WORLD NUCLEAR ASSOCIATION

Defence-in-Depth and Diversity: Challenges Related to I&C Architecture

Cooperation in Reactor Design Evaluation and Licensing Working Group of the World Nuclear Association

Title: Defence-in-Depth and Diversity:
Challenges Related to I&C Architecture
Produced by: World Nuclear Association
Published: April 2018
Report No. 2018/003

Cover image: Framatome

Contents

Foreword

The Cooperation in Reactor Design Evaluation and Licensing Working Group (CORDEL) was established by the World Nuclear Association in 2007 with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors and operators) and nuclear regulators on the benefits and means of achieving a worldwide convergence of industry standards for reactor designs.

The Digital Instrumentation & Control Task Force (DICTF) of CORDEL was set up in 2013 to investigate key issues in digital instrumentation and control (I&C) related to the licensing of new nuclear power plants, and to collaborate with the International Electrotechnical Commission (IEC) and the Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG).

On the basis of a survey of its members, the CORDEL DICTF has identified four main issues for investigation:

- Safety classification for I&C systems in nuclear power plants.
- Defence-in-depth and diversity[1].
- Field-programmable gate arrays (FPGA): criteria for acceptance.
- Reliability predictions.

These are discussed in more detail in *CORDEL DICTF 2014-2016 Outlook* [Ref 1].

This report is the first in the series on *Defence-in-Depth and Diversity,* and builds upon the work carried out in the series of reports on *Safety Classification for I&C Systems in Nuclear Power Plants* [Ref 2, 3].

This report was drafted by Gregory Droba (GE Hitachi), with the input and support from the members of the Task Force.

[1] Referred to as diversity and common cause failure (CCF) in *CORDEL DICTF 2014-2016 Outlook* [Ref 1]

Executive Summary

Inconsistencies in the definitions of terms, attributes, assessment methodologies, and scope associated with the concepts of 'defence-in-depth' and 'diversity' can lead to significant challenges in design, licensing and cost of nuclear power plants. The differences between these definitions were first investigated in *Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts* [Ref 3] and are expanded upon here.

The concept of 'diversity' in particular has changed as concern over common cause failure (CCF) in digital instrumentation and control (I&C) systems has become more prevalent. This has in turn affected the development of I&C design for the main line of defence (*e.g.* protection system). Previously, redundancy and separation of structures and components – such as the use of identical equipment in a four/three divisional arrangement – was an acceptable approach to meet the N+2 criterion[2] and thereby demonstrate diversity. However, the N+2 criterion has now been extended by the conservative assumptions associated with digital I&C and thus digital CCF has come to replace redundancy as the main driver for designing diverse digital protection systems.

This report is organized as follows:

- A review of the terms and definitions associated with defence-in-depth and diversity used by different organizations.
- Outline of the challenges in defining 'defence-in-depth' and 'diversity'.
- Analysis of the challenges related to the application of defence-in-depth and diversity, for example during the upgrading of existing nuclear plants or the implementation of regulatory guidance.
- Recommendations of potential solutions.

[2] The N+2 failure criterion means that it must be possible to perform a safety function even if any single component designed for that function fails and any other component or part of a redundant system (or a component of an auxiliary system necessary for its operation) is simultaneously out of operation due to repair or maintenance.

1 Terms and Definitions

To overcome the challenges of implementing digital I&C systems, the terms and definitions in use around the world associated with 'defence-in-depth' and 'diversity' need to be understood. A detailed analysis of the differences in definitions between regulatory bodies and major nuclear codes and standards (see Table 1) was presented in *Safety Classification for I&C Systems in Nuclear Power Plants: Comparison of Definitions of Key Concepts* [Ref 3].

In this report, the International Atomic Energy Agency (IAEA) and, when relevant, the US Nuclear Regulatory Commission (NRC) definitions are given. This section provides the definitions of 'defence-in-depth', 'diversity', their attributes and their use in the treatment of digital common cause failures (CCF) by regulatory bodies.

1.1 Defence-in-Depth and Diversity

The term 'defence-in-depth and diversity', which is sometimes referred to as simply 'D3', is not defined by most regulatory bodies [Ref 3]. The concepts of 'defence-in-depth' (DiD) and 'diversity' are therefore most often considered separately, though they are strongly interrelated, with 'diversity' defined as an attribute of 'defence-in-depth' in most cases.

