WORLD NUCLEAR ASSOCIATION




Different Interpretations of Regulatory Requirements

Cooperation in Reactor Design Evaluation and Licensing – Licensing & Permitting Task Force

Title: Different Interpretations of Regulatory Requirements
Produced by: World Nuclear Association
Published: December 2021
Report No. 2021/004

Cover images clockwise from top left:
AP1000, Haiyang (photo courtesy Shandong Nuclear Power Company, Ltd)
ABWR, Shimane 3 (photo courtesy Chugoku Electric power Company Co, Inc)
EPR, Flamanville 3 (photo courtesy EDF)
VVER-1200, Ostrovets (photo courtesy Rosatom)

This report reflects the views of industry experts but does not necessarily represent those of any of the World Nuclear Association's individual member organizations.

World Nuclear Association is the international organization that represents the global nuclear industry. Its mission is to promote a wider understanding of nuclear energy among key international influencers by producing authoritative information, developing common industry positions, and contributing to the energy debate.

The Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group of the World Nuclear Association was created in January 2007 with the mission of establishing international standardization of individual reactor designs and harmonization of approaches to licensing. CORDEL is currently working with its six task forces covering a wide range of technical areas, while maintaining close cooperation with the OECD Nuclear Energy Agency, the International Atomic Energy Agency, and standards developing organizations (SDOs), in pursuit of the CORDEL goals.

Technical Author & Coordinator

Allan Carson, World Nuclear Association

Contributors

Claude Mayoral, Edvance
Igor Mischenko, Rosatom
Helena Perry, Westinghouse
Takao Kurihara, Hitachi-GE
Hidehiro Segawa, Hitachi-GE

Reviewers

Robert Ion, Terrestrial Energy
Tania Veneau, EDF
William Ranval, ENISS
Michelle Catts, GE
Byung-Chan Na, World Nuclear Association

Foreword

In January 2007 the World Nuclear Association established the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors, and licensees) and nuclear regulators (national and international organizations) on the benefits and means of achieving a worldwide convergence of reactor safety standards and approaches to licensing for reactor designs.

The Licensing & Permitting Task Force (LPTF) was set up jointly by the Law and CORDEL Working Groups in 2011, with the objective to highlight challenges with current licensing practices and benchmark leading approaches with a view to promoting innovation and more efficient licensing processes.

CORDEL and the LPTF since their inception have closely observed the ability of reactor vendors to export their reactor designs for development in other countries. During this time many projects to build a nuclear power plant outside of the reactor vendor's country of origin have experienced delays and/or cost overruns associated with responding to local regulatory requirements and expectations.

Some of the challenges and decisions required in developing a nuclear reactor in a host country are discussed in an earlier CORDEL LPTF report, *Licensing and Project Development of New Nuclear Plants*.

This report focuses on the specific challenges to new nuclear plant projects posed by the interpretations of fundamental safety objectives and requirements by different national regulators, the consequences this has in relation to design standardization, and ultimately the impacts on project development.

Abbreviations and Acronyms

ALARA	As low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME BPVC	American Society of Mechanical Engineers Boiler & Pressure Vessel Code
CCF	Common cause failure
CNRA	Committee on Nuclear Regulatory Activities
CORDEL	Cooperation in Reactor Design Evaluation and Licensing
CSNI	Committee on the Safety of Nuclear Installations
DAS	Diverse actuation system
DBA	Design basis accident
DEC	Design extension condition
DICTF	Digital Instrumentation & Control Task Force
DiD	Defence-in-depth
ENISS	European Nuclear Installations Safety Standards Initiative
ENSREG	European Nuclear Safety Regulators Group
EUR	European Utility Requirements
FOAK	First-of-a-kind
GDA	Generic design assessment
HEPA	High-efficiency particulate absorbing
HVAC	Heating, ventilation and air conditioning
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INSAG	International Nuclear Safety Group
JEAG	Japan Electric Association Guide
LPTF	Licensing & Permitting Task Force
LWR	Light water reactor
MCSTF	Mechanical Codes and Standards Task Force
MCR	Main control room
MDEP	Multinational Design Evaluation Programme
NEA	Nuclear Energy Agency
NOAK	N^{th}-of-a-kind
OECD	Organisation for Economic Co-operation and Development
ONR	UK Office for Nuclear Regulation
OSART	Operational Safety Review Team
NRC	US Nuclear Regulatory Commission
PWR	Pressurized water reactor
QA	Quality assurance
RCC-M	French Design and Construction Rules for the Mechanical Components of PWR Nuclear Islands (Règles de Conception et de Construction des Matériels Mécaniques des Ilots Nucléaires REP)

RCS	Reactor control system
RHR	Residual heat removal
RHWG	Reactor Harmonization Working Group
SAPs	Safety assessment principles
SAS	Safety automation system - EPR
SDO	Standards developing organization
SMR	Small modular reactor
SMRTF	Small Modular Reactors Task Force
SRL	Safety Reference Levels
SQEP	Suitably qualified and experienced person
SSCs	Structures, systems and components
SSLC	Safety system logic and control system
TAG	Technical Assessment Guide
WENRA	Western European Nuclear Regulators Association
WGRR	Working Group on Research Reactors
WGWD	Working Group on Waste and Decommissioning

Contents

List of tables

Executive Summary

All countries with a civilian nuclear programme apply the same fundamental nuclear safety standards. However, the incorporation of these standards into specific national regulatory standards and guidance continues to result in significant differences in the designs of reactors deployed across national borders.

These differences in design solutions are often the result of differences between the way in which national regulators identify fault scenarios and acceptance criteria, which ultimately define the design provisions.

The differences between the acceptance criteria amongst national regulators can be difficult to discern as they are not always part of the written requirements but may result from the deliberation of a group of individuals or be strongly influenced by the interpretations of specific inspectors/assessors. This variability creates risks that present major barriers for new build projects.

These discrepancies between national regulatory requirements can be minimized through reactor design standardization and harmonization of regulatory approaches. This would result in a common understanding of the safety evaluation, concepts, and requirements, which in turn would minimize the design changes and licensing complexity when moving across national borders.

In addition to the differences in acceptance criteria, the method of demonstrating a safety case can vary widely among national regulators (*e.g.* prescriptive versus non-prescriptive regulatory approaches). When a reactor vendor wishes to license its design in a country with a different regulatory framework, the form of the regulations and guidance can lead to a complete reframing of the original safety case and ultimately a significant amount of effort from the reactor vendor to produce new documentation that was not required by other national regulators.

If the same fundamental safety requirements are applied by all countries, it might be expected that licensing a reactor design under a non-prescriptive regulatory regime would result in only minor changes. However, there are a number of examples of extensive design changes that were requested by non-prescriptive regulators because of different interpretations or applications of safety requirements. It is therefore possible that significant design changes may be required by any national regulator, regardless of how prescriptive the regulatory approach is.

There are multiple examples, across various reactor designs and countries, in which different interpretations or applications of fundamental safety requirements either have resulted in or had the potential to result in design changes, with no clear impact on overall safety of the nuclear power plant.

These changes can turn what should be an n^{th}-of-a-kind (NOAK) project into another first-of-a-kind (FOAK), incurring some of the risks and costs associated with new projects.

Building upon the lessons from the regulatory approach to previous reactor generations, to support wider deployment of emerging technologies, to improve the standardization of reactor designs and to achieve harmonization of regulatory approaches, national regulators and the nuclear industry should cooperate to:

- Understand the differences in regulatory approaches and assess the impact on reactor designs, thereby understanding the level of regulatory readiness

for a given design and allowing the proposal of broader design solutions that are aligned to a wider range of regulatory requirements.

- Further develop common terminology used in the documentation of the International Atomic Energy Agency, European Nuclear Installations Safety Standards, CORDEL, and others, and develop guidance on how they should be applied to all reactor types.
- Develop and support a suitable framework to undertake joint regulatory design and safety reviews, share technical reviews, establish common position statements on safety requirements, and identify other areas for collaboration.
- Expand upon the areas identified in this report (defence-in-depth, postulated initiating events, design basis accidents and design extension conditions, internal and external hazards, and instrumentation and control) to define the key safety requirements to focus on in joint regulatory reviews, and develop guidance on how these should be implemented within reactor designs.

To fulfil these recommendations, governments, regulators, and the nuclear industry will need to increase collaborative efforts at an international level to develop an approach and framework that can be applied to future regulatory review efforts.

The urgency to deploy new nuclear units around the world to help meet decarbonization goals makes the need for a harmonized approach to regulatory requirements greater today than ever.

The World Nuclear Association report on *Harmonization of Reactor Design Evaluation and Licensing: Lessons Learned from Transport* proposes a new international framework for nuclear regulation. Through this framework, regulators could undertake joint assessments, validate other regulatory assessments where appropriate, develop bounding envelopes for assessment outputs and/or develop equivalence methodologies for the safety requirements.

Such an international framework to facilitate streamlining of regulatory approaches, could minimize the design changes required when licensing in new countries, reduce the project development risks, and thus facilitate the wide scale deployment of emerging reactor designs.

1 Introduction

Nuclear safety fundamental objectives have been well-harmonized between countries and national regulators through cooperation at an international level and the creation of standards such as the International Atomic Energy Agency (IAEA) *Safety Standards* series, and the Western European Nuclear Regulators Association (WENRA) safety reference levels for existing reactors or safety objectives for new power reactors.

Despite these standards and reference levels being applied in countries around the world, their application and interpretation by specific national regulatory standards and guidance can result in significant differences between the same reactor design deployed in different countries.

The design changes required between countries can be significant, leading to increased workload for reactor designers and regulators, with ultimately unpredictable timescales and cost for licensing activities.

