MDEP Generic Common Position

Multinational Design Evaluation Programme
Generic Common Position
CP-DICWG-07 – MDEP USE ONLY

Date: 09 July 2014
Validity: **until next update or archiving**
Version 3

MDEP Common Position CP-DICWG-07

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

Participation

Countries involved in the MDEP working group discussions:	All MDEP Member Countries
Countries which support the present common position	
Countries with no objection:	
Countries which disagree	
Compatible with existing IAEA related documents	

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO7: COMMON POSITION ON SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given the increase of 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:

The nuclear power industry is increasingly interested in using industrial digital devices of limited functionality in systems important to safety, but that have not been developed specifically for use in nuclear power applications. These devices should meet certain specific requirements in order to be selected and used in systems important to safety at nuclear power plants.

Typically, some of these devices are found embedded in plant components and actuating devices, e.g. sensing instrumentation, motors, pumps, actuators, breakers.

Definition of terms:

Industrial digital device of limited functionality (IEC 62671):

A digital device to which this common position applies should comply with the following criteria:

a) The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g. an hardware description language programed device) and is a candidate for use in an application important to safety.

b) The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, controlling speed of a mechanical device, or performing an alarm function.

[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.

c) The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).

d) The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.

e) If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process (such as process range), performance (speed or timing), signal interface adjustment (such as selection of voltage or current range), or gains (such as adjustment of proportional band).

All other devices are not considered to be 'industrial digital devices of limited functionality', e.g., complex devices such as those that use commercial computers (PCs, PLCs).

Scope:

This common position applies to the selection and use of industrial digital devices of limited functionality that are to be used in systems important to safety at nuclear power plants.

Generic Common Position on the selection and use of industrial digital devices of limited functionality:

The rigor of the application of the positions on the selection and use of industrial digital devices of limited functionality should be commensurate with the safety classification.

1. Confirmation of the suitability of industrial digital devices for their intended functions should produce evidence:

    a. That the primary function of the device meets the functional and performance requirements for the application;

    b. That neither operation nor failure of secondary functions within the device can result in unsafe operation of the primary function.

    Note: Secondary functions include, for example, functions used to maintain or configure the device and functions that are not needed for the intended application.

    c. That any constraints imposed by the design of the device meet the functional and performance requirements for the application.

2. Confirmation of the correctness of industrial digital devices for their intended functions should produce evidence:

    a. Potential systematic faults including those that could cause coincident failures have been evaluated and the impact of these faults on plant safety has been assessed;

b. The development process was systematic and followed the general principles of management systems for I&C design[2,3]; and

c. Quality assurance for manufacturing is sufficient to provide a basis for accepting identical replications of the device.

3. If any of the recommendations above are not met, compensatory evidence should be provided that directly addresses the identified gaps in the evidence of suitability and correctness. Compensatory evidence should be shown to be applicable to the device in question.

4. Sufficient evidence and justification need to be provided to demonstrate that the compensatory evidence is adequate.

   Examples of techniques which may be used to provide compensatory evidence include:

   - Evaluation of applicable and verifiable operational experience;
   - Verification of design outputs;
   - Statistical testing;
   - Evaluation for potential failures of the device and their impact on the primary function through the use of appropriate failure analysis methods identified in the applicable industry standard.

5. Information developed during certification for safety purposes in industries other than nuclear power may be used as evidence to support device selection and use. A certificate alone is not sufficient; rather, it is the information used in the certification process (e.g., information that is generated from the device development process) that may provide value.

6. Restrictions that are to be observed for the safe use of the device in the intended application should be identified and documented. Such restrictions may include, for example:

   a. The applications for which the device is intended;

   b. Specific options and unused functions that are to be enabled or disabled;

   c. Limits on operating environments and design life;

   d. Measures that are to be observed during operation, testing, and maintenance.

7. The use of industrial digital devices of limited functionality should be consistent with the assumptions in the plant safety analysis and should not result in an adverse impact on plant safety and security.

[2] IAEA DS 431 Section 2 Management System for I&C Design

[3] DICWG GCP No2 and DICWG GCP No3

References

IAEA DS 431 Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series

IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems

IEC 62671 Ed.1: Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality