NUCET NUCLEAR ENERGY AND TECHNOLOGY

Nuclear Energy and Technology 8(2): 77–90
DOI 10.3897/nucet.8.82296

Research Article

Innovation needs in nuclear reactor safety and risk

Francesco D'Auria[1], Romney B. Duffey[2]

1 *University of Pisa, Pisa, Italy*

2 *Idaho National Laboratory, Idaho Falls, USA*

Corresponding author: Francesco D'Auria (dauria@ing.unipi.it)

Academic editor: Boris Gabaraev ♦ **Received** 15 February 2022 ♦ **Accepted** 29 April 2022 ♦ **Published** 27 June 2022

Citation: D'Auria F, Duffey RB (2022) Innovation needs in nuclear reactor safety and risk. Nuclear Energy and Technology 8(2): 77–90. https://doi.org/10.3897/nucet.8.82296

Abstract

After three quarters of a century using nuclear fission to produce energy, Nuclear Reactor Safety and Risk constitutes an established technological sector. A key feature is continuous updating following new discoveries and progress in knowledge, resulting in extensive and elaborate safety methodologies, which are still not internationally accepted, generally applicable or technically consistent. Each country developed its own methods, guides, traditions and requirements to deal with evolving design, safety, siting and licensing issues. There is a clear parallel in societal risk perception between nuclear radiation exposure in accidents and viral infection in pandemics and the fear of the "unknown". Unfortunately, over the last 20–30 years the declining introduction of electricity by nuclear fission in the countries that contributed most to its earliest development also has broken the bond between new scientific advancements and improvements of existing safety methodologies. By looking at the origins and fundaments of nuclear technology, we consider the following topics of both deterministic and probabilistic interest: a) Loss of Coolant analysis; b) nuclear fuel accident performance weaknesses; c) role of containment and ultimate heat sinks; d) residual risk and emergency system deployment, and e) independent and risk informed decision making assessment. As a key outcome, we propose modifying the traditional licensing methodology, and the use of active and/or passive systems by being subsumed into a broader Engineered Safety Features Management process. Furthermore, we emphasize the need of connecting the As Low As Reasonably Achievable principle with the analyses to demonstrate the safety of nuclear installations minimizing the need for excessive "paper" safety analyses and licensing efforts.

Keywords

Nuclear reactor safety, risk, perspectives in licensing of nuclear reactors, independent assessment

Introduction

Nuclear Reactor Safety and Risk (NRSR) constitutes a deep technology anchored on the one hand to the nuclear reactor design and operation and, on the other hand, to the human society. The connection with society has the potential to allow the exploitation of nuclear fission consistently with acceptable risk.

It is difficult or even impossible to classify in a coherent and rational way the existing wide literature dealing with NRSR, including rules, laws, 'atomic acts', etc.: this would require, among other things, resources for issuing and size of the paper well beyond or above the current context.

Rather, in the first part of the paper we focus on selected aspects and concepts that provide a synthetic view of NRSR in an unconventional and conventional way, respectively sections 2 and 3. This constitutes the background for the performed investigation.

Namely we introduce the need to address the question (section 2) 'what is wrong with NRSR and the coupled

societal risk perception?' Although the questions digs in the bottom of human knowledge (technology) and strategy making (politics), we realize the weakness of the question whose relevance depends upon the structure of the society where it applies, in a similar way as the parallel question 'what should be done to remove the ghost coming from the Hiroshima use of nuclear weapon?

Both above questions remain unsolved; possibly they are unsolvable. However, the attempt to address the former question provides the motivations and a road map to arrive at recommendations suitable for a technology (of NRSR) improvement.

Furthermore, the title of the paper opens to the consideration of innovative reactors, fusion reactors, etc. Here we restrict the scope for the use of results from our investigations to existing (large) nuclear reactors. In different terms, reactors designed in the 50's of previous century still provide almost 100% nuclear energy production for electricity generation: the safety of those reactors, including hardware modification, needs 'adaptation' to the latest knowledge and technology progress.

Having in mind key facts associated with the discussion of the former question we restrict the target of the paper to selected features close to our day-life experience. These are, (a) the consideration of the Large Break Loss of Coolant Accident (LBLOCA), (b) the residual risk, and (c) the independent assessment, discussed in sections 4 to 6.

How and where anomalous situations happened

The flawed societal concepts of risk and safety

Initially, nuclear safety was born together with nuclear engineering and the demonstration of the nuclear fission chain and became a dominant aspect of the design of reactors. Considering core damage or melt causing large radioactivity releases, with emergency systems, containment became unavoidable component of a nuclear power plant adding significant cost and licensing complexity. The intent was to reduce potential public radiation exposure, which became a massive mantra of requirements, physical modeling, probabilistic reasoning, complex calculations and national and international regulatory guidance.

These wide ranging and complex procedures within nuclear reactor safety and risk (NRSR) still did not avoid or prevent the unfortunate nuclear, political and financial disasters of Three Mile Island, Chernobyl and Fukushima. Nuclear safety benefitted from technological development, in some cases preceded and imposed that development, USAEC (1990), and the word "risk" became popular after the Rasmussen report, USNRC (1975), being the possibility of exposure to harm. Nowadays Nuclear Reactor Safety and Risk (NRSR) still strictly controls the design, the construction and the operation of nuclear reactors and the supporting research.

Severe initiating events, detailed failure sequences, complicated event trees, procedural human actions, and postulated failure probabilities are combined in producing endless regulations and paper safety cases often far removed from the realities of daily operational requirements and the demands of the commercial market place. The nuclear "scene" quickly became overlaid with well-meaning national energy policies, socio-economic industrial strategies, subsidized power market distortions, commercial and investor self-interests, anti-nuclear factions and continued non-proliferation postures that overshadow truly competitive innovation. Via bi-lateral "technical exchange" or cooperation agreements, the struggle for market share intensified between existing or modified large designs or differing "domestic" variants (e.g. in USA, France, Russia, China, South Korea, Japan, Canada and India, primarily) and multiple small reactor concepts appeared (over 50 at the last count) all vying for government funding and political support as cheap natural gas rendered them uncompetitive.

Fear of the "unknown and invisible" leads to the equally false hope of risk elimination, while how to place *real* risk in its correct context is a vitally important, and widespread societal issue. Nuclear radiation risk has a perfect parallel and a key analogy with viral infection risk especially if we require any potential exposure to harm - no matter how small - is to be avoided or minimized at any cost. Simply compare the reactions to societal and personal exposure to unseen viruses and radiation when the personal risk is actually quite low, except if having pre-existing conditions, co-morbidities or weak immune system response.

During the recent COVID-19 pandemic, the fear of any small but finite risk of exposure to the virus lead the medical profession and political decision makers to require or recommend desperate countermeasures even when the chance of personal harm or adverse consequences was and is extremely low (e.g. imposing stay in or "lockdown" rules, banning travel and certain societal activities, limiting most gathering sizes, restricting outdoor activities, quarantine and testing requirements, and sometimes symbolic public face-masking). These measures are now known to be largely ineffective against the inevitable spreading of viral mutations and societally embedded global infections, as was also the case in the 1918 flu epidemic. Similarly, the fear of any small but finite exposure to radiation leads the medical profession and political decision makers to require or recommend countermeasures, even when the risk of personal harm or adverse consequences was and is extremely low (e.g. also by imposing evacuations or stay in rules, banning travel, limiting exposure times and amounts, plus assuming an arbitrarily linear exposure risk and regulations). Despite the precise countermeasures being different, the parallels are startling, and show the impact of societal risk perceptions, beliefs and psychological reactions, due to the key role of the fear of the unknown reflected in reactive governmental and political decision-making implemented via regulatory rules and restrictions.

Such "public safety" examples become unduly restrictive and distort the scientific facts by incorrectly justifying excessive prudence and risk avoidance, with the well-intended but misguided simplification is to attain the nirvana of "zero' or "tolerable" risk. The protocols, agencies or committees provide "evidence based" guidance for decision-makers allowing public bureaucracies not to be accused of permitting undue or unknown risk exposure; or of not promoting or enforcing all possible or even symbolic remedial risk reduction measures. The resulting fear of the unknown then trumps, indeed emotionally overwhelms any purely rational response. Typical policies and goals invariably avoid using or explicitly mentioning nuclear power as a major contributor, while knowing that adding several thousand Gigawatt reactors by 2050 would be needed just to help stabilize – not even reduce – future atmospheric emissions and CO2 concentrations, Miller et al. (2005).

Therefore, what is wrong with NRSR and the coupled societal risk perception? The key answer is a fact: the production of electricity by nuclear fission is on decline in the countries that originally contributed to its development because of unnecessary fears and unexpected failures – given the availability of alternate fuels like natural gas, and the ability to sub-contract or outsource industrial manufacturing to "cheap labor" sources. This generated lack of attention by young generations and consequent crystallization of decisional structures within (NRSR) organizations, literally resulted in formation of splendid and rigid arrangements like carbon atoms in a diamond. The interaction with the nuclear industry became both standard and weak, i.e. without the impulse and the strength generating the documents USAEC (1971) and USNRC (1975). Hereafter, we cannot refrain to enter trivial reflections (the expert Novak Zuber would call these 'kaffe klatch', Zuber 2010) that spotlight the analysis and contribute a deeper basis for our conclusions.

Evaluating reactor risk and safety

First, terminology is important; however, fashionable changes in nomenclature and revisionist language are not based upon technical investigation or quantitative research and have the potential to bring confusion rather than innovation. The example here is the substitution of: (a) the half-a-century old acronyms Design Basis Accident and Beyond DBA (BDBA) terminology with the terminology Design Basis Conditions (DBC) and Design Extension Conditions (DEC); (b) as an option for safety analysis, of Best Estimate Plus Uncertainty with 'realistic' which is not equivalent; (c) replacing deterministic Hypothetical Core Disruptive Accidents (HCDA) with probabilistic Core Damage Frequency (CDF); and (d) reformulating engineering or expert judgment with fashionable risk-informed decision making (RIDM) schemes as proposed and used in conjunction with PSA/PRA for all existing, advanced or new system safety evaluations supporting licensing decisions, GIF (2011, 2014), USNRC (2004a, 2007a, 2020), CNSC (2008) and Apostolakis et al. (2012). An authoritative institution, e.g. International Atomic Energy Agency (IAEA), even has proposed, or accepted many of those new terms, IAEA (2019a). Adaptation to such new nomenclature may seem ridiculously easy, but 'design' and 'design extension' are a prerogative of country regulatory bodies and not of an international institution. Even worse, 'realistic' is a term embedded into the old 'BEPU', D'Auria (2019), and now is substituting the old term, 'option 4' for safety analysis; the term BEPU remains for 'option 3'.

Second, performance of virtual but not real safety improvement activities happened in the immediate aftermath of the Fukushima accident. Communication media emphatically reported that 'stress tests' confirm the safety of reactors against the sequence of failures that occurred as a consequence of the earthquake and the unanticipated flooding. The concerns are as follows:

- The frequency of the natural event hitting Fukushima was considered too unlikely to require an immediate-urgent and incomplete action. Based on prior data, severe earthquakes and Tsunamis [higher 'amplitude' than the North-East Japan Fukushima ones], were measured since 1960s, and big tectonic fault [the biggest in the world] was known to exist at the location of the Fukushima earthquake; so, inexplicably countermeasures were not undertaken. Geoscientists and informed technicians knew of this, just as technicians knew the weaknesses of the fallen viaduct in Genoa, Italy in August 2018, but no countermeasures were taken until after the event.
- Stress tests of existing operating plants did not imply any physical check of component status. Strictly this could have been of some benefit, e.g. testing capability of diesel generator to survive for 40 plus hours of station blackout, after 40 years of permanence in the reactors buildings, but only documentation control (i.e. paper safety) was performed. The 'stress test' process was aimed at assuring the public, just as imposed on banking and insurance system reserves after the Great Financial Crisis of 2011, but further damaged the seriousness of the people involved and the thrust toward the nuclear technology. The stress tests did not actually 'test' anything: they were just a double check of paper-procedures and QA documents, which are obviously very well done by industry … and very well known that those documents were well written. This was disappointing as actual failure rates were not determined even after the event.

The third consideration has its origins in the 1960's, when design and construction of reactors materialized without a deep understanding of accident consequences, so systematic planning of research according to needs then filled the knowledge gap. Ironically, once suitable knowledge became available, i.e. nowadays possibly

since around the year 2000, the erection of new reactors stopped or slowed down in many countries except by China, Russia and India with their continued state support and preferential funding for large reactors and improved designs. Furthermore, fashionable topics hitting the attention of policy makers and investors and the exigency to keep nuclear laboratory staff working, drove the research in NRSR; available budgets or funding sources rather than needs, then, determine the objective for research and the (presumed) innovation targets. But most R&D today is still focused on so-called "advanced" reactor concepts ideas that, like fusion, have basically existed for 50 years and have not successfully ever penetrated the energy or electricity marketplaces; or on specialized (and expensive) military-type micro-units unsuitable for bulk power systems; or modules and co-generation options that cannot compete with natural gas without subsidies, guaranteed price contracts, and/or emissions credits. This does not prevent the existence of oases of technical progress, like material science and computational methods, useful for many technologies other than nuclear, but does result in wasting ill-directed resources and entrepreneurial funds where enthusiastic but inexperienced concept promoters vie for government development, FOAK and demonstration support funding.

Fourthly, the dramatic events of Three Mile Island, (TMI 1979), Chernobyl (CHE 1986) and Fukushima (FMA 2011) hugely negatively affected the deployment of fission energy, where reactor failures became an emblem for the disaster [*here we do not wish to rewrite the history or replace dozens of books and thousands of documents related to each accident*]. All were avoidable accidents but only afterwards, compounded by human error and insufficient safety margins. Inadequate operating and emergency procedures, plus lack of attention to a number of minor precursors having little or no connection with the nuclear process itself (e.g. minor valve leakage, misleading water level indication, insufficient safety test data, flooded emergency power sources, inadequate containment buildings, …). TMI occurred because of the operators not being aware of a small leak and then misinterpreting the water content and hence deliberately turning off the ECCS and causing the core to overheat. The CHE situation framework resembles the case of a driver crashing a bus against a wall as once shutdown, restart of fission reactions in any core is difficult because of Xenon build-up as the operators tried to restart. The FMA accident lies in the same picture of a broad natural disaster causing 20000+ deaths but the reactors had inadequate back-up ECCS and cooling systems, so causing the core(s) to overheat.

The benefits and lesson learned after TMI triggered important researches for improvement of NRSR and nuclear technology but also lead to the demise of designs using once-through steam generators, and abandonment of nuclear in many parts of Europe. Similarly, CHE started questionable roadmaps for an extended use of passive systems and the complete abandonment of the graphite moderated – channel type – design. FMA led to intensification of researches to understand what should not happen in a highly safety conscious society, but also possibly to the effective abandonment of the BWR pressure-suppression type of containment design and caused even more expensive BDEE requirements and plant shutdowns.

Like studying the death process of passengers following the failure of an airplane, our fourth consideration is the emotional and policy-driven reactions rather than rational and technology-driven consequences that are the follow-up of TMI, CHE and FMA dramatic events. These largely contributed to the nowadays situation. Safety benefit is even "quantified" by incremental changes to the CDF (a "Delta CDF") even when far outweighed by the overall dominant uncertainties inherent in human performance particularly when using current PRA/HRA/HEP methods for modeling unpredictable "human performance'.

Fifthly, consideration is given to two key statements in a recent article [Stakeholder coordination essential for nuclear to innovate, April 6, 2021, Reuters Events, Nuclear]. The first is "*From the utilities, innovation must mean improved safety and lower cost while the regulator considers new technology as something that must be categorized and quantified before it's given the green light amid concerns surrounding the risks of changing a legacy safety system*". The second [attributed to Kemal Pasamehmetoglu, Associate Director at Idaho National Laboratory], asserts "*The issue is not that we don't have ideas. The issue, as we found out, is that getting those ideas to the finish line is difficult in nuclear. It is expensive and quite often people with innovative ideas don't have access to the facilities to test their ideas*". An obvious note is the difference of society and technological contexts compared with late 40's and 60's of the previous century. Today, both nuclear industry proponents and existing regulators appear to be addressing new non-PWR challenges by introducing generalized "technology neutral" and "risk informed" criteria for so-called "advanced" or non-specific "modular" designs but without actually demanding or fully funding the complex technology background, prototype demonstrations and experience necessary for new commercial deployments. As a consequence, researchers (with and without innovative ideas) can get funding to continually perpetuate the current technological status; well-meaning (wealthy) entrepreneurs are persuaded to invest in re-packaged but already known/proven developmental and commercial dead ends; while sincere nuclear business and political supporters provide influence, access and high-level contacts but themselves obviously cannot provide anything new technology. The result is a critical waste of time and resources, avoiding the needed reforms of the embedded fundamental processes.