The definition of 'defence-in-depth' provided by the International Atomic Energy Agency (IAEA) is:

A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions. [Ref 4]

Table 1. List of organizations whose terms and definitions are considered

Organization	Acronym
Atomic Energy Regulatory Board (India)	AERB
Nuclear Safety Authority (France)	ASN
Canadian Nuclear Safety Commission	CNSC
Federal Authority for Nuclear Regulation (UAE)	FANR
Federal Environmental, Industrial and Nuclear Supervision Service of Russia	Rostechnadzor
International Atomic Energy Agency	IAEA
International Electrotechnical Commission	IEC
Institute for Electrical and Electronic Engineers	IEEE
Nuclear Safety and Security Commission (Korea)	NSSC
National Nuclear Regulator (South Africa)	NNR
National Nuclear Safety Administration (China)	NNSA
Nuclear Regulatory Authority (Japan)	NRA
United States Nuclear Regulatory Commission	NRC
Office for Nuclear Regulation (UK)	ONR
Swedish Radiation Safety Authority	SSM
Radiation and Nuclear Safety Authority (Finland)	STUK
Turkish Atomic Energy Authority	TAEK

'Diversity' is defined as:

The presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. [Ref 4]

Diversity can also be effectively applied within a system, for example, signal or sensor diversity within a reactor protection system.

1.2 Common Cause Failure

The design criteria for a nuclear plant's safety systems encompass principles such as high quality, integrity, reliability, independence, and qualification. Separation, redundancy, physical barriers, and electrical isolation are design measures that are applied to address potential vulnerabilities related to a single failure of equipment and the propagation of failure effects. These measures tend to minimize shared components or equipment and non-essential interconnections within I&C system architectures. While these measures reduce the potential for CCF they cannot eliminate CCF, therefore diversity provides an additional level of assurance to mitigate CCF vulnerabilities.

A CCF is defined as a "failure of two or more structures, systems and components due to a single specific event or cause" [Ref 4], hence the broad definition of CCF can be very complex. This report focuses on the relationship between CCF and diversity, particularly where a CCF of two or more structures, systems or components is the result of a triggering event or condition that exposes a latent design or manufacturing flaw.

For nuclear applications, the use of a robust software development lifecycle process is a means to reduce latent defect errors and therefore also contributes to the mitigation of software CCF.

Regulatory-based design considerations for potential CCF in digital instrumentation and control (I&C) systems have evolved over time and have affected the development of protection system I&C architectures. The N+2 criterion used to be the main design driver for a protection system's I&C architecture and resulted in the familiar four-fold and three-fold system architectures. The N+2 criterion has now been extended by the conservative assumptions associated with digital CCF concerns (*i.e.* assumed digital CCF coincident with an anticipated operational transient or postulated accident). These types of failure were historically classified as 'beyond design basis events', but they have come to be considered controlling factors in safety system design.

It is interesting to note that in non-nuclear standards, failure propagation and environmental impacts are the primary focus of CCF vulnerabilities while latent design or manufacturing flaws play only a minor role in these standards. Only 20% of the CCF assessment criteria in such standards are concerned with the risk of design or manufacturing flaws. The remaining 80% of CCF assessment criteria is focused on failure propagation and environmental impact. [Ref 5].

1.3 Attributes of Defence-in-Depth

Various attributes can be used when performing a defence-in-depth (DiD) evaluation. Depending on the purpose, scope, and objectives of the evaluation, one attribute or several may be required. Additionally, the particular mix of these attributes needs to be considered depending on the regulatory regime.

Several attributes associated with DiD were identified and highlighted on the Digital Instrumentation & Control Task Force (DICTF) list of key terms which frequently cause trouble in the interpretation of requirements [Ref 2, 3]. The IAEA approach to DiD is defined more specifically than the Nuclear Regulatory Commission (NRC) approach and many European regulators have adopted the IAEA approach. Thus, for this report, the IAEA definitions are used [Ref 4].

1.3.1 Independence

For digital I&C systems, equipment is considered to be independent if it possesses the following characteristics:

- The ability to perform its required function is unaffected by the operation or failure of other equipment.
- The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

1.3.2 Separation

'Separation', also referred to as 'physical separation', concerns separation by geometry (*e.g.* distance or orientation), barriers, or a combination of these. Separation is also used in the context of electrical isolation, functional independence and independence of communication [Ref 6, Requirement 21].

1.3.3 Redundancy

Redundancy is the provision of alternative (identical or diverse) system, structure and components (SSCs), so that any of the redundant SSCs can perform the required function regardless of the state of operation or failure of the other.

1.3.4 Reliability

Reliability is the probability that a SSC will meet its minimum performance requirements when called upon to do so.

1.3.5 Availability

Availability is the fraction of time for which a system is capable of fulfilling its intended purpose. It is defined as the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, with the assumption that the necessary external resources are provided.

1.3.6 Levels of Defence

In nuclear engineering, all safety activities, whether organizational, behavioral or equipment-related, can be organized into levels of overlapping provisions, so that if a failure should occur it would be mitigated, compensated for, or corrected without causing harm to individuals or the public at large.

1.4 Attributes of Diversity

It has long been recognized that vulnerabilities related to a single failure of equipment by common cause (CCF) can be mitigated through diversity of safety systems.

Various attributes can be used to evaluate the diverse nature of two systems. As with DiD evaluations, the purpose, scope, and objectives of the diversity evaluation may require one or more attributes, and the approach required by different regulators may require a different mix of these attributes.

The definitions of 'human', 'design', 'software', 'functional', 'signal' and 'equipment' diversity [Ref 7] are widely accepted by most nuclear suppliers, operators and regulators. Additional or refined definitions of attributes such as 'life-cycle', 'logic', 'equipment manufacture', and 'logic processing manufacture' diversity have been proposed, but are not as widely adopted [Ref 8].

1.4.1 Human Diversity

The way in which human beings can affect design is referred to as human diversity. It can be extremely variable and is a contributing factor in determining overall diversity. Using separate designers and testers to design and test functionally diverse safety systems may reduce the possibility of design errors [Ref 7, Section 3.2.4].

1.4.2 Life-Cycle Diversity

Life-cycle diversity is an aspect of human diversity that focuses specifically on the impact of human influences on the software life-cycle [Ref 8, Section 2.2.3.5].

1.4.3 Design Diversity

Design diversity is the use of different approaches, including both software and hardware, to solve the same or similar problem. The rationale for design diversity is that different designs will have different failure modes and will not be susceptible to the same common influences [Ref 7, Section 3.2.1].

1.4.4 Software Diversity

Software diversity is the use of different programs designed and implemented by different development teams to accomplish the same goal. The rationale for software diversity is that different programmers will make different mistakes. Factors that contribute to software diversity are the use of different algorithms, logic, program architecture, timing, operating systems, and computer languages [Ref 7, Section 3.2.6].

1.4.5 Logic Diversity

Logic diversity is a specific type of software diversity that excludes any aspect of human diversity and instead focuses on the diverse manner in which the executables are constructed [Ref 8, Section 2.2.3.6].

1.4.6 Functional Diversity

Two systems are functionally diverse if they perform different physical functions even though they may have overlapping safety effects. Functional diversity is often useful when determining if sufficient mitigation means have been employed for the postulated accidents. For example, a combination of alternative systems in the face of primary system failure may be enough to mitigate the effects of an accident. Factors that contribute to functional diversity are the use of different underlying mechanisms, purposes, functions, control logic, actuation means, and response timescales [Ref 7, Section 3.2.3].

1.4.7 Signal Diversity

Signal diversity is the use of different sensed parameters to initiate protective action. Factors that contribute to signal diversity include the following:

- Different reactor or process parameters sensed by different physical effects.
- Different reactor or process parameters sensed by the same physical effect.
- The same reactor or process parameters sensed by a different redundant set of similar sensors [Ref 7, Section 3.2.5].

1.4.8 Equipment Diversity

Equipment diversity is the use of different equipment to perform similar safety functions. For example, the use of diverse computer equipment

may have an effect on software diversity; using different equipment can force the use of diverse compilers, linkers, and other support software. This illustrates the deep connection between the diversity attributes [Ref 7, Section 3.2.2].

1.4.9 Equipment Manufacture Diversity

Equipment manufacturer diversity is a subset of 'equipment diversity'. It considers the process and product aspects of the equipment manufacture, which includes, for example, components, manufacturing lines, humans, and the use of different or diverse equipment [Ref 8, Section 2.2.3.2].

1.4.10 Logic Processing Equipment Diversity

Logic processing equipment diversity is a subset of 'equipment diversity'. It considers the architectural aspects of the equipment such as the use of different processing architectures (*e.g.* different processor manufacturers) and the component integration of the equipment [Ref 8, Section 2.2.3.3].

1.5 Comparison of Definitions

The review of the terminology in CORDEL's report on *Safety Classification for I&C Systems: Comparison of Definitions of Key Concepts* [Ref 1] found:

- There is no direct definition of 'defence-in-depth and diversity' by any organization.
- Typically, the definitions for 'defence-in-depth' and for 'diversity' are found separately. Other terms such as 'diversification' or 'diversity principle' are used to refer to the concept of 'diversity'.
- In general, the IAEA definitions appear to be the most practical for both terms.

The IAEA definition of 'defence-in-depth' does not conflict with other organizations' definitions and can be used by organizations that adopt the INSAG DiD model, the WENRA DiD model, or no specific model. The IAEA definition of 'diversity' is equivalent to that of most other relevant organizations and none of the other definitions conflict with it.

2 Challenges of Defence-in-Depth and Diversity

2.1 Definitions and usage

As highlighted in Section 1.1, no nuclear regulatory organization defines the specific term 'defence-in-depth and diversity'. In addition, when the term is used, it is not used in any consistent manner.

2.1.1 Defence-in-Depth Versus Diversity

For the organizations that define 'defence-in-depth', it is common for diversity to be seen as one method of defence-in-depth. However, at least half of the nuclear regulatory organizations reviewed have no definition of 'defence-in-depth', and instead define 'diversity' or 'diversity principle'. Conversely, only two organizations define 'defence-in-depth', but not 'diversity'. The concept of 'diversity' was defined using different principles such as 'diversification' and 'diversity principle' [Ref 3]. The set of permutations used by the organizations that were considered is shown in Table 2.

