THE NEED OF ADDING A SAFETY BARRIER TO WATER COOLED NUCLEAR REACTORS

D'AURIA F.

University of Pisa – Italy

DEBRECIN N.

University of Zagreb – Croatia

GLAESER H.

Retired from GRS, Munich - Germany

Abstract

The present paper deals with the proposal of an additional safety barrier for the class of large (1000 MWe or more) Light Water Reactors (LWR) now in operation, in construction, or under design. Emphasis is given to the motivations or the needs for the barrier. Two main parts of the paper can be distinguished. The following topics are discussed in the former part: (a) the weakness of the barrier constituted by the current design of nuclear fuel; (b) the continuously increasing complexity of the system, with main reference to the Instrumentation and Control (I&C); (c) the role that the Large Break Loss of Coolant Accident (LBLOCA) had for arriving at the current layout of the Reactor Coolant System (RCS). Furthermore avoiding the severe accidents in 1979, 1987 and 2011, is at the basis of the proposal. In the latter part, the elements of the proposed technological safety barrier are discussed: the As-Low-As-Reasonably-Achievable (ALARA) principle, the Best Estimate Plus Uncertainty (BEPU) approach, the Extended Safety Margin Detection (E-SMD) hardware, the Emergency Rescue Team (ERT) strategy (or a virtual entity for the reactor) and the Independent Assessment (IA) concept. The additional safety barrier, although not demonstrated in the paper, is expected to reduce for a factor in the range 10-1000 the probability of core melt and to have a cost in the order of 1% the cost of a nuclear reactor unit.

1. Introduction

The class of large (1000 MWe or more) Light Water Reactors (LWR) in operation, in construction or under design constitutes the framework for the present paper. The decline in many Countries in the application of nuclear technology for electricity generation, or the high cost of building new plants and declining profitability of current plants which are driving nuclear plant closures complement the framework for the activity. Highlights to justify the performed research are:

- Severe accidents implying radiation impact upon the humans and the environment should not occur, or, the probability should be minimized down to acceptable values.
- Increasing complexity of design, construction and operation of LWR may create (or may have created) unexplored paths for accidents.
- The inherent safety barriers constituted by UO2 pellet and by Zircaloy clad demonstrated unexpected weaknesses during the last two decades, primarily at high burn-up values.

- The improvement in the awareness of technological details and the availability of sophisticate and powerful computer tools produced two counterfeiting outcomes: (a) the in-principle capability to control the LWR safety has improved; (b) Independent Assessment is not deemed as important as it was at the beginning of the nuclear era.
- Public confidence towards nuclear technology may need to be restored at least in selected Countries: the ambiguity of nuclear clean energy controlled by competent scientist-regulators should be clarified.

Then, nuclear technology is the general framework and Nuclear Reactor Safety (NRS) constitutes the main focus for the present paper. NRS is a (well-established) technology by itself and cannot be dis-joined by nuclear technology. About five-hundred Nuclear Power Plant (NPP) units have been safely operated since the demonstration of the capability to control the fission reaction in 1942 and the connection of nuclear fission driven electricity generator to the electrical grid in 1954. A much larger number of reactors (a few thousands) have been constructed and safely operated for purposes different from electricity production including research and production reactors as well as reactors used for marine propulsion. Notwithstanding the achieved safety records, a) the number of NPP built and operated is far below the number envisaged by nuclear pioneers in the 50's and far below a number consistent with the industrial growth, and, b) accidents occurred, including a few catastrophic ones which severely impacted the exploitation of the technology.

Two paradoxical situations can also be identified for NRS nowadays: first, maturity was achieved at a time when the number of NPP units commissioned-constructed per year sharply dropped mainly as a consequence of unique catastrophic events in 1979 and in 1986 (see below); second, interest from industry in implementing research findings and new ideas after those events declined leading to a sort of misalignment between technological capabilities and implementation status. Furthermore, concepts and principles in NRS were proposed by those who developed the nuclear technology in the middle of the past century and since then are embedded into any step of the process leading to electricity production. Those concepts and principles were adopted by other technologies later on and, still today, appear unsurpassed. The implementation of those concepts and principles followed the progress in understanding and the development of new techniques.

The Defense-in-Depth (DiD) which connects the principle of radioprotection with the design, the construction and the operational features of the nuclear reactors, can be taken as the imaginary skyline which drives the development of NRS. On the one hand, the Design Basis Accidents (DBA) have been introduced to demonstrate the robustness of DiD. On the other hand, safety functions, barriers and calculated safety margins resulting from computational analyses constitute perceptible outcomes and provide a measure of the safety of current reactors.

The established technological picture has been rusted (a) by the nuclear tragedies involving [now] conceivable accidents outside the DBA envelope, like Three Mile Island Unit 2, 1979, Chernobyl Unit 4, 1986, and Fukushima Units 1-4, 2011, Galassi & D'Auria 2017, and (b), in an elusive way, by the evidence collected in the last two or three decades, of the weakness of what is still considered a safety barrier, i.e. the clad of nuclear fuel rods.

The mentioned and somewhat irreversible decline of nuclear technology is occurring mostly in the Countries who led the development of the technology; the encouraging perspectives of the same technology in other Countries created a discontinuity between research-expertise and application-expertise. Indeed transfer of competences in on-going among both groups of Countries; however, a market-driven mode is controlling the process where the original competences for the design and ensuring the safety of reactors may have a marginal role.

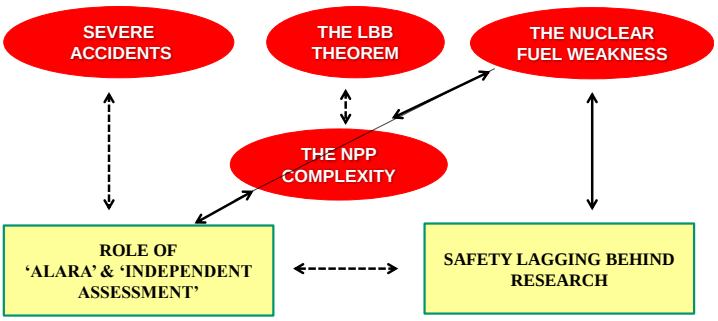
Thus, an ambitious proposal is at the basis of the effort leading to the present paper, D'Auria et al., 2017, see also D'Auria et al., 2015: an innovative vision for NRS is proposed by cross-connecting fundamental safety-to-design-oriented issues and recent research findings; an even thin bridge is created between established and perspective competences, possibly contributing to the awareness of young scientists within a bright future for nuclear technology. More in detail, a risk-informed technological safety barrier is discussed, D'Auria et al., 2018, with the purposes of:

- Preventing or mitigating the occurrence of any conceivable accidents: this includes the outline of possible impact of the new barrier with the Three Mile Island, Chernobyl and Fukushima events.
- Exploiting the research findings in the last two-three decades mostly in relation to accident analysis capabilities and nuclear fuel material performance.
- Extensively and intensively adopting the concepts of pioneers who developed the nuclear technology in the past century like ALARA and IA.
- Putting the bases for demonstrating that the probability of large radiation release equals the frequency of a large meteorite falling on the site of the concerned NPP unit.

As a preliminary disclaim, two topics which are marginally or not considered hereafter are: human factors as key part of NRS and global political and economic strategies in the world which have an inevitable impact upon the exploitation of nuclear technology.

2. The framework for the 'need'

Decades (summing-up, more than a century) spent (by the authors) in connecting research findings with applications in nuclear reactor safety and design are the basis of the topic discussed hereafter. Conceived, hidden and perceptible motivations do exist and provide a roadmap for the performed activity: the diagram in Fig. 1 helps in identifying those motivations.



Red and clear yellow blocks in the figure are perceptible and conceived motivations, respectively. Various interconnections may be envisaged among the blocks and only a few of those are reported. Starting from the bottom left:

Fig. 1 – Motivations for the performed activity.

1) ALARA and Independent Assessment (IA) constitute elements for the proposed safety barrier and are discussed in section 3, see also D'Auria et al., 2017a.
2) Safety lagging behind research is discussed hereafter; noticeably, this also implies the nuclear fuel weakness, next item.
3) The nuclear fuel weakness is considered in section 2.2.
4) The NPP complexity mostly connected with I&C is considered in section 2.3.
5) The Leak Before Break (LBB) constitutes an established technological finding. The related LBB theorem is outlined hereafter: this also constitutes one motivation for section 2.1.
6) Severe accidents involving core melt and core melt plus large radioactivity releases struck over nuclear technology during the past decades: remarks about the role of severe accidents within the present context are provided below.

The occurred severe accidents

A key triggering motivation for the proposal of an additional safety barrier is the occurrence of the accidents in Three Mile Island (1979), Chernobyl (1986) and Fukushima (2011), as well as the occurrence of events where core integrity was nearly missed; see e.g. D'Auria & Galassi, 2017. Large radiation releases to the environment and high frequency for near-to-disaster events cannot be tolerated. Probability of core melt and associated radioactive impact on the environment must be reduced to the expected frequency of a large meteorite fall upon or around the site of the concerned nuclear reactor. Corresponding risk, involving the impact of radiation upon the hit region and the survived population shall be accepted.

