



HITACHI

GE Hitachi Nuclear Energy

Mr. David L. Rahn, P.E.
Sr. Electrical Engineer
Office of Nuclear Material Safety
and Safeguards
Washington DC 20555-0001

Glen H Smith.
Principle Engineer
Global Laser Enrichment

P.O. Box 780 M/C H-82
Wilmington, NC 28402

T 910 675 5677
C 910 547 1047

Glenh.Smith@ge.com

Dear Dave,

Attached is a first cut of the proposal I suggested during our last TWG meeting. This document is not complete nor meant to be portrayed as a final product consider it as a "thought starter"

I am sure not everyone was totally clear on what I was suggesting so I would like this to serve as a discussion paper for our next meeting on September 3, 2008 or whenever you feel appropriate.

This document represents a concept that attempts put forth three major cases for discussion;

- A case for the allowance of Process control and safety logic running on a well designed, tested and maintained Digital Control System
- A case that IROFS applied to safety functions can be considered independent if the Digital Equipment and Control System is designed for reliability and the robustness of the design and management measures applied assure a high degree of Reliability
- A case for the choice of approved standards and references for the licensees to use which addresses the individual licensee's design uniqueness with respect to processes, operating principles and risk management practices.

Please feel free to contact with any feedback questions or concerns.

I look forward to the discussions with the whole team.

Best regards,

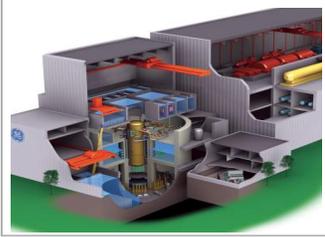
Glen H. Smith
Principle Engineer
Global Laser Enrichment
GE-Hitachi Nuclear Energy
Office: 910-675-5677
Mobile: 910-547-1047

*"We are what we repeatedly
do, Excellence then is not
an act but a habit"*

Enclosure

Aristotle

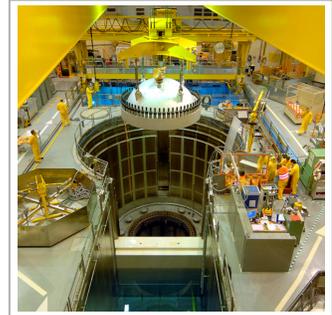
GE Hitachi Nuclear Energy



Author

Glen H Smith

Revision 0 08/22/2008
(Draft for Comments)



DIGITAL INSTRUMENTATION AND CONTROLS

Reference: DI&C-ISG-07

Task Working Group #7:
Fuel Cycle Facilities

ALTERNATIVE APPROACH FOR EVALUATING INDEPENDENCE OF DIGITAL CONTROLS

PREMISE

This Technical paper provides a concept for an alternate approach in identifying independence and Reliability criteria for implementing digital instrumentation and control (I&C) system designs in fuel cycle facilities.

This paper does not embrace any particular standard, rather allows for the use of a set of approved standards and references based on the needs of each Licensee.

The intention of this paper is to:

- Explain the Relationship of Reliability to Independence
- Offer a methodology for Qualitatively scoring a reliability factor
- Allow individual Fuel Cycle facilities to reference Standards / References applicable to their plant design in lieu of the NRC dictating a particular standard to follow verbatim.
- That depending on design and the reliability of the design, more than one control can exist within a common logic resolver and still be considered independent.
- And lastly, operational and safety logic can reside within a well designed single logic resolver while strategically implementing many of the current standards criteria, producing a Highly reliable and Robust system.

This approach also clarifies and provides acceptance criteria that the NRC staff would use to evaluate whether proposed digital I&C system designs used as an engineered control measures serving as Items Relied on for Safety (IROFS) is consistent with existing guidelines within NUREG 1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility." This approach is also consistent with current NRC policy on Integrated Safety Assessments submitted as part of the licensing process for fuel cycle facilities. 10CFR Part 70

The Double Contingency Principle within ANSI 8.1 States; "Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible".

