MDEP Generic Common Position

Multinational Design Evaluation Programme
Generic Common Position
DICWG No8 – PUBLIC USE

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

MDEP Common Position No DICWG-08

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON THE IMPACT OF CYBER SECURITY FEATURES ON DIGITAL I&C SAFETY SYSTEMS

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

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO8: COMMON POSITION ON THE IMPACT OF CYBER SECURITY FEATURES ON DIGITAL I&C SAFETY SYTEMS

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:

Cyber security measures are generally implemented at nuclear facilities to protect against cyber attacks that may compromise safety. The implementation of such cyber security measures may vary based on site specific requirements and each country's regulatory frameworks. Safety measures and cyber security measures for a nuclear power plant should be designed and implemented so that they do not compromise one another. This common position is intended to only apply to systems classified to the highest level of safety.

Definition of Terms

In accordance with the IEC definition, cyber security seeks to prevent unauthorized accesses to information, software and data in order to ensure that three attributes are met, namely:

- The prevention of disclosures that could be used to perform malicious or misguided acts which could lead to an accident, an unsafe situation or plant performance degradation,
- The prevention of unauthorized modifications (integrity),
- The prevention of unauthorized withholding of information, data or resources that could compromise the delivery of the required service by I&C function.

IAEA uses the term computer security in most of its documents addressing this issue. It is recognized that cyber security, IT (information technology) security, and computer security are generally used to identify the same issues.

[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.

Various regulatory authorities may use different terms but the purpose of this common position is intended to address the same issue.

In the context of this common position, the use of the term intrusion detection system is defined as a technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks (ISO/IEC 27033-1).

Generic Common Position on the impact of Cyber Security Features on Digital I&C Safety Systems:

1. Implementation of cyber security features should not adversely impact the performance (including response time), effectiveness, reliability or operation of safety functions.

2. Implementation of cyber security features directly in the safety system should be avoided when practical.

   2.1 Adding cyber security features to safety I&C system may increase system complexity and may introduce potential failure modes to the system that would challenge its ability to perform its safety functions in a reliable manner. For this reason, inclusion of cyber security features should be carefully evaluated and only implemented when it is not practical or otherwise feasible to accomplish an equivalent measure of cyber security protection by other means.

3. Where cyber security features need to be implemented in safety system displays and controls, they should not adversely impact the operator's ability to maintain the safety of the plant.

4. Where cyber security features need to be implemented on digital I&C safety systems, adequate measures should be taken to ensure that these features do not adversely affect the ability of a system to perform its safety functions.

   4.1 Where cyber security features are implemented within safety systems, this should be justified.

   4.2 The failure modes and effects of these cyber security features on the systems' safety functionality should be considered.

   4.3 Cyber security features such as intrusion detection systems should be implemented peripherally to the safety systems. Passive cyber security features could be applied at all times. Active cyber security features, with the potential to effect safety functions, should only be applied when safety systems are not required to perform their safety functions.

   4.4 A cyber security feature, when challenged, should not inhibit or deactivate safety functions.

5. Cyber security features included in safety systems should be developed and qualified to the same level of qualification as the system these features reside in.

References

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

Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities"

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

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

Project IEC 62645 "Nuclear Power Plants Instrumentation and Control Systems – Requirements for Security Programs for Computer-based Systems

IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities" 2011

IAEA NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants," 2000

IAEA NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," 2002

ISO/IEC 27033-1, Information technology – Security techniques – Network security part 1: network security overview and concepts, 2009