Sixthly, in principle the modern RIDM concept allows "safety" assessments to nominally encompass uncertainties using some formulation of expert judgment that must be informed by relevant data. The specific Risk Informed Decision Making (RIDM) requirement is ensuring a negligible or "tolerable" probability of core damage for the multitude of possible or potentially different initiating

events or hazards forming the finite BDEE collection or set {flood, fire, hurricane, ice storm, typhoon, earthquake, cyber-attack …}. Quantitative evaluation must include the reliability of 'active' and 'passive' emergency back-up systems to supply or restore power and cooling using applicable and "exchangeable" data for nuclear and non-nuclear systems for a wide range of known catastrophic events. Unfortunately, the risks and uncertainties (both aleatory and epistemic) of core damage caused by prolonged loss of power and cooling may be underestimated in RIDM, today. The governing paradigm used by nuclear plant regulators for quantifying or assessing risk consequence up to now is standard PRA/PSA methods (also promulgated as ASME and ANS "standards") using multiple event trees and Boolean logic sequences, and are deemed "complementary to deterministic analyses", WENRA (2009, 2013). These analyses have not used prior real event information directly, but proscribe and postulate a host of separately classified Beyond Design Basis Extreme Events, BDEE (floods, fires, hurricanes, ice storms, earthquakes etc.) constituting a "hazard group" initiating system failures provoking radiation release and some level of public harm for quantifying or assessing risk consequence. The subsequent probabilities of core damage for differing designs are actually all (directly or indirectly) dominated by the chance and risk of core damage following loss of power and cooling and/or of the ultimate heat sink (LUHS).

In general, the existing RIDM paradigm develops hypothetical *F*-*C* risk-informed boundaries or "performance based" activity release "targets". The implication of any such "limit" or region (whether risk-informed or not), is small, or incremental changes in postulated annual frequency, ΔF, with a large consequence, C, have equivalent relative acceptable incremental safety improvement, risk significance, or decisional "value" as small consequences, ΔC, with large frequency, F. The NEI proposed an allowable "risk significant" annual frequency-consequence evaluation "target" using regulatory public dose exposure limits measured in rem exposure, USNRC (2007b) and NEI (2018). But for core damage with some probability of even negligible activity release, the major fiscal, societal and commercial consequences and risk exposure are really entire plant loss, corporate/company bankruptcy, job termination, clean-up and power replacement costs (as demonstrated by, say, the prior reactor events). So the existing paradigm indeed should protect "public health and safety" but does not protect against any other major risks not within the regulatory focus, purview or duty.

The pillars of NRSR

A comprehensive picture of Nuclear Reactor Safety and Risk needs whole textbooks or even an encyclopedia. A related figure of merit for the size of information at the basis of NRSR derives from considering the Code of Federal Regulations (CFR) in the US and the IAEA in Vienna. Hundreds of CFR and IAEA documents form what is nowadays NRSR: these include thousands of (properly cited) reports and publications. We limit ourselves to comment using snapshot concepts from those documents without introducing rigorous definitions or demonstrating interconnections existing within the NRSR structure. To this aim, we distinguish principles (and concepts), expected achievements and available tools and procedures.

Selected principles and concepts

As *presently* constituted, the NRSR basis can be synthesized as a set of overlapping but complementary principles that provide a complete whole but are themselves interleaved as shown in Fig. 1. These are complementary but separate elements of the overall safety construct and ideally are independent of the design, technology, methods and processes.

ALARA is an operational goal and a foundational principle. As Low As Reasonably Achievable (ALARA) is the translation and use of the good engineering practice driving human civilization, and is equivalent to 'the best one can do'. Cost-benefit studies, Best Estimate Plus Uncertainty (BEPU) approach and Integrated Risk Informed Decision Making (IRIDM) strategy are examples of technology driven or oriented by ALARA.

LNT is an unobtainable aspiration. The Linear No Threshold (LNT) is the principle issued by International Commission for Radiation Protection (ICRP) effectively stating that even very low radiation exposure is harmful. Even though not necessarily mentioned, this principle has the potential to enforce or to stay behind any acceptance threshold within the framework of NRSR. In effect, LNT is the competitor and the alternative of ALARA where the emissions equivalent would be 'even a microgram of CO2 damages the environment' for the automotive industry; or 'any one gram of methane affects climate change' for livestock raising. Radiation hormesis and non-linear effects need proper consideration.

The Safety Goal is a design target. The Safety Goal (SG) is the practical bridge between ALARA and LNT, although it does not mention any of those, e.g. IAEA formulation in IAEA (2006), recently recalled in IAEA (2019b). The current Safety Goal, i.e. to protect humans and environment from ionizing radiations, appears correct provided it refers (explicitly) to ALARA and not to LNT. The Safety Goal is at the origin of Safety Requirements for the design of reactors.

Fail-to-Safe is the desirable end state. The target behind the Fail-to-Safe (FS) principle-concept is ensuring that failure of any structure and/or component adopted for safety purpose shall not aggravate the evolution, complexity and consequences of any accident. In the past, the relatively small number of components made check of compliance of any nuclear reactor unit against the concerned principle easier. Nowadays, the targets of minimizing planned and unplanned outages, refining operating margins and improving the overall efficiency

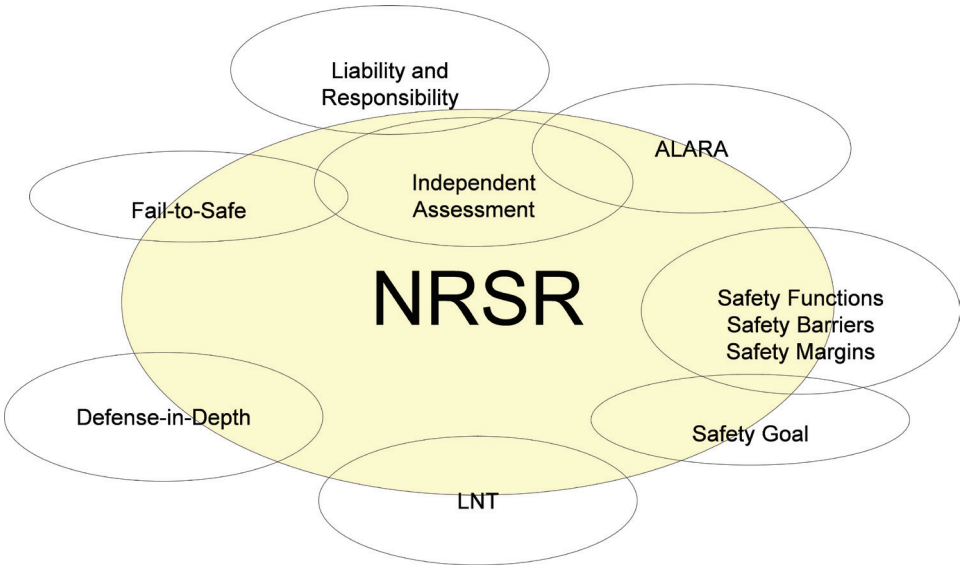

Figure 1. The selected overlapping NRSR elements and principles.

and performance of the system led to the increase in the sophistication and number of Instrumentation and Control (I & C) components. These unavoidably interact among each other, create a huge number of paths for failure and make difficult the demonstration of fulfillment for the principle, as in the recent crash of Boeing 737-Max, Duffey and D'Auria (2020).

Defense-in-Depth (DiD) is simply a recognition that mistakes and accidents do occur. DiD is the correct way to establish a conceptual and dynamic distance between harmful radiations and the environment, being the interface between Safety Requirements and design-construction features of reactors (the terminology derives from the military field where the objective is to protect the defense force). Prevention and mitigation are part of DiD, where traditionally, multiple levels are distinguished, both physically and probabilistically. A correct application of DiD shows, among other things, the positive safety impact of utilizing diversity and redundancy, defense against common mode failures, and the usefulness of only adding a limited array of specific "engineered" systems because of the dominant contribution of human performance and reliability to real outcomes and accidents. The term DiD is sometimes used improperly in literature, specifically when perspective research activities are concerned with innovative fission and fusion reactors.

Safety Functions (SF), Safety Barriers (SB) and Safety Margins (SM) concepts are to minimize the potential dangers from inadequacies in design or operation. NRSR makes wide use of the SF, SB and SM concepts, bringing to the design, among other things, of Emergency Cooling Systems (ECCS), the wider category of Emergency Safety Features (ESF) and to the need for a containment building. Related to SF and SB, SM constitute a deeper feature for NRSR: SM are the target of analyses; performing of analyses needs suitable computational tools, design details of the system (including SF and SB) and acceptance limits (set by regulators). Containment deserves two comments: a) venting is a proper design feature, though competing with LNT, or better, limited by LNT; b) additional use of containment strength appears necessary, e.g. discussed in section 3.