Although no nuclear regulatory organization specifically defines 'defence-in-depth and diversity', several NRC publications, including NUREG-0493 and NUREG/CR-6303 [Ref 7], use the terms 'defence-in-depth and diversity' as well as 'diversity and defence-in-depth'. IEEE Standard 7-4.3.2, which adopts NRC terminology, uses the terms 'D3' and 'defence-in-depth' [Ref 9].

Defence-in-depth was originally a military concept and NUREG/KM-0009, *Historical Review and Observations of Defense-in-Depth*, provides more detail. The term 'defence-in-depth and diversity' in the context of I&C systems appears to have its origins with the NRC, first in NUREG-0493, *A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System*, and then later through NUREG-6303 and NUREG-7007 to quantify diversity of software to mitigate CCF.

Almost all organizations refer to 'diversity' or 'diversity principle', which is applied to the concept of defence-in-depth. The concept of 'diversity' has evolved to being one way in which DiD can be accomplished. Most approaches use an analysis to identify aspects of the plant design where diversity is required to mitigate CCF concerns.

2.1.2 Qualitative Versus Quantitative Assessment

Assessment methods typically include both qualitative as well as quantitative assessment. An assessment method usually includes the identification of the relevant attributes of diversity, such as human, design, or functional diversity.

Attributes of diversity are defined in order of effectiveness, where a higher or more effective attribute would be more strongly weighted. Effective attributes provide strength in diversity and where this can be demonstrated, the contribution of less effective attributes may be minimal or in some cases not needed to establish diversity. Less effective

Table 2. Organizations whose definitions were considered

Defined Terms	Organizations
Only 'diversity'	CNSC, NRA, IEC, TAEK, ONR
Only 'defence-in-depth'	NNR, NSSC, SSM, NRC
Both 'diversity' and 'defence-in-depth'	ASN, AERB, IAEA, FANR
No definitions	IEEE, ROST, NNSA, STUK

attributes may be able to mitigate CCF vulnerabilities when diversity using the preferred attribute cannot be demonstrated.

The factors of each diversity attribute should be defined and ordered based on effectiveness. For example, the arrangement and connection of the same components in a different manner may constitute design diversity, but the attribute is subjective and thus qualitative. For a quantitative assessment, factors about the design architecture must be defined, which will be subjective. Such postulated factors could include process inputs, output control, the type of bus, or the level of modularization. Finally, values must be assigned to these factors. If modularization is considered to be a factor of the design architecture, values of 'high', 'medium' or 'low' might be acceptable. This example illustrates that any quantitative aspect of the assessment will rely to some extent on subjective or qualitative aspects, which ultimately will be accepted or rejected based on the strength of the argument made for the assessment.

Current methods [Ref 8] that present strategies using quantitative scores are based on subjective or qualitative attributes. The complexity of a purely quantitative approach increases with the aggregate. When the parts of a complex digital software system are integrated, additional CCF vulnerabilities may be identified, which may require additional assessment across types, attributes and factors of diversity.

The challenge then is to balance the qualitative and quantitative aspects of the assessment to present a substantiated argument showing that both aspects of the system being assessed are sufficiently diverse to achieve the level of safety required.

2.1.3 Incomplete and Ambiguous Rules

The purpose of the defence-in-depth analysis is to identify the multiple protective measures needed to ensure the safe operation of the plant. The application of diversity is intended to mitigate the effects of CCFs that would have an adverse impact on the I&C system itself as well as between the different layers of the defence-in-depth scheme. As discussed previously, quantification of defence-in-depth, as well as of diversity, is difficult to justify and separate from the qualitative aspects. These subjective aspects result in ambiguous or incomplete rules relating to how quantification is achieved.

While there are strategies that have attempted to weight and normalize defence-in-depth and diversity criteria [Ref 8], these strategies have relied on the evaluation of qualitatively selected base criteria to calculate a basis for normalization. The inherent ambiguity in starting from a qualitative basis raises questions of the overall analysis, and thus the completion of the analysis can remain unbounded. Additionally, most methods and strategies for defence-in-depth and for diversity extend beyond CCF of software to the hardware and system environment that the software executes.

When the extent and conditions for completion of the analysis are unbounded, subjective, incomplete or ambiguous, the quantification of 'defence in depth' and 'diversity' is difficult to achieve. This situation is likely to continue to remain a challenge without sound scientific information that supports the effectiveness of 'defence-in-depth' and 'diversity' measures.

2.1.4 Definitions of Diversity Attributes

The six diversity attributes (human, design, software, functional, signal and equipment) previously described, originated with NUREG/CR-6303, which was published in 1994 [Ref 7]. NUREG/CR-7007 [Ref 8] builds upon and in some cases redefines the attributes introduced in NUREG/CR-6303.

