Multinational Design Evaluation Programme	Date: 17 June 2013
Generic Common Position	Validity: **until next update or archiving**
DICWG No1 – PUBLIC USE	Version A

MDEP Generic Common Position No DICWG-01

Related to : Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON THE TREATMENT OF COMMON CAUSE FAILURE CAUSED BY SOFTWARE WITHIN 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 NO1 : COMMON POSITION ON THE TREATMENT OF COMMON CAUSE FAILURES CAUSED BY SOFTWARE WITHIN 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 increased 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:

Common cause failures (CCF)[2] have been a significant safety concern for nuclear power plant systems. The increasing dependence on software-in safety systems for nuclear power plants has increased the safety significance of CCF caused by software, when software in redundant channels or portions of safety systems has some common dependency. For example, the effect of systematic failures can lead to a loss of safety in many ways:

- unwanted actuations
- a safety function is not provided when needed.

Therefore, nuclear power plants should be systematically protected from the effects of common cause failures caused by software in DI&C safety systems. Software for nuclear power plant safety systems should be of the high quality necessary to help assure against the loss of safety (i.e. developed with high-quality engineering practices, commensurate quality assurance applied, with continuous improvement through corrective actions based on lessons learned from operating experience). However, demonstrating adequate software quality only through verification and validation activities and controls on the development process has proved to be problematic. Therefore, this common position provides guidance for the assessment of the potential for CCF for software. It is recognized that programmable logic devices do not execute software in the conventional sense; however, the application development process using

[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] It is not necessary to consider common cause failures due to software errors in the application of the single failure criterion.

these devices have many similarities with software development, and the deficiencies that may be introduced during the application development process may induce errors in the programmable logic devices that can result in common cause failures of these devices of a type similar to software common cause failure.

Although deficiencies with the potential to give rise to software common cause failures can be introduced at all phases of the software life cycle, this common position will only consider the potential for software common cause failures within digital safety system safety functions arising from latent design deficiencies introduced in any of the three software development activities; software requirements, software design and software implementation (as illustrated in Figure 1 “Typical digital I&C system development lifecycle” of Generic Common Position No.3). While deficiencies created during system development life cycle phase activities (e.g. the system requirements phase) can also lead to common cause failures, these design deficiencies would occur regardless of whether the system developed is using software or not. As this common position only considers the software requirements, software design, and software implementation lifecycle phases the scope of this document is limited to the consideration of the potential for software common cause failures caused by the introduction of latent errors in the design of digital safety systems.

Definition of terms:

Common Cause Failure: Failure of two or more structures, systems or components due to a single event or cause. [IAEA SSR2/1, 2012]

Diversity: The presence of different attributes between systems or components intended to minimize the potential for common cause failure.

Generic Common Position on the Treatment of Software Common Cause Failures:

1. For each design basis event an analysis should be performed to demonstrate that the plant can cope with the effects of a common-cause failure caused by software.

   1.1 The analysis should postulate credible CCF caused by software that result in systematic failures of safety functions.

   1.2 The analysis need only consider one postulated CCF caused by software at a time.

   1.3 Existing measures can be credited to mitigate the effects of the CCF. However, it should be verified that these measures are sufficient. Where manual action is credited, response times should be justified in accordance with each country’s acceptance criteria.

2. Actuation of plant components resulting from credible CCF caused by software should be considered by the safety analysis.

3. Diversity is a way to reduce the potential effects of CCF (e.g. incorporation of inherent diversity in the design of the instrumentation and control system, or by the use of a diverse backup system). It is recognized that there are varying degrees of diversity.

   3.1 If CCF caused by software could adversely affect a safety function that is required to respond to a design basis event, a diverse means of effective response (with documented basis) should be provided and its effectiveness should be justified.

3.2 If diversity is proposed to be used in the I&C design to mitigate effects of CCF caused by software, and if adequate mitigation cannot be demonstrated, then the design should be modified and re-analysed.

3.3 Different member countries have different regulatory positions regarding the quality and classification of diverse backup systems, and use of manual actions to mitigate against potential common cause failures caused by software in safety systems (see Annex 1). Therefore, if a design seeks to mitigate against the potential for CCF caused by software through the implementation of diverse backup systems or manual action, consideration of the different member country's regulatory position regarding the quality and classification of diverse backup systems or manual action should be included in the analysis.

4. Different member countries may accept different methods to mitigate against the potential for CCF caused by software (e.g., formal methods to prove software correctness).

References

IAEA SSR 2/1, "Specific Safety Requirements: Design", 2012

10 CFR Part 50, "General Design Criteria for Nuclear Power Plants"

USNRC NUREG-0800, Standard Review Plan, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems", 2012

USNRC NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems", 1994

USNRC Staff Requirements Memorandum to SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Item II.Q, 1993

IEC 60880, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions", 2006

IEC 62340, "Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)", 2007

IEEE 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems", 2000

IEEE 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", 2009

IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 2010

Annex 1: National positions

Member Country	Diverse Backup System Classification	Diverse Backup: Software-based or not?	When manual, instead of automatic, backup allowed?
Canada	Safety (by regulation) for category A software. For category B & C, only redundancy requirement no diverse backup system requirement.	Software-based backup with full diversity	When manual backup meets licensing conditions, e.g. functional/performance requirements, reliability when <20 minutes protective action required, operator action is allowed with manager's approval.
China	Non-safety class allowed	Software-based allowed with adequate diversity demonstrated.	When adequate human factors engineering analysis performed; When <30-minute protective action required, automatic backup system recommended.
France	Lower safety class	Software-based allowed with adequate diversity demonstrated.	When adequate human factors engineering analysis performed; When <30-minute protective action required, automatic backup system recommended.
Finland	Lower safety class allowed	Software-based allowed with adequate diversity demonstrated.	No requirements
India	Safety	Software-based allowed with adequate diversity demonstrated.	Design shall not take credit for operator action within the first 30 minutes of Postulated Initiating Event.
Japan	Non-safety allowed	Hardwired system allowed.	Manual back-up is allowed in Japan, but there is no time requirement for back-up system.
Korea	Non-safety hardware; "safety-related" software	Software-based allowed with adequate diversity demonstrated.	• Not allowed for diverse reactor trip • Allowed for ESFAS
Russian Federation	Safety	Both	Manual actions aimed against safety are prohibited for 30 minutes after emergency is originated.

Member Country	Diverse Backup System Classification	Diverse Backup: Software-based or not?	When manual, instead of automatic, backup allowed?
South Africa			
United Kingdom	Safety or safety related (requirements of IEC62166 and the reliability claim are taken into consideration)	A software CCF limit for reliability claims is applied. Hardware-based backup systems strongly preferred due to their inherent design diversity. Diversity in hardware compared to that used in primary system also a relevant factor in assessment.	When adequate human factors engineering analysis has been performed showing that typically 30 minutes can elapse before the manual action is required.
United States	Non-safety allowed; "enhanced quality"	Software-based allowed with adequate diversity demonstrated.	When adequate human factors engineering analysis performed; When <30-minute protective action required, automatic backup system recommended.
UAE	Non-safety class allowed	Software-based allowed with adequate diversity demonstrated.	Manual initiation and control of protective action is permitted provided that adequate human factors engineering analysis has been performed. Within 30 min following onset of initiating event backup protective action should be automatic.

Note: MDEP members currently have different safety classifications and definitions for I&C systems. The IAEA is developing a safety guide (DS-367, "Safety Classification of Structures, Systems, and Components in Nuclear Power Plants") to promote harmonization on safety classifications. The adoption of this guidance into digital I&C systems by MDEP members would require revisions to this table.