Scientific Research Publishing

Energy and Power Engineering, 2020, 12, 193-236
https://www.scirp.org/journal/epe
ISSN Online: 1947-3818
ISSN Print: 1949-243X

Nuclear Energy and Its History: Past Consequences, Present Inadequacies and a Perspective for Success

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

[1]Senior Retired Scientist, Idaho Falls, USA
[2]University of Pisa, Pisa, Italy
Email: duffeyrb@gmail.com, dauria@ing.unipi.it

How to cite this paper: Duffey, R.B. and 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

Received: March 20, 2020
Accepted: May 29, 2020
Published: June 1, 2020

Abstract

An attempt is made to locate nuclear technology within a logical context considering history, risks, societal catastrophes and perspectives: the need is identified for a new direction in the exploitation in order to restore the role in energy production. We depict the situation coming from a marvelous history of discoveries started at the beginning of the XX century; heroes are recalled who made possible something that is inconceivable today: design, construction and production of electricity in a few years; that history was tainted by intentional nuclear explosions, *i.e.* the original sin that we are now paying. Then, we attempt to show that the societal risk is an inherent part of the civilization. Restoring the public trust (towards nuclear fission technology) by matching nuclear safety with the current technological status and advancers in risk assessment is the key objective. The "independent assessment", or a principle for the exploitation of nuclear energy already stated in the 50's of the previous century, shall then re-appear. This is used to erect the signpost for a "dynamic barricade" to further reduce the risk of operation of nuclear reactors and to match the design with current technological capabilities and with the frontiers of the research.

Keywords

Societal Risk, Risk and Probability, Catastrophes, Nuclear Fission, Nuclear Reactor Technology, Dynamic Barricade, Cost of Safety

1. Introduction

The motivations for the present paper can be summarized by the following statements:

- Nuclear fission discovery is like fire discovery: fire and associated chemical reactions burn the humans and the environment and is definitely dangerous, but it is necessary for civilization and fully accepted; nuclear fission is not globally accepted.
- Nuclear technology history is very short compared with history of humanity: fission technology has not had the possibility so far to demonstrate its benefits: those benefits profoundly counterbalance drawbacks caused by unavoidable and technological explainable catastrophes.
- Foggy future for nuclear technology (at least in some countries) caused, in addition to lack of benefits from nuclear energy, lowering of industrial investments and, unavoidably lowering of research investments: this caused lower interest by young generations, lower interest in safety and, ironically, higher costs that further decreased the interest toward this technology.
- Authors of the paper had the possibility to follow and to participate in the gigantic effort to finalize the design and to demonstrate the safety of nuclear installations: regrettably and ironically (again!) once the safety demonstration for nuclear reactors became possible, the decline of the technology started or accelerated. The same authors regret that young scientists have no possibility to experience stimulating times unless innovation occurs.
- Climate change (whatever coming from pollution and human impacts or from universe-connected changes) is a strong advocate for nuclear energy: there is no recognition of this (easy) statement in a market-policy driven context where the web works as a constraint rather than a freedom ploy (as it happens in different sectors of society).

For many years, we have been studying nuclear energy and its key role in providing power to the modern world, and we are concerned about its future and its success. The pathway to the present and the road into the uncertain future of this vital energy source must be viewed and placed in historic context. Such is the rapid changes of science, technology and civilization and their evolution, we still are unsure of the lost art of building the Pyramids, what marvels are still lying in the tombs in China, what Newton discovered (or not) in his chemistry studies, or even how human life and civilization itself began.

Lest we all forget, just longer than one century history characterizes the nuclear era during a fast changing world: it took nearly two millennia for Galileo Galilei to update the ideas of Archimedes; and a few hundred years to Albert Einstein to improve the physics picture provided by Galilei and Newton. However, during less than a century all discoveries that made possible the exploitation of the fission chain reaction suddenly and almost miraculously occurred. Possibly, the foundations of the nuclear era are still weak and without strengthening may collapse due to challenges put by the same civilization that originated and took the benefit of nuclear energy. In particular, epochal changes for fission energy technology are expected in next few years. Many reactors may be forced to disappear like dinosaurs and the nuclear fission technology may collapse like the dirigible technology; deep research findings in many areas that

sustained the nuclear technology are already buried alongside the many amazing pioneers who performed the research; an avalanche is falling down of incompetence and misunderstandings which are at the origin of cost increases for Nuclear Power Plants, delays in project execution and even cancellations. Un-clarified scientific and technical topics become fertile ground for anti-nuclear scientists who have easy access and listening from policy makers, who often remain uniformed about the scientific underpinnings and the past experience and knowledge—and where it leads.

As we have stated before, [1]: "*Certainly, the risk from energy systems, energy production, and energy use is low. But societies do not have a unified and universal measure of what constitutes acceptable risk. The attitude to risk varies with the activity, history, technology, and the regulatory or legal framework. This is already well known and documented in the study of risk analysis and is unlikely to change towards some more rational basis. Clearly related to self-preservation, personal experience, and our perceptions, most people accept some necessary everyday risks, such as driving a car, ignore others like living in an earthquake-prone area, pursue some by, say, buying stocks, and reject others like not jumping off a cliff. The risk from nuclear energy use poses special questions, as its potential radiation threat is unseen and not very well understood by the public. This is rather like electricity itself, which in its earliest days was even perceived as some unknown threat or hazard. Should the risk from an energy source be compared to natural disasters such as floods or earthquakes? Or to the risks of other technologies? Or to some legal or societal norm or standard?*"

Indeed we have this recent statement from religious leader Pope Francis: "*I have a personal opinion: I wouldn't use nuclear energy until it is totally safe to use*", the Pope told a group of reporters aboard the plane returning to Rome from Tokyo, emphasizing that a nuclear accident could "always happen" and would necessarily be "big" once it occurred (engish.kyodonews.net/news/2019/11/306063dc6f54-urgent-pope-airs-opposition-to-nuclear-energy-over-safety-risks.html).

Therefore, four main issues or challenges confront nuclear energy today:

1) Acceptance: despite past accidents demonstrating, achieving and retaining public confidence as a safe and cheap source of energy, e.g. [2];

2) Sales: competing head-to-head in open energy market places against stiff competition from cheap natural gas and high efficiency fossil power plants and subsidized renewables; plus

3) Investment: retaining political and financial support for nuclear-related policies worldwide, including non-proliferation, enrichment technology and use, research demonstration, and managing and recycling used nuclear fuels, e.g. [3].

4) Innovation: many of the so-called new or advanced nuclear energy concepts and ideas have been around for decades, or are recycled reincarnations already not accepted in the marketplace; and (possibly, apart from in China) the needed prototypes, (expensive) demonstrations, risky testing and "true" innovations are not now happening.

This is clearly "tough sledding" for any technology, development or science, and the intertwining of nuclear energy with the nuclear weapons past, national policies of the present, and the global energy supplies of the future cannot be just dismissed. Nuclear energy is in the middle of all these tensions, needs and debates, as emerging regional economies like India, China Africa strive to power their nations and assure their people's future. Meanwhile, existing "world powers" still grapple for supremacy and influence, while other countries just seek energy security—especially those without lots of oil, gas, coal or uranium. Just to add to the mix, along comes the concerns about "global climate change" due in part to human energy use and carbon-based fuels, which are now driving worries about the world and its atmosphere, and may even imperil the survival of many low lying countries and lands if sea levels continue to rise inexorably.

Nuclear energy is not the one solution to all these issues—but it is an indispensable and vital part of any and all of the necessary and needed solutions, [1]. However, there are also real questions about the future—particularly today.

The scope for the present paper is the intersection between nuclear energy, current technology and knowledge and the society with "visible" issues like catastrophes and risks in different sectors of today civilization and the permanent concern of climate change are concerned. Within the nuclear technology arena, the objective for the paper is fixed by the following considerations:

- The fundamental design basis has remained largely unchanged, see below, and numerous accident mitigation measures have been included into the existing unit designs to varying degrees (e.g. core catchers, vessel external cooling, remote control rooms, severe accident management guidelines and filtered vented containments).
- None of these preclude the consequences of extreme events which by definition are beyond the design basis, whatever that is, and include the key role of human intervention (e.g. in decision making, core cooling, system restoration and activity release), [5].
- Prudent "stress testing" and enhanced emergency preparedness become the tools for accident management and mitigation measures, despite the remaining potential for severe social disruption, [4], see also [6].
- The key challenge is to comprehensively derive a quantified risk assessment, e.g. [7], for a design basis for a complex technology which includes the indirect as well as the direct social impacts, which is not the historical regulatory approach which focuses on activity release.
- Also included must be human involvement and decision making for extreme events, which defines and acknowledges uncertainties and the dynamic nature of risk, [8].
- Given there is no such thing as "absolute safety", the overall objective to ensure employee and corporate safety, to assure environmental preservation, and to attain public and political trust, e.g. [9].

Therefore, a two-pronged analysis is considered in the paper. On the one hand we attempt to show that current nuclear fission is not an exotic energy

source. Rather its bases and background are consistent with society's needs: the deployment of a suitable number of nuclear reactors is well within acceptable safety boundaries; and the source of electricity by the nuclear fission has the potential to be harmonized with other energy sources including alleviation of the suspected major causes for climate change. On the other hand, a deep revision of safety concepts and applications for existing and new reactors is needed, both to deal with public negative trust by introducing a new way of thinking, and to create a dynamic cross-link between existing safety features (of nuclear reactors) and the advancement of knowledge and modern science.

The logical structure of the paper may be distinguished into three parts in addition to this Introduction and the Conclusions.

Firstly identifying the past road, examining selected key interactions between nuclear energy and societal aspects shows the roots by which nuclear energy is conceived: the history of physics in the last century (Section 2); the weaknesses associated with the global market and the picture of accidents (Section 3); a vision for the new risk concept (Section 4); and the response of safety technologists *i.e.* "the barriers" (Section 5).

Secondly, defining the present road, proposing a dynamic framework to build-up a safety context for nuclear reactors based on continuously moving research boundaries and consistent with current societal needs (Section 6): items include motivation in the workplace, independent assessment overpassing the industry proprietary information, and intervention (if requested) of a technology-security team to restore eventually endangered safety infrastructure, are examples of assembled constituents opposing the release of radioactive material.

Thirdly, signposting the future, considering of risk-defined "extreme events" to support the demonstration of resilience for the conceived dynamic framework and ensure public trust (Section 7): *i.e.* to identity a way to slow down and to stop the decline of nuclear technology.

2. The History: The Past Growth Path and Technology Basis

Industrial progress during the XIX century led to break-through applications like electricity and thermal engines. However the physics did not move far away from the discoveries of Galileo and Newton. Suddenly, at the end of the century and during the initial two decades of XX century, the discoveries in physics became overwhelming (see e.g. what Einstein, Rutherford, Curie, Schrödinger, etc., found). In such a context the nuclear physics era started: the discoveries of neutron and fission followed during the fourth decade: the related developments in technology (from ideas by Hahn, Meitner, Bohr, Compton, Lawrence, Szilard, Kistiakowsky, etc.) culminated with the construction of the Fermi pile in 1942 and the working atomic bomb. The background history of nuclear energy is outlined hereafter.

2.1. The Growth along the Past Road

The entire timeline is sketched in **Figure 1**, and is framed as the developments

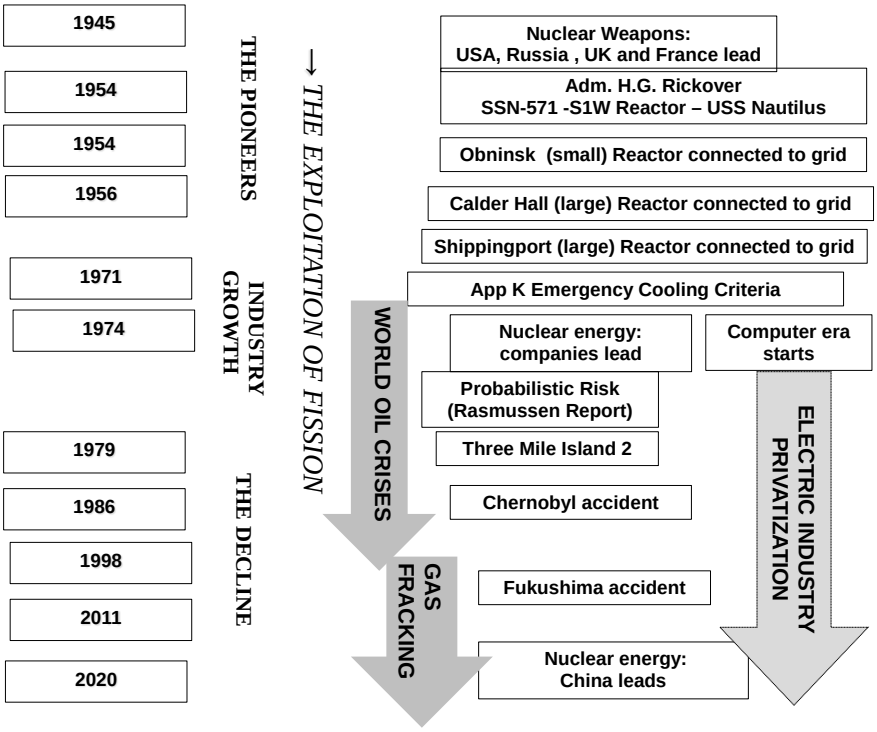

Figure 1. Summary history diagram for nuclear technology.

since WWII with the nuclear weapons development fully described by Richard Rhodes in two masterly books, [10] and [11]. The advent of nuclear energy derived from a reactor core was a specific turning point in the world and for an excellent account and detailed insider's view of the whole development since WWII, see the text by B. Goldschmidt, [12].

