MDEP
Technical Report
TR-DICWG-01

DIC Working Group

Technical Report on the Relational Structure of the Digital Instrumentation and Controls Working Group (DICWG) Common Positions

Participation

Regulators and TSOs involved in the MDEP working group discussions:	CNSC (Canada), NNSA (China), STUK (Finland), IRSN (France), AERB (India), NRA (Japan), KINS (Korea), FSUE VO "Safety" (Russia), NNR (South Africa), SSM (Sweden), FANR (UAE), ONR (UK), NRC (USA)
Regulators and TSOs which support the present report:	CNSC (Canada), NNSA (China), STUK (Finland), IRSN (France), AERB (India), NRA (Japan), KINS (Korea), FSUE VO "Safety" (Russia), NNR (South Africa), SSM (Sweden), FANR (UAE), ONR (UK), NRC (USA)
Compatible with existing IAEA related documents:	Yes

TABLE OF CONTENTS

1. SUMMARY

This document describes the relational structure between the MDEP DICWG common positions (CPs), as well as addressing their scope, content and how they relate to the mission of DICWG.

2. CONTEXT

Unlike other technical disciplines, digital instrumentation and controls (DI&C) is a field which reflects the constant evolution in electrical and electronics technologies. The continual evolution in DI&C technology presents challenges for power plant operators, designers, suppliers, as well as the regulators. Contemporary regulations and guidance can be made either obsolete or insufficient as technology changes push the boundaries of what was originally considered or completely change the assumptions that were the foundation when they were first enacted. As such, producing timely and practical guidance is essential to the safe operation of nuclear plants. The goal of MDEP is not to independently develop new regulatory standards. The overall philosophy of MDEP DICWG is to use the collective knowledge and experiences from nuclear power regulatory organisations from around the world to effectively and efficiently create CPs to address current and future DI&C topics of concern to its member countries.

The CPs provide an effective and efficient means to convey a general framework that includes input from both member countries and international standards organisations. Each CP produced by DICWG represents an agreed upon approach to address the specific topic for which it has been created. CPs are not legally binding and do not constitute additional obligations for the regulatory organisations or the licensees but are guidelines, recommendations or assessments that the MDEP participants agree are good to highlight during their safety reviews of new reactors. MDEP member countries may decide to implement the CPs through their own national regulatory processes.

The topics that are addressed in current and upcoming CPs reflect a wide variety of technical topics that are challenging in the DI&C field and oftentimes require a holistic approach to reach resolution. The topics for CPs are selected based upon the use of DI&C in new reactor designs, issues of concern arising from regulatory activities in member countries, safety implications, or the general need to develop a common understanding of the topic. DICWG provides a forum for nuclear regulatory organisations from around the world that is vital in demonstrating to the industry that regulatory organisations are actively engaged with these topics and understand their significance.

3. MDEP DICWG COMMON POSITIONS

The focus of the CPs is to establish an international regulatory outlook on a given DI&C topic. The CPs expound upon generally agreed DI&C design principles, with a specific focus on DI&C safety systems while considering the importance of lower safety class DI&C systems. Table1-1 below provides a summary of the content within each of the published CPs and CPs under development.

Table 1-1: MDEP DICWG CPs

CP#	CP Title	Summary of Content
01	CP on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems.	This CP addresses the topic of common cause failures of software-based, safety DI&C systems. The CP directs readers to consider the effects of software common cause failures of plant components within the safety analysis and that 'Diversity' can be an effective means to reduce the potential effects of software common cause failure.
02	Software Tools.	This CP addresses software tools used to design and develop DI&C systems based on the ability of software tools to affect the integrity and reliability of DI&C products. The CP establishes guidelines for the usage and limitations of software tools and the applicability of software tools to the overall DI&C system life cycle. This CP does not apply to software tools that support programmable logic devices (e.g. FPGAs).
03	Verification and Validation throughout the Life Cycle of Safety Systems Using Digital Computers.	This CP sets forth basic guidelines regarding V&V activities for DI&C safety systems throughout the system's lifecycle. It addresses a plant's overall V&V approach, as well as specific concerns to digital computers such as pre-developed software V&V.
04	Communication Independence.	This CP focuses on data communications independence between safety systems and between systems of differing safety classification. This CP provides guidelines for specific areas of interest such as communications between safety divisions, between systems of differing safety classification and command prioritization.
05	Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems.	The development lifecycle of HDL-based programmable devices (e.g. FPGAs) is the primary subject of this CP and comes as a result of the proliferation of HDL-based devices in the nuclear industry and their similarity to traditional software.