This uncertainty creates risks that present major barriers for new build projects. Reactor design standardization and the harmonization of regulatory approaches to support a common understanding of the safety evaluation, safety concepts and requirements are essential for minimizing design changes and licensing costs when moving across national borders.

This report analyses several fundamental safety requirements, outlining examples across various reactor designs and countries where different interpretations or applications of these requirements either resulted, or had the potential to result, in design changes, without achieving an obvious improvement in the overall safety of the nuclear power plant.

These changes in design can turn what should be an n^{th}-of-a-kind (NOAK) project into another first-of-a-kind (FOAK) project, incurring the major risks and costs associated with FOAK projects. This report explores the lessons that can be learned from these examples, while also examining the potential implications these design changes could have for the future deployment of new reactors.

2 Approach

The Licensing & Permitting Task Force of World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group analysed the experiences of four of its members (EDF, Hitachi-GE, Rosatom, and Westinghouse Electric Company) in which they had experienced different regulatory interpretations or applications of regulatory requirements that led to significant changes to a reactor design or delays to licensing activities. The reactor designs for which examples were provided are as follows:

- EPR (EDF / Framatome).
- ABWR (Hitachi-GE).
- VVER-1200 (Rosatom).
- AP1000 (Westinghouse Electric Company).

The examples provided were then categorized according to the relevant regulatory requirements or safety design principles, as defined in *IAEA Safety Standards – Safety of Nuclear Power Plants: Design* [1]. The requirements and principles identified were as follows:

- Defence-in-depth (DiD).
- Identification, application and evaluation of design basis accidents (DBAs) and design extension conditions (DECs).
- Application of codes and standards.
- Common cause failure (CCF).
- Safety classification.
- Human factors.
- Heating, ventilation and air conditioning (HVAC) requirements.
- Location of items important to safety in relation to internal and external hazards.

The examples compare the approaches of the national regulators that have undertaken licensing reviews for each reactor type. This is generally limited to two national regulatory approaches for each example, the country-of-origin regulator and at least one host country regulator.

These are not an exhaustive list of all differences in regulatory approach experienced by that reactor design. Each example provided is described in terms of its impact on one reactor design; however, where the national regulator associated with a specific example has undertaken licensing for any of the other reactor designs discussed in the report, those other designs are likely to have experienced the same or similar challenges.

It is worth noting that all the reactor designs covered in this report are light water reactor (LWR) technology. The impact on future reactor designs and implications for licensing is based on best available information of potential future designs and the views of the CORDEL Small Modular Reactors Task Force (SMRTF) members.

3 International Safety Frameworks and Harmonization

There are a number of international organizations that provide guidance for nuclear safety considerations or are actively engaged with CORDEL in harmonization of nuclear safety requirements. These range from: international organizations such as the International Atomic Energy Agency (IAEA) and its International Nuclear Safety Group (INSAG), and the Nuclear Energy Agency (NEA) of the Organisation for Economic Co-operation and Development (OECD); regulatory bodies such as the Multinational Design Evaluation Programme (MDEP), European Nuclear Safety Regulators Group (ENSREG) and the Western European Nuclear Regulators Association (WENRA); and industry bodies such the European Utilities Requirements (EUR) association.

3.1 CORDEL

The mission of World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group is to promote the standardization of nuclear reactor designs and harmonization of regulatory approaches.

To meet its objectives, CORDEL addresses broad industrial perspectives in design and licensing issues, analyzing and developing recommendations on specific elements of licensing requirements and international standards, both regulatory and industrial, that could be harmonized, or accepted as being equivalent in terms of meeting standards.

CORDEL currently undertakes this work through several task forces which are focused on specific areas, namely:

- Design change management.
- Digital instrumentation & control.
- Licensing and permitting.
- Mechanical codes and standards.
- Nuclear safety standards.
- Small modular reactors.

Each task force has its own remit and publishes industry reports on specific areas that support the development of a worldwide nuclear regulatory environment, where internationally accepted standardized reactor designs, certified, and approved by a recognized competent authority in the country of origin, can be widely deployed without major design changes due to national regulations.

The following reports produced by CORDEL task forces provide reference material:

- Licensing and Project Development of New Nuclear Plants, Licensing & Permitting Task Force [2].
- Design Maturity and Regulatory Expectations for Small Modular Reactors, Small Modular Reactors and Licensing & Permitting Task Forces [3].
- Making Use of the Reference Plant Concept for Licensing New Nuclear Units, Licensing & Permitting Task Force [4].
- Defence-in-Depth and Diversity: Challenges Related to I&C Architecture, Digital I&C Task Force [5].
- Harmonization of Reactor Design Evaluation and Licensing: Lessons Learned from Transport, CORDEL [6].

3.2 IAEA

All countries generally adhere to the International Atomic Energy Agency (IAEA) Safety Standards when

developing or revising their national requirements and guidance. These form a baseline for member states in considering their own requirements and are also used by the IAEA in its own activities. For example, IAEA Operational Safety Review Teams utilize these standards when carrying out safety reviews of operating plants.

The IAEA Safety Standards consist of three sets of publications: the Safety Fundamentals, the Safety Requirements and the Safety Guides.

The Safety Fundamentals [7] provide the fundamental safety objectives alongside ten safety principles. The Safety Requirements establish more specific requirements that must be met to ensure the protection of people and the environment, while recommendations and guidance on how to comply with the safety requirements are provided in the Safety Guides, which are considered to be good international practice to help users achieve high levels of safety.

3.3 INSAG

The International Nuclear Safety Group (INSAG) is an advisory group of experts, convened under the auspices of the IAEA, with the objective to provide authoritative advice and guidance on nuclear safety approaches, policies and principles. In particular, INSAG provides recommendations and opinions on current and emerging nuclear safety issues to the IAEA, the nuclear community and the public.

INSAG has authored a report on Basic Safety Principles for Nuclear Power Plants [8] which describes:

- Safety objectives (general nuclear safety objectives, radiation protection objectives, and technical safety objectives).
- Safety principles (fundamental safety management principles, fundamental defence-in-depth (DiD) principles, and general technical principles).

The objectives define what is to be achieved and the principles state how the objectives could be met.

A further INSAG report is INSAG-10, Defence-in-Depth (DiD) in Nuclear Safety [9], which outlines the approach of DiD (historical definition and evolution of the concept, its objectives and strategy) and its implementation for existing reactors and new power plants.

3.4 ENSREG

The European Nuclear Safety Regulators Group (ENSREG) is an independent, expert advisory group created in 2007 following a decision of the European Commission. It is composed of senior officials from the national nuclear safety, radioactive waste safety or radiation protection regulatory authorities and senior civil servants with competence in these fields from all Member States in the European Union and representatives of the European Commission.

ENSREG's role is to help to establish the conditions for continuous improvement and to reach a common understanding in these areas. ENSREG is working to:

- improve the cooperation and openness between Member States on nuclear safety and radioactive waste issues;
- improve the overall transparency on nuclear safety and radioactive waste issues; and
- as appropriate, advise the European Commission on additional European rules in the fields of the safety of nuclear installations and the safety of the

management of spent fuel and radioactive waste.

ENSREG initially established four working groups (WGs) to undertake its work programme:

1. Nuclear Safety
2. Waste management and decommissioning
3. Transparency arrangements
4. International Cooperation

In order to enhance the coordination of international cooperation, the Working Group 4 was merged in 2016 within Working Group 1, on nuclear safety, as a Task Group. This task group is currently mainly in charge of providing advice on the management of the Instrument for Nuclear Safety Cooperation (INSC).

3.5 WENRA

The Western European Nuclear Regulators Association (WENRA) is an association bringing together the heads of regulators for nuclear safety within Europe to develop a common approach to nuclear safety. The WENRA Reactor Harmonization Working Group (RHWG) issued a report on safety reference levels (SRLs) for existing reactors in January 2006, which was revised several times (January 2007, January 2008, September 2014) until the latest revision in February 2021 [10]. These SRLs reflect expected practices to be implemented in the WENRA countries with members being committed to improve and harmonize their national regulatory systems by implementing these SRLs.

3.6 MDEP

The Multinational Design Evaluation Programme (MDEP) was established in 2006 as a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities that are currently or will be tasked with the review of new nuclear power reactor designs. The nuclear regulatory authorities of 15 countries participated in MDEP, which included five design-specific working groups and one issue-specific working group.

MDEP activities were conducted across three levels: steering committee, design-specific, and issue-specific. The key accomplishments are:

- Steering committee
  - Common position addressing first-plant-only-tests – CP-STC-01.
  - Common position addressing the Fukushima Daiichi nuclear power accident – CP-STC-02.
  - Position papers on safety goals and their application [11].
- Design-specific
  - 14 common positions and numerous technical reports.
  - Increased cooperation in design evaluations.
  - Increased communications.
  - Greater quality of national safety assessments.
  - Greater harmonization of regulatory reviews.
- Issue-specific
  - 17 common positions and numerous technical reports.
  - Vendor inspection, codes & standards, digital I&C[1].
  - Greater harmonization of regulatory practices.
  - Effective engagement with industry stakeholders.

Following 10 years of cooperation under MDEP, some of these activities have been moved to the Committee on Nuclear Regulatory Activities (CNRA), see § 3.6 for further details.

[1] MDEP's Codes & Standards Working Group and Digital I&C Working Group were transferred to the NEA Committee on Nuclear Regulatory Activities (CNRA) in 2017.

3.7 OECD-NEA

The Nuclear Energy Agency (NEA) operates within the framework of the OECD. Specific areas of competence of the NEA include safety and regulation of nuclear activities, through two specific committees, the Committee on the Safety of Nuclear Installations (CSNI) and the Committee on Nuclear Regulatory Activities (CNRA).

