

# **Nuclear Energy Agency’s Consensus Position on the Common Cause Failure in Digital Instrumentation and Control Systems – Evaluation Framework**

**Mr. Ismael L. Garcia, P.E., CISSP<sup>1\*</sup>**

<sup>1</sup>Nuclear Regulatory Commission, Rockville, MD

## **ABSTRACT**

The Nuclear Energy Agency (NEA) has agreed that a consensus position on the treatment of Common Cause Failure (CCF) within and between digital Instrumentation and Control (I&C) systems important to safety is warranted given the increased use of digital I&C in new reactor designs and upgrades on operating plants, the safety implications of this use, and the need to develop a common understanding from the perspective of regulatory authorities. The evaluation framework discussed in this paper was derived from the ongoing efforts for developing a consensus position on this topic being performed by a Task Group under the auspices of the NEA Committee on Nuclear Regulatory Activities (CNRA) Working Group on New Technologies (WGNT). The evaluation framework discussed herein provides information to be used to develop regulatory guidance on relevant aspects: (1) for the design of digital I&C systems important to safety to cope with the potential effects of CCF; (2) for the analysis of the design to ensure that CCF do not compromise safety; and, (3) for avoiding faults throughout the lifecycle of digital I&C systems important to safety, which therefore reduces CCF.

*Keywords:* failure, digital, instrumentation, regulatory, safety, systems

## **1. INTRODUCTION**

CCF is an important safety concern for nuclear power plants. CCF can lead to a loss of safety in many ways including, but not limited to: (1) Placing a nuclear plant in an un-analyzed state with respect to its safety analysis, for example creating a new initiating event; (2) Increasing the frequency of an existing initiating event; or, (3) Challenging the ability of systems important to safety to provide their intended functions, for example failing to mitigate a failure leading to a hazard.

This important safety concern has existed prior to the introduction of digital I&C systems. Despite the improvements associated with the use of digital I&C systems in nuclear power plants, inherent complexity and coupling within and between these systems increases the concern.

CCF is a cross-cutting safety issue that can affect multiple disciplines. Adequate resolution to this issue may necessarily involve personnel with expertise in digital I&C, safety analysis, human factors, electrical, probabilistic safety assessment, etc. Therefore, evaluating CCF necessitates a multi-disciplinary approach to ensure that the potential consequences of CCF on plant safety are fully understood and accounted for. The evaluation framework documented herein is intended to provide guidance to regulators.

---

\* Ismael.Garcia@nrc.gov

This paper documents an evaluation framework on CCF for digital I&C systems important to safety. This paper was derived from the ongoing work being performed by the NEA/CNRA WGNT.

## 2. DISCUSSION

### 2.1. Definition of Terms

The following definitions are specific to this paper:

**CCF:** Failures of two or more structures, systems or components due to a single event or cause [1].

**Note:** CCF includes, but is not limited to, common mode failure in which the structures, systems or components fail in the same way (although they may not be in close proximity).

**Diversity:** The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to prevent the occurrence and/or mitigate the effects of CCF [1].

**Note:** For example, a diverse backup system may provide a diverse means in the implementation of one or more of the three fundamental safety functions: (1) Control of reactivity; (2) Removal of heat from the nuclear fuel; (3) Confinement of radioactive material [2].