The demonstration of sustainability of the fission reaction is a fundamental landmark for mankind equivalent to the discovery of fire, achieving the ability to produce carbon steel products (the "Iron Age"), the discovery of thermal engine, or the proposition of the "$E = mc^2$" formula. At that historical moment, *i.e.* the end of the WWII, Hyman Rickover entered the nuclear era and made nuclear energy useful for peaceful purposes—the nuclear submarine deterrent and the nuclear powered aircraft carrier, able to strike anywhere at any time. The first nuclear-powered engine and the first atomic-powered submarine, the USS Nautilus, were launched in 1954, and soon sailed the world.

As in the case of Fermi, several excellent books have been written to describe the life and the findings of Admiral Rickover, whose determined and driven leadership focused on attaining needed results despite much opposition, e.g. [13], [14] and [15]. For the Nuclear Navy, the selection of water fixed a roadmap involving high pressures and the consideration of the vessel as the key component for the system design. Other peculiarities of the resulting PWR loop can be stated as follows:

1) Avoid saturated boiling in the core to preserve the uniformity of neutron flux as much as possible.

2) Introduce steam generators to allow boiling and steam production, *i.e.* in a fluid different from the fluid passing through the core, suitable to move a turbine.

3) Relative elevation difference between core and steam generators in such a way that natural circulation can remove the decay power should main coolant pumps go out of order.

4) Piping connection with the pressure vessel at an elevation above the core and with a size (pipe diameter small enough) to allow core cooling following the unfortunate event of pipe break.

The design of PWR incidentally included technological facets which made replication specialized: key ones are the pressure vessel itself with thick walls unsuited even for heavy industry, the sophisticated control rod drive, and the fuel assemblies. So as commercial power plant designs emerged, and the commercial industry took off worldwide, many technology licensing agreements were signed between the USA manufacturers with industry partners in France, Japan and Korea, not only to bolster the defense of the then "free world" but also enable further development of their post war economies. The restraints on fuel enrichment know-how and on nuclear technology transfer eventually lead to "new" national designs and independent nuclear weapons and reactor programs (in UK, France, India, Pakistan, China, etc.). We need not dwell deeply on these topics, and it is fully described in many texts elsewhere, see e.g. [16] (nuclear fuel and enrichment) and [17] (nuclear reactors in the world), and the consequences continue today.

The privatization of electricity industry, [18], was born in the late 50's to improve the industry performance inside a competitive market, [19], and received an impulse for the electric sector in the USA towards the end of 70's and later on reflected in EU. Noticeably, France a major nuclear energy user is among the last Countries to adapt the electricity industry to the new market exigence.

2.2. The Decline: From Active to Passive

But there was real progress, with 400 reactors (considering those permanently closed reactors that have been in operation are 500 or more) successfully operating worldwide, with numbers continuing to grow despite international tensions, various wars and conflicts and the ending of the Cold War. In fact this even freed up the Russian nuclear sector to partnering and build agreements .As shown by **Figure 1**, the overall evaluation is that from the 1970's, nuclear safety was driving the technology. Nowadays (2020's) nuclear safety is lagging behind. Partly due to the low popularity of nuclear energy, but also the decrease of many governments' involvement in favor of supposedly "greener" energy "options", lacking commitment to nuclear fuel re-cycling since there was no global energy or uranium supply crisis, and the emergence of higher efficiency combined-cycle gas and supercritical coal plants.

As a result, new technology developments of breeder and high temperature reactors have been largely abandoned or downsized in US, UK, France, Germany

and Japan, and although it was recognized that international cooperation in R&D must take place (e.g. via the Generation IV International Forum and other organizations like the IAEA and OECD/NEA) the designs actually sold in the marketplace still all used technology fundamentally firmly rooted in the 1950's along with the traditions in licensing and engineering standards that had emerged as a result.

The uncertain political support for nuclear energy, the adoption of an arbitrary risk perception metrics in decision making, instead of outcomes from rigorous risk analysis and the ease with which it is possible to manipulate public opinion, exhausted major nuclear industries mainly in what formerly (last few decades of the XX century) was the "industrialized world". One may provocatively state that the nuclear industry was hit by technology un-relevant events and reacted by pursuing purely fashionable developments.

The first example is the use of gravity-driven emergency cooling systems to remove megawatts of thermal power from the relatively small core region despite the "wheel being invented", where the wheel signifies energized and active pumps. The emergence of so-called passive systems constitutes challenging designs which lead to changes in the overall layout and indeed coolant of reactors. The fashionable motivation to use passive systems at any technological cost does not create question marks on the reliability of the gravity force, but opens unsolved (and not easily solvable) queries about the demonstration of minimizing the risk when relying on natural circulation as the dominant heat removal process.

The second example is the possible deployment of Small Modular Reactors (SMR). If those SMR constitute a technological need, e.g. in remote regions of the planet or for special application other than electricity production, their use is unavoidable and consistent. On the opposite, if the SMR are the product of an energy market incapable of providing suitable financing to the construction of larger size nuclear reactors, a defeat of rationality occurs together with the return to the witch hunt of middle age blaming the designs of current nuclear reactors despite smaller designs costing more per unit output (***Note*-1: *having more units deployed is generally a greater overall societal risk being this roughly proportional to the number*; *so deploying* (*more*) *smaller units must be made proportionally "safer" than* (*fewer*) *larger ones***). The SMR may also suffer because of claims of the fashionable connection with gravity forces discussed in the previous paragraph.

The third example is the so-called Gen IV reactors consisting of those concepts not yet commercially deployed, [20]. For the time being those are chimeras (possibly similar to the fusion reactors) since basically their design and demonstration is at a stage far away from deployment (*i.e.* more than two decades) and innovations are in the hands of capable scientists and entrepreneurs rather than technologists connected with industry. So, Gen IV results are far away the present context, where facts in the past and frequency based risks are in the focus.

But now silently and simultaneously arising was the "Computer Age", which not coincidentally also had its origins in the need for complex nuclear weapons implosion calculations, reactor physics analyses and nuclear cross-sections and reactions. It arose due to the original and brilliant minds of von Neuman, and Turing, and the many now profitable developers of the GUI, integrated circuits, memory cards, Fortran, HTML, Mosaic, Google, e-mail, the internet, iPhones, parallel and "cloud" computing , virtual reality, computer-aided design (CAD), and, of course, movie downloads.

3. Nuclear Energy and the Road Today: Accidents, Markets and Their Impacts

Nowadays two or three governing poles can be distinguished as moving progress of the civilization on the earth, one of those being the former group of "industrialized countries", driven by the US. The control of the global market constitutes the main way to orient the progress; the energy sources are the key element of the market: it can easily be deduced that any decision related to nuclear energy affects the direction of the progress, [21].

The accidents and the resulting damages, mostly in terms of human lives, are tools to drive the decision passing through the public opinion; nonetheless the knowledge of facts about accidents appears important. Selected insights about the global market and the accidents are given below.

3.1. Accidents Actually Happened

We are where we are today partly because unexpected nuclear accidents strongly affected the nuclear era. The description of major accidents is well beyond the purposes of this paper: details of the technological conditions that brought to the accidents as well as the concerned system performances before the loss of core geometric integrity core is given in [22]. Here a few notes are outlined. One of the major problems is that everyone was caught off guard by accidents that should not have happened, at least according to the best expectations of the design rules and complex regulations. Even the best practices of Probabilistic Risk Assessment (PRA) with complex event trees and sequences show unverifiable low frequencies for core damage, and, of course, fail to actually prevent the accidents themselves, [23]. So what happened?

Until 1979 safety records for civil nuclear power plants were excellent everywhere, *i.e.* no sign of safety weaknesses (more details in the next paragraph); costs and construction time were under control; no public opposition was detectable: the importance of Fast Breeder Reactors to close the fuel cycle was recognized and related projects were underway; the future for fission energy was bright.

A refrain from nuclear teachers at University till before the TMI-2 accident (1979), was that nuclear technology as a difference from any other technology (oil, chemistry, car, etc.) has never induced fatalities with the noticeable excep-

tion of the SL-1 research reactor in Idaho (1961) (***Note-2: this "refrain" was actually questionable, because, in addition to SL-1 other nuclear technology induced fatalities occurred in the period 1955-1979—not further discussed here***).

The Rasmussen report in 1974, was a landmark in nuclear technology (**Figure 1**) marking the historical development of Probabilistic Risk Assessment, [24], see also [25]. The US NRC report demonstrated that current safety standards of nuclear technology were higher (or much better) than in other sectors of human civilization like transportation and car industry, health care, etc.; however, the comparison of fatalities and injuries coming from heterogeneous sectors of civilization might not prove to be fully justified.

The Three Mile Island (TMI-2) accident occurred in 1979, e.g. [26]; this had, at least, one less severe precursor in another US reactor. Human errors on the site (operator mistakes) associated with some inadequate knowledge transfer between research findings and industrial applications had a role for causing the core melt. However, safety barriers constituted by pressure boundary for primary fluid and containment proved to be strong enough and negligible radiation impact upon environment occurred. Noticeably, the TMI-2 type of event is part of the findings of the Rasmussen report, but did not receive adequate attention.

But it got even worse with the Chernobyl, [27], and Fukushima, [28], reactor accidents, and the causes have been extensively studied elsewhere and were due to combinations of design flaws, inadequate safety analysis and systemic management issues. However, "*The problem wasn't so much the damage from those accidents per se, but the sheer cost, which was enough to bankrupt even the most deep-pocketed owner or operator. Public panic has resulted in increased licensing times, design costs, and provision of extra backup power and cooling options for existing and new plants*", [4]. Purely political decisions to phase out or essentially abandon nuclear power occurred for instance in Germany after Fukushima; and in Italy which before 1986 had six reactors in operation or close to operation and 20 more under advanced design.

As we have also said, [1]: "*Superficially, the trends and outcomes from rare events in energy systems and technologies worldwide are different from the risks involving massive financial defaults, crises, and losses. But all technological and transactional systems share the common involvement of human learning and risk-taking when goods, products, and services are involved.*"

And:

"*What were the major impacts from Fukushima and from Deepwater Horizon? Those accidents put people in fear and trepidation of potential harm, even at large distances away when the actual risk is negligible. There was also societal fear and media reinforcement of possible extensive damage to homes and the environment, which can cause social disruption, trauma, and even evacuations. Of course, these accidents did also produce actual economic, financial, and social consequences, with losses in energy production, corporate value, and business markets. And there was a consequential reduction of public confidence in*

political, industrial, and social institutions."

3.2. Market Reforms and Investments Consequences

The overall structure and functioning of world energy markets is well covered elsewhere, and the DoE Energy Information Agency, the World Energy Conferences and many oil and gas companies publically share comprehensive reports on past, present and future energy use, nationally and globally, e.g. [29] [30], and [31]. Although varying in the details, viewed in a global context, these reports and massive economic models all show a declining future for nuclear energy's market share.

The consequence of the seriously frightening accidents and of electricity market "reforms" upon the nuclear industry can be easily perceived. There was abandonment of nuclear energy by some like Germany, making Europe even more reliant on imported gas; more safety requirements for back-up power systems; and lower interest from the USA to expand the nuclear energy market. A more subtle impact comes from privatization, which together with the unavoidable split of ownership of energy market quotas, makes difficult large investments and long-term (several decades) strategies, which are intrinsic characteristics or needs for investment in the nuclear industry.

If that was not enough, post 2010 cheap natural gas and oil from new and innovative US "fracking" technology exploded onto national and world energy markets, lowering market prices, lowering emissions by substituting for coal, and increasing efficiency with combined cycle technology and low capital cost modular units of 20 through 300 MW(e). By providing lower cost energy, world economic growth is enabled, since 90% comes from such sources, but this does not solve the issue of rising carbon dioxide levels in the atmosphere and the potential for possibly irreversible climate change. Only nuclear energy, by deploying thousands of GW(e)-size plants between now and 2050, can really and truly help stabilize anthropogenic emissions, enable electrification of transportation, and support needed alternative fuels (like hydrogen), while synergistically helping intermittent renewables to flourish, [32].

This is all been well known for 20 years—but 20 years of inaction and missed international targets has now lead to historically high CO_2 concentrations and almost hysterical reactions. In any case atmospheric pollution should be halted… and nuclear option is a viable option: clearly pollution is not stopped by more fracking.

Finally, while major nuclear projects succeeded in China and the Middle East, new builds in France, Finland, USA and UK suffered $B in budget overruns, plus years of delay in schedules. These projects were still mainly "one-off" despite attempts to standardize features and streamline licensing reviews, with local changes to requirements that can often take several years. This is a clear message that new approaches and skills are needed and necessary in both licensing and project management.