Independent Assessment (IA) is a means to ensure rigorous review of all these prior elements and claims. IA implies the capability to perform analysis by regulators independent of industry, going ahead particularly as embodied in "concept-neutral" and "performance based", e.g. USNRC (2020). In terms of competencies, IA is a principle stated at the beginning of nuclear era and easy to achieve when, specifically in US, regulators were proposing and leading the research in nuclear technology (i.e. until about 1970's). Complexity has been added to nuclear systems (see also discussion of Fail-to-Safe) and the data being proprietary with methods claimed as Intellectual Property (IP): regulators not 'understanding' the importance of non-disclosed data upon safety evaluations, notwithstanding the theoretical accessibility of all plant data, prevents the fulfillment of this principle (see further discussion in section 5).

The Liability and Responsibilities of the Owner/Operator is a fundamental risk tenet related to the overall risk and managerial structure. The liability, i.e. the legal responsibility arising from the possession and safe operation of an asset, must fall on the owner and is a well-understood principle, e.g. commonly applied to vehicles even if the Owner is not the Operator. This is valid notwithstanding the presence of a regulator that, among the other things, has the responsibility to fix proper rules to make the risk from the asset societally acceptable. The financial investment and anticipated income from the operation of any large nuclear reactor are of the order of 10 Billion USD; however, a nuclear disaster may cause a damage and related costs in the order of Trillion USD. No private (owning) industry can survive the market and social consequences when a massive amount of radiation diffuses into the environment following an accident, as only normal decommissioning funds are set aside and Nuclear Liability Laws do not cover investor risk exposure.

Therefore, in nuclear technology, as in other fully licensed cases like inadvertent oil and chemical spills, assigning blame, responsibility and penalties ends up in court, so limiting the financial liability-of-the-owner principle needs a change, discussed more in section 5.

The expected achievements

How can extreme event prior data and non-nuclear specific information be used in a 'concept neutral' regulatory and safety system design process? There is well established risk informed guidance already available: *'...it is very certain that, when it is not in our power to determine what is true, we ought to act according to what is most probable*', Rene Descartes, 1596–1650.

The problems we now face are how to make prior rare and other "failure" knowledge useful and applicable for predicting - and indeed anticipating - the quantitative probability of future events, with the intent to reinforce and validate the extensive "paper" bottom-up PRA/PSA calculations and submissions, so we can quantify, accept and believe the predictive uncertainties and reduce intolerable financial risks. What do we expect from the implementation and consideration of NRSR principles and requirements? The not-in-depth answer is as follows:

a. From the side of the owner-industry: the efficient operation of nuclear facilities including affordable design, construction and operation costs and an acceptably small probability of loss of investment.
b. From the side of regulators and public: the safe and efficient operation of nuclear facilities coincide following the tight links between NRSR and design.
c. The trust of the public towards nuclear technology and the evolution of the interaction between industry, operators, owners, investors and regulators.
d. As a result, many more numbers of units built for meeting the necessary global environmental preservation, societal development, and financial investment returns and infrastructure needs (i.e. several thousand GWe units by 2050).

Public trust as well as costs, being different in different regions of the world, contribute to determining and defining the current situation for nuclear technology.

The survey of NRSR is incomplete without mentioning the way to implement and check from principles (section 3.1) to achievements (section 3.2), which occurs within the licensing process of individual nuclear units and imply the interaction between industry and regulators. Tools, procedures and related applications within Deterministic Safety Analysis (DSA) and Probabilistic Safety Analysis (PSA) provide the desirable interconnection between principles and achievements. The key aspect is the qualification for those tools and procedures, as well as for the application modalities.

Furthermore, very low probability accidents with large consequences occur in any technology and industry (space, military, chemical, oil, transport, etc.) particularly at the dawn of development; these are unavoidable and are inherently part of the process to progress in civilization.

Detailed discussions of those topics are beyond the scope for the present paper and provided elsewhere, e.g. Duffey and D'Auria (2020). We limit ourselves to note that suitable tools and procedures exist, consistent with current knowledge; however, application of those tools lags (sometimes too much) behind their development and qualification proof, e.g. D'Auria (2019).

The LOCA and BDEE issues

These two 'types" of initiating events overlap, but are treated independently and artificially separated as being deterministic (top down for LOCA) or probabilistic (bottom up for BDEE) in origin for historical reasons. Then, in formal NRC and licensing FSARs the LOCA and BDEE occupy different Chapters 15 and 19, respectively. In response to *any* initiating event, the fundamental concern is non-restoration of power and losing capability to cool the reactor core, although considering the reliability of 'active' and 'passive' emergency back-up systems using applicable data for nuclear *and* non-nuclear systems (or the accident management field, not further discussed in this paper). The ESF, ECCS and EPS (Electrical Power Supply) are all designed to minimize the consequences. Any reactor design or concept must be robust and survive a Loss of Coolant Accident (LOCA) or BDEE, which constitute both an old issue and a new challenge for NRSR, e.g. Duffey et al. (1980) and D'Auria (2021). The following logical path is at the origin of the basic safety issue:

Choice of coolant-moderator → Temperature and cycle to achieve acceptable thermal efficiency → Design pressure or temperature → Need for retaining pressure or coolant boundary → Probability of Initiating event(s) → Possibility that pressure boundary is broken → LOCA and/or possible loss of cooling → Probability of core damage, P(CD) → Probability or frequency of external activity release

In addition to LOCA role in design of Pressurized and Boiling Water Reactors (PWR and BWR), the 'old-issue' feature derives from skepticism about results of analyses, whether deterministic, best-estimate and/or probabilistic. The 'new-challenge' features derive from:

- Discovery during the last 2–3 decades occurred of fuel weakness in addition to clad ballooning, e.g. D'Auria et al. (2019). High burn-up and long term permanence of clads into the reactor core environment create a cascade of interacting mechanisms that make the fuel rod prone to failure in a brittle mode, should a LOCA event happen. Detection and characterization of those mechanisms derive from post irradiation examination of nuclear fuel.
- USNRC issued before 2015 a still draft Regulatory Guide (RG 1.224-draft, USNRC 2018), where

possible and more restrictive acceptability thresholds, i.e. related to the current ECCS rule in USAEC (1971), are proposed. The 'new' ECCS rule envisaged in RG 1.224-draft (when and if enforced) may cause failure in fulfillment of acceptance criteria in the case of LBLOCA analyses of any existing reactor.

- Presently, quantitative estimates of the probability of reactor core damage, P(CD), are universally derived from bottom-up PRA/PSA, where restoring power and hence cooling involves postulating sequences with multiple (dependent) steps, actions and/or independent failures, including both 'active' and 'passive' safety systems. The probabilistic analyses have not used prior real event information directly, but adopt generic failure rate data and postulate a host of separately classified Beyond Design Basis Extreme Events, BDEE (floods, fires, hurricanes, ice storms, earthquakes, etc.), or a "hazard group" of events potentially provoking radiation release and some level of public harm used for assessing risk consequence.
- The subsequent probabilities of core damage for differing designs are actually all (directly or indirectly) dominated by the loss of power and cooling and/or LUHS, as in USNRC (2004b, 2007b), WEC (2004), NEI (2012) and NuScale (2020).
- To compute the probability of reactor core damage, P(CD), involves postulated sequences of multiple (dependent) actions and/or independent failures of both 'active' and 'passive' safety systems, WEC (2004), Bhatt and Wachowiak (2006), CE (2016), Barr et al. (2018) and NuScale (2020), including deploying FLEX equipment and any and all improvisation, NEI (2012). The analysis uncertainties are largely undefined and the PRA methods not validated by actual prior events (e.g. CHE and FMA), but the use of the methods are already promulgated and formalized in a Draft Regulatory Guide 1.200 and Standards.

For LOCA, debate in progress within the international community, as well as delay in updating the rules, has the purpose to prevent reduction in the nominal reactor power, the decrease of burn-up and of the time permanence of fuel in the core. Possible way-outs are (assuming that a 'new' ECCS takes into account of RG 1.224-draft):

i. Delete LBLOCA from the list of accidents to comply with licensing rule in Chapter 15 of FSAR, e.g. USNRC (2007a).
ii. Create an exception for LBLOCA in the 'new' ECCS rule.
iii. Introduce new materials for fuel design, i.e. Accident Tolerant Fuel (ATF), e.g. Guo et al. (2021).
iv. Provide a decisive role for containment in 'future' licensing rule, e.g. the ESF RIDM in present proposal.