Likewise the same rationale can be applied to IROFS failures within Digital Instrumentation and Controls when determining independence. In the case of Digital Control Systems an argument can be made and a definition has been applied that; *Independence is achieved if the failure of the first IROFS does not cause the Failure of the second and subsequent IROFS.*

A secondary and equally important factor to consider when evaluating Digital Controls is the reliability of the digital instrumentation and controls to be available on demand and when called upon.

Historically, management / assurance measures have been applied to ensure reliability. However, system design and implementation, in conjunction with management / assurance measures in adequately designed managed and maintained should be considered when evaluating the overall likelihood of meeting the performance requirements of 10CFR Part 70. Reliability strength or Robustness is highly dependent on all of these factors.

The **major premise** is that there is a definitive relationship between Independence and Reliability.

This paper will outline an approach then to determine the reliability Beta factor for Digital Instrumentation and Controls such as a Basic Process Control Systems, (BPCS).

The approach taken is based in part on *R.A Humphreys Methodology* and *Layers of Protection Analysis*, which take into account Defense in Depth measures.

BACKGROUND

DI&C-ISG-07 Problem Statement 3

Independence of Control Measures used as IROFS for Criticality Prevention

1. ISSUE

Guidance has been needed to define “independence” for control system IROFS and to identify an acceptable means of addressing independence for control system channels and functions used to meet the double contingency requirements of 10 CFR 70.64(a)(9) for criticality safety. Guidance is also needed to clarify the applicability and need for channel independence for digital Instrumentation and Controls performing non-criticality related safety actions.

2. PURPOSE

The purpose of this ISG is to clarify the NRC staff’s guidance with regard to the implementation of digital I&C equipment used as independent engineered control measures for meeting the double contingency requirement of 10 CFR 70.64(a)(9) to prevent the occurrence of a criticality event. In addition, this ISG will serve to provide a basis for evaluating the **reliability** of digital Instrumentation and Controls equipment performing both criticality and non-criticality safety functions at fuel cycle facilities.

OBSERVATIONS

Part 70 of 10 CFR, Subpart H contains three separate requirements to ensure nuclear criticality safety. One requirement, 10 CFR 70.64(a)(9), requires that the design of new facilities and processes provide for criticality control including adherence to the double contingency principle. A second requirement, 10 CFR 70.61(b), requires that high consequence events (which typically will include criticality accidents) be highly unlikely. A third requirement, 10 CFR 70.61(d), requires that nuclear criticality accidents be limited by assuring that under normal and abnormal conditions all nuclear processes are subcritical, including use of an approved margin of subcriticality, and also requires that the primary means of criticality protection be prevention.

The presence of two controls may not be necessary, or may not be sufficient, to meet the DCP. The DCP does not necessarily require two controls; it requires “at least two...changes in process conditions” be needed before criticality is possible. Meeting this may necessitate one, two, or more than two controls depending on the possible conditions that can lead to criticality. In general, there will be many pathways more than one pathway to criticality and, therefore, in some cases more than two controls required to meet the DCP for an entire process. This ISG was prepared to provide guidance to reviewers of license applications for facilities in which criticality prevention functions where the use of two or more independent engineered control measures, each making use of digital I&C equipment to accomplish the criticality prevention function to meet the double contingency principle are being proposed.

Operational events that occur regularly should not be credited as a contingency relied on to meet the DCP (although they may constitute part of a contingency if a combination of events may be considered unlikely). Therefore, the occurrence of any such event generally reveals a deficiency in the design that should result in corrective action. Determination that a contingency is unlikely should be based on objective attributes of the criticality controls, rather than on subjective judgment alone. Examples of such attributes are environmental factors that can degrade the **reliability** and availability of controls, margin, and redundancy and diversity of controls.