It is clear that zero-risk owing to the operation of NPP is impossible to attain, as well as zero-probability per year of core melt. The following statements by concerned scientists, Wang et al., 2013, may be taken as backing the present study:

- **"*In such a dangerous world, a high priority must be placed on efforts aimed at upgrading and enhancing nuclear safety regulatory system. With effective nuclear regulatory system nuclear accident like the Fukushima can be prevented*".**
- **"*Upgrading and strengthening a nuclear regulatory system is not optional but imperative to prevent the next core meltdown*".**
- **"*A credible nuclear watchdog must be an independent agency …*" [current situation not satisfactory].**

The LBB theorem

LBB is based upon the experimental observation that detectable fluid leakage from a large diameter pressure pipe is expected before disruptive double ended break, see e.g., Heckmann & Sievers, 2018, and Bourga et al., 2015. The LBB may have a wide range of applicability in nuclear technology, e.g. it can be used as an argument to justify the elimination of pipe whip restraints, or to design instrumentation capable of early detection of leakages, i.e. before the occurrence of large pipe ruptures. In order to connect with the framework of the present paper, a literature review brought to the following formulation of what we called the 'LBB theorem': "*The LBB implies detection of fluid leakage including supporting analytical studies and is used as an early alarm to scram the reactor; this may exclude the consideration of Large Break Loss of Coolant Accident (LBLOCA) from the list of events to be considered in safety analyses of individual NPP*". The first sentence of the theorem appears reasonable; however, the last sentence is not acceptable within: for instance, seismic events (see also section 2.1.2) and unforeseen thermal stress induced corrosion erosion processes may cause a bypass of the LBB process or sudden large failure of a pipe without prior leakages.

Safety lagging behind research and loss of expertise

An additional key motivation for the present study comes from observing that NRS is lagging behind the technological progress. This is associated to the loss of expertise: a lower number of researchers engaged in nowadays nuclear technology do not have access to funding resources as in the past; selected organizations actually replaced those scientists who contributed to the development of current reactor design. Thus the loss of expertise contributes or enlarges the gap between research findings and application.

Safety lagging and loss of expertise are envisaged in several areas of technology. The nuclear fuel area is considered in detail, as already stated.

2.1 Design/layout features and safety connection

The LBB theorem and, more faintly, the fuel weaknesses (section 2.2) may suggest dropping the LBLOCA from the list of reference accidents for water cooled nuclear reactors; see e.g. Charignon & Lecoy, 2016 (those authors generically mention the "*revision of the safety regulation for LOCA studies*" to justify the exclusion of LBLOCA from the list of design basis accidents). This may

either create an undue gap between the design of vessel equipped NPP and the safety evaluation or may overshadow the design features of those reactors.

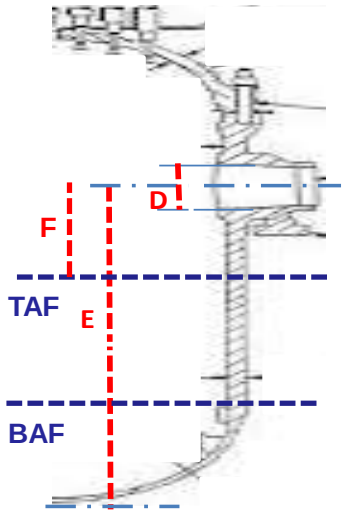
The adoption of water as coolant and moderator in vessel equipped LWR brings as a main consequence the high pressure to ensure efficiency for the thermal cycle to produce electricity. High pressure makes the system vulnerable to the hypothetic loss of mechanical integrity because of unavoidable coolant discharge (i.e., Loss of Coolant Accident, LOCA). The need to ensure core cooling by Natural Circulation (NC), including the use of steam generators as heat sink (in case of PWR), to remove decay heat in case of lack of pumping power, brings additional safety requirements. Thus, LOCA and NC had a key role in defining the layout of primary loop. Details about LOCA impact are given hereafter.

2.1.1 Key primary system features

The key geometric and layout features of concerned RCS were first decided (then planned and designed) in the 50's of the last century; later on, till current year, those features were accepted by coming generations of designers and technologists. Design to safety is a requirement: three aspects connected with LBLOCA are emphasized below which are relevant to the present context:

1) Elevation of Cold Leg (CL) axis [related to the bottom of the Reactor Pressure Vessel (RPV) and to the elevations of the Top and Bottom of Active Fuel (TAF and BAF)].
2) Diameter of the CL pipe.
3) Presence of containment.

The sketch of the RPV of a Pressurized Water Reactor (PWR) is given in Fig. 2. The relative position of CL axis and the bottom of the RPV and the TAF, 'E' and 'F' dimensions, item 1), is such to allow cooling of the core following guillotine break of the same CL pipe: the location of CL at the bottom of the RPV, which might be convenient to reduce the pressure drops, however it causes loss of the injected emergency cooling liquid by gravity and the consequent impossibility to cool the core following the depressurization of the primary system. Any larger size for CL pipe, item 2), is convenient from the view point of minimizing the loop pressure drops during normal operation; however, an upper limit for the diameter is fixed to demonstrate fulfilling of Emergency Core Cooling System (ECCS) design criteria including pressure wave propagation from break location, mechanical load of internals, rod surface temperature excursion (maximum value and slope in a time diagram) during the early blowdown phase.



In the case of Boiling Water Reactor (BWR) the statements above can be repeated: the CL shall be replaced by Recirculation Line (RL). Moreover, the configuration of RPV internals is designed taking into account of the needs to reflood the core after LBLOCA in RL and to achieve suitable value for the Net Positive Suction Head (NPSH) at the RL axis location.

Design targets of Engineered Safety Features (ESF) including ECCS ensure no or acceptable radiation releases such that the containment, item 3), is not needed. However, early designers of PWR decided to add the containment barrier to account for unforeseen (including unforeseeable) deficiencies of the design process.

Fig. 2 – Sketch of RPV in a PWR.

2.1.2 Miscellaneous LOCA related topics

Additional arguments pinpointing the LBLOCA role and importance in NRS, i.e. the critical issues in LBLOCA analysis, are:

- The accumulator size and number, the initial nitrogen pressure, the delivery line size and port connected with the RCS are defined based on the LBLOCA system performance.
- Earthquake may be at the origin of a double ended guillotine break: soil-structure generated loads may combine with thermal loads and corrosion/erosion in primary coolant pipeline.
- Internals are designed to protect the core and the nuclear fuel and 'to absorb' mechanical loads originated by a large break in the proximity of the RPV (see also discussion below).
- Long term core cooling is calculated implying water circulation through the containment sump. Critical issue is the impact of debris upon core cooling, see e.g. Lee et al., 2014, and Azam et al., 2018.

Depressurization wave induced loads

The complex phenomenology associated with mechanical loads induced by depressurization wave generated at the break, last bullet item, deserves additional comments. Break size, and distance from the RPV, local subcooling and, primarily, Break Opening Time (BOT), determine stress upon internals of vessel and upon fuel rods.

The BOT seems to be the puzzling and the most important parameter for the analysis, e.g. see Ylonen, 2008: BOT values in the range (0.1-10) m-s have been calculated by Baum, 1984, although measured values appeared larger. The unfortunate situation, also confirmed by Bandhari & Leroux, 1993, is the difficulty to prove BOT values longer than a few tens m-s. In those conditions the amplitude of break-upstream-propagated depressurization wave remains large. Unpublished work performed by one of the current authors (F. D'Auria) shows that the amplitude of the depressurization wave in typical PWR conditions substantially decrease for BOT in the range 100 ms to 1 s: unlikely, this finding is of limited applicability if BOT cannot be calculated based on the mechanical [including fracture] properties of the concerned piping and the local stress conditions.

The depressurization wave generated at the break enters the annular space between the reactor vessel and the core barrel, it will travel down to the lower internals, as it wraps around the barrel. This is illustrated in Fig. 3 by Krieg et al., 1977, and later on by Hosford et al., 1981 (USNRC NUREG-0609). The depressurization wave, depending upon its amplitude and the upon subcooling of the encountered fluid, may generate voids with a delay of the order of m-s after its passage, and it causes complex Fluid Structure Interaction (FSI), as partly discussed by Robbe et al., 2003, and Mahmoodi et al., 2019. FSI is affected by void and by motion of internals (see also Fig. 3).

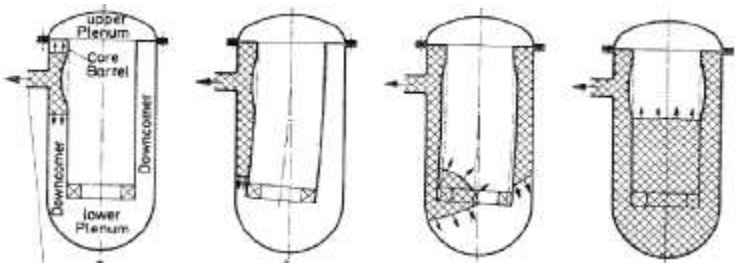


Fig. 3 – Propagation of depressurization wave from the break (shadowed region is at low pressure), Krieg et al., 1977.

2.2 Evidence for fuel and clad weakness

A short summary of components of primary circuit of LWR, i.e. including the vessel, the barrel (PWR), the steam generator and the pressurizer (PWR), the separators (BWR), the control rod drive mechanisms, the main coolant pumps, the shroud and the fuel boxes (BWR) and the pressure lines (cold leg and hot leg in PWR and steam line and recirculation line in BWR), shows that from a structural viewpoint fuel pins constitute the weakest elements to withstand mechanical loads. Nevertheless the overall systems (namely the primary circuit) in PWR and BWR are designed to protect the pins avoiding or minimizing the risk of non-tolerable mechanical loads. Earthquake and pressure wave propagation should a LOCA occur can be identified as the major, low probability, origins of mechanical loads. Chemical and physical mechanisms associated with high burn-up and/or with long term duration in the core have been found, primarily in the last few decades, to heavily corrode the clad of fuel pins.

Accident conditions are of concern. Two further observations drove the present section:

a) The tendency by the industry to attain high burn-up and longer time of fuel in the core.
b) The United States Nuclear Regulatory Commission (US NRC) 'preliminary-draft' Regulatory Guide (RG)1.224, USNRC, 2018b, dealing with new maximum values of both Peak Clad Temperature (PCT) and Equivalent Clad Reacted (ECR): the values for PCT and ECR, never changed (so far) since the original values, part of the 10 CFR 50.46 in 1971, i.e. 2200 °F and 17% respectively; those values are now foreseen to be reduced to 2050 °F and linearly down to 2%, as a function of 'pre-transient H2 content into the clad'.

