamination costs that were such a major element of the Fukushima accident. In Reference Denning and Mubayi, 2017 consideration is given to the development of a quantitative societal objective that would provide a limit on the societal cost of NPP accidents. The hypothetical goal is that the societal risk of NPP accidents including the costs associated with property loss and land decontamination should be less than 0.1% of the societal cost of other major events to which the public is exposed, such as hurricanes, earthquakes, epidemics and wars. In this study, the impacts of all events (including fatalities) were monetized as a convenient metric. Using the results of NUREG-1150 sequence frequencies, reduced source terms based on SOARCA findings, and characteristic meteorological conditions, MACCS calculations were performed for four representative plant sites and extended to a full population of 100 plants. The results of the study are shown in Fig. 3. The overall societal risk curve was obtained by monetizing the costs of societally disruptive events over the course of U.S. history inflated to current dollars. Because of the uncertainty in the actual average core damage frequency of the U.S. population of reactors a range of 1E-5 per yr to 3E-4 per yr was considered (shown with hash marks in the figure). The study leading to these results was performed to demonstrate the concept

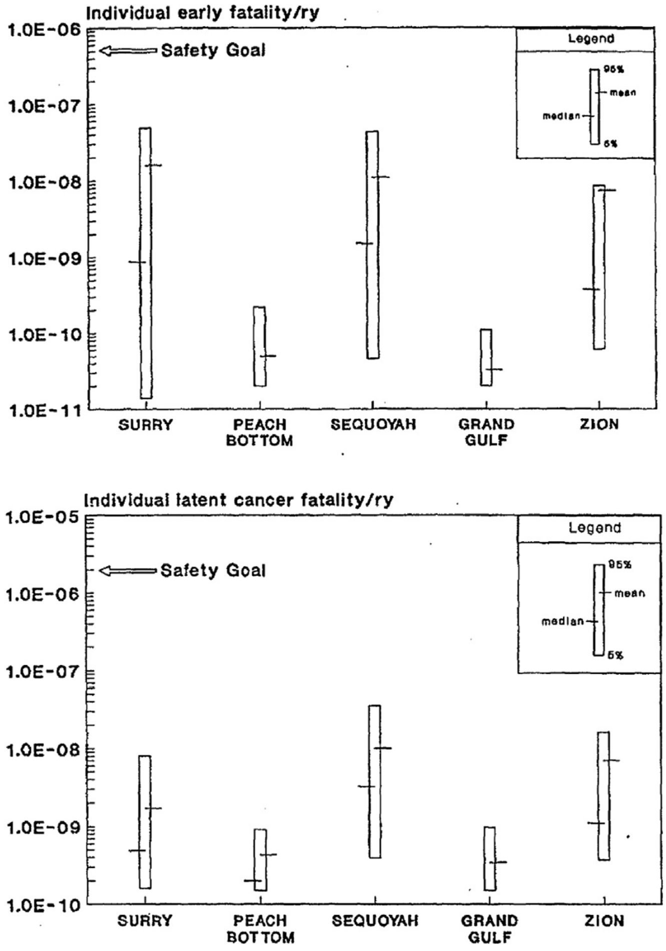

Fig. 2. NUREG-1150 comparison of risks to people living near NPPs with safety goals (Fig. 13.2 of reference US NRC, 1990).

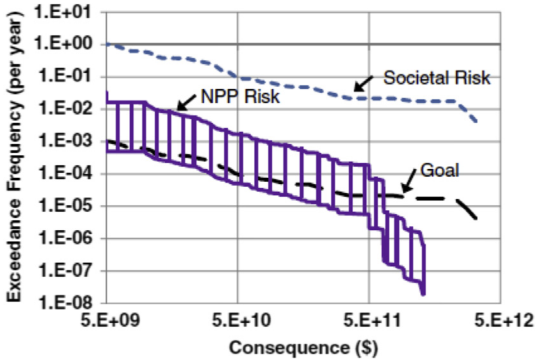

Fig. 3. Comparison of monetized societal risk for 100 plants Vs. Other societal risks (Denning and Mubayi, 2017).

and did not have the level of effort and peer review of the major studies described elsewhere in this paper.