**Error:** Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretical value or condition [3].

**Failure:** Loss of the ability of a structure, system, or component to function within acceptance criteria [1].

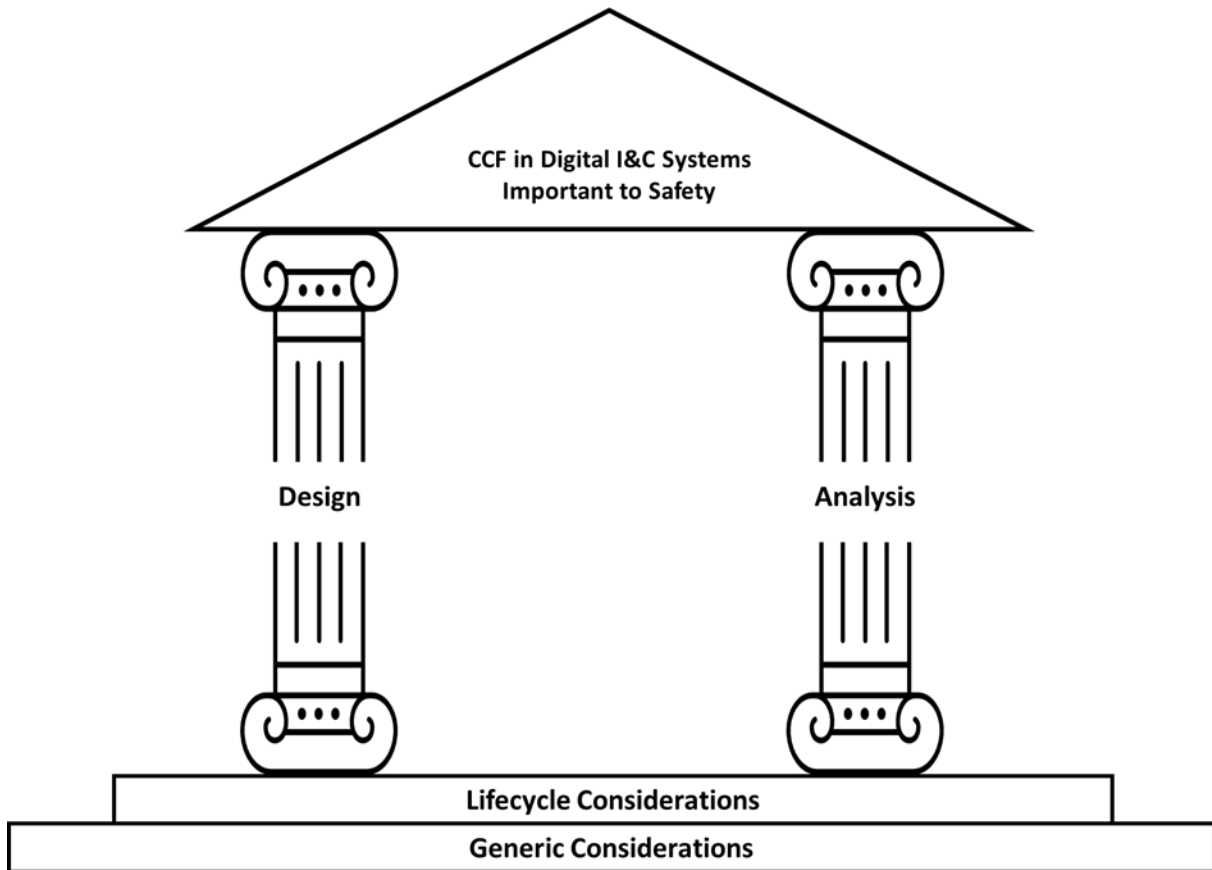
**Fault:** Defect in a hardware, software or system component [3]. An error may lead to a fault, a fault may lead to a failure, and failure may lead to a hazard, and a hazard may lead to harm.

**Postulated Initiating Event (PIE):** An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

**Note:** The primary cause of a PIE may be credible equipment failures and operator errors (both within and external to the nuclear power plant) or human induced or natural events [1].

**Systems important to safety:** Systems that are part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public [1].

## 2.2 Evaluation Framework



**Figure 1. CCF in Digital I&C Systems Important to Safety – Evaluation Framework.**

Fig. 1 above shows the evaluation framework intended to apply to all digital I&C systems important to safety at nuclear power plants, both hardware and software. As shown in Fig. 1, the evaluation framework relies on two key pillars, design and analysis, and foundational concepts in the form of lifecycle and generic considerations. The following sections discuss the details associated with this evaluation framework.

### 2.2.1. Scope

This evaluation framework applies to CCFs both within and between digital I&C systems important to safety. In these systems, example causes of CCF include: (1) Systematic faults in software and hardware common to different parts of the I&C being triggered concurrently as they experience similar input conditions; (2) Cyber security threats and vulnerabilities; (3) Environment stress from outside of the digital I&C system to all redundant channels within a system or to multiple systems; (4) Faults in digital I&C supporting systems (e.g., heating, ventilation, and air conditioning, electrical systems) including any digital equipment used within those systems; (5) Propagation of unwanted behavior, such as corrupted data which is transferred from one faulty channel to other redundant channels within a system, or from one system to

other systems; and, (6) Improper operation and maintenance actions, for example, due to inadequacy in the system design or failing to incorporate design requirements in the maintenance process.

This evaluation framework provides information to be used to develop regulatory guidance on relevant aspects: (1) for the design of digital I&C systems important to safety to cope with the potential effects of CCF; (2) for the analysis of the design to ensure that CCF do not compromise safety; and, (3) for avoiding faults throughout the lifecycle of digital I&C systems important to safety, which therefore reduces CCF.

