MDEP
DICWG
Programme Plan
2017 - 2018

Related to: Digital Instrumentation and Control Working Group Activities

DICWG Programme Plan
For 2017 and 2018

MDEP DICWG Programme Plan

1. MDEP DICWG Long-Term Goals

- Develop Generic Common Positions (GCP) concerning current and emerging technical challenges in the digital instrumentation and control (DI&C) field.
- Make a substantial influence toward harmonization of DI&C standards of significance.
- Increase collaboration, cooperation, and knowledge transfer among members and with other stakeholders to achieve the goals above.

Actions to Reach Long-term Goals

- Identify, prioritize, and update issues of significance from the members and other stakeholders.
- Develop common positions among members for issues of significance, which may be based on a review of the existing standards, national regulatory guidance, best practices, and group inputs. A description of the relational structure between the common positions can be found at the OECD NEA MDEP DICWG public website.
- Work jointly to formally incorporate common positions into the regulatory guidance of MDEP DICWG member states. Common positions that have been incorporated into the regulatory guidance of a majority of DICWG member states are considered GCPs.
- Identify research needs where the working group concludes that the current level of technical knowledge is not sufficient to support establishment of a common position.
- Work closely with IAEA and standards development organisations, e.g., IEC and IEEE, for the working group's efforts to develop common positions and compare relevant requirements, guidance, and standards.
- Jointly research and comment on proposed IEC, IEEE, and IAEA standards that are relevant to the regulatory review of DI&C systems.
- Jointly research and comment on proposed reports from the Cooperation in Reactor Design Evaluation and Licensing DI&C Task Force (CORDEL DICTF) and similar organisations that are relevant to the regulatory review of DI&C systems.
- Make suggestions to, and share observations and insights learned with, standards development organizations regarding harmonization and convergence of standards.
- Engage a broad spectrum of utilities and equipment vendors to exchange relevant information and lessons learned relevant to the working group's efforts.
- Utilize the MDEP Library to facilitate the central storage and efficient exchange of information among members and other participants.

- Facilitate timely and efficient mechanisms for sharing of knowledge and experience among members, thus allowing knowledge transfer and more effective safety reviews.
- Interact frequently and effectively with the design-specific DI&C technical experts subgroups (e.g., AP1000) and other MDEP working groups as well as the Steering Technical Committee (STC).
- Develop and implement communication plan and problem solving model to maximize member involvement and foster regulatory cooperation.

2. Intermediate objectives (2017/2018)

- Develop GCPs.
- Utilize a structured process, called Quick Inquiries, to efficiently share knowledge and experience among members.
- Interact with and promote continued participation of IAEA, IEC and IEEE representatives in working group meetings and activities.
- Communicate to IAEA and standards development organizations regarding the observations and insights learned during the working group activities (e.g., comparison of standards during development of Generic Common Positions) regarding harmonization and convergence of standards.
- Interact periodically with the design-specific DI&C technical expert subgroups and have a joint meeting if necessary and practical.
- Invite utilities and vendors to working group meetings for presentations and information sharing.
- Promote presentations by members and other participants regarding their practices, experience, and lessons learned.
- Keep the working group Project Plan updated.

3. Outputs of the DICWG

The outputs of the DICWG include but are not limited to:

- Common Positions
- Programme Plan [Completed; Update as needed]
- Project Communication Plan [Completed; Update as needed]
- Problem Solving Model [Completed; Update as needed]
- Quick Inquires Table [Update after each meeting in MDEP Library]

- Suggestions to standards development organizations (IEC/IEEE) and IAEA for harmonization and convergence [Add them to MDEP library as issued]
- Suggestions to organisations such as the CORDEL DICTF concerning their draft reports that are relevant to the regulatory review of DI&C systems

4. Key Stakeholders with whom the DICWG members will interact

The DICWG members will interact with key stakeholders such as the following:

- Among its DICWG members
- MDEP STC
- MDEP Policy Group
- NEA Secretariat
- MDEP Design-Specific Working Groups and Technical Expert Subgroups
- Other MDEP Issue Specific Working Groups (e.g. Vendor Inspection Cooperation Working Group)
- Standards development organizations (IEC, IEEE, etc.)
- IAEA
- NEA/CNRA – Working Group on Inspections and Practices
- Utilities and vendors
- Industry Organisations such as the CORDEL DICTF
- DICWG Members' Home Organization
- Public are stakeholders, however, the national regulators involved in DICWG activities should take the lead in communicating with the public.