In addition to indicating the potential importance of land contamination and relocation of people as impacts of severe nuclear power plant accidents, the Fukushima accident also illustrated the importance of multiple-unit considerations in risk assessment. In future PRAs it is recommended that more emphasis should be placed on the joint response of multiple units at a site associated with the sharing of some common equipment, exposure to the same external hazard, and impact of radioactive material release from one unit on the ability to prevent severe core damage at other units. These risk insights will provide an improved basis for multi-unit design and operating considerations such as associated with interties among safety systems and for the development of multi-unit siting criteria.

6.2. Changes in reactor risk

In 1957 when WASH-740 was issued the frequency of a severe accident with a major release of radioactive material was subjectively assessed to be in the range of 1E-5 per yr to 1E-9 per yr (US AEC, 1957). Prior to WASH-1400, severe accidents were often classified as "incredible" with an assumed frequency less than 1E-6 per yr.

The overall median core damage frequency for internally initiated accidents in WASH-1400 is approximately 7E-5 per reactor year. This corresponds to an overall mean value of approximately 1E-4 per reactor year. This number is reasonably consistent with actual severe accident experience in LWRs.

Integrating the total world-wide experience with LWRs there have been approximately 10,000 reactor years of operating experience. In that period, there have been two events resulting in severe accidents, the Three Mile Island Unit 2 accident in 1979 and the tsunami at Fukushima Dai-ichi in 2011 leading to the meltdown of three reactors. Depending on whether the Fukushima event counts as one or three events, objectively (based on operating experience) the core damage frequency over the history of LWR operation has been 2E-4 to 4E-4 per reactor year of operation.

The NUREG-1150 PRA involved a number of advances relative to WASH-1400 including consideration of external events for two of the five reactors. The following bottom line mean core damage frequencies are reported in NUREG-1150: Surry (4E-5 per yr internal events; 1.3E-4 per yr external events); Peach Bottom (4E-6 per yr internal events; 9.7E-5 per yr external events), Zion (3.4E-4 per yr internal events); Sequoyah (5.7E-5 per yr internal internal); Grand Gulf 4E-6 per yr internal events) (US NRC, 1990). The two BWR plants (Peach Bottom and Grand Gulf) had lower internal event core damage frequencies than the PWRs. The Zion plant results are particularly interesting because the high core damage frequency is the result of a design vulnerability identified by the systematic nature of the PRA approach. The utility provided a fix to the vulnerability that resulted in a reduction of the internal event core damage frequency to 6E-5 per yr.

The initial focus of PRA was on accidents arising from internal event faults. The risk arising from external events such as the risk from large earthquakes is amenable to analysis using the ET/FT approach but the overall uncertainties in the final risk numbers are quite large, principally because of major uncertainties associated with the frequencies of the initiating events. For example, the principal uncertainty in seismic risk is associated with the characterization of the seismic hazard, specifically the frequency of ground accelerations of different amplitudes at a site. For seismic PRA, considerable effort is placed on assuring that the uncertainty associated with the site-dependent hazard captures the diverse interpretations of various seismic experts. A probabilistic approach is taken to establishing the seismic design basis for a plant that provides high confidence that the seismic risk will be substantially less than 1E-4 per yr. The owner of the plant must demonstrate that given the design basis seismic hazard there is high confidence of a low probability of failure (HCLPF) of safety-related structures, systems and components (Budnitz et al., 1985). In contrast, the design bases for high winds and external floods are based on deterministic criteria involving assumed maximum events, as conventionally used for non-nuclear risks. As indicated earlier, if the tsunami protection for Fukushima had been risk-informed, the accident would have been averted. Consideration should be given to risk informing the regulatory requirements for all natural phenomena hazards.

