

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

February 4, 1993

NRC INFORMATION NOTICE 93-11: SINGLE FAILURE VULNERABILITY OF ENGINEERED SAFETY FEATURES ACTUATION SYSTEMS

Addressees

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

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this notice to alert addressees to potential single failure vulnerabilities in engineered safety features actuation systems. 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

On July 6, 1992, during a planned outage at the Millstone Nuclear Power Station, Unit 2, with the core off loaded to the spent fuel pool, the licensee, the Northeast Nuclear Utilities Company, was preparing to replace two vital inverters. Millstone Unit 2 uses four inverters, two on each vital dc bus, to power two trains of engineered safety feature actuation comprised of four sensor cabinets and two actuation cabinets. Operators removed power from one actuation train, which caused a false loss of normal power signal and a false start signal for the emergency core cooling system. The effect of this action was similar in consequence to the complete loss of one of the two vital dc buses.

One emergency diesel generator (EDG) started and tied onto the bus. The second EDG did not start because it was out of service for maintenance. After the one EDG started, the safety loads failed to sequence onto the bus because of a continuous false load shed signal. Operators recovered from the event by stopping the EDG and restoring power to one of the sensor cabinets. This action removed the false loss of power signal and thus the load shed signal.

The licensee reviewed the event and concluded that an unblocking feature of the automatic test insertion (ATI) system had caused the continuous load shedding signal. The ATI system, a continuous, on-line, logic tester that is common for both trains, was still energized and permitted the spurious loss of power signal to continue to shed the loads. The ATI system applies 2-millisecond unblocking pulses to the input of the actuation logic modules

9301290025

PDR I&E Notice 93-011 930294

IDR-11C JPD

11

cc:

and checks the module outputs for proper operation. The 2-millisecond pulses are too brief to actuate relays and start equipment. In 1978, the licensee added a feature to permit ATI testing of the loss of normal power logic. To test the logic, the licensee determined that the ATI system needed to provide an unblocking of the loss of power signal for 500 milliseconds. In the actual event, the false signal generated by the lack of control power was continuously present during the 500 ms ATI unblocking signal. This caused a recurring load shed signal to be generated even though the EDG was ready to accept loads; therefore, the EDG load breakers never closed.

In reviewing the event, the licensee determined that the engineered safety feature actuation system could also cause other unintended actions under certain power supply failure conditions. These automatic actions are not related to the ATI modification.

- (1) If power is lost to either one of the two dc vital buses, both the safety injection actuation signal and sump recirculation actuation signal would be simultaneously initiated. The recirculation actuation signal would result in tripping all low pressure injection pumps. Also, the spurious sump recirculation actuation signal would cause one of the containment sump outlet valves to open.
- (2) If power was lost only to the sensor cabinets in one actuation train, both containment sump outlet valves would open. If this occurred during a loss-of-coolant accident, high pressure in containment could shut both refueling water storage tank check valves, inhibiting flow to all emergency coolant injection pumps.
- (3) The loss of all dc power to one actuation train would cause a power operated relief valve in the other train to open. In addition, when control power alone is lost to only the sensor cabinets in a single actuation train, spurious high pressurizer pressure signals would cause the relief valves in both trains to open. Both cases would result in a loss of primary coolant.

Discussion

The design deficiency in the on-line testing feature could have prevented both emergency diesels from accepting emergency loads under certain single failure conditions. The licensee investigated this event at Millstone Unit 2 and found several single failure vulnerabilities related to loss of a vital dc bus which may apply to engineered safety features actuation systems at other plants. Although the described event resulted from an ATI modification, the other vulnerabilities are inherent in the actuation system design and its power supplies.

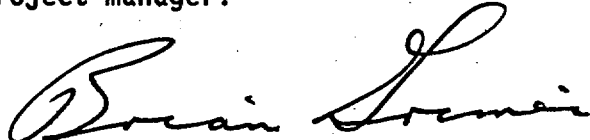
Millstone Unit 2 uses two-out-of-four logic supplied by Consolidated Controls Incorporated to actuate automatically a number of safety features. In the actuation system, a sensor, and subsequent interposing electronic logic, condition the signal for use by the actuation logic. Upon loss of power, the interposing logic generates a signal to perform the safety function. The problems discussed above result from having a two-out-of-four logic powered by

only two safety-related power sources coupled with a lack of coherence in specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC requested licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have automated safety-related actions with no preferred failure modes.