This evaluation framework considers CCF within and between digital I&C systems important to safety. Member countries may apply different methods to prevent or mitigate CCF. This evaluation framework accounts for both deterministic and risk-informed approaches.

Hardware includes centralized and non-centralized digital I&C devices (e.g., field devices, digital devices of limited functionality) as well as conventional electronics. Software includes firmware and logic in any form, including but not limited to: (1) Application and platform software including operating systems; (2) Custom and pre-existing software; (3) Supporting data; (4) Programmable logic devices (e.g., field programmable gate arrays); (5) Intellectual Property cores; and, (6) Exchange of information via communication channels.

Software tools for activities such as design and maintenance are also within the scope of this consensus position.

### **2.2.2. Generic considerations**

The nuclear power plant, including the I&C architecture, should be designed so that CCF do not compromise safety. To achieve this objective, the overall requirements definition, design, manufacture, operation, maintenance, and modification of digital I&C systems important to safety should take due account of CCF.

The requirements for consideration of CCF within and between digital I&C systems important to safety should be derived from the plant requirements. Therefore, the digital I&C specialists should engage with other technical disciplines to understand the requirements for consideration of CCF because this is a cross-cutting safety issue.

The susceptibility of the overall I&C architecture and I&C systems important to safety to CCF and its consequences should be analyzed as an input to the design requirements. The final design should also be analyzed to determine that CCF do not compromise safety. The solution to cope with CCF need not always be addressed by I&C. It may be more effective to use alternatives to I&C in the first place; for example, relying on nuclear power reactor design characteristics such as inherent, passive, or other innovative means of avoiding or protecting against some faults in the plant.

Documentation should be provided by the licensee to demonstrate how the design and analysis of the overall I&C architecture and I&C systems important to safety address CCF.

### **2.2.3. Design considerations**

CCF should not compromise the achievement of defense in depth by the overall I&C architecture design. Design simplicity, including reducing any unnecessary functionality and interconnectivity to a level that allows systems to be analyzable, verifiable, and testable, should be implemented to reduce the potential for systematic faults that may result in CCFs. Where activities such as design and maintenance are dependent

on the use of software tools, then the potential for CCF should be considered and addressed. Cyber security threats and vulnerabilities should be considered and addressed as a potential for CCF of the I&C architecture and the I&C systems important to safety.

The design should also consider operation and maintenance requirements, for example definition of test intervals and calibration values, which if inadequately specified could lead to CCF. Human factors should be considered and addressed to avoid operator actions causing CCF in subsequent lifecycle stages, such as operations and maintenance.

Provisions should be included to account for environmental stresses that may result in CCF. Environmental stresses may include, but not be limited to seismic, vibratory, electromagnetic interference, electrical surge, and temperature/humidity. These provisions include but are not limited to a high-quality equipment qualification program, and the use of design features such as shielding and mechanical isolation for seismic events. Provisions should also be included to account for internal and external hazards that may result in CCF. Hazards may include but are not limited to fires and floods. These provisions include but are not limited to independence by employing physical separation with physical barriers and isolation.

A CCF may result from inadequate design of supporting systems (e.g., heating, ventilation, and air conditioning, electrical systems) to the digital I&C systems important to safety. These supporting systems should be designed so that they do not compromise the provisions for CCF of the systems they support.

Where it is necessary to prevent or mitigate CCF due to systematic faults within and between digital I&C systems important to safety, diversity is the primary means for doing so. Hence, appropriate diversity should be provided in these cases. The I&C design should be informed by the results of the defense-in-depth and diversity assessment (see Section 2.2.4 below).

The following documents could be used in conjunction with the design considerations of this evaluation framework: (1) GCP DICWG-02, “Common Position on Software Tools for the Development of Software for Safety Systems;” [4]; (2) WGDIC CP-04, “Consensus Position on Data Communication Independence;” [5]; (3) GCP DICWG-06, “Common Position on Principle on Simplicity in Design;” [6]; (4) WGDIC CP-08, “Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants;” [7] and, (5) GCP DICWG-09, “Common Position on Safety Design Principles and Supporting Information for the Overall I&C Architecture.” [8]

#### **2.2.4. Analysis considerations**

For each postulated initiating event within scope of the safety analysis, the required response of the overall I&C architecture and digital I&C systems important to safety, including any supporting systems, should be analyzed to determine that the plant can cope with relevant CCF. Such safety analysis is typically undertaken by specialists other than I&C; however, I&C specialists should ensure that the analysis is informed by sufficient information and understanding of the I&C. The contribution of software tools to CCF should be considered and addressed as part of the analysis.

