UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, D.C. 20555

July 8, 1993

NRC INFORMATION NOTICE 93-49: IMPROPER INTEGRATION OF SOFTWARE INTO OPERATING PRACTICES

Addressees

All holders of operating licenses or construction permits for nuclear power reactors.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to alert addressees to recent events involving improper integration of software-based digital systems into operating practices. It is expected that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response is required.

Description of Circumstances

AMSAC Time Delay Error

On December 31, 1992, the New York Power Authority (the licensee for Indian Point, Unit 3) performed a routine semiannual logic test for the anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC). The AMSAC system failed the test when a required 40-second time delay was not observed. The absence of the time delay would have prevented the automatic initiation of the motor-driven auxiliary feedwater pumps in response to an AMSAC initiation signal under certain conditions.

After initial review, the licensee concluded that the deficiency had existed since July 8, 1992, when a Foxboro (vendor) field technician reinstalled the hard drive and manipulated software in the AMSAC logic. When the hard drive was reinstalled, the vendor technician loaded AMSAC software from an uncontrolled version of the software in his possession. The controlled, plant-specific version of the software had not been retained by the licensee nor had the licensee made arrangements for the vendor to maintain configuration management. The vendor technician attempted to modify the uncontrolled version of the software to customize it for plant-specific use. Use of the improper version of the software caused the system to reboot incorrectly. The system failed the surveillance test, and the vendor technician modified the software to allow proper system reboot. During this

software manipulation, the 40-second time delay was incorrectly implemented in the software logic. This activity was not documented, and after the changes were made, the AMSAC system was not adequately retested. Because the actual system logic was not retested, the vendor technician and the licensee were unaware of the fact that the location of the 40-second time delay of the AMSAC signal had been mistakenly altered during the software manipulations, rendering the AMSAC inoperable under certain conditions.

Annunciator Driver Failure

On December 13, 1992, with the Salem Nuclear Generating Station, Unit 2, at 100-percent power, the overhead annunciator (OHA) system in the control room was inadvertently placed in a configuration in which it did not update the OHAs to indicate true alarm status. The inoperable status of the OHAs went unrecognized by the operators for 90 minutes until an alarm typewriter printed a change in alarm status while the corresponding OHA failed to respond. The OHAs remained inoperable until the OHA sequence event recorder computer was rebooted.

The OHA system is a real-time, multi-tasking, distributed processing computer system with 35 microprocessors and the associated software. The OHA system design permitted an operator to place the sequence event recorder in the data transfer mode versus the operating mode and enter the password-protected software without warning to the operator, which allowed unauthorized system manipulation. The event occurred because the operator at a remote configuration workstation failed to follow procedure while attempting to obtain system status data by having the "black box" switch placed in the incorrect position. The incorrect position routed commands entered on the remote configuration workstation to a high priority link on the sequence event recorder. The operator miskeyed the command characters, but the miskeyed command characters happened to be valid commands on the high priority data link which required additional data input. The sequence event recorder processed the command and suspended communications to other data links (including the OHAs), while it waited for additional data input over the high priority link, until the condition was recognized after 90 minutes and the system was rebooted.

Diverse Scram System Failure

On March 13, 1993, at the Maine Yankee Nuclear Power Plant, flashing trouble indications appeared on the intelligent non-nuclear safety digital automation control system (INNSDACS). An instrumentation and controls (I&C) technician attempted to clear the alarms by rebooting the control processor. On March 14, the plant engineer determined that the diverse scram system had been inoperable since the reboot. The diverse scram system was restored by March 16. The I&C technician did not have sufficient training on INNSDACS to respond to system malfunctions without rendering the diverse scram system inoperable. Licensee implementation of the diverse scram system did not ensure comprehensive training and administrative controls for maintenance activities.

Inoperable Torus Temperature Monitoring System

On November 14, 1991, at the James A. FitzPatrick Nuclear Power Plant, the licensee found that 3 of 12 circuit cards in the torus temperature monitoring system "A" train had defective solder joints. The torus temperature monitoring system consists of 15 resistance temperature detectors (RTDs) positioned at various locations throughout the torus that feed two redundant instrumentation channels and provide a bulk temperature output via an averaging circuit. The defective cards in the "A" channel were replaced, and the channel was declared operable. Checkout testing of the system on November 15, 1991, showed that the programming of a module in the "A" channel was loaded with an incorrect software algorithm. The algorithm is designed to discard RTD input signals that deviate more than 100 percent from the average signal. The as-found setting for the module (which controls four of the RTDs) would have discarded any RTD readings deviating more than 10 percent from the average. This could have affected bulk temperature readings in a nonconservative direction in the event of localized torus heating. The correct software was immediately loaded into the module.

Discussion

The events described above are examples of how inadequate integration of software-based digital systems into operating practices and how inadequate knowledge of the intricacies of software-based digital systems on the part of technicians and operators caused systems to become inoperable. The above events indicate the susceptibility of software-based digital systems to failure modes different from those of analog or hardware-based digital systems.