The CSNI develops and coordinates the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. It delivers state-of-the-art reports, technical opinion papers and best practice guidelines providing licensees and regulators with approaches that are generally the result of an international consensus under a collaborative research framework. It also offers a framework for facilitating cooperative projects especially in experimental activities.

The CNRA is a forum for the exchange of information and experience among regulatory organizations. It is responsible for the programme of the NEA concerning the regulation, licensing and inspection of nuclear installations with regard to safety. The CNRA's main tasks are to review developments which could affect regulatory requirements in order to provide members with an understanding of the motivation for new regulatory requirements under consideration, and an opportunity to offer suggestions that might improve them or avoid disparities among member countries.

Two of the working groups currently operating within CNRA are the Codes and Standards Working Group and the Digital I&C Working Group. There is active collaboration between these working groups and their respective counterparts ***i.e.***, Mechanical Codes and Standards Task Force, and the Digital I&C Task Force, within CORDEL.

3.8 EUR Organisation

The EUR Organisation was formed in 1991 by five major European electricity producers to develop common specifications for new designs to be proposed by reactor vendors in Europe and to promote harmonization of requirements across Europe and worldwide. Nowadays the EUR Organisation comprises 13 utilities which represent the major European electricity producers. The European utilities involved in the EUR Organisation aim at harmonizing and stabilizing the conditions in which new LWRs will be designed, built, commissioned, operated and maintained[2].

The main product developed, and regularly updated by the EUR Organisation is the European Utility Requirements for LWR Nuclear Power Plants (EUR), presented in the EUR Document [12].

The purpose of the EUR Document is to present a clear, complete statement of utility expectations for Generation III nuclear power plants. The EUR Document consists of comprehensive specifications in three volumes (Volumes 1, 2&4). It promotes the development of standard designs that can be built and licensed in several European countries with only minor variations. The current version of the EUR Document applies to both pressurized water reactors and boiling water reactors; only mid- and large size LWR plants are dealt with. Work is in progress to include requirements for small modular light water reactors, including a set of key positions published as chapter 1.5 in Volume 1 in June 2021.

[2] EPRI have also produced a utility requirements document with similar aims to that of the EUR organization.

Reactor vendors can apply for an assessment of one of their designs against the current revision of the EUR Document. The result of each specific design assessment is contained in a dedicated subset of Volume 3 of the EUR Document.

3.9 ENISS

ENISS is the European Nuclear Installations Safety Standards Initiative. Established in 2005, it represents nuclear installation licence holders from 16 European countries with nuclear power units, fuel reprocessing plants or large waste storage facilities. ENISS provides the nuclear industry with a platform to exchange information on national and European regulatory activities, to express its views and provide expert input on all aspects related to international safety standards. ENISS is the common channel through which European nuclear licence holders interact with WENRA (nuclear regulators), the European Institutions and the International Atomic Energy Agency (IAEA).

ENISS covers the following technical scope: nuclear safety and associated regulations during the whole lifecycle of nuclear installations, including radiation protection and security, for long term operation, new build, waste management and decommissioning.

4 Examples of Different Interpretations of Regulatory Requirements

This section outlines a number of examples from licensing activities of large Generation III LWR designs. Although the fundamental requirements produced by the IAEA are accepted by national regulators, the examples show that the way in which these requirements are applied can vary significantly, which can affect the nuclear power plant design, licensing process and schedule, supply chain, construction schedule, and cost of the project development.

It should be noted that nuclear regulations first started as national regulations and guidance from a small number of national regulators that did not have an overall objective of convergence or compatibility. International standards and guidance were subsequently developed so that safety standards could be consistently applied across nations.

The examples are described in terms of the main fundamental design safety requirement, as defined by the IAEA's *Safety of Nuclear Power Plants: Design* [1]. In many cases the IAEA, or others, provides specific guides related to the design or safety features being discussed. These guides, while providing a greater level of detail and items for consideration, are often at too high a level to lead to the same practice or the same detailed design and do not eliminate different possible interpretations.

The first few examples described below are focused on challenges related to I&C systems, while later examples focus on other areas such as mechanical and electrical systems. The examples provided do not reflect the full breadth and depth of the challenges observed within each of the described safety requirements and are provided here to illustrate the range of safety requirements that the different interpretation national regulators can impact.

4.1 Approach to defence-in-depth

Nuclear safety requirements were developed using deterministic approaches with a defence-in-depth (DiD) philosophy at their foundation. Different approaches have been used in different countries, with some using more risk-informed approaches than others, but in all cases, DiD philosophy is centred on several levels of protection including successive barriers and conservative considerations to prevent the release of radioactive material to the environment [11].

Some guidance on the approach to DiD for LWRs has been produced, notably by the IAEA in *Defence in Depth in Nuclear Safety* [9].

It is fundamental to the DiD approach that the lines of defence be independent as far as reasonably possible; therefore, the deterministic engineering and safety concepts of redundancy, diversity, and segregation must be applied during development of the design.

This DiD approach has been applied to the design of all Generation III nuclear reactors that have been licensed and built. Despite this, different national regulatory approaches and interpretations of how to implement the approach continue to exist.

One area in which these different approaches to DiD are evident is in the differences observed between the generic western European approach and that applied within Russia, which, while being broadly similar, varies in two distinct areas, as shown in Table 1.

Table 1. DID approaches in western Europe and Russia

		Did Level 1	DiD Level 2	DiD Level 3		DiD Level 4	DiD Level 5
				Level 3a	Level 3b		
Western European Approach (as described by WENRA)	Associated Plant Conditions	Normal operation, with plant conditions remaining within normal operating limits	Anticipated operational occurrences (AOOs) with plant conditions remaining within reactor trip limits	Postulated single initiating events Purpose: control of design basis accidents	Postulated multiple failure events Purpose: control of design extension conditions to prevent core melt (corresponds to level 4a according to the IAEA)	Postulated core melt accidents (short- and long-term) It corresponds to level 4b according to IAEA	
	Objective	Prevention of abnormal operation and failures	Prevention of abnormal operation and failures to avoid exceeding reactor trip limits	Control of events to limit radiological releases and prevent escalation to core melt conditions		Control of accidents that result in core melt, to limit offsite releases	Mitigation of radiological consequences of significant releases of radioactive material
Russian Approach	Associated Plant Conditions	Normal operation, with plant conditions remaining within normal operating limits	Anticipated operational occurrences (AOOs) with plant conditions remaining within reactor trip limits	Design basis accidents		Accidents with core melt	
	Objective	Prevention of abnormal operation and failures	Prevention of abnormal operation and failures to avoid exceeding reactor trip limits	Prevention of beyond design basis accidents by safety systems: prevention of the escalation of initial events into design basis accidents, and design basis accidents into beyond design basis accidents with the use of safety systems; and mitigation of the consequences of accidents that could not be prevented, by maintaining the releases in a limited area		Management of beyond design basis accidents: return of the plant to a controlled state, at which the fission chain reaction stops, the fuel is constantly cooled and radioactive substances are kept within the established limits; prevention of the development of beyond design basis accidents and mitigation of their consequences, including with the use of special technical means to manage beyond design basis accidents.	Emergency planning: preparation and implementation of action plans for the protection of personnel and the public
Conclusion		No difference	No difference	Difference		No difference	Difference

The key difference in the approach to the DiD is the presence of two sublevels (3a, 3b) within the European approach, with a common aim in both approaches to control the events to limit radioactive releases and prevent an escalation to core melt conditions.

VVERs are currently being deployed in seven countries outside of Russia (China, Finland, Hungary, India, Turkey, Bangladesh & Egypt). Of these seven projects, two are required to be adapted to the specific requirements of the national regulators[3]: Hungary (Paks II) and Finland (Hanhikivi). The national regulatory approach in Hungary and Finland[4] to the application of DiD is aligned with that of the western European approach. As a result, VVER projects in Hungary and Finland have been required to add additional diverse I&C protection systems at the 3b DiD level, whereas the Belarus nuclear plant does not have an additional diverse protection system at DiD level 3, since the main protection is implemented on different platforms, by different equipment manufacturers providing internal diversity.

Since 2016, new plant designs in Russia have been implementing a diverse I&C protection system at DiD level 3, which is bringing the approach closer to that expected by western European regulators; however differences in how the diversity is to be implemented remain between national regulators.

Whether national regulators have different approaches to DiD or apply different standards to the application of DiD, it can result in the reactor vendor having to change overall systems and adjust the basic design of systems, *e.g.* redistribution of the I&C systems design, to account for the national regulatory requirements that divide the DiD level 3 into levels 3a and 3b. In such circumstances there are also necessary changes associated with the different categorization of the safety functions and/or the different classifications of systems, which have knock-on effects on system and plant layout as well as on operations and maintenance procedures.

This rework requires significant design and licensing efforts that will ultimately increase the uncertainty of the cost and schedule of the licensing timescales and subsequently the overall project. There may also be a requirement to purchase additional equipment that will then further increase capital expenditure.

Alternatives to full design change may also be possible depending upon the regulatory framework. When utilizing such alternatives, the main challenge is then in respect to the project timeline because successfully agreeing these alternative approaches normally takes a long time, with uncertain outcomes and slow project risk reduction.

4.2 Identification, application and evaluation of design basis accidents and design extension conditions

Requirements 19 and 20 of *Safety of Nuclear Power Plants: Design* [1] address design basis accidents (DBAs) and design extension conditions (DECs), respectively:

- DBA – a set of accidents shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand.

[3] The other five are being designed in accordance with the safety requirements in Russia in agreement with the country of deployment.

[4] Stuk's YVL Guide B.1 §4.3 defines DEC-A differently from WENRA (DiD level 3b) and the IAEA (DiD level 4a), sub-dividing it into:

- DEC-A (AOO and accidents until DBC-3 involving an additional common cause failure in a system required to execute a safety function).
- DEC-B (combination of multiple failure events selected as significant on the basis of a probabilistic risk assessment).
- DEC-C (relative to rare external events, which the facility is required to withstand without severe fuel failure).

- DEC – a set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand accidents that are either more severe than design basis accidents or that involve additional failures.

These requirements are supplemented further by the IAEA safety standards on *Deterministic Safety Analysis for Nuclear Power Plants* [13], which states:

> *The conservative analysis of anticipated operational occurrences and design basis accidents should demonstrate that the safety systems alone in the short term, along with operator actions in the long term, are capable of achieving a safe state.*

The approaches for the deterministic analyses differ between DBA and DEC events:

- For DBA events, the design and the analysis are covered by considering conservative bounding cases.
- For the selection of representative cases for DEC analyses, the aim is to demonstrate that core melt can be prevented with an adequate level of confidence and that there is a sufficient margin to avoid any cliff edge effects. Using a more realistic approach for DEC events, as opposed to the conservative approach for DBA, aims to identify reasonably practicable provisions for the prevention of such accidents or mitigation of their consequences (radioactive releases should be minimized as far as reasonably achievable).

These differences in approach generally relate to the less frequent occurrence of DEC scenarios which take into account complex situations (including common cause failure). It is therefore necessary to analyse these scenarios differently as a very demanding enveloping scenario for the DEC analysis, or a very low radiological target for mitigative measures, might lead to the conclusion that no reasonably practicable measures can be identified.

While these same requirements exist at the international level, some differences remain through the national regulatory frameworks, particularly in the areas of defining postulated initiating events and the undertaking of deterministic and probabilistic assessments (including the contribution of engineering judgement and experience feedback).

One such example of these differences shows up in the design of the I&C systems of various EPR projects. The I&C architecture of all EPR projects is different to that developed within France.

On all EPR projects there are two I&C digital platforms: safety I&C platform (including the back-up I&C protection system); and operational I&C platform.

In the identification of the DEC resulting from Category 2 design basis conditions (DBCs)[5] and the loss of the protection system, through the original design in France it was possible to credit the availability of the safety automation system (SAS)[6] within the operational I&C platform to satisfy the safety requirement. However, in Finland and the UK the national regulators determined that it was not possible to credit the availability of the SAS to satisfy this DEC case and a 'non-computerized safety system' or 'hardwired back-up system' would have to be implemented.

[5] Generally there are four categories of design basis condition: DBC-1: normal operation; DBC-2: anticipated operating occurrences; DBC-3: design basis condition category 3 (may occur once during the lifetime of fleet of operating plants); and DBC-4: design basis condition category 4 (not expected to occur).

[6] Safety automation system (SAS): system specifically designed and validated to meet intermediate safety classification level requirements (CEI 62138 and French Fundamental Safety Rule II.4.1.a).

While the different national regulatory reviews result in changes to the ways in which the requirements should be satisfied by the design, these different outcomes are often driven by the way in which national regulators identify fault scenarios and conditions.

One such difference in approach can be observed by reviewing the national regulatory approaches of France, Finland, China and the UK in terms of how they are applied to the respective EPR projects. For all EPR projects in France, Finland and China, identification of DBC and DEC sequences follow a similar approach, *i.e.*:

- DBCs of Categories 2-4 are based on single initiating events and conservative assumptions such as single failure criterion, consideration of preventative maintenance, and stringent analysis rules. This leads to design provisions that are intended to limit the effects of the selected events according to the DBC criteria.
- DECs covering notable DBCs with additional failures selected on a deterministic and probabilistic basis. The unavailability of safety features due to maintenance is not systematically applied.

The approach in the UK is more complicated and derived from the ONR's *Safety Assessment Principles for Nuclear Facilities* [14], which states that the following do not need to be included in the initiating faults list:

- Faults in the facility that have an initiating frequency lower than about 1 x 10^{-5} per year.
- Failures of structures, systems or components for which appropriate specific arguments for preventing the initiating fault have been made.
- Natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10,000 years.
- Those faults leading to unmitigated consequences which do not exceed the basis safety level for the respective initiating fault frequency in numerical target 4.[7]

This is further supplemented by the ONR *Design Basis Analysis* technical assessment guide [15], which contains the following guidance:

- *Fault sequence: a combination of an initiating fault and any additional failures, faults and internal or external hazards which have the potential to lead to an accident.*
- *A DBA[8] is the sequence considered in the (conservative) design basis analysis. It can bound several similar initiating faults with a range of severities.*
- *Single initiators of anticipated operational occurrences (AOOs) and design basis accidents are covered to include multiple failure events as part of Level 3 defence-in-depth:*
  - *AOOs and a postulated common cause failure (CCF) of redundant trains of a safety system.*
  - *Single postulated initiating evens and a postulated CCF of redundant trains of a safety system.*
  - *Complex or specific scenarios including CCF of safety systems or safety-related systems needed to fulfil the fundamental safety functions in normal operation.*
- *It may also be possible to exclude some fault sequences from design basis analysis on the basis of frequency… [However, this] should be treated with caution. It is difficult to substantiate the necessary levels of reliability and resilience to CCF expected in a safety case for faults with significant consequences without design basis analysis techniques and expectations…*
- *The tolerance of the facility to a fault sequence made up of the*

[7] Numerical Target 4 is the on- and offsite dose targets set by the basis safety level for differing frequencies of events. These can be found in §727 of *Safety Assessment Principles for Nuclear Facilities* [14].

[8] The ONR technical assessment guide describes a 'design basis accident' as a 'design basis fault sequence'.

identified initiating event and the failure of a safety measure should be demonstrated through design basis analysis…

- *A second fault sequence should also be identified with diverse and independent safety measures for delivering the necessary safety functions. These secondary means still need to be reliable and robust to meet the expectations of design basis analysis, but they do not necessarily need to be designed with the same levels of redundancy and single failure tolerance as the principal means identified for delivering the required safety functions. As a result, the second means could be Class 2 SSCs, from which appropriately graded design and reliability requirements follow.*

This ultimately means that the UK regulators expect DBAs and DECs to be developed utilizing the concepts of reliability and lines of defence, and therefore a DBA should be based on the event occurrence probability, independent of its nature (single or multiple initiating event).

This difference means that during safety case development in the UK some multiple initiating events must be analyzed with the more stringent DBA rules, whereas they are assessed under DEC rules within other countries. This can lead to changes in the safety classification of structures, systems and components (SSCs) that can have far-reaching impacts through the design, licensing, procurement and construction of those SSCs.

For example, as a result of having to assess some multiple initiating events with DBC rules in the UK, the EPR heating, ventilation and air conditioning (HVAC) system was required to implement additional safety-related HVAC chillers, which has led to the upgrade of two previously non-classified preventative maintenance HVAC trains to safety classified systems, implying changes in the design documentation, and the codes and standards to be applied to the design, manufacture and test requirements for the equipment, as well as delays in the licensing process.

There can also be differences in the approaches to the assessment of DBAs and DECs between national regulators, which can lead to very different transient evolutions for the same initiating event and the same reactor design. This makes it difficult to translate analysis results and consequences between projects in different countries.

For example, on the EPR project at Flamanville 3, the approach to evaluating Category 2 DBCs (anticipated operational occurrences) is to only credit safety grade systems (with some exceptions). However, the practice in Finland for the Olkiluoto 3 project allows more realistic operational and physical limitations of equipment and systems to be credited.

4.3 Application of codes and standards

Requirement 18 of *Safety of Nuclear Power Plants: Design* states: "The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards" [1].

Different national codes and standards have been applied to the design of nuclear power plants around the world, for example the American Society of Mechanical Engineers (ASME) Boiler & Pressure Vessel Code (BPVC) in the USA, and the Design and Construction Rules for the Mechanical Components of PWR Nuclear Islands (RCC-M) in France. Additional examples of differences in the use of national standards are described in the Mechanical Codes and Standards Task Force (MCSTF) report *Comparison of Fatigue Life Analysis Methods – Comparison of Pressure Vessel Fatigue Codified Design Rules Based on S-N Approach* [16], which compares the different standards used in reactor pressure vessel design.

National regulators can prefer the use of one set of codes and standards over another for multiple reasons. It could be that they are the standards which have traditionally been developed and used within that regulator's country and therefore they are familiar and confident with their application. Alternatively, it could be that the regulators have recognized that one set of codes and standards are more compatible with their requirements. In some cases, this preference can mean that the codes and standards are an integral part of the nuclear safety requirements, whereas in other cases the preference is less obvious in the written requirements.

It is not a case of one standard being better than another; however, when different regulators prefer the use of different standards it has the potential to result in a lot of work to demonstrate compliance with the regulators' preferred standards as opposed to what the plant was originally designed against.

Codes and standards usually overlap, but also have some key differences which can be subtle and not obvious. For example, RCC-M requires qualification of welding and fabrication workshops, whereas such a requirement is not mentioned in ASME. Such a difference means that if a regulator were to prefer the strict use of RCC-M but the original design

and supply chain was based on ASME, then the suppliers would need to be qualified against the RCC-M requirements in order to use the same supply chain in the host country.