The risk of internally-initiated fires is potentially a dominant contributor to reactor risk because the initiation frequency is high and there is a high potential for common cause failures. Recent experience with the transition from a deterministic fire protection program to a risk-informed fire protection program as described by NFPA-805 has been a source of contention between the NRC and the industry (National Fire Protection Association, 2015). Nevertheless, we believe that the performance of fire PRA is an invaluable tool in the management of fire risk.

Combining the objective assessment of CDF based on 10,000 reactor-years of LWR experience with the results of WASH-1400 and NUREG-1150, we conclude that the overall mean CDF for the population of U.S. plants prior to the application of PRA analyses to identify vulnerabilities was approximately 1E-4 to 3E-4 per yr. In 2008, the Electric Power Research Institute (EPRI) developed a white paper, "Safety and Operational Benefits of Risk-Informed Initiatives," that discusses how risk-informed initiatives have resulted in an improvement in reactor risk in the U.S. (Gaertner et al., 2008). The paper is limited to the consideration of improvement in CDF, so measures that would have reduced the consequences of accidents are not included. From 1992 (the year in which the IPEs (US NRC, 1988) were completed) to 2005, their assessment indicated that the industry average CDF had decreased by a four-fold factor from 9E-5 per yr to 2E-5 per yr. During this period, the rate of occurrence of "significant safety events" also decreased by a factor of four providing strong evidence that the assessed relative reduction in CDF is real. The EPRI assessment cites a number of risk-informed activities as contributing to risk reduction: the NRC Maintenance Rule, configuration risk management, the NRC's Regulatory Oversight Process, risk-informed allowed outage times, emergency Technical Specification changes, risk-informed mode change assessments, treatment of missed surveillances, in-service inspection, and containment integrity testing. Many of these risk-informed activities have also resulted in improved capacity factors for the plants. Thus, the evidence indicates that CDF has been decreased over the past four decades by approximately a factor of ten (from 2E-4 per yr to 2E-5 per yr) as the result of the application of PRA results to improving reactor safety. Because much of the emphasis in making plant modifications has been associated with sequences with potentially high consequences, such as the interfacing system LOCA event, in which the containment would be bypassed, the average potential consequences of severe accidents has also decreased.

One of the activities undertaken in the SOARCA study was to examine whether mitigative activities as prescribed in NRC's regulation 10CFR50(hh) (US NRC, 2017b) would effectively reduce the probability of dominant accident scenarios in the two plants analyzed. Their results indicated a substantial reduction in the likelihood of key scenarios, in particular ones involving station blackout. Thus, it can be expected that some further reduction in core damage frequency may be found to result from the implementation of mitigative actions, including the use of FLEX equipment. However, in discussing reduction in CDF it is important to recognize the associated uncertainties, particularly for very small CDFs. As the dominant accident sequences are reduced in frequency by scenario-specific fixes, a much larger set of potential scenarios now become relatively more important that may have previously received less detailed attention.

Although the band in Fig. 3 was developed as representing a possible range for the average core damage frequency of the population of U.S. NPPs, it also provides a measure of risk reduction of approximately an order of magnitude representing the change in risk that has occurred as the result of PRA-related improvements. The figure indicates that U.S. NPPs could marginally satisfy the hypothetical quantitative societal objective proposed. However, the factor of difference between the NPP risk and the background of other societally-disruptive events is not as large as that for latent cancer fatality risk or early fatality risk in the existing QHOs.

7. Summary and conclusions

The introduction of PRA as a safety assessment tool has resulted in reduced risk. The structured, logical method of analysis in PRA has been effective in identifying design and operational vulnerabilities that existed despite the inherent conservatism in a deterministic, defense-in-depth design approach. The magnitude of improvement in CDF over the last four decades appears to be approximately a factor of ten, although care must be exercised in trusting the quantitative aspects of PRA. Risk-informed regulatory oversight has been of value to both the regulator and the plant operators in minimizing activities that are ineffective in assuring the safe operation of plants and focusing on risk-significant issues.