To ensure that relevant CCF have been addressed, the vulnerabilities to CCF and foreseeable CCF mechanisms need to be adequately identified. An assessment of defense in depth and diversity, including failure modes and undesired behaviors, of the overall I&C architecture and digital I&C systems important to safety, including any supporting systems, should be performed to achieve this objective. This assessment should be informed by and feed into the plant safety analysis. The scope and rigor of the defense-in-depth and diversity assessment can be graded according to the plant safety analysis. The assessment may be qualitative and/or quantitative, and grading may be according to the risk or consequences of a fault or the safety class of the system.

The results of the defense-in-depth and diversity assessment on the final I&C design should demonstrate that CCF is reasonably prevented or mitigated, or is not risk significant. Thus, the I&C design should be modified to address any deficiencies identified in the defense-in-depth and diversity assessment, where this is necessary to satisfy the stated objective. This may be an iterative process between assessment and design. The level of technical justification should be according to the risk significance of the CCF.

In some cases, manual action may be used as an alternative to automatic action of the I&C to mitigate the effects of CCF. If manual action is credited, then the role of I&C in implementing the action should be understood and the potential for CCF should still be analyzed. The human response should be feasible within the time available for mitigating the effects, and it should be clear how I&C facilitates the manual action to be credited.

Residual risk accepted as a result of the cyber security risk management process should be sufficiently documented and demonstrated not to compromise the conclusions of the CCF analyses discussed herein.

The following documents should be used in conjunction with the analysis considerations of this evaluation framework: (1) GCP DICWG-02, “Common Position on Software Tools for the Development of Software for Safety Systems;” [4]; (2) GCP DICWG-10, “Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems;” [9] and, (3) GCP DICWG-13, “Common Position on Spurious Actuation.” [10]

### **2.2.5. Lifecycle considerations**

This portion of the evaluation framework is intended to provide guidance to avoid faults throughout the lifecycle of digital I&C systems important to safety, which therefore reduces CCF. This includes the following lifecycle phases: (1) Overall requirements definition; (2) Design; (3) Manufacture; (4) Operation; (5) Maintenance; and, (6) Modification.

A fault in digital I&C systems important to safety can be introduced at any point during the lifecycle. For each of the lifecycle phases listed above, the applicant/licensee should use high-quality processes as defined by the nuclear standards, practices, and regulatory framework applicable to the country.

Operations and maintenance activities could introduce faults within or between digital I&C systems important to safety. Operations and maintenance-induced faults should be prevented, for example via well-defined and established procedures that ensure adequate traceability of the requirements for preventing or mitigating CCF from the design documentation into the maintenance procedures, and administrative controls (e.g., equipment change controls).

Any change at any phase of the lifecycle should be reviewed to determine its potential effects on CCF, such as a revision of a device with the same model number introducing software for the first time. Any change that has the potential to affect CCF should trigger a review of the relevant analyses (discussed in the Analysis Considerations section above) to ensure they remain valid.

Cyber threats are continuously changing; therefore, cyber security risks should be managed throughout the lifecycle to maintain adequate protection against CCF. This requires constant vigilance, particularly during operations and maintenance.

The following documents should be used in conjunction with the lifecycle considerations of this consensus position: (1) GCP DICWG-03, “Common Position on Verification and Validation throughout the Life Cycle of Digital Safety Systems;” [11] and, (2) WGDIC CP-08, “Consensus Position on the Impact of Cyber

Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants.” [7]

### 3. CONCLUSIONS

The evaluation framework discussed herein provides information to be used to develop regulatory guidance on relevant aspects: (1) for the design of digital I&C systems important to safety to cope with the potential effects of CCF; (2) for the analysis of the design to ensure that CCF do not compromise safety; and, (3) for avoiding faults throughout the lifecycle of digital I&C systems important to safety, which therefore reduces CCF.

### ACKNOWLEDGMENTS

This paper was derived from the ongoing work being performed by a Task Group under the auspices of the NEA/CNRA WGNT, which I have the honor and privilege to lead. For additional information concerning the NEA/CNRA WGNT visit: [https://www.oecd-nea.org/jcms/pl\\_88343/working-group-on-new-technology-wgnt](https://www.oecd-nea.org/jcms/pl_88343/working-group-on-new-technology-wgnt).

(Note: The goal of the NEA/CNRA WGNT is not to independently develop new regulatory standards. As such, the technical work develop by the NEA/CNRA WGNT is not legally binding and do not constitute additional obligations for the regulators or the licensees. Instead, the technical work resulting from the NEA/CNRA WGNT constitutes guidelines, recommendations, or assessments that the NEA/CNRA participants agree are good to highlight during their safety reviews of operating and new reactors. The development of technical guidance for ensuring the potential for CCF resulting from systematic faults in digital I&C systems important to safety at nuclear power plants follows the WGNT examination of the regulatory requirements of the participating members and of relevant industry standards and International Atomic Energy Agency (IAEA) documents.)

### REFERENCES

1. “IAEA Nuclear Safety and Security Glossary,” <https://www.iaea.org/publications/15236/iaea-nuclear-safety-and-security-glossary> (2022).
2. “IAEA-TECDOC-1848, Criteria for Diverse Actuation Systems for Nuclear Power Plants,” <https://www.iaea.org/publications/12367/criteria-for-diverse-actuation-systems-for-nuclear-power-plants> (2018).
3. “IEC 61513: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems,” [https://global.ihs.com/doc\\_detail.cfm?document\\_name=IEC%2061513&item\\_s\\_key=00378381](https://global.ihs.com/doc_detail.cfm?document_name=IEC%2061513&item_s_key=00378381) (2011).
4. “MDEP Generic Common Position DICWG-02 - Common Position on Software Tools for the Development of Software for Safety Systems,” [https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-02-Software\\_Tools\\_Ver\\_C.pdf](https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-02-Software_Tools_Ver_C.pdf) (2013).
5. “NEA/CNRA/R(2018)2 - Consensus Position on Data Communication Independence [CP-04],” [https://www.oecd-nea.org/jcms/pl\\_19870/consensus-position-on-data-communication-independence-cp-04?details=true](https://www.oecd-nea.org/jcms/pl_19870/consensus-position-on-data-communication-independence-cp-04?details=true) (2019).
6. “MDEP Generic Common Position DICWG-06 – Common Position on Principle on Simplicity in Design,” [https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-06\\_Simplicity\\_in\\_Design\\_Ver\\_C.pdf](https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-06_Simplicity_in_Design_Ver_C.pdf) (2013).

7. “NEA/CNRA/R(2021)2 - Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants [CP-08],” [https://www.oecd-nea.org/jcms/pl\\_75241/consensus-position-on-the-impact-of-cyber-security-features-on-digital-instrumentation-and-control-systems-important-to-safety-at-nuclear-power-plants-cp-08](https://www.oecd-nea.org/jcms/pl_75241/consensus-position-on-the-impact-of-cyber-security-features-on-digital-instrumentation-and-control-systems-important-to-safety-at-nuclear-power-plants-cp-08) (2022).
8. “Multinational Design Evaluation Programme (MDEP) Generic Common Position DICWG-09 – Common Position on Safety Design Principles and Supporting Information for the Overall I&C Architecture, 2015,” [https://www.oecd-nea.org/mdep/common-positions/GCP-09\\_Overall\\_IC\\_Architecture\\_final.pdf](https://www.oecd-nea.org/mdep/common-positions/GCP-09_Overall_IC_Architecture_final.pdf) (2015).
9. “MDEP Generic Common Position DICWG-10 - Common Position on Hazard Identification and Controls for Digital Instrumentation and Controls Systems,” [https://www.oecd-nea.org/mdep/common-positions/MDEP\\_GCP-DICWG-10\\_HazardIDandControl.pdf](https://www.oecd-nea.org/mdep/common-positions/MDEP_GCP-DICWG-10_HazardIDandControl.pdf) (2016).
10. “MDEP Generic Common Position DICWG-13 – Common Position on Spurious Actuation,” <https://www.oecd-nea.org/mdep/common-positions/cp-dicwg-13.pdf> (2017).
11. “MDEP Generic Common Position DICWG-03 – Common Position on Verification and Validation throughout the Life Cycle of Digital Safety Systems,” [https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-03\\_VV\\_Ver\\_H.pdf](https://www.oecd-nea.org/mdep/common-positions/gcp-dicwg-03_VV_Ver_H.pdf) (2013).