RIDM progress is compounded by the emergence of new rules and methods that are claimed to be based on PSA and "allowable" or "tolerable" risks of core damage and activity release targets, GIF (2014), and NEI (2018). The use of data from similar prior events has even been dismissed as not directly "exchangeable" system-to-system, due to concomitant changes in knowledge, continuous learning and design changes, Apostolakis (2014, 2016), implying the posterior chance of any significant core damage is fundamentally different from the prior.

The statement of belief using this logic is that prior core damage events, like FMA and TMI, can only provide *guidance* for "risk informed" posterior judgments because: "It is the qualitative insights from operational experience that are useful in regulatory decision making, not the frequencies of core damage and release derived from this experience", Apostolakis (2016). By this definition, safety regulation and RIDM is subjective and qualitative, while not using any formal legal "balance of probabilities" of at least a 50% chance of being true, and without any numerically or scientifically defined judgmental uncertainty. The unresolved fundamental question is whether the (tiny) unverified core damage probabilities from PRA/PSA are believable, credible or justifiable as an aid to qualitative judgment of probable severe event outcomes when adopting the circular argument of not being validated or compared to actual "non-exchangeable" severe events.

There are at least two more definitions and many implications of something being "exchangeable", beyond the implied common grammatical usage of substituting some item for another of "equivalent value". Mathematically and statistically, "exchangeable" is defined for probabilistic sequences by: "… the probability is invariant under any permutation of (distribution values) xi", Jaynes (2003), and "a sequence of random variables is invariant under variable permutations", Niepert and Domingos (2014), which also allows finite or partial exchangeability. The NRC has independently added a third definition, where "exchangeable events" are *only* "independent events generated from a population of nominally identical reactors", Siu et al. (2016). A reactor suffering an event may be similar in concept or layout to others in the world, but there is no such thing as an average or generic reactor, and they cannot and never will be identical in detailed or even "nominal" system design or core physics due to inevitable differences in designers, components, computers, software, margins, set points, layouts, manufacturer, builder, age, turbine, maintenance and service conditions. This *ad hoc* definition justified NRC and others basing their input for RIDM solely on hypothetical design-by-design PRA/PSA event sequences[1] and rejecting as not 'exchangeable' or directly usable the actual prior core-damage accident or INES significant event failure rates and probabilities, e.g. as proposed in Engler (2020), or Rose and Sweeting (2016).

1 NB: In an unintended paradox, the NRC and industry guidance on PRA/PSA sequences or event trees themselves do not even satisfy the formal statistical definition of invariance with permutation exchangeability, which also applies to uncertainty methods based on propagation of input uncertainty parameters.

Strategies depicted or needed may contradict pillar analyses (not principles) in reactor design and NRSR applications, D'Auria (2021), which then has the potential to expand public disbelief in nuclear technology. For example, instead of summing core damage probabilities from separate multiple event trees, grouping together the risk set {BDEE} can provide the overall top-down or integrated probability of core damage for any reactor design or concept. For RIDM and NRSR purposes and completely independently of existing PRA/PSA methods and analyses, all that is needed are suitably validated probability, failure rates and uncertainty values *based on applicable data* to provide the needed physical insights and risk-dominant contributors.

For reducing the explosive threat from hydrogen production associated with core damage from Zircaloy-water and/or graphite-water reactions, important progresses occurred in designing ATF; related researches are ongoing as a valid response by industry and national R&D programs to the issues raised in RG 1.224-draft and RG 1.200-draft. However, demonstration that selected ATF may withstand corrosion erosion damage mechanisms (e.g. those identified in USNRC (2018) and cited support documents) may need a decade or more, as well as the complete substitution of current fuel in all cores of current or future reactors with the associated costs. Furthermore, the capability to withstand pressure wave propagation (among the 'old-issues') is not part of current ATF design (to our knowledge).

Our proposal (item iv above) starts from noting that LOCA and BDEE should be part of the design and safety of all reactors, D'Auria (2021), related to LOCA, and that the current rules needs updating according to new evidence, USNRC (2018). Namely, regulatory authorities must consider both active and passive emergency systems reliability, and ESF where containment is more relevant than in current rules.

Residual risk and proposal for 'future' ESF RIDM rule

The characterization of residual risk may benefit of the following paradigm-discussion also constituting the background for the ESF RIDM rule, Duffey (2012), and Duffey and Saull (2002).

In order to interpret the probability of a catastrophic event, in general we do not know precisely when and if the event happens; the probability of occurrence, is independent of the system, and can be infinitesimally small so we do not have any exact predictive capability. Conventionally adopted are the wording 'rare event', or 'black swan' to characterize this situation, Duffey (2015).

Thus, the similarities between apparently dissimilar catastrophic events both having the invisible and spreading potential for harm are: a) basic unpredictability of the event occurrence as to time, place and extent; b) occurrence of the event whatever effective countermeasures taken at the design and personal levels to reduce the probability of the event. The last statement is true in case of perfect human-system design and in the case of NPP, NRSR principles are applied to the best of the knowledge; and in the case of a COVID virus, preventive health measures and principles are applied also to the best of the knowledge. Under these circumstances, we can introduce a quantum-mechanics type of principle; the event is independent of the system (i.e. only connected with its existence) and is not a function of its complexity but only of the probability of actually being observed (as in the case of Schrödinger's cat).

Therefore, human civilization must simultaneously accept residual risk *and* attempt to identify and quantify what is acceptable risk, which here is associated with the 'ultimate' probability. In the parallel cases of NPP core damage and pandemic viral infection risks: 1) adding up of safety barriers and countermeasures does not prevent the existence of their failures; 2) a non-perfect or sub-optimized systems cause a higher probability of occurrence for the catastrophic event; 3) adding complexity (layered defenses and/or countermeasures) makes more difficult the achievement of a perfect system. In different words, increasing the complexity of any system or sub-systems may reduce the possibility of damage by an assigned event but unavoidably increases the possible number of events that bring to the same damage.

We can now define an *ultimate probability*, connected with the nature of the system but independent of the system under consideration, in such a way that it is meaningless to attempt any design having a lower failure probability. For the virus and the NPP, the ultimate probabilities are the event-probability 'killing of a person by an immune system attacker' and 'catastrophic events causing destruction upon the NPP site', respectively. Therefore, we define:

- p_{CE} = Probability of a Catastrophic Event, well designed system
- $p_{CE\text{-}B}$ = Probability of a Catastrophic Event, badly designed system
- p_{CE}^{virus} = Probability of unavoidable risk in a Catastrophic Event for the virus
- p_{CE}^{sys} = Probability of unavoidable risk in a Catastrophic Event for a complex system (NPP)
- $P_{LOCA/BDEE}$ = Probability of LOCA occurrence (specific for each NPP)
- P_U = Ultimate Probability for a Catastrophic Event (system dependent)
- f_U = Inferred Frequency for destruction upon the NPP site.

Then, we summarize the paradigm-discussion as the following inequalities and equivalences:

$$p_{CE\text{-}B} > p_{CE} \tag{1}$$

$$p_{CE}^{virus} \approx p_{CE}^{sys} \tag{2}$$

$$P_U \lesssim p_{CE} \tag{3}$$

$$P_U \equiv f_U \tag{4}$$

$$P_{LOCA/BDEE} \gg p_{CE} \quad (5)$$

Here one may note that adding sophisticated controls may bring to an increase in p_{CE} value (i.e. increasing into $p_{CE\text{-}B}$), e.g. equation (1). The equation (2) symbolically reflects the Schrödinger cat observational existence conditions, while equation (4) is a prerogative of regulators.

The proposed ESF rule

For new "non-LWRs", the NEI proposed an allowable "risk significant" annual Frequency-Consequence, F-C, evaluation "target" using regulatory public dose exposure limits measured in rem, USNRC (2007a), and NEI (2019). For PRA/PSA frequencies within nominal "5–95% uncertainty" bounds, NEI (2018), there is an arbitrary "anchor" at 1 rem, with a constant minimum below a frequency of 5.10^{-7} per annum[2]. The suggestion is that there are statistical uncertainty bounds on input probabilities derived from sensitivity to failure rate uncertainties; however, this is itself subject to unknown uncertainty given there are no comparisons to prior (deemed as non-exchangeable) NPP event data. Note that for infinitesimal releases, the implied allowable target is more than one event per year per reactor *even if the core damage causes total investment loss but negligible societal disruption or public harm*.