5. MDEP DICWG Work Plan

Table 1 below shows the status of the common positions work as well as the lead(s) for developing/updating them.

Table 1 Common Positions Development Status

Common Positions	**Lead**	**Status**
1. Treatment of Common Cause Failure Caused by Software within Digital Safety Systems	USA	Issued on 17 June 2013
2. Software Tools The use of appropriate software tools can increase the integrity of the software development process, and hence software product reliability, by reducing the risk of introducing faults in the process.	UK	Issued on 12 March 2013
3. Verification and Validation throughout the Life Cycle of Safety Systems Using Digital Computers For software-based safety systems an independent assessment of the system is essential to provide the degree of confidence in the design process, in the product and in the personnel involved.	Japan	Issued on 12 March 2013
4. Data Communication Independence One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence between different safety systems, thereby guaranteeing that errors in one channel or division or lower class systems will not cause the failure of another channel or division or higher class systems.	Korea	Issued on 05 December 2012; Currently under revision (see enclosure (1) for scope of work)
Phase 1 Assessment of comments on the issued version	Ongoing	
Phase 2 First draft of revised common position	by fall 2017	
Phase 3 Discussion within DICWG	by fall 2017	
Phase 4 Final Draft of revised common position	by Q1 2018	
Phase 5 Approval from DICWG members	by Q2 2018	
Phase 6 Issue to STC for comments	by Q2 2018	
Phase 7 Resolve STC comments	by Q4 2018	
Phase 8 Publication	by Q4 2018	
5. Treatment of Hardware Description Language (HDL) Programmed Devices For Use in Nuclear Safety Systems	France	Issued on 13 march 2013
6. Simplicity in Design Selected architecture should demonstrate a balance between simplicity in concept and the capacity to satisfy performance requirements.	USA	Issued on 13 March 2013

Table 1 Common Positions Development Status (Cont.)

Common Positions	Lead	Status
7. Selection and Use of Industrial Digital Devices of Limited Functionality	IAEA	Issued on 09 July 2014
8. Impact of Cyber Security Features on Digital I&C Safety Systems The general understanding is that, independent of the specific implementation, the cyber security program shall not adversely impact the performance and reliability of safety functions.	USA	Issued on 5 December 2012
9. Safety Design Principles and Supporting Information for the Overall I&C Architecture	IAEA/ France	Issued on 02 July 2015
10. Hazard Identification and Control for Digital I&C Systems	USA	Issued on 21 March 2016
11. Digital I&C System Pre-installation and Initial On-site Testing	Russian Federation	Issued on 11 December 2013
12. Use of Automatic Testing in Digital I&C Systems as part of Surveillance Testing	Korea	Issued on 11 December 2013
13. Spurious Actuations of Important to Safety I&C Systems	Finland/ USA	Under Development
Phase 1 Scope and Prioritization	Completed	
Phase 2 First draft common position	Completed	
Phase 3 Discussion within DICWG	Completed	
Phase 4 Final draft common position	by spring 2017	
Phase 5 Approval from DICWG members	by spring 2017	
Phase 6 Issue to STC for comments	by summer 2017	
Phase 7 Resolve STC comments	by fall 2017	
Phase 8 Publication	by end of 2017	
14. Generic Qualification of I&C platform (see enclosure (2) for scope of work)	UK	Under Development
Phase 1 Scope and Prioritization	Completed	
Phase 2 First draft common position	Ongoing	
Phase 3 Discussion within DICWG	[TBD]	
Phase 4 Final draft common position	[TBD]	
Phase 5 Approval from DICWG members	[TBD]	
Phase 6 Issue to STC for comments	[TBD]	
Phase 7 Resolve STC comments	[TBD]	
Phase 8 Publication	[TBD]	