CP#	CP Title	Summary of Content
06	Simplicity in Design.	Complexity in DI&C design can lead to more faults in the design, difficulty in detecting and correcting faults as well as increasing licensing uncertainty. This CP outlines how simplicity in DI&C design and alleviate these concerns while making designs more straightforward and easier to understand.
07	Selection and Use of Industrial Digital Device of Limited Functionality.	This CP addresses digital devices, of limited functionality, that can be found embedded in plant components such as pumps and breakers. These devices are not necessarily designed for use in nuclear applications and this CP provides criteria for their selection and usage.
08	Impact of Cyber Security Features on DI&C Safety Systems.	This CP provides guidelines on aligning cybersecurity measures with DI&C system of the highest safety classification. The goal of the CP is to ensure that safety measures and cybersecurity measures do not adversely impact each other.
09	Safety Design Principles and Supporting Information for the Overall DI&C Architecture.	As modern DI&C systems become more integrated and perform more functions, it is critical to implement safe design principles and documentation to ensure safe operation. This CP sets guidelines for safety design principles and supporting information that should be demonstrated for the entire DI&C architecture of a plant.
10	Hazard Identification and Controls for Digital Instrumentation and Control Systems.	This CP lays the foundation for addressing hazards internal and external to DI&C systems. The CP outlines a systematic approach for determining the hazards associated with DI&C system and the controls to address those hazards.
11	DI&C System Pre-installation and Initial On-site Testing.	Pre-installation and initial onsite testing can confirm that DI&C systems comply with their requirements at different phases of a system's life cycle. This CP sets forth guidelines regarding these types of testing for DI&C systems.
12	Use of Automatic Testing in DI&C Systems as part of Surveillance Testing.	Automated fault detection features are a common aspect of modern DI&C systems and can provide early detection of system issues in advance of surveillance testing, therefore allowing for a reduction in the need for some manually surveillance activities while maintaining safe operation. This CP addresses automated testing feature alignment with DI&C system implementation and performance.

CP#	CP Title	Summary of Content
13	Spurious Actuation (In development).	This CP continues DICWG's focus on hazard assessment and controls, focusing on a specific hazard referred to as spurious actuation. Spurious actuation of plant equipment (regardless of safety class) can potentially place a plant in an un-analysed state and this CP explores controlling for this hazard from a DI&C perspective. This CP also ties into CP01.

The CPs relational structure is based on the following categories (as depicted in Figure 1), with regard to their focus:

- I&C Architecture and Design
- Quality and Validation and Verification (V&V)
- Hazards and Reliability

The working group considers these categories as important and inter-related factors[1] to address during the design and implementation of I&C systems and equipment. Designers would need to factor the: (1) I&C architecture and design features; (2) quality and V&V of both hardware and software; and (3) hazards and reliability associated with the system and equipment being developed.

[1] It is important to note that these are not the only factors to consider during the design and implementation of I&C systems and equipment. Additional factors may be considered in the future in support of the continual evolution in the DI&C technology and its associated challenges.

	I&C Architecture and Design	Quality and V&V	Hazards and Reliability
CP 01 (CCF)			✓
CP 02 (Software tools)		✓	✓
CP 03 (V&V)		✓	✓
CP 04 (Comm. Independence)	✓		✓
CP 05 (Hardware Description Language)	✓		
CP 06 (Simplicity)	✓		
CP 07 (Industrial Digital Device)	✓		
CP 08 (Impact of Cyber Security)	✓		✓
CP 09 (Overall Architecture)	✓		
CP 10 (Hazard ID. & Control)			✓
CP 11 (Pre-installation & initial testing)		✓	
CP 12 (Auto. test as Surveillance test)	✓	✓	✓
CP 13 (Spurious Actuation)			✓

Figure 1: MDEP DICWG CPs relationships

The above categorisation provides the framework for current and future development of CPs. DI&C architecture and systems design, as well as consideration for the Quality and V&V form a large area of interest for DICWG. The CPs that fall under these categories reflect topics that are germane to these considerations. The shift in focus to hazards and reliability provides an improved conceptual framework to identify conditions in modern DI&C systems that might compromise the defence-in-depth or the strategy for diversity of the plant design. Considering a hazards-based approach better accounts for current technological trends as well as potential future technologies and design techniques. It also provides a holistic means to account for a wider array of hazards beyond those that are internal to the DI&C system. CPs under this category reflect these considerations as well. Future CPs should follow this relational structure as it provides a clear framework for which to focus future efforts.