The principal impacts of severe accident research have been in improving our understanding of the risk and how to respond to potential severe accidents while they are evolving. Through the development and validation of severe accident analysis codes, this research has provided the technical basis for Severe Accident Mitigation Guidelines, which make it more likely that control room staff and their technical advisors will take appropriate corrective actions that will return the plant to a safe stable state or minimize accident consequences. For example, research on high pressure melt ejection and direct containment heating has led to guidelines for decreasing primary system pressure prior to a time at which vessel failure would occur. Similarly, for a Mark I BWR, severe accident analyses indicate that it is essential to initiate venting from the wetwell prior to the time at which the head of the drywell would fail and provide a direct pathway from containment to the reactor building (a message that was clearly not recognized by the operators at Fukushima).

The objective of PRA is to provide an unbiased assessment of risk including characterization of the associated uncertainties. Crucially, severe accident research has improved our perspective about the magnitude and nature of reactor risk. It is evident that in the early PRA studies, which lacked an adequate basis for the modeling of severe accidents, some modeling assumptions resulted in a significant conservative bias with regard to the timing and magnitude of severe accident source terms. In particular, as understanding of severe accident phenomenology and modeling capability have improved, the assessed likelihood of early failure of containment with a large release of radioactive material has been shown to have been over stated. The two metrics commonly employed in risk-informed regulation are CDF and large early release frequency (LERF). These are considered surrogates for the safety goals. Based on the current state of knowledge, we conclude that it is much less likely than had been assessed earlier that a severe accident would result in off-site early fatalities. This finding has implications for both risk-informed regulation and emergency response planning. LERF no longer appears to be as effective a risk metric as previously thought. At the same time, as demonstrated by the Fukushima accident, the societal impact associated with extensive land contamination in a severe accident is an important element of reactor risk, perhaps more important than the risk of radiation-induced human health effects. Large release frequency (LRF) appears to be a more meaningful risk metric than LERF. It more directly addresses not only societal risks associated with land contamination but also the risk of latent cancer fatalities.

The scope of this paper has been limited to examining the impact of PRA and severe accident research on the current generation of LWRs. Most advanced reactor types (Generation III LWRs, Generation III+ LWRs, small modular LWR reactors with integral steam generators, and reactors with different coolants and fuel forms) are being designed using PRA as a design evaluation tool and are explicitly addressing the need to provide both preventive and mitigative features for beyond-design basis events. For these advanced reactors, as for the existing LWRs, a strong ongoing program of reactor safety research is needed to provide the foundation for understanding and managing the beyond-design-basis risks, and to add to our knowledge base, thereby supporting continuous improvements in safety. The major topics covered here, the understanding of severe-accident behavior and the PRA-based understanding of how accident sequences arise and evolve, have always been (and need to continue to be) major elements of such a research program.

The two major topics discussed in this paper have been (i) how the advent and use of PRA methods have been an important contributor to the significant decrease in overall risk of reactor accidents in the last four decades, and (ii) why, based on an extensive body of experimental and analytical studies, we now understand that the likelihood of an accident that would produce a very early and large release of radioactive material to the environment is much less than had been thought earlier. Conversely, another insight is that the importance of major contamination to off-site property has not received the degree of attention it deserves, either in the regulations or in the considerations of decision-makers at the policy level.

References

45 FR40101, June 13, 1980. Nuclear Power Plant Accident Considerations under the National Environmental Policy Act of 1969.

Aldrich, D.C., et al., 1982. Technical Guidance for Siting Criteria Development. NUREG/CR-2239.

Allison, C.M., Hohorst, J.K., 2010. Role of RELAP/SCDAPSIM in nuclear safety. Sci. Technol. Nucl. Installations.

Apostolakis, G., et al., 2012. A Proposed Risk Management Regulatory Framework.

NUREG-2150. U.S. Nuclear Regulatory Commission.

Baker, L., Just, L.C., 1962. Studies of Metal-water Reactions at High Temperatures III. Experimental and Theoretical Studies of the Zirconium-water Reaction. ANL-6548.