A good example of this was during the UK generic design assessment (GDA) of the AP1000 I&C system. The original plant was designed in accordance with Institute of Electrical and Electronics Engineers (IEEE) standards leading to a two-tier classification system, *i.e.* safety-related and non-safety related; however the preference in the UK is a four-tier classification system as presented by the International Electrotechnical Commission (IEC). This led to the UK regulator raising a number of GDA issues, such as:

- GI-AP1000-CI-08: "A number of areas for improvement including to: the [UK regulator's] safety assessment principles (SAPs) and IEC standards conformance demonstration; and justification of the scope and adequacy of the independent confidence building measures." [17].
- GI-AP1000-CI-09: "A number of key areas for improvement, namely: demonstration that the development process is compliant or equivalent to IEC standards; and identification of the evidence to support the demonstration." [18].

Along with further regulatory findings [19] such as:

- AF-AP1000-CI-002: "The licensee shall put in place an overarching quality assurance programme for the AP1000 I&C systems important to safety development consistent with the Westinghouse quality management system that either: adopts appropriate IEC nuclear sector standards; or uses standards that are demonstrated to be equivalent to the IEC standards (*e.g.* through demonstrating the equivalence of Westinghouse procedures and processes to the IEC standards)."
- AF-AP1000-CI-005: "The licensee shall produce a comprehensive demonstration of compliance with the five level 1 IEC nuclear sector I&C standards (*i.e.* BS IEC 61226, BS IEC 61513, BS IEC 60987, BS IEC 60880 and BS IEC 62138) for the AP1000 I&C systems important to safety (SIS). The demonstration shall address: all relevant clauses; the operation and maintenance part of the SIS lifecycle; platforms and systems individually; and Class 3 systems."
- AF-AP1000-CI-023: "The licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in systems important to safety. This shall include a demonstration of conformance to relevant IEC standards."

The GDA issues and some of the findings in relation to codes and standards were resolved by Westinghouse during Step 4 and close-out of the GDA. However, some actions for further clarification remain. One example is in relation to the safety case for the diverse actuation system (DAS) for which the GDA close-out forward programme requires the licensee to "fully develop the safety case outlined in the DAS basis of safety case as the detailed design of the DAS is completed post-GDA, and implement the basis of safety case plan including:

- Document and justify the adequacy of the final DAS architecture and design in the safety case (that is, changes from (1-out-of-2)x2 to 2-out-of-4 as committed to in the basis of safety case).
- Implement the compensating measures identified in the SAPs, IEC 61513 and IEC 61508-2 compliance assessments (for example, by including design and implementation detail, addressing all clauses and all 'should'/'may' statements within clauses).
- Ensure that the equipment qualification programme addresses the detailed UK AP1000 reactor DAS design and UK specific equipment qualification conditions.
- Implement the requirements of the DAS safety lifecycle document (for example, adequate coverage of diversity-seeking decisions in the DAS safety lifecycle and verification of lifecycle outputs)" [20].

These requirements could result in changes to the I&C design basis, drawings, equipment supply, qualification requirements, maintenance requirements, operating instructions, *etc.* This would incur additional design and licensing costs as the necessary documentation and demonstrations are performed, as well as the possible need to use non-standard AP1000 suppliers.

The preference of one code over another can also lead to more subtle design changes associated with design and operability aspects built into the codes, for example the reliability of the I&C systems. In both Japan and the UK, it is required not only to provide physical and electrical separation for I&C systems but also separation of data communications between the Class 1 I&C and other Class 2&3 I&C systems.

While the requirement is the same, UK relevant good practice required a higher standard of data isolation than in Japan, with strict one-way communication enforced by data diodes between the Class 1 and the Class 2&3 I&C systems.

While this change is relatively minor and by itself would not have a significant impact, the requirement to

review and reassess the entire design through the licensing processes results in uncertain timescales and increased risk.

4.4 Common cause failure

Requirement 24 of *Safety of Nuclear Power Plants: Design* states: "The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability" [1].

At national level, differences often exist between country interpretations of what is meant by the terms 'diversity', 'redundancy', 'physical separation' and 'functional independence', and how these concepts are to be applied.

For example, for I&C systems this requirement in Japan is supplemented by two suites of further guidance, namely: the Japan LWR design safety guide [21][9] and Japan Electric Association Guides (JEAG) such as JAEG 4611 – Guideline for Design of Instrumentation & Control Equipment with Safety Functions, while in the UK the IAEA safety standards guidance is complemented by safety assessment principles (SAPs) and technical assessment guides (TAGs)[10] *e.g.*, NS-TAST-GD-003 Revision 9 (March 2018)and NS-TAST-GD-046 Revision 6 (April 2019), which indicate a preference for the use of IEC standards.

The differences in how the requirements have been interpreted through the development of these national standards and guidance has led to a number of differences in the implementation of concepts required to mitigate common cause failure (CCF).

These differences were summarized by Hitachi-GE during the generic design assessment (GDA) of the ABWR and are detailed in section 14.3.2 of the *UK ABWR Generic Design Assessment Pre-Construction Safety Report Chapter 14* [22].

One of the key differences stemming from this was in relation to the interpretation regarding diversity and redundancy of the backup for the safety system logic and control system[11]. This difference led to the requirement to introduce two additional systems: the hardwired A1 (Category A & Class 1) and A2 (Category A & Class 2) I&C systems.

The impact of these new systems and associated hardware meant that the main control room (MCR) would have to be redesigned, leading to additional design studies on the impact of enlarging the MCR within the control building. Significant engineering work would also be required to understand the cabling routing and impacts of this additional cabling, *e.g.* in terms of electromagnetic interface and heat loads in cable trays.

Furthermore, should a developer wish to build an ABWR in the UK, they would also have to develop new operational procedures and implement a new training programme for operators that would be different to every other operational ABWR, reducing any potential safety benefits from operating a standardized fleet of reactors.

When assessing DBCs and DECs, the requirements of CCF can add further layers of complexity in cases where national regulators not only assess DEC differently but also have different interpretations of the

[9] The Nuclear Safety Commission has been merged with the Nuclear and Industrial Safety Agency to form the Nuclear Regulation Authority and regulatory guidance in Japan is currently being updated.

[10] UK SAPs and TAGs are not official guidance for reactor vendors; they are principles and guides for the ONR inspectors to conduct their assessments.

[11] The primary Class 1 digital I&C safety systems.

requirements to mitigate CCF. One such example was highlighted in section 5.2 relating the DEC cases for the I&C system on the EPR.

4.5 Application of safety classifications

Requirement 22 of *Safety of Nuclear Power Plants: Design* states:

"All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

- The safety function(s) to be performed by the item.
- The consequences of failure to perform a safety function.
- The frequency with which the item will be called upon to perform a safety function.
- The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function."

This requirement allows for a national interpretation of how to classify safety significance meaning that there is the possibility that SSCs important to safety could be classified differently between countries for the same reactor design.

In general, the safety classification of the most safety significant SSCs are well-aligned between various countries. It is however not uncommon that SSCs defined in lower safety categories in a vendor country can have their safety classification raised by another regulator.

When differences, in the approaches used by national regulators to classify SSCs important to safety, do exist, they have wide-ranging impacts on design and licensing efforts. In addition to the time and effort incurred through the licensing process to undertake comparison studies, any prospective licensee wishing to develop the respective reactor in the host country would have to ensure any changes are carried through any engineering documentation. This would include altering any procurement specifications to ensure that suitable quality requirements are being applied to the equipment at a now higher safety classification, possibly altering the available supply chain.

It is also possible that these changes to equipment classifications have an impact on spatial parameters through the requirements for different equipment and additional trains of equipment. In certain scenarios this could mean that equipment designed to go into specific modules or rooms within the original reactor design would no longer fit, and must be redesigned, leading to significant cost and potential delay to the power station development programme.

One such example of when these differences in safety classifications have occurred is between the US and UK approaches and the subsequent impact this had on the AP1000 design during the UK GDA process.

US approach

The US approach is one in which equivalence must be demonstrated against several different regulations and standards. The US safety classifications are applied to the AP1000 in accordance with the requirements in US Code of Federal Regulations (10 CFR 50.55a) as well as considering the following:

- American National Standards Institute (ANSI) N18.2 – safety classification.
- American Nuclear Society (ANS) 51.1 – safety classification.
- American Nuclear Society (ANS) 58.14 – safety and pressure integrity classification criteria for light water reactors.
- Regulatory Guide 1.26 – quality groups.
- Regulatory Guide 1.97 – instrumentation requirements.
- 10 CFR 21.

For the purposes of equipment classification, AP1000 SSCs are classified as Class A, B, C, DiD Class D and non-safety. For mechanical equipment Classes A, B, and C are equivalent to ANS Safety Class 1, 2, and 3. For electrical equipment Class C is equivalent to Class 1E. SSCs classified as equipment Class A, B, or C or seismic Category I are basic components as defined in Table 3.2-1 in 10 CFR Part 21[23].

The approach adopted by Westinghouse was reviewed and approved by the US Nuclear Regulatory Commission.

UK Approach

In the UK, safety classification of SSCs is tied to safety assessment principles (SAPs) [24] *e.g.*:

- Engineering safety classification and standard ECS.1: "The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety."
- Engineering safety classification and standard ECS.2: "Structures, systems and components that have to deliver safety functions should be identified and classified

on the basis of those functions and their significance to safety."