The CPs are aligned with IAEA SSG-39 “Design of Instrumentation and Control Systems for NPPs” as well as with other international standards. Table 1-2 demonstrates how each of the published CPs aligns with international standards.

Table 1-2: Harmonisation of CPs with International Standards

CP#	Standard Organisation(s)	Standards Harmonised with CPs
01	IEEE IEC IAEA	IEEE Standard (Std) 7-4.3.2, "Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," Clause 5.16 and Annex B. IEC 61513, "Nuclear Power Plants Instrumentation and Control Important to Safety-General Requirements for Systems." IEC 60880, "Instrumentation and Control Systems Important to Safety. Software Aspects for Computer-based Systems Performing Category A functions." SSG-39, "Design of Instrumentation and Control Systems for NPPs."
02	IEEE IEC IAEA	IEEE 7-4.3.2, Clause 5.3.2. IEC 61513 and IEC 60880. SSG-39.
03	IEEE IEC IAEA	IEEE 7-4.3.2, Clause 5.3.3. IEC 61513 and IEC 60880. SSG-39.
04	IEEE IEC IAEA	IEEE 7-4.3.2, Clauses 5.5.4, 5.6, and Annex E. IEC 61513 and IEC 60880. SSG-39.
05	IEEE IEC IAEA	IEEE 7-4.3.2, as a whole. IEC 61513 and IEC 60880. SSG-39.
06	IEEE IEC IAEA	IEEE 7-4.3.2, Clause 5.18. IEC 61513 and IEC 60880. SSG-39.
07	IEEE IEC IAEA	IEEE 7-4.3.2, Clause 5.17. IEC 62671, "Nuclear Power Plants-Instrumentation and Control Important to Safety-Selection and Use of Industrial Digital Devices of Limited Functionality." SSG-39.
08	IEEE	IEEE 7-4.3.2, Clause 5.9.3.

CP#	Standard Organisation(s)	Standards Harmonised with CPs
	IEC IAEA	IEC 62645, "Nuclear Power Plants-Instrumentation and Control Systems-Requirements for Security Programmes for Computer- Based Systems." SSG-39.
09	IEEE IEC IAEA	IEEE 7-4.3.2 as a whole. IEC 61513 SSG-39.
11	IEEE IEC IAEA	IEEE 7-4.3.2, Clause 5.3. IEC 61513 and IEC 60880. SSG-39.
12	IEEE IEC IAEA	IEEE 7-4.3.2, Clauses 5.5.3 and 5.18. IEC 61513 and IEC 60880. SSG-39.

4. FUTURE DEVELOPMENT

As stated previously, the DI&C field is an evolving area and there remains a significant amount of work that can be addressed by DICWG, in terms of legacy items and emerging topics based on new technologies. As part of the working group's mission, DICWG continues to pursue areas of interest including, but not limited to, the following:

- Hazards in DI&C Systems: DICWG recognises that the focus of evaluating DI&C systems must shift to a hazards-based approach (expanding on the work of CP10) due to their potential complexity and integration risks. In addition to hazards such as spurious actuation, DICWG will pursue other areas such as DI&C interface requirements, including organisational and technical interfaces.
- Technology: Building upon prior work, DICWG will continue to pursue emerging topics regarding DI&C technology.

5. CONCLUSION

In conclusion, the CPs reflect the DICWG's efforts to address the current and emerging technical challenges in the DI&C field. As the DICWG has matured as a group, the CPs have also seen further refinement in terms of content and applicability to prior work efforts. In support of the continual evolution in the DI&C technology and its associated challenges, the DICWG will continue to assess any gaps not being addressed by contemporary regulations and guidance. Future CPs will allow

breaching those gaps while maintaining their relational structure as discussed herein. Further, the working group will continue to assess published CPs for continued relevance and adequacy, and revising accordingly.