Related Information Notices

- IN 92-06, SUPPLEMENT 1: RELIABILITY OF ATWS MITIGATION SYSTEMS AND OTHER NRC-REQUIRED EQUIPMENT NOT CONTROLLED BY PLANT TECHNICAL SPECIFICATIONS
- IN 93-47: UNRECOGNIZED LOSS OF CONTROL ROOM ANNUNCIATORS

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact one of the technical contacts listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

Brian K. Grimes, Director
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Technical contacts: Jerry L. Mauck
(301) 504-3248

Eric J. Benner
(301) 504-1171

Attachment:
List of Recently Issued NRC Information Notices

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact (one of) the technical contact(s) listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

orig /s/'d by BKGrimes

Brian K. Grimes, Director
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Technical contacts: Jerry L. Mauck
(301) 504-3248

Eric J. Benner
(301) 504-1171

Attachment:
List of Recently Issued NRC Information Notices

*See previous concurrence

OFC	OEAB:DORS	SC/OEAB:DORS	PUB:ADM	SICB:DRCH
NAME	EBenner*	EGoodwin*	Tech Ed*	JMauck*
DATE	6/7/93	6/7/93	6/7/93	6/9/93

OFC	C/SICB:DRCH	C/OEAB:DORS	C/OGCB:DORS	D/DORS
NAME	JWermiel*	AChaffee*	GMarcus*	BGrimes
DATE	6/9/93	6/9/93	6/10/93	07/1/93

[OFFICIAL RECORD COPY]
DOCUMENT NAME: 93-49.IN

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact (one of) the technical contact(s) listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

Brian K. Grimes, Director
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Technical contacts: Jerry L. Mauck
(301) 504-3248

Eric J. Benner
(301) 504-1171

Attachment:
List of Recently Issued NRC Information Notices

*See previous concurrence

OFC	OEAB:DORS	SC/OEAB:DORS	PUB:ADM	SICB:DRCH
NAME	EBenner*	EGoodwin*	Tech Ed*	JMauck*
DATE	6/7/93	6/7/93	6/7/93	6/9/93

OFC	C/SICB:DRCH	C/OEAB:DORS	C/OGCB:DORS	D/DORS
NAME	JWermiel*	AChaffee*	GMarcus*	BGrimes
DATE	6/9/93	6/9/93	6/10/93	/ /93

mkm

[OFFICIAL RECORD COPY]
DOCUMENT NAME: G:\EJB1\SOFTWARE.IN

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please contact (one of) the technical contact(s) listed below or the appropriate Office of Nuclear Reactor Regulation (NRR) project manager.

Brian K. Grimes, Director
Division of Operating Reactor Support
Office of Nuclear Reactor Regulation

Technical contacts: Jerry L. Mauck
(301) 504-3248

Eric J. Benner
(301) 504-1171

Attachment: List of Recently Issued NRC Information Notices

*See previous concurrence

OFC	OEAB:DORS	SC/OEAB:DORS	PUB:ADM	HICB:DRCH
NAME	EBenner*	EGoodwin*	Tech Ed*	JMauck
DATE	6/7/93	6/7/93	6/7/93	6/9/93

OFC	C/HICB:DRCH	C/OEAB:DORS	C/OGCB:DORS CVH	D/DORS
NAME	JWermiel	AChaffee	GMarcus FOR	BGrimes
DATE	6/9/93	6/9/93	6/10/93	/93

WITH COMMENT

[OFFICIAL RECORD COPY]
DOCUMENT NAME: G:\EJBI\SOFTWARE.IN

LIST OF RECENTLY ISSUED NRC INFORMATION NOTICES

Information Notice No.	Subject	Date of Issuance	Issued to
93-48	Failure of Turbine-Driven Main Feedwater Pump to Trip Because of Contaminated Oil	7/6/93	All holders of OLs or CPs for nuclear power reactors.
92-06, Supp. 1	Reliability of ATWS Mitigation Systems and Other NRC-Required Equipment not Controlled by Plant Technical Specification	07/01/93	All holders of OLs or CPs for nuclear power reactors.
93-47	Unrecognized Loss of Control Room Annunciators	06/18/93	All holders of OLs or CPs for nuclear power reactors.
93-46	Potential Problem with Westinghouse Rod Control System and Inadvertent Withdrawal of A Single Rod Control Cluster Assembly	6/10/93	All holders of OLs or CPs for Westinghouse (W)-designed nuclear power reactors.
93-45	Degradation of Shutdown Cooling System Performance	06/16/93	All holders of OLs or CPs for nuclear power reactors.
93-44	Operational Challenges During A Dual-Unit Transient	06/15/93	All holders of OLs or CPs for nuclear power reactors.
93-43	Use of Inappropriate Lubrication Oils in Safety-Related Applications	06/10/93	All holders of OLs or CPs for nuclear power reactors.
93-42	Failure of Anti-Rotation Keys in Motor-Operated Valves Manufactured by Velan	06/09/93	All holders of OLs or CPs for nuclear power reactors.

OL = Operating License
CP = Construction Permit