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: Ram S. Bhatia, Region I
(215) 337-5262

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

See file jacket

LIST OF RECENTLY ISSUED
NRC INFORMATION NOTICES

Information Notice No.	Subject	Date of Issuance	Issued to
93-10	Dose Calibrator Quality Control	02/02/93	All Nuclear Regulatory Commission medical licensees.
93-09	Failure of Undervoltage Trip Attachment on Westinghouse Model DB-50 Reactor Trip Breaker	02/02/93	All holders of OLs or CPs for nuclear power reactors.
93-08	Failure of Residual Heat Removal Pump Bearings due to High Thrust Loading	02/01/93	All holders of OLs or CPs for nuclear power reactors.
93-07	Classification of Transportation Emergencies	02/01/93	All licensees required to have an emergency plan.
93-06	Potential Bypass Leakage Paths Around Filters Installed in Ventilation Systems	01/22/93	All holders of OLs or CPs for nuclear power reactors.
93-05	Locking of Radiography Exposure Devices	01/14/93	All Nuclear Regulatory Commission industrial radiography licensees.
93-04	Investigation and Reporting of Misadministrations by the Radiation Safety Officer	01/07/93	All U.S. Nuclear Regulatory Commission medical licensees.
93-03	Recent Revision to 10 CFR Part 20 and Change of Implementation Date to January 1, 1994	01/05/93	All byproduct, source, and special nuclear material licensees.
93-02	Malfunction of A Pressurizer Code Safety Valve	01/04/93	All holders of OLs or CPs for nuclear power reactors.

OL = Operating License
CP = Construction Permit

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67

only two safety-related power sources coupled with a lack of coherence in specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC requested licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have automated safety-related actions with no preferred failure modes.

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.

Original signed by

Brian K. Grimes

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

Technical contacts: Ram S. Bhatia, Region I
(215) 337-5262

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	*C/OGCB:DORS:NRR GMarcus 01/22/93
*HICB:DRCH:NRR IAhmed 11/15/92	*C/HICB:DRCH:NRR SNewberry 11/24/92	*C/EELB:DE:NRR * CBerlinger 12/17/92	OEAB:DORS:NRR TKoshy 01/27/93
*SC/OEAB:DORS EGoodwin 01/15/93	NRC:DRS:R1 WRuLand 01/ /93	*C/OEAB:DORS:NRR AChaffee 01/19/93	D/DORS:NRR BKGrimes 1/29/93

Document Name: S:\DORS_SEC\93-11.IN

only two safety-related power sources coupled with a lack of coherence in specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC requested licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have "Automated Safety-Related Actions with No Preferred Failure Modes."

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: Ram S. Bhatia, Region I
(215) 337-5262

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	*C/OGCB:DORS:NRR GMarcus 01/22/93
*HICB:DRCH:NRR IAhmed 11/15/92	*C/HICB:DRCH:NRR SNewberry 11/24/92	*C/EELB:DE:NRR CBerlinger 12/17/92	OEAB:DORS:NRR TKoshy 1/27/93
*SC/OEAB:DORS EGoodwin 01/15/93	NRC:DRS:R1 WRuland 01/ /93	*C/OEAB:DORS:NRR AChaffee 01/19/93	D/DORS:NRR BKGrimes / /93

Document Name: S:\DORS_SEC\ESASIN.TK

only two safety-related power sources coupled with a lack of coherence in specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC required licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have "Automated Safety-Related Actions with No Preferred Failure Modes."

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-5262

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	C/OGCB:DORS:NRR GMarcus <i>gu for</i> 1/22/93
*HICB:DRCH:NRR IAhmed 11/15/92	*C/HICB:DRCH:NRR SNewberry 11/24/92	C/EELB:DE:NRR CBerlinger* 12/17/92	OEAB:DORS:NRR TKoshy* 01/15/93
SC/OEAB:DORS EGoodwin* 01/15/93	NRC:DRS:R1 WRuland* 01/ /93	C/OEAB:DORS:NRR AChaffee* 01/19/93	D/DORS:NRR BKGrimes / /93 <i>mlm</i>

Document Name: S:\DORS_SEC\ESASIN.TK

specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC required licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have "Automated Safety-Related Actions with No Preferred Failure Modes."

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-5262

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES			
*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	C/OGCB:DORS:NRR GMarcus <i>off for GHM</i> 1/22/93
*HICB:DRCH:NRR IAhmed 11/15/92	*C/HICB:DRCH:NRR SNewberry 11/24/92	C/EELB:DE:NRR CBerlinger* 12/17/92	OEAB:DORS:NRR TKoshy <i>SH</i> 1/15/93
SC/OEAB:DORS <i>S</i> EGoodwin 1/15/93	NRC:DRS:R1 WRuand * 1/93	C/OEAB:DORS:NRR AChaffee 1/19/93	D/DORS:NRR BKGrimes 1/93

Document Name: S:\DORS_SEC\ESASIN.TK

specifying the preferred failure mode for automated safety-related actions, given a loss of power.