Implementation of safety rule is the prerogative of regulators only who are not formally concerned about financial losses and risks. Therefore, we submit the proposal below, with the support of the diagram in Fig. 2, to the attention of regulators, well recognizing that it has not any robustness, completeness and self-consistency characteristic. Exploiting the containment strength, introducing specific consideration of residual risk and locating LOCA and BDEE (and additional 'similar' events) constitute targets and attributes for the newly proposed ESF RIDM rule.

We qualitatively report selected parameters in the vertical axis versus decreasing values of the probability of accidents. Corresponding to nominal (or normal) operation, one may infer LOCA occurrence and ultimate probability, i.e. the RIDM limit, or P_U Nominal operation is the 'probability' event during the operating life of any reactor. Reactor-dependent value for the LBLOCA probability of occurrence, eventually extended to the entire spectrum of DBA, constitutes the intermediate value. What is currently reported as severe accident (SA) or BDEE probability might involve towards Large Releases (LR) of radioactivity to environment (i.e. sum of probabilities of occurrence for all SA-LR events) and constitutes the smallest value on the right of the horizontal axis.

The expected containment response and the ECCS rule originated by USAEC (1971) constitute the vertical axis; one may add the BEPU (e.g. CSAU supported) domain, not shown in the diagram, to predict the events and associated uncertainties until the occurrence of BDEE-LR under the condition of (nearly) intact core geometry.

Containment protects the environment, should an accident occur having probability lower than P_U. However, the amount of radiation in the containment is substantially different for accident having probabilities larger or smaller than $P_{LOCA/BDEE}$ (because of unavoidable containment leakages one may also expect different releases to environment). Containment bypass, or LR condition, constitutes the residual risk. The graded approach characterizes the current ECCS rule: acceptability thresholds are more stringent for most probable events. The proposed ESF RIDM rule keeps the same ECCS rule, USAEC (1971), within the domain <normal operation – $P_{LOCA/BDEE}$>; step relaxation occurs at $P_{LOCA/BDEE}$until P_U. In the domain <$P_{LOCA/BDEE} - P_U$> the current ECCS rule is not necessarily fulfilled. Summarizing, the key features for the proposed ESF RIDM rule are:

a. The definition of P_U.
b. The adoption of current ECCS rule, USAEC (1971), or similar rule modified based on RG 1.224, USNRC (2018), and RG 1.200, USNRC (2020), until $P_{LOCA/BDEE}$.
c. The exploitation of containment strength in the domain <$P_{LOCA/BDEE} - P_U$> (e.g. allowing massive release of radioactivity in the containment should a LOCA occur).

Rough definitions unavoidably characterize the parameters in Fig. 2. Furthermore, the BEPU use in the region <$P_{LOCA/BDEE} - P_U$> implies the calculation (and the assessment) of radiological releases from the failure of individual fuel rods and tracking of radiation transport from the core to the containment and from containment to environment through unavoidable leakages. Current acceptability thresholds apply for radiation release to the environment, i.e. for accidents having probability greater than P_U.

Connected with the ESF RIDM rule, regulators could allow the reduction of liability of NPP owner for accidents having probability lower than P_U.The NPP owner could contribute a maximum value for damages in such conditions.

The problem of independent assessment and major observations

The overall regulatory structure of NRSR risks (ironically) collapses owing to inadequate fulfillment of the Independent Assessment (IA) principle. During the 50's of previous century, when putting the bases for the design of existing reactors, an intimate connection existed

2 Specific parameter values for the F-C "target" or boundary lines are not given in USNRC (2007a), or NEI (2019), but can deduced from NEI's Fig. 3.1.

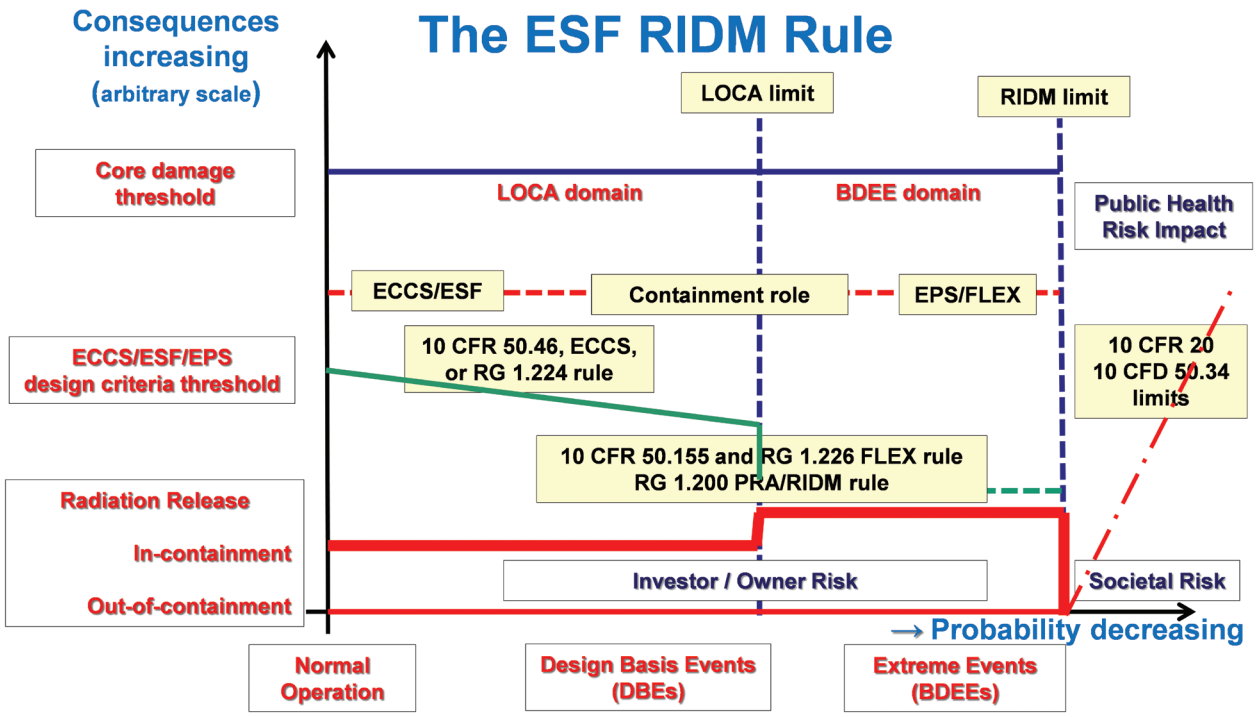

Figure 2. The proposed 'ESF RIDM Rule'.

for staff/personnel of both industry and regulator: hence, IA was possible. Nowadays, sophistication of design and proprietary data make IA (almost) impossible as stated in section 2. Here we are extending IA into the broader RIDM uncertainty quantification domains, and not restricting the concept to limited reviews as defined and used elsewhere for PRA, NEI (2019), or to the formalized use of expert solicitation proposed for assessing seismic occurrence risk, USNRC (1997), where it was found "the most important conclusion is that differences in PSHA results are due to procedural rather than technical differences".

Current DSA and PSA performed outside of the industry appear to be likely based on virtual and generic analysis while not fully reflecting the actual reactor construction and operational realities. At least two solutions are possible.

Niels Bohr already proposed in 1950 in his letter to United Nations, Bohr (1950), not only dealing with nuclear weapons: "*The creation of new barriers, restricting the free flow of information between countries, further increased distrust and anxiety. In the field of science, especially in the domain of atomic physics, the continued secrecy and restrictions deemed necessary for security reasons hampered international co-operation to an extent which split the world community of scientists into separate camps*". He also recognized "*The ideal of an open world, with common knowledge about social conditions and technical enterprises, including military preparations, in every country, might seem a far remote possibility in the prevailing world situation*". In this vision, nuclear energy is a patrimony of human civilization and not the topic for business. Clearly, this is desirable but not accepted by current civilization.

A second possible solution was proposed by D'Auria et al. (2015). The design of a nuclear reactor, the Intellectual Property (IP) of an assigned industry or investor, splits in a large number of conceptual boxes. One or a few boxes are accessible to each group of concerned scientists and technologists, i.e. the IA analysts or assessors in charge of performing DSA and PSA. Minimum cross-dialog, under the control of the IP occurs among those groups of analysts: the assessors commit to not transfer data to any third-part industry or informing regulators of results of analyses. In this manner, IA becomes a mean to consolidate and develop the design and safety case of reactor rather than an informative message provided to regulators. Typically, those results help the IP owner to improve the original design and to transmit (to regulators) details of formal Final Design, as in the current Design Control Document (DCD). Fig. 3 provides an analog sketch of the process: scientists and engineers having access to one or a few elements of the Monna Lisa frame on left side of the figure, deeply examine only a piece of that frame (one of which includes the RIDM logic) but cannot reproduce the overall picture on the right.