Concurrent does not mean that the two changes in process conditions must occur simultaneously, but that the effect of the first contingency persists until the second contingency occurs. Prompt detection and correction of abnormal conditions should thus be provided to restore double contingency protection. The time (duration) required for the detection and correction of failures should be significantly shorter than the anticipated time between failures in order for there to be significant risk reduction provided from failure detection.

Fail-Safe/Self-Announcing: This is the characteristic of an IROFS that determines the degree to which failure of an IROFS is detected and appropriately corrected. For the purpose of the ISA and ISA summary, an IROFS is only considered to fail when it fails to perform its intended safety function. Thus, a valve that is an IROFS is not considered to fail in the context of the accident sequence (i.e., contribute to the progression of an accident sequence) as long as it fails safe. If the valve is designed to fail closed (and closed is the safe configuration), credit may be taken for the fact that the valve is designed to fail closed. The likelihood thus is not the likelihood that the valve fails, but the likelihood that it fails in a way other than how it is designed to fail. An IROFS that is fail-safe may include within its boundary a system designed to put the process into a safe condition upon failure of a component. An IROFS whose failure is self-announcing is one in which failure is either self-revealing (e.g., by presence of solution on a floor where operators are continuously present) or which results in an alarm to alert operators. The main effect for the ISA Summary is to limit the duration of failure by ensuring that the upset condition is essentially

immediately corrected. Similarly, surveillance may be relied on to limit the duration of failure to a specified period.

Degree of Independence: To qualify as independent, the failure of one IROFS should neither cause the failure nor increase the likelihood of failure of another IROFS. No single credible if, however, the common-cause failure is sufficiently unlikely, it may be possible to treat IROFS as independent for purposes of the ISA and ISA Summary.

It is not always possible to provide absolute assurance that IROFS are perfectly independent. However, if the cumulative likelihood of all common-mode failures of a system of IROFS is significantly less than the independent failure should point in the ISG to where this performance is defined of the system of IROFS, then the IROFS may be treated for all practical purposes as independent. Quantitatively, this means the likelihood of the common-cause failure should be at least two orders of magnitude less than that of the independent failure of the system of IROFS. Qualitatively, this means the likelihood of the common-cause failure should be sufficiently low that it does not change the score for the system of IROFS.

It is the NRC staff position that if the combined sum of the likelihoods of all potential common-mode failures, which can occur for a system of IROFS, is significantly less than the independent failures which can occur for a system of control measures serving as IROFS, then the IROFS may be treated for all practical purposes as independent. It is also the NRC staff position that "significantly less" means that the likelihood of the cumulative effect of the common-cause failures should be at least two orders of magnitude ($1E-2$) less than the estimate for the independent failures within the system of IROFS. (That is, the common mode failure contribution to the total likelihood of failure is no more than an additional 1% (0.01) of the estimate of total likelihood of failure.)

INTRODUCTION

Accident Sequences and Consequences are identified for each Initiating Event. When analyzing accident sequences, the Hazard Analysis considers process deviations, human errors, internal facility events and credible external events. Also evaluated is the Independence and systems interaction where preventative actions and/or control measures are required to prevent and/or mitigate accident sequences.

A qualitative evaluation of the system reliability either as implemented or planned can be used to estimate the beta reliability factor. A successful solution of an equation does not make a decision when designing Digital Instrumentation and Control Systems. Therefore it is the intent of this paper to introduce a qualitative framework by applying a variety of defenses and design disciplines to minimize the occurrence of systematic failures by acknowledging the Reliability / Robustness of the system.