Budnitz, R., et al., 1985. An Approach to the Quantification of Seismic Margins in Nuclear Power Plants. NUREG/CR-4334.

Buhl, A.R., Carter, J.C., Fontana, M.N., Henry, R.E., Mitchell, R.A., 1987. The IDCOR program – severe accident issues, individual plant examinations and source term developments. In: Lave, L.B. (Ed.), Risk Assessment and Management. Springer Science, New York.

Clement, B., Zeyen, R., 2005. The PHEBUS fission product and source term international programme. Proc. Int. Con. Nucl. Energy New Eur. INIS-SI-06-002.

Deitrich, L.W., Dickerman, C.E., Klickman, A.E., Wright, A.E., November 1998. A Review of Experiments and Results from the Transient Reactor Test (TREAT) Facility. ANL/RE/cp-96982, ANS Winter Meeting.

Denning, R., Mubayi, V., January 2017. Insights into the societal risk of nuclear power plant accidents. Risk Anal. 37 (1), 160–172.

DiNunno, J., Baker, R., Anderson, F., Waterfield, R., 1962. Calculation of Distance Factors for Power and Test Reactors Sites. TID-14844.

Drouin, M., Wagner, B., Lehner, J., Mubayi, V., April 2016. Historical Review and Observations of Defense-in-depth. NUREG/KM-009.

EPRI, December 2013. Modular Accident Analysis Program (MAAP5) Version 5.02 – Windows, 3002001978. www.epri.com.

Fleming, K.N., Mosleh, A., Deremer, R.K., 1986. A systematic procedure for the incorporation of common cause events into risk and reliability models. Nucl. Eng. Des. 93 (2–3), 245–273.

Gaertner, J., Canavan, K., True, D., February 2008. Safety and Operational Benefits of Risk-informed Initiatives. An EPRI White Paper, 1016308.

Garrick, B.J., 2008. Quantifying and Controlling Catastrophic Risks, first ed. Academic Press.

Ghosh, S.T., Mattie, P.D. and Sallaberry, C.J., 2017. Uncertainty analysis for the U.S. NRC state-of-the-art reactor consequence analyses, ML12180A434, www.nrc.gov.

Gieseke, J.A., et al., July 1986. Source Term Code Package: a User's Guide. NUREG/CR-4587.

Hodge, S.A., Ott, L.J., 1990. BWRSAR calculations of reactor vessel debris pours for Peach bottom, short-term station blackout. Nucl. Eng. Des. 121, 327–339.

Humphries, L.L., Beeny, B.A., Gelbard, F., Louie, D.L., Phillips, J., January 2017. Reference Manual, Version 2.2.9541 2017, SAND2017–0876 O. MELCOR Computer Code Manuals, vol. 2.

Johnson, J., Rasmuson, D., 1996. The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information. Reliab. Eng. Syst. Saf. 53, 205–216.

Keller, W., Modarres, M., 2005. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor norman C. Rasmussen. Reliab. Eng. Syst. Saf. 89 (3), 271–285.

Merriam-Webster Dictionary, 2017. https://www.merriam-webster.com/dictionary/risk.

National Academy of Science, 2006. BEIR VII: Health Risks from Exposure to Low Levels of Ionizing Radiation. Committee to Assess Health Risks of Low Levels of Ionizing Radiation. National Academies Press, Washington, DC.

National Fire Protection Association, 2015. NFPA 805, Performance-based Standard for Fire Protection for Light Water Reactor Electric Generating Plants.

National Research Council, 2014. Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants.

Nuclear Energy Institute, 2012. Diverse and Flexible Coping Strategies (FLEX), Implementation Guide. NEI 12-06.

Petrangeli, G., 2006. Nuclear Safety, first ed. Elsevier, New York, p. 9.

Rogovin, M., 1979. Three Mile Island, a Report to the Commissioners and to the Public. Nuclear Regulatory Commission Special Inquiry Group.