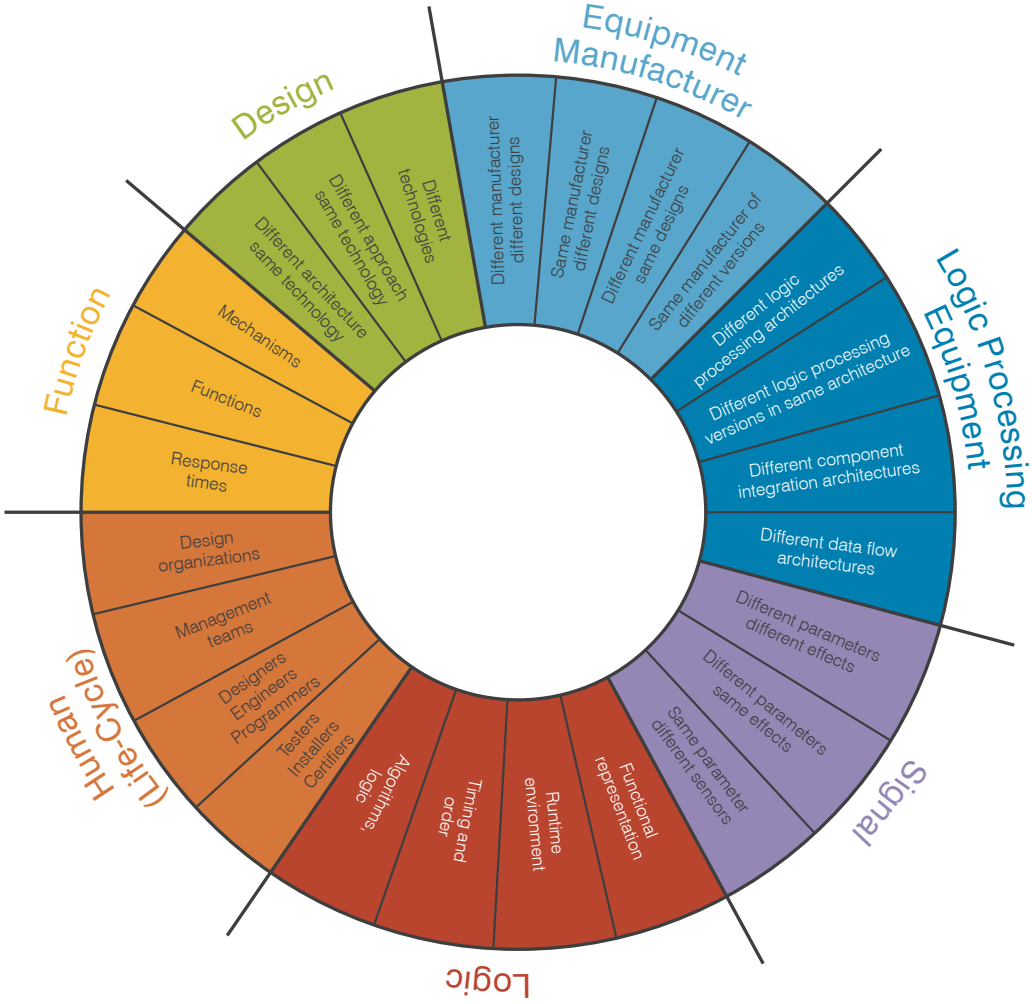
The main differences between NUREG/CR-6303 and NUREG/CR-7007 are:

- The 'human' diversity attribute is designated the 'life-cycle' diversity attribute to account for the fact that the attribute relates to addressing human-induced faults throughout the system development life-cycle process.
- The 'software' attribute, is renamed 'logic' as the former is often misconstrued as only applying to a limited set of programmable devices when the attribute should apply to all programmable devices.
- The 'equipment' attribute is divided into two groups: one group is for the manufacture of equipment, which includes the core criteria described by NUREG/CR-6303; the second group is for the logic processing equipment, which includes the additional criteria in NUREG/CR-6303 for the assessment of computer equipment.

NUREG/CR-7007 [Ref 8] presents the attributes and associated attribute criteria as shown in the Figure on page 11.

The division of the equipment attributes into 'equipment manufacturer' and 'logic processing equipment' is especially interesting as the logic processing equipment criteria appear to be the generic (device agnostic) additional details specified in NUREG/CR-6303. The original aim of the logic processing equipment criteria in NUREG/CR-6303 was to provide clarity to the general equipment criteria.

Figure 1. Diversity Attributes and Associated Criteria Derived from NUREG/CR-6303



For example, a central processing unit (CPU) or a field programmable gate array (FPGA) designed and manufactured by Intel will be fundamentally different in manufacture and design from a CPU designed and manufactured by Motorola. However, it may be difficult to describe the differences between ones designed and manufactured by Intel and AMD. This is because AMD aims to be compatible with Intel designs. This would be considered to be the same design executed by different manufacturers. With this in mind, the different logic processing architectures are already covered by a different manufacturer of a fundamentally different design and therefore there may not be a need to differentiate the equipment diversity attribute from the equipment manufacturer attribute.

Additional confusion is generated by what appears to be repeated criteria across attributes. Is, for example, the design architecture different from the equipment manufacturer's architecture or from the logic processing equipment architecture? The criteria for a given attribute, as defined in NUREG/CR-6303, are given in order of effectiveness. This implies that the most effective criteria may be the only criteria necessary; however, if an implementation is unable to demonstrate adequate diversity for the most effective criteria, then one or presumably several of the less effective criteria may compensate enough.

The spectrum of attributes addresses different types of potential CCF. No single attribute is a panacea and it may not be practical to apply them all. Understanding the relationship of an attribute to the type of CCF it mitigates would allow for a more targeted and quantifiable analysis.

While it is arguable whether or not the changes represented in NUREG/CR-7007 are an improvement, they do highlight the challenge in not only identifying the attributes, but also in defining the criteria associated with those attributes. As digital devices evolve, so too must the attributes, definitions and criteria.

2.2 Upgrading Existing Nuclear Plants

Focused, or even limited, digital I&C licensing has been problematic in upgrading existing plants and this issue has been compounded with the advent of the desire for plant-wide digital I&C systems upgrades.

With smaller systems or single instruments, the argument of same form, fit, and function is easier to make, but as more systems are replaced, along with the desire to carry out a complete modernization of some plants, regulators have become more concerned about CCF.

Digital upgrades, even limited ones, face the following challenges:

- The original design basis and architecture may be lost or is not controlled or updated with the plant maintenance and modernization. This might require costly reverse engineering to re-establish the design basis and architecture prior to any upgrades.
- The application of modern regulatory requirements may invalidate parts of the existing design basis or architecture, and may require more extensive measures than just replacement.
- Even smaller instrument or system upgrades require some sort of 'defence-in-depth' and 'diversity' analysis, which faces the same challenges of regulator guidance and quantification. Furthermore, most diversity guidance was developed within the context of plant protection systems. Guidance that is reasonable for protection systems may be excessive for smaller upgrades, especially for systems where the redundant elements neither see the same input trajectories, nor experience similar operational history, nor communicate with each other; or where the system's inputs and responses to accident conditions are identical, or nearly identical, to surveillance test conditions.
- As whole systems are replaced, the interfaces become more digitalized. With all analog interfaces there are fewer CCF vulnerabilities. As the interfaces are upgraded to digital, the potential for CCF increases.

2.3 Implementation of Regulatory Guidance

All regulatory organizations aim to ensure safety and reliability in the design, construction and operation of nuclear facilities. However, the path to this goal differs depending on the regulatory environment. In particular the approach of defence-in-depth and diversity varies from region to region. For example, implementation of the US approach of defence-in-depth is different from European approaches, and even within Europe there is no generic or harmonized approach for I&C systems.

The variations within the European Union exist, in part, due the initial implementation of the defence-in-depth approach and I&C architecture of the original equipment manufacturers (OEMs). Suppliers from the USA (*e.g.* Westinghouse), Russia (*e.g.* JSC Rusatom Automated Control Systems), France (*e.g.* EDF/Areva) or Germany (*e.g.* Siemens KWU) have supplied nuclear plants to a number of European countries. The European nuclear power providers can be subdivided into countries with and ones without their own OEMs. In countries without their own OEMs (*e.g.* Spain, Switzerland) the supplier provided its overall design philosophy including the defence-in-depth approach at the time the plants were constructed. In order to harmonize the approach to nuclear safety and radiation protection regulation for western European countries, the Western European Nuclear Regulators Association (WENRA) co-operation was formed and its Reactor Harmonization Working Group published its recommended defence-in-depth levels [Ref 10]. Additionally, about the same time, EPRI also provided recommendations on defence-in-depth levels [Ref 11]. However, a comparison of defence-in-depth levels between the IAEA, WENRA and EPRI reveals that there are still minor variations to approaches within Europe.

Implementation of regulatory guidance can often be interpreted, or misinterpreted, in several ways, and the attempt to apply multiple regional regulations to a single product can aggravate the issue.

The application of national regulation to a standardized technology (*e.g.* EPR, AP1000, ABWR) results in the implementation of different I&C architectures to meet the different regulatory guidance. One of the reasons for the variation in defence-in-depth efforts to date is that the problem being solved is not clearly defined, which might be due to ambiguous rules or guidance, as described in Section 2.1.3. Thus, different perceptions of the problem lead to very different I&C architectures.