Major financial and corporate restructuring occurred of major designer/builder companies (*i.e.* AREVA and Westinghouse) and the UK and Canada had already given up state or government control of their nuclear build enterprises. Into this void have rushed many entrepreneurs asking for funds while promising smaller, cheaper, easier to build concepts—but despite the claims none yet openly competitive with natural gas and large plants, [33] and [34]. Governments have responded and sounded their support for new nuclear plants and concepts, but the competitive market place has not. So state subsidies, financing guarantees, power purchase agreements, carbon "offsets" or "emissions credits" and assigned values have or are having to be employed to sustain the industry and also keep some existing units operating. New research grants and funds have also been put aside for keeping some level of knowledge and expertise at the national level.

4. Nuclear Safety Evolution as of Today: "Barriers" and Advancing Safety

Meanwhile in modern society, considerable evolution of thinking about safety has lead to reinforcing purely "deterministic" analyses of specific accidents with the extensive use of probabilistic methods and their related performance indicators. For an excellent and comprehensive summary in multiple industrial applications see e.g. [35], where the "… *the aim is to find safety indicators*, *existing or newly developed*, *that can be used successfully as tools in safety management*", concluding with the need to progress from purely reactive (past performance) to proactive (future) indicators. Risk-informed decision-making processes and methods are already embraced in a number of other arenas where catastrophic failures can be a very public spectacle, e.g. [36]. It is in the spirit of adapting this approach that the following evolution is developed for advancing nuclear and operational safety from the stasis where it resides today.

4.1. The Use of "Barriers" as Part of Defense-in-Depth

To minimize accident occurrence and any consequences, traditionally in the nuclear, oil and gas, chemical and airline industries, safety "barriers" have been included in the designs against catastrophic failures and their consequences.

However, it is silent on the financial consequences. Postulating some event, engineered systems and computerized controls are in place, supplemented by physical barriers, redundant back-ups and reinforced by operating procedures, intensive training, administrative controls and safety "management" systems. Sometimes called "defense-in-depth", these multiple barriers are layered or interleaved, supplementing and reinforcing each other. They are superimposed on design margins to failure, which are adequate to account for data uncertainties, lifetime performance degradation, and simple lack of knowledge. So for nuclear energy currently we presently have all of these "barriers" types in play:

Procedural:

1) Codes and standards for design with built-in safety margins;

2) Licensed professional operators who are fully trained;

3) Security staff, controlled access and anti-intrusion measures;

Safety control:

4) Physical barriers against failure, like fuel cladding and primary circuit materials;

5) On-line monitoring of the performance, operating state and limits;

6) Engineered safety and back-up systems for assuring power and cooling;

Event management:

7) Large containment structures to retain any radioactivity or damage;

8) Exclusion "zones" around the site boundary as a precaution;

9) Emergency supplies of equipment and personnel from offsite;

Societal protection:

10) Evacuation procedures for any potential exposed population;

11) Restrictions on radioactive releases, doses and materials;

12) Extensive independent licensing, management safety and performance reviews.

4.2. Why Barriers Do Not Work or Can Be Penetrated

A formidable and comprehensive list indeed, and are all desirable and self-evidently safe—or are they? In James Reason's classic "Swiss cheese" analogy, barriers of all such types and schemes can be "penetrated" or bypassed or be vulnerable, so we now know even these listings are not sufficient.

We already know that physical, design and administrative barriers can be breached (the classic clad, circuit and containment as already shown by TMI, Chernobyl and Fukushima). We already know that computer, administrative and procedural barriers can be breached when involving human actions and decisions (TMI, Chernobyl, Deepwater Horizon, Boeing Max 8 …). The airline industry has reached the lowest possible demonstrated crash/failure rate for any industry (other than concrete dams) and still has accidents that are attributable to human induced failures and mistakes, [7].

Accidents are no respecter of international boundaries, national culture or even national pride, let alone barriers. It has happened in the USA, where licensing complexity, safety procedures, design rigor and investment protection are crucial, and accidents should be controllable but barriers failed by turning needed systems off. It has happened in Soviet Union, where state control of everything failed to foresee simple mistakes in the pursuit of doing the tests that were ordered despite being unsafe and unstable to do so.

And it has happened in Japan, one of the safety conscious and risk averse nations in the world, where safety margins against flooding due to a tsunami wave were simply not sufficient. This occurred in a nation whose trains always run on time, whose pedestrian crossing and road safety signs abound, whose people wear masks if they have a virus to protect their fellow citizens, and where there is so little expected risk there is even not an original Japanese word for "risk".

As a panacea, there seems no point in just adding more barriers, layer on layer, or even adding a real time "risk monitor" overlay because they have already been shown to be penetrable or rendered inoperable. The increase in the level sophistication of I&C, as an alternative (or an addition) to more barriers, may also results as a no-achievement from the safety view point, [37]: new components create new pathways for events and new statuses for the system which cause potential bifurcations more and more difficult to be characterized. The failure of Boeing Max8 aircraft computerized anti-stall system to stop the pilot fatally stalling the aircraft is a recent tragic example.

Also the overwhelming temptation in probabilistic risk assessments is then to multiply the probabilities of "independent" failure of each, resulting in extremely small numbers that then cannot be verified experimentally or by human experience (see any modern PRA…)! We have truly taken the modern probabilistic risk methodology (event trees and sequences) to the limits of its applicability and credibility, particularly as actual events occur more frequently than ever predicted.

The ever-popular use of "Risk Matrices" has been widely adopted as a means to identify major hazards, including fiscal exposure and business risks. But apart from arbitrarily and conveniently categorizing risks (say, into high, medium or low; or likely, unlikely, extremely unlikely, etc.) there are no technically quantified risks or frequencies. Their consequence ranking, small, large, and unacceptable, simply enable some objective scrutiny and a means of setting relative priorities-while implying that management is being shown to be prudent and/or following regulatory requirements.

5. Risk Is Not Probability Times Consequence

Risk is relative, and although we may adopt a loss probability function where the probability is less the greater the damage or loss, risk will still depend on the future (posterior) exposure and the number of prior outcomes or events.

5.1. Defining Risk

We need to think about what we mean by "risk". Risk can be defined as due to uncertainty, and is perceived by us, individually and collectively, as being a high risk or not based on how we feel about it, and have been taught, trained, experienced, learnt, or indoctrinated. The implications are for the development of socially acceptable safe design and operation of modern technological systems. In particular, for nuclear plants, the exclusion of core melt and of radioactive releases may indeed form the new Social Design Basis (SDB), [38].

The key and clearest definition comes from the financial arena where fortunes are won and lost, and financial crises come and go, [39]: "*Risk entails two essential components: exposure and uncertainty. Risk then, is exposure to a proposition of which one is uncertain.*"

The key challenge is to comprehensively derive a quantified risk assessment

for a design basis for a complex technology which including the social impacts or consequences, h. Note that the relative consequence or the total risk exposure, R, is not given by the commonly adopted point value multiplier of (probability-times-consequence) or $P \times h$, but depends on the varying risk exposure. In that traditional usage, just multiplying the numbers can make a low probability high consequence event which is quite destructive the same "risk" as a high probability but low consequence happening, which it clearly is not. Equivalently and physically, the total risk exposure is the total area under the probability-consequence risk curve, whatever shape or slope it has, and the fractional risk, ΔR, is defined as the magnitude of any incremental consequence or risk, Δh, times its probability of occurrence, viz

$$\Delta R = P \times \Delta h.$$

The risk from energy systems, energy production and energy use is low. But societies do not have a unified and universal measure of what constitutes acceptable risk—that varies with the activity, history, technology, substance and the regulatory or legal framework. The patchwork quilt of "tunnel vision, random agenda selection, and inconsistency" is already well known and documented, [40], and is unlikely to change towards some more rational basis. Clearly related to self-preservation, personal experience, and our perceptions, irrationally most people accept some necessary everyday risks (having a car accident), ignore others (being in a large earthquake or flood), take some (buying stocks), and reject others (jumping off a cliff). In today's energy-driven world, reactions vary worldwide to energy system accidents, like the meltdowns and explosions at Fukushima, major oil spills in the Gulf of Mexico, gas pipeline fires in California, and mine explosions and other disasters. There are thousands of related everyday casualties from global energy use, both directly from automobile accidents, airline crashes, train derailments, gas leaks, coal mining, and indirectly from industrial plant accidents and emissions. These events all inform us that the risks of existing within modern society are tolerated and even ultimately beneficial in some way, but only until they are no longer perceived to be safe or environmentally acceptable, irrespective of the actual potential presence of possible future harm, danger or exposure.

The whole topic of "societal safety" has received attention in Japan, one of the most risk-averse nations in the world. "*Dealing with problems that surround societal safety thus, requires not only revealing the physical and chemical mechanisms of accidents and disasters but also studying human, social, and economic environments that the problems relate to*", [41].

For those who wish to delve more deeply into the more academic aspects of this topic, the reference is full of useful information and perspectives that lead directly into the next key question.

5.2. Acceptable Risk: What Is It?

Nuclear energy use poses a special question, as its potential radiation threat is

unseen, just like carbon dioxide emissions. What is an acceptable risk for nuclear power? Or for any technology? Should they be compared to natural disasters, like floods or earthquakes? Or to the risks of other technologies? Or to some legal or societal norm or standard? Traditionally, for nuclear technology risk has been accepted the general heading of "adequate health and safety protection for the public". Attempts to define the "boundaries" or regions between acceptable/tolerable and unacceptable/intolerable risks have traditionally been based on the consequences, namely of the numbers of deaths, injuries, releases, or equivalent or actual costs, and the frequency of how often these events may occur. The regions and the boundary are both difficult to define, let alone implement. Even "relative" risk has been suggested as a measure of acceptability comparing, say, deaths from lightning strikes with death from cancer, or multiplying "probability times consequences" as some indicator. But, because of human errors and blunders, actual events occur that exceed these nominal limits, causing outcry, recrimination, inquiries, negative press, and even more regulations. They are the "rare events" or "black swans" that we did not expect and were not prepared for. So it is difficult to define a clear boundary while acknowledging the real uncertainties due to the finite significant probability of a rare event.

Superficially, the trends and outcomes from rare events in energy systems and technologies worldwide are different from, say, the risks involving massive financial defaults, crises and losses. But all technological and transactional systems share the common involvement of human learning and risk taking when goods, products and services are involved. The same issues of planning and preparedness against the unknown risk or rare event is the objective of risk assessment and safety management in the nuclear, aircraft, and oil and gas industries, as well as in the financial and military sectors. So we may apply universally the method of simply finding an estimate for the probability of any sized loss as a function of the risk exposure in order to determine the required dynamic response and management actions to reduce or at least contain the consequences. This preparedness for the unexpected is necessary, despite our best efforts at safety improvement and risk reduction; because we can never be sure that something similar will "never happen again".

Traditionally, the paradigm was that licenses to operate nuclear plants could be granted, since even if an accident occurred the consequences could be minimized. There was an "acceptable" risk because specialized training, safety assessments, engineered safeguards and containment buildings would work, so public health and safety impacts would be negligible and rare. Severe accidents involving core melt or, worse, radioactivity releases to the environment were not originally conceived within the design of nuclear reactors. Unfortunately those accidents actually happened, although caused directly or indirectly by humans, and causing widespread alarm.

The uncertainty of an Extreme Event happening, and its fiscal and social consequences, can be defined using probability and consequence measures, including social and political costs. We repeat that the risk of such an event is not given

by the often-used Risk = (probability-times-consequence), or by defining a negatively-sloped risk boundary between acceptable and unacceptable risks or some frequency vs deaths "FN" plot or frequency-consequence "F-C" curve. The risk is given by the total integral risk due to all possible exposure to releases, fears, damages, social and political disruption, and we can derive the exact expression for relative social risk using a social damage relation. Therefore, it is not correct to adopt "expected deaths" or probability of release or severe-damage consequence which use the traditional safety measures, calculating radiation doses to hypothetically exposed populations using a hypothetical and overly conservative linear dose-response relationship, [42]. We need to know the real societal risk not solely the postulated risk of radiation exposure, especially since real severe events cause more deaths by or due to evacuation and psychological stress than by actual irradiation harm.

But actually the accident at the Fukushima reactors was notionally an "accepted risk" at least according to international reports from 17 countries, [43]. Using Probabilistic Safety Analysis, (PSA) and judgment the "acceptable" core damage frequency criteria for any existing plant is of order 0.0005 to 0.00001 per operating-year. This means for every 10,000 reactor-years of operation and we should expect a disaster. Now, between Chernobyl and Fukushima there are indeed about 10,000 reactor-years… so, simply we should not be surprised also in view of the fact that no safety renovation was done in Fukushima—possibly again due to Japanese culture. In addition, the so called "coping times" for operators and emergency staff to deal with loss of power (on-site and off-site) by restoring power (on-site and off-site blackout) and cooling were successively raised from 24 to 48 hours, [44] and [45]. But in reality, in Fukushima the back-up power failed due to the flooding for many days, so now 72 hours is judged to be the coping time frame, [46], when in fact natural disasters can and do cause severe infrastructure damage and power outages lasting several weeks, [47].

Following Fukushima, thousands of miles downwind and downstream, due to panic buying pharmacies in Vancouver in Canada ran out of iodine tablets widely known to limit iodine uptake to the thyroid gland. Nowadays severe accidents are part of the design of reactors; however, not even entering the discussion about the common-cause-failure, at least two philosophical questions, which have no accepted answer, occur:

1) What is the minimum probability for a severe accident that needs consideration in the design?

