NRC FORM 390
(12-2003)
NRCMD 3.9

U.S. NUCLEAR REGULATORY COMMISSION

RELEASE TO PUBLISH UNCLASSIFIED NRC STAFF SPEECHES, PAPERS, AND JOURNAL ARTICLES

(Please type or print)

1. TITLE *(State in full as it appears on the speech, paper, or journal article)*
Discerning the Need for Fault Detection and Self Diagnostics

ADAMS Accession No.
(Use Template OCIO 039)

2. AUTHOR(s)
Royce D. Beacom

3. NAME OF CONFERENCE, LOCATION, AND DATE(s)
**Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies.
Knoxville, TN; April 5-9, 2009**

4. NAME OF PUBLICATION
Proceedings of the Sixth American Nuclear Society International Topical Meeting on NPIC and HMIT

5. NAME AND ADDRESS OF THE PUBLISHER
**American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60526**

TELEPHONE NUMBER OF THE PUBLISHER
800-323-3044

YES	NO	6. PAGE CHARGES
	√	If yes, attach a completed and signed NRC Form 30, " Request for Administrative Services." The NRC Form 30 must be transmitted for funding and an obligating document issued by ADM before the paper is sent for publication. ***If an NRC Form 30 is not submitted, NRC may refuse to pay the page charges, and the author will become personally responsible.***

YES	NO	7. CERTIFICATION *(ANSWER ALL QUESTIONS)*		
√		A. TECHNICAL AND POLICY REVIEWS -	Speeches, papers, and journal articles require management and policy reviews of technical and policy issues per NRC MD 3.9, Part 1(A)(2). Please check the "YES" box to certify that the speech, paper, or journal article complies with this statement.	
	√	B. COPYRIGHTED MATERIAL -	Does this speech, paper, or journal article contain copyrighted material? If yes, attach a letter of release from the source that holds the copyright.	
	√	C. PATENT CLEARANCE -	Does this speech, paper, or journal article require patent clearance? If yes, the NRC Patent Counsel must signify clearance by signing below.	
		NRC PATENT COUNSEL *(Type or Print Name)*	SIGNATURE	DATE
√		D. REFERENCE AVAILABILITY -	Is all material referenced in this speech, paper, or journal article available to the public either through a public library, the Government Printing Office, the National Technical Information Service, or the NRC Public Document Room? If no, list below the specific availability of each referenced document.	
		SPECIFIC AVAILABILITY		
	√	E. METRIC UNIT CONVERSION -	Does this speech, paper, or journal article contain measurement and weight values? If yes, all must be converted to the International System of Units, followed by the English units in brackets, pursuant to the NRC Policy Statement implementing the Omnibus Trade and Competitiveness Act of 1988, Executive Order 12770, July 25, 1991.	

8. RESPONSIBLE STAFF MEMBER

NAME *(Type or print name)*		OFFICE/DIVISION	MAIL STOP
Royce D. Beacom		**NRO/ DE**	**T10E06**
SIGNATURE Royce D. Beacom	DATE	TELEPHONE NUMBER **301-415-2781**	E-MAIL I.D. **royce.beacom**

9. AUTHORIZATION ***(Cannot be the same person listed in block 8.)***

NRC OFFICIAL AUTHORIZING RELEASE *(Type or print name)*
Terry W. Jackson

SIGNATURE Terry W Jackson

DATE 2/17/09

Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies
NPIC&HMIT 2009, Knoxville, Tennessee, April 5-9, 2009, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2009)

DISCERNING THE NEED FOR FAULT DETECTION AND SELF DIAGNOSTICS

Royce D. Beacom
U.S. Nuclear Regulatory Commission
11555 Rockville Pike, MS: T10E06
Rockville, MD 20852
Royce.Beacom@nrc.gov

