MDEP Generic Common Position

Multinational Design Evaluation Programme
Generic Common Position
DICWG No10 – MDEP USE ONLY

Date: 21 March 2016
Validity: **until next update or archiving**
Version 7, Updated on 03-21-2016

MDEP Common Position No DICWG-10

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON HAZARD IDENTIFICATION AND CONTROLS FOR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Multinational Design Evaluation Programme
Generic Common Position
DICWG No10 – MDEP USE ONLY

Date: 21 March 2016
Validity: **until next update or archiving**
Version 7, Updated on 03-21-2016

Participation

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

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO 10: HAZARD IDENTIFICATION AND CONTROL FOR DIGITAL INSTRUMENTATION AND CONTROLS SYSTEMS

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:

Faults within I&C systems may lead to failures that may be potential hazards that can affect plant safety, block or prevent the actuation of a safety system protective function or cause an operating condition for which the safety systems protective functions cannot mitigate. Examples of the cause of such faults include incorrect requirements and interface specifications, software errors, and errors as a result of maintenance and periodic testing. Such faults can lead to undesired behaviour of I&C systems, which could create hazards that challenge plant safety. In comparison to hazards associated with localized failures (e.g. conventional hardware component failures), hazards associated with digital I&C systems can be more difficult to identify and control. These difficulties arise from system complexity and the pervasive and latent impact of faults due to interconnectivity or functional relationships of systems. Therefore, a systematic approach to identify and control such hazards is necessary[2].

Definition of terms:

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

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

[2] Hazard identification and control may also be referred to as hazard analysis.

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 two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure (IAEA Safety Glossary, 2007).

Defect: A problem which, if not corrected, could cause an I&C component or system to either fail or to produce incorrect results. (Adapted from ISO/IEC 20926:2003.)

Fault: Defect in a hardware, software or system component (IEC 61513-2011). An error may lead to a fault, a fault may lead to a failure, and failure may lead to a hazard, and a hazard may lead to harm.

Failure: Loss of the ability of a structure, system, or component to function with acceptance criteria (IAEA Safety Glossary, 2007 – modified).

Hazard: Potential source of harm (ISO/IEC Guide 51:1999, Definition 3.5).

Hazard Identification: The process of recognizing that a hazard exists and of defining its characteristics (US NRC RIL 1101).

Hazard Control: Means to prevent, eliminate or mitigate hazards through corresponding design requirements and constraints, operational controls, coping strategies, etc. (Adapted from US NRC RIL 1101).

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 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).

Scope:

This common position addresses the identification and control of hazards associated with I&C systems that can challenge plant safety. The scope of this common position includes hazards caused by postulated failure modes, such as single failures and common cause failures (see CP-DICWG 01 for additional guidance on CCF), and hazards identified during the I&C system life cycle. Hazards affecting I&C systems may arise from internal or external sources. This may include the interface of I&C systems with other plant systems and the interface between organizations involved with the I&C system life cycle.

Of particular concern from a safety standpoint is the potential for single or common cause failures to result in a failure of I&C systems to act or cause a spurious actuation of plant components. Spurious actuation of plant components (of the same type or combinations of differing types of components) has the potential to place a given plant into an unsafe operating condition that is not bounded by the plant's safety analysis (see CP-DICWG 13 on spurious actuation). I&C systems can exhibit failures from within the I&C system itself or have failures induced from external interfaces, human interactions, and environmental conditions.

The faults that can result in single failures or common cause failures are of greater concern in systems with high levels of integration and complexity and are best addressed through a systematic approach. Although this common position could be applied to all types of I&C systems, this CP focuses on the hazard identification and control associated with digital I&C systems due to their potential for integration and complexity. The scope of this common position accounts for the full breadth and depth of I&C systems, from the plant level, down to the individual device level, as applicable.

This common position is not intended to provide an inclusive list of all potential hazards sources nor is it an inclusive list of solutions for addressing hazards. Each plant design will have its own unique design attributes and consequently, its own unique hazards for which this guidance can help to determine design solutions tailored to each plant.

This common position does not endorse any specific hazard identification or control method.

Generic Common Positions

A. HAZARD IDENTIFICATION

1) For each I&C system, hazards that could challenge plant safety should be identified.

2) Hazard identification should complement the plant safety analysis (e.g. consider hazards not analysed).

3) Hazard identification should be performed for all stages of the system life span (including development, commissioning, modifications, operation, maintenance and decommissioning).

    a. Hazard identification should assess for hazards during the entire system life cycle development process from the planning through the testing phases.

    b. Hazard identification should also consider hazards induced by activities such as commissioning, maintenance and testing, equipment ageing, operational procedures, etc.

    c. Hazard identification should be revisited at appropriate times (e.g. digital upgrades, changing or emerging information regarding internal or external hazards to I&C systems, etc.)

4) Hazard identification should consider hazards that arise from interactions between I&C systems and other plant systems. Other hazards may arise during the I&C system lifecycle due to organisational interactions between different technology areas.

5) Regardless of the technique used to perform hazard identification (e.g. hazard and operability analysis (HAZOPs), functional failure modes and effects analyses (FFMEAs), systemic theoretic process analysis (STPA), top-down fault tree analysis (FTA), or purpose graph analysis (PGA)),

the limits of the technique should be understood. Documentation should be provided to justify the techniques used.

6) All identified hazards, including the causes and consequences for the identified hazards, should be properly documented.

B. HAZARD CONTROLS

1) Hazard controls should be implemented for the identified hazards from Section A of this common position. Hazard controls can include, but are not limited to:

- Preventing the hazard by removing the cause of the hazard (e.g. design the system such that the hazard cannot arise)
- Inherent design features within the I&C system (e.g. independence, automated self-testing, diversity, etc.)
- Analyses that demonstrate plant safety is ensured in the presence of the hazard

Note: Hazard controls using measures such as external I&C systems, mechanical controls, operational procedures, etc. should be considered. Engineered features, however, are preferable.

2) Hazard controls should be as simple as possible to facilitate activities such as inspections, configuration management, fulfilling procedural requirements, etc.

3) The hazard control process should be performed for all stages of the system life span. Unidentified hazards should reduce as the life span progresses.

4) Hazard controls should consider the potential consequences of each hazard that could challenge plant safety.

5) The evaluation or testing of hazard controls should verify the effectiveness of each hazard control.

6) Hazard controls should not prevent the system from meeting its functional and performance requirements.

7) Hazard controls should be adequately documented. Hazard control documentation should clearly and concisely describe criteria to trigger re-evaluation when changes occur to internal and external hazards that may impact the I&C system.

8) Hazard controls should be periodically reviewed and re-evaluated when necessary. A review may be triggered by changes to I&C system design requirements and constraints, emerging information, mandatory periodic review, etc.

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. 11: Common Position on Digital I&C Systems Pre-installation and Initial On-site Testing, 2013.

IAEA SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants, 2015

IAEA SSG-25: Periodic Safety Review for Nuclear Power Plants, 2013

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

US NRC Research Information Letter (RIL) 1101: "Technical Basis to Review Hazard Analysis of Digital Safety Systems" (ADAMS Accession No. ML14237A359)

US NRC Design-Specific Review Standard (DSRS) Section 7.0, Appendix A: Hazard Analysis (ADAMS Accession No. ML12318A200)