IAEA levels [Ref 6]		WENRA levels [Ref 10]			EPRI levels [Ref 11]		
Level	Objectives	Level	Objectives	Essential means	Level	Objectives	Associated Plant Conditions
1	Prevention of deviations from normal operation and the failure of items important to safety.	1	Prevention of abnormal operation and failures.	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits.	1	Prevention of abnormal operation and failures.	Normal operation, with plant conditions remaining within normal operating limits.
2	Detection and control of deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.	2	Control of abnormal operation and failures.	Control and limiting systems and other surveillance features.	2	Control of abnormal operation and failures to avoid exceeding reactor trip limits.	Anticipated operational occurrences (AOOs), with plant conditions remaining within reactor trip limits.
3	Escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop.	3a	Control of accident to limit radiological releases and prevent escalation to core melt conditions.	Reactor protection system, safety systems, accident procedures.	3a	Control of event to limit radiological releases and prevent escalation to core melt conditions.	Postulated single initiating events[1].
4	Mitigate the consequences of accidents that result from failure of the third level of defence-in-depth.	3b		Additional safety features[2], accident procedures.	3b		Postulated multiple failure events.
5	Mitigate the radiological consequences of radioactive releases that could potentially result from accidents.	4	Control of accidents with core melt to limit offsite releases.	Complementary safety features[3] to mitigate core melt, management of accidents with core melt (severe accidents).	4	Control of accidents that result in core melt, to limit offsite releases.	Postulated core melt accidents (short- and long-term).

[1] May include AOOs that are not mitigated by the control and limitation systems, but take the plant beyond reactor trip limits and thus mitigated by reactor trip/scram.

[2] The task and scope of the additional safety features of level 3b are to control postulated common cause failure events on 'multiple failure events'.

[3] The task and scope of the complementary safety features of level 4 are on 'provisions to mitigate core melt and radiological consequences'.

As an example, consider three different regulatory regimes applied to a single technology. The different regulatory guidance could lead to the I&C architecture needing to be redesigned. This would result in three fundamentally different I&C architectures to address the different approaches:

- One I&C architecture could require two subsystems in each redundancy that is based on employing functional diversity for the protection logic implemented in the application layer. This approach implies that the application software is the main CCF concern.
- The second architecture could require diverse digital technology to be employed for the reactor trip and engineered safeguard measures to provide vendor diversity between two protection layers. This approach implies that the vendor platform is the main CCF concern.
- The third architecture could require the addition of a non-digital diverse actuation system in parallel with the digital technology used on the traditional reactor trip and engineered safeguard measures. This approach implies that digital technology (or the operating system software layer) is the main CCF concern.

The interpretation and implementation of the degree of diversity results in significant differences in requirements between nuclear regulators, as existing codes and standards do not provide detailed guidelines. For example, the regulating organizations of different countries have different rules on allowing the use of software-based diverse backup systems (defence-in-depth Level 3b) [Ref 12, Sections 7.2 and 7.4].

The topic of diversity continues to be closely associated with CCF concerns. In the past, the focus on CCF was on events initiated by hazards, internal or external, not initiated directly by the I&C systems. Internal and external hazards like fire, air plane crash or flooding are managed by physical separation measures such as employing four redundant I&C systems separated by civil means.

Standards like the German KTA 3501 contend that a bad design, defects in manufacturing or incorrect operation could create a vulnerability that could be triggered and result in a CCF. To mitigate CCF, KTA requires: “For each incident to be controlled by the reactor protection system at least two physically different initiation criteria should be employed.” While in France, diversification is used either technologically to mitigate a hypothetical failure of a system due to a common cause, or functionally to mitigate a hypothetical error in the specification or in the design.

3 Conclusions

The term ‘defence-in-depth and diversity’ does not have any specific or direct organizational definition, but the two terms ‘defence-in-depth’ and ‘diversity’ are identified separately by most organizations. With respect to standard terminology, CORDEL DICTF makes the following recommendations:

- Use of the abbreviation ‘D3’ has the effect of amalgamating two distinct concepts into a single concept to casual readers. The term ‘defence-in-depth’ should be distinguished from ‘diversity’, to emphasize that the two are separate concepts that must work together.
- The definitions used by the IAEA for the two terms ‘defence-in-depth’ and ‘diversity’ appear to be the most practical as they do not conflict with other organizational definitions. All relevant organizations should adopt these definitions.
- The current diversity attributes used by most organizations appear to be those defined by NUREG/CR-6303. NUREG/CR-7007 supports the conclusion that these attributes should be revisited, updated, and modernized. Well-defined attributes support clear completion criteria for ‘defence-in-depth’ and ‘diversity’ analysis and should be a topic for future work.
- The terms ‘levels of defence’ and ‘echelons of defence’ have different definitions and add to the complexity and confusion of the application of services and products in a globalized industry. The IAEA uses ‘levels of defence’ and this term is widely accepted and understood by organizations using the term ‘echelons of defence’. It would be beneficial for the different regulatory organizations to adopt the term ’levels of defence’ and discontinue the use of ‘echelons of defence’.
- The IAEA levels of defence provide a standard or base that could be used by vendors and augmented as needed for specific regional regulators. The WENRA and EPRI proposed levels of defence are examples where the IAEA levels have been augmented. Adoption of the common defence principles by national regulators would reduce confusion and the likelihood that I&C designs would require significant re-work for regional acceptance.