DISCUSSION

Assessing Reliability for Digital Instrumentation and Control Systems

Three factors for achieving reliability and safety integrity are:

- a. Complexity – In general, the fewer the component parts and the fewer types of materials and resources involved in them, the greater is the likelihood of a reliable item.
- b. Duplication / Replication – The use of additional, redundant parts whereby a single failure does not cause the overall system to fail is a frequent method of achieving reliability. It is probably the major design feature which determines the magnitude of reliability that can be obtained
- c. Excess strength or Margin – Deliberate designs to withstand stresses higher than are anticipated and / or conservatively operating with a large margin of safety will reduce failure rates

Achieving reliability, safety and maintainability results from activities in three main areas:

- a. *Design*
 - Reduction in Complexity
 - Duplications to provide fault tolerance
 - Derating of stress factors / Conservatively operating with a high margin of safety
 - Qualification testing and design reviews
 - Feedback of failure information – Validation
 - Configuration Management
- b. *Manufacture*
 - Control of Materials, methods, changes
 - Control of work methods and standards
 - Configuration Management
- c. *Operations*
 - Adequate Training
 - Configuration Management
 - Adequate operating and maintenance procedures

The single most important document for the use and implementation of Digital Instrumentation and Controls is the “Functional Specification” These reliability criteria as well as many others are typically discussed within the functional Specification.

See **Appendix B** for a Typical Digital Instrumentation and Controls Functional Specification outline

The proposal is to identify the applicable standards / references etc., within the body of the Functional Specification along with the acceptance criteria.

As an appendix to the Functional Specification a Qualitative Grading Checklist would be included for grading the Digital Instrumentation and Control System’s Reliability. (See **Appendix A**)

Example of Functional Specification**Controller Hardware Layout**

Rev A

Pg 14

All Input and Output channels shall be isolated from each other

Standard Reference: IEEE-XXXX

Acceptance Criteria: Optical isolation

a. Hardware Addressing

The Chassis Processor in each chassis contains a bank of switches for assigning the rack address. These addresses determine the rack numbers indicated in the I/O Configuration form. Rack numbers start at "00".

Node Processor card configuration and I/P address, subnet mask, node number, and other parameters are entered through the Device Configuration Editor.

b. Cabinet layout

Cabinets shall contain the appropriate number of I/O racks. The racks will be mounted in the front of the cabinet. The uppermost rack will be assigned the lowest address number. Where possible the first rack will contain the analog I/O cards. The discrete I/O should be segregated in separate racks.

c. Network Layout

The "A" I/O Communications port of the Node Processor card (J3) connects To an Ethernet switch, which then connects to the "A" I/O communications port (J1) on each Chassis Processor. The "B" I/O Communications port of the Node Processor card (J4) connects to a second Ethernet switch, which then connects to the "B" I/O communications port (J2) on each Chassis Processor. This allows the Node Processor to communicate through either the "A" or the "B" port. Note that both host Ethernet connections on the Node Processor (J1 and J2) are used in this configuration for redundant links to the host.

d. Rack Layout

The Node Processor is installed in Slot "V" and an 8600/01 Chassis Processor is installed in Slot "CC". I/O cards are installed in slots "0" through "15", which correspond to slots 00 through 15 in the I/O Configuration form.

e. I/O Card Layout

Empty I/O card slots are not allowed between I/O cards in SOE systems. Vacant card slots must contain an 8700 Interrupt Pass Through card, or must be located to the right of the occupied I/O card slots. Whenever possible, place analog and low-voltage digital I/O cards in the lowest numbered card slots; place high-voltage digital I/O cards to the right of the low-voltage I/O slots.

Standard Reference: IEEE-XXXX, ISA-XX

Acceptance Criteria: Signal and Voltage wiring Isolation

f. Wiring Topology

Analog termination modules (1 per card) will be mounted below the racks in the front of the cabinet. All field wiring (2/c#18 Shld.) shall terminate on 3-tier terminal blocks then to the termination module. AO wiring will be terminated directly to the termination module.

Example of Reliability Index

System Design Reliability Beta Factors

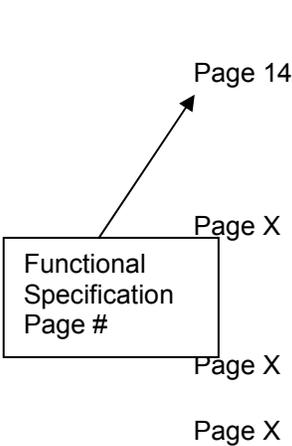
Compliant is the degree of compliance to a Licensee referenced Consensus standard

References

Attributes

Compliant

Beta



Hardware

- Isolated Channels
- Redundancy
- 1 IROFS per accident sequence per card
- 1 IROFS per accident sequence per file
- Robust Diagnostics and Monitoring
- Fail Safe – Fail Evident

	100%	75%	50%	25%	0%
	.166				
					0
	.166				
			.333		
	.166				
	.166				

The beta factor for each attribute of a given Functional Area (e.g. Hardware) is calculated simply by dividing the % compliance by the number of attributes.

A beta factor of 1 equates to complete compliance for each Functional Area

Total Beta 9.5

The Total Beta for Reliability is the sum of all Functional Area betas. (i.e. Hardware, Software, maintenance etc) See Appendix A

Acceptance Criteria is as follows:

- A total Beta of 8-10 represents a highly robust and reliable system.
- A total Beta of 5-7 represents a system requiring additional controls or systems.
- A total Beta of 1-4 represents an unacceptable system.

RATIONALE

Logical Conclusion:

While events may be calculated as “Mutually Exclusive”, in support of the Double Contingency Principle, in the world of physics and science there still remains a degree of interdependency no matter how casual.

Application Conclusion:

Independence of Digital Instrumentation and Controls should use the definition of the Double Contingency Principle with the addition of the acknowledgement of Reliability.

Controls may be regarded as Independent based on the Reliability of the Digital and Control system even if they reside in a single logic controller or redundant safety systems. The Digital Instrumentation and Controls must be dependable / reliable; it can be counted on to do what it was intended to do.

The ultimate failure of all is that the safety requirement specification is incorrect at the beginning of the design process.

The safety logic's primary purpose is to place the control system in the shutdown condition after a trip so that the system can be restarted in a controlled manner.

Licensees must consider all applicable approved standards when determining Digital Instrumentation and Control System design criteria for the purposes of meeting the regulatory requirements of 10CFR Part 70 and NURG-1520.

While standards and Industry references / guidelines provide methods and processes for calculating design dependent parameters, most do not explicitly advise on how to reach a decision for a given industry, commercial entity, or the individual designer.

Appendix A

System Design Reliability Beta Factors

<u>References</u>	<u>Attributes</u>	<u>Compliant</u>					<u>Beta</u>
		100%	75%	50%	25%	0%	
	Hardware						
	Isolated Channels						
	Redundancy						
	1 IROFS per accident sequence per card						
	1 IROFS per accident sequence per file						
	Robust Diagnostics and Monitoring						
	Fail Safe – Fail Evident						
	Software						
	Diversity in Programmers						
	Diversity in Operational vs. Safety Programs						
	Fail Safe – Fail Evident						
	Robust Diagnostics and Monitoring						
	Environment						
	Cabinetry sufficient for operating conditions						
	Access Controlled						
	Networking						
	Redundant						
	Proprietary Protocol						
	Secure						

References

Attributes

Compliant

Beta

Software Quality

- Third part Certification
- Interfacing with other systems
- Custom Scripting
- Simulation Testing
- 1/1 Verification

	100%	75%	50%	25%	0%

Maintenance

- Diverse System Wide maintenance
- Diverse Calibrations
- Predictive / Reliability Centered Maintenance

HU Training

- Operator Qualification
- Technician Certification

Configuration Control

- Development Documentation
- Robust Software Change Approval Testing and Acceptance
- Limited Access to Source-code

References

Attributes

Compliant

Beta

HU HMI

- Standardization
- Accessibility
- Degree of Complexity

	100%	75%	50%	25%	0%	

Testing / Surveillance

- Periodic Functional Testing
- Post Maintenance Testing
- 1/1 Verification

Total Beta

Appendix B***A Typical Table of Contents for Digital Instrumentation and Controls
Functional Specification*****1 Overview**

- 1.1 Purpose of this document
- 1.2 Scope of this document
- 1.3 Document Overview
- 1.4 Identification
- 1.5 Relationship to Other Plans
- 1.6 Related Documents
- 1.7 Key Stakeholders
- 1.8 Points of Contact
- 1.9 Traceability

2 Current System

- 2.1 Background
- 2.2 Application Overview
- 2.3 System Objectives
- 2.4 Current Methods and Procedures
 - 2.4.1 Equipment
 - 2.4.2 Input and Output
 - 2.4.3 Provisions
 - 2.4.4 Deficiencies
- 2.5 Business Context
- 2.6 Organization Profile
- 2.7 Business Functions
- 2.8 Component Description

3 Requirements Specifications

- 3.1 Introduction
 - 3.1.1 Goals
 - 3.1.2 System Users
 - 3.1.3 Assumptions
- 3.2 System Description
 - 3.2.1 System Overview and Environment
 - 3.2.2 Functional Structure and Inter-relationships
- 3.3 Functional Requirements
- 3.4 User Roles
- 3.5 System Operational Requirements
- 3.6 Input and Output Requirements
- 3.7 Performance Requirements
- 3.8 Communication Requirements
- 3.9 Communications Requirements
 - 3.9.1 Communications Overview
 - 3.9.2 Communications Hardware
 - 3.9.3 Communications Software
- 3.10 Security Requirements
- 3.11 Hardware Requirements
 - 3.11.1 Hardware Functionality

- 3.11.2 Hardware Characteristics
- 3.12 Software Requirements
 - 3.12.1 Software Functionality
 - 3.12.2 Software Characteristics
- 3.13 Usability Requirements
- 3.14 Data Requirements
 - 3.14.1 Data Structures and Relationships
 - 3.14.2 Data Framework and Relationships
 - 3.14.3 Data Inputs
 - 3.14.4 Data Outputs
 - 3.14.5 Interfunctional Data Definitions
 - 3.14.6 Component Cross Reference
- 3.15 Functional Component Specifications

4 Proposed Methods and Procedures

- 4.1 Improvements
 - 4.1.1 Functional Improvements
 - 4.1.2 Improvements to Existing Capabilities
 - 4.1.3 Timeliness
- 4.2 Impacts
 - 4.2.1 User Organizational Impacts
 - 4.2.2 User Operational Impacts
 - 4.2.3 User Developmental Impacts
- 4.3 Product Functions
- 4.4 Similar System Information
- 4.5 User Characteristics
- 4.6 User Problem Statement
- 4.7 User Objectives

5 Design Constraints

- 5.1 Software Design Constraints
 - 5.1.1 Software Interfaces
 - 5.1.2 Software Packages
 - 5.1.3 Database
 - 5.1.4 Operating System
 - 5.1.5 Tolerance, Margins and Contingency
- 5.2 Hardware Design Constraints
 - 5.2.1 Hardware Requirements and Environment
 - 5.2.2 Hardware Standards
 - 5.2.3 Hardware Interfaces
 - 5.2.4 Capacity
- 5.3 User Interface Constraints
 - 5.3.1 User Characteristics
 - 5.3.2 Environment/Operational Constraints

6 Detailed Characteristics

- 6.1 System Description
- 6.2 System Functions
- 6.3 Flexibility
- 6.4 Performance Requirements
 - 6.4.1 Accuracy
 - 6.4.2 Timing

- 6.4.3 Capacity Limits
- 6.5 Functional Area System Functions
- 6.6 Input and Output
- 6.7 Failure Contingencies

7 Functional Requirement [x]

8 Resources

- 8.1 Personnel Requirements

9 Appendixes

- 9.1 Support Material
- 9.2 Glossary of Terms
- 9.3 Acronyms and Abbreviations

Index of Tables

- Table 1 — Functional Requirements Matrix
- Table 2 — User Roles
- Table 3 — Resources
- Table 4 — Glossary of Terms
- Table 5 — Acronyms and Abbreviations