ABSTRACT

Computer systems could potentially experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system during normal operation. These can be latent defects which are created by a manufacturing error or even "designed" in errors, manifesting themselves in hardware or software and not discovered until the most inopportune time. In the case of a computer system functioning as a safety system in a nuclear power plant, this can potentially affect the capability of the system to perform its safety function. Self-diagnostics are one means that can be used to assist in detecting these failures. The reliability requirements of the safety system should dictate and establish the need for self-diagnostics. Self diagnostics should not be used for systems in which failures can be detected by alternate means in a timely manner. For several generations of computer systems, self diagnostics have been considered a potential source for latent defects. Due to their added complexity and sheer size of coding added to the application, they could potentially add different types of latent errors, this same categorization of errors which they were created to detect. If self-diagnostics are incorporated into the system requirements, these functions should be subject to the same V&V processes as the safety system functions. But that is no guarantee of an error free operating system. What has been done and what the needs for fault detection and self-diagnostics are addressed in this paper.

Key Words: self diagnostics, fault detection, self testing

1 INTRODUCTION

Computer technology has now achieved a requisite level of maturity which has demonstrated successful applications to the nuclear industry. In addition, there is tremendous operating experience leverage, as well as research and development, applied to digital computers by the defense, aerospace, and communications industries which can be adapted to the nuclear power sector. However, all features and aspects of the technology must be proven safe, from outside and within the nuclear industry before complete implementation and use. One unique feature of this technology is the evolutionary deployment of fault detection and self diagnostics. The focus of this paper is on the intrinsic fault detection and self diagnostics of the main signal processing portion of the safety I&C system. Computer self testing is most effective at detecting random hardware failures. Typical self-tests include monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity. These self testing attributes are

implemented by specific built in software and hardware of the signal processing electronics in the safety portion of the I&C systems[1].

These embedded self tests of the system electronics use the same software and run on the same processors as that which is used to perform the critical safety functions. The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system. The design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. Also, like all safety system software, fault detection and diagnostic software cannot typically be proven to be error-free although use of high quality software and hardware reduce failure probability [2]. The positive aspects of self-test features should not be compromised by the additional complexity that may be added to the safety system by the self-test features. The improved ability to detect failures provided by the self-test features should outweigh the increased probability of failures associated with the self-test feature. For obvious reasons then it is desirable to keep these features as simple as possible in implementation. An attempt to detect every possible fault would increase total system complexity and increase response time of the overall system. Thus, the embedded diagnostics have been designed to detect the more probable faults quickly.

As the technology advances stake holders of the industry are proposing self tests in place of surveillance tests. The characteristics of digital systems should be carefully considered in the review of technical specification surveillance features and particularly which ones can be substituted by computer self testing. Architectural differences between digital and analog systems warrant careful consideration during the review of surveillance test provisions. Furthermore, the concepts used to determine test intervals for hardware-based systems do not apply directly to the software used in digital computer-based I&C systems. Therefore, previous reliability analysis used to establish test intervals will now have to address the effects of software usage.

An additional goal of fault detection and diagnostics technology development is to aid control information and knowledge processing and to offer fault-tolerant instrumentation and control systems so that transient initiations and challenges to the plant systems can be safely dealt with and reduced. A goal of control and diagnostics technology development is to aid control information and knowledge processing and to offer fault – tolerant control instrumentation systems so that the transient initiations and challenges to the p l a n t systems can be reduced. This would help limit unanticipated and heavy burdens on the operating staff to simultaneously diagnose malfunctions and initiate proper corrective actions. The human cognitive process of Control & Diagnostics in nuclear power plants is explained by the Rasmussen's information model of control process [1]. The control process of a human operator is generally categorized into three stages:

1. Skill-based automatic response
2. Rule-based guided responses
3. Knowledge-based problem solving

---

[1] This paper defines self tests as a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics [5].