During Stage 3 of the GDA process, it was determined that the approach adopted and approved within the USA would not be acceptable in the UK. This led to Westinghouse producing a comparison between the US categorization system, and the three-tier system in the UK SAPs:

- Category A – Principal means for maintaining nuclear safety; failure has potential for significant core damage or release to the environment within 72 hours of accident, *e.g.* decay heat removal, reactivity control, main control room (MCR) habitability, reactor control system (RCS) integrity, RCS inventory control, containment heat removal/integrity, spent fuel cooling.
- Category B – Significant contributor to maintaining nuclear safety; failure may reduce safety margins significantly, but not result in a design basis accident, *e.g.* radioactive waste system integrity, instruments to monitor Category A functions, post-72-hour functions, isolation of control systems which could reduce margins.
- Category C – Contribution to nuclear safety; failure will not result in a design basis accident, *e.g.* long-term support of Category A and B functions, beyond design basis accident events, monitoring of environmental releases.

In addition to the time and effort needed to undertake the comparison work, this difference led to changes in the classification of certain SSCs within the AP1000 design, for example: startup feedwater pumps and standby diesel generators are classified as Class D in the USA, and as Category A Class 2 in the UK.

This difference in approach to safety classification of SSCs has also been observed between Japan and the UK during the GDA of the ABWR. One such example was the difference in approach to the safety classification of the spent fuel pool cooling system.

In Japan, the fuel pool cooling and clean-up system is designed to cool down the spent fuel pool water and eliminate impurities from water using a single circuit. This configuration comes from the following technical considerations:

- The cooling function is able to maintain the integrity of the spent fuel pool which is designed with the highest safety class (Class 1).
- Redundant water injection means are provided with the residual heat removal (RHR) system which consists of three independent divisions and is designed as a Class 1 safety system.
- There is sufficient time margin to recover from the loss of pumps/heat exchangers before the loss of the pool water inventory above the spent fuel racks by connecting the RHR to the fuel pool piping. Therefore, the fuel pool cooling and clean-up system is designed as a Class 3 system for Japanese ABWRs.

However, established UK relevant good practice implies the fuel pool cooling function (not just the spent fuel pool structure) is safety Category A, which requires at least a safety Class 1 system to fulfil the required function.

As a result, a design change was implemented to provide an additional cooling circuit to ensure that the RHR safety function dedicated to reactor core cooling can be separated from the fuel pool cooling and clean-up system, avoiding complex operation which may result in human error when both RHR functions (reactor core and fuel pool cooling) are required simultaneously.

This design change improved the operational aspects of the reference fuel pool cooling system design by providing, for example, equipment segregation and an additional cooling circuit which makes the system fully single-failure tolerant. However, it caused a lot of redesign effort and would imply the installation of new equipment and changing of operating manuals and procedures.

4.6 Application of human factors

Requirement 32 of *Safety of Nuclear Power Plants: Design* states: "Systematic consideration of human factors, including the human-machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process"[1].

Among other requirements for human factor implementation in design, this requirement states: "The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator."

These requirements, while providing some guidance on areas for consideration, are not explicit enough to eliminate different interpretations between national regulators, leading to different requirements relating to human factor implementation in different countries.

One example of where these differences in interpretation between national regulators resulted in significant design change was in the design of the AP1000 spent fuel pool.

The intended design of the AP1000 spent fuel pool is divided into two regions. Region 1 can accommodate any fuel including an emergency offload from the core. Spent fuel elements are thereafter moved from Region 1 to Region 2[12] during the operation of the plant. Safety is achieved through having sufficient capacity in Region 1 for an emergency offload at all times. Region 2 is designed to be managed in line with a designated loading curve which traces enrichment against irradiation.

In the safety case development in the USA, in order to show that fuel would not be placed in Region 2, which falls outside the loading curve, it is possible to credit the operators as suitably qualified and experienced personnel (SQEP), along with the designed IT systems and programs within the fuel handling machine [24]. The activities required to be undertaken by the operators in the movement of fuel within the spent fuel pool are not considered to be safety-related. This is because it is considered that "due regard for the time available for action has been provided" (*i.e.* 12 months), which eliminates the possibility for errors as a result of time pressure.

However, during the GDA assessment in the UK, it was determined that the use of SQEP operators and computer programs was insufficient to demonstrate that the Region 2 racks of the spent fuel pool would remain subcritical in all foreseeable operating conditions. As a result, GDA issue GI-AP1000-RP-01: *Spent Fuel Pool – Criticality Safety Case* was raised in Step 4 [26].

The immediate impact of this was that Westinghouse undertook significant design studies during the licensing process to assess potential options to satisfy the requirements of the UK regulator, including possibly redesigning the entire pool to the same standard as Region 1.

The longer-term impact of this finding is that if an AP1000 project would be developed in the UK, the project would be required to implement one of the solutions proposed, which could lead to the redesign of the spent fuel pool, incurring additional design and licensing costs. It may also lead to changing of materials or operational regime within the fuel ponds.

Such redesign may also result in an overall reduction in capacity of the spent fuel pool leading to further knock-on effects on the safety case, which would then have to be further evaluated, leading to additional effort.

4.7 Interpretation of the requirements of HVAC systems

The nuclear heating, ventilation and air conditioning (HVAC) systems are generally required to employ appropriate filtration techniques to ensure that the concentration of particulate matter within the gaseous radioactive waste stream is minimized during normal and accident conditions.

Requirement 73 of *Safety of Nuclear Power Plants: Design* states: "Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states." This requirement includes the need "to control gaseous radioactive releases to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable (ALARA)"[1].

[12] Any fuel element can be put anywhere in Region 1, while placement of fuel elements in Region 2 requires more management of elements that have not spent significant time in the core, to ensure that they are not placed close together.

However, there remain differences in the interpretation of how to keep the discharges to the environment ALARA and thus the criteria used to determine the required filter types is not consistent between different countries.

One example of this is the difference observed between the Japanese and UK nuclear regulator during the GDA assessment of the ABWR HVAC systems.

In Japan, the determination of which filter type is used on each HVAC extract is based on public dose assessments accounting for exhaust air from HVAC systems during normal operation. For the ABWR, these dose assessments determined that high-efficiency particulate absorbing (HEPA) filters are not required for the reactor building or turbine building; however they are required for the radioactive waste building HVAC system. Medium efficiency bag-type filters are used on the HVAC systems of the reactor and turbine buildings. In addition, in Japan the casing of all exhaust air filters are made from reinforced concrete.

In the UK, standards regarding nuclear ventilation [27][28] require the use of HEPA filters on all HVAC exhaust ducts. In addition, further UK nuclear ventilation standards require use of a safe change type casing for the exhaust filter to minimize worker dose during filter exchange activities.

During the GDA process the dose rates to the public with and without HEPA filtration during normal operation were assessed. It was found that the additional requirement for HEPA filtration on the ABWR decreased the dose rate from HVAC discharges by 0.1μSv/yr – see section 5.2.3.2 of *UK ABWR Generic Design Assessment, Demonstration of BAT* [30].

Despite the minimal reduction in dose rate, Hitachi-GE was required to redesign the HVAC exhaust systems for the reactor, turbine and radioactive waste buildings to install safe change HEPA filtration units. This would require significant engineering work to redesign the filter rooms and HVAC ducting layout to accommodate the new units. There was also a significant burden during the GDA process during which Hitachi-GE expended significant effort to demonstrate that the installation of HEPA filters on the reactor and turbine buildings would have a very limited impact on dose rates. Despite this, the UK regulator still required the change to HEPA filters on the reactor and turbine buildings.

4.8 Location of items important for safety in relation to internal and external hazards

Requirement 17 of *Safety of Nuclear Power Plants: Design* states: "All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant" [1].

This requirement allows national regulators to interpret how hazards should be considered in the design of the layout, which may depend on their approach to determining the postulated initiating events and industrial best practice identified within their specific country. This can lead to changes in the layout of the plant as different regulators define

different initiating events and have different best practice guidance.

One example of where these differences have occurred is in the location of the emergency diesel generators (EDGs) between the Japanese ABWR and what was required by the UK regulators during the GDA review.

The EDGs are the primary means of delivering emergency power supply to SSCs and undertake fundamental safety functions, fulfilling safety design Requirement 68 – *design for withstanding the loss of off-site power* [1].

The location of the EDGs within the Japanese ABWR is driven by the risk of earthquakes which, if not suitably protected against, could result in damage to the generator-supporting equipment, preventing it from operating when required.

As a result, the EDGs are located within the reactor building along with other safety critical SSCs such as containment, drywell, major portions of the nuclear steam supply system, steam tunnel, refuelling area, essential power, non-essential power, emergency core cooling systems, as well as additional supporting systems. The reactor building is designed to seismic Category 1 requirement to protect necessary safety functions against external hazards. In the reactor building there are three redundant EDGs, each EDG supplying power to one of the three mechanical and electrical safety divisions of SSCs.

It was determined during the UK GDA process, that because of UK relevant good practice [31], the EDGs would have to be removed from the reactor building and placed in dedicated buildings. The reasoning behind this was varied but included the aspects of segregation, and protection from external hazards such as aircraft impact and fire simultaneously affecting more than one EDG. The risk of earthquakes is not so prevalent in the UK when compared with Japan, and it is likely that many other regulators would have requested similar changes.

For the UK licensing, each EDG building is a structure which houses the engine, generator, fuel oil system, air intake and exhaust system and other related facilities for the EDG system. Each building also includes a fuel storage tank for seven days' operation of the EDG without offsite supply.

This resulted in increased effort associated with design and licensing while engineering rework was undertaken to redesign the reactor building, design three new seismic Category 1 buildings and change the layout of the plant, which resulted in further rework and delay associated with the submissions of licences and permits.

Should an ABWR project be developed in the UK, these changes would result in an increased cost related to three additional dedicated safety Class 1 buildings and associated components, such as connecting tunnels, HVAC components, cables, and piping.

5 Implications and Lessons Learned

This report provides a number of examples of where different national regulatory interpretations of fundamental safety requirements, or their application has led to design change requests. These changes can have far-reaching consequences to plant design, licensing timescales, supply chain availability, construction schedule and cost, hence incurring high project risks to reactor vendors and/or prospective licensees.

Approach to defence-in-depth

Differences in approaches used for defence-in-depth (DiD) have been identified between Russia and Western European regulators, which are predominately associated with the division of the Level 3 DiD into two subcategories by western European regulators. However, it is not clear if these different approaches result in any change in overall safety of the nuclear power plant. Whether Level 3 is split between two levels or just defined by one overarching level, the overall safety objective is the same, *i.e.* to limit radiological releases and prevent escalation to core melt conditions.

Therefore, in order to minimize the impact of these different approaches, regulators should agree, for a certain reactor type, what parameters (*e.g.* postulated events) need to be considered and these should be quantitatively developed and agreed at an international level. The methods via which the deterministic safety analysis should be conducted should also be agreed.

This might be particularly relevant for certain emerging reactor designs that have greater levels of inherent and passive safety, which might affect the systems needed to provide the required level of protection at each DiD level compared to a large-scale LWR. In addition, it may be necessary to completely revise the implementation of the approach to DiD for certain reactor types (*e.g.*, molten salt reactors), particularly those of a homogeneous core concept, for which the severe accident model used for water-cooled reactor core melt scenarios do not apply.

It is worth noting that the SMR Regulators' Forum has recognized the need to address DiD in its *Report from Working Group on Defence-In-Depth* [32]. While this report is still quite high-level and focused on LWR technology, it has been written to highlight features of SMRs that are different from Generation III designs and provides recommendations on how to manage these differences.

Design basis conditions and design extension conditions

Various examples associated with EPR projects in China, Finland, France and the UK outline how the different approaches to identification, application and evaluation of design basis conditions (DBCs) and design extension conditions (DECs) can lead to differences in nuclear power plant design.

Therefore, further harmonization on approaches for identification, application and evaluation of DBCs between designs is needed. This can be achieved through collaboration between national regulators on joint assessments of reactor designs to develop bounding envelopes in which all regulatory authorities could accept the outcomes from each other's assessments. Such an approach may also require a level of equivalence demonstration from one regulatory approach to another.

This will be particularly important for some future reactor designs in which core melt accidents have been practically eliminated because DEC identification and analysis will

be considerably different to that which most regulators are currently familiar with (*i.e.* the approach used for land-based water-cooled nuclear power plants).

Application of codes and standards

Although a particular code or standard may not necessarily be better than another, national regulators have preferences for using codes and standards they are most familiar with or best fit their requirements. These preferences can lead to a large number of findings during regulatory review that take a significant amount of effort to resolve.

The need to demonstrate equivalence between different codes and standards is well-understood and much work is being carried out in this area by CORDEL and standards developing organizations (SDOs). However, codes and standards may have their own approaches to developing design solutions that achieve the same safety objectives, and it can be difficult to demonstrate the equivalence of a consistent, but different, set of rules. In addition, provisions within codes and standards for quality assurance, requirements for qualification of people and processes, and for assessment of products may depend on the context and the regulations in place.

It is unclear if the use of one standard over another has any impact on the overall safety of a nuclear power plant design, as long as the codes and standards have been applied consistently. Therefore, regulatory authorities should be able to assess designs against different codes and standards to their preferred ones or to accept the outcomes of other national regulators in this area.

Common cause failure

The common cause failure (CCF) examples provided in this report specifically concern I&C systems and demonstrate that the most prevalent difference between national regulators in this area is in the interpretation of the terms ‘diversity’, ‘redundancy’, ‘physical separation’ and ‘functional independence’.

These different interpretations of terminology can have a significant impact on the design of nuclear power plants, with no clear impact on overall safety. Common terms should therefore be developed to prevent or minimize different interpretations. The *IAEA Safety Glossary* [33] and CORDEL report on *Defence-in-Depth and Diversity* [5] define certain terms such as ‘diversity’, ‘redundancy’ and ‘physical separation’; however, to support harmonization, how these terms are applied needs to be defined.

Application of safety classifications

The different approaches used to develop the safety classification of SSCs can have a significant impact on nuclear plant design, as well as further down the supply chain. The design solutions created by these different approaches have no meaningful impact on the overall safety of the design and alternative approaches could be used to mitigate the perceived risks.

This could have a detrimental impact on new reactor designs and increase risk, as the benefits of using less complex and more inherent safety features, or of having smaller plant footprints, could be lost through the possible addition of equipment that other regulators have deemed to be unnecessary. The various approaches used by regulators should therefore be aligned, or equivalence demonstrated to allow validation of each other’s assessments.

Application of human factors

The different implementation of fundamental safety requirements concerning human factors appears to be based on different operating experience within countries. The requirement of the UK regulators in the example discussed (see Section 5.6), relating to design and operating requirements for the spent fuel pool, reduce the potential for operator error. However, the cost of doing so may outweigh the degree of risk the regulators are trying to mitigate.

This might be particularly the case for future reactor designs in which current regulatory approaches to the application of human factors may be incompatible with the small nature or innovative features of these designs. It would be beneficial if regulators applied human factors within their assessments, based not just on their own experiences, but also on those of other national regulators, and the determination of which measures to implement should be weighed against the risk of not doing so.

This approach should be applied to all decisions on which measure to implement, not just in relation to human factors, and can be done so through risk-informed decision making.

Interpretation of the HVAC requirements

In the example provided (see Section 5.7), the changes required to the HVAC systems lowered both worker and public dose. However, in the case of lowering the dose to the public, the changes required additional and increased efficiency filters to be added to the design which achieved a very minimal reduction in dose. This is another example of where the costs to implement the change outweigh the benefits. The greatest increase to overall safety in this example was in requiring the change of existing filter types to the safe change type, thus reducing worker dose during maintenance.

This example highlights the need for regulatory commonality of terms, in this case ALARA, or at least the approach to how national regulators should apply such terms.

Items important for safety in relation to internal and external hazards

The changes required by the UK regulators in relation to emergency diesel generator (EDG) layout improved the redundancy and operability of the design during loss of offsite power events; however, it may have been possible to develop a solution that mitigated most of the perceived risk without taking the drastic steps of redesigning the reactor building and creating new seismically rated buildings onsite.

This example demonstrates that greater regulatory harmonization of which internal and external hazards are to be considered would greatly help reactor vendors in developing plant layouts that can be standardized across multiple national boundaries.

This is an area that could also affect future reactor plant layout designs, depending upon their need for EDGs or alternative back-up systems, which would increase their overall footprint.

6 Conclusions and Recommendations

Nuclear safety objectives have been well-harmonized between countries and national regulators through cooperation at an international level and the creation of standards such as the IAEA Safety Standards series and the Western European Nuclear Regulators Association (WENRA) safety reference levels.

Despite the same safety objectives demonstrably being achieved in countries around the world, the application and interpretation of these objectives into specific national regulatory requirements and guidance can result in significant differences between reactor designs deployed in different countries.

This report outlines that there are many differences in the way in which national regulators interpret and apply the fundamental safety requirements. It is also apparent that the divergence between countries does not always occur at the same level in the hierarchy of the safety requirements. The safety requirements described in this report are:

- Defence-in-depth.
- Design basis conditions (DBC) and design extension conditions (DEC).
- Internal and external hazards.
- Codes and standards.
- Common cause failure (CCF).
- Safety classifications.
- Human factors.
- HVAC requirements.

Previous efforts to harmonize the differences between national regulatory requirements have taken place through the activities of the Multinational Design Evaluation Programme (MDEP) and WENRA among others, however these efforts have not gone far enough and significant variations between national regulatory requirements remain. The differences between the acceptance criteria of national regulators can be difficult to distinguish as it is not always part of the established requirements but in some cases may result from the deliberation of a group of individuals or strongly influenced by the different interpretations of specific inspectors/assessors, making the licensing process unpredictable and increasing project development risks.

In addition to the application and interpretation of the fundamental safety requirements differing between national regulators, the method of demonstrating a safety case can also vary widely (*e.g.* prescriptive versus non-prescriptive regulatory approaches). When reactor vendors wish to license their design in a country with a different regulatory framework, different levels of prescriptiveness and guidance can lead to a complete reframing of the original safety case and ultimately a significant amount of effort from the reactor vendor to produce new documentation that was not required by other national regulators.

If the same fundamental safety requirements are applied by all countries, it might be expected that licensing a reactor design under a non-prescriptive regulatory regime would result in only minor changes. However, this report discusses examples of design changes requested because of different interpretations or applications of safety requirements by regulators across various types of regulatory framework. One key finding from this report has been that the significance of the design changes requested by a national regulator does not correlate to the level of prescriptiveness of that regulator's framework.

Another finding of this report is that differences in the outcome of design solutions, when the same

reactor design is applied to different regulatory regimes, are often driven by differences between the way in which national regulators identify fault scenarios/conditions and criteria, which ultimately define the design provisions.

These differences in approach and interpretation can have significant impacts when reactor vendors are developing projects in host countries. They very often lead to design changes which can have knock-on effects and reduce the predictability of licensing timescales, costs, supplier interactions and plant layout, essentially turning what should be an n^{th}-of-a-kind (NOAK) project into another first-of-a-kind (FOAK) one.

Some of the examples identified the installation of new SSCs or changes to their safety classification and/or plant location. These changes represent increased risks for vendors and project developers, as the benefits of new designs with less complexity, greater inherent safety and smaller plant footprints would potentially be lost through the addition of equipment that other regulators have deemed to be unnecessary.