2) To what extent the new spectrum needs to be considered in the design?

One opinion we have on this topic can be summarized as follows, e.g. [4] and [9]: The limit probability to be considered for design against severe accidents shall be comparable to that for rarely occurring cataclysmic events that may damage or disrupt the world (e.g. meteor impact, super-volcano eruption, disease epidemics, and thermonuclear war) which populations today accept as part of being alive, *i.e.* constitute a negligible everyday risk.

But there is a major and unavoidable problem with this ideal relative risk approach because it deals with happenings that may be totally outside human experience and, importantly, we actually are unable to prove the probability by testing or even analysis. After all, most modern technologies have had their very own catastrophic failures (e.g. Deepwater Horizon oil leak, Concorde aircraft and shuttle crashes, train accidents, bridge collapses, chemical plant explosions, etc.): these are accepted events as we learn and try to avoid what happened. The major involvement and the most dominant cause is not some random act of nature, but systematically due to the unavoidable human involvement. Humans make mistakes: always have done, always will do. Still, the arguments above are suitable to explain that unavoidable severe consequences exist (and related occurrences shall be quantified to the best of our knowledge) and are part of our life.

As we have already stated, [1], "*If nuclear power is going to play a role in meeting the myriad energy challenges of the* 21st *century… then the industry has to embrace a risk model that integrates not just potential loss of life but social, economic, and political costs as well.*"

5.3. Design and Regulatory Complexity: The Need to Retain Control

The present approach to reactor safety is far too complex and for historical reasons largely based on showing or claiming "paper" safety. It has deeply layered standards, "requirements", volumes of regulations and technical reviews. In addition, following Fukushima, there was a plethora of "guidance" (so-called Regulatory Guides), lengthy reviews, and more binding legal enforcement and requirements.

But the need for reform was clear: "*This regulatory approach, established and supplemented piece-by-piece over the decades, has addressed many safety concerns and issues, using the best information and techniques available at the time. The result is a patchwork of regulatory requirements and other safety initiatives; they are all important, but not all given equivalent consideration and treatment by licensees or during NRC technical review and inspection*", [48].

Undue complexity, duplication of effort and unnecessary rules and regulations exist while every nation wants to retain its own decision making. Even the Regulators themselves recognize there is a problem, and is reinforced by the latest reporting (https://dailyenergyinsider.com/news/23528-nrc-proposes-new-rule-for-emergency-preparedness-for-reactors/) that the "*The NRC is proposing to create an alternative emergency preparedness framework for SMRs and other new technologies. The NRC would adopt a risk-informed, performance-based, and technology-inclusive approach.*"

This is at least a first step, but still leaves in place the existing myriad of regulations, guides and requirements that affect safety systems design, and multiple overlapping regulatory "regimes" which is now also recognized as requiring

coordination.

"*If two mature regulators conclude they have no reservations with a design during a pre-licensing review, there should be minimal impediments during the licensing process … I think the time is now to think boldly and look critically at regulatory frameworks and be open to the need to re-engineer them. It may be time for a paradigm shift in the regulatory space*" (extract from remarks by President Velshi, CNSC, Canada, at the International Framework for Nuclear Energy Cooperation, Washington, DC, November 13, 2019).

The actual safety objective is a very simple one, is not based on how often the core might melt or activity release might occur, but has already laid down clearly for some time: "*Humans must remain in control of their machinery at all times. Any time the machine operates without the knowledge, understanding and assent of its human controllers the machine is out of control*", [49].

We just need to remain in control at all times which is a fundamental safety precept.

Even for the safest technology presently operating and quoted as an example, there are still key issues. The recent (Oct. 29, 2018) crash of a brand-new Boeing (large) airliner (Lion Air Flight 610) in Indonesia is sadly taken to enter the subject of (I&C) and the man-in-control-of-machine requirement. "*The accident had been caused by a complex chain of events, Indonesian air accident investigator Nurcahyo Utomo told reporters at a news conference*, (www.bbc.com/news/business-50177788) repeatedly declining to be drawn on providing a single dominant cause. "*From what we know, there are nine things that contributed to this accident*," he said. "*If one of the nine hadn't occurred, maybe the accident wouldn't have occurred*." Moreover, the official report states what must seem blindingly obvious: "*The aircraft design should provide the flight crew with information and alerts to help them understand the system and know how to resolve potential issues*", NTSC Aircraft Investigation, 2018 (knkt.dephub.go.id/knkt/ntsc_aviation/baru/2018).

The following items arise:

1) Complexity is the design answer to efficiency and cost savings in a competitive world.

2) Progress of civilization is connected with increasing complexity.

3) Cable and component aging may be seen as a huge (controversial) issue

4) Cyber-security for critical infrastructure constitutes a modern issue.

5) Vulnerability of components to fire, possibly in conjunction with radiation hazards.

6) Resistance of components to thermal and mechanical conditions following an accident.

These recent crashes of the Boeing Max8 aircraft are due to faults in the overall anti-stall computer system with its all-too-human interface with pilots who lose control. As a consequence: I&C may fail in a complex modality; I&C may bring the reactor status in an unforeseen or unknown condition; hidden (or la-

tent) I&C failures including humans interactions may occur which add-up and bring any safe reactor status into a unrecoverable radiation spreading nightmare

I&C, including automated and digital systems in water cooled nuclear reactors are part of an exponentially growing technology including several connections with non-nuclear industry and a wide variety of expertise. Any effort to synthesize the current status or to characterize weaknesses within a paper like the present one may sound ambitious or impractical (see also connected insights in Section 4.2).

We can introduce new thinking by applying what we know from past accidents and the failure of past and present practices. We can learn how to improve on "paper" licensing, using real safety, actual builds and plant operation, and by using the precepts and discipline of Process Safety Management in adopting modern tools and technology.

6. The Future Signpost: Proposed "Safety Approach" and Objective

Hereafter an attempt is made to pursue the objective of the paper: *i.e.* to identity a way to slow down and to stop the decline of nuclear technology by erecting a sign post for the future. This implied the identification of technological areas where substantial improvements can be attained based on current knowledge and established research outcomes.

6.1. A New Safety Construct

What is needed going forward is a new safety construct, building on what has been done and achieved to date, but also simplifying and removing unnecessary multi-layers of defense-in-depth "stuff" (margins, rules and regulations) adopted in the name of safety while not actually improving it. Generalized risk-based concepts have been proposed before e.g. by NRC for new not existing designs and linked to over 200 other 10CFR rules and regulations, [50], but are literally layered on top of these existing rules rather than constituting a new paradigm.

A "new" safety is philosophy and approach is technologically feasible which, among the other things, based on the intelligent and continuous monitoring of the existing schemes, but which integrates and simplifies them. Not all then have to be or remain "safety grade" (the implications of those words are not discussed here) equipment, fully qualified and comprehensively tested, nor do they have to have repetitive extensive safety reviews.

The existing defense-in-depth (DiD) systems simply represents common sense measures that back-up the overall system, and is related to what Robert Bea and many others call Process Safety Management defined by this distinguished risk analyst as: "… *a disciplined*, *highly organized set of approaches and strategies whose goal is the prevention of catastrophic failures involving complex engineered*, *human-based systems*", [51]. Further he stated: "*We take those insights*, *put them back into the proactive planning types of things to prevent*

making future failures. Learning is crucial." Furthermore, process safety has two components, paraphrasing the testimony ([51], p. 293):

1) the proactive element, things done before to ensure that as operations are carried out, that the likelihoods and the consequences of catastrophic failure are acceptable.

2) the reactive element after performing important activities and pervading the entire life cycle of a system from concept to decommissioning, cradle to grave.

Further the approach is modeled after the commercial nuclear power industry and includes supporting and reinforcing human decision making such that ([51], p 341) "*it takes special things at that sharp end to manage crises, particularly when the pressures of time, information are present so that they can observe, orient, decide and act*." In addition: "*Decision-making capabilities have and will be impaired during a crisis. Whether a crisis turns into a major accident depends on the planning that is done in the months and years before the crisis arrives*", ([51], p. 343). Applied in real time to real events, these pro-active and re-active components are necessary for retaining control, at all times, which is the overriding safety objective.

Examples of such nascent decision-making capability also already exist operating at amazing speeds with massive impacts on dynamic and/or evolving risk: internet searches with instantaneous updating, short and long term weather forecasting and storm tracking, algorithmic e-trading of stocks, military C3I and missile interception, satellite and personal surveillance using i-phone tracking, GPS driven trucks, robots and drones in armies, transportation and traffic flow management, deep well drilling just-in-time delivery, just-in-time manufacturing—the list is endless and growing. Why not for nuclear reactor safety?

Today, compared to when present nuclear reactors were first introduced many years ago, we are now capable of much enhanced information gathering, processing, assessing and managing in support of decision making:

- remotely controlling what distant spaceships are doing,
- viewing and manipulating how complex or robotic surgeries are being performed,
- targeting weapons with extreme accuracy over great distances,
- performing detailed calculations of how the world's oceans, weather and climate change,
- remote monitoring of movement and transport by satellites and miniature sensors
- communication links at extreme speeds,
- digital "reality" of systems, components and in extraordinary detail,
- virtual design and engineering, including full "caves" and system walk-throughs,
- mass production using computer driven machines,
- security and surveillance at the macro and micro scales,
- "intelligent" processing of information and signals,

- complex modeling of system response and predicted behavior in supercomputers.

What we call a safety "barricade" can also be called "the consistent consideration of current Defense-in-Depth". So the minimum number seems to be four distinct but overlapping defense-in-depth requirements (not "barriers") that follow the principles of Process Safety and what we have learned from prior events:

1) Elimination of unacceptable system statuses in and by design and by the margins to failure (e.g. no melt, no radioactivity release…).

2) Elimination of unacceptable system statuses by control (e.g. safe limits never exceeded, redundancy/diversity of indefinite cooling and of power …).

3) Elimination of unacceptable system statuses by relentless focus on safety by the humans involved (e.g. in management, maintenance and operation...).

4) Elimination of unacceptable financial risk so the focus remains on safety not on profit and price (e.g. investment incentives, guaranteed ROI, large market place penetration…).

They are not the layered combined probabilistic deterministic "protective strategies" defined by the NRC, [50] (§ 4-4, pp 4-15, 16), since that includes "*the uncertainty associated with the parameter values and models*" used in the PRA to "*verify that the quantifiable margins… are acceptable*". From actual events and Fukushima, we already know these layers combine to provide potentially misleading and unverifiable estimates of the core damage frequency and do not fully or adequately include the human element in severe event prediction, causation and remediation.

In Fukushima at very beginning (*i.e.* 10' - 30' after tsunami hit the units) among other things they did not catch the severity of the situation. This is why we need a possibly automatic tool (part of what is termed "new" system) to autonomously (as far as possible) detect the severity of the accident and eventually react: the automatic, instant reaction (e.g. related to ERT, see below) should be in addition to later human reaction.

The "reliability" of successfully deploying the Emergency Rescue Team (ERT, or any and all back-up systems) can be used to determine the probability of success (*i.e.* incident/event conclusion, containment or aversion). It is not possible to show a failure probability less than about 10^{-2} per demand (from learning theory and comparisons with actual human performance and emergency equipment data).When there is serious deployment or access difficulty little credit can be claimed for enhanced or speedy recovery, as shown by the Fukushima and all severe event data; however, (preventive) emergency preparedness and exploitation of technological tools available from the progress of civilization constitute duties for the designer. .

6.2. The Dynamic Barricade for Safety; A, B, C, D and E

The outline of the possible structure for the dynamic barricade is given here.

Previous published documents, [52], provide a view of what is called a "technological safety barrier" coming from: 1) currently identified weaknesses (e.g. nuclear fuel pellet and clad, noticeably at high burn-up), 2) fundamentals of reactor design (e.g. circulation modes and mutual elevation between cold leg and core, size of cold leg, etc.), 3) concerns associated with increasing system complexity (e.g., as already discussed, I&C issues). Although advancement in nuclear safety and related probabilistic assessment had a key role when defining the features of the new technological barrier (see cited documents and the IAEA Integrated Risk Informed Decision Making, IRIDM, [53], as discussed below) a different background perspective for the need of what is called a dynamic barricade is provided hereafter.

The new barricade is technological in its philosophy and is constituted by a combination of the following elements, which have a heterogeneous nature and role:

Element A: the As Low As Reasonably Achievable (ALARA) principle,

Element B: the Independent Assessment (IA) requirement,

Element C: the Best Estimate Plus Uncertainty (BEPU and PRA) approach,

Element D: the Extended Safety Margin Detection (E-SMD) concept,

Element E: the Emergency Rescue Team (ERT), nowadays a virtual entity.

The entirely new element is a dynamic risk-informed "technological" barrier, needing electric and electronic (E-SMD) and latest computational tools (BEPU) applied to the analysis of any safety related aspect (so-called BEPU-FSAR, [54]); it is ERT supported. The words "risk-informed" require full consideration of Probabilistic Safety Assessment, (PSA), as well as integration of related techniques into the Integrated Risk Informed Decision Making (IRIDM) framework IAEA, [53]; but, how to achieve these is not pre-specified or prescribed in rules, regulations or guidelines.