Sehgal, B.R., 2012. Nuclear Safety, Severe Accident Phenomenology, first ed. Elsevier, New York.

Siefken, L.J., Coryell, E.W., Harvego, E.A., Hohorst, J.K., January 2001. NUREG/CR-6150. SCDAP/RELAP5/MOD 3.3 Code Manual: Code Architecture and Interface of Thermal Hydraulic and Core Behavior Models, vol. 1. Rev 2.

Silberberg, M., Mitchell, J.A., Meyer, R.O., Ryder, C.P., July 1986. Reassessment of the Technical Bases For Estimating Source Terms. NUREG-0956.

SNL, January 2012. State-of-the-Art Reactor Consequence Analyses Project. NUREG/CR-7110, Albuquerque, NM.

Swain, A.D., February 1987. Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772.

Theofanous, T.J., Yuen, W.W., April 1995. The probability of alpha-mode containment failure. Nucl. Eng. Des. 155 (1–2), 459–473.

US AEC, March 1957. Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants. WASH-740.

US NRC, 2017a. Title 10, code of federal regulations, Part 50, Domestic Licensing of Production and Utilization Facilities.

US NRC, “SPAR Model Development Program,” Office of Reactor Safety Research, Division of Risk Analysis, 2017d, https://www.nrc.gov/docs/ML1029/ML102930134.pdf.

US NRC, 2017b. Title 10 Part 50.54(hh), Conditions of License.

US NRC, 2017c. Title 10, code of federal regulations, Part 52, Licenses, Certifications, and Approvals for Nuclear Power Plants.

US NRC, 1975. Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG 75/014).

US NRC, 1976. Recommendations Related to Browns Ferry Fire. NUREG-0050.

US NRC, 1978. Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission. NUREG/CR-0400.

U.S. NRC, 1982. The Development of Severe Reactor Accident Source Terms: 1957–1981,amprdquosemicolon. NUREG-0773.

US NRC, 1983. PRA Procedures Guide. NUREG/CR-2300.

US NRC, August 1986. Safety Goals for the Operation of Nuclear Power Plants. Federal Register, 51 FR 30028, Washington, DC.

US NRC, 1988. Individual Plant Examination For Severe Accident Vulnerabilities. Generic Letter 88-20.

US NRC, December 1990. Severe Accident Risks: an Assessment for Five U.S. Nuclear Power Plants. NUREG-1150.

US NRC, 1995a. Accident Source Terms for Light-water Nuclear Power Plants. NUREG-1465.

US NRC, 1995b. Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities: Final Policy Statement, 60FR42622.

US NRC, 1998. Code Manual for MACCS2, User's Guide. NUREG/CR-6613.

US NRC, 2002. Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program. NUREG-1742.

U.S. NRC, 2005. MELCOR Computer Code Manuals. NUREG/CR-6119, Vol 2, Rev. 3 (SAND2005-5713).

US NRC, 2011a. An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant Specific Changes to the Licensing Basis. R.G. 1.174, Rev. 2.

US NRC, 2011b. Recommendations for Enhancing Reactor Safety in the 21st Century, the Near-term Task Force Review of Insights from the Fukushima Dai-ichi Accident.

US NRC, 2015. Staff Requirements Memorandum Response to SECY-15-0085 – Evaluation of the Containment Protection and Release Reduction for Mark I and Mark II Boiling Water Reactors Rulemaking Activities.

US NRC, August 2016. WASH-1400, the Reactor Safety Study, the Introduction of Risk Assessment to the Regulation of Nuclear Reactors. NUREG/KM-0010,.

US NRC, Federal Register, 1985. No. 153. Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants, vol. 50.

Van Dorsselaere, J.P., et al., 2009. The ASTEC integral code for severe accident simulation. Nucl. Technol. 165 (3), 293–307.

Verlag Tuev Rheinland, 1980. Deutsche Risikostudie Kernkraftwerke, Eine Untersuchung zu dem durch Storfalle in Kernkraftwerken. Germany.