6. Maintenance of Issued Common Positions

- The MDEP DICWG's common positions are authored by a sponsoring national member of the working group, but are only issued when unanimous agreement has been reached of participating members and approved by the STC. Therefore all participating regulators effectively endorse each issued common position.
- Common position should only be revised when significant technical developments or experience would challenge or contradict the issued text.
- The DICWG recommends each issued common position to be reviewed every 3 to 5 years (starting upon completion of all common position work in accordance with the programme plan) by the sponsoring national regulator and recommendations made to the working group with respect to any necessary revision. The sponsoring member country for each common position and the secretariat will be responsible for collating comments/suggestions.
- Regulators joining the DICWG should be allowed six months to review the existing issued common positions. After six months, they should endorse each common position or they should provide comments for disposition/resolution to be discussed during the next MDEP DICWG meeting.
- If a new or non-participating member is not able to endorse a particular common position, their concerns should be documented for consideration when the next regular common position review is performed. As an interim measure, and if agreed by the working group, a note may be added to a common position to document its partially endorsed status.
- Any member of the working group may propose comments or recommendations to revise any Issued common position. These comments or recommendations should be gathered and maintained by the sponsoring member country and the secretariat. The MDEP DICWG will discuss and resolve comments or recommendations at the next revision period for the common position.

7. Potential MDEP DICWG Transition to the Nuclear Energy Agency (NEA)

Previous versions of the programme plan discussed a two-phase closure approach to be executed during the Q4 2016 to Q4 2017 timeframe. The MDEP and NEA stakeholders are currently evaluating a potential MDEP DICWG transition to NEA under one of two options: joining the Committee on the Safety of Nuclear Installations (CSNI) or the Committee on Nuclear Regulatory Activities (CNRA). During this process, the following key factors need to be addressed as part of a potential MDEP DICWG transition to NEA and the selected forum: (1) It should promote having discussions on DI&C-related technical issues, which are complex and rapidly changing; and (2) It should promote having open discussions among regulators.

8. MDEP DICWG meetings

Prior to completion of the transition process discussed in the Section 8 above, the DICWG will continue to meet three times per year. Upon completion of the transition process, the DICWG will abide to the meeting periodicity requirements to be imposed by NEA. Factors such as the DICWG's workload and ability to meet the technical products demand should be taken into consideration when defining the DICWG meetings periodicity. For example, some DICWG members consider that in order to meet the current technical products demand (e.g., between 1 to 2 new common positions issued per year), the working group should continue to meet three times per year. Such a meeting periodicity allows for maintaining an open channel of frequent communications to discuss the current and emergent technical challenges in the DI&C field that would otherwise not be possible via other venues such as e-mail correspondence. Other member countries consider that the DICWG meetings periodicity could be reduced to: (1) twice per year by adding extra days to the legacy agenda; or (2) once per year by relying more heavily on e-mail correspondence. Proponents of a reduced meeting periodicity consider that such an approach would reduce travel expenses and thus could promote additional attendance from national regulators. In spite of these different views, all DICWG members agree that the selected meetings periodicity needs to support the working group's ability to maintain a sustainable throughput of technical products.

At each DICWG meeting the following items will be considered:

- The number of common positions currently in development
- Any outstanding or impending requests for additional common positions
- Any requirements to update existing common positions
- The level of activity and the effectiveness of the Quick Inquires process
- The number of participating national regulators and the level of their participation
- Any instructions/advice received from the STC

The outcome of each DICWG meeting will be documented in working group meeting minutes and reported to the STC.

