MDEP Generic Common Position

Multinational Design Evaluation Programme
Generic Common Position
DICWG No3 – PUBLIC USE

Date: 12 March 2013
Validity: **until next update or archiving**
Version H

# MDEP Generic Common Position No DICWG-03

Related to: Digital Instrumentation and Controls Working Group activities

## COMMON POSITION ON VERIFICATION AND VALIDATION THROUGHOUT THE LIFE CYCLE OF DIGITAL SAFETY SYSTEMS

**Participation**

| | |
|---|---|
| Countries involved in the MDEP working group discussions: | Canada, Finland, France, India, Japan, People's Republic of China, Republic of Korea, Russian Federation, South Africa, the U.A.E., the U.K. and the U.S. |
| Countries which support the present common position | Canada, Finland, France, India, Japan, People's Republic of China, Republic of Korea, Russian Federation, South Africa, the U.A.E., the U.K. and the U.S. |
| Countries with no objection: | |
| Countries which disagree | |
| Compatible with existing IAEA related documents | Yes |

**Multinational Design Evaluation Programme**

**Digital Instrumentation and Controls Working Group**

# GENERIC COMMON POSITION DICWG NO3: COMMON POSITION ON VERIFICATION AND VALIDATION THROUGHOUT THE LIFE CYCLE OF DIGITAL SAFETY SYSTEMS

## Summary

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given the use of Digital I&C in new reactor designs, its safety implications, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and IAEA documents. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues[1].

## Context

Verification and validation (V&V) is essential throughout the life cycle of nuclear power plant safety systems. Please refer to Figure 1 for a typical representation of digital I&C system development life cycle.

## Scope

This common position applies to V&V activities for digital safety systems throughout their life cycles.

This encompasses both the software and hardware of such systems.

## Definition of terms

- Verification – Confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity [IEC 61513].

- Validation – The process of determining whether a product or service is adequate to perform its intended function satisfactorily [IAEA glossary ed.2007].

[1] The goal of MDEP is not to independently develop new regulatory standards. Common Positions are not legally binding and do not constitute additional obligations for the regulators 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. Any MDEP member may decide to implement the common positions through its national regulatory process.

**Generic Common Position on Verification and Validation:**

1. V&V should confirm that the products of each development phase fulfil the requirements or conditions imposed by the previous phase, and confirm compliance with the system functional performance and interface requirements.

   1.1 The scope and methodology of the V&V should address all system life cycle activities and should be stipulated in a comprehensive written and pre-approved V&V plan.

   1.2 It should be verified that all relevant aspects of the plant-level requirements have been properly reflected in the Instrumentation and Control (I&C) system(s) requirements.

   1.3 Verification should confirm that I&C system(s) requirements have been properly reflected in the software and hardware requirements.

   1.4 V&V should demonstrate, as far as reasonably practicable, that software released for use contains no defects that can cause the system to fail to perform safety functions.

   1.5 V&V should confirm that the software and hardware of digital safety systems fulfil all safety function requirements.

   1.6 Verification should confirm that the software and hardware component have been correctly integrated into the final system(s).

   1.7 Validation should confirm that the final system(s) appropriately fulfil their functional requirements.

   1.8 The test cases used for validation should include scenarios that comprehensively cover practical and reasonable events selected on the basis of the plant safety analysis.

   1.9 Appropriate use of tools for V&V activities is recommended (refer to Generic Common Position 2 for guidance).

   1.10 Verification should confirm that all documentation produced to support use of the system is consistent and correct.

2. In the digital safety system's life cycle, all relevant processes should be defined. V&V should be conducted in accordance with the V&V plan.

3. V&V should be performed by technically qualified individuals in an appropriately independent group who has not been engaged in design & development of the system.

4. All information and processes required for V&V should be properly documented.

   4.1 Documents prepared in the execution of V&V should be properly maintained under a configuration management plan as part of the overall quality assurance process.

   4.2 Acceptance criteria for V&V processes, V&V documentation and measures for correcting V&V processes and their results should be clearly stipulated.

5. Pre-developed software

5.1 The scope and technical basis of use of pre-developed software should be clearly identified and documented.

5.2 The V&V plan should address the use of qualified pre-developed software, that was already deemed acceptable for use in safety system applications.

6. Change control

6.1 The V&V plan should include relevant activities for change and configuration management as part of the overall quality assurance process.

6.2 Change control should be implemented throughout the life cycle. Design changes should be subject to V&V commensurate with original design.

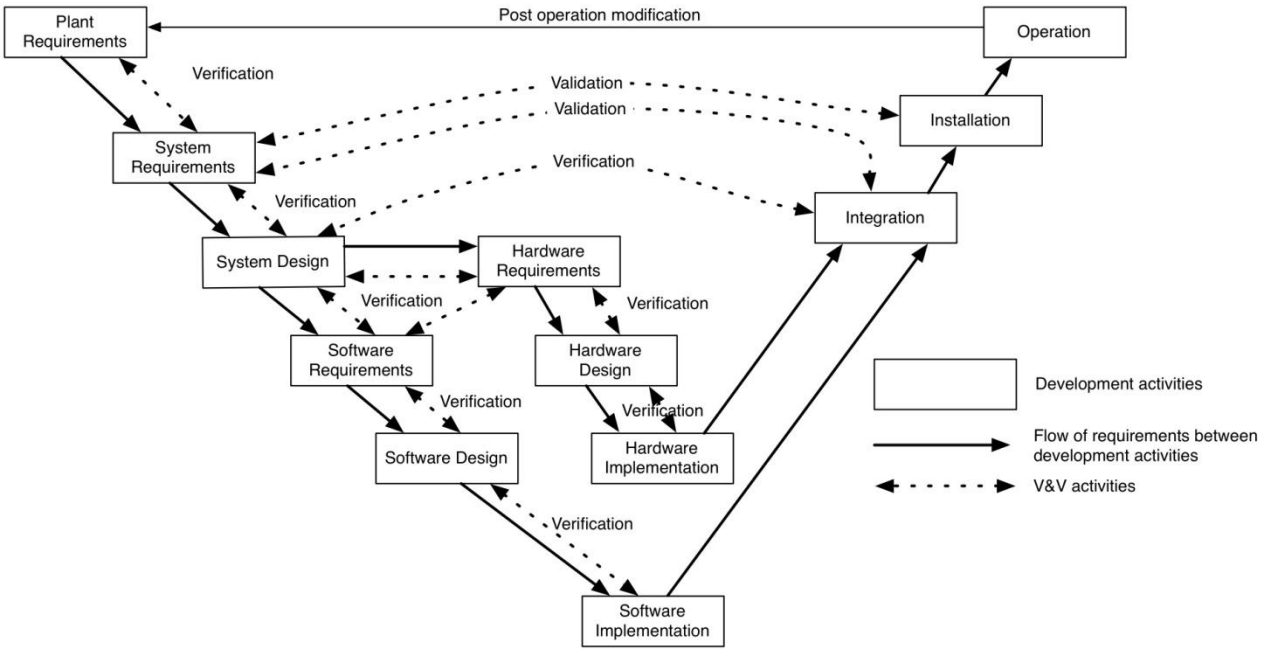


Figure 1. Typical digital I&C system development life cycle

**References**

JEAG 4609-2008 and JEAC 4620-2008 (originally in Japanese, just translated in English not official in the MDEP library)

Seven party report titled "Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations."

Four Party Regulatory Consensus Report On The Safety Case For Computer-Based Systems In Nuclear Power Plants, November 1997

IEEE Std. 1012, IEEE Standard for Software Verification and Validation, 2004,

IEC 61513, Ed.2 : Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, 2011

IEC 60880, Ed.2: Nuclear Power Plants – Instrument and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, 2006

IAEA NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, 2000

IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection 2007 Edition