In pursuing the analysis, we also uncovered a number of aspects which constitute a corollary and a complement to the major conclusions below, so these are randomly reported hereafter, not in order of importance:

- Quality assurance is essential and desirable in all fields for design and safety demonstration of nuclear reactors; however, structured algorithms for uncertainty quantification should substitute, as much as possible, the use of qualitative statements.

Figure 3. The possible approach for Independent Assessment.

- The major investor/owner operator risk is due to LOCA/BDEE causing core damage without significant radiation release to the public, so a likely acceptable corollary is adoption of properly designed emergency containment and venting.
- The regulatory authority is correctly independent of industry-owner of nuclear facilities but rightfully is not concerned with financial risk. Not only should the independency of nuclear regulators from policy, politics and science be assured, in different sectors, but also specifically LNT should not be an (hidden) imposition for regulatory purposes.
- Beyond having open websites and requiring masses of official paperwork, nuclear regulators must streamline the licensing process and directly communicate to the public and re-gain the public trust, as at beginning of the nuclear era before the major societally disastrous events at TMI, CHE and FMA.
- Changing nomenclature continues not just for accident types ("beyond design" or "practical elimination"); shifting terminology and concepts include "passive safety", "small modular", "risk informed", "concept neutral", "tolerable risk", "frequency-consequence", "exchangeability", "performance based" and "non-LWR", all of these being recently introduced without adequate quantification and definition, and without having complete supporting research and development bases. The danger is being potentially misleading in the general public domain: for sure, these changing foci, good intentions and fashionable trends promise much but slow the progress by potentially adding, i.e. not removing, layers of licensing complexity and certainly not directly addressing or reducing new investor/owner costs and risks.
- Artificial Intelligence and "machine learning" methods (e.g. processing of big data) are a help, not a substitute, to creativity and intellectual capacity of nuclear scientists and are a supplement and aid but not a replacement for human experience and knowledge. Here we hope that from the marvelous dawn of development, Carr (2021), we are not falling into the twilight of the human mind.
- We have entered the computer age since the origins of nuclear power. We are suggesting and recommending here that this "new safety" be continuous, dynamic, online and immediate 24/7/365, and openly available, according to the principles of Process Safety Management and the objective of retaining control and the *safety management* of any industrial system.
- The plethora of Small and Modular Reactors (SMR) concepts, at last count over 50 different types in multiple countries, and the consequential creation of many (small) industries without deep expertise and build know-how leading the design of reactors, has the potential to disrupt the complex NRSR framework available today. This trend will undoubtedly lead to many failures to adequately demonstrate their safety cases, while claiming potential economic benefits and risk reduction.
- The SA-BDEEs leading to core damage are sufficiently understood by technicians in industry and shall not become the driving activity for the development of skills for new generations of young researchers. The recent crash of airplanes, enormous industrial explosions and collapse of submarine in industrial sectors different from nuclear, does not trigger intricate multi-year research to forensically understand everything that happened during those dramatic events. Avoiding those events, as demonstrated by TMI, CHE and FMA, is and should be the (only) major societal focus of attention.

Conclusions

Nuclear fission technology deployment is on the brink of extinction in some countries that mostly contributed to its early development. Reactor safety is also at a decisive crossroads where keeping to traditional paradigms for risk assessment, definitely losing competences by young generations, excessive economic investment and market risk and lack of trust by the public may occur.

These summary statements justify the ideas in the present paper as a means to help unify and update the historical

basis for safety design and regulations, and therefore we expect opposition to their acceptance and implementation. The timely parallel of the personal and societal fear from the probability of exposure to invisible viral infection and to radiation helps to illustrate the key issues of public risk perception, i.e. the need for effective countermeasures, as well as quantifying and communicating uncertainties while minimizing the financial and societal risks.

We bring together the aspects of probabilistic and deterministic safety methods, attempting to unify within one framework the rigid rules and historical paradigms for LOCA and PRA for analyzing the onset of core damage due to DBE/BDEE of all types. We propose three sets of conclusions, respectively related to comments on Nuclear Reactor Safety and Risk (NRSR), the proposal of the Engineered Safety Features Risk Informed Decision Making (ESF RIDM) rule as a substitute of the Emergency Core Cooling (ECCS) and Probabilistic Risk Assessment (PRA) rule, and a way forward to deal with Independent Assessment (IA).

As Low as Reasonably Acceptable (ALARA) principle and Best Estimate Plus Uncertainty (BEPU) approach, need proper and definitive acceptance by major players in the technology and licensing for all reactor concepts and designs. ALARA, rather than Linear No Threshold (LNT) hypothesis should be at the origin of safety objective and consequential safety requirements. The concept of beyond design extreme events (BDEE) should play a role in decision-making; for instance, the risk exposure and liability of industry-owner-investors for the consequences caused by a core damage accident even without large radiation release is not economically sustainable. It also discourages investment in new concepts and innovative design evolutions.

Invoking a quantum-mechanics analogy to the principle of observational existence, even in the case of a "perfectly designed" system, shows a probability of disruptive failure and/or core damage, as there is never zero risk. Correspondingly, an ultimate probability value, P_U has been introduced: design quality shall be consistent with P_U that is associated with the expected frequency of a rare event. One hypothesis is that P_U is the probability or frequency of the fall of a powerful meteorite on the reactor site. The current ECCS rule became obsolete following the discovery of nuclear fuel failure mechanisms, should a Loss of Coolant Accident (LOCA) occur; therefore, we proposed a new ESF RIDM rule, where the containment is a robust barrier against radiation releases. Proper LOCA and BDEE considerations in safety demonstrations are the key elements of the ESF RIDM rule, where all events with probability higher than P_U cause doses to public and to the environment below current artificial health limits.

We note that 'virtual' safety analyses are part of both Deterministic Safety Assessment (DSA) and Probabilistic Safety Assessment (PSA), because of lack of availability of industry proprietary data (the safety is inside the details). Therefore, we propose a deep change in the application of the IA principle where groups of respected and concerned scientists and engineers shall perform open IA work to proper supporting regulators and to improve industry-owner design. Rather than just providing informative "guidance" or "review report" messages to regulatory bodies, we consider open IA applicability as the key obstacle for a suitable risk reduction and for re-gaining public trust towards nuclear energy.

References

- Apostolakis G, Lui M, Cunningham G, Pangburn W, Reckely J, Adams M, Call D, Damon E, Easton T, McCartin G, Mizuno T, Piper J (2012) A proposed risk management regulatory framework, NRC Risk Management Task Force report. April, NRC access # ML 12109A277, Washington, DC, USA, 318 pp.
- Apostolakis G (2014) Global statistics vs. PRA results: which should we use? Presentation, Eastern Carolina, USA, March 27.
- Apostolakis G (2016) A perspective on the use of risk information. Proceedings Am. Nucl. Soc. PSAM, Seoul, Korea, October.
- Barr J, Basu S, Esmaili H, Stutzke M (2018) Technical basis for containment protection and release reduction rulemaking for BWRs. NUREG-2206, US NRC, ONRR, Washington, D.C., 373 pp.
- Bhatt SC, Wachowiak RM (2006) ESBWR certification probabilistic risk assessment. General Electric Energy Nuclear, Wilmington, NC. Report No. NEDO 33201, rev 1 (also GE-Hitachi), ESBWR Certification Probabilistic Risk Assessment, Report.
- Bohr N (1950) Open Letter to the United Nations, Copenhagen. June 9. Published in Copenhagen by J.H. Schultz Forlag. Reprinted in the Bulletin of the Atomic Scientists 6–7: 213–217. https://doi.org/10.1080/00963402.1950.11461268
- Carr AB (2021) Thirty minutes before the Dawn. Nuclear Technology 207: 2–24. [supplement 1]. https://doi.org/10.2172/1764862
- CNSC (2008) Design of New Nuclear Power Plants. Report RD-337, Canadian Nuclear Safety Commission, Ottawa. [ISBN 978-1-100-10645-8]
- D'Auria F, Glaeser H, Kim M-W (2015) A vision for nuclear reactor safety. Invited (Key-Speaker) at 46th Jahrestagung Kerntechnik Annual Meet, Berlin (G), May 5–7, and 9th International Scientific and Technical Conference Safety Assurance of NPP with VVER, OKB Gidropress, Podolsk (Ru), May 19–22.
- D'Auria F (2019) Best Estimate Plus Uncertainty (BEPU): Status and perspective. Nuclear Engineering and Design 352: e110190. https://doi.org/10.1016/j.nucengdes.2019.110190
- D'Auria F, Debrecin N, Glaeser H (2019) The technological challenge for current generation nuclear reactors. Nuclear Energy and Technology (NUCET) 5(3): 183–199. https://doi.org/10.3897/nucet.5.38117
- D'Auria F (2021) An old issue and a new challenge for nuclear reactor safety. Frontiers in Energy 15: 854–859. https://doi.org/10.1007/s11708-021-0729-0
- Duffey RB, Kalra SP, Merilo M, Sun KH, Zvirin Y (1980) Beyond the large LOCA: Current heat transfer aspects of LWR safety analysis. International seminar Aug. 25 – Sept. 5, Dubrovnik, Yugoslavia. Nuclear Reactor Safety Heat Transfer, 731–745. https://doi.org/10.1615/ICHMT.1982.AdvCourHeatTransfNucReactSaf.470

