NATIONAL NUCLEAR REGULATOR

For the protection of persons, property and the environment against nuclear damage

POSITION PAPER

DESIGN AND IMPLEMENTATION OF DIGITAL INSTRUMENTATION AND CONTROL FOR NUCLEAR INSTALLATIONS

PP-0017

Rev 0

professionalism integrity valuing our people excellence teamwork

APPROVAL RECORD

	Name	Designation	Signature	Date
Prepared	S Alexander	Principal Engineer, USTSO (ISL, Inc.)		
Reviewed	P Mkhabela	Functional Coordinator: Design Safety		
	P Bester	Special Nuclear Projects Coordinator		
	G Lekhema	Specialist: Electrical Engineering		
	S Tshobeni	Senior Specialist: Electrical Engineering		
Recommended for Approval by	O Phillips	Senior Manager: SARA		
Approved	B Tyobeka	Chief Executive Officer		

Please note:

The original, signed document is retained by Record Management.

TABLE OF CONTENTS

1 INTRODUCTION

There have been tremendous advances in electronics, computers and digital communication networks. These new technologies have been incorporated into the digital instrumentation and control (DI&C) hardware and software currently available. Even though advanced DI&C systems have been used extensively in many other industries, their use in the nuclear industry is still very limited. The complexity of DI&C systems requires a comprehensive implementation plan to ensure that plant safety is maintained.

The main objective of the National Nuclear Regulator (NNR) is to provide for the protection of persons, property, and the environment against nuclear damage through the establishment of safety standards and regulatory practices. In accordance with these nuclear safety standards and regulatory practices, the NNR regulates the nuclear installations (NIs) in South Africa.

Most of the analog electrical and electronic instrumentation and control (I&C) systems in existing NIs are being upgraded to digital I&C systems (DI&C), i.e., digital computer-based and computer program (software)-driven systems. New NIs will most likely be designed with DI&C systems for original installation. This position paper details the NNR position on the design and implementation of these DI&C systems.

DI&C systems involve varying degrees of computer-based processing of digital signals, converted from analog electrical and electronic instrument signals, or from certain types of advanced sensors, which may provide digital output signals directly. The computer processing of instrument outputs, whether directly digital or converted from analog signals, involves various functions, including analysis/evaluation of measured parameters and trends against established set points, complex algorithms for derived parameters, sampling, comparison and combinations of signals (e.g., reactor protection functions, engineered safety feature actuation functions, sub-cooling margin monitors, etc.). The sensed parameters or derived, computed parameters provide input into display devices for indication and annunciation/alarm functions, recording, and are sent to other systems or functional modules via data communication channels. The parameters are also input into various programmed control functions, e.g., steam generator water level control, and automatic protective functions, the most important of which are those of the reactor protection system (RPS) such as automatic shutdowns (reactor trips or SCRAMs).

The upgrade of analog electrical and electronic instrumentation systems and analog electronic and electro-mechanical controls to DI&C systems in existing NIs is expected to involve a gradual transition period during which DI&C equipment will be integrated incrementally into the various analog electrical and electronic I&C systems.

In new NIs, which will undoubtedly be fitted with DI&C systems, the DI&C systems may also be integrated with analog I&C systems in certain critical applications as backup systems. In addition, it is expected that there will always be provisions for manual operator backup and override in certain applications, such as reactor shutdown.

The various phases of the life cycle of DI&C high important to safety and important to safety systems involves various parties, organisations, processes, and documents and require regulatory oversight.

For example, interventions carried out in the procurement process for DI&C components or software important to nuclear and radiation safety (hereafter referred to as safety) may be identified by the applicant, designer, independent inspector (if the code or standard requires the involvement of an independent inspector) and the NNR.

2 PURPOSE

The purpose of this position paper is to detail the NNR position regarding regulatory oversight by the NNR of the design and implementation of DI&C systems important to safety in existing NIs in South Africa as well as for new DI&C installations in future NIs. This position paper will:

i. Summarise and discuss the publicly available international guidance on nuclear safety DI&C;

ii. Discuss international DI&C regulatory standards and practices;

iii. Define and outline the process to be followed to commence the life cycle of DI&C important to safety in a nuclear installation, both in conjunction with and in advance of a nuclear installation license (NIL) for construction and/or operation;

iv. Specify the NNR requirements and deliverables associated with the authorisation process;

v. Define the pre-requisites for each nuclear safety DI&C life cycle phase; and

vi. Define actions in event on of non-compliance with NNR requirements.

The position of NNR on each key issue concerned with DI&C highly important to safety and important to safety is emphasized in boxed italic text.

3 SCOPE

3.1 All Nuclear Installations (Existing and future NIs)

This position paper is applicable to life-cycle aspects of highly important to safety and important to safety DI&C components of nuclear installations in South Africa. Non-safety related DI&C are not part of this position paper and such applications may be reviewed by NNR on a case by case basis. The NNR DI&C position addresses not only DI&C upgrades for operating nuclear installations (Nis), but also DI&C for proposed new designs. New NI designs involve a unique challenge in that the NI vendor and/or nuclear authorisation holder or applicant may not have sufficient design detail at the time of the application to facilitate meaningful review and evaluation.

3.1.1 Nuclear Power Plants (NPPs)

The provisions of this paper apply primarily to licensing of NPPs.

3.1.2 Research Reactors (RRs) and other NIs

The provisions of this paper will be applied to licensing of non-power (e.g., research) reactors and other licensing of NIs (e.g., fuel cycle facilities) as deemed appropriate by the NNR on a case-by-case basis.

3.2 Design and implementation (the entire DI&C life cycle)

The position paper addresses regulatory oversight of the entire DI&C life cycle, i.e., not only the design process, the design itself, and design verification activities, but also regulation of the implementation or execution of approved designs in terms of hardware manufacture, software development, hardware and software testing, software verification and validation, hardware installation and software integration, system operation, maintenance, and modifications. To accomplish its stated purpose, in the appropriate locations, this position paper addresses, among others, the following aspects:

i. International Regulatory Practice and Standards (Section 5)

ii. Industry standards (Section 5.3)

iii. Importance to safety, and safety classification (Section 6.5.1)

iv. Reactor Protection system requirements (Section 6.5.2)

v. Design requirements (Software Common Cause Failures in Safety Systems, Data Communication Independence, Complex Electronics, Simplicity in Design, Software Tools, Safety-Security Interface, System Architecture Considerations for Systems Classified at the Highest Safety Level) (Section 6.5.3)

vi. Verification and Validation throughout the life cycle of safety systems using digital computers, Qualification of Industrial Digital Devices of Limited Functionality for Use in Safety Applications, Factory and Site Acceptance Testing) (Section 6.5.4)

vii. Quality Management (Section 6.5.5).

viii. Configuration Management for Software (Sections 6.5.6)

ix. Surveillance and Periodic Testing (Section 6.5.7)

x. Applicable South African legislation and existing NNR licensing documentation (Section 6)

xi. Relevant nuclear authorisation holder requirements and international practices (Section 5)

3.3 DI&C Training and Qualification

It is the position of the NNR that authorisation holder and applicants for nuclear installation licenses in which one or more DI&C systems important to nuclear safety will be newly installed or in which existing I&C will be upgraded to or augmented by DI&C shall establish and effectively implement a formal training and qualification programme. Such programme shall be consistent with the staff duties and responsibilities, for all members of their staff whose duties and responsibilities include any aspect of the design, procurement, safety assessment, operational safety assessments and implementation of DI&C in new NIs or upgrade of DI&C in existing NIs, through all phases of the DI&C life cycle.

4 TERMS, DEFINITIONS AND ABBREVIATIONS

4.1 Terms defined in the NNRA or in the NNR regulations

In this position paper any word or expression to which a meaning has been assigned in the NNRA or SSRP shall have the meaning so assigned.

Verification means the process of evaluating whether the final product or system of a development phase meets the specified requirements for that phase.

Validation means the process of evaluating whether the final product or system of a development process satisfies the initial business requirement.

4.2 Abbreviations

Abbreviation	Explanation
AIA	Authorised Inspection Authority
ASME	American Society of Mechanical Engineers
BTP	Branch Technical Position (USNRC guidance – Similar to NNR PP)
CCF	Common-Cause Failure
CFR	Code of Federal (US) Regulations (Title 10, “Energy,” of the CFR, Parts 1 through 100, contain the USNRC regulations)
CM	Configuration Management
C&I	Control and Instrumentation (same as I&C)
COTS	Commercial, off-the-shelf
DAC	Design Acceptance Criteria
DBT	Design Basis Threat
DI&C	Digital Instrumentation and Control (same as DC&I or DIC)
DICWG	Digital Instrumentation and Control Working Group (of the MDEP)
DiD	Defense-in-Depth (also DID)
EPRI	Electric Power Research Institute
FSAR	Final Safety Analysis Report
GSR	General Safety Requirement
HDL	Hardware Description Language

Abbreviation	Explanation
HPD	HDL Programmed Devices
I&C	Instrumentation and Control (legacy type – same as C&I)
IAEA	International Atomic Energy Agency (United Nations)
IEC	International Electro-Technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IN	Information Notice (USNRC generic communication)
INPO	Institute for Nuclear Power Operations (US - affiliated with WANO)
ISG	Interim Staff Guidance (USNRC guidance – Similar to NNR PP)
ISO	International Organisation for Standardisation
MDEP	Multinational Design Evaluation Program (of the NEA)
NEA	Nuclear Energy Agency (of the OECD)
NEI	Nuclear Energy Institute (US)
NI	Nuclear Installation (includes NPPs, RRs, and fuel cycle facilities)
NIL	Nuclear Installation Licence
NNR	National Nuclear Regulator
NNRA	National Nuclear Regulator Act
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (United States – same as USNRC)
OECD	Organisation for Economic Co-operation and Development (parent organisation of the NEA and its MDEP)
PP	Position Paper
PRA	Probabilistic Risk Assessment (Analysis)
RD	Regulatory Document
RG	Regulatory Guide (USNRC guidance)
RPS	Reactor Protection System
RR	Research Reactor
RTD	Resistance Temperature Detector
QA	Quality Assurance
QC	Quality Control
QM	Quality Management
SANAS	South African National Accreditation System
SANS	South African National Standard
SARA	Standards, Authorisations, Reviews and Assessments (Division of NNR)
SARA-DS	Design Safety Department (of SARA)
SCM	Software Configuration Management
SDOE	Secure Development and Operating Environment
SRP	Standard Review Plan (USNRC – NUREG-0800)
SSC	Structures, Systems and Components
SSRP	Regulations in terms of section 36, read with section 47 of the NNR Act no. 47 of 1999 on Safety Standards and Regulatory Practises
Std	Standard

Abbreviation	Explanation
STUK	Finnish nuclear regulatory authority
TR	Technical Report
UK	United Kingdom
US	United States
V&V	Verification and Validation
WENRA	Western European Nuclear Regulators Association

5 INTERNATIONAL REGULATORY EXPERIENCE, PRACTICE AND STANDARDS

The processes and activities of the NNR in its oversight of nuclear safety DI&C design and implementation are informed by international nuclear regulatory practice and standards as prescribed and described in the standards and guidance of various international nuclear safety agencies and organisations as well as by the NNR's membership in and active participation in the deliberations of many of these organisations.

International experience relating to the licensing and implementation of DI&C are summarized in Appendix A. Fortunately, the difficulties experienced and the causes identified have resulted in some important lessons that can be used to inform the NNR DI&C design review and approval process going forward. The principal lessons learned are:

- Establish regulatory position and requirements as early as possible;
- Early and frequent interaction with applicants to develop sound understanding of regulatory expectations; and
- Consider developing defined regulatory review phases, especially for new reactors, so that licensing can proceed in a predictable way. Although Design Acceptance Criteria may not be ideal, waiting for the application final safety analysis report (FSAR) may not be ideal either.

The following sections list the requirements and guidance provided by international nuclear safety or regulatory organisations that South Africa and/or the NNR are members of. For details about requirements and guidance provided by other nuclear safety organisations, please consult Appendix B.

5.1 International Atomic Energy Agency (IAEA)

The NNR subscribes to the relevant guidance of the IAEA and such IAEA standards serve as references and benchmarks for the NNR's regulation, requirements and guidance, including that applicable to DI&C.

Whether IAEA guidance referenced herein is incorporated directly or by reference into the NNR DI&C regulatory framework, it is the position of the NNR that nuclear authorisation holders and applicants are expected to comply with relevant IAEA guidance*.*

5.1.1 IAEA Safety Requirements Relevant to DI&C

The following IAEA requirements documents are relevant to DI&C:

i. GSR Part 4 Safety Assessment for Nuclear Facilities and Activities;

ii. SSR-2/1 Safety of Nuclear Power Plants: Design; and

iii. SSR-2/2 Safety of Nuclear Power Plants: Commissioning and Operation;

5.1.2 IAEA Safety Guides Relevant to DI&C

The following IAEA guide documents are relevant to DI&C:

i. DS-431 (draft), "Safety Guide for I&C Systems in Nuclear Power Plants";

ii. NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants"; and

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

It is the position of the NNR that the provisions of IAEA Safety Guides NS-G-1.1 and NS-G-1.3, should continue to be used as guidance for applications for DI&C in existing NIs and for the DI&C to be used in new NIs. In addition, applicants for authorisations for DI&C upgrades to existing NIs and applicants for NILs for new NIs may also treat these guidance, as modified by MDEP recommendations, as interim NNR guidance.

5.2 Multinational Design Evaluation Programme (MDEP)

The NNR participates in the MDEP, which is a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities that will be conducting reviews of new reactor power plant designs.

MDEP has developed or is developing common positions on twelve (12) key issues for DI&C. Approved common positions are being submitted to the IAEA by the MDEP, and those presented have been accepted by the IAEA and will be incorporated into the appropriate safety guides.

MDEP has finalised common positions on 9 of the twelve (12) DI&C key issues it has identified relating to DI&C. These 9 positions are publicly available on the MDEP website: http://www.oecd-nea.org/mdep/working-groups/dicwg.html. The NNR has endorsed these common positions as a member of MDEP. The reader should consult the respective documents for context, references and definitions where applicable.

The titles of the developed common position papers are:

1. Generic Common Position DICWG-01: Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems
2. Generic Common Position DICWG-02: Software Tools
3. Generic Common Position DICWG-03: Verification and Validation throughout the Life Cycle of Safety Systems Using Digital Computers
4. Generic Common Position DICWG-04: Communication Independence
5. Generic Common Position DICWG-05: Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems
6. Generic Common Position DICWG-06: Simplicity in Design
7. Generic Common Position DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems
8. Generic Common Position DICWG-11: Digital I&C System Pre-installation and Initial On-site Testing
9. Generic Common Position DICWG-12: Use of Automatic Testing in Digital I&C Systems as part of Surveillance Testing

The titles of the three common positions which are in development process are:

i. Generic Common Position DICWG-07: Qualification of Industrial Digital Devices of Limited Functionality for Use in Safety Applications.

ii. Generic Common Position DICWG-09: Design Principles for the Overall I&C Architecture.

iii. Generic Common Position DICWG-10: Configuration Management for Software

It is the position of the NNR that the common positions listed above, once finalised by the MDEP, and described below are considered applicable to nuclear safety DI&C in authorised/licensed NIs.

Nuclear authorisation holders, citing this position paper as interim authority, may consider these common positions to be interim NNR guidance regarding DI&C. It is the expectation of the NNR that holders of or applicants for NILs or authorisations for DI&C upgrades, will adopt and comply with these common positions, adapted as *technically required by the application-specific circumstances. Deviations from these common positions should be documented and reported to the NNR and justifications shall be made available for NNR review.*

5.3 International Industry Standards and Guidance Relating to Nuclear Safety DI&C

The NNR recognises the international industry standards and guidance. However, except where codes and standards have been incorporated, or incorporated by reference in an element of the NNR regulatory framework applicable to DI&C, the NNR neither prescribes, nor endorses their use by nuclear authorisation holders. Instead, as is the normal practice, the nuclear authorisation holder or applicant is to select the codes and standards that it determines to be best suited and that represents good engineering practice for its particular NI and DI&C systems and provide the safety case or justification for their use to the NNR. The NNR will review the case and make a determination whether the justification is adequate.

6 NNR REGULATORY FRAMEWORK APPLICABLE TO DI&C

The NNR licenses and regulates NIs under the various provisions of the NNR Act, and therefore exercises regulatory oversight of all phases of the life cycle of DI&C used or to be used in nuclear safety applications in NIs.

6.1 National Nuclear Regulator Act – Applicability of the NNRA to DI&C

Section 2(1) (a) of the NNRA [1] provides, in part, that the NNRA applies to the design, construction, and operation of any NI. Design of the NI would include design of the SSCs of the NI and their component parts, which would include DI&C hardware and software. Design is the initial phase of the DI&C life cycle and is therefore subject to the provisions of Section 2(1) (a) of the NNRA. NNR Position Paper PP-0008 [9], "Design Authorisation Framework," further describes the overall NNR regulatory framework and processes for the regulation of the design of NIs and their SSCs.

Section 5(b)(i) of the NNR Act provides, in part, that the NNR, amongst others, exercises regulatory control related to safety over the design, manufacturing, construction, and operation of nuclear installations (NIs), through the granting of nuclear authorisations. For this purpose the safety assessment and supporting documentation submitted in support of an application for approval by the NNR of the upgrade and/or supplementation/augmentation of nuclear safety C&I with DI&C, or for the approval of nuclear safety DI&C in new/proposed NIs, must cover the all phases of the life cycle of nuclear safety DI&C as specified in the boxed text below.

Specifically, with regard to DI&C systems and equipment (including hardware, software, and software tools) to be used in applications important to safety in NIs, the position of the NNR is as stated in PP-0012, and for the purposes of this position paper, additionally as follows:

- *The terms "design," "manufacture," "construction," and "operation," as referred to in Section 5(b)(i) of the NNR Act, are deemed to include all phases of the life cycle of DI&C to be used in applications important to safety in NIs.*
- *For the purposes of this position paper, the term "NIs" includes existing and proposed nuclear power plants (NPPs), research reactors (RRs), and fuel cycle facilities. The provisions of this position paper are fully applicable to NPPs and will be applied to other types of NIs in a graded, risk-informed manner, commensurate with safety significance and other factors as determined by the NNR on a case-by-case basis.*
- *The phases of the DI&C life cycle recognised by the NNR, encompassed by the terms "design," "manufacture," "construction," and "operation," within the meaning of Section 5(b)(i) of the NNR Act include equipment and software design important to nuclear safety, design verification (including equipment qualification (seismic and environmental) and software verification and validation (V&V)), equipment manufacture and software development, vendor equipment and software testing, procurement, acceptance by the nuclear authorisation holder for DI&C upgrades to existing NIs, or acceptance by the applicant for new construction (including, for commercial, off-the-shelf (COTS) equipment, software and software tools, commercial-grade dedication), safety assessment by the NNR, installation of equipment and integration with software, inspection and pre-operational testing, and operation, which is deemed to encompass DI&C maintenance and modification.*

The NNR is therefore mandated to perform regulatory control over all phases of the life cycle of DI&C in applications important to nuclear safety in NIs. To this end, the NNR will determine, informed by international standards and practice, which phases of the life cycle of DI&C important to nuclear safety may commence prior to obtaining a relevant nuclear authorisation from the NNR for applicants for new NI licenses (NILs) and for existing NIs, which phases require prior approval by the NNR for nuclear authorisation holders. In cases in which certain phases may commence without prior approval, the NNR will exercise final approval authority. In all cases, under the auspices of Section 5(b)(i) of the NNR Act, and other legislation, regulations/standards and guidance cited herein, the NNR will exercise regulatory oversight before, during and after all phases of the life cycle of DI&C in nuclear safety applications.

6.2 Safety Standards and Regulatory Practices (SSRP)

The SSRP [2] sets forth high-level safety standards. Those most directly applicable to the design and implementation of DI&C important to safety are as follow:

6.2.1 SSRP Section 3.4 Good Engineering Practice

Installations, equipment or plant requiring a nuclear installation license, a nuclear vessel license or a certificate of registration and having an impact on radiation or nuclear safety must be designed, built and operated in accordance with good engineering practice.

6.2.2 SSRP Section 3.5 Safety Culture

A safety culture must be fostered and maintained to encourage a questioning and learning attitude to radiation protection and nuclear safety and to discourage complacency.

