Westinghouse Electric Corporation
Water Reactor Divisions

Nuclear Technology Division
Box 355
Pittsburgh, Pennsylvania 15230

November 7, 1979
NS-TMA-2150

Mr. Victor Stello, Jr.
Director
Office of Inspection and Enforcement
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Dear Mr. Stello:

Subject: Undetectable Failure in Engineered Safety Features Actuation System

As a result of our continuing reviews of systems important to safety, Westinghouse has identified an undetectable failure which potentially could exist in a circuit associated with Engineered Safeguards and which is required for reactor protection.

The specific circuit is described in the attachment. The design function of the circuit is a permissive to provide the operator, depending on plant conditions, the capability to manually reset and block Safety Injection.

A failure analysis, which assumed a failure of the affected circuit in both of the redundant protection trains (per IEEE-379), showed that the system's ability to automatically initiate the protective function could be lost under certain conditions.

Despite the low probability of the events necessary to set up the conditions, the NRD Safety Review Committee concluded on November 6, 1979, that the potential loss of the protective function is reportable to the NRC under Title 10CFR Part 21 for operating plants and Title 10CFR50.55(e) for plants under construction.

Detailed information, affected plants and recommended corrective action is contained in the attachment. This information has already been communicated to the utility owners of the affected plants.

Please refer any questions to Mr. D. H. Rawlins, the Manager of Safety Standards in the Westinghouse Nuclear Technology Division.

Very truly yours,

T. M. Anderson, Manager
Nuclear Safety Department

FMM/TMA/bek
Attachment

1342 011

7911160 111

Undetectable Failure in Engineered Safety Features Actuation System (ESFAS)

Design (refer to accompanying typical functional logic diagram)

The P-4 permissive is used to input the status (open or closed) of the Reactor Trip breakers to the Engineered Safety Features Actuation System (ESFAS). This P-4 permissive provides an interlock in the ESFAS to enable or defeat the capability to manually reset and block Safety Injection (SI).

In operation, the initiation of SI instantly trips the reactor and simultaneously starts an electric timer. After a preset time interval, determined by plant specific system analyses, the timer effectively returns system control to the operators for manual reset and block of SI in order to either begin ECCS switchover from the injection phase to the recirculation phase or terminate SI. The system permits manual reset and block of SI only if the P-4 permissive indicates that the trip breakers are open (i.e., the reactor is tripped).

During normal plant power operation, the P-4 permissive prevents manual actions which could electrically block SI.

Implementation

The P-4 permissive is derived from a switch contact operated via a mechanical linkage within the reactor trip breaker. When the breakers move (open or closed), the switch contact changes position. The contacts are hardwired to the ESFAS input logic which registers the trip breaker position to allow or prevent operator action as described above.

Testing

During normal plant operation, ESFAS logic is required to be periodically tested. On newer plants with the Solid State Protection System, this

testing is performed via automatic self test circuits which verify system operability. On older plants with a relay logic protection system, this testing is performed manually.

In addition, the reactor trip breakers are also periodically tested.

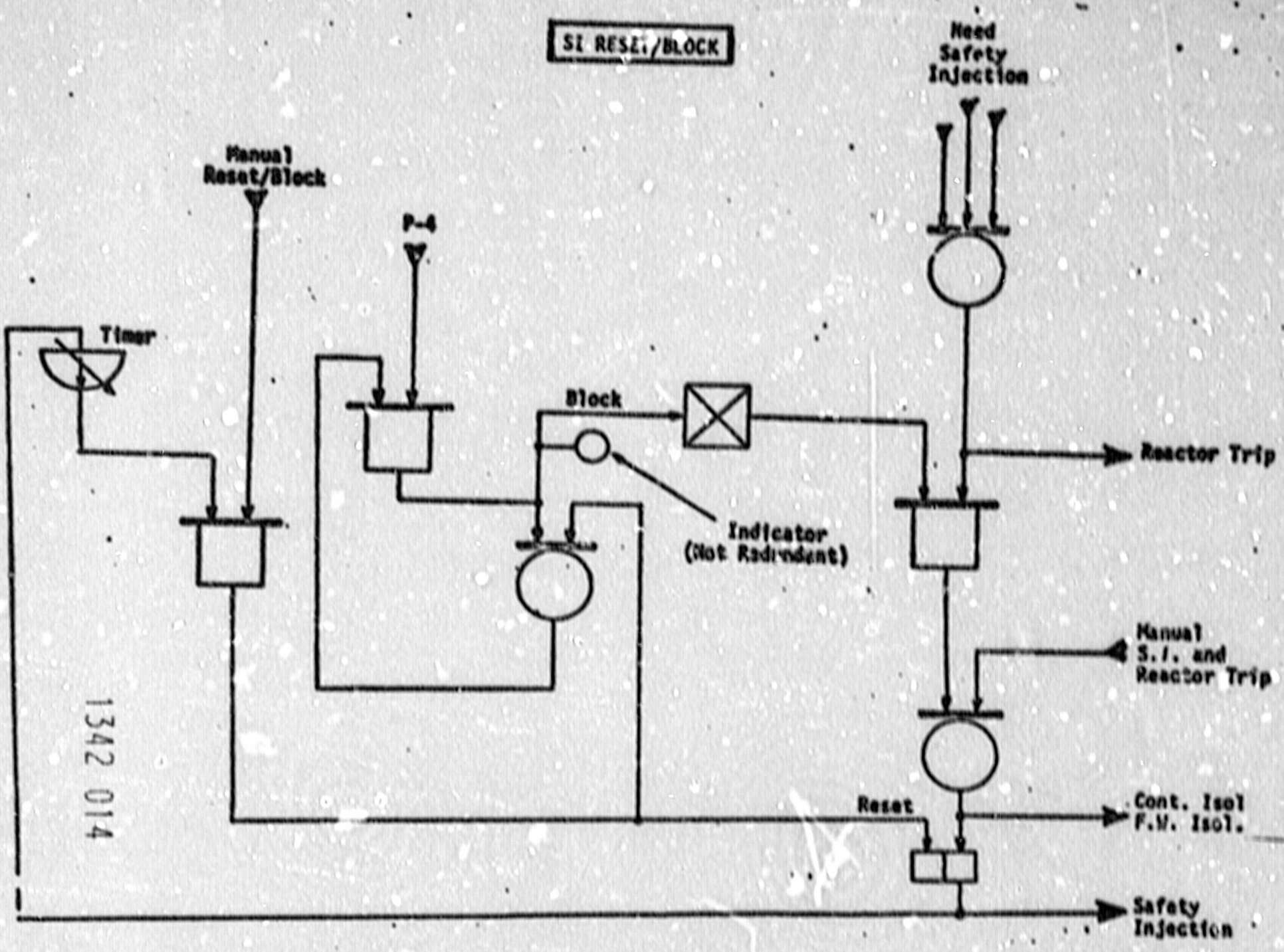
Potential Concern

Currently, the tests described above do not provide for checking the operation of the P-4 contacts or the interconnecting wiring. Therefore, a potential failure of the P-4 contacts or in the wiring would be undetectable.

IEEE 379 requires that in the case of undetectable failures either (1) provide revised test schemes to identify failures or redesign to eliminate them, or (2) in system failure analyses demonstrate that the safety function can be assured assuming both the undetectable failures have occurred and a random single failure has also occurred.

The failure modes of the P-4 contacts are (1) contacts fail to close when the reactor trip breakers open, or (2) contacts fail to open when the breakers are closed. Failure mode (1) could prevent the normal mode of resetting and blocking SI and alter the sequence of switchover operations from injection to recirculation phase. The consequences of failure mode (2) are such that following a previous initiation of SI and manual reset and block, the block of SI could remain following the reset of the reactor trip breakers and when the plant was returned to power.

No credit can be taken for illuminated Control Board windows (lamp bulbs) which would alert the operators to the hazard since they are not safety grade and are not implemented as such.


SI RESET/BLOCK
Need Safety Injection
Manual Reset/Block
P-4
Timer
Block
Reactor Trip
Indicator (Not Redundant)
Manual S.I. and Reactor Trip
Reset
Cont. Isol
F.W. Isol.
Safety Injection
1342 014

Affected Domestic Plants

Operating Plants

SSPS

D. C. Cook Units 1 and 2
Farley Unit 1
Beaver Valley Unit 1
Trojan
Salem Unit 1
North Anna Unit 1

Relay Logic

Zion Units 1 and 2
Prairie Island Units 1 and 2
Milwaukee
Indian Point Unit 3

Non-Operating Plants

SSPS

Farley Unit 2
Byron Units 1 and 2
Braidwood Units 1 and 2
Virgil C. Summer
Shearon Harris Units 1, 2, 3 and 4
McGuire Units 1 and 2
Catawba Units 1 and 2
Beaver Valley Unit 2
Vogtle Units 1 and 2
Jamesport Units 1 and 2

Non-Operating Plants (continued)

SSPS

Seabrook Units 1 and 2
Millstone Unit 3
Marble Hill Units 1 and 2
Diablo Canyon Units 1 and 2
Salem Unit 2
SMUPPS Units
Comanche Peak Units 1 and 2
South Texas Project Units 1 and 2
Sequoyah Units 1 and 2
North Anna Unit 2
Watts Bar Units 1 and 2
Haven Units 1 and 2

All other domestic plants are unaffected.

Recommended Corrective Actions

A. Plants Using Reactor Tripped Signal in Safety Injection Reset Circuit of Engineered Safeguards Relay Racks

Zion Units 1 and 2
Kewaunee
Prairie Island Units 1 and 2
Indian Point Unit 3

In the Engineered Safeguards Relay Racks for the above plants, a reactor tripped signal (Reactor Trip Breaker RTA and Bypass Breaker BYA open for Train A and Reactor Trip Breaker RTB and Bypass Breaker

BYB open for Train B) energizes Relay RTA in Train A and Relay RTB in Train B. These relays are located in the rear compartment of the relay racks. The relay coils and contacts are tested during on-line testing of the Safeguards Relay Racks. In addition to this testing, it is necessary to verify that the relays are operated by the auxiliary switch contacts of the Reactor Trip Switchgear.

1. During normal plant operation, immediately verify that relays RTA and RTB are deenergized.

2. After each reactor trip operation, verify that relays RTA and RTB are energized.

3. After closing the reactor trip breakers on plant startup, verify that relays RTA and RTB become deenergized.

4. If verification shows a relay is not in the correct position, check the interconnecting wires to the Reactor Trip Switchgear and the breaker auxiliary switch and cell switch contacts.

5. Verification of the correct relay position can be made by visual observation of the relays. (For Indian Point Unit 3, verification is made by observing the test lamp - "Reactor Trip Auxiliary Relay" - on the front of the Engineered Safeguards Relay Rack.)

NOTE 1: During on-line testing of the reactor trip breakers, relays RTA and RTB do not change position due to the closing of the bypass breaker for the test. Following on-line testing of the reactor trip breakers, observe that relays RTA and RTB remain energized.

NOTE 2: The interconnecting wiring from the Engineered Safeguards Relay Racks to the Reactor Trip Switchgear for relays RTA and RTB can be verified during normal plant operation. At the switchgear