Document Preparation Profile (DPP)

1. IDENTIFICATION

Document Category:	**Safety Guide**
Working ID:	**DS 431**
Proposed Title:	**Design of I&C Systems for NPPs**
Proposed Action:	**Combine and update NS-G-1.1 and NS-G-1.3 into a new Safety Guide**
Published Title/Date:	**NS-G-1.1, Software for Computer Based Systems Important to Safety in Nuclear Power Plants (2000)** **NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants (2002)**
Safety Series No.:	**NS-G-1.1 and NS-G-1.3**
SS Committee(s):	**NUSSC**
Technical Officer(s):	**Gary Johnson**

2. BACKGROUND

NS-G-1.3 provides recommendations regarding the implementation of NS-R-1 requirements for Instrumentation and Control (I&C) Systems. NS-G-1.3 is extensively used and referenced. In some countries it is used as the basis for regulatory requirements for such systems. It also provides the underlying guidance that sets the framework for International Electrotechnical Commission standards for specific I&C functions, systems, and equipment. Since its publication in 2002, new issues have arisen in the design of modern instrumentation and control systems and improved consensus has developed in the approach to certain existing topics. Such issues include cyber-security, soft-control, use of complex electronic components, and connections between communications networks of different safety classification.

A related guide, NS-G-1.1, provides detailed guidance on the development of software for I&C systems important to safety. Safety is a systems issue and the segregation of guidance for I&C systems into to two documents, one dealing with hardware and systems, and the other dealing with software, complicates discussion of the interactions of these topics in the guidance documents. NS-G-1.1 was developed before the systems guidance of NS-G-1.3, consequently, NS-G-1.1 had to set the systems context necessary to inform the interpretation of software recommendations. The result is that much systems guidance is now contained in both NS-G-1.1 and NS-G-1.3, producing not only unnecessary duplication but the possibility inconsistencies between the two texts.

The current NS-G-1.1 is also extremely detailed.. The deep level of detail makes the guide difficult to update. The guide also competes with both national and international nuclear standards that provide focused guidance on issues of concern in nuclear power plant applications. IAEA guidance in the I&C software area should focus on the critical guidance specific to developing real-time software for nuclear power plants in such a manner that safety functions are assured, unexpected functions are not introduced, and evidence is produced to allow confirmation of the software quality and functionality. The more detailed guidance, both general and specific to nuclear power, should be left to national and international standards organizations which can apply more resources to update their standards in pace with evolution of software methods and applications.

3. OBJECTIVE AND JUSTIFICATION

The objective is to combine the existing safety guides into a new updated guide that deals with both

topics and to update the recommendations for I&C system design and software development to reflect consensus that has emerged in several areas since the original publication of NS-G-1.3 and NS-G-1.1. The existing guidance of NS-G-1.1 needs to be reviewed to confirm that it represents the critical elements that focus on issues of particular significance to nuclear power plant applications. The resulting guidance will then be merged with the updated content of NS-G-1.3 to produce one guide that gives a unified view of the design guidance (including security guidance) for nuclear power plant I&C systems, hardware, and software important to safety. Such a merger is consistent with the "Strategy for Establishment of Safety Standards," which set out the principles that the number of safety standards should be minimized, that topics should be addressed in a single guide when possible, and that guidance related to design should be integrated as much as possible.

4. POSITION IN THE OVERALL STRUCTURE OF THE RELEVANT SERIES AND INTERFACES WITH EXISTING AND/OR PLANNED PUBLICATIONS

The new guide would be one of the design safety guides providing recommendations for the implementation of NS-R-1, "Safety of Nuclear Power Plants: Design." The standard would also have interfaces with the following Safety Guides

- NS-G-1.2: Safety Assessment and Verification for Nuclear Power Plants[1].
- NS-G-2.2: Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants[2]
- NS-G-2.14 Conduct of Operations at Nuclear Power Plants[3]
- NS-G-1.8: Design of Emergency Power Systems for Nuclear Power Plants[4]

The new guide must avoid conflicts with the following guides that guide the development of design inputs for the I&C systems or give guidance on engineering methods that ensure operability of systems and components:

- NS-G-1.5: External Events Excluding Earthquakes in the Design of Nuclear Power Plants
- NS-G-1.6: Seismic Design and Qualification for Nuclear Power Plants
- NS-G-1.7: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants
- NS-G-1.11: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants

The new guide should provide principles suitable to ensure correct performance and sufficient reliability of instrumentation functions identified in the following guides.