6.2.3 SSRP Section 3.7 Regulatory approval of radiation protection and nuclear safety measures

SSRP Paragraph 3.7.1 - The holder of the nuclear authorisation is responsible for radiation protection and nuclear safety, including compliance with applicable requirements such as the preparation of the required safety assessments, programmes and procedures relating to the siting, design, construction, operation and decommissioning of facilities.

SSRP Paragraph 3.7.2 - Situations where formal approval of radiation protection and nuclear safety measures by the Regulator is necessary should be limited to those where this is appropriate taking into account the nature and extent of the risk and the need for building stakeholder confidence.

6.2.4 SSRP Section 3.8 Accident Management and Emergency Planning, Emergency Preparedness and Emergency Response

Where the prior safety assessment or operational safety assessment has identified the reasonable possibility of a nuclear accident, accident prevention and mitigation measures based on the principle of defence-in-depth and which address accident management procedures including emergency planning, emergency preparedness and emergency response must be established, implemented and maintained. The principle of defence-in-depth must be applied as appropriate.

The applicability of this standard to DI&C important to safety lies mainly in the C&I functions in support of accident prevention, mitigation and emergency response.

I&C systems involved with accident prevention would include operational plant process control systems, process variable indication, nuclear instruments, display, alarm and recording functions (e.g., safety parameter display system), reactor protection system interlocks, and any other pre-accident automatic protective actions. It could be argued that automatic and manual reactor shutdown functions are not accident-preventive measures for pre-accident, but unsafe plant conditions in which prompt reactor shutdown are directly necessary to prevent core damage.

I&C systems or functions involved with accident mitigation would include the sensors, processors (e.g., analogue-to-digital converters for DI&C) indicators/displays, control function processors, alarms, and recorders, and data communications. These support the reactor protection system, emergency onsite electric power and switch-over systems (e.g., automatic load sequencers), engineered safety features such as safety coolant injection system(s), emergency core cooling system(s) (including short- and long-term decay heat removal), reactor pressure relief systems, emergency boron injection system, sub-cooling margin monitors, reactor vessel level indication system(s), containment isolation system, containment pressure indication, alarm and manual and automatic control measures (e.g., containment spray), containment heat removal system(s), containment atmosphere radionuclide mitigation and system(s) (e.g., chemical spray), reactor coolant effluent collection and disposition system(s) (e.g., sump), hydrogen combustion prevention measures, radiation monitoring (including ex-core neutron detection), control room radiation protection and atmosphere control, post-accident monitoring systems, and dedicated emergency data communications channels.

6.2.5 SSRP Section 3.9 Defence-in-Depth (DiD)

One of the major concerns with DI&C is the increased failure probability inherent with complexity and the increased vulnerability to distributed-fault or common-cause failures (CCFs). One of the main means to prevent and mitigate the effects of CCF in DI&C, especially software-related CCF, is DiD. DiD is achieved through a systematic combination of multi-layered measures implemented for failure prevention (including reduced probability of failure and failure propagation, fault tolerance, and early detection through advanced diagnostics and prognostics) and failure mitigation in both the design and mode of operation of DI&C systems.

These measures include (1) redundancy (e.g., multiple parallel channels, backup(s) & spares, etc.), (2) diversity (multiple fundamentally different means of function performance), and (3) independence (including functional and physical separation) of redundant and diverse systems, trains or channels. An example of redundancy and independence would be the typical multiple RPS channels with comparison protocols to prevent protective action based on invalid (or test) signals, yet ensure protective action with valid signals (e.g., the so-called “2-out-of-4, taken twice” scheme).

Regarding DiD (equally applicable to DI&C), SSRP Section 3.9 defines DiD and states: “A multilayer (defence-in-depth) system of provisions for radiation protection and nuclear safety commensurate with the magnitude and likelihood of the potential exposures involved shall be applied to sources such that a failure at one layer is compensated for or corrected by subsequent layers, for the purposes of

(a) preventing nuclear accidents;

(b) mitigating the consequences of any such accidents; and

(c) restoring sources to safe conditions after any such accident.”

The position of the NNR regarding defence-in-depth in DI&C is that the design and available modes of operation will increase fault tolerance and minimise the probability of adverse effects of failures, failure propagation, and especially CCF, by providing not only for redundancy (as SSRP Section 3.9 focuses on), but also diversity (alternate and different means or paths) with independence among the successive layers, and diverse paths to assure reliability of satisfactory accomplishment of critical DI&C functions under all design-basis conditions.

6.2.6 SSRP Section 3.10 Quality management

SSRP Section 3.10 states: "A quality management programme must be established, implemented and maintained in order to ensure compliance with the conditions of the nuclear authorisation."

The general requirements for a quality assurance (QA) and management (QM) programme are delineated in RD-0034 [6].

For DI&C, the position of the NNR is that safety through DI&C reliability, through QA is achieved through a rigorous nuclear safety-grade QM and safety management programme established and effectively implemented throughout all phases of the DI&C life cycle and includes QA and quality control (QC) in design, design verification, software verification and validation (V&V), design safety assessment, procurement (including component (hardware and software) and supplier selection and qualification), factory acceptance testing, hardware installation, software integration, site acceptance testing and commissioning, operation, maintenance and modification.

Effective QM in hardware and software configuration management (CM), in which the QM programme ensures rigorous adherence to the approved configuration management plan, is needed to provide absolute assurance that modifications post-commissioning will only serve to enhance performance and reliability and not degrade them. Effective QM and CM should also provide reasonable assurance that modifications will not introduce incompatibilities (or create single-point vulnerabilities) with other modules or functions (upgradability while maintaining downward compatibility with other modules, functions or interconnected or interdependent systems).

The QM programme of a nuclear authorisation holder or applicant must meet the requirements of RD-0034, and conform to an accepted and justified implementing standard.

While not generically prescribing or endorsing a particular QM programme, the NNR will routinely review the QM programmes (and their implementation) of nuclear authorisation holders, applicants, DI&C vendors, and subcontractors (e.g., installation and site acceptance testing technicians) through audit and inspection at various strategic junctures to determine or confirm the adequacy of the program consistent with its particular application and its effective implementation. Applicants for an authorisation for the DI&C of a new plant or an authorisation to upgrade parts of its existing I&C systems should carefully select a QM programme suitable for its particular application and submit the written QM programme governing documents, plans and procedures for NNR review. Then they should maintain auditable records of objective quality evidence to demonstrate compliance during NNR audits and inspections to determine the effectiveness of the programme implementation.

6.2.7 SSRP Section 3.11 Application of Radiation Protection and Nuclear Safety

The application of the radiation protection and nuclear safety requirements contained in these regulations to any action should be commensurate with the characteristics of the action and with the magnitude and likelihood of the exposure, as determined in the safety assessments. Not all the requirements are relevant to every action. The applicability of this high-level standard to DI&C should be self-evident and consistent with the DI&C function(s) supporting safe operation of the NI.

6.2.8 SSRP Section 4: Requirements Applicable to Regulated Actions

The performance and reliability of the DI&C of a safety system is necessary for normal safe operation and for the system to pass technical specification surveillances. The following high-level requirements apply to actions and have relevance to DI&C safety systems performance and reliability:

i. SSRP Section 4.2 Controls and Limitations on Operation
ii. SSRP Section 4.3 Maintenance and Inspection Programme
iii. SSRP Section 4.4 Staffing and Qualification

6.3 Requirements Documents

The NNR establishes requirements based on international best practices. These requirements are registered either directly in the authorisations or in requirements documents.

6.3.1 Existing NNR Requirements Documents (RDs) with Relevance to DI&C

Currently there are no RDs directly applicable to DI&C, but the three listed below have some relevance applicable to DI&C (i.e., installed in plant systems important to safety). At this time, all of the DI&C-specific detailed guidance is at the additional requirements level; and is considered interim guidance as stated in each case. However, the NNR is considering the guidance as described in this position paper and may elevate some of it as deemed appropriate to the level of requirements.

i. RD-0016: Requirements for licensing submissions involving computer software and evaluation models for safety calculations

ii. RD-0024: Requirements on Risk Assessment and Compliance with Principal Safety Criteria for Nuclear Installations

iii. RD-0034, “Quality and Safety Management Requirements for Nuclear Installations”

6.4 Interim DI&C Specific Guidance

The DI&C-specific guidance expressed in this section is interim guidance, pending further consideration by the NNR, which will be informed by its participation in DI&C-related international working groups (e.g., the DCIWG of the MDEP) and other forums of a similar nature as described in Section 5 above as well as by the interaction of the NNR with other organisations. This section will state the NNR position on various international and other national regulations, guidance and practices.

The NNR position on industry codes and standards, as expressed in the existing guidance is that in general, it neither prescribes, nor endorses particular industry codes and standards generically as is the practice of certain other nuclear regulators (e.g., the USNRC). Rather the NNR will consider the suitability of codes and standards proposed and justified in applications for authorisations on a case-by-case basis, except as may be stated herein.

6.4.1 NNR Position on International Nuclear Safety Standards and Practices

Pending formal adoption and integration of selected DI&C-related international and other national safety standards and practices by the NNR into its regulatory standards, the position of the NNR is that the DI&C-related IAEA documents cited in Section 5.1 above and the MDEP/DICWG Generic Common Positions as specified in Section 5.2 above may be relied upon as NNR interim guidance governing the design and implementation of DI&C in applications important to safety in NIs.

6.5 Discussion and NNR Position on Key Issues Related to DI&C

6.5.1 Importance to safety, and safety classification

The safety classification system used by the NNR is defined in RD-0034. It has three levels of classification:

1. Level 1: Highly important to safety
2. Level 2: Important to safety and
3. Level 3: Not important to safety

For new NIs and upgrade of C&I in existing NIs, the DI&C for systems important and highly important to safety will be classified in general at the same level as the parent system, which will in general, be the same safety class in which current I&C systems are classified.

The process of modern safety classification is performed through both deterministic and probabilistic evaluations. The classic deterministic approach would result in a qualitative characterisation regarding the nature of the importance to safety of any structure, system or component (SSC), or process, evolution, procedure or practice.

If desired, a quantitative assessment of the safety or risk significance or the degree of importance to safety of SSCs can be developed using insights from a probabilistic safety assessment (PSA).

Many important to safety I&C systems and equipment are classified as being safety-related (level 2) and highly safety/risk-significant systems (level 1) in the plant. The highly important to safety systems typically include the following:

- reactor protection systems,
- engineered safety features actuation systems (ESFAS), e.g., emergency core cooling and feed-water,
- safe shutdown systems, e.g., for the fast insertion of absorber rods or injection of neutron absorbing liquid,
- emergency power supply and diesel generator control systems.

The safety related systems typically include the following:

- information systems important to safety, e.g., displays in the main control room or the neutron flux in-core monitoring system,
- interlock systems important to safety,
- reactor control systems and access control systems,
- some data communications systems, and
- essential auxiliary supporting systems, e.g., control room heating, ventilation, and air conditioning.

6.5.2 Reactor Protection System (RPS) Requirements

In general, the RPS must be capable of automatically recognising plant conditions that fall outside specified limits and initiate prompt action to put the plant in a safe condition (e.g., shut down the reactor) in a manner that minimises the possibility of false indications causing unwanted reactor protection action, but reliably acts upon recognition of valid protection conditions. This is typically done by having several independent protection channels with a scheme to confirm the validity of the sensed unsatisfactory condition, e.g., 2 out of 4 signals, taken twice.

The RPS should also allow for testing without causing unwanted or unnecessary protective action; while not preventing a valid signal from initiating protective action. In addition, the RPS must provide for operator initiation of protective action.

To that end, the RPS may be responsible for automatic alarms or warnings to operators of plant conditions that are trending in an unsafe direction and/or have exceeded limits within those that cause automatic protective actions, to allow the operators to assess the situation and take corrective action before it becomes necessary for the RPS to initiate protective action.

The automatic inputs to the RPS are typically direct reactor plant parameters – conditioned signals from plant instruments and nuclear instruments, or specialised combinations and/or comparisons of parameters that are better indicators of the plant’s proximity to its limits. The direct reactor plant parameters of pressures, temperatures, power (neutron flux), reactor coolant flow and reactor period or startup rate are often used. In addition, some RPSs also use combinations of parameters such as over-temperature/delta temperature. Some systems also use direct indicators of loss-of-coolant accidents (LOCAs) (e.g., drop in pressuriser level more than a specified amount without a corresponding proportional change in reactor coolant average temperature and absent normal operations or evolutions that reduce coolant inventory without a change in temperature (e.g., discharging coolant or pressuriser venting), or high-energy line breaks (e.g., feed water or main steam-line ruptures)

The system must provide for various types of reactor trips (scrams) that cause the prompt and rapid insertion of certain or all control rods partially or fully depending on the situation. The system should be fail-safe such that functional failures put the plant in a safe condition. In addition, it may be necessary to prevent certain plant conditions that could result in large and rapid reactivity additions for which trips or scrams are not sufficient to prevent exceeding thermal limits before power is turned on. Such preventive measures may include automatic interlocks that won’t allow certain actions that could cause reactivity addition accidents.

There should be measures for reliability through defence-in-depth, including redundancy and diversity in the various RPS functions. In addition, like other DI&C systems important to safety, the RPS should have surveillance, diagnostic, and prognostic functions that continuously monitor system performance (process and data) to detect and recognise system failures and/or known failure precursors in order to alert operators, or under certain conditions, take corrective action, in a timely manner. There are various techniques including the simplest data parity checking to more sophisticated techniques such as parallel processing of identical inputs with output comparison, analysis of output changes with no input changes, etc.

When the RPS is a digital system, it introduces additional capability, coupled with a higher level of complexity which affects the reliability of software and hardware..

6.5.3 Design Requirements

This discussion of DI&C design requirements will address the key areas of interest, including the following: Software Common-Cause Failures in Safety Systems, Data Communication Independence, Complex Electronics, Simplicity in Design, Software Tools, Safety-Security Interface, System Architecture Considerations for Systems Classified at the Highest Safety Level.

There are many challenges related to the use of DI&C systems, e.g., common-cause failures (CCFs). As explained in IAEA Safety Guide NS-G-1.3, and as alluded to above, the greater complexity of DI&C systems, and the greater interaction among subsystems, increase the possibility that a latent fault can exist in the system that could be triggered and propagate, thus causing the system to not perform as expected. The fact that the generation of software can be prone to failures, and the possibility that copies of the same software might be used in redundant channels of a safety system, create an additional potential for CCFs. Common measures to prevent CCFs, which contribute to defence-in-depth, are diversity, redundancy and independence. Additional diversity, redundancy and independence, however, also increase a system’s complexity and raise the possibility that the additional complexity may pose a larger risk of human errors in design, operation, and maintenance than the common cause failure they were intended to avoid. To compensate, one way to simplify the design, manufacture and use of digital I&C systems is to use prequalified ‘commercial off-the-shelf’ (COTS) hardware and software components that have been thoroughly tested and evaluated for nuclear power plant applications (dedication, including seismic and environmental qualification).

In summary, the NNR position on fundamental DI&C design principals expects the following:

i. *Design of digital systems for the highest safety classification should be as simple as practical.*

ii. *All unnecessary complexity should be avoided both in the functionality of the system and in its implementation, both in software and hardware.*

iii. *All features should be demonstrated to be beneficial to safety in consideration of the impact of their added complexity to the design. This complexity cannot lead to violation of other design principles (for example, independence, redundancy, diversity).*

Highly integrated control room designs with safety and non-safety displays and controls will be the norm for new reactor designs and implements digital communication systems. The following sections highlight pertinent issues that must be considered in the design of DI&C systems.

6.5.3.1 Communication between Safety and Non-Safety Systems

With DI&C technology, judicious communication between redundant safety channels and between safety and non-safety systems may enhance reliability and safety more than could have been attained when existing operating nuclear power plants were designed with analog technology. Proposed designs include varying degrees of communication between redundant safety channels and between safety and non-safety systems to validate signals and ensure high reliability.

6.5.3.2 Requirement for Unimpaired Safety Function

It should be demonstrated that the provisions for the implementation of communications among redundant safety channels and between safety and non-safety systems and the communication processes and messages themselves do not impair the proper execution of the associated safety functions through unintended behaviors or inadequately managed failure modes or by any other means or influence. Issues such as two-way communication, data density, and communication traffic levels appropriate for safety-related applications need to be addressed in the documentation of proposed designs.

The protection system shall be separated from a system of lower classification to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems does not result in loss of the necessary minimum reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

These provisions regarding interconnection of protection and control systems limit two-way communication between safety and non-safety systems. International industry consensus standards indicate such communication pathways are acceptable provided that:

- failure of the communication system does not impair the safety function, and
- the safety function does not rely on non-safety system inputs to operate.

The NNR will consider for authorisation on a case-by-case basis digital safety systems that use limited two-way communications between safety and non-safety components to allow safety system reconfigurations while in operating modes specifically designed to accept changes (e.g., test mode for testing a channel and Inoperative mode for changing set-points and performing channel maintenance).

6.5.3.3 Requirement for Independence and Isolation

Some of the new control room designs may apply strategies for integrating safety- and non-safety-related controls within the same controller or display device. The proposed controls and displays could include extensive two-way communications among safety channels and between safety and non-safety channels.

Applicants should demonstrate that proposed mixed-channel displays and controls and operation of safety devices by means of non-safety controls or of controls in other channels maintain the required independence and isolation of redundant safety systems.

6.5.3.4 Failure Analysis Techniques and Mitigation Measures

The NRC is developing failure analysis techniques for use in the evaluation of complex digital communication systems proposed for use within and among redundant safety channels and between safety and non-safety channels. The primary objective of this effort is to develop a comprehensive process for confirming that an integrated control room design conforms with 10 CFR Part 50.55a(h), "Protection and Safety Systems" requirements and the requirements in associated standards and regulatory criteria for areas such as

- electrical separation and independence between safety- and non-safety-related displays and controls;
- single failure criterion;
- equipment qualification of Class 1E safety-related displays and controls; and
- data communication isolation.

The NRC's regulatory criteria for these requirements are found in Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

Nuclear authorisation holders or applicants who cite this guidance in applications for authorisations of new NILs, or to upgrade the I&C of an existing nuclear installations should justify suitability of their particular nuclear installations and the NNR will consider approving each application on a case-by-case basis.

6.5.3.5 Highly Integrated Control Rooms - Human Factors

Vendors of proposed new nuclear power plant designs and modernised control rooms for existing reactors are taking advantage of advances in digital technology to change the control room from a collection of discrete controls and analog displays to a highly integrated glass cockpit-style control room design. These technologies may include touch-screen video display devices, semi-autonomous controls, and other advanced operator interfaces and technologies.

Applicants should identify relevant international standards and demonstrate that the following factors meet specified requirements to help the plant operator, to both (1) understand current plant conditions and unexpected events and (2) respond promptly and effectively to them:

- *physical and virtual locations of displays and controls;*
- *the distribution of functions among display panels and backup devices;*
- *the use of color and other graphical display attributes;*
- *provisions for navigation among display screens;*
- *provision of backup devices and the conditions and procedures under which they are used; and*
- *other factors relating to the use of the control and protection systems by plant operators.*

6.5.3.6 Defense in Depth – Diversity, Redundancy, and Independence

Industry experience with DI&C systems has shown that reliance upon quality assurance processes alone has not been adequately effective at preventing CCFs even in high integrity digital systems. Unanticipated CCFs or distributed faults are more likely in digital systems than in analog systems. Therefore, it is also more important to ensure that digital technology is applied in a manner that addresses functional DiD, functional diversity, and system diversity features. In addition, it is necessary to confirm that CCF vulnerabilities are not introduced when a system is modified or during version upgrade.

Nuclear power plant safety system functionality rely on design principles to compensate for failures that could degrade safety system reliability, specifically:

i. Functional DiD

ii. Functional diversity, and

iii. System diversity

Each safety function in a nuclear plant must operate regardless of failures from within or outside the safety system. The NNR regulation establishing the requirement for DiD is Section 3.10 of the SSRP.

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident and associated environmental conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable to the specified requirements. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. These requirements mandate diverse design features to minimise the possibility of a CCF that could result in the loss of a protection function.

6.5.3.7 Cyber Security in Digital Instrumentation and Controls

The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside or inside of the digital instrumentation and control system. The process of defending against this class of failures is made more challenging by the rapidly evolving "industry" that continues developing new attack methods. Various individuals and undocumented organisations develop viruses, worms, and associated computer programs. Others concentrate on developing methods for gaining access to protected data and systems with the intent to disrupt system operations or illegally obtain information from the systems.