- Duffey RB, JW Saull (2002) Know the risk. Butterworth and Heinemann, Boston, Mass., US, 1st edn., 227 pp.
- Duffey RB (2012) Extreme events: The New social design basis. In: Proceedings of the 20th International conference on Nuclear Engineering, ASME 2012 Power Conference, ICONE20-POWER2012, 30 July-1 August, Anaheim, Ca, USA, 635–638.
- Duffey RB (2015) The Seven risk paradoxes. American Nuclear Society Conference, Probabilistic Safety Analysis, PSA2015. Sun Valley, Idaho, US, April 21–26, 12223.
- Duffey RB, D'Auria F (2020) Nuclear Energy and its History: Past consequences, present inadequacies and a perspective for success. Energy and Power Engineering 12: 193–236. https://doi.org/10.4236/epe.2020.126014
- Engler J-O (2020) Global and regional probabilities of major nuclear reactor accidents. Energy Management, 269 pp. https://doi.org/10.1016/j.jenvman.2020.110780
- GE (2016) General electric company, certification of the world's Safest reactor paves way for commercial deployment in the U.S. and worldwide. https://www.ge.com/news/pressreleases/,Wilmington,NC,ge-hitachis-esbwr-receives-nrc-design-certification-approval [accessed 4/12/2021[
- GIF (2011) Generation IV international forum. An Integrated Safety Assessment Methodology (ISAM) for generation IV nuclear systems, GIF/RSWG/2010/002/rev1, Version 1.1.
- GIF (2014) GEN IV international forum. Guidance document for integrated safety assessment methodology (ISAM) – (GDI), European Commission Joint Research Centre Report for GIF Risk and Safety Working Group, GIF/RSWG/2014/001, Version 1.0.
- Guo Z, Dailey R, Zhou Y, Sun Z, Wang J, Corradini ML (2021) Effect of ATF Cr-coated-Zircaloy on BWR In-vessel Accident Progression during a Station Blackout. Nuclear Engineering and Design, 372 pp. https://doi.org/10.1016/j.nucengdes.2020.110979
- IAEA (2006) Fundamental Safety Principles, IAEA Safety Standards - Series No. SF-1, IAEA, Vienna, Austria.
- IAEA (2019a) Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, SSG-2 (Rev. 1), Vienna, Austria.
- IAEA (2019b) Hierarchical Structure of Safety Goals for Nuclear Installations, Tecdoc 1874, Vienna, Austria.
- Jaynes ET (2003) Probability theory: the logic of science. Cambridge University Press, Cambridge, UK, 758 pp. [Ed. G.L Bretthorst] https://doi.org/10.1017/CBO9780511790423
- Miller AI, Suppiah S, Duffey RB (2005) Climate change gains more from nuclear substitution than from conservation. Proceeding 13th International Conference. Nuclear Engineering, Beijing, China, May 16–20, Paper ICONE13-50448.
- NEI Nuclear Energy Institute (2012) Diverse and flexible coping strategies (FLEX) implementation guide, Nuclear Energy Institute, Report NEI 12–06 [Draft Rev. 0], Washington, DC, USA (NRC Access number ML122221A205).
- NEI (2018) Risk-informed performance-based guidance for non-light water reactor licensing basis development. Technical Report 18–04, Washington, DC, NRC access # ML 18271A172.
- NEI Nuclear Energy Institute (2019) NEI 17-07, Performance of PRA Peer Reviews Using the ASME/ANS PRA Standard, NEI report 17-07 Revision 2, Washington, DC. NRC ADAMS Accession # ML19241A615.
- Niepert M, Domingos P (2014) Exchangeable variable models, Proc. 31st Conf. on Machine Learning, Beijing, China, arXiv: 1405.0501v1, 2 May, JMLR:W&CP, vol 32.
- NuScale (2020) Standard plant design certification application, Part 2 Tier 2, Rev5, Chapter 19, USNRC on-line access # ML20224A508.
- Rose T, Sweeting T (2016) How safe is nuclear power? A statistical study suggests less than expected. Bulletin of the Atomic Scientists 72(2): 112–115. https://doi.org/10.1080/00963402.2016.1145910
- Siu N, Stutzke M, Dennis S, Harrison D (2016) Probabilistic risk assessment and regulatory decision making: some frequently asked questions. US NRC report, NUREG-2201, ONR, Washington, DC, NRC access # ML 16245A032.
- USAEC (1971) Interim Acceptance Criteria (IAC) for ECCS, US-AEC, Washington, DC, USA; and 10CFR50.46 Acceptance criteria for ECCS for light water nuclear power reactors, 39 FR 1002, Jan. 4, 1974, as amended at 53 FR 36004, Sept. 16, 1988; 57 FR 39358, Aug. 31, 1992; 61 FR 39299, July 29, 1996; 62 FR 59276, Nov. 3, 1997; 72 FR 49494, Aug. 28, 2007.
- USNRC (1975) Reactor Safety Study – an assessment of accident risk in U.S. Commercial Nuclear Power Plants. WASH-1400, (Rasmussen Report), NUREG-75/014, Washington DC, USA.
- USNRC (1997) Recommendations for probabilistic seismic hazard analysis: guidance on uncertainty and use of experts. Senior Seismic Hazard Analysis Committee (SSHAC), NUREG /CR-6372, Vol 1 and 2. Division of Engineering Technology Office of Nuclear Regulatory Research, Washington DC, NRC access # ML080090003.
- USNRC [United States Nuclear Regulatory Commission] (2004a) Nuclear power plant licensing process, NUREG/BR-0298, Rev. 2, Washington DC, USA.
- USNRC [United States Nuclear Regulatory Commission] (2004b) Final safety evaluation report related to the certification of the economic simplified boiling-water reactor standard design, NUREG-1966, ADAMS Accession number ML14100A187.
- USNRC [United States Nuclear Regulatory Commission] (2007a) Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing, Main report, NUREG 1860, vol 1 and 2, Washington DC, USA.
- USNRC [United States Nuclear Regulatory Commission] (2007b) Standard review plan for the review of safety analysis reports for nuclear power plants. U.S. Nuclear Regulatory Commission, Washington, DC, Report No. NUREG-0800 (continuously updated).
- USNRC (2018) Establishing analytical limits for zirconium-alloy cladding material, regulatory guide 1.224, Draft (originally issued as DG-1263, March 2014), Washington, DC, USA, 1–32.
- USNRC [United States Nuclear Regulatory Commission] (2020) Acceptability of probabilistic risk assessment results for risk-informed activities, Draft Regulatory Guide 1.200 revision 3, June, Washington, DC, access # ML19308B636.
- WEC [Westinghouse Electric Corporation] (2004) Design reference AP1000 Design Control Document (DCD), WEC, Pittsburgh, PA, Report No. APP-GW-GL-700 (also "AP1000: Passive safety systems and timeline for station blackout").
- WENRA [Western European Nuclear Regulators Association] (2009) Safety objectives for new power reactors, 30 pp. http://www.wenra.org/harmonisation/reactor-harmonisation-working-group
- WENRA [Western European Nuclear Regulators Association] (2013) Safety of new reactor designs, 52 pp. http://www.wenra.org/harmonisation/reactor-harmonisation-working-group
- Zuber N (2010) Scaling: from quanta to nuclear reactors. Nuclear Engineering and Design 240: 1986–1996. https://doi.org/10.1016/j.nucengdes.2010.01.021