The words "technological elements" reflect the irresistible progress of modern technology including the database of knowledge (e.g. a new magnitude of earthquake in an assigned geographical region) and shall be constantly upgraded. The words "electric" and "electronic" give the proper emphasis to:

1) the consideration of Instrumentation and Control (I&C) into the safety analysis;

2) the design, and the operation of necessary detectors for fulfilling the needs of the E-SMD element.

The word "computational" stresses the importance of analyses that are qualified and independent from the designer and operator of the reactor.

The words "ERT supported" emphasizes the need for ERT, while the E-SMD continuously monitors the NPP, the environment and the actions of the staff, and eventually solicits the intervention of ERT.

Any implication or suggestion is not correct that this is some form of auto-safety wresting control away from operators and humans. Instead it reinforces their decision-making but does not replace it, as stated by the key INSAG-25 report, [53]: "*It is a fundamental aspect of Integrated Risk Informed*

Decision Making that the consequences of decisions affecting safety should be monitored and feedback provided on their effectiveness. Performance measures should be developed and monitored. Such measures should be measurable, observable, or calculable and should be sufficiently comprehensive as to provide the capability to assess safety in a comprehensive and complete fashion. If a performance measure is not satisfied, there should be a process in place that will result in immediate and heightened safety awareness."

We propose that these measures are NOT static risk or performance "indicators", or incremental changes of calculated "core damage frequency", some form of "industry trends" or "performance-based metrics", or whatever jargon is prevalent as part of current regulatory "oversight"; see e.g. [55]. These can be discarded—a thought unlikely to be popular with those currently wedded to and invested in such items. 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.

This technological barrier is and must be a dynamic system tailored to each reactor, although design philosophy as well as procedures and databases are in common to all reactors, reflecting the need of consistency. We can then replace and discard other monitoring metrics, reporting requirements and paper studies to enable focus on real safety.

Furthermore: 1) Element A, the ALARA or ALARP principle imposes we have to do our best, considering severe events, the threats to critical infrastructure and necessary "resilience" measures, [47]: among the other things this requires safety analyses, defense deployment and restoration actions dealing with the worst situation(s) that we may expect or conceive; 2) Element D, the E-SMD implies an early (as quick as possible) detection of the severity of the event, in real time based on accurate knowledge of the potentially degraded plant status, risk assessment options and degree of system control; here one may also state that E-SMD looks at the derivative of the event, requesting protective actions before reaching an assigned system degradation status; 3) Element E, the ETT takes and processes these inputs, assessments and principles (*i.e.* from previous item) and would call for an immediate action by ERT who should be prepared to deal with such condition because of item (1) and undertake unequivocal decision making, not hampered by any perceived or artificial divisions of responsibilities and interfaces (e.g. between operator, manager, owner, local, state, regulatory, emergency and federal and national entities).

The principles of using such a dynamic risk analysis approach have already been demonstrated for the major Deepwater Horizon/Macondo oil spill caused by well blowout, [56]. Using a suite of event trees and analysis of barrier failures, including not only physical but management and emergency systems, enabled the prediction of the probability of not attaining a safe end state. The key statement is: "*The prior probability provides a snapshot of likelihood of failure. However, it fails to provide better understanding of how a system deteriorates*

with time. Similarly, the prior risk provides understanding of risk at a given time; however, it is not able to change with time or the situation. Therefore, it is not preferable to derive safety critical decisions based on prior risk. For better understanding of system safety in changing conditions, posterior probabilities (or updated probabilities) are studied". Importantly then "*It is concluded that if the proposed dynamic risk assessment methodology with comprehensive abnormal event investigation method were used and implemented properly at the Macondo well, this accident could have been avoided, or at least could have been controlled with less severe outcomes*." This fact and capability was shown by continuous updating of the "risk profile" during the entire event.

The current NRS derives from the amazing history of nuclear technology when in less than fifteen years (*i.e.* from the demonstration of the fission chain reaction to the operation of the first power reactor) nuclear physics became nuclear technology. The impulse for design innovation is understandably attenuated (or weakened) once reactors entered into operation: attention of designers was rather given to the safety demonstration, namely after the issuing of the Interim Acceptance Criteria (IAC) for Emergency Core Cooling Systems, [57]. Nuclear catastrophes (Three Mile Island, Chernobyl and Fukushima) also triggered new activities and important researches for design improvements mostly focusing towards the origins of those catastrophes. Definitely, technology advancements were consistently included in subsequent designs of nuclear reactors: however a mechanism was never actuated to check whether design (and safety) improvements are consistent with current knowledge. The decline of the interest from the public and policy makers in combination with the global market exigencies also brought to this situation: so it is understandable that stagnation followed the gigantic effort completed in the 50's of the last century.

6.3. The Overall Functional Design and Essential Features

These insights into the history of nuclear physics and societally acceptable risks create a different background perspective (*i.e.* related to previous description documents) for here we introduce the idea of the dynamic barricade, see below. This should be seen as an attempt to re-establish the close connection (which existed during the 50's of the previous century) between safety-design of nuclear reactors and advancements and competences acquired in research. The attempt is made concrete by the elements discussed above and superimposed in the diagram of **Figure 2**.

Nuclear Reactor Safety (NRS) can be imagined as formed by the two boxes colored green and pink, respectively, in **Figure 2**. The green Requirements box includes the safety objective, and principles; the pink Features and Functions box includes the process safety design that constitutes the glue between the above two boxes and can be imagined as constituting the functional integration of both key overarching principles like "Fail-to-safe" and "ALARA" (on right, as derived in radioprotection) also connect the two boxes. The yellow Safety Analysis

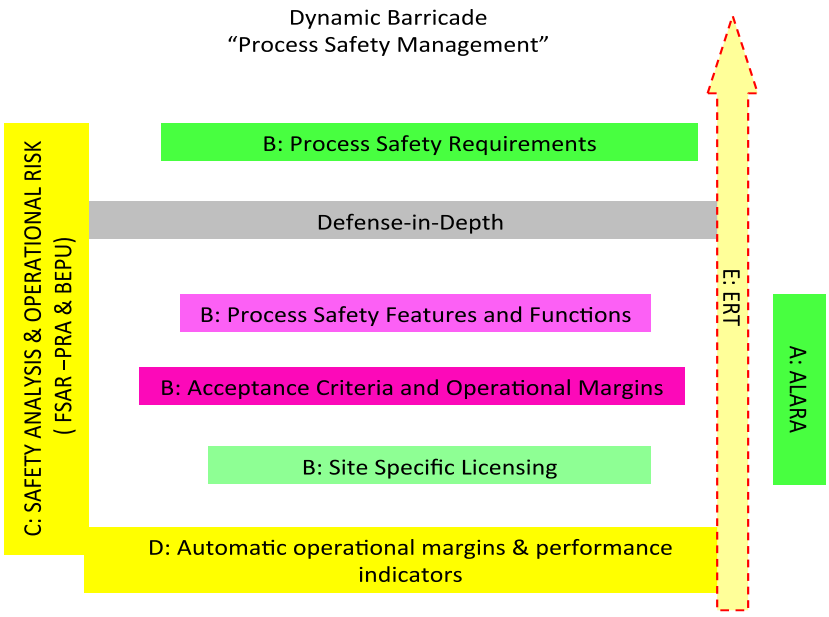

Figure 2. The ABCDE vision for nuclear reactor safety.

and Assessment (left side of the figure), includes whatever updated and situation specific "probabilistic" or "deterministic" methods that allow the demonstration that safety is correctly part of the design of the nuclear reactors and confirmed in and by operation.

The vertical dotted yellow arrow is the ERT, which is the needed additional constituent of the dynamic barricade, providing continuous operational feedback, current and projected systems status and dynamic risk profile. This is based on the safety margins and performance indicators determined by the process state and history, totally integrated with the safety analysis and its uncertainties, thus minimizing the opportunity for errors in dynamic risk-informed decision making.

The following constituents are distinguished (details for their role, interconnections, design targets and quality demonstration shall be found in standard nuclear technology documents and cannot be detailed in one paper) as follows:

1) the Systems, Structures and Components (SSC);

2) the Engineered Safety Features (ESF) including the Emergency Core Cooling Systems (ECCS);

3) the physical barriers such as containment (to the release of radioactive products);

4) the safety functions and the alarms alsoconnected with so-called technical specifications for the operation of SSC;

5) the Emergency Operating Procedures (EOP) and the Severe Accident Management Guidelines (SAMG) informing the operators for the best management of ESF;

6) the Instrumentation and Control (I&C) monitoring the SSC and the ESF;

7) the Final Safety Analysis Report (FSAR) connecting all the items above

(basically, the left side of Figure 2) and demonstrating the compliance of the entire system (as built) with the Defense in Depth (DiD), also represented in Figure 2.

When introducing the dynamic barricade one may note that the SSC, item 1), the ESF (including ECCS), item 2), the barriers, item 3), and the basic features of EOP and SAMG, item 5) and of I&C, item 6), are considered as consistent with current technology. However the safety function and the alarms, item 4), as well as the FSAR, item 7), are those technological constituents through which the idea of dynamic barricade is introduced.

Starting from the FSAR and the BEPU approach systematically applied to any related analytical part, the BEPU FSAR, [54], is obtained: this is, among the other things, the key origin of E-SMD which largely expands the concepts of safety function and alarms, item 4). The BEPU-FSAR shall be completed within an IA framework, not currently part of nowadays assessment processes.

In order to complete the consideration of elements of the barricade, the ALARA or ALARP established principle in radioprotection) should be translated as the "best possible" and adopted for technological processes including the risk evaluation and the ERT can be seen as an unavoidable outcome of the consideration of extreme risks (see also below in this paper).

The E-SMD should be perceived as a diffused hardware which (tightly) interconnects all constituent elements of nuclear reactors. The ALARA is transformed from a radiation-protection related principle into a DiD principle. The ERT is the needed additional constituent of the dynamic barricade.

7. Extreme Events: Causes and Prediction, and What to Expect

A methodological approach and applications are discussed hereafter in order to inform about expected event possibility or likelihood. This shall be considered for the safety and design of any technologically relevant industrial installations and, namely for supporting the proposal for the new dynamic barricade.

Whatever engineered system may fail following extreme situations as already mentioned in section 5.2 (meteorite, war, etc.), powerful empires have ended too in the past three to five millennia.

The attitude of having unstoppable failures in mind and of preparing the most strenuous defense is the only rational reaction and precaution Apart from detecting operational anomalies, monitoring and controlling departure from everyday limits, reduction in manual reporting and enabling plant performance optimization (which are key benefits), any new protective approach has literally to predict what is or might be going to happen. So what might we expect? How are we to react?

7.1. What to Expect

As stated clearly before by someone who knows: "*Accidents are inevitable in*

complex and tightly coupled systems", [58].

Extreme events still occur and we continue to be surprised about them, even as: "*The events are all reported in great detail in massive reports, often running to thousands of pages, and multiple organizations, committees and inquiries. None of these are particularly complicated or hard to understand—after all reactors should not melt and explode, oil rigs should not explode and leak, planes should not fall from the sky, financial markets should not collapse, and power outages should not last for weeks*", [5].

The underlying and common cause is that the known but unexpected event caused the human involved difficulty in controlling what was happening. The approximate rates and probabilities are easy to calculate, and are reproduced in Table 1.

The lowest risk is by achieving the lowest (but not zero!) possible failure, outcome or barrier penetration rate due to simply having human involvement. Even for so-called passive or automatic systems, perfection of performance is extremely difficult to prove unless something like the T.G. Theofanous criterion, [59], see recent related consideration in [60], is adopted of complete exclusion by design and/or operation of cause or sequence (*i.e.* the core cannot melt, explosions cannot happen, radioactivity cannot be released, cooling is assured forever and ever, no leaks or additional failures occur, the worst that can happen is really benign etc.).

In this connection, by adopting so-called passive systems, e.g. in nuclear technology, we do not get rid of human factors and of impact of humans upon the passive system (necessarily transient) performance; rather, human impacts move from (mainly) the operation stage (as in active systems) to (mainly) the design stage (where, in case of active systems, design errors and approximations are minimized), see e.g. [61].

We have established and quantified the lowest actually observed failure probability for a truly "passive" system using recently obtained actual data for a human designed, human engineered and human operated system. This data is for dams, which of course after being built require—or should require—little interference, minimal maintenance and almost no changes while "operating" or in standby mode *i.e.* containing water and releasing it safely only when as designed

Table 1. Some typical past severe event risk estimates based on actual events (from [5]).

Extreme Event	Frequency and Probability	
	Upper Event Rate, λ (per year)	Probability of Major Loss, **p**
Reactor meltdown	**0.0003**	**0.02 per reactor**
Oil well blow-out	**0.02**	**0.0014 per offshore rig**
Loss of aircraft	**0.043**	**0.02 per aircraft**
Loss of grid power	**0.03**	**0.02 per customer**
Financial crisis	**0.06**	**0.02 per $T of GWP**

or activated. They must do their safety job passively for many, many years, and there is no other human designed, built, operated and maintained system that is essentially so totally "passive" (even bridges require more maintenance and are also often newer technology structures these days). Dams are not only amongst the oldest structures made by man to control floods and supply power, but they also occasionally fail (with consequences) due to unforeseen circumstances and events (overtopping, excessive subsidence, structural weaknesses, inadequate inspections, etc.). Earlier analysis of dam failures, [62], was for the limited data available from the US Bureau of Reclamation but we now have access to data from the US National Performance of Dams Program, [63] and [64] (***Note-3: We are extremely grateful to Professor M.W. McCann* 2019, *NPDP for supplying these data***).

The failure data for all causes for a population of up to 90,000 such dams in the USA (of all known ages and lifetimes) suggest the observed probability of failure is circa 0.0001 per dam. This number does not depend on construction and does not vary much by dam age either (for the range of 1 - 120 years of operation) and is for some 136 million total dam-years of operation, yielding a frequency of 2296/136,000,000 = 2.10^{-5} per dam-year. This failure probability and rate are about two orders of magnitude less than the lowest than can be shown or derived for (any and all) modern "active" technology systems that depend on human involvement (emergency power restoration, nuclear reactors, transportation accidents, chemical plant explosions, train wrecks, various disasters…) as shown in the various papers, e.g. [65].

7.2. Implementation and Confidence in Process Safety Management—Not Regulation

We, the Peoples and Public should rather be convinced and understand that residual risk exists, that technologists did their best to minimize that risk; that residual risk is quantified and continuous controlled (e.g. the part of the "new barrier"); and the "value" of risk is calculated at each time, *i.e.* even after any initiating event (this is mentioned, not hidden and not emphasized reason for the "new barrier"). Any "technological barrier" will surely need some kind of "AI" or rule-based "intelligent" system to exist. But it is the unexpected and the unanticipated that occur, the failures that are 'hidden" or not known, and the sequences we had discounted or not imagined. Even software is not perfect, and can contain errors and residual faults after extensive testing, e.g. [66] and [67], because they are linked to human learning. Software is still the product of the imperfect human mind. Hence even today's so-called "autonomous vehicles" have crashes and literal "blind spots" even if they contain self-correcting learning.

For the "design stage" remember engineers and designers are not perfect and make mistakes, [68], and so do the managers and operators. From published work on millions of actual accidents, errors and events in massive software, entire systems and multiple technologies, [7] and [67], and from actual design in-

formation that there is always a residual small but potentially fatal number of mistakes, errors or faults (hidden or so-called "latent") in the design. It is known that despite extensive testing, beta-version releases, QA/QC procedures, independent V&V and functional reviews, some design flaws and system performance errors still occur at a rate of a few per million person-hours of engineering, design, software, hardware, analysis, review, construction effort, the only questions being ensuring can we find and fix them all and whether they are not "fatal". The list today includes engineering issues for EPR construction delays, the Deepwater Horizon oil spill, Space Shuttle crash, Fukushima reactor explosions, Concorde crash, plus Chernobyl, Titanic, Boeing Max 8, etc.; the list is very long and still growing as technologies and knowledge change. The dominant origins clearly are operational management and human decisional mistakes in Defense-in-Depth that can also give rise to or be compounded by Common Cause Failures (CCF) and/or lack of diversity and redundancy.

For effective Process Safety Management, the job and purpose of management, project directors, safety reviews, and of independent experts is simply to find the mistakes—before they can surface and/or problematic operation occurs. It is tough, it is difficult, it is expensive, it is not popular, but it must be done… and then redone… and then done again.

We must also recognize that paradoxes exist, both in human thinking and in societal acceptance of risk, [65] "… *Having accepted that the worst might happen, and having taken all reasonable precautions, and constructing barrier after barrier, the only thing to do is prepare for it*", and "… *Recognizing these interwoven and overlapping risk paradoxes, we are better prepared and understand more how to reduce risk, and how to develop better systems, greater understanding and more effective behavior. The solutions lie not just in more robust engineering, or adopting 'fail safe' technology, or implementing more and more 'barriers' to failure, but simply in relentless efforts to enhance human learning and reduce mistakes*".

Then, what to do? … the answer is a continuous (each one minute or even each one second) evaluation of the risk and, based on that, identification of counter-actions and implementation of counteractions with still continuous risk monitoring and etc.

Here again, eliminating complexity will be a real issue, avoiding hidden interconnections and dependencies, underlying linkages. Being a "continuous risk monitor" is a real challenge. It is partly used today, and is called "online monitoring" for keeping within Tech Spec operating limits (DNB, CHF, PLHGR, peaking/form factors, power output, etc.), tracking plant thermal performance, and optimizing fuel performance and component maintenance in today's LWR. There is no requirement for it to be "safety grade" or "safety critical"—the requirement is that it must just work, and not endanger operational critical safety functions.

Adding more or different sensors is also very difficult, especially to any existing or already licensed operating plants and will be opposed as unnecessary

having already been judged to be adequately safe. They will always need to be "grand-fathered", having obeyed all prior rules, applicable requirements and enforced regulations within their existing licensed operating envelope or basis. But, somewhat perversely, there is no incentive to change the regulations or process safety if it means additional hearings, licensing applications and unnecessary expense, and any changes can only be justified on the basis of "cost vs benefit" arguments. Safety changes are presently also only judged on the basis of any incremental reduction in the calculated core damage frequency, which we already know is a purely synthetic measure which is not validated by actual data, see e.g. [69].

Consider an example. The one simplest improvement after TMI for risk monitoring purposes was a "melt down thermocouple" attached to the lower vessel head—to tell if the vessel was overheating or failing or not. The utilities and plant owners opposed it as being too expensive, never needed day-to-day, and subject to too much regulation, inspection, testing and their additional costs. If the cost and inconvenience exceed the benefit, as the plant output is not increased—but would surely have helped the operators at TMI and Fukushima, and aided the post-accident inspections looking for such damage. Newer designs of LWR plants have expensive "core catchers" placed below the primary vessel, when it surely would be more and highly desirable not to have any vessel damage occur or at least know if it likely in real time, not just by and from remarkable post-mortem forensic examination, [70].

Under the new safety construct, the potential for large uncontrolled environmental releases indicate the importance of risk assessment and the need to quantify the consequences. These consequences will include the direct and indirect social, economic and related costs. All risks are relative to some known or acceptable total consequence. It is generally the case that a probabilistic-based analysis should be used as part of the safety case and risk assessment to:

1) define and quantify potential event sequences or scenarios;

2) identify and prioritize the risks from and in management, design, maintenance, and operation;

3) assist decision-making for estimating the future risk and consequences of the many phases and aspects of well operation;

4) help define the qualifications, procedures, controls, training, skills and knowledge needed for risk critical aspects;

5) provide guidance to management and operators on relative risks and consequent potential losses;

6) define mitigation and safety measures; and, most importantly,

7) define uncertainties to ensure employee and corporate safety, to assure environmental preservation, and to attain public and political trust.

But valuable as it is, PSA must be an aid to judgment, not a replacement for actual data, observation, and Process Safety Management responsibility.

All these difficult aspects must be included in a structured risk assessment, to assess the priority, purpose, and potential consequences of the risk. A systematic

process for evaluating operational risk is vital and necessary to prioritization and quantification of relative risk.

Since the Chernobyl event, passive systems were considered a possible solution to human mistakes. Actually, different features of current WCNR, like mutual position of core and steam generators, steam generator design (or secondary side cooling) and presence of accumulators among the ECCS, are fixed based on passive systems which make use of gravitational (hydraulic head) forces. Passive systems implying a minimum number of components needing external source of energy to operate are superficially attractive from a reliability view point. The key drawback, not receiving sufficient attention, is connected with the thermal-hydraulic operation: low driving forces may be overrun by low intensity perturbations and instability in passive systems performances may be expected, [61] (***Note-4: In a somewhat surprising parallel, the Deepwater Horizon oil and gas backflow also occurred because of an unstable hydrostatic head imbalance between the "mud" in the drilling well and the Macondo oil reservoir pressures at great depths, when a concrete well seal failed that was not properly installed and the NRV or "blowout preventers" also then failed on demand***). Reliability of thermal-hydraulic phenomena in passive systems recently became a "new" research sector: findings and procedures are available and need to be considered by regulators and designers. Complex (and/or high-tech) active system for core cooling driven by on-site available steam energy, e.g. [71], might be preferable to more or less "pure" passive systems like accumulators.

7.3. Estimating Consequence Losses and Future Risks

Large uncontrolled environmental releases from energy systems created fear, uncertainty and adverse public reaction. These Extreme Events indicate the importance of risk assessment and human decision-making during emergencies that challenge the existing design basis. In particular, an overall safety case must exist which goes beyond the expected to the unexpected; with structured risk review in planning changes during the (many) phases of operations and emergency actions; and adequate knowledge and measurement of accident conditions by qualified instruments to ensure informed decisions and correct actions. Additionally, since in an Extreme Event multiple physical and procedural "barriers" can be and are bypassed or made inoperable, or made ineffectual due to operational considerations and procedures, the public can and will be exposed to the risk and fear of releases.

Having determined the consequence probability, in principle the financial loss or risk can also be estimated. Losses can occur at any time, and if we are insuring against, investing in, or estimating the risk of incurring them we need to know how often adverse consequences or losses may occur and how big the financial and other damages might be. There must be a formal, assumed, known or empirical relationship of some form between the loss from the consequences of any event and its probability of occurrence, P, otherwise risk assessment and insur-

ance are not feasible concepts. In industrial accidents, for example, it turns out that the value of damages incurred is a function of the frequency of the event or loss. Fortunately, there is an inverse dependency in that large damages (or losses) are less likely than small ones, and there exists a distinct "damage curve" (***Note-5: Hanayasu and Sekine, Damage Assessment of Industrial Accidents by Frequency-Magnitude Curve, Proc. PSAM, 2004, which parameters can be altered or adjusted according to relevant data***), or colloquially a "Whitman plot". In this way we know for civil structures that the severity or magnitude of the risk is mathematically related to the frequency or failure rate, so here we presume that the same ideas can be applied to financial loss events.

We may also define the consequences as including the sum total of both the costs from:

1) direct physical damage, equipment loss, replacement or alternate production, and regulatory fines; and

2) indirect damages of reputation, stock losses, social disruption, compensation payments or settlements, liability exposure or accounting set asides.

This summation of losses or fiscal risk exposure provides an "all loss" basis for "all risks", and suggests that overall quantification is necessary. Such assessments have already been done for other major events (e.g. the Exxon Valdes oil spill in Alaska) so the methodology and methods exist.

For Fukushima, analyses have been made of the social impacts: "*The tsunami directly killed over* 18,000, *most in neighboring prefectures. In* 2014 *the government of Fukushima prefecture reported a death toll from the evacuation as* 1656, *as determined by municipal panels. About* 90% *of these indirect deaths were people over age* 66. *The figure is greater than for Iwate and Miyagi prefectures, though they had much higher loss of life in the 'quake and tsunami. As of March* 2019, *the Fukushima prefecture government reported* 2268 "*disaster-related" indirect deaths in the prefecture. Causes of indirect deaths include physical and mental stress stemming from long stays at shelters, a lack of initial care due to hospitals being disabled by the disaster, and suicides.*" Source: World Nuclear Association, Weekly Digest, 25 October and 1 November, 2019.

The loss ratio is solely a function of the loss or consequence probability variation with risk exposure.

Indeed, functional forms for losses due to disasters abound in the literature, from the simplest power functions, to complex formulae for infrastructure damage assessment, [72]. In fact such methods are well developed and have already been applied to forward planning for disasters, [73], and estimating infrastructure damage using complex computer modeling, [74].

The lowest attainable risk probability depends on achieving the lowest possible failure, outcome or barrier penetration rate due to human and management involvement in operational, procedural and managerial decision making.

Fortunately, or unfortunately, we already know estimates or ranges from prior universal studies of systems with human involvement with learning, including

notably the average interval between global financial crises and busts2, and data from other multiple industries for millions of accidents and events.

(*Note-6*: *The coronavirus and its social impact. During the publication process of the present manuscript, the coronavirus disease is striking the whole world. Although no deep scientific activity has been done by the authors who do not have any specific expertise in microbiology they do have knowledge of catastrophes and public risk, which is precisely the context of the present manuscript. This has lead us to make this further suggestion on enhancing real public safety.*

First, we can associate the coronavirus effect with an industrial catastrophe, e.g. Fukushima nuclear reactor radiation release, or Gulf of Mexico oil platform collapse, causing widespread public concern; i.e. coronavirus victims socially correspond to victims of industrial disasters.

Second, we observe that the virus appears to spread more effectively in highly industrialized regions where population density and industrial and societal pollution has reached the highest levels. In the case of Italy (but also each EU Country and also China) emblematic is that the spread of the disease was fastest in the industrialized and polluted (also due to orographic conformation) regions of Lombardy and Veneto and Bologna surroundings, but not so fast in Tuscany and even less fast (hopefully) in the South less industrialized regions (and where the sea beneficial effect keeps the pollution relatively low, i.e. compared with the Milan areas far away from the sea). In China, the spread also occurred by the mass movement of people which is now largely forbidden or restricted.

Third, the (up to now) the defeat of the virus in China and Korea is associated with the reduction of most of industrial and social activities and the consequent detected decrease of the pollution. So the working hypothesis is that there is a correlation between the virus spread as facilitated by pollution (e.g. respirable PM 10, but not only) in addition to the usual hand-to-hand, person-to-person or aerosol droplet mechanisms. There is no consideration here of potential chemical interaction between such particles and virus; and without considering the "obvious" relationship between pollution and average resilience of—mainly older-people.