Authorisation holders have to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design-basis threat (DBT).

In particular, authorisation holders shall protect digital computer and communications systems and networks associated with the following categories of functions, from those cyber-attacks:

i. safety-related and important-to-safety functions

ii. security functions

iii. emergency preparedness functions, including offsite communications, and

iv. support systems and equipment, which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Authorisation holders should further protect such systems and networks from those cyber-attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, services, or data; and impact the operation of systems, networks, and equipment.

It is important to establish a Secure Development and Operational Environment (SDOE) for digital safety systems. The establishment of a SDOE refers to:

(1) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications; and

(2) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational. Note that while these SDOE features may also serve a cyber-security function.

6.5.4 Verification and Validation (V&V)

This section addresses V&V throughout the life cycle of safety systems using digital systems factory and site acceptance testing.

In simple terms verification confirms whether the development process is building the product or system right, whereas validation confirms whether the development process is building the right product or system.

It is the position of the NNR that V&V should be applied after each phase of the software life cycle in which errors or faults could have been introduced, especially after modifications, failures of software or hardware, and periodically as a surveillance measure to confirm the basis for continued confidence in the software reliability.

V&V tools are used to simplify and organise the testing required for each phase of the software development life-cycle. They do not have a direct effect on the final software output. However, they can be susceptible to failing to locate errors in the software or they may be used to justify eliminating other verification and validation tasks or to justify eliminating programming functions that can catch faults such as fault handling subroutines.

Therefore, just as flawed software development tools can introduce errors, and flawed software V&V tools can fail to detect errors, it is the position of the NNR that those used for V&V of DI&C software important to safety should be developed under nuclear QA controls, or undergo rigorous dedication under QA controls.

The following table delineates the types of tools used for V&V tasks:

V&V tasks	Software Tool	Description
Verification	Specification Traceability Analysis	Tools that support the ability to perform traceability analyses.
	Specification Analyses	Tools that support the ability to perform analyses based upon the requirements and design data available to the tool.
	Source Code Analysis	Tools that support the ability to input source code in one or more specific languages and perform analyses.
Validation	Proof of Correctness Techniques	Tools that support the ability to formally prove assertions about features or operations of the software to be validated.
	Failure Analysis	Tools that support the ability to analyse failures and trace them back to defects.
	Defect Analysis	Tools that support the ability to analyse defects and trace them forward to failures.
	Test Case and Expected Result Entry	Tools that support user entry of test cases and entry of expected test case results.
	Test Case and Expected Result Generator	Tools that support the ability to automatically generate test cases based upon existing requirements, and/or design specification data available to the tool, and to automatically generate expected test case results.
	Test Traceability	Tools that support the traceability of test activities and data.
	Source Code Instrumentation	Tools that support the ability to automatically instrument code to be tested in order that test events can be identified and recorded.
	Input Capture and Replay	Tools that support the ability to capture operator inputs (e.g., keyboard, mouse) and the extent to which such data can be edited and replayed in subsequent test cases.
	Test Driving	Tools that support the ability to execute and/or replay test cases.
	Run-time Analysis	Tools that support the ability to analyse the performance of a program as it executes.
	Reliability Analysis	Tools that support the ability to analyse measures of software reliability.

V&V tasks	Software Tool	Description
	Test Coverage Analysis	Tools that support the ability to analyse and report on test coverage, including system coverage analysis and function coverage analysis.
	Test Procedure Management	Tools that support the ability to manage test activities and a test program.
	Regression Testing	Tools that support regression testing.
	Automatic Result Checking	Tools that support the ability to automatically compare expected test case results and actual test case results.
	Test Statistical Analysis	Tools that support the ability to statistically analyze and report on test results.
	Operations Environment Simulation	Tools that support the simulation of a real operations environment, such as a large number of users, as well as various scenarios of use and various configurations.
	Integration Testing	Tools that support software integration activities.

For commercial-grade (commercial, off-the-shelf or “COTS”) DI&C systems, equipment, software and services to be used in nuclear plant applications important to safety that were not designed and manufactured/ developed under a suitable nuclear QA program, prospective important-to-safety components should undergo a process of so-called **commercial-grade dedication**, which is itself conducted under the applicable controls of an approved nuclear QA program, and provides equivalent, reasonable assurance that the item (or service) will reliably perform its intended function(s) for its prescribed mission time throughout its design service life, and is compatible with its parent systems and service conditions.

The dedication process shall include a design verification process as part of qualification to demonstrate that the item will function under all design-basis conditions, including normal, abnormal, and accident harsh environments, and not fail in a manner that could impact safety and/or mislead the operator. The dedication process should also include consideration of relevant operating experience and any other technical information.

6.5.5 Configuration Management for Software

Configuration management is required for all systems especially SSCs important to safety, including DI&C hardware and software. The principles and intentions of traditional configuration management apply equally to software, but with software there is a greater emphasis on design process, and the deliverable product is more like a design output. In the production of engineered hardware, design outputs are inputs to a manufacturing process, and configuration management activities focus on ensuring that design outputs and manufacturing process variables are traceable to identifiable manufactured products. In contrast, with engineered software, a large amount of design process information and many intermediate design outputs are associated with the final design output. Relatively many software engineering changes are expected and encountered. Consequently, with software configuration management (SCM), there is greater importance of intermediate design baselines and associated design process information. The needs for rigorous change management and identification and control of product versions are also substantially increased.

Applicants applying for NNR approval of DI&C systems should, submit software configuration management plans for NNR review. The quality assurance criteria should include criteria for administrative control, design documentation, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information associated with parts and components.

6.5.6 Surveillance and Periodic Testing

The NNR position in this area is that surveillance and periodic testing be performed throughout the software life cycle, subject to review of individual applications by the NNR, which may specify additional guidance as it deems appropriate. Software testing, including software unit testing, is a key element in software verification and validation activities. However, with the complexities of DI&C systems and software, and as mentioned above, there is increasing chance for development and propagation of errors. The NNR supports programs for vigilant monitoring through automated diagnostic and prognostic functions as well as periodic operator conducted surveillance testing according to the interim guidance as a key component of high reliability in critical applications. Applicants for DI&C authorisations should propose codes and standards, which will be considered by the NNR on a case-by-case basis.

6.5.7 Relationship of DI&C to Conventional I&C

The following numbered provisions detail the position of the NNR on the relationship between digital instrumentation to analog electrical and electronic instrumentation (sensors, processors, display, recording, annunciation, alarm, and input to control functions) and to purely mechanical instrumentation (i.e., direct reading gages for pressure, temperature, level, and flow, and direct reading indicators for position and condition, e.g., open/shut, run/stop, etc.). This includes the relationship of digital controls (e.g., programmable logic controllers (PLCs)) to conventional electric, electro-mechanical controls, purely mechanical controls, and manual controls. Technically justifiable relaxations of these positions may be approved by the NNR on a case-by-case basis, consistent with international standards and practice.

Nuclear authorisation holders and applicants shall establish appropriate procedures and conduct appropriate training to effectively implement these provisions:

1. *Where purely mechanical instrumentation is provided in existing nuclear installation it may be retained, used, but shall be maintained according to currently approved procedures and practices. When one or more instrumentation systems of an existing nuclear installation are being upgraded to be replaced by or augmented / supplemented with digital instrumentation, the proposed designs for new nuclear installations, shall be consistent with the requirements and constraints of new nuclear installation designs.*
2. *Where purely mechanical, manual controls such as manual valves, levers, switches, pumps, hand-cranks, adjustment or selection devices, etc., are*

provided in existing nuclear installation, they may be retained, used/operated, but shall be maintained in accordance with currently approved procedures and practices. When one or more control systems, functions or devices of an nuclear installation are being upgraded to be replaced by or augmented/supplemented with digital, i.e., computer-controlled functions, the proposed designs for new nuclear installations, shall be consistent with the requirements and constraints of new nuclear installation designs.

3. *In certain safety systems of highest importance to safety, existing analog electric and electronic instrumentation for critical parameters may be supplemented or augmented with digital systems and equipment to perform one or more of the following functions for those critical parameters and conditions: sensing, display, recording, annunciation, alarms, and inputs to automatic control and protective functions, to the extent technically feasible/practicable and appropriate for normal/routine operation. However, the existing instrumentation for such critical parameters and conditions shall be retained and maintained for DiD (diversity and redundancy).*
4. *Whether in existing nuclear installations or proposed new designs, the digital instrumentation systems that are to augment or supplement existing or required analog systems of the type subject to Provision No. 3 above shall use dedicated, independent sensors, whether conventional, requiring analog-to-digital conversion of their output, or advanced special sensors with direct digital output. For example, where a conventional cold-leg temperature instrument channel uses the output of a resistance temperature detector (RTD) as its sensor for direct input to a bridge circuit, the corresponding supplemental digital instrument channel, shall have a dedicated, separate and independent RTD, thermocouple or other electrical or electronic temperature sensing element. The output signal of this sensor is sent to an analog-to-digital converter to enable processing in the digital channel, or an advanced, special sensor with direct digital output compatible with the digital channel. In cases where an existing system is already fitted with spare sensors, they may be used for the digital instrument channel provided that it does not reduce the design margin in terms of DiD (redundancy, diversity and independence) or maintainability.*
5. *In certain cases in existing nuclear installations in which installation of an additional fitting, e.g., a thermal well or pressure tap in piping or vessels, that forms part of the reactor coolant or other critical, highly safety-significant fluid system pressure boundary is required when existing thermal wells or taps cannot accommodate additional sensing elements for the supplemental digital instrument channel, and where installing a new fitting could reduce the design margin of the integrity of the pressure-retaining boundary, then the NNR will consider on a case-by-case basis technically justifiable requests for sharing of existing sensing elements.*
6. *In addition to normal alignment and calibration, there shall be documented, periodic, simultaneous comparisons of corresponding indicated values of the analog instrumentation of the type specified in Provision No. 4 above with those of the corresponding digital instrumentation, and deviations that exceed the known and/or allowable/prescribed instrument errors shall be promptly investigated, and the cause(s) determined and corrected.*

7. *Similarly, in the safety systems of highest importance to safety, existing critical, manually initiated or automatic analog electronic, electric, electro-mechanical, or automatic mechanical (e.g., diesel engine governor) control and protective systems or devices may be supplemented or augmented with digital, i.e., computer-controlled, plant control functions to the extent technically feasible/practicable and appropriate for normal operation. However, the existing systems and/or devices for such critical control and protective functions may be retained, but shall be maintained for DiD (diversity and redundancy etc). There shall be a provision in existing or new nuclear installations the capability for independent, manual shutdown of the reactor in NPPs and RRs, and other potentially hazardous processes in other types of nuclear installations.*
8. *In addition to normal adjustments and operational checks, there shall be documented, periodic, simultaneous comparisons of corresponding performance factors of the conventional controls of the type specified in Provision No. 6 above with those of the corresponding digital controls, and deviations that exceed known and allowable/prescribed tolerances, shall be promptly investigated, and the cause(s) determined and corrected.*
9. *Any DI&C intended to be used in nuclear safety applications shall conform as a minimum to the highest level of applicable conformity assessment requirements for analog electrical and electronic instrumentation and electric and electro-mechanical controls as already in effect along with the additional NNR requirements.*

7 REGULATORY OVERSIGHT AND ENFORCEMENT

Oversight process is implemented on a case by case basis for each phase of the DI&C life cycle, including detailed technical requirements and acceptance criteria for oversight and verification (technical and quality assurance) of design, design verification, manufacture, testing (including qualification, dedication), installation, and pre-operational testing (including software unit testing/V&V)

Regulatory oversight shall be achieved in accordance with the provisions specified in PP-0012.