Enclosure 1 – High-level summary of required updates to
CP-04 (Communications Independence)

Background:

I&C architectures in new plants make extensive use of digital communications, both between redundant divisions of safety systems and between systems of different safety classes. One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence between redundant divisions of safety systems; thereby guaranteeing that errors in one channel or division or lower class systems will not cause the failure of another channel or division or higher class systems. CP-04 as issued in December 2012 was intended to provide the agreed-upon principle of the MDEP DICWG member states on data communication independence for the design of the digital systems.

Discussion: An evaluation performed by the DICWG revealed that the issued text in CP-04 needs to be revised to address, among other issues, recent technical developments in the field of data communications. Examples include:

- Need to evaluate improving the document in terms of the technical criteria for data communications based on the latest guidance from documents such as: (1) International Atomic Energy Agency (IAEA) Specific Safety Guide (SSG) -39 (issued in 2016); and (2) Institute of Electrical and Electronics Engineers (IEEE) 7-4.3.2-2016.

- Need to include a definitions section to address terms such as “Data Communications”, “Priority Function”, and “Safety Benefits.”

- Need to define criteria for establishing the order of priority function inputs.

- Need to ensure consistency with the format used in previous CPs such as the need to include a “Scope” section.

- Need a better description of the “handshaking” concept along with a brief discussion of when and why this concept can be used on data communications among different safety class systems and between redundant channels or divisions.

- Need to correct typographical and format issues.

Enclosure 2 – Scope of Work for the new CP-14 (Generic Qualification of I&C Platform)

Background:

I&C platforms have been used for systems important to safety in nuclear power plants. Some of these platforms have been developed for nuclear power applications but many were developed for a wide range of industrial applications. In either case, the generic qualification of I&C platforms for use in systems important to safety at nuclear power plants is needed in order to demonstrate these I&C platforms are suitable for their intended applications.

Definitions:

Equipment platform: a set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An I&C platform usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software.

Note to entry: An I&C platform may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier. (IEC 63084 TR)

Qualification: process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements.

Note to entry: Qualification of I&C systems is always a plant- and application-specific activity while platform qualification relies to a large degree on qualification activities performed outside the framework of a specific plant design (these are called “generic qualification” or “pre-qualification”). (IEC 63084 TR)

Safety function: A specific purpose that must be accomplished for safety. (IAEA Safety Glossary)

Scope:

This common position will address issues for the generic qualification of the hardware and software of I&C platforms intended for systems important to safety at nuclear power plants. This common position will address topics including:

- Demonstration that the I&C platform is suitable for the intended applications including:
    - Safety Classification (Safety/Non-Safety, SIL, Class etc.)
    - Safety Function
    - Functional and Non-Functional Requirements (e.g. Reliability, Performance, Environment)

  Note: Although the specific application may not be known at the time of generic qualification, the range of applications should be defined.

- The application of appropriate development standards (for ground-up developments)

- The generic qualification of commercial grade I&C platforms (e.g. Commercial Off-the-Shelf (COTS) platforms)
- Re-use of a previously qualified I&C platform that was qualified for a specific application
- Third party certification for I&C platforms
- The integration of the generically qualified platform and the intended application
- Platform and application development tools (CP02 should apply)
- Maintenance of the I&C platform generic qualification throughout the lifecycle (including configuration control, response to operational experience, etc.)

The following points would need to be covered:

- The platform shall be classified according to its importance to safety which will be driven by the application.
- The expectation is that the platform is developed in accordance with the nuclear standards applicable to the domain (country) for the classification of the system in question.
- If the platform has not been developed to such standards then a demonstration of conformance of the actual development processes to those standards shall be provided (e.g. dedication of a commercial grade item).
    - Any discrepancies between the actual development process and the standards shall be addressed through the undertaking of compensating activities e.g. additional V&V
    - The demonstration shall address third party hardware and software components e.g. operating systems, libraries, tools etc.

It should be noted that IEC 63084 TR Ed.1 is focused on the pre-qualification of platforms (see section 5.1 of that document), the CP should cover this but also cover the development of platforms for nuclear safety applications from the ‘ground up’. It may possible to share the draft IEC Technical Report for reference however the following copyright is applicable: