MDEP Generic Common Position

Multinational Design Evaluation Programme
Generic Common Position
DICWG No9

Date: 02 July 2015
Validity: **until next update or archiving**
Version 0

MDEP Common Position No DICWG-09

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON SAFETY DESIGN PRINCIPLES AND SUPPORTING INFORMATION FOR THE OVERALL I&C ARCHITECTURE

Multinational Design Evaluation Programme
Generic Common Position
DICWG No9

Date: 02 July 2015
Validity: **until next update or archiving**
Version 0

Participation

Countries involved in the MDEP working group discussions:	Canada, China, Finland France, India, Japan, Republic of Korea, Russian Federation, South Africa, Sweden, United Kingdom, United States, and United Arab Emirates
Countries which support the present common position:	All Working Group member Countries
Countries which disagree	Not Applicable
Compatible with existing IAEA related documents	Yes

Multinational Design Evaluation Programme
Generic Common Position
DICWG No9

Date: 02 July 2015
Validity: **until next update or archiving**
Version 0

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO 9: COMMON POSITION ON SAFETY DESIGN PRINCIPLES AND SUPPORTING INFORMATION FOR THE OVERALL I&C ARCHITECTURE

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 overall I&C architecture establishes the assignment of plant functions to individual I&C systems and the specification of the interface requirements of the individual I&C systems, including the layout of communications between individual I&C systems.

Modern digital I&C (DI&C) is more integrated and performs more functions (e.g. self –tests, enhanced data communication) than did the earlier generations of I&C systems. This increased integration and functionality can contribute to more complexity. A well designed overall I&C architecture will ensure a proper implementation of the relevant safety principles (e.g. defence-in-depth concept) in order to ensure safe operation, and to facilitate the safety demonstration.

Definition of terms:

Architecture: Organisational structure of the I&C systems of the plant which are important to safety (IEC 61513).

[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.

Common Cause Failure (CCF): Failure of two or more structures, systems, or components due to a single event or cause (IAEA Safety Glossary, 2007).

Complexity: The degree to which a system or system components has a design or implementation that is difficult to understand or verify (CP-06).

Diversity: The presence of different attributes among systems or components intended to minimize the potential for CCF (CP-01).

I&C system: System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself (IEC 61513).

Item important-to-safety: An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or member of the public (IAEA Safety Glossary, 2007).

Safety Group: The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded (IAEA Safety Glossary, 2007).

Safety related system: A system important to safety that is not part of a safety system (IAEA Safety Glossary, 2007).

Safety System: A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. (IAEA Safety Glossary, 2007)

Single Failure: Loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it. (IEC 61513)

Single Failure Criterion: A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure. (IAEA Safety Glossary, 2007)

Postulated Initiating Event: An event identified during design as capable of leading to anticipated operational occurrence or accident conditions. (IAEA Safety Glossary, 2007)

Defence-in-Depth: A hierarchical deployment of different levels of [protection] to prevent escalation of anticipated operational occurrences [AOO] and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states, [i.e. normal operation and AOO], and, for some barriers, in accident conditions. (Adapted from IAEA Safety Glossary, 2007)

Independence: [Property that is exhibited between 2 or more systems or components] that possess both of the following characteristics: (a) the ability to perform their required function is unaffected by the operation or failure of the other [systems or components]; and (b) the ability to perform their function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which they are required to function. (Adapted from IAEA Safety Glossary, 2007)

Reliability: The probability that a system or component will perform its intended function satisfactorily when called upon to do so, for a specified time, under stated operating conditions, which may be assessed in either a quantitative or qualitative manner.

Scope:

This common position applies to the overall I&C architecture, i.e. the organization of I&C systems of the plant which are important to safety (including those that interact with a safety group). This common position addresses the safety design principles and supporting information regarding the overall I&C architecture for the demonstration of safety. This information includes details on associated design features (e.g. design characteristics, commitments, etc.) that ensure safety.

This common position does not address specific safety design principles or supporting information associated with individual I&C systems. This common position assumes that each individual I&C system (e.g. protection system, control system) satisfy all its requirements, applicable safety design principles, design constraints, environmental qualification, etc. All these information will also be part of the safety demonstration.

It is recognised that other design requirements, such as security, may affect the I&C architecture. These requirements are not in the scope of this common position.

Generic Common Position

A. SAFETY DESIGN PRINCIPLES

The following are a set of principles expected to be demonstrated by the overall I&C architecture. For the application of these principles, the context of the plant design has to be taken into account.