- NS-G-1.4: Design of Fuel Handling and Storage Systems for Nuclear Power Plants

---

[1] Relative to guidance on implementing NS-R-1 requirements on engineering aspects important to safety

[2] Relative to guidance on implementing NS-R-1 and NS-R-2 requirements for limiting safety system settings

[3] Relative to operational conduct that must be supported by the I&C systems.

[4] Regarding services provided by the electric power system which are an integral part of the I&C systems and requirements for I&C functions within the electrical power systems.

- NS-G-1.9: Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants
- NS-G-1.10: Design of Reactor Containment Systems for Nuclear Power Plants
- NS-G-1.12: Design of the Reactor Core for Nuclear Power Plants

The new guide must also consider new and revised IAEA safety standards that are currently under development, such as the revision to NS-R-1, and the new guide on safety classification. These will be considered as they near completion.

5. OVERVIEW

Summary of proposed scope

This Safety Guide will provide recommendation for design and implementation of I&C systems important to safety and the software used in these systems. The guidance will be broadly applicable to nuclear power plants and are intended for application to both the design of new I&C systems and the modernization of existing systems. Guidance will be provided for classifying I&C systems by their importance to safety and on the application of design requirements to systems and components of different safety classification.

Draft Outline

The main headings of the proposed guide are given here. A preliminary detailed outline is attached to illustrate the specific topics to be addressed.

1. INTRODUCTION
    - Background
    - Objective
    - Scope
    - Structure
2. INSTRUMENTATION AND CONTROL FUNCTIONS AND SYSTEMS IMPORTANT TO SAFETY
3. SAFETY CLASSIFICATION
4. DESIGN BASIS
5. GENERAL DESIGN GUIDELINES (Including Human-Machine Interface)
6. SYSTEM SPECIFIC DESIGN GUIDELINES
7. COMPUTER BASED SYSTEMS AND SOFTWARE
8. HUMAN–MACHINE INTERFACE (Including Main Control Room and Emergency Control Room)
9. DESIGN CONFIRMATION AND DOCUMENTATION

REFERENCES

GLOSSARY

6. PRODUCTION: Provisional schedule for preparation of the document, outlining expected dates for:

Approval of DPP by the Coordination Committee	March 2009
Approval of DPP by the Safety Standards Committees*	June 2009
Approval of DPP by the CSS*	October 2009
Approval of draft by the Coordination Committee	April 2010
Approval by the Safety Standards Committees for submission to Member States for comments*	June 2010
Approval of the revised draft by the Coordination Committee*	March 2011
Review in NS-SSCS*	March 2011
Approval by the Safety Standards Committees for submission to the CSS*	June 2011
Endorsement by the CSS*	October 2011
Approval by the Publications Committee	November 2011
Target publication date	Early 2012:

Note * is necessary only for the Safety Standards.

7. RESOURCES

It is estimated that development of the new guide would involve approximately 40 weeks of effort by member states experts. This is based upon assuming 4 one-week expert meetings involving no more than 5 experts and an average of one week of work per expert between meetings.

Secretariat resources involved are estimated at 10 weeks of effort by agency staff plus support for expert travel and honoraria for experts whose effort is not otherwise funded.

Attachment – Preliminary detailed outline

DESIGN OF I&C SYSTEMS FOR NPP

PROPOSED OUTLINE OF NEW DOCUMENT

2009.08.12

1. INTRODUCTION

1.1 Background

1.2 Objective

1.3 Scope

1.4 Structure

2. INSTRUMENTATION AND CONTROL functions and SYSTEMS IMPORTANT TO SAFETY

2.1 Identification of I&C systems

2.1.1 I&C functions important to safety

2.1.1.1 Protection functions

2.1.1.2 Control functions

2.1.1.3 Testing functions

2.1.2 Types of I&C system important to safety

2.1.2.1 Protection systems

2.1.2.2 Interlock systems

2.1.2.3 Control systems

2.1.2.4 Information systems

2.1.2.5 Limitation systems

2.1.2.6 Risk reduction systems

3. SAFETY CLASSIFICATION

4. DESIGN BASIS