7.1 DI&C upgrade for existing nuclear installations

The main focus in this situation is integration of one or more DI&C systems into the existing I&C for the nuclear installations. This is expected to be done incrementally, involving first integration of the main DI&C platform and then commissioning various applications.

This may include adding sensors and control devices for the virtual plant to interface with the physical plant.

However this process is complicated by on-going operations and maintenance.

7.2 DI&C for new nuclear installations

For new nuclear installations, the design, manufacturing, testing in plant and commissioning of DI&C system and any analogue I&C shall be carried out more or less in parallel. This will lead to a much more controlled process requiring many field problems to be solved ahead of time, especially with the use of computer-aided design and manufacturing.

7.3 DI&C life cycle phases

The following are typical DI&C life cycle phases:

- Integrated System and Application Design
- Hardware Design
- Software Design
- Hardware Design Verification (qual-seismic and EQ)
- Software Design V&V
- Hardware Manufacturing
- Software Development
- Software V&V and Unit Testing
- Procurement (including COTS dedication as required)
- Factory Hardware and Software Acceptance Testing
- Hardware-Software Integration
- Site System/Application Acceptance Testing
- Hardware Installation
- Software Integration
- Pre-Operational Testing
- Operation
- Maintenance
- Modification

The following sections describe the regulatory oversight in the various phases of the DI&C life cycle to cover technical/safety and QA aspects (software QA and Configuration Management)

7.3.1 Prior to Hardware Design and Manufacturing and Software Design and Development

The NNR will assess the adequacy of the applicant's Quality and Safety Management system. This shall be supported by various processes for manufacturing as part of the applicant's compliance assurance processes. This will be tested against the requirements of RD-0034 before issuance of an authorisation to manufacture and NNR will verify compliance to these processes on a routine basis.

7.3.2 Procurement - Supplier Selection and Qualification, Product Acceptance

The NNR will assess, and observe where necessary, the implementation of the applicant's supplier qualification process. The NNR reserves the right to perform its own audits on suppliers if it deems it necessary. The following conditions will apply when the NNR observes audits by the applicant or its suppliers:

- The NNR is not a member of the audit team but an independent observer.
- The NNR can introduce questions for consideration during audits in advance of the audits to avoid an active role during the audit.
- The NNR will maintain independent audit records and an independent audit report.

7.3.3 Authorisation to Manufacture

Existing authorisation holders wishing to manufacture new or modified components important to nuclear safety have to comply with the relevant conditions in their respective nuclear authorisation relating to manufacturing and modification of the nuclear installation. These conditions should include the conditions, as referred to below or equivalent. The prerequisites and conditions defined in this section can be equally applied to existing holders of a NIL for the manufacturing of new or modified components important to nuclear safety and should be used as guidance where appropriate.

The NNR acknowledges that certain DI&C hardware and software may require long procurement and manufacturing times, so-called long-lead-time Items, and that the need may arise to start manufacturing/development prior to the assessment and acceptance of the safety case for construction by the NNR. As stated in PP-0012 for component manufacturing in general, any applicant wishing to start with manufacturing/development of nuclear safety DI&C prior to review and acceptance of the safety case must apply for an Authorisation to Manufacture and must make provisions in the schedule for regulatory oversight and assessment prior to the start of manufacturing and prior to installation of DI&C hardware and integration of software into the I&C systems. Note that the subsequent assessment of the safety assessment may conclude that the chosen code or standard, material and/or design specifications are inappropriate for whatever reason.

Commercial, “off-the-shelf” (COTS) DI&C hardware and software that is to be used in nuclear installation will already have been manufactured and/or developed beforehand; so an authorisation to manufacture is not applicable. However, even with the possible advantage of having operating experience with which, in part, to judge its reliability, COTS DI&C hardware and software, and the software tools used in application software development and testing, will not have been designed and manufactured/developed under the controls of a nuclear-grade QA program. Therefore, such DI&C must successfully undergo a process of commercial-grade dedication, as discussed above, with NNR oversight and approval of the process and results before the COTS DI&C hardware and/or software may be used in NI I&C applications important to safety.

7.4 Regulatory enforcement

7.4.1 Applicants for nuclear authorisations

Should the NNR identify noncompliance by applicants or their proposed facilities, or DI&C upgrade systems, with its regulations or guidance, inadequately justified deviation from international standards and practices, or other technical, quality or regulatory deficiencies, the NNR will suspend granting of the authorisation for new or upgrade DI&C and request further information and/or demonstration of correction of the deficiencies.

7.5 Nuclear authorisation holders

Normal enforcement policy and procedures as already established within the existing NNR regulatory framework will be implemented.

7.6 Vendors, Subcontractors

Compliance with the NNR requirements shall be ensured. In case of non-compliance, manufacturing shall be suspended and manufacturing process corrected before the manufacturing is resumed. The applicant has to inform the NNR of all non-compliances to requirements and agreed processes.

8 REFERENCES

Note that this position paper by its nature lists numerous external references that need not be repeated here. Thus these are the principal internal references.

[1] “Act No. 47 of 1999: National Nuclear Regulator Act, 1999”, published in Republic of South Africa Government Gazette, Vol. 414, No. 20760, 23. December 1999.

[2] Regulations in terms of Section 36, Read With Section 47, of The National Nuclear Regulator Act, 1999 (Act No. 47 Of 1999), on Safety Standards and Regulatory Practices (Published in Government Gazette 28755, April 2006)

[3] RD-0024: Requirements on Risk Assessment and Compliance with Principal Safety Criteria for Nuclear Installations.

[6] RD-0034: Quality and Safety Management Requirements for Nuclear Installations

[7] RD-0016: Requirements for licensing submissions involving computer software and evaluation models for safety calculations

[8] INSAG-12: Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev 1

[9] PP-0008, NNR Position Paper, “Design Authorisation Framework”

[10] PP-0012, NNR Position Paper, “Manufacturing of Components for Nuclear Installations”

9 APPENDIX A: REGULATORY EXPERIENCE RELATED TO DI&C

9.1 Finland (STUK)

Olkiliuto 3: Apparent AREVA misunderstanding of STUK position on use of computer-based systems has caused significant delays.

Olkiliuto 3 delays involving Instrumentation and Control.

The STUK regulatory review of the instrumentation and control design for Olkiliuto 3, an EPR design being constructed in Finland, has been one of the reasons for delay in construction. Although we understand that the reasons for the delays are the subject of a dispute between the utility (TVO) and the supplier, available literature, including annual public workshop presentations in Helsinki coordinated by STUK, indicates that the difficulties stem from two issues:

1. Lack of understanding of the STUK regulatory requirements by the Supplier-after issuance of the construction permit - the STUK regulatory process requires submission of construction plans and pre-inspection information prior to authorisation of construction. In his presentation on lessons learned, STUK Director General Mr Jukka Laaksonen notes that, “In Finland, the regulatory practice is different from what Areva had met elsewhere.”
2. Instrumentation and Controls Design not fully developed - In 2008; Laaksonen wrote a letter to Areva’s Lauvergeon, expressing concern with the lack of design detail available to STUK.

9.2 United States

The USNRC developed both an operating experience and a construction experience database. Screening and evaluating incident and problem reports form nuclear facilities around the world, important insights and lessons learned were and are still being learnt. One of the principle uses of the information is inspection planning in addition to inspection and other guidance development and generic communications. For this subject area, for example, one could find all the DI&C-related problems and even refine the search to identify the root cause(s) and proximate cause(s).

9.2.1 Oconee Proposal to the NRC

It required a lengthy review time and significant review resources. January 2011 issue of Nuclear Engineering describes lessons learned from NEI perspective

Digital Design at the Duke Oconee Station:

1. The original proposed design was not final and ready for regulatory review. Duke submitted an application to the NRC in 2006 later withdrawing it because the vendor design of the application-specific software and hardware elements was still in progress and the NRC wanted to review the final approved documents. Duke submitted a revision in January 2008.

2. Considerable information was needed by the NRC to complete the regulatory review. From its submission in January 2008 to NRC approval in January 2010, the review included 142 document submissions to the NRC, two rounds of requests for additional information, 16 supplements, and four NRC audits (of the Oconee site, Areva's Alpharetta, Georgia office and twice at its Erlangen, Germany test field).
3. NRC regulatory guidance was not final and had not been tested with previous reviews. Duke had to evaluate new guidance from NRC during its submittal efforts for Oconee to ensure that they were providing the type of information the NRC needed to perform a review.
4. Previous generic design reviews by the NRC could not be fully relied on. Because of the long lag between NRC's generic approval of the Teleperm design being proposed for Oconee, the information provided in the generic approval of the Teleperm XS platform had to be updated by Areva.
5. The proposed design did not conform to NRC's published guidance and did not provide sufficient information for the NRC to evaluate proposed alternatives to the guidance. For example, Areva proposed using a software simulation test tool to verify and validate (V&V) the RPS software by way of a series of built-in malfunctions. However, the NRC did not approve of the use of un-reviewed tools as a substitute for the validation testing.