Defence in Depth

1) The overall I&C architecture should support the plant defence-in-depth concept.

2) The overall I&C architecture should not compromise the defence-in-depth strategies (i.e. different methods for implementing the DiD concept, such as having unidirectional communication flow from higher safety class to lower safety class systems) of the plant design.

Consideration of Common Cause Failures

3) Design requirements may be given to the individual systems to address potential common cause failures of items important to safety, and to determine how the concepts of diversity (including functional diversity) redundancy, independence (including physical separation) can be applied to achieve the necessary reliability.

4) I&C should be designed with defences against CCF to preserve the plant's defence-in-depth.

Independence

5) The overall I&C architectural design should establish the level of independence between the I&C systems that support the different levels of the plant's defence in depth and diversity concepts.

6) The overall I&C architecture should promote independence among the plant's levels of defence-in-depth.

7) The overall I&C architecture should provide measures to maintain the required independence between systems in the presence of undesired behaviour.

8) The overall I&C architecture should facilitate partitioning to avoid unnecessary complexity and unnecessary interactions between individual I&C systems.

9) The overall I&C architecture should neither compromise the required independence between redundant portions of safety systems, nor the independence implemented at the different levels of the plant defence-in-depth.

Diversity

10) The overall I&C architectural design should establish the diversity strategy to be implemented.

11) The overall I&C architecture should not compromise diversity strategies of the plant design.

Compliance of safety groups with the single failure criterion

12) The overall I&C architecture should support each safety group in performing all actions required to respond to a Postulated Initiating Event (PIE) in the presence of any single failure.

Reliability

13) The overall I&C architecture design should be established to fulfil the reliability requirements of each safety function and support the overall plant reliability goals.

Complexity

14) The overall I&C architecture should be as simple as practical but still fully implement its safety requirements.

15) The overall I&C architecture should be amenable to sufficient analysis or verification to facilitate an adequate safety demonstration.

Examples of complexity to be avoided are the inclusion of functions that do not contribute to the safety functionality or its reliability, use of design and implementation features not amenable to sufficient analysis or verification, and use of implementation platforms that are too complex to facilitate an adequate safety demonstration.

MDEP Common Position No. 6 on Principles on Simplicity in Design describes how to avoid unnecessary complexity in the design of digital I&C safety systems.

B. SUPPORTING INFORMATION FOR THE OVERALL I&C ARCHITECTURE

The following information and associated design features (e.g. design characteristics, commitments, etc.) about the overall I&C architecture should be provided to assist in the safety demonstration and ensure safety:

1) The information that demonstrates how the overall I&C architecture satisfies the plant requirements, including requirements for system interfaces, safety function (e.g. reactor trip), and safety performance (e.g. timing constraints).

2) The overall I&C architecture information including:

    a. The basis for allocating specific plant functions to individual I&C systems and demonstration that all I&C functions needed to fulfil the plant design basis are included;

    b. The identification, role and classification of those individual I&C systems required to perform important-to-safety functions

    c. Criteria for the performance of integrated support activities such as maintenance, periodic testing, etc.;

    d. Criteria for selecting the technology (i.e. digital vs analogue) used for I&C systems;

    e. Communications design (i.e. physical and logical topologies among I&C systems);

    f. The configuration of the systems within the plant environment under all relevant plant operational states [CP-11];

    g. Failure modes and undesired behaviours of the systems at the architectural level, including single failures, common cause failures, and spurious failures.

3) Information to demonstrate that the overall I&C architectural design considered design constraints generated by other disciplines such as electrical system design, human factors, mechanical and civil engineering design.

4) Information regarding how the overall I&C architecture facilitates the provision of necessary human machine interfaces (e.g., in the main control room, the supplementary control room and other areas) as required by the plant design.

5) Information regarding how the overall I&C architectural design supports its pre-installation and initial on-site testing, operations, maintenance, replacement and decommissioning.

6) Overall I&C architectural documentation and supporting information. This documentation should be updated throughout the design life cycle and be maintained throughout the life of the plant. The documentation should be traceable to the appropriate plant design documentation.

References:

MDEP Generic Common Position DICWG No. 1: Common Position on Treatment of Common Cause Failures Caused by Software within Digital Safety System, 2013.

MDEP Generic Common Position DICWG No. 6: Common Position on Principles on Simplicity in Design.

MDEP Generic Common Position DICWG No. 11: Common Position on Digital I&C Systems Pre-installation and Initial On-site Testing, 2013.

IAEA DS-431, Design of Instrumentation and Control Systems for Nuclear Power Plants, Draft M, March 2014.

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

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