Fourth the social safety hypothesis is that without pollution or with a reasonably low pollution level the spread of such a potentially airborne virus can be more easily and readily controlled. Therefore, the vital capability of nuclear power in producing electricity notwithstanding the unavoidable risks should be restored and strengthened but only with the needed safety enhancements suggested in this paper. It will be helpful to enter a new era by human kind: same energy "pro-capita", less pollutants and more electricity by nuclear sources.)

8. Conclusions

We have brought together the perspectives of the theoretical, the practical, the

desired and the possible. Namely, we propose here a massive change in safety direction, content and method, using past history and present knowledge of traditional methods as a sign post towards achieving a new future. Metaphorically, fishing net with hooks and a series of anchors has been thrown into the ocean to catch the big fish. The fishing net is the knowledge acquired during a lifetime of activity by the authors in nuclear reactor technology; the anchors are the cornerstones topics in the many listed references; the hooks are the argumentations presented in the present paper; and the reward is the big fish is the restoration of a rational role for the nuclear fission for electricity production. Selected argumentations (the hooks), or key findings from the performed analysis are summarized hereafter, whereas the evidence of the catch of the big fish is left to posterity.

As exemplified by the major accidents to date, the lack or inadequate possibility to perform truly Independent Assessment is at the basis of the mistrust towards the capability of today regulations to guarantee the highest achievable safety of nuclear installations, where inextricably intertwined market and governing rules bear (some) responsibility.

A re-foundation is needed in nuclear technology and nuclear reactor safety, [75] (see also [76]). The ABCDE proposal for the new safety barricade coming from previous studies (*i.e.* the main hook in the above metaphor) has been strengthened by the consideration of the scientific laws of probability and human learning that dominate risk in all modern technological societies (*i.e.* the anchors, above).

Summarizing what has been discussed or implied in the present paper:

1) Changes in the status of the system which are not sufficiently understood, and/or monitored, are precursors of disasters.

2) Civilization's progress depend on learning from risk analysis and accidents, whatever their severity; lessons learned must be transferred to design.

3) Disasters cannot be avoided; they are embedded into the progress: since the loss of caravels by the navigator Colombus disasters are associated with the natural evolution of civilizations.

4) Disasters, extreme events and unforeseen rare situations must be understood in order to minimize their probability of replication: again, learning is crucial.

5) Introducing additional barriers is not effective if the barriers are not "intelligent" and do not dynamically adapt to the time evolution of the system to protect.

6) Profit should not be the key target for nuclear fission technology, being a necessary part but not the main one.

7) Simplification (e.g. passive systems) must be a target but are not the panacea for the safe design; nonetheless, like the construction of pyramids in Egypt, complex systems require state of art, sometimes pioneering, solutions.

8) Conscious designers shall not wait for regulations improvements or just be "within allowable limits": rather new ideas should open the way to new rules

(this is not always possible… or possible in an "ideal" world).

9) Dead-end pathways in design are possible, sometimes caused by fashionable research or undue requests by regulators: these should promptly be detected and properly replaced by designers.

10) Catastrophes create fear, uncertainty and adverse public reaction: scientists should maintain their fact-based opinions, noticeably considering the correct (given) definition of risk.

11) Probability of occurrence of any event (e.g. of a disaster) may be a strongly time-varying function: it increases when the event time becomes closer; thus, as well established probability alone cannot be taken as a characterizing element, and a "dynamic" reaction is needed when attempting to protect from the disaster.

12) A working hypothesis has been formulated (though not performing activities in the area) connecting coronavirus and pollution.

Like a doctor who has not become cynical after seeing hundreds of patients die and fights to ensure the well-being of the living ones, so a scientist has a duty to improve the design of the systems based on the analysis of the catastrophes he has dealt with.

Finally, none of the physical barriers may preclude the consequences of extreme events which by definition are beyond the imagination. This is why a dynamic barricade is needed which adapts to the evolution of an accident whatever is the severity: this is the best one may do. It may be all we can do. Insights into the idea of dynamic barricade are provided in the **Appendix**.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Duffey, R.B. (2012) A Future at Risk. *Mechanical Engineering*, **134**, 34-38. https://doi.org/10.1115/1.2012-JUL-2

[2] Gupta, K., Nowlin, M.C., Ripberger, J.T., Jenkins-Smith, H.C. and Silva, C.L. (2019) Tracking the Nuclear "Mood" in the United States: Introducing a Long Term Measure of Public Opinion about Nuclear Energy Using Aggregate Survey Data. *Energy Policy*, **133**, 110888. https://doi.org/10.1016/j.enpol.2019.110888

[3] Bosetti, V., Marangoni, G., Borgonovo, E., Anadon, L.D., Barron, R., McJeon, H.C., Politis, S. and Friley, P. (2015) Sensitivity to Energy Technology Costs: A Multi-Model Comparison Analysis. *Energy Policy*, **80**, 244-263. https://doi.org/10.1016/j.enpol.2014.12.012

[4] Duffey, R.B. and Pioro, I. (2019) Ensuring the Future of Nuclear Power. *Mechanical Engineering*, **141**, 30-35. https://doi.org/10.1115/1.2019-NOV1

[5] Duffey, R.B. (2015) Extreme Events: Causes and Prediction. *American Nuclear Society Conference*, *Probabilistic Safety Analysis*, *PSA*2015, Sun Valley, 21-26 April 2015, Paper No. 12222.

[6] Muellner, N., Cherubini, M., Kromp, W., D'Auria, F. and Petrangeli, G. (2007) A

Procedure to Optimize the Timing of Operator Actions of Accident Management Procedures. *Journal of Nuclear Engineering and Design*, **237**, 2151-2156. https://doi.org/10.1016/j.nucengdes.2007.03.011

[7] Duffey, R.B. and Saull, J.W. (2008) Managing Risk: The Human Element. J. Wiley and Sons, Chichester.

[8] Duffey, R.B. and Ha, T.-S. (2010) Human Reliability: Benchmark and Prediction. *Proc. Inst. Mech. Eng., Part O*, **224**, 185-196. https://doi.org/10.1243/1748006XJRR307

[9] D'Auria, F. (2019) Nuclear Fission: from E. Fermi to Adm. Rickover, to Industrial Exploitation, to Nowadays Challenges. *Journal of Advancement in Scientific and Engineering Research*, **4**, 17-30.

[10] Rhodes, R. (1987) The Making of the Atomic Bomb. Touchstone, New York.

[11] Rhodes, R. (1995) Dark Sun: The Making of the Hydrogen Bomb. Simon and Schuster, New York.

[12] Goldschmidt, B. (1982) The Atomic Complex. American Nuclear Society, LaGrange Park.

[13] Rockwell, T. (1995) The Rickover Effect: The Inside Story of How Adm. Hyman Rickover Built the Nuclear Navy. J. Wiley & Sons, Publisher Inc., Hoboken, 1-411.

[14] Duncan, F. (1989) Rickover and the Nuclear Navy: The Discipline of Technology. Naval Institute Press (US), Annapolis, 1-424.

[15] Rockwell, (2002) The Rickover Effect: How One Man Made a Difference. Backinprint.Com (An Open Library for the World), Chicago, 1-486.

[16] Crossland, I. (2012) Nuclear Fuel Cycle Science and Engineering. Woodhead Publishing, Sawston, Cambridge, 1-648. https://doi.org/10.1533/9780857096388

[17] IAEA (2017) Nuclear Power Reactors in the World. 37th Edition, IAEA-RDS-2/37, Vienna, 1-79.

[18] Houston, D.A. (1991) Privatization of Electricity in the United States. In: Crew, M.A., Ed., *Competition and the Regulation of Utilities—Topics in Regulatory Economics and Policy Series*, 7, Springer, Boston. https://doi.org/10.1007/978-1-4615-4048-9_11

[19] Vlahinic, N. (2011) The Effect of Privatization in Electricity Sector: The Case of Southeast European Countries. In: Sanders, G.G. and Tichy, L., Eds., *Öffentliche Daseinsvorsorge in Deutschland und Ostmitteleuropa zwischen Daseinsvorsorge und Wettbewerb*, Verlag dr Kovac, Stuttgart, 121-137.

[20] Pioro, I. (Ed.) (2016) Handbook of Generation IV Nuclear Reactors (A Volume in Woodhead Publishing Series in Energy). Woodhead Publishing, Sawston, Cambridge, 1-940.

[21] Kessides, I.N. (2012) The Future of the Nuclear Industry Reconsidered: Risks, Uncertainties, and Continued Promise. *Energy Policy*, **48**, 185-208. https://doi.org/10.1016/j.enpol.2012.05.008

[22] Galassi, G.M. and D'Auria, F. (2017) Thermal-Hydraulics Aspects of Key Nuclear Accidents. In: D'Auria, F., Ed., *Thermal Hydraulics in Water-Cooled Nuclear Reactors*, Elsevier, Woodhead Publishing, Sawston, Cambridge, Chapter 16, 1099-1152. https://doi.org/10.1016/B978-0-08-100662-7.00016-6

[23] US NRC (2009) An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results from Risk Informed Activities. Regulatory Guide, RG 1-2000, Washington DC, 1-191.

[24] US NRC (1975) WASH-1400, NUREG-75/014, Washington DC.

[25] Keller, W. and 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 Carl Rasmussen. *Reliability Engineering and System Safety*, **89**, 271-285. https://doi.org/10.1016/j.ress.2004.08.022

[26] Rempe, J. and Knudson, D.L. (2013) TMI-2—A Case Study for PWR Instrumentation Performance during a Severe Accident. Idaho National Laboratory, INL/EXT-13-28043, Idaho Falls. https://doi.org/10.2172/1097179

[27] IAEA (1993) The Chernobyl Accident: Supplement to INSAG-1. Report by the International Consultative Group on the Nuclear Safety, Safety Series N75, INSAG-7, Vienna.

[28] Mizokami, S. and Kumagai, Y. (2015) Event Sequence of the Fukushima Daiichi Accident. In: Ahn, J., Jensen, M., Juraku, K., Nagasaki, S. and Tanaks, S., Eds., *Reflections on the Fukushima Daiichi Nuclear Accident*, Springer, Cham, 21-50. https://doi.org/10.1007/978-3-319-12090-4_2

[29] US EIA (2019) Annual Energy Outlook (with Projections to 2050). 1-83. https://doi.org/10.24050/reia.v16i31.1286

[30] IAEA (2017) Energy, Electricity and Nuclear Power Estimates for the Period up to 2050. Reference Data Series No 1, 2017 Edition, Vienna, 1-156.

[31] Newell, R.G., Raimi, D. and Adana, G. (2019) Global Energy Outlook 2019: The Next Generation of Energy. Resources for the Future, 1-46. https://creativecommons.org/licenses/by-nc-nd/4.0/

[32] Pioro, I. and Duffey, R.B. (2015) Nuclear Power as a Basis for Future Electricity Generation. *ASME Journal of Nuclear Engineering and Radiation Science*, **1**, Article ID: 011001. https://doi.org/10.1115/1.4029420

[33] Australian Government (2019) Australian Energy Update 2019. Department of the Environment and Energy, 1-43. https://www.energy.gov.au/government-priorities/energy-data/australian-energy-statistics

[34] OECD/NEA (2019) The Cost of Decarbonisation: System Costs with High Shares of Nuclear and Renewables. @OECD 2019, Paris, NEA No. 7299, 1-224.

[35] Jalonen, R. and Salmi, K. (2009) Safety Performance Indicators for Maritime Safety Management: Literature Review. Report TKK-AM, University of Technology Faculty of Engineering and Architecture, Helsinki.

[36] NASA (2010) Risk-Informed Decision Making Handbook. NASA/SP-2010-576, ver 1.0, Office of Safety and Mission Assurance, US.

[37] D'Auria, F., Camargo, C., Muellner, N., Lanfredini, M. and Mazzantini, O. (2012) The Simulation of I & C in Accident Analyses of Nuclear Power Plants. *Nuclear Engineering and Design*, **250**, 656-663. https://doi.org/10.1016/j.nucengdes.2012.04.022

[38] Duffey, R.B. (2012) Extreme Events: The New Social Design Basis. *Proceedings of the 20th International Conference on Nuclear Engineering Collocated with the ASME 2012 Power Conference*, *ICONE20POWER*2012, 30 July-1 August 2012 Anaheim, No. 54253.

[39] Holton, G.A. (2004) Defining Risk. *Financial Analysts Journal*, **60**, 19-25. https://doi.org/10.2469/faj.v60.n6.2669

[40] Breyer, S. (1993) Breaking the Vicious Circle: Towards Effective Risk Regulation. Harvard University Press, Cambridge, MA.

[41] Abe, S., Ozawa, M. and Shiroshita, H. (2018) What Do Societal Safety Sciences Aim

At? In: *Science of Societal Safety*: *Living at Times of Risks and Disasters*, Springer, Singapore, 3-13. https://doi.org/10.1007/978-981-13-2775-9_1

[42] Cuttler, J.M. (2013) Commentary on Fukushima and Beneficial Effects of Low Radiation. *Dose-Response*, **11**, 432-443. https://doi.org/10.2203/dose-response.13-008.Cuttler

[43] OECD/NEA/CSNI (2009) Probabilistic Risk Criteria and Safety Goals. NEA/CSNI/R(2009)16, Paris, 17 December 2009, 1-179.