9.2.2 New US Reactors

NRC has had some difficulty certifying proposed designs due to insufficient design detail. The NRC regulatory model has limitations.

Insufficient Level of Design Detail in New Reactor Computer Based Designs

New reactor designs submitted to the NRC for certification in accordance with NRC's regulation, 10 CFR Part 52, proposed DI&C designs that were not sufficiently developed for regulatory review. The NRC has had difficulty certifying (approving) the DI&C designs provided by the vendor because sufficient design detail could not be provided for the NRC staff to make an independent conclusion regarding the safety of the design. The NRC determined that "the I&C and control room design areas are characterised by a rapidly evolving technology and requiring completion of the design in these areas may result in the design becoming obsolete by the time a plant is constructed." Therefore, the NRC developed a phased review approach. This approach was based on the development of design acceptance criteria (DAC), which were proposed by the vendor in their application for a license and approved by the NRC. As the vendor and the licensee or applicant (nuclear authorisation holder or applicant) develop the design in accordance with each of the previously reviewed elements and acceptance criteria of the DAC, after issuance of the license, the NRC inspects the design for conformance to the acceptance criteria in the DAC. This process is now underway for the Vogtle plant in the US. The licensee cannot load fuel until all such inspections are demonstrated to be complete by the licensee and approved by the NRC.

9.2.3 Causes of Difficulties:

The NRC has attributed the difficulties in review and approval of new reactor DI&C designs to the following primary causes:

- Regulatory positions still under development at the time of review,
- Regulatory concerns with proposed design common cause failure prevention and mitigation
- Apparent lack of communication between the applicant and the regulator early in the regulatory process
- Regulatory uncertainty resulting from inexperience with computer based system regulatory reviews

9.2.4 Lessons Learned:

Fortunately, the difficulties experienced and the causes identified have resulted in some important lessons that can be used to improve the DI&C design review and approval process going forward. The principal lessons learned are:

- Publish regulatory position for comment as early as possible;
- Early and frequent interaction with applicants to develop sound understanding of regulatory expectations; and
- Consider developing defined regulatory review phases, especially for new reactors, so that licensing can proceed in a predictable way. Although Design Acceptance Criteria may not be ideal, waiting for the application final safety analysis report (FSAR) may not be ideal either.

10 APPENDIX B: OTHER INTERNATIONAL NUCLEAR SAFETY REGULATORY ORGANIZATION GUIDANCE

10.1 WENRA – Western European Nuclear Regulators Association

The WENRA publication with relevance to DI&C is “Safety of New NPP Designs,” Study by WENRA Reactor Harmonisation Working Group (RHWG), October 2012. Of particular concern with DI&C are failures of safety systems at NIs due to common-cause failure for other reasons than a postulated hazard, e.g., software problem, affecting similar equipment in the same safety system, or several safety systems. The report addresses safety at a high level, but it focuses on a key principle in preventing and dealing with/minimising the impact of common-cause failures, a significant concern with complex DI&C systems often driven by common software, and that is defence-in-depth (DiD). WENRA considers that independent SSCs for safety functions on different DiD levels shall possess both of the following characteristics:

- the ability to perform the required safety functions is unaffected by the operation or failure of other SSCs needed on other DiD levels;
- the ability to perform the required safety functions is unaffected by the occurrence of the effects resulting from the postulated initiating event, including internal and external hazards, for which they are required to function.

This can be achieved through redundancy, diversity; physical separation (structural or by distance); and functional isolation. For example, this principle requires that the reactor protection system (RPS) be adequately independent from other I&C systems and be functionally isolated from them. The RPS may have C&I functions on other DiD levels than postulated design-basis accidents or events (DBEs), e.g. the scram system may be actuated by the RPS for certain abnormal operational occurrences (AOOs). Diverse I&C means shall be designed for DBEs (what the report calls DiD level 3) in case the common-cause failure of the RPS has to be postulated. Limitation and control systems (other than the RPS) for the actuation of systems needed to handle AOOs (DiD level 2) may be combined with I&C for normal operation.

10.2 Finland (STUK)

STUK publishes their requirements in YVL Guides that hold the force of regulatory requirements. YVL Guide 5.5, “Instrumentation Systems and Components at Nuclear Facilities”, includes requirements for computer-based systems in Section 4.6, “Specific Requirements for Computer-based Systems and Equipment”. This guide, available on STUK’s website, addresses:

4.6.1 Qualification of the platform and the application

4.6.2 Software tools and design methods

4.6.3 Pre-existing software and equipment

4.6.4 Prevention and analysis of common cause failures

4.6.5 Testing of a computer-based system or equipment

4.6.6 Other requirements for a computer-based system or equipment

Section 4.6.4, regarding common-cause failures, appears to require an approach similar to that of the USNRC:

> "Software faults are typically caused by design errors. This means that the same failure mode may surface simultaneously in redundant parts of the system. The risk of a common-cause failure related to design errors shall be brought to a low enough level by using the diversity principle and other possible means to ensure a sufficiently high reliability of the system function. The measures taken to avoid a common cause failure shall be documented and justified and presented as part of the analyses required by Guide YVL 2.7."

10.3 United States (USNRC)

10.3.1 Regulations

Title 10, "Energy," of the Code of Federal Regulations (10 CFR), provides binding requirements on all persons and organisations who receive a license from NRC to use nuclear materials or operate nuclear facilities. The relevant chapters in these requirements are: Chapter 1, Nuclear Regulatory Commission, Parts 1 through 100, in particular, Part 21, "Reporting of Defects and Noncompliance," Part 50, "Domestic Licensing of Production and Utilisation Facilities," and Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." In particular, the applicable codes and standards among those referred to 10 CFR 50.55a(h), protection and safety systems, and 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants." The relevant requirements of DI&C-related NRC regulations and the associated guidance and acceptance criteria, are given in Chapter 7 of NUREG 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (the SRP), and are summarised below.

1 CFR 50.55a(a)(1), "Quality Standards"

2 CFR 50.55a(h), "Protection and Safety Systems," which requires compliance with IEEE Std. 603 1991 and the correction sheet dated January 30, 1995

3 CFR 50.34(f), "Additional [Three Mile Island] TMI Related Requirements," or equivalent TMI action requirements imposed by NRC generic letters (GLs):

(a) CFR 50.34(f)(2)(v), bypassed and inoperable status indication

(b) CFR 50.34(f)(2)(xi), direct indication of relief and safety valve position

(c) CFR 50.34(f)(2)(xii), auxiliary feed-water system automatic initiation and flow indication

(d) 10 CFR 50.34(f)(2)(xvii), accident monitoring instrumentation

(e) 10 CFR 50.34(f)(2)(xviii), instrumentation for detection of inadequate core cooling

(f) 10 CFR 50.34(f)(2)(xiv), containment isolation systems (CISs)

(g) 10 CFR 50.34(f)(2)(xix), instrument for monitoring plant conditions following core damage

(h) CFR 50.34(f)(2)(xx), power for pressuriser level indication and control for pressuriser relief and block valves.

4 CFR 50.62, “Requirements for reduction of risk from anticipated transients without scram [ATWS] events for light water cooled nuclear power plants”

5 CFR Part 50, “Domestic Licensing of Production and Utilisation Facilities,” Appendix A, “General Design Criteria for Nuclear Power Plants,”

(a) General Design Criterion (GDC) 1, “Quality Standards and Records”

(b) GDC 10, “Reactor Design”

(c) GDC 13, “Instrumentation and Control”

(d) GDC 19, “Control Room”

(e) GDC 20, “Protection Systems Functions”

(f) GDC 21, “Protection System Reliability and Testability”

(g) GDC 22, “Protective System Independence”

(h) GDC 23, “Protection System Failure Modes”

(i) GDC 24, “Separation of Protection and Control Systems”

(j) GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”

(k) GDC 29, “Protection Against Anticipated Operational Occurrences”

10.3.2 Regulatory Guidance

Guidance for NRC Staff Safety Assessment (Review and Evaluation) of Authorisation Holder Submissions

i. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants - LWR [light-water reactor] Edition,” (the “SRP”), Chapter 7, “Instrumentation and Control,” is the overall reference for staff safety assessments of DI&C applications.

ii. SRP Appendix 7-A includes the following Branch Technical Positions (BTP) that address digital system issues (listed in SRP Table 7-1, Section 5):

- BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”
- BTP 7-17, “Guidance on Self-Test and Surveillance Testing”
- BTP 7-18, “Guidance on Use of Programmable Logic Controllers”
- BTP 7-19, “Evaluation of Defense-in-Depth and Diversity (D3) of Digital I&C”
- BTP 7-21, “Guidance on Digital Computer Real-Time Performance”

SRP Section 7.0 and Appendix 7.0-A,“Review Process for Digital Instrumentation and Control Systems,” describe the overall review process for digital systems.

SRP Appendix 7.1-C provides guidance with respect to review according to Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991 (referenced in 10 CFR 50.55a(h)).

SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," provides guidance for evaluation of conformance to IEEE Std. 7-4.3.2 as endorsed by Revision 2 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," and BTP 7-14.

SRP Sections 7.2 through 7.9 focuses on systems that include references to digital system guidance in Section 7.1.

iii. USNRC Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)" and Interim Staff Guidance DI&C-ISG-06, "Information to be Submitted with Applications for NRC Approval of DI&C Systems for Use in Nuclear Safety-Related Applications in NRC Licensed Facilities," January 19, 2011

iv. Internal Procedures for the Review, Evaluation and Approval/Licensing Process – USNRC Office of Nuclear Reactor Regulation (NRR) Office Instruction LIC-101, "License Amendment Review Procedures," and LIC-500, "Processing Requests for Reviews of Topical Reports"

v. Regulatory and Industry Technical Guidance for DI&C Systems - USNRC Regulatory Guides (RGs) cited in BTP 7-14 and listed in SRP Table 7-1, Section 4, referenced NUREG publications, and the industry standards endorsed by those RGs (e.g., endorsed standards of the Institute of Electrical and Electronics Engineers (IEEE)), other referenced or endorsed industry publications (e.g., applicable publications of the Electric Power Research Institute (EPRI), IAEA Safety Fundamentals, Requirements, Guides and Practices, and applicable standards of the IEC as follow:

Interim Staff Guidance (ISG) Addressing Key DI&C Areas of Concern:

i. DI&C-ISG-01, "Interim Staff Guidance on Digital Instrumentation and Control Cyber Security, December 31, 2007

ii. DI&C-ISG-02, "Interim Staff Guidance on Diversity and Defense-in-Depth (D3)," Revision 2, June 5, 2009

iii. DI&C-ISG-03, "Interim Staff Guidance on Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments"

iv. DI&C-ISG-04, "Highly Integrated Control Rooms & Digital Communication Systems, Revision 1, March 2009, provides interim staff guidance for data communication independence.

v. DI&C-ISG-05, "Interim Staff Guidance on Highly Integrated Control Rooms - Human Factors Issues (HICR-HF), Revision 1, provides interim staff guidance on the process of crediting manual operator actions in a diversity and defence-in-depth analysis.

NRC Staff White Papers on DI&C to the Secretary (SECY) of the Commission

i. SECY-91-292 Digital Computer Systems for Advanced Light Water Reactors, Sept. 26, 1991

ii. SECY-93-087 Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, (Item II Q), April 2, 1993

iii. Staff Requirements Memorandum (SRM) to SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs,” (Item II Q, “Defense Against Common-Mode Failures in DI&C Systems,” and Item IIT Control Room Annunciator (Alarm) Reliability)

iv. SECY-01-0155 NRC Research Plan for Digital Instrumentation and Control

v. SECY-08-0033 Approaches for an Integrated Digital Instrumentation and Control and Human-Machine Interface Test Facility in the United States

vi. SECY-08-0033, Enclosure 1 Answers to Nine Questions from the Staff Requirements Memorandum for COMPBL-07-0001

vii. SECY-08-0033, Enclosure 2, “The Hub and Spoke Model”

viii. SRM-COMPBL-07-0001 Development of a U.S. Digital Instrumentation and Control and Human-Machine Interface Test Facility

Other DI&C-Pertinent Regulatory Guides

i. RG 1.97, Revision 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, June 2006

ii. RG 1.180, Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, October 2003

iii. RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, March 2007

DI&C-Specific NUREG Series Publications

i. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems", June 1993 - Discusses the role of software in conjunction with computer hardware in safety related systems at nuclear power plants. This document also discusses methods to ensure engineering reliability and safety in computer systems throughout the software life cycle.

ii. NUREG/CR-6263, "High-Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs", June 1995 - Examines technical basis for candidate guidelines that could be considered in reviewing and evaluating high-integrity computer software used in the safety systems of nuclear power plants. Addresses the following software development and assurance activities:

- requirements specification
- design; coding
- verification and validation (including static analysis and dynamic testing)

- safety analysis
- operation and maintenance
- configuration management
- quality assurance planning and management.

Each activity (framework element) was subdivided into technical areas (framework sub-elements). The report describes the development of approximately 200 candidate guidelines that span the entire range of software life-cycle activities; the assessment of the technical basis for those candidate guidelines; and the identification, categorisation and prioritisation of research needs for improving the technical basis. The report has two volumes: Volume 1, Executive Summary, includes an overview of the framework and of each framework element, the complete set of candidate guidelines, the results of the assessment of the technical basis for each candidate guideline, and a discussion of research needs that support the regulatory function; Volume 2 is the main report.

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

iv. NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," March 1996 - Proposes a process for acceptance of commercial off-the-shelf (COTS) software products for use in reactor systems important to safety. An initial set of four criteria establishes COTS software product identification and its safety category. Based on safety category, three sets of additional criteria, graded in rigor, are applied to approve (or disapprove) the product. These criteria fall roughly into three areas: product assurance, verification of safety function and safety impact, and examination of usage experience of the COTS product in circumstances similar to the proposed application. A report addressing the testing of existing software is included as an appendix. NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems

v. NUREG/CR-6680 Review Templates for Computer-Based Reactor Protection Systems

vi. NUREG/CR-6812 Emerging Technologies in Instrumentation & Controls

vii. NUREG/CR-6842 Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants

viii. NUREG/CR-6847 Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants (not publicly available)

ix. NUREG/CR-6848 Preliminary Validation of a Methodology for Assessing Software Quality

x. NUREG/CR-6888 Emerging Technologies in Instrumentation and Controls: An Update

xi. NUREG/CR-6895 Technical Review of On-Line Monitoring Techniques for Performance Assessment

xii. NUREG/CR-6901 Current State of Reliability Modelling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments

xiii. NUREG/CR-6942 Dynamic Reliability Modelling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments

xiv. NUREG/CR-6962 Traditional Probabilistic Risk Assessment Methods for Digital Systems

xv. NUREG/CR-6985 A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modelling of Digital Instrumentation and Control Systems

xvi. NUREG/CR-6997 Modelling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods

xvii. NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems

xviii. NUREG/GR-0019, "Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems"

xix. NUREG/GR-0020, "Embedded Digital System Reliability and Safety Analyses"

Generic Communications

i. Generic Letters - GL 95-02, "Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades in Determining the Acceptability of Performing Analog-to-Digital Replacements under 10 CFR 50.59"

Information Notices (INs)

i. IN 07-15, "Effects of Ethernet-Based, Non-Safety-Related Controls on the Safe and Continued Operation of Nuclear Power Stations"

ii. IN 07-08, "Potential Vulnerabilities of Time-Reliant, Computer-Based Systems Due to Change in Daylight Saving Time Dates"

iii. IN 03-14, "Potential Vulnerability of Plant Computer Network to Worm Infection"

iv. IN 96-62, "Potential Failure of the Instantaneous Trip Function of General Electric RMS-9 Programmers"

v. IN 96-56, "Problems Associated with Testing, Tuning, or Resetting of Digital Control Systems While at Power"

vi. IN 94-20, "Common-Cause Failures Due To Inadequate Design Control and Dedication "

vii. IN 94-04, "Digital Integrated Circuit Sockets with Intermittent Contact"

viii. IN 93-75, "Spurious Tripping of Low-Voltage Power Circuit Breakers with GE RMS-9 Digital Trip Units"

ix. IN 93-57, "Software Problems Involving Digital Control Console Systems at Non-Nuclear Reactors"

x. IN 93-49, "Improper Integration of Software into Operating Practices"

xi. Regulatory Issue Summaries (RISs) - RIS 2002-22, “Use of EPRI/NEI Joint Task Force Report, ‘Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI-01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule”

10.4 France (ASN)

The publically available information relevant to DI&C directly from the ASN website indicated only that the ASN belongs/subscribes to most of the same organisations and programs related to DI&C that the NNR does, including the IAEA and the MDEP, in which the ASN belongs to the DICWG. There was no public information on French DI&C-related regulations or the ASN’s DI&C-related regulatory experience. With a large number of NIs that within a few types are much standardised, the ASN utilises most of the widely recognised guidance cited in this position paper. It is a signatory to the major nuclear safety conventions, the IAEA and the OECD/NEA, and endorses the major DI&C-relevant industry standards, especially those of the IEC.

10.5 Japan

The regulatory body to ensure the safety of NIs in Japan is the Nuclear and Industrial Safety Agency (NISA), which has responsibilities for safety regulations pursuant to the Atomic Energy Basic Law and the Reactor Regulation Law. The high-level nuclear regulations of Japan are similar to those of most nations with NIs including those of South Africa. Note that license holders prepare and implement their nuclear QA programs according to JEAC 4111-2003, “Rules of Quality Assurance for Safety of Nuclear Power Plants” established by the JEAC based on ISO9001:2000. In addition the following individual guides with relevance to DI&C is used by the regulators for reviewing safety design of light-water nuclear power reactor facilities:

Guideline 8 - Design considerations against operator actions [presumably automatic blocks and interlocks]

Guideline 9 - Design considerations for reliability

Guideline 10 - Design considerations for testability

Guideline 14 - Reactivity control system

Guideline 15 - Independence and testability of reactor shutdown system

Guideline 16 - Reactor shutdown margin by control rods

Guideline 17 - Shutdown capability of reactor shutdown system

Guideline 18 - Reactor shutdown system capability at the accident

Guideline 34 - Redundancy of safety protection system

Guideline 35 - Independence of safety protection system

Guideline 36 - Function of safety protection system during transients

Guideline 37 - Function of safety protection system in case of the accident

Guideline 38 - Function of safety protection system in case of failure

Guideline 39 - Separation of safety protection system from instrumentation and control systems

Guideline 40 - Testability of safety protection system

Guideline 41 - Control room

Guideline 42 - Reactor shutdown function from outside of control room

Guideline 44 - On-site emergency station

Guideline 45 - Design considerations for communication equipment

Guideline 47 - Instrumentation and control system

10.6 United Kingdom

The Office for Nuclear Regulation (ONR) of the Health and Safety Executive (HSE) has the responsibility for regulating the safety of nuclear installations in Great Britain. The Safety Assessment Principles (SAPs) for Nuclear Facilities provide a framework to guide regulatory decision-making in the UK nuclear authorisation process. The SAPs are supported by Technical Assessment Guides (TAGs) which further aid the decision-making process. The following are the principal examples of over 100 UK documents available on the ONR website at www.hse.gov.uk that have relevance to the design and implementation of DI&C in NIs: While the ONR performs design safety assessments, the Nuclear Installation Inspectorate conducts direct regulatory oversight of the operating facilities.

TAG T/AST/059, Issue 1 – Human Machine Interface

ONR Nuclear Research Index, Section 1, Control and Instrumentation

Technical Measure Document – Control Systems

New Reactor Build – Generic Design Assessment, Step 2 Summary of Overseas Regulatory Assessments

Generic Design Assessment – New Civil Reactor Build, Step 3 C&I Assessment of the EDF and Areva UK EPR, Division 6 Assessment Report No. AR 09/038-P

TAG T/AST/046, Issue 2, “Computer-Based Safety Systems”

“Licensing of Safety Critical Software for Nuclear Reactors - Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations”

HSE Nuclear Directorate Technical Report, “New Reactor Build - Areva/EDF EPR Step 2 C&I Assessment”

Technical Area: Control and Instrumentation, Issue Number: 9.1, Issue: Computer based safety systems, Sub-Issue Number: 9.1.1 Sub-Issue: Reliability quantification of software based systems, by dynamic testing”

“The Use of Computers in Safety-Critical Applications - Final Report of the Study Group on the Safety of Operational Computer Systems”