The licensee is preparing modifications to correct these problems and is reviewing the design of Unit 2 for other similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC required licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have "Automated Safety-Related Actions with No Preferred Failure Modes."

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-9465 *5262*

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES			
*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	C:OGCB:DORS:NRR GMarcus / /93
*HICB:DRCH:NRR IAhmed 11/15/92	*C:HICB:DRCH:NRR SNewberry 11/24/92	C:EELB:DE:NRR CBerlinger* 12/17/92	OEAB:DORS:NRR TKoshy <i>AK</i> 1/14/93
SC/OEAB:DORS EGoodwin / /93	NRC:DRS:R1 <i>AK</i> <i>for</i> WRuland <i>BT</i> <i>Tels</i> / /93	C:OEAB:DORS:NRR AChaffee / /93	D:DORS:NRR BKGrimes / /93

Document Name: S:\DORS_SEC\ESASIN.TK

The licensee is preparing modifications to resolve these vulnerabilities and is reviewing the design of Unit 2 for other similar problems.

It should be noted that in NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC required licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems. In addition, in NRC Generic Letter 89-18, "Systems Interactions in Nuclear Power Plants," the NRC highlighted concerns regarding actuation system designs which may have "Automated Safety-Related Actions with No Preferred Failure Modes."

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-9465

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR R Moore 10/22/92	*OGCB:DORS:NRR JBirmingham 11/18/92	*TECH ED JMain 10/19/92	C:OGCB:DORS:NRR GMarcus 12/ /92
*HICB:DRCH:NRR IAhmed 11/15/92	*C:HICB:DRCH:NRR SNewberry 11/24/92	C:EEB.DE:NRR CBerlinger 12/17/92	OEAB:DORS:NRR TKoshy 12/17/92
NRC:DRS:R1 WRuland 12/ /92	C:OEAB:DORS:NRR AChaffee 12/ /92	D:DORS:NRR BKGrimes 12/ /92	

Document Name: A:\ESASIN.TK

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC addressed the review of this type of design vulnerability. The NRC required licensees to evaluate the effects of a loss of power to 1E and Non-1E instrument and control systems and to describe any proposed modifications resulting from the evaluation.

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-9465

Thomas Koshy, NRR
(301) 504-1176

Attachment: List of Recently Issued NRC Information Notices

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR R Moore 10/22/92	OGCB:DORS:NRR JBirmingham 11/17/92	*TECH ED JMain 10/19/92	C:OGCB:DORS:NRR GMarcus 11/ /92
HICB:DRCH:NRR IAhmed 11/15/92	C:HICB:DRCH:NRR SNeuberry 11/17/92	C:EELB:DE:NRR CBerlinger 11/ /92	OEAB:DORS:NRR TKoshy 11/ /92
NRC:DRS:R1 WRuland 11/ /92	C:OEAB:DORS:NRR AChaffee 11/ /92	D:DORS:NRR BKGrimes 11/ /92	

Document Name: A:\ESASIN.TK

power. The design problems resulted from having two-out-of-four logic combined with a single safety-related power source for two sensor cabinets.

The licensee is preparing modifications to resolve these vulnerabilities and is reviewing the design of Unit 2 for similar problems.

In NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," the NRC addressed the review of this type of design vulnerability. The NRC required the licensees to determine which instrument and control system loads connected to 1E and non-1E power sources and evaluate the effects of a loss of power to those loads.

This information notice requires no specific action or written response. If you have any questions about the information in this notice, please call 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: Ram S. Bhatia, Region I
(215) 337-9465

Thomas Koshy, NRR
(301) 504-1176

DISTRIBUTION:

*SEE PREVIOUS CONCURRENCES

*OGCB:DORS:NRR	OGCB:DORS:NRR	*TECH ED	C:OGCB:DORS:NRR
RMoore <i>un</i>	JBirmingham	JMain	GMarcus
10/22/92	10/ /92	10/19/92	10/ /92

HICB:DRCH:NRR	C:HICB:DRCH:NRR	C:EELB:DE:NRR	OEAB:DORS:NRR
IAhmed	SNewberry	CBerlinger	TKoshy
10/ /92	10/ /92	10/ /92	10/ /92

C:OEAB:DORS:NRR	DD:DRCH:NRR	D:DORS:NRR
AChaffee	CThomas	BKGrimes
10/ /92	10/ /92	10/ /92