Multinational Design Evaluation Programme
Generic Common Position
DICWG No4 – PUBLIC USE

Date: 5 December 2012
Validity: **until next update or archiving**
Version B

MDEP Generic Common Position No DICWG-04

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON PRINCIPLE ON DATA COMMUNICATION INDEPENDENCE

Participation

Countries involved in the MDEP working group discussions:	Canada, China, Finland, France, India, Japan, 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, China, Finland, France, India, Japan, 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
Generic Common Position
DICWG No4 – PUBLIC USE

Date: 5 December 2012
Validity: **until next update or archiving**
Version B

Multinational Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO4: COMMON POSITION ON PRINCIPLE ON DATA COMMUNICATION INDEPENDENCE

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given its growing applications to the new reactors, 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. DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues.

Context:

I&C architectures in new plants will make extensive use of digital communications, both between safety systems and between systems of different safety classes. One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence between different safety systems, thereby guaranteeing that errors in one channel or division or lower class systems will not cause the failure of another channel or division or higher class systems. This common position provides the agreed-upon principle of the MDEP DICWG member states on data communication independence for the design of the digital systems.

Generic Common Positions for Treatment of Data Communication Independence:

1. Communication between safety divisions

Communications between computers in different safety divisions should have no detrimental effect on the safety division in question due to any failure or error in communications either from or to another division.

Broadcast communication is an acceptable approach for the communication independence between computers in different safety divisions. “Broadcast” means that transmitter put data into the designated space for the buffering function, and then receivers just read the data from the buffering space without handshaking.

Architectures utilizing a central hub or router where communications from multiple safety division are transmitted across a single channel should be prohibited.

2. Communication between systems of different safety classes

Communication computers performing functions of a higher safety category should be adequately isolated from communication computers performing functions of a lower safety category (including non classified functions). When the communication between systems of different safety classes is required, then the plant data flow should be from the higher safety classified systems to the lower safety class systems. For data flows from lower to higher classified safety systems, there should be a demonstrable safety benefit and a demonstration that safety functions of the higher category cannot be adversely affected by such a connection[1]. Data flows from lower to higher classified safety systems that are not necessary for safety, even if they enhance reliability, should be prevented.

3. Priority function

A priority function should be a safety function. Devices that perform safety functions may be actuated by both safety systems and systems of a lower safety class provided that the completion of safety actions cannot be interrupted by commands, conditions, or failures outside the function's own safety division. This is commonly accomplished by use of a priority function.

4. Communication interfaces and buffering function

Devices (e.g., processors) that perform safety functions should perform no communications handshaking or interrupts that could disrupt deterministic safety function processing. Buffering should be provided between communications links and devices performing safety functions. The buffers should ensure that faults and failures on communications originating outside of a safety division do not propagate to the devices performing the safety function within the division."

References

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

IEC 61500, "Instrumentation and Control Important to Safety – Data Communication in Systems Performing Category A Functions", 2009

DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)", Rev.1 2009

IEC 60709, "Instrumentation and Control Systems Important to Safety – Separation", Ed2, 2004

IEC 61513, "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", Ed1, 2001

[1] India's AERB present regulation does not accept data communication from lower to higher safety classified systems for performing safety functions.