[44] US NRC (2012) State-of-the-Art Reactor Consequence Analyses (SOARCA). NUREG-1935, Washington DC.

[45] US NRC (2013) Modeling Potential Reactor Accident Consequences: State-of-the-Art Reactor Consequence Analyses (SOARCA): Using Decades of Research and Experience to Model Accident Progression, Mitigation, Emergency Response, and Health Effects. NUREG/CR-0359, Washington DC.

[46] NEI (2016) External Flooding Assessment Guidelines. Report NEI 16-05, Washington DC, 1-98.

[47] Zio, E. and Duffey, R.B. (2020) The Risk of the Electrical Power Grid Due to Natural Hazards and Recovery Challenge Following Disasters and Record Floods: What Next? Chapter in Book, to be published.

[48] Miller, C., Cubbage, A., Dorman, D., Grobe, J., Holahan, G. and Sanfilippo, N. (2011) Recommendations for Enhancing Reactor Safety in the 21st Century (The Near-Term Task Force Review of Insights from the Fukushima Daiichi Accident). USNRC ML112510271, Washington DC, 12 July 2011, 1-96.

[49] Howlett, H.C. (2001) The Industrial Operator's Handbook. 2nd Edition, Techstar, Pocatello, 40, 63 and 76.

[50] US NRC (2007) Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, NUREG-1860, Vols 1 and 2, Washington DC.

[51] Bea, R. (2013) Testimony, United States District Court, Eastern District of Louisiana, Oil Spill by the Oil Rig Deepwater Horizon in the Gulf of Mexico on April 20, 2010 Civil Action No. 10-MD-2179, p 281, New Orleans, Louisiana (US), Feb. 26, Official Transcript, 268-364.

[52] D'Auria, F., Debrecin, N. and Glaeser, H. (2019) The Technological Challenge for Current Generation Nuclear Reactors. *Nuclear Energy and Technology* (*NUCET*), **5**, 183-199. https://doi.org/10.3897/nucet.5.38117

[53] IAEA (2011) A Framework for an Integrated Risk Informed Decision Making Process. INSAG-25, Vienna.

[54] Menzel, F., Sabundijan, G., D'Auria, F. and Madeira, A. (2016) Proposal for Systematic Application of BEPU in the Licensing Process of Nuclear Power Plants. *Int. J. Nuclear Energy Science and Technology*, **10**, 323-338. https://doi.org/10.1504/IJNEST.2016.081998

[55] Eide, S.A., Wierman, T.E., Gentillon, C.D., Rasmuson, D.M. and Atwood, C.L. (2007) Baseline Risk Index for Initiating Events (BRIIE). US NRC Report NUREG/CR-6932, Washington DC.

[56] Rathnayaka, S., Khan, F. and Amayotte, P. (2013) Accident Modeling and Risk Assessment Framework for Safety Critical Decision-Making: Application to Deepwater Drilling Operation. *Journal of Risk and Reliability*, **227**, 86-105. https://doi.org/10.1177/1748006X12472158

[57] US AEC (1971) Interim Acceptance Criteria (IAC) for ECCS. US AEC, Washington

DC.

[58] Greenfield, M.A. (1998) The Changing Face of NASA and Aerospace. Deputy Associate Administrator, Office of Safety and Mission Assurance Normal Accident Theory, Hagerstown.

[59] Theofanous, T.G. (1996) On Proper Formulation of Safety Goals and Assessment of Safety Margins for Rare and High Consequence Hazards. *Reliability Engineering and System Safety*, **54**, 243-257. https://doi.org/10.1016/S0951-8320(96)00079-8

[60] Galushin, S. (2019) Development of Risk Oriented Accident Analysis Methodology for Assessment of Effectiveness of Severe Accident Management Strategy in Nordic BWR. Doctoral Thesis No. 08, February, KTH Royal Institute of Technology, Stockholm, 1-93.

[61] D'Auria, F. (2018) Status Report on Thermal-Hydraulic Passive Systems Design and Safety Assessment. Invited at *Focus Session* "*Safety of Advanced Nuclear Power Plants*" (*coordinators A. Schaffrath, T. Mull*) *of Annual Meeting on Nuclear Technology* (*AMNT*), Berlin, 29-30 May 2018. http://www.kernenergie.de/ http://www.nucleartech-meet.com/

[62] Duffey, R.B. and Saull, J.W. (2002) Know the Risk. Butterworth and Heinemann, Boston.

[63] NPDP (2019) National Performance of Dams Program. National Performance of Dams Program Dam Failure Data, Provided 11/23/2019 by M.W. McCann, Jr.

[64] McCann, M.W. and Lundqvist, A. (2017) Development of F-N Curves for Public Safety Risks Associated with Dam Failures in the US. *Proceedings of the Association of State Dam Safety Officials Annual Conference*, San Antonio, 10-14 September 2017.

[65] Duffey, R.B. (2015) The Seven Risk Paradoxes. *American Nuclear Society Conference*, *Probabilistic Safety Analysis*, *PSA*2015, Sun Valley, 21-26 April 2015, Paper No. 12223.

[66] Duffey, R.B. and Fiondella, L. (2014) Software, Hardware and Procedure Reliability by Testing and Verification: Evidence of Learning Trends. *IEEE Transactions on Human-Machine Systems*, **44**, 395-405. https://doi.org/10.1109/THMS.2014.2306932

[67] Fiondella, L. and Duffey, R.B. (2015) Software and Human Reliability: Error Reduction and Prediction. *American Nuclear Society Conference*, *Probabilistic Safety Analysis*, *PSA*2015, Sun Valley, 21-26 April 2015, Paper No. 12221.

[68] Petrowski, H. (1994) Design Paradigms. Cambridge University Press, New York, 1-222.

[69] París, C., Queral, C., Mula, J., Gómez-Magán, J., Sánchez-Perea, M., Meléndez, E. and Gil, J. (2019) Quantitative Risk Reduction by Means of Recovery Strategies. *Reliability Engineering and System Safety*, **182**, 13-32. https://doi.org/10.1016/j.ress.2018.09.024

[70] Rempe J. [Ed.] (2019) U.S. Efforts in Support of Examinations at Fukushima Daiichi-2019 Evaluations. ANL Report 19/08, Office of Nuclear Energy, US DoE, 1-387. http://www.osti.gov/ http://www.ntis.gov/

[71] SPX (2014) Enhancing Nuclear Power Safety. *World Pumps*, **12**, 12-13. https://doi.org/10.1016/S0262-1762(14)70304-9

[72] US DHS (2019) Multi-Hazard Loss Estimation Methodology, Flood Model. Hazus®-MH, Dept. of Homeland Security, Washington DC, 1-569.

https://www.fema.gov/media-library-data/20130726-1820-25045-8292/hzmh2_1_fl_tm.pdf

[73] IRGC (2006) Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures. International Risk Governance Council, White Paper #3, Geneva.

[74] US DHS (2018) Strengthening the Cyber Security of Federal Networks and Critical Infrastructure, Washington DC. https://www.energy.gov/downloads/report-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

[75] D'Auria, F., Debrecin, N. and Glaeser, H. (2017) Strengthening Nuclear Reactor Safety and Analysis. *Nuclear Engineering and Design*, **324**, 209-219. https://doi.org/10.1016/j.nucengdes.2017.09.008

[76] Mazzantini, O., Galassi, G. and D'Auria, F. (2019) Reprint of "The Role of Nuclear thermal-Hydraulics in the Licensing of Atucha-II: The LBLOCA". *Nuclear Engineering and Design*, **354**, 110292. https://doi.org/10.1016/j.nucengdes.2019.110292

Appendix: Focus to the Dynamic Barricade

Paraphrasing Galileo Galilei engaging Salviate, a tiny, virtual dialogue between two chief world systems comparing the Copernican and the Ptolemaic systems (the two systems are opposed interpretation of reality), in the present case between, the deterministic and the probabilistic viewpoints (the two viewpoints are complementary, though in most cases pursued independently from each other), is attempted hereafter, and for the reader to explore further.

✓ "Kindly provide one insight for 'deterministic' and 'probabilistic'".

Answer (making reference to the safety and the design of nuclear reactors): The deterministic approach is based upon a model of the physical reality and aims at predicting the system transient evolution following a hypothetical initial condition (system status). The probabilistic approach aims at determining the probability of a given status (level 1), the consequences of malfunctions (level 2) and the related radiological impact (level 3).

✓ What are (examples of) key advantages and drawbacks of deterministic and probabilistic approaches?

Answer: Validation is possible for the results of deterministic approach (advantage); otherwise, an extremely limited number of situations can be analyzed, and resources needed for performing qualified analyses may reveal huge (drawbacks). The probabilistic evaluation allows the evaluation of role and significance of the myriad systems and components which constitute a nuclear reactor (advantage): optimization of the number of those systems and components is possible; however, a time dependent evaluation of probabilities of a given system status is still at the frontier of knowledge and errors in estimating probabilities, specifically when related values are low, are difficult to be quantified (drawbacks).

✓ Is the combination of deterministic and probabilistic approaches an established practice, nowadays?

Answer: Yes, but not to the extent that is possible. In other words, the need to take into account of deterministic analyses into probabilistic studies and *vice-versa* is felt; however, all potential connections between the two approaches are not consistently and systematically considered.

✓ "What is the new barrier?"

Answer: What we have called a "new barrier" and, better in the present context, "dynamic barricade" is not going to replace any existing system in the reactor. The "new barrier" is a dynamic boundary that adapts to the (we assume targeting any) accident that may happen. The "new barrier" is NOT a wall or similar physical entity; rather it implies:

1) the full use of existing components;

2) specific additional analyses;

3) consistency with current technological capabilities in all the various sectors of human society and behavior (e.g. including illness of operators).

✓ "How can the 'dynamic barricade' be further characterized?"

Answer:

1) the full implementation of existing safety technology and principles as been stated and prescribed since several decades but for a number of motivations because of too many prescriptive rules, undue fights between regulators and designers, targeting profits, pursuing fashion tendencies from researchers, etc.), eliminating the lag between those principles and continuous technology advancement (the industry often may prefer to not follow all technological innovation e.g. when performing safety analyses preferring to use what is currently "licensable");

2) installation of a large number (ten thousand) of new monitors and instantaneous signals processing to assure E-SMD ;

3) having available a rescue team (ERT is fast response … order of one hour to reach the reactor site) dealing with technology, security, situation assessment, and decision making.

✓ "Do such methods exist already?" Do there is any application in practical problems in nuclear technology?

Answer (1): Sophisticated best estimate analytical techniques (so-called BEPU best estimate plus uncertainty) are now mature but are not fully applied to the safety evaluation of nuclear reactors. These techniques allow the evaluation of errors when assessing the safety and the safety margins of nuclear reactor (discussion about those techniques can be found in many recent reports e.g. issued by IAEA).

Answer (2): The case of instabilities involving coupled fluid-dynamic and neutron flux oscillations in Boiling Water Reactors constitutes a valid example: stability events occurred in operating nuclear reactors bringing the systems close to the core disruption. The probability of initiating an instability event is relatively high under the current design and operating conditions, as well as the consequences: however, the current instrumentation (e.g. available E-SMD) is accredited with the capability to detect the incubation period of an unstable event. Bottom-end of a specific international study accepted by regulators (OECD/NEA/CSNI, BWRS report, 1997) was: high probability event with a rapidly (few tens of seconds) increasing probability of high consequences does not require a design change and proper consideration of neutron detectors signals is enough to guarantee the safety of the reactors.

✓ "How would the ERT have reacted to, say, the Chernobyl event?"

Answer: The ERT team following clear inadequacies detectable by an E-SMD (both ERT and E-SMD are defined in our paper) would have reached the reactor site (maybe not in Soviet Union at that time … this is a political issue) and prevented several hour before the explosion, the operation of the reactor by the on-site operators who were apparently incapable to deal with information coming from outside and from the system.

✓ "Can the newly conceived 'dynamic barricade' restore or regain public confidence?"

Answer: It has the potential to regain the confidence of the public and get rid

of their gut feelings concerning nuclear reactors. However we are fully aware that there are difficulties for its implementation: the most important (maybe the only important one) is the need that industry makes available deep proprietary information to perform valid Independent Assessment.

✓ "Do you think a nuclear reactor can ever be completely safe?"

Answer: This depends on what is meant by "safe". Can be safe to the best (with our knowledge) when it cannot withstand the fall of a meteorite on the site (never), as well as other extreme situations; or can it be safer than many other human built and operated systems. Scientists and technicians should admit they cannot do anything in many "act of God" situations: this is our limit which may become part of the accepted residual risk (*i.e.* a continuously moving boundary based on current knowledge): a reference extreme situation, for instance the fall of a meteorite, shall fix the limit for the probability (or the frequency) where acceptable risk starts.

✓ "How much will the deployment of 'dynamic barricade' cost?"

Answer: The dynamic barricade is conceptual at the time being:

1) The design cost shall not overpass 1% the cost of a single reactor unit (so many reactors could benefit and regulations/requirements/reviews highly simplified);

2) The implementation cost (including the operation) shall not overpass 1/1000 cost of a single reactor unit;

3) It is expected to achieve a (relative) factor greater than 10 in overall risk reduction, where this is measured in effective reduction in total societal impact not just some delta in "core damage frequency" or using an antiquated linear dose—response relationship for "allowable" or tolerable activity release.