Multinational Design Evaluation Programme
Generic Common Position
DICWG No12 – PUBLIC USE

Date: 11 December 2013
Validity: **until next update or archiving**
Version A

MDEP Generic Common Position No DICWG-12

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON THE USE OF AUTOMATIC TESTING IN DIGITAL I&C SYSTEMS AS PART OF SURVEILLANCE TESTING

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, Sweden, 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, Sweden, 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
Generic Common Position
DICWG No12 – PUBLIC USE

Date: 11 December 2013
Validity: **until next update or archiving**
Version A

Multinational Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO12: COMMON POSITION ON THE USE OF AUTOMATIC TESTING IN DIGITAL I&C SYSTEMS AS PART OF SURVEILLANCE TESTING

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:

Digital I&C systems, that have the capability to use automatic tests to reveal and manage faults, may use these capabilities to support surveillance testing. Automatic tests may provide early detection of potential system failures and can address aspects of surveillance testing, and thus they may reduce the need for manually performed surveillance activities (e.g., continuously monitor system behaviour during operation to alarm operators to take appropriate actions). This common position applies to the use of such automatic tests after system deployment.

Definitions:

Automatic test: a test in which the operation of all or part of the instrumentation and control system is checked in a completely automatic sequence. The automatic test sequence can be started either manually by the operator, cyclically by a clock or automatically by the verification of a well-defined condition [IEC 60671].

Note: for the purpose of this common position, only those automatic tests initiated and fully performed by the digital I&C system itself are considered.

Surveillance testing: complete scope of activities to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and confirmation that the design basis requirements are met [IEC 60671].

[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 the use of automatic testing in digital I&C systems as part of surveillance testing:

1. Execution of automatic tests should neither degrade the performance of the system functions (e.g., by delaying system response time beyond requirements) nor impair the system's ability to perform its functions (e.g., by causing system lock-up).

2. Implementation of automatic tests should not compromise safety characteristics (e.g., independence, diversity).

3. Where automatic tests are used in lieu of or to reduce the frequency of manual tests:

   3.1 The faults that can be detected by the automatic test features should be documented.

   3.2 Adequate overall test coverage should be demonstrated.

   3.3 The adequacy of the frequencies for automatic tests [as combined with manual tests] should be justified in accordance with reliability and safety requirements.

   3.4 Adequate detection and management of faults should be demonstrated.

   3.5 The safety benefits of automatic tests such as improved fault reporting and increased reliability, should be balanced against any potential increase in system complexity (see GCP 06 – simplicity in design).

4. Faults revealed by automatic tests should be made known to the plant operating staff through appropriate means, such as alarms, displays and logs.

5. System actions to be taken on the automatic detection of a fault should be reflected in system requirements and design. These actions should not degrade safety.

References

IAEA NS-G-2.2, "Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants," 2000.

IEEE Std. 338-2012, ″IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems.″

IEEE Std. 603-2009, ″IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.″

IEC 60671, Instrumentation and control systems important to safety, Surveillance testing, 2007.

IEC 61226 Ed. 3, "Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions," International Electrotechnical Commission, Geneva, Switzerland, 2009.