2.2.1 Pin failure modes and burn-up

A coherent vision, as possible, of nuclear fuel weakness is provided below by putting together information from recently published papers; see Fig. 4 (modified from Garcia de la Infanta, 2015, see also Georgenthum et al., 2006) for nomenclature and fundamentals: the oxide (or zirconia) impact upon clad ultimate resistance is illustrated.

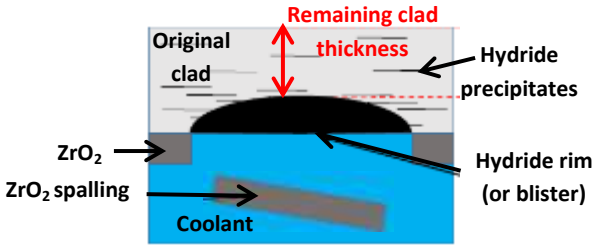


Fig. 4 – Sketch for clad oxide, hydride rim, hydride precipitates and spalling.

Solid-to-solid interference, or Pellet Clad Mechanical Interaction (PCMI), and irradiated fuel materials chemistry, or Fuel Clad Chemical Interactions (FCCI), are considered separately below, although they closely interact.

PCMI Let's start the review from Samal et al., 2011, who studied the already complex rupture mechanisms of Zircaloy tubes in the absence of material degradation processes including irradiation and high temperature: they found that the re-crystallization annealed Zircaloy-2 specimens have higher initiation fracture toughness as well as higher resistance to crack growth compared to non-annealed specimens: this can be attributed to the presence of finer grain and sub-grain micro-structure and lower density of defects in the material.

Reactor start-up power ramp is at the origin of a complex PCMI as discussed by Kim & Jerng, 2011, based on post irradiation examination of leaking fuel rods: at a pellet-pellet interface plane, in a position opposite to a radial crack (in one of the two interfacing pellets), a through wall crack is formed owing to stress concentration. Subsequently and consequently, hoop stress causes a crack

initiation at a 180° azimuthal distance from the first crack; the second crack slowly (30 days estimated) propagates into the clad causing another through wall crack. The inlet of coolant from both cracks induces local oxidization growth; in addition, a number of secondary hydride (or hydride precipitates, see Fig. 4) are formed closely due to steam starvation (steam migrates with difficulty owing to closure of the pellet-clad gap). All of this measured at burn-up around 40 kwd/kgU, corresponding to about 125 μm zirconia thickness in zircaloy-4 clads, at LHGR of about 25 kw/m and power ramp 3%/hr in rods located next to the control rod guide thimble with a control bank maneuvering during the power ramp.

Georgenthum et al., 2006, found, during a Reactivity Initiated Accident (RIA), that the zirconia (or oxide) loading is "equivalent to the loading of a brittle thin film on a ductile substrate submitted to a tensile or a biaxial loading: after a first phase of cracks multiplication perpendicular to the loading direction, the crack density saturates, and spalling can occur". The zirconia detachment or spalling is a complex phenomenon that depends on several interdependent parameters including the oxide thickness, the oxide-clad interface and the loading modes. The interrelation between PCMI and RIA were considered, later on, by Sartoris et al., 2010, based on experiments performed in the CABRI facility. Basically, the authors pointed out the relationship in a Zircaloy clad, between zirconia (oxide) formation, hydride rim depth and Burn-up. One may synthesize a complex scenario by the following rough-snapshot figure: PCMI failure may occur at 40 cal/g following RIA with 60 kwd/kgU burn-up in presence of 100 μm (continuous) oxide and 150 μm (local) hydride rim depth; PCMI failures at values lower than 40 cal/g are documented.

In 2011, Kim, 2011, pointed out the complex nature of pellet-clad mechanical interaction (PCMI)-induced failure. PCMI combined with excessive Zry-4 oxidation and clad hoop stress, following a reactor start-up power in presence of oxide thicknesses and surface cracks cause fuel leak initiation: oxide thicknesses exceeding the oxide design limit of 100 □m at a fuel rod burn-up of 46 Kwd/kgU were measured. Furthermore, the oxide thicknesses were found to vary from 10 to 200 □m in the azimuthal direction at the upper level of fuel pins: a few radial cracks were observed in the azimuthal position having the less oxide, whereas a radial crack was hardly developed in the position having the larger oxide thickness; clad surface cracks in the oxidized region are strongly related to oxide spall-out. Clad damage mechanisms were found to be affected by relatively low coolant temperature (associated with low duty PWR) and by linear heat generation rate.

The difficulty in modeling PCMI is pointed out by Rozzia et al., 2012: experimental data evidence either one or two failure thresholds depending upon the adopted figure of merit (e.g. including the consideration of unavoidable power ramp transients which occur during start-up of reactors) and are not affected by burn-up at values below 20 kwd/kgU. The used model assumes burn-up dependent failures above 20 kwd/kgU. The pellet gaseous swelling during the power ramp is identified having the largest contribution to the discrepancies between measurements and predictions. Otherwise, PCMI modeling capabilities are discussed by Stimpson et al., 2018.

Ballooning and burst Ballooning of a few or of a large number of fuel pins following LOCA cannot be excluded; consequent burst and fuel release to the coolant may occur. Ammirabile & Walker, 2014, compared experimental data with results of code application during reflood. Rods having different power decay and internal gas pressure, derived from the different power peak factors and presence of burnable poisons and pellet eccentricities were installed in the experimental facility. Three typical ballooning peaks associated with the regions between spacer grids were measured. The axial strain profile of the rods with burnable poisons (lower linear heat generation rate) is characterized by a plateau upstream the fifth grid and a peak at the upper elevation: enhancement in cooling conditions that stops the swelling of the rod at that location possibly occurred; better cooling conditions are due to the flow diversion. Suitable modeling capabilities were found.

Electrically heated nuclear fuel simulators were used by Kim et al., 2017, to investigate the effects of the fuel rod deformation and relocation on the reflood. If the effect of fuel relocation is not considered the peak clad temperature in the ballooned rods is lower than in the intact rods: the beneficial effects resulting from the increase in blockage heat transfer override the penalty of flow diversion in the by-pass. On the other hand, when the effect of both fuel rod deformation and fuel relocation are considered, the peak temperature in the ballooned rods became higher than in the intact rods for a value in the range 50 – 100 K. Lower penalties were measured in relation to reflood timing.

A comprehensive set of ballooning-burst experiments for Indian PHWR, is discussed by Sawarn et al., 2014, and Sawarn et al., 2017. The database may not be directly applicable to LWR conditions because of lower clad thickness, lower burn-up and lower internal pressure. Nevertheless the derived experimental data may be used for validating numerical models: burst temperatures and pressures in the range 600–1300°C and 5-70 bar, respectively, are documented.

Fuel rod burst following RIA conditions are considered by Sartoris et al., 2010. The analysis of experimental data showed a significant dependence of burst pressure on oxide layer thickness: this was explained by the existence of a hydride rim layer on the outer wall; the hydride rim layer makes brittle the clad and is similar to an incipient crack.

FCCI Oxygen release from UO2 pellets constitutes an envisaged physical-chemical process even at low burn-up, Besmann et al., 2016. The O2 is supposed to create a clad inside oxide layer up to 8 □m at about 40 kwd/kgU burn-up.

An extensive literature overview is at the basis of the paper by Matthews et al., 2017, dealing with FCCI mechanisms. Although experimental evidence comes from the analysis of the EBR-II Sodium Fast Reactor, selected findings appear of concern for different nuclear fuel, either zirconium or steel cladded. Two main mechanisms having the potential for fuel damage are considered: a) formation of (U,Pu)Fe eutectics into the fuel; b) lanthanides creation from fission and migration to the pellet periphery. More than one eutectic can be formed by U, Pu and Fe and related melting temperatures (obtained in a post-irradiation fuel annealing process) as low as 950 °C are reported. The lanthanides diffuse into the pellet and collect at the clad interface, penetrating the clad. The zirconium rich layer at the pellet boundary (this eventually forms during the fabrication process, or anyway before the in-core life) which may prevent FCCI is destroyed by burn-up originated fuel cracking. The authors conclude: "***Unfortunately, FCCI behavior observed in U-xPu-yZr fuel is a very complex and interconnected phenomenon, historically resulting in limited curve-fit relationships that can only be applied to specific fuel/clad combinations***".

Crud The sketch in Figure 4 becomes more complex if Crud is brought into the picture. Crud formation implies the deposit on the fuel clad, possibly above the oxide, of impurities of the coolant. The word 'crud' is used for fuel pins and corresponds to the word 'fouling' commonly adopted for industrial heat exchanger. Crud and fouling are well known in heat transfer technology namely when nucleate boiling occurs. Crud, other than affecting the clad surface temperature and unavoidably the PCT during a LOCA transient, includes the absorption of boron particles which may locally distort the neutron flux, giving rise to the so-called Axial Offset Anomaly (AOA). Detachment of crud from the clad surface may create local fission power excursions. Crud definitely adds complexity to both the nuclear fuel modeling and the failure mechanisms. The controversy represented by the consideration of crud in licensing of LWR is well depicted by the letters that R. Leyse sent to USNRC, e.g. Leyse, 2007, and by answers he got from USNRC and from industry. Current understanding and capabilities in detecting crud formation can be deduced from the paper by Shim et al., 2016.

Regulatory requirement under (on-going) development at USNRC United States Nuclear Regulatory Commission (US NRC) 'preliminary-draft' Regulatory Guide (RG) 1.224, dealing with new maximum values of both Peak Clad Temperature (PCT) and Equivalent Clad Reacted (ECR) is available for comments, USNRC, 2018b, see also USNRC, 2018, and USNRC, 2018a: the values for PCT and ECR, never changed (so far) since the issued values, part of the 10 CFR 50.46 in 1971, i.e. 2200 °F and 17% respectively; those values are now reduced to 2050 °F and linearly down to 2%, as a function of 'pre-transient H2 content into the clad', noticeably at high Burn-up values (concerned range is 60-70 kwd/kgU). It may be noted that high H2 concentration in the clad can be associated not necessarily with high burn-up; furthermore, the reduction in thresholds value is based upon experiments independent from those considered in the present review.

2.2.2 Implementation of new ECCS criteria

New evidence of nuclear fuel weakness will indeed cause changes (improvements) in ECCS design criteria. The operation of NPP by current fuel violates the 'new' and presumably the existing ECCS rule, e.g. in case of LBLOCA.

A spectrum of consequences from either the implementation of 'new' ECCS rule or from the consideration of recently characterized fuel weaknesses is provided in Table 1.

The design of Accident Tolerant Fuel (ATF), third line in the table, has the potential to provide a technological feedback to the detected weakness and, definitely it constitutes a direction to be pursued by industry and by researchers; e.g. see Karoutas et al., 2018, and Wagih et al., 2018. Both new pellet and new clad materials are currently investigated. The drawbacks associated to ATF are: (a) ATF adoption in all existing reactors may need a decade or more; (b) there is no guarantee that ATF survives blast consequent to depressurization wave propagation from the break (section 2.1) or high burn-up conditions (PCMI, FCCI, ballooning, etc., as discussed in section 2.2).

Table 1 – Consequences from the implementation of 'new' ECCS criteria or from consideration of fuel weaknesses in USA.

Implications: new ECCS rule, or fuel weaknesses	Outcome		Consequence
LBLOCA deleted from the DBA list(1)	Risk oriented – event low probability		Safety-to-design relevance of LBLOCA ignored (sect. 2.1).
Core power reduction	Fulfill the rule		Difficult to be accepted by utilities.
New fuel designed (ATF)	Long time (several years) needed to prove validity		Cost for industry & uncertain end-result at high burn-up.
Perform BEPU analysis – risk oriented [by coupled thermal-hydraulics / neutron physics model & simulating individual fuel pins]	Case 1	ECCS criteria not overpassed	NPP licensable.
	Case 2	ECCS criteria overpassed	Need 'to re-interpret' licensing rules (focus on out-of-containment radiation impact)

(1) This might be the case for other accidents part of current DBA

A different solution is needed and is proposed within the present context: this is cited in the last line (right side) of Table 1 and can be explained with the help of Figure 5. Two statements are needed in advance: 1) proposing or fixing acceptable regulatory limits is only the entitlement of regulatory body; 2) formulating a proposal for ECCS criteria is needed here to provide a consistent framework for the new safety barrier.

An analysis implying the application of the Best Estimate Plus Uncertainty (BEPU) approach, e.g. simulating LBLOCA is needed, D'Auria, 2018, to evaluate the fuel performance. The analysis may end-up either into Case 1 or Case 2 in Table 1: the former outcome is unlikely and so focus is given hereafter to the latter having in mind that each topic mentioned in section 2 is considered in the analysis. Thus, the envisaged BEPU analysis ends-up with the demonstration that current ECCS

design criteria cannot be fulfilled. At this point, if LBLOCA (and, possibly, any other accident for which the ECCS criteria are not fulfilled) remains part of the DBA, the concerned reactor cannot operate at full power.

A probability related domain is depicted in Fig. 5, with probability (events per reactor/year) decreasing from left to right. The Design Basis Accident (DBA) and the Design Extension Condition areas fill the left and the right regions of the diagram respectively; DEC is consistent with IAEA definition, IAEA, 2016. The right vertical line characterizes the (undefined in the present context) predictable value for the frequency of a large (again undefined here) meteorite falling on (or around) the site of the concerned nuclear reactor.

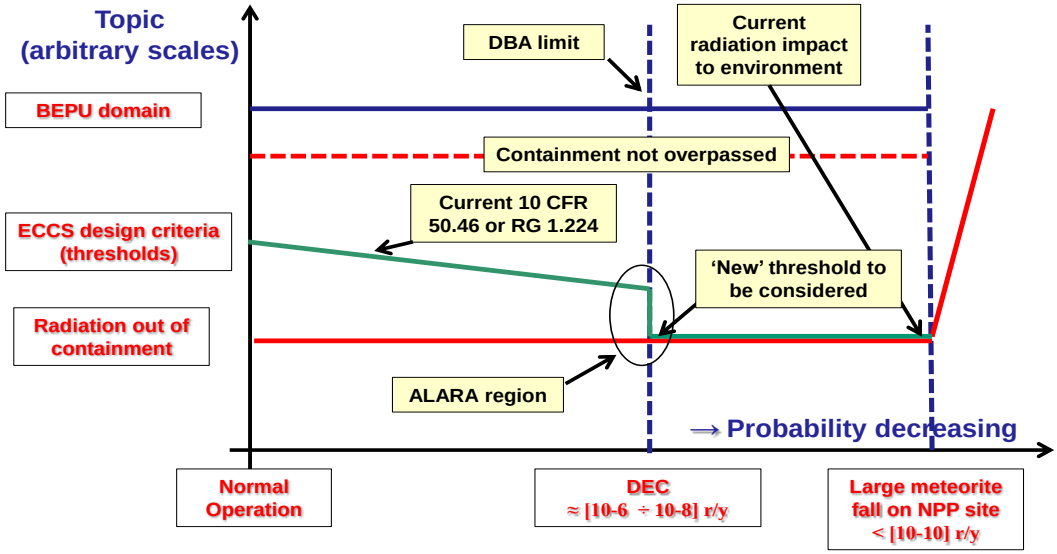


Fig. 5 – Proposal for a consistent regulatory framework.

The diagram is proposed having in mind LBLOCA as part of DBA. Explanatory statements are:

- Radiation impact out of the containment should not change within the probability range down to the 'meteorite frequency' (bottom full line) and containment integrity shall be ensured (horizontal dotted line); outside the range, radiations impact cannot be excluded or controlled (and proper mitigative actions shall be undertaken, not part of the context for the present paper).
- ECCS requirements are more stringent for high than for low probability events (oblique line), so called graded approach: e.g. DNB limit should not be overpassed for high probability events while PCT is the limit for low probability events. Here the proposal is that current or new rules remain valid for LBLOCA; however, ALARA driven overpassing of acceptability thresholds (for the minimum possible extent, e.g. failure of fuel pins minimized) shall be tolerated provided that the integrity of the containment barrier is kept (see section 3.1 for the ALARA role).
- The BEPU approach (upper full line) has capabilities to determine reactor performance in case of accident covering the reported probability domain in a situation 'before loss of core geometric integrity' (see also discussion above).

2.3 Design complexity

The recent (Oct. 29, 2018) crash of a brand-new Boeing (large) airliner (Lion Air Flight 610) in Indonesia, "... ***not (on) a single lapse but (on) a cascade of troubling issues that ended with the deaths of all 189 people on board***", Beech & Bradsher, 2018, is sadly taken to enter the (I&C) complexity subject.

Let's restrict the topic to I & C. The following can be stated:

A) Complexity is the design answer to efficiency and cost savings in a competitive world. Progress of civilization is connected with complexity.
B) Cable aging may be seen as a huge (controversial) issue in nuclear safety.
C) Cyber-security also constitutes an issue.
D) Vulnerability of components to fire.
E) Resistance of components to thermal and mechanical conditions following an accident.

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

2.3.1 The I&C issue

I&C 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. Nevertheless a few random-selected topics are considered hereafter which may substantiate the remarks given in the previous paragraph.

I&C and Defense-in-Depth (DiD) DiD implies diversity, redundancy and independence of components. Adding diversity, redundancy, and independence also increases a system complexity, expanding the range of possible error or failure scenarios, Hashemian, 2011.

Field-Programmable Gate Array (FPGA) The nuclear power community has attempted to address the complexity issue through stringent regulation. The FPGA technology has emerged as an answer to the risks posed by overly complex I&C software. An FPGA is a device made up of thousands or millions of logic gates on integrated circuit chips that can be programmed to perform various tasks, ranging from simple logic to complex mathematical functions. FPGA executes only that program repetitively and results simpler than an equivalent microprocessor, minimizing the risk posed by complexity, Hashemian, 2011.

Software Reliability (and Verification) The Verification and Validation (V&V) of numerical programs, with main reference to the verification in the case of I&C software, constitutes an extraordinary challenge for designers. Textbooks have been written, see e.g. Roache, 1998, and developments are on-going, see e.g. D'Auria & Lanfredini, 2018. Despite all possible efforts to prevent software faults, these faults are inevitable. A philosophical issue is triggered by Fan et al., 2013, who quote the words of a statesman of last century "If a problem has no solution, it may not be a problem, but a fact – not to be solved, but to be coped with over time." This appears to be current situation for complex I&C software. The adoption of FPGA technology (previous paragraph) may represent a solution. However, although FPGA does not use software, it needs a specific 'Hardware Description Language': this again needs verification, Maerani et al., 2018, see also Ahmed et al., 2017, and Kang et al., 2018.

Communication and cyber-security The transition from analogic to digital I&C implies the need to transfer larger volume of data generated by digital equipment; interconnections between Programmable Logic Controllers (PLC) based on data communication protocol, which allow effective data transmission between PLC for multiple operational functions including safety functions, have been employed to replace conventional hard-wired signal transmission. This communication system is not immune from faults and risks as discussed by Lee et al., 2017. The challenges such as fast obsolescence, the vulnerability to cyber-attack, and other related issues of

software systems have currently led to the consideration of FPGA as an alternative to PLC, as discussed in previous sections. A safety margin estimation approach has been proposed for cyber threat prioritization by Wang et al., 2018: this includes the consideration of multiple failure modes due to random failures or induced by malicious external attacks.

2.4 Summary remarks

Making reference to Fig. 1, nuclear fuel weakness (key words are PCMI, FCCI, crud, hydride formation, ballooning and burst), NPP complexity (key words are I&C), and occurred severe accidents constitute incontrovertible arguments, sections 2.2 to 2.4, which may be used to justify the need for a new safety barrier.

Safety lagging behind research and the connected loss of expertise are perceptions: the provided discussions may be used to enforce the awareness for those issues and the importance of the safety barrier. The ALARA concept and the requirement for Independent Assessment are embedded into the proposal for the new barrier (sections 3.1 to 3.5)

Furthermore, the need to consider LBLOCA in NRS as a DBA, and the further justification for the new safety barrier is based upon argumentations (section 2.1) summarized hereafter:

1) The LBB is an important technological finding which shall not be used to remove the LBLOCA from the DBA list.
2) The elevation and diameter of CL (case of PWR) and the RL (case of BWR) and the current containment design bases are used here to confirm the importance of LBLOCA.
3) The BEPU approach (part of the proposed barrier) may cope with the following issues:
    a. Integrity of RPV internals: internals were designed without the capability to assess their resistance, namely following depressurization wave propagation after a double ended guillotine LBLOCA.
    b. Debris in the containment sump: debris may cause cavitation of ECCS pumps and blockage of core channels, threatening the long term cooling capability.
    c. Containment resilience. Containment was designed as the ultimate barrier preventing radiations into the environment: the strength of the barrier and no-radiation impact can be proved.
4) All of the above, based upon the ALARA principle (Fig. 5), shall be used for a ‘flexible’ or risk-informed interpretation of ECCS rules (either current 10 CFR 50.46 or the possible ‘new’ RG 1.224 based requirements): fault fuel may release radioactivity to primary circuit and containment, however environment is protected according to current requirements.

3. The elements of the technological safety barrier

Elements are introduced below which are consistent with current technological advancement and understanding and form the new safety barrier (section 4).

3.1 ALARA

ALARA (As Low As Reasonably Achievable) constitutes a recognized and accepted principle in radioprotection: a huge variety of definitions & applications can be found in the literature. Baumer, 2015, writes “***After the war, as the United States moved toward further investment …, the Atomic Energy Commission (AEC)… laid out increasingly stringent safeguards to protect both civilians and nuclear workers. This effort culminated in the ALARA protocol, which eventually became adopted as the gold standard of nuclear safety***”. Protection and safety shall be optimized in order that the magnitude of individual doses, the number of people exposed and the

likelihood of incurring exposures all be kept as low as reasonably achievable, economic and social factors being taken into account.

The ultimate goal for ALARA is radiation control: intermediate steps for the implementation shall be considered as working as a whole; in other terms overpassing of one barrier may reveal un-influent for the fulfilling of the final goal if other barriers have enough strength.

ALARA implies that rigorous analytical demonstration for the value of any needed parameter either in safety or in design of nuclear reactor may not be available. More subtle, one may envisage that lack or insufficient knowledge of phenomena and/or system performances are expected. Conservatism is actually added to the analyses: the presence of containment with related strengths can be taken as the ultimate barrier to cope with lack of knowledge or unforeseen events. In other terms ALARA is not needed to design a dog-house: in this case the properties of adopted materials, the expected loads are well known and costs do not put constraints for the design.

Within the present context, the consideration of ALARA brings to:

1) Accepting a relaxation of ECCS acceptability criteria (i.e. determined by recently discovered nuclear fuel structural weakness), provided radiation impact upon humans and environment remains consistent with current regulations.
2) Recognizing the full role of containment as the ultimate (or final) barrier for the release of fission products provided demonstration that failing of 'upstream' barriers does not affect the capability of the final barrier.
3) Endorsing (by regulatory body) the role of BEPU as the needed approach to perform NRS analyses, e.g. extending from radiation protection the wording 'as low as … achievable' to the words 'the best one can do' in performing computational analyses relevant to the licensing process.

3.2 BEPU

BEPU (Best Estimate Plus Uncertainty) is the outcome of several decades worldwide researches. It constitutes a mature technology based upon the application of sophisticate numerical codes to the analysis of accidents, primarily, D'Auria, 2018.

ALARA can be thought as the logical origin of BEPU, as already mentioned, D'Auria et al., 2017. Suitable procedures for Verification and Validation (V&V), addressing the scaling issue, demonstration of quality of calculation, the evaluation of uncertainty in code predictions and for suitable coupling of codes (e.g. neutron physics and structural mechanics with thermal-hydraulics) are among the pillars of BEPU.

BEPU applications can be found in D'Auria & Mazzantini, 2009, Pla et al., 2009, D'Auria et al., 2012, and Rivas-Lewicky et al., 2016. Recently an activity has been completed to demonstrate the possibility to expand BEPU to all the analytical parts of Final Safety Analysis Report (FSAR), Menzel et al., 2016.

Within the present context BEPU approach is needed:

1) To connect NRS and current knowledge.
2) To identify a number of parameters part of the E-SMD (see next section).
3) To help in preventing the removal of LBLOCA from the list of DBA.
4) To make possible the Independent Assessment.

3.3 E-SMD

Safety Margin (SM) is a well-known concept in NRS: suitable safety margins must be demonstrated and are part of design, construction and operation of existing reactors, D'Auria et al., 2017b, and D'Auria et al., 2017c.

The acronym E-SM, or Extended Safety Margins, D'Auria et al., 2015, implies a substantial increase, related to 'original' SM, in the number of parameters which shall be considered for identifying the safety status of a reactor. An order of magnitude of about 10^4 is expected for the signals in any operating reactor to form the E-SM database. Furthermore, one SM signal, the combination of two or several SM signals are used to create a macroscopic SM.

The acronym E-SMD, or Extended Safety Margin Detection, is introduced as a hardware element of the new safety barrier, D'Auria et al., 2018. Each of E-SMD detectors produces an electronic signal which is recorded in proper computers: all signals are combined to get the overall (safety) status of NPP unit: nothing is visible to the operators (obviously everything is accessible to 'some' of them). Operators enter in touch with the signals only before an action (all actions should be automatic) is taken by the overall E-SMD system. One may summarize that the role of E-SMD is to get a continuous detailed picture of instantaneous reactor safety status in order:

1) To allow scram following low and very low probability events.
2) To inform in advance the operators about actions to be undertaken to prevent or to mitigate the evolution of any event.

3.4 IA

The Independent Assessment (IA) is a fundamental, worldwide accepted NRS requirement established since the early development of nuclear technology. Later on, IA became more difficult due to increasing sophistication of NPP which implies more proprietary data needed for safety demonstration, D'Auria et al., 2017a. Within the present context IA is a necessary condition for the application of BEPU. This is expected to generate the major hurdle for the implementation of the new safety barrier.

3.5 ERT

The Emergency Rescue Team (ERT) consists of a group of highly trained and specialized rescuers who own suitable machinery and equipment (helicopters, diesel generators, etc.), D'Auria et al., 2012a, see also Powell et al., 2016. Those rescuers have access to each nuclear reactor installed within an assigned geographic region. Here, 'access' means: (a) availability of plugs to connect DG feed-pump delivery sides to primary and secondary circuits of reactor and to ensure cooling of even damaged core; ERT team should arrive at the concerned site within one-hour (i.e. a time span lower than the time needed for massive core melt), based on E-SMD signals; (b) possibility to induce scram of the reactor from remote location (this capability is already available in some Countries: special Nuclear Center under the control of a Government regulatory institution are connected with the control rooms of existing reactors). The ERT is assumed to be part of a devoted center (the ERT center) which may serve the power plants in one geographical region. Within the present context ERT is needed to cope at due time with expected and non-expected situations which have the potential to endanger the availability of the ultimate electrical power source on the site.

4. The new safety barrier

As an alternative to the irreversible decline of the large NPP technology an innovative accomplishment seems unavoidable: this shall cope with identified issues or drawbacks (embryonic idea already submitted to international community in 2015, see e.g. D'Auria et al., 2015): those are

nuclear fuel weakness, possible inadequate consideration of NPP complexity (I&C is identified with some detail) and inadequacy of current safety regulation. Within the present context, drawbacks are balanced by current progress, namely the analytical capabilities associated with BEPU, the proposed information technology based E-SMD and the powerful ERT. Those elements are supported by ALARA and IA.

4.1 The concept and the features

A vision for the existing safety barriers and the new technological barrier is provided in Figure 6.

Starting from the irradiated nuclear fuel (red ellipse at the center of the picture; the barrier sometimes associated with the pellet is neglected here), the following barriers are identified (red labels B1 to B5 in the figure):

- The B1 deals with fuel and clad (basically the clad); this is the barrier in relation to which the weakness is discussed in section 2.2.
- The B2 is constituted by the pressure boundary for the primary circuit: this exists in all water cooled reactors.
- The B3 is not usually recognized as a barrier in NRS technology: this is designed according to different philosophies and exists in all water cooled reactors. This is constituted by the installed Engineered Safety Features (ESF) and, noticeably, includes the Emergency Core Cooling Systems (ECCS).
- The B4 is constituted by the containment and [including the 'confinement' installed in majority of VVER-440, the common pressure building installed in one Canadian Deuterium Uranium (CANDU) NPP and the reactor cavity in RBMK], exists in all water cooled reactors.
- The B5 is the additional 'risk-informed - technological' barrier which constitutes the topic of the proposal in the present paper.

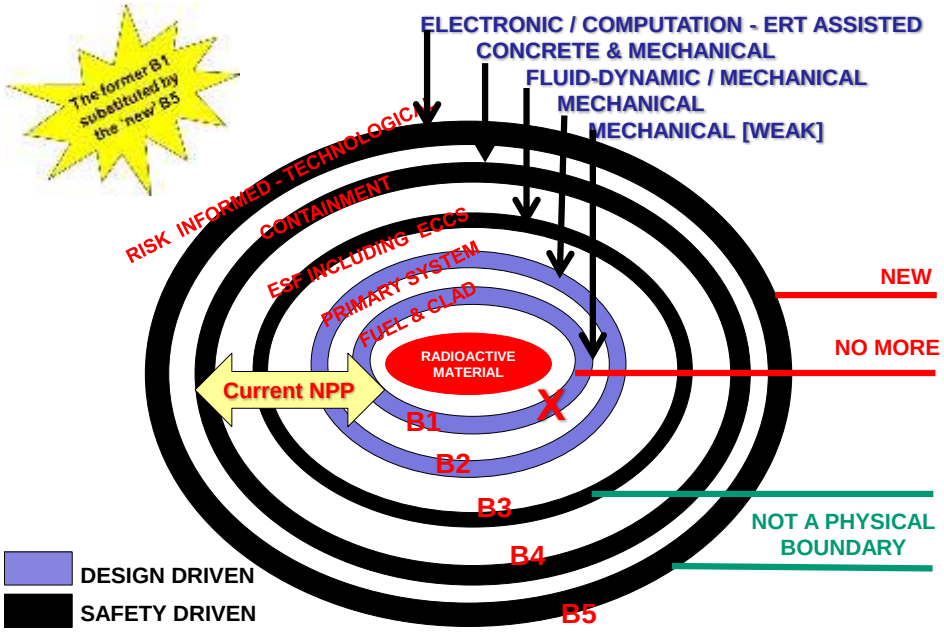


Fig.6 - The vision for safety barriers.

Furthermore, the following notes apply:

- The B1 and the B2 (clear blue in Fig. 6) are introduced according to design needs of reactors.

- The B3, the B4 and the B5 (when it will be available) are designed according to NRS needs.
- The B5 is expected to substitute the B1 when B1 weakness is (formally) recognized.
- In relation to each barrier, further characterization is provided in above figure (upper right), e.g. including the attributes 'mechanical', 'concrete', 'electronic', etc.

The additional barrier B5 is constituted by a combination of the following elements, which have a heterogeneous nature and role as discussed in section 3: the As Low As Reasonably Achievable (ALARA) principle, the Independent Assessment (IA) requirement, the Best Estimate Plus Uncertainty (BEPU) approach, the Extended Safety Margin Detection (E-SMD) concept and the Emergency Rescue Team (ERT), nowadays a virtual-desired entity.

A summary sketch of the elements which constitute B5 is provided in Fig. 7.

ALARA and IA are philosophical elements; BEPU constitutes the software element; E-SMD and ERT constitute the hardware elements of B5.

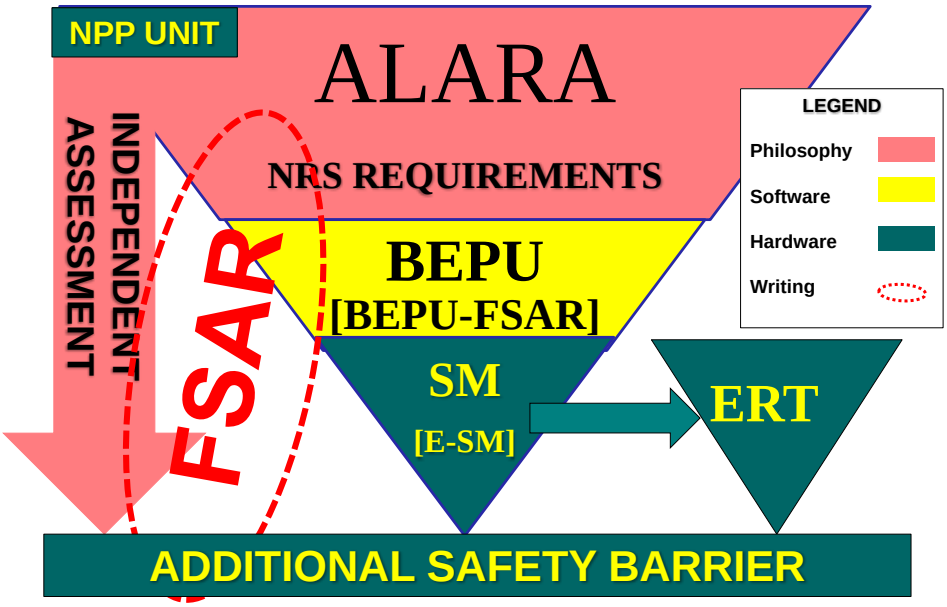


Fig.7 – Summary sketch of elements which constitute the additional safety barrier (B5).

Let's first substantiate the connection among the terms adopted for defining the B5 in Fig. 7. B5 is a risk-informed technological barrier, needing electric and electronic tools (E-SMD) and computational tools (BEPU); it is ERT supported. The words 'risk-informed' requires full consideration of Probabilistic Safety Assessment (PSA) techniques as well as integration of those techniques into the Integrated Risk Informed Decision Making (IRIDM) framework, IAEA, 2011. The word 'technological' reflects the need of consistency between the elements of the barrier and the progress of technology including the database of knowledge (e.g. a new magnitude of earthquake in an assigned geographical region): the B5 shall be constantly upgraded. The words 'electric' and 'electronic' give the proper emphasis to: a) the consideration of Instrumentation and Control (I & C) into the safety analysis; b) the design, the installations and the operation of (an order of magnitude) 10^4 detectors for fulfilling the needs of the E-SMD element. The word 'computational' stresses the importance of analyses which are qualified and independent from the designer and utility of the reactor. The words 'ERT supported' emphasizes the need for ERT: E-SMD continuously monitors the NPP, the environment and the actions of the staff, and eventually solicits the intervention of ERT.

The B5 safety barrier is a dynamic system tailored to each reactor, although design philosophy as well as procedures and databases are in common to all reactors.

The concerned NPP Unit is the starting point for the design of B5: the information database dealing with design, construction and operation of the reactor is relevant. The regulatory framework at the basis of the licensing of the Unit (i.e., the item 'NRS Requirements' at the top of the diagram) shall form the second database needed to start the process for constituting the B5. ALARA is a driving principle in this connection.

A 'standard' Final Safety Analysis Report (FSAR), according to regulations is available for any existing Unit or is expected to be issued for new (future) built reactors. This is part of the second database mentioned in the previous paragraph. A new FSAR, independent of the first one and basically including the same information is expected to be created and to form a cross-cutting element for the B5: the new FSAR is called BEPU-FSAR, central element in the diagram Fig. 7); its cross-cutting nature is visualized by the dotted bounded ellipse on the central-left of the diagram.

The BEPU techniques and/or approach (central element in the diagram), originally derived from nuclear thermal-hydraulics and applied for accident analysis, e.g. D'Auria, 2018, are extended to cover any analytic parts of the (new) FSAR, Menzel et al., 2016, leading to the so called BEPU-FSAR (i.e. the 'new' FSAR).

IA, left of the diagram, constitutes a requirement for the 'new' FSAR. Independent assessors should have access to the NPP Unit design and licensing information (mentioned databases) and develop the 'new' FSAR, D'Auria et al., 2017a. Because of the proprietary nature of information in the databases, although independent assessors are not in competition with industry (either designer or utility of the NPP), the IA is expected as the critical element for the overall process.

The E-SMD set of safety margins and corresponding transducers for the current safety status of the reactor (central bottom of the diagram) can be determined by a specific procedure, D'Auria et al., 2017c, supported by the outcomes of BEPU-FSAR analyses.

The ERT operation (bottom right of the diagram) is expected to be informed by the E-SMD, i.e. horizontal arrow in the diagram.

Finally, the combination of BEPU application (noticeably leading to BEPU-FSAR) and E-SMD, driven by IA and under the umbrella of ALARA, with the support of ERT, forms the additional dynamic safety barrier (bottom of diagram).

The cost

A detailed cost evaluation for the new barrier is beyond the purposes of the present paper; still the feasibility of any technological product shall be associated with costs. In the present case, the following notes apply:

- The ALARA and the IA cost shall be 'zero USD' by definition: related cost consideration is embedded into BEPU.
- BEPU should be performed by an institution independent of the vendor or utility of a power plant. The direct experience of current authors in relation to BEPU activities leads to a cost estimate for a "first-of-kind" activity in the order of 50M USD.
- E-SMD cost can be estimated considering that majority of the detectors, in the order of magnitude 10^4 needed as already mentioned, are displacement or temperature sensors (e.g. thermocouples). Assuming a 1000 USD/[detector (and cable)], the E-SMD cost can be estimated as 10M USD.

- The ERT cost shall be estimated as 10M USD (the cost in this case is per year of reactor operation), if ten or more reactors are served by the same ERT center.

The cost of a first-of-a-kind' B5 results to be less than 100M USD or in the order of magnitude of 1% of the overall cost of a large (1000 MWe) water cooled reactor unit.

4.2 The cross-link between the elements and the challenges

In addition to the situations that lead to the major accidents in NPP (see also below), the challenges for the B5 derive from the LBLOCA analysis and from identified weaknesses, e.g. the topics outlined in section 2. A cross-connection between the elements of B5 and the challenges can be found in Table 2.

The evaluations X, Y and Z in each box of Table 2 shall be considered as qualitative, i.e. without the definition of the boundary between prevention and mitigation. Comments about the cross-link are provided below in relation to the accidents in the lines one to three, Galassi & D'Auria, 2017. Details about the other lines should be derived from text in sections 2 and 3.

Table 2 – Challenges and expected response for the new safety barrier (B5).

Challenge		ALARA	BEPU	E-SMD	IA	ERT	Notes
Three Mile Island			X	X			Either BEPU analysis or E-SMD would have prevented the event.
Chernobyl		X				Y	Following strictly procedures (safety culture) would have prevented the accident. ERT action would have reduced radiological impact.
Fukushima		X	X	X	X	Y	Consideration of external events as far as known (ALARA) and IA would have prevented the event; ERT would have mitigated the event.
Fuel weakness		X	X	X	X	Y	Additional safety barrier needed.
I&C complexity		X	X	X	X	Y	
LBLOCA related	Pressure wave loads	Z	Z				Challenging 1 of 5 ECCS design criteria – core integrity.
	Ballooning-burst and H2 reaction	Z	Z				Challenging 2 of 5 ECCS design criteria – PCT, '17% maximum local oxidation of fuel clad thickness'.
	Radiation out-of-containment		Z				Radiation transport from fuel to primary loop to containment.
	Debris in the sump		Z				Challenging 1 of 5 ECCS design criteria – long term cooling.
	Seismic generated LBLOCA	Z	Z				Consideration needed of low probability.

X = prevented; Y = mitigated, Z = justified (criteria fulfilled)

Three Mile Island Accident

In case of the TMI-2 accident, B5 would have stopped (i.e. by generating a scram signal) the operation of the unit well before the event. The simultaneous closure of the manual Auxiliary Feed-Water (AFW) valve and the leaking Pilot Operated Relief Valve (PORV) are a typical combined failure which would have caused a red alarm from E-SMD detectors. BEPU analysis with current capabilities would have excluded the operation of Main Coolant Pumps (MCP) during the accident and the operator consideration of the pressurizer liquid level as a valid signal (e.g. to stop ECCS water delivery or MCP operation). So the accident would have not even been triggered, or in case triggered, would have not evolved to core melt. ERT was definitively not needed.

Chernobyl Accident

The conditions which caused and/or are the roots for the explosion came into place at least 24 hours before the event. A number of mismatches between measured parameter values and allowed

parameter values occurred different times in this period. The issue was that the operators decided to ignore, and /or they were demanded to ignore, those mismatches. A critical human factors problem occurred. Remote alarms eventually triggered by E-SMD could also have been ignored by (negative) operator actions.

ERT intervention became needed because of the repeated controversial actions by NPP operators. At first, a remote ERT controlled scram would have occurred. An ERT team, properly supported by Country Army should have intervened removing negligent operators. The Chernobyl accident would have not occurred.

Fukushima Accidents (Units 1, 2 and 3)

The signal challenging the B5 in each of the three units would have been the earthquake: its magnitude above the design value would have caused scram (which actually happened during the event) and would have alerted ERT (clearly this did not happen).

A concrete application of the IA based BEPU approach would have demonstrated deficiencies in the characterization of external events, noticeably earthquake and tsunami, by providing the latest evidence from the occurrence of those events all over the world. Especially an earlier earthquake above design-earthquake level in Japan (hitting Kashiwasaki-Kariwa NPP in July 2007) and an earlier severe tsunami in Thailand (2004) should have alarmed responsible persons. Stronger physical barriers, e.g. including location of emergency diesel generator at high elevation and stronger doors to the emergency diesel buildings, would have prevented core degradation.

ERT intervention needed because of the severity of the earthquake and of the consequent tsunami (possible satellite-based measurement of the tsunami wave height should have contributed to the early alert of the ERT team). Proper ERT action would have prevented extended core damage.

5. Conclusion

Reference is made to large Water-Cooled Nuclear Reactors now under operation, construction or design. New reactor concepts including SMR may benefit of the argumentations in the paper.

The activity is triggered from noting the weaknesses of nuclear fuel primarily at high burn-up and the increasing complexity of NPP. Key related conclusion is the characterization of selected fuel failure mechanisms: this is also connected with the need of regulatory countermeasures. Similarly, selected I&C features are described to outline the NPP complexity.

The difficulty to finalize the analysis of complex transient scenarios (e.g., in case of LBLOCA, connected with the nuclear fuel weaknesses, the propagation of pressure waves, and the presence of debris in the coolant in case of sump recirculation), might suggest dropping LBLOCA from the mandatory list of events to be analyzed within the licensing process. Therefore, design related motivations to keep LBLOCA as a key accident in safety analyses have been re-stated: this might imply a relaxation in the application of licensing criteria and the (obvious) full consideration of the role of containment.

The key result from the activity is the proposal and the characterization of a ‘new technological’ safety barrier which seems unavoidable in view of the identified issues. The new barrier has the capability:

- To deal with the nuclear fuel weakness and the NPP complexity.

- To reduce the core melt probability down to the value corresponding to the fall of a large meteorite around the concerned NPP site.
- To possibly restore the public confidence towards nuclear technology.

The concept for the new barrier is based on the As-Low-As-Reasonably-Achievable (ALARA) principle, the Best Estimate Plus Uncertainty (BEPU) approach, the Extended Safety Margin Detection (E-SMD) hardware, the Independent Assessment (IA) requirement and the Emergency Rescue Team (ERT) strategy. A rough cost has been performed ending with evaluation of an overall cost for the barrier given by 1% the cost of a unit reactor. The main difficulty for the implementation of the barrier appears to be associated with the rigorous satisfying of the IA requirement.

The human factors as key part of nuclear reactor safety and the worldwide global political and economic strategies are not considered within the present framework: those topics shall have a role as far as the implementation of the safety barrier and the public acceptance are concerned.

References

Ahmed I., Jung J., Heo G., 2017, Design verification enhancement of field programmable gate array-based safety-critical I&C system of nuclear power plant, Nuclear Engineering and Design, 317, 232–241

Ammirabile L., Walker S.P., 2014, Dynamic ballooning analysis of a generic PWR fuel assembly using the multi-rod coupled MATARE code, Nuclear Engineering and Design, 268, 24–34

Azam M.S., Niu F., Wang D., Zhuo W., 2018, Experimental and CFD analysis of the effects of debris deposition across the fuel assemblies, Nuclear Engineering and Design, 332, 238–251

Bhandari S., Leroux J.C., 1993, Evaluation of crack opening times and leakage areas for longitudinal cracks in a pressurized pipe Part II. Application of proposed model and fracture dynamics, Nuclear Engineering and Design, 142, 1-2, 21-25

Baum M.R., 1984, Break opening times for axial rupture of a gas-pressurized pipe, Nuclear Engineering and Design, 77, 161–167

Baumer M., 2015, ALARA: The History and Science of Radiation Safety, Coursework 'Introduction to Nuclear Energy', PH241, Stanford University, (Ca, US)

Beech H., Bradsher K., 2018, A fatal dive with just seconds to pull out, The New York Times – International Edition, Nov. 10-11

Besmann T.M., McMurray J.W., Simunovic S., 2016, Application of thermochemical modeling to assessment/evaluation of nuclear fuel behavior, CALPHAD: Computer Coupling of Phase Diagrams and Thermochemistry, 55, 47–51

Bourga R., Moore P., Janin Y-J., Wang B., Sharples J., 2015, Leak-before-break: Global perspectives and procedures, Int. J. of Pressure Vessels and Piping, 129-130, 43-49

Charignon C., Lecoy J-C., 2016, A New IB-LOCA Evaluation Model Based on the CATHARE System Code, 11th Int. Top. Meet. on Nuclear Reactor Thermal Hydraulics, Operation and Safety (NUTHOS-11), Gyeongju (Kr), October 9-13, N11P1234

D'Auria F., Mazzantini O., 2009, The Best-Estimate Plus Uncertainty (BEPU) Challenge in the Licensing of Current Generation of Reactors, IAEA Int. Conf. on Opportunities and Challenges for Water Cooled Reactors in the 21st Century, Vienna (A), Oct. 27-30

D'Auria F., Camargo C., Mazzantini O., 2012, The Best Estimate Plus Uncertainty (BEPU) approach in licensing of current nuclear reactors, Nuclear Engineering and Design, 248, 317-328

D'Auria F., Galassi G.M., Pla P., Adorni M., 2012a, The Fukushima Event: The Outline and the Technological Background, J. Science and Technology of Nuclear Installations, Article ID 507921, 1-25

D'Auria F., Glaeser H., Kim M-W., 2015, A Vision for Nuclear Reactor Safety, Invited (Key-Speaker) at 46th Jahrestagung Kerntechnik Annual Meet., May 5-7, Berlin (G) and 9th Int. Scientific and Technical Conf. Safety Assurance of NPP with VVER, OKB GIDROPRESS, Podolsk (Ru), May 19-22

D'Auria F., Debrecin N., Glaeser H., 2017, Strengthening nuclear reactor safety and analysis, J. Nuclear Engineering and Design, 324, 209-219

D'Auria F., Glaeser H., Debrecin N., 2017a, Independent Assessment for new nuclear reactor safety, EPJ Nuclear Science and Technology, 3, 31, 1-4

D'Auria F., Debrecin N., Glaeser H., 2017b, Conjugating ALARA, BEPU, Safety Margins and Independent Assessment in Nuclear Reactor Safety, Invited at Plenary Session of "Safety Assurance of NPP with VVER", Podolsk (Russia), May 16-19

D'Auria F., Glaeser H., Debrecin N., 2017c, BEPU and Safety Margins in Nuclear Reactor Safety, Int. Conf. Topical Issues in Nuclear Installation Safety - Safety demonstration of Advanced Water Cooled Nuclear Power Plant Vienna (A), June 6-9, IAEA-CN-251

D'Auria F., 2018, BEPU status and perspectives, Invited at ANS Best Estimate Plus Uncertainty Int. Conf., Lucca (I), May 13-19

D'Auria F., Lanfredini M., 2018, Introducing V&V&C in nuclear Thermal-hydraulics, ASME Verification and Validation Symposium (VVS2018), paper 9321, Minneapolis (MN, USA), May 16-18

D'Auria F., Debrecin N., Glaeser H., 2018, New safety Barrier for current and future nuclear reactors, Invited at 5th Int. Scientific and Technical Conf. "Innovative Designs and Technologies of Nuclear Power", ISTC NIKIET, October 2–5, Moscow (Ru)

Fan C.F., Yih S., Tseng W.H., Chen W.C., 2013, Empirical analysis of software-induced failure events in the nuclear industry, Safety Science, 57, 118–128

Galassi G. M., D'Auria F., 2017, Thermal-hydraulics aspects of key nuclear accidents, Book 'Thermal Hydraulics in Water-Cooled Nuclear Reactors', [F. D'Auria, Ed.], Chapt. 16, Elsevier, Woodhead Publishing, 1099-1152

Garcia de la Infanta J.M., 2015, On the impact of the fuel assembly design evolution in the spent fuel management, Int. Conf. on the Management of Spent Fuel Nuclear Power Reactors: An Integrated Approach to the Back End of the Fuel Cycle, Vienna (A), June 15-19, IAEA–CN–226 ID122

Georgenthum V., Desquines J., Bessiron V., 2006, Influence of Outer Zirconia Transient Cracking and Spalling on Thermomechanical Behavior of High Burnup Fuel Rod Submitted to RIA, Nuclear Science and Technology, 43, 9, 1089–1096

Hashemian H.M., 2011, Nuclear Power Plant Instrumentation and Control, Nuclear Power, Pavel Tsvetkov (Ed.), IntechOpen, DOI: 10.5772/18768, 1-21

Heckmann K., Sievers J., 2018, Leak-before-break analyses of PWR and BWR piping concerning size effects, Nuclear Engineering and Design, 326, 383–391

Hosford S.B., Mattu R., Meyer R.O., Throm E.D., Tinkler C.G., 1981, Asymmetric Blowdown Loads on PWR Primary Systems, USNRC NUREG 0609, Washington (DC, US)

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

IAEA, 2016, Safety of Nuclear Power Plants: Design, Specific Safety Requirement, SSR-2/1 (Rev. 1), Vienna (A), 1-99

Kang H.G., Lee S.H., Lee S.J., Chu T-L., Varuttamaseni A., Yue M., Yang S., Eome H.S., Cho J., Li M., 2018, Development of a Bayesian belief network model for software reliability quantification of digital protection systems in nuclear power plants, Annals of Nuclear Energy, 120, 62–73

Karoutas Z., Brown J., Atwood A., Hallstadius L., Lahoda E., Ray S., Bradfute J., 2018, The maturing of nuclear fuel: Past to Accident Tolerant Fuel, Progress in Nuclear Energy, 102, 68-78

Kim B.J., Kim J., Kim K., Bae S.W., Moon S-K., 2017, Effects of fuel relocation on reflood in a partially-blocked rod bundle, Nuclear Engineering and Design, 312, 239–247

Kim K.T., 2011, The effect of fuel rod oxidation on PCMI-induced fuel failure, Journal of Nuclear Materials, 418, 249–260

Kim K.T., Jerng D.W., 2011, Oxide thickness-dependent transient cladding hoop stress, Nuclear Engineering and Design, 241, 5055–5063

Krieg R., Schlechtendahl E.G., Scholl K.H., 1977, Design of the HDR experimental program on blowdown loading and dynamic response of PWR-vessel internals, Nuclear Engineering and Design, 43, 2, 419–435

Lee S., Hassan Y.A., Abdulsattar S.S., Vaghetto R., 2014, Experimental study of head loss through an LOCA-generated fibrous debris bed deposited on a sump strainer for Generic Safety Issue 191, Progress in Nuclear Energy, 74, 166-175

Lee S.H., Son K.S., Jung W., Kang H.G., 2017, Risk assessment of safety data link and network communication in digital safety feature control system of nuclear power plant, Annals of Nuclear Energy, 108, 394–405

Leyse R.H., 2007, letter to Ms. Annette L. Vietti Cook, Secretary USNRC, Rulemaking and Adjudications Staff, Public Comment on PRM-50-84: PRM-50-84 and MELLLA+, July 27

Maerani R., Mayaka J.K., Jung J.C., 2018, Software verification process and methodology for the development of FPGA-based engineered safety features system, Nuclear Engineering and Design, 330, 325–331

Mahmoodi R., Zolfaghari A., Minuchehr A., 2019, Simulation of pressure waves propagation following LOCA in piping systems using Laplace Transform Finite Volume, Annals of Nuclear Energy, 124, 164–171

Matthews C., Unal C., Galloway J., Keiser D.D. Jr., Hayes S.L., 2017, Fuel-Cladding Chemical Interaction in U-Pu-Zr Metallic Fuels: A Critical Review, Nuclear Technology, 198, 3, 231-259

Menzel F., Sabundijan G., D'Auria F., 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, 4, 323-338

Pla P., Parisi C., D'Auria F., Galassi G., Galetti R., Ivanov K. N., 2009, Analysis of LB LOCA in PWR through TH-3D NK Coupled Code, Int. Top. Meet. On Nuclear Reactor Thermal Hydraulics (NURETH-13), Kanazawa (J), Sept. 27-Oct. 2

Powell M., Wilcox M., Taylor J., 2016, Analytical Basis for the Use of a Rapidly Deployable Mobile Pump to Recover from and Extended Loss of AC Power with a Failure of the Turbine Driven Auxiliary Feedwater Pump, The 11th Int. Top. Meet. Nuclear Reactor Thermal Hydraulics, Operation and Safety (NUTHOS-11), Gyeongju (Kr), Oct. 9-13, N11P1234

Rivas-Lewicky J., Queral C., Zugazagoitia E., 2016, Thermomechanical Analysis of a LBLOCA Sequence in a PWR-Westinghouse 3 Loop with TRACE5 patch4, The 11th Int. Top. Meet. Nuclear Reactor Thermal Hydraulics, Operation and Safety (NUTHOS-11), Gyeongju (Kr), Oct. 9-13, N11P0295

Roache P.J., 1998, Verification and Validation in Computational Science and Engineering, Hermosa Publishers, Albuquerque (NM, USA)

Robbe M.F., Potapov S., Téphany F., 2003, Simulation of the depressurization occurring at the beginning of a LOCA in a 4-loop PWR, Nuclear Engineering and Design, 224, 33–63

Rozzia D., Del Nevo A., Adorni M., D'Auria F., 2012, Modeling of BWR Inter-Ramp Project experiments by means of TRANSURANUS code, Annals of Nuclear Energy, 50, 238–250

Samal M.K., Sanyal G., Chakravartty J.K., 2011, Investigation of failure behavior of two different types of Zircaloy clad tubes used as nuclear reactor fuel pins, Engineering Failure Analysis, 18, 2042–2053

Sartoris C., Taisne A., Petit M., Barré F., Marchand O., 2010, A consistent approach to assess safety criteria for reactivity initiated accidents, Nuclear Engineering and Design, 240, 57-70

Sawarn T.K., Banerjee S., Pandit K.M., Anantharaman S., 2014, Post Study of clad ballooning and rupture behavior of fuel pins of Indian PHWR under simulated LOCA condition, Nuclear Engineering and Design, 280, 501–510

Sawarn T.K., Banerjee S., Sheelvantra S.S., Singh J.L., Bhasin V., 2017, Study of clad ballooning and rupture behavior of Indian PHWR fuel pins under transient heating condition in steam environment, Nuclear Materials, 495, 332-342

Shim H-S., Baek S.H., Lee D.H., Hur D.H., 2016, Fuel crud deposition under subcooled nucleate boiling in PWR primary coolant using acoustic emission monitoring, 11th Int. Top. Meet. on Nuclear Reactor Thermal Hydraulics, Operation and Safety (NUTHOS-11), Gyeongju (Kr), October 9-13, N11A0433

Stimpson S., Powers J., Clarno K., Pawlowski R., Gardner R., Novascone S., Gamble K., Williamson R., 2018, Pellet-clad mechanical interaction screening using VERA applied to Watts Bar Unit 1, Cycles 1–3 , Nuclear Engineering and Design, 327,172-186

USNRC, 2018, Regulatory Guide 1.222, Measuring Breakaway Oxidation Behavior, Washington (D.C., US), 1-49

USNRC, 2018a, Regulatory Guide 1.223, Determining Post Quench Ductility, Washington (D.C., US), 1-58

USNRC, 2018b, Regulatory Guide 1.224, Preliminary Draft (Draft was issued as DG-1263, dated March 2014), Establishing Analytical Limits for Zirconium-Alloy Cladding Material, Washington (D.C., US), 1-32

Wagih M., Spencer B., Hales J., Shirvan K., 2018, Fuel performance of chromium-coated zirconium alloy and silicon carbide accident tolerant fuel claddings, Annals of Nuclear Energy, 120, 304–318

Wang Q., Chen X., Yi-Chong X., 2013, Accident like the Fukushima unlikely in a country with effective nuclear regulation: Literature review and proposed guidelines Renewable and Sustainable Energy Reviews, 17, 126–146

Wang W., Cammi A., Di Maio F., Lorenzi S., Zio E., 2018, A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants, Reliability Engineering and System Safety, 175, 24–37

Ylonen A., 2008, Large Break Blowdown Test Facility Study, Master Thesis at University of Lappeenranta, Lappeenranta (Fin)