It is therefore vital that national regulators and reactor vendors learn the lessons, demonstrated within this report, associated with the national approaches to regulation of Generation III reactor designs and apply these lessons to the review of emerging technologies, such as SMRs, to facilitate a wider deployment of standard designs.

While this report identifies the need for greater regulatory harmonization across the areas discussed, it is recognized that the differences in the requirements between regulators are difficult to resolve as they are derived using different approaches and assumptions and can be based on specific technologies and/or regulator experience.

It should also be noted that reactor vendors have a significant role in supporting these activities, as they will be the first to develop the associated safety requirements for new designs and early dialogue with the regulators would help to ensure a common understanding.

To support the standardization of reactor designs and to achieve harmonization of national regulatory approaches, reactor vendors, licensees and regulators should:

- Engage at an international level to understand the differences in regulatory approaches, and assess impacts on designs, thereby understanding the level of design regulatory readiness and allowing broader design solutions to be proposed that are aligned to a wider range of regulatory requirements.
- Develop and support a suitable framework to undertake joint regulatory design and safety reviews, share technical reviews, establish common position statements on safety requirements, and identify other areas for collaboration.
- Further develop common terminology within the *IAEA Safety Glossary* [33], and the CORDEL Digital Instrumentation and Control (DICTF) *Defence-in-Depth and Diversity* report [5] (diversity, physical separation, ALARA, *etc.*), including guidance on how they should be applied, with consideration of the novelties of future reactor designs. The extent of, and level of detail within, this guidance should be detailed enough to provide a consistent output from safety assessments without being so prescriptive that it limits design innovation.

- Expand upon the areas identified in this report (defence-in-depth, postulated initiating events, design basis accidents and design extension conditions, internal and external hazards, and instrumentation and control) defining the key design and licensing requirements to focus on in joint regulatory reviews, and develop guidance on how these should be implemented within reactor designs.

Greater detail on how to understand design regulatory readiness has been discussed in the CORDEL report *Design Maturity and Regulatory Expectations for Small Modular Reactors* [3], which also made a number of specific recommendations to reactor vendors, licensees and regulators.

In order to develop an approach which can be applied to future regulatory review efforts, collaboration at an international level between reactor vendors, licensees and regulators will need to increase. One such proposal to facilitate greater international harmonization was developed by the World Nuclear Association's CORDEL report, *Harmonization of Reactor Design Evaluation and Licensing: Lessons Learned from Transport* [6], which proposes a new international framework for nuclear regulation. It is envisaged that the starting point for such a framework would be a series of meetings between the nuclear industry and regulators to agree on priorities, scope and plan.

As part of this proposed framework, regulators should consider the areas identified within this report on different interpretations of regulatory requirements, as well as other areas that require harmonization. It is proposed that this is done in a systematic manner such that the approaches developed can be traced back to the original requirements (applicable to each reactor design).

It is envisaged that any joint reviews would make appropriate use of the reference reactor design review, where one exists, as outlined in CORDEL report *Making Use of the Reference Plant Concept for Licensing New Nuclear Units* [4], and joint assessments would be undertaken using a consistent risk-informed approach, adopting other regulatory assessments and experience where appropriate.

References

[1] IAEA Safety Standards – Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1), International Atomic Energy Agency, February 2016

[2] Licensing and Project Development of New Nuclear Plants, World Nuclear Association, January 2013, reprinted August 2015

[3] Design Maturity and Regulatory Expectations for Small Modular Reactors, World Nuclear Association, June 2021

[4] Making Use of the Reference Plant Concept for Licensing New Nuclear Units, World Nuclear Association, September 2019

[5] Defence-in-Depth and Diversity: Challenges Related to I&C Architecture, World Nuclear Association, April 2018

[6] Harmonization of Reactor Design Evaluation and Licensing: Lessons Learned from Transport, World Nuclear Association, December 2020

[7] IAEA Safety Standards – Fundamental Safety Principles, Safety Fundamentals No. SF-1, International Atomic Energy Agency, November 2006

[8] Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, October 1999

[9] Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, June 1996

[10] WENRA Safety Reference Levels for Existing Reactors 2020, Western European Nuclear Regulators Association, February 2021

[11] The Structure and Application of High Level Safety Goals, A Review by the MDEP Sub-committee on Safety Goals, OECD Nuclear Energy Agency, January 2011

[12] EUR Specification Document, Revision E, Volumes 1, 2&4, EUR Organisation, December 2016

[13] IAEA Safety standards – Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2 (Rev. 1), July 2019

[14] Safety Assessment Principles for Nuclear facilities, Office for Nuclear Regulation, 2014 Edition, Revision 1 (January 2020)

[15] Design Basis Analysis, NS-TAST-GD-006 Revision 5, Office for Nuclear Regulation, October 2020

[16] Comparison of Fatigue Life Analysis Methods – Comparison of Pressure Vessel Fatigue Codified Design Rules Based on S-N Approach, CORDEL Mechanical Codes and Standards Task Force, World Nuclear Association, June 2020

[17] New Reactors Programme, GDA close-out for the AP1000 reactor, GDA Issue GI-AP1000-CI-08 – PMS Adequacy of Safety Case, Assessment Report: ONR-NR-AR-16-034, Revision 0, Office for Nuclear Regulation, March 2017

[18] New Reactors Programme, GDA close-out for the AP1000 reactor, GDA Issue GI-AP1000-CI-09 Component Interface Module, Adequacy of Safety Case, Assessment Report: ONR-NR-AR-16-035, Revision 0, Office for Nuclear Regulation, March 2017

[19] Generic Design Assessment – New Civil Reactor Build, Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000 Reactor, Assessment Report ONR- GDA-AR-11-006, Revision 0, Office for Nuclear Regulation, 11 November 2011

[20] New Reactors Programme, GDA close-out for the AP1000 Pressurised Water Reactor, GDA issues GI-AP1000-CI-01 Revision 0 DAS – Adequacy of Safety Case and GI-AP1000-CI-02 Revision 0 DAS – Adequacy of Architecture, Assessment Report: ONR-NR-AR-16-029, Revision 0, Office for Nuclear Regulation, March 2017

[21] *Regulatory Guide for Reviewing Safety Design of Light Water Nuclear Power Reactor Facilities*, NSCRG: L-DS-I.0, Nuclear Safety Commission of Japan, first published 1970, revised 1977, 1981, 1990, 2001
N.B Updated guidance is being produced by the Nuclear Regulation Authority following the merging of the Nuclear and Industrial Safety Agency and the Nuclear Safety Commission

[22] UK ABWR Generic Design Assessment – Generic PCSR Chapter 14: Control and Instrumentation, 3E-GD-A0063 Rev C, Hitachi-GE Nuclear Energy, 2017

[23] Westinghouse AP1000 Design Control Document Rev. 19 - Tier 2 Chapter 3 - Design of Structures, Components, Equipment & Systems - Section 3.2 Classification of Structures, Components and Systems ML11171A425, US Nuclear Regulatory Commission, June 2011

[24] Categorization of safety functions and classification of structures, systems and components, NS-TAST-GD-094 Rev 2, Office for Nuclear Regulation, July 2019

[25] Westinghouse AP1000 Design Control Document Rev. 19 – Tier 2 Chapter 9 – Auxiliary Systems, US Nuclear Regulatory Commission, June 2011

[26] New Reactors Programme, GDA close-out for the AP1000 reactor, GDA Issue GI-AP1000-RP-01 Rev 0: Spent Fuel Pool – Criticality Safety Case, ONR-NR-AR-16-019-AP1000 Revision A, Office for Nuclear Regulation, March 2017

[27] An Aid to the Design of Ventilation of Radioactive Areas, Issue 1, NVF/DG001, Nuclear Industry Safety Directors Forum January 2009

[28] ISO 26802:2010 Criteria for the design and the operation of containment and ventilation systems for nuclear reactors, International Organization for Standardization, August 2010

[29] Ventilation Nuclear Safety Technical Assessment Guide, Office for Nuclear Regulation, NS-TAST-GD-022 Rev 7, June 2020

[30] UK ABWR Generic Design Assessment – Demonstration of BAT, XE-GD-0097, Rev G, Hitachi-GE Nuclear Energy, 2017

[31] Nuclear Safety Technical Assessment Guide, Emergency Power Generation, NS-TAST-GD-103 Revision 1, Office for Nuclear Regulation, February 2019

[32] SMR Regulators' Forum Pilot Project Report, Report from Working Group on Defence-In-Depth, SMR Regulators' Forum, January 2018

[33] IAEA Safety Glossary – Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, International Atomic Energy Agency, June 2019

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

Fundamental safety requirements for nuclear energy have been agreed at an international level through the Convention on Nuclear Safety and the International Atomic Energy Agency's (IAEA) safety standards. Various international initiatives have attempted to further harmonize the interpretation of these high-level standards into specific national regulatory standards and guidance. Yet, different versions of the same reactor design continue to be built in different countries.

This report outlines this variability by reviewing the different interpretations of fundamental safety requirements when reactor designs have been licensed outside their country-of-origin. The report shows that the nuclear industry is being held back by national approaches to regulation, turning what should be Nth-of-a-Kind projects into First-of-a-Kind ones.

This is not solely a regulatory challenge. If we are to take advantage of the opportunities emerging reactor designs provide, it is essential that governments, regulators, and industry alike take on board these lessons, drive greater collaboration, and implement a suitable framework that would allow a more streamlined approach to regulation. The report recommends a framework under which harmonized approaches to licensing could be developed, and identifies areas, such as defence-in-depth and postulated initiating events, that would be the major focus of harmonization under such a framework.

This report has been produced by the Licensing and Permitting Task Force with support from both the Small Modular Reactor Task Force and Digital Instrumentation & Control Task Force of World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group.