While the principles and approach of different regulatory organizations may vary, the fundamental goal of safety and reliability are the same. There is recognition by regulators that modernization and clarity is required for defence-in-depth and for diversity, as well as for techniques to mitigate CCF concerns associated with the I&C architecture in nuclear plants. To that end, it is recommended that CORDEL DICTF members participate in activities centred around:

- Quantification of diversity attributes, the interaction of attributes with each other (*i.e.* the effective priorities of attributes), and the removal of subjectivity so that the completion criteria can be identified and agreed to.
- Different defence-in-depth approaches between regulating authorities. These can result in costly redesign of I&C architectures, but could be avoided through the adoption of universal definitions and requirements.
- Clarification of rules for mitigation of CCF. This includes: the use of graded approaches to differentiate between main line protection systems and end

devices with some embedded digital features; and techniques, or a combination of techniques, that can be applied to digital instruments and devices to ensure reliability and mitigate credible CCFs. Additionally a preferred regulatory solution is to introduce diversity into I&C systems design to guard against digital CCF. However, the lack of clear criteria on how to define sufficient diversity has led to more complex I&C architectures. The trend has been towards lengthy and more difficult reviews for the treatment of digital CCF vulnerabilities and I&C system architectures because of the subjective definition of digital CCF vulnerabilities and the lack of clear acceptance criteria for diversity strategies. Improvement in the treatment of digital CCF is needed to reverse the trend of increased I&C system architecture complexity and longer regulatory reviews.

Two additional CORDEL DICTF reports are recommended on defence-in-depth and diversity:

- The quantification of defence-in-depth and diversity analysis remains a challenge largely because the extent and conditions for completion of an analysis are unbounded, subjective, incomplete or ambiguous. While the criteria are reasonably well defined, they are applied in a fairly subjective manner. More work is needed to evaluate the interaction between levels of defence-in-depth and particularly the manner in which diversity criteria interact with each other (to provide evidence on diversity) so that the completion criteria can be recognized and agreed to by those performing the analysis.
- To better understand the challenges of regulatory variations, a report dedicated to documenting the different approaches is needed.

While the challenges of upgrading existing nuclear plants have been touched upon, this is a complex topic that requires further exploration and will be covered by the reports on I&C modernization.

4 References

1. CORDEL DICTF 2014-2016 Outlook, Cooperation in Reactor Design Evaluation and Licensing Digital Instrumentation and Control Task Force, World Nuclear Association, September 2014

2. Safety Classification for I&C in Nuclear Power Plants – Current Status & Difficulties, Cooperation in Reactor Design Evaluation and Licensing Digital Instrumentation and Control Task Force, World Nuclear Association, September 2015

3. Safety Classification for I&C in Nuclear Power Plants: Comparison of Definitions of Key Concepts, Cooperation in Reactor Design Evaluation and Licensing Digital Instrumentation and Control Task Force, World Nuclear Association, September 2017

4. IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, International Atomic Energy Agency, June 2016

5. Appendix F of ISO 13849-1:2006, Safety Machinery – Safety-Related Parts of Control Systems, International Organization for Standardization, November 2006

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

7. NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, U.S. Nuclear Regulatory Commission, December 1994

8. NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, February 2010

9. IEEE Std 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Standards Association, 2003

10. Safety of new NPP designs, Study by Reactor Harmonization Working Group RHWG, Western European Nuclear Regulators Association, March 2013

11. Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environments, Electric Power Research Institute, November 2014

12. Common Position on the Treatment of Common Cause Failure Caused by Software Within Digital Safety Systems, MDEP Generic Common Position No DICWG-01, Multinational Design Evaluation Programme, June 2013

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

Inconsistencies in the definitions of the concepts of 'defence-in-depth' and 'diversity' can lead to significant challenges in the design, licensing and cost of nuclear power facilities. *Defence-in-Depth and Diversity: Challenges Related to I&C Architecture*, produced by the World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing Working Group, reviews these challenges and provides recommendations to address them. This report is the first in a series on *Defence-in-Depth and Diversity*, and builds upon the work carried out in the series of reports on *Safety Classification for I&C Systems in Nuclear Power Plants*.

The World Nuclear Association is the international organization supporting the people, technology and enterprises that comprise the global nuclear energy industry. Its membership encompasses uranium mining, conversion, enrichment and fuel fabrication; reactor vendors; major nuclear engineering, construction, and waste management companies; and the majority of the world's nuclear generation.