Westinghouse, 2017. AP-1000 Nuclear Power Plant Design. http://www.westinghousenuclear.com/New-Plants/AP1000-PWR/Overview.

World Health Organization, 2013. Health Risk Assessment from the Nuclear Accident after the 2011 Great East Japan Earthquake and Tsunami. Geneva, Switzerland.

Comments on NEI Digital I&C strategy presentation 20190131 Gary Johnson

Slide 6 “Solution #1 - CCF”

(1) If the risk informed approach is looking at the consequences of CCF, well ok. It seems to me that this should already come out of the plant safety analysis of each postulated CCF. I have a feeling that vendors are avoiding doing the analysis. And I also have the feeling that NRC has been inflexible when applying 7-19 to hypothetical events that are in the design basis.

- I was dismayed to learn that NRC required the APR-1400 DAS to deal with CCF for large break LOCAs. This was not required for System 80+ that was the basis for the Korean plant that was a safety upgrade of the 80+.

(2) If it means something like importance measures from an I&C system reliability analysis, I don’t buy it. PSA and fault trees are good tools for assessing failure, but the CCF we are worried about are not that kind of failure. The CCF of concern are human errors introduced during the design. We have no good method for understanding the probability of such failures. Petroski’s book “To Engineer is Human” is a pretty good story about CCF, although he doesn’t talk about it that way.

Slides 8&9

(1) Before the SRP the software guidance came from NQA. That guidance was fine for analytical codes, but not for realtime software. The SRP changed that.

(2) We picked up the IEEE Software standards because we expected that Westinghouse, GE, and others already had good processes that were based upon current software engineering guidance (i.e., IAEA software society standards). Apparently that was not the case.

(3) Nevertheless, the 7-4.3.2 committee picked up the new Reg. Guides without much complaint.

(4) In the mid 90’s we considered IEC 60880 as an acceptable alternative that filtered much of the other guidance to give NPP engineers just what they needed to know. But in the mid-90’s 60880 had too much basic plant content to mesh with the NRC regulations. John Gallagher was the SC45A chairman at that time and pushed to have 60880 simplified and general plant information moved out. This more or less happened. The more general information went to 61513.

- At that time I&C staff in NRR intended to endorse the new 60880, but Jerry Vermeil killed any further work on this idea in NRR. RES wasn’t interested. Not bleeding edge enough.

Slide 10 Barrier #3 - I&C System Architecture Development.

(1) I couldn’t agree more. In 2000 or so, part of the LLNL SRP team worked for GE as an outside reviewer of V&V for the Lungmen project. We were shocked to see how GE was using BTP 14 as a checklist rather than as a short list of fundamental principles to meet attached to a list of suggestions that might be used to confirm that the principles were being met. The answers were always yes. Yes to the relevant things and Yes the irrelevant things. After that we wanted to change BTP-14 into a systems level document, but we didn’t get the chance. Most of our supporters in NRC had retired or died before the 2007 update came around.

Sllide 12 - Limited Functional I&C devices.

(1) I also couldn’t agree more. The original BTP-19 excluded such items because we thought that the BTP didn’t apply. We had the intent to do some more work on this, but it was one more thing taken away from NRR.

(2) BTP-19 came from NUREG 0493. I dare you to match the concerns about limited functional devices to the concerns raised by that report.

(3) My view is that devices of limited functionality are generally not a big CCF concern. Most of these devices have one or more characteristics that limit the problem such as:

A. Not connected to more than one safety channel.

B. Limited functionality

C. Small range of input or output trajectories (sometimes just one division and sometimes just start stop)

D. Use in normal operation is the same as in safety service

E. Surveillance testing closely simulates the range of possible input and output trajectories.

I.e., Not a big harry system involving hundreds of inputs and outputs and cross channel communications.

Still, some thinking is needed to avoid things like the Turkey Point load sequencer, the DB50, the BWR scram volume, and the HFA relay problems.