In most transients or events, well trained operators can quickly detect the abnormal situations and execute control functions to shut down or recover the plant through automatic responses. However, in some low-probability complex events which fall outside the scope of routine operator skill-based training and rule-based operating procedures, the operators need to use knowledge-based problem solving techniques to evaluate and predict the next possible plant states, to define tasks for control, and to recover the plant to a safe state. The TMI-2 accident demonstrated the unfortunate situation that complex and multiple events which went beyond the skill-based and rule-based controls was degenerated into a severe accident when the operating crew were inadequately informed to recognize and control the accident correctly.

However, the concern for distracting operators from their important duties and support systems with specific features and requiring specialized training is a world wide industry concern. It was reported [7] that the Electricité de France (EDF) at one point had initiated a moratorium on the installation of new plant operational support systems in their control rooms. The explanation for such drastic action was that the proliferation of such systems was introducing undue complexity in the instrumentation and control systems of the plants and that the operations of such systems were diverting the operators from their other important duties. The challenge is to develop simpler, less intrusive and more useful and integrated operational support systems for the plant operators. The industry simply does not want multiple, independent plant operational support systems, each with its own unique features and each requiring dedicated training to operate. Equally important is for the plant operational support system developers to secure the "buy-in" and support of the plant operators of the systems that are installed, or they will not be used.

1.1 Evolution of fault detection and self diagnostics into current Nuclear Power Plant Safety Systems

Diagnostics and detection of faults have been incorporated into the main processing section of digital I&C systems almost since the inception of digital systems in the nuclear industry. In the mid to late 1980's, as a result of the post Three Mile Island upgrades and requirements, a plethora of standalone digital processing safety systems appeared in several monitoring applications of the U.S. operating nuclear plants, many with these features. The fault detection and diagnostics grew into large scale architectures involved in system wide and even whole plant I&C in Europe and VVER modernizations. This influx of digital systems on the safety system side was just behind the non safety digital systems replacing the existing analog counterparts for obsolescence concerns, reliability and other enhanced features. Many of the basic fault detection and self diagnostic features of these systems are the same as those being proposed for the new generation of reactors and their digital I&C safety systems. A library of diagnostic algorithms for use in real-time microprocessor-based systems was developed by many manufacturers. The major design goals were to detect the most common failures as quickly as possible and to detect a majority of the less common failures in a timely manner. Many software algorithms were intended to be used with Intel Corporation's 8086 family of microprocessors. This included the 8086, 8088, 80186, 80188, and 80286 (in real mode only) [3]. The following are types of devices in the system which is checked by associated diagnostic algorithms.

- Read-only memory
- Read/write memory
- Access to read/write memory
- Main and Numeric Processors
- Deadman timers

These are the types of diagnostic messages which are presented to the operator in existing plants:

- PROM Checksum Error
- RAM Write Error
- NVMEMORY Checksum Error
- TIMED OUT or Deadman timer Error

None of these message types necessarily indicate a fatal system error but they do require the operator or I&C staff to review the message and take actions appropriately. In addition to the messages in current operating plants, these digital systems are able to provide status of calculated and real time sensor inputs, status of auto-calibrations being done, use of manually entered values and assignment of generalized quality codes to input values such as good, suspect, poor or bad. This information is usually presented to the operator on a limited text basis, usually accessed on a separate diagnostic page, and requires some form of knowledge based problem solving due to their digital form (examples; single characters, quality codes, bit codes or binary coded decimal representations). This nature of specialized, independent, decoding activity invited, or necessitated in many cases, the additional step by the operator to request assistance from I&C or system personnel who were better versed and trained on this system and, particularly, in this technology.

These safety related digital systems, incorporating error detection and diagnostics, are approaching 20 years of U.S. nuclear plant operation. The original intent of the error detection and methods, and the accumulated operational data base, has not manifested itself in credit being taken for existing manual surveillance testing or, on the negative side, added to system failures as a result of further complexities in the software logic or data structures. In other words, a basis has not been presented that would augment the inclusion or removal of fault and diagnostic features based on actual historical operating numeric data. However, as is explained below, there are superior baseline issues that should have a greater determinate on the existence or tempered use of fault detection and diagnostics

1.2 Inclusion of fault detection and self diagnostics in the Next Generation of Reactors

The I&C system capabilities of the new reactors, currently in various design certification

stages, go beyond what is currently configured in existing operating plants. As what may be easily interpolated with the inclusion of new hardware and software technology, the proliferation of error detection and diagnostics has been taken to a higher level. The actual individual diagnostics features in the new generation of reactor designs are very similar to those described above for the current operating fleet. These individual tests have been incorporated into nearly every input or output module and communication channels. Also, the consistent capability in the new reactor diagnostic systems is to detect the location of a given fault or problem down to the modular level and present this to the operator as some sort of an alarm with the system continuing in its current operating mode. A progressive feature of these digital systems is the capability to not only detect an anomaly but to also determine if it is a fault tolerant or fatal flaw, alarm the operator in a more understandable and efficient manner than current operating methods and take itself, by the division or system, out of service. Also, if a system is configured with a subsystem or redundant controller, the failed controller will transition control over to the other controller or redundant portion of the system. This type of progression of the technology will lessen the burden on the operator to problem solve and All of this would be based on the predetermined severity or how the detected fault can be tolerated. Understandably, the progression of these features has led to the desire to credit these surveillances, normally done by the operators, partially or in total. Though for most new reactor designs, the features are only in the planning and implementation stages of the life cycle process. Little has been disclosed and therefore substantiated in how these new features will address regulatory guidance, standards and guidelines used by the NRC staff.

1.3 Regulatory Requirements, Guidance, Standards and guidelines

1.3.1 NRC Regulatory Requirements

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 5.7, requires, in part, that capability for testing and calibration of safety system equipment be provided while retaining the capability of the safety systems to accomplish their safety functions. Clause 5.1, requires that the safety system be able to perform its safety function required for a design basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

10 CFR Part 50 Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.

GDC 22, "Protection System Independence," requires in part that the protection system be designed to assure that the effects of natural phenomena and of normal operating, maintenance and testing do not result in loss of protection function.

10 CFR Part 50 Appendix B, Criterion XII, "Control of Measuring and Test Equipment," requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

1.3.2 NRC Regulatory Guidance

Regulatory Guide 1,152, "Criteria for use of Computers in Safety Systems of Nuclear Power Plants." In this Regulatory Guide the NRC has unconditionally endorsed the IEEE standard 7-4.3.2 with regards to fault detection and self-diagnostics, described in Section 1.3.3 below.

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method of complying with the requirements of IEEE Std. 279-1971 with regard to indicating the inoperable status of a portion of the protection system, systems actuated or controlled by the safety system, or auxiliary supporting features and other auxiliary features. IEEE Std 603-1991, Clause 5.8.3, gives the equivalent requirements for safety systems.

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," states that the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable, failures. Consequently, self-testing and diagnostics are important elements in the design's ability to meet the single-failure criterion.

Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," states that the criteria of IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," are considered acceptable methods for the periodic testing of protection systems (subject to the specific exceptions discussed in Regulatory Guide 1.118). IEEE Std. 338-1987 provides design and operational criteria for the performance of periodic and automatic testing; its criteria are supplementary to IEEE Std. 603-1991.

Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," systems. The Regulatory Guide and endorsed standard provide guidance applicable to the development of self test and diagnostic software and to making safety functions independent from these functions.

1.3.3 Industry Standards

Industry guidance by the IEEE [4], summarized as follows, on the subject of computer system partial failures, which may not be immediately detectable:

1. Self-diagnostics are one means to assist in failure detection
2. Reliability requirements shall be used to establish the need for self-diagnostics
3. Self-diagnostics are not required if there are alternate means of detection
4. Self-diagnostics shall not affect the safety function performance
5. Infrequent communication link failures that do not result in a system failure or lack of system functionality do not require reporting.

1.3.4 NRC Standard Review Plans

The staff standard review plan guidance on fault detection and diagnostics, primarily found in [4], is summarized as follows:

1. The safety system (including self-test) is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation.
2. The positive aspects of self-test features are not compromised by the additional complexity that may be added to the safety system by the self-test features.
3. Hardware and software design support the required periodic testing.
4. Failure modes assumed to be detectable by the single-failure analysis are in fact detectable. Failures may be detectable by observing operational characteristics as well as other methods.

2 CONCLUSIONS

2.1 Conclusions within the Regulations, Requirements & Guidance

The concerns of the NRC staff for diagnostics unnecessarily adding complexity to the safety software, which may impact the safety system functional performance, is prominent and materialized by the NRC referenced regulations, guidance and review plans

2.2 Limits of the Fault Detection and Diagnostic Technology

Since the embedded self-diagnostics run while the system is performing the critical safety functions, it is desirable to keep them as simple as possible. As recognized by the industry, that for at least current technology used, an attempt to detect every possible fault, or indiscriminate and excessive use of embedded diagnostics, would increase total system complexity and response time. Consequently, the overall performance of the safety system could be affected or even diminished. Thus, the current day embedded diagnostics, used in operating plants, have been designed to detect the more probable faults quickly [3].

2.3 When Self-Diagnostics should be used

Self-diagnostics are one means that can be used to assist in detecting partial failures that degrade the capabilities of the digital I&C safety system. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely matter. In fact, the reliability requirements of the safety system shall be used to establish the need for self-diagnostics [4]. There should be a method of verifying self-test functions during functional tests. Also, the design should have either the automatic or manual capability to take compensatory action on detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other.

2.4 Future of Fault Detection and Self-Diagnostics

Assimilation of fault detection and self diagnostics of the electronics platforms is being done for the next generation of reactors in the planning and implementation cycles. When diagnostics should be used is clearly documented. The reliability analysis, and potential use of other means are available for failure detection, has not been comprehensively presented. Whereas, the effects associated with complexities generated with additional self testing, at least within constraints of the current technology, has been well defined by the nuclear industry. In fact, there is credence for the addition of self testing once the initial systems are operating and actual reliability data can be used to determine the need for this aspect and the extent of implementation. That approach is from the elimination of errors in software is a realistic and necessary goal in safety systems, but not in an entire intelligent control hierarchy in its first use.

Compartmentalization, involving discrete knowledge interfaces for communication between modules, offers the possibility of building reliable systems in which the software qualification can proceed incrementally, in which errors in individual modules do not challenge the system as a whole, and in which the task of verification and validation will scale linearly with the growth of the system [6].

3 REFERENCES

1. B. K.-H Sun, "Control and Diagnostics for Nuclear Power Plant Performance and Safety Enhancement," *IEEE Fourth Conference on Human Factors and Power Plants*, Monterey, CA, USA, 06/05/1988 – 06/09/1988, pp.13-21 (1988).

2. Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" of *NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington DC (March 2007)

3. M.D. Bowers, J.P. Arnold, A.W. Crew, R.J. Gibson, W.D. Ghrist, "Diagnostic Software and Hardware for Critical Real-Time Systems," *IEEE Transactions on Nuclear Science,* Orlando, FL, 11/09/1988 – 11/11/1988, Vol. 36, pp. 1291 – 1298 (1989).

4. IEEE Standard 7-4.3.2 - 2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," (December 2003).

5. Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions," of *NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington DC (March 2007).

6. J.G. Williams, W.C. Jouse, "Intelligent Software Control for Nuclear Power Plants," *IEEE Nuclear Science Symposium and Medical Imaging Conference*, Orlando, FL, 10/25/1992 – 10/31/1992, Vol.2, pp. 733 – 735 (1992).

7. D. Raun, W. Hines, I. Pazsit, "Intelligence in Nuclear Applications: Lessons Learned and Recent Developments, " *Progress in Nuclear Energy,* 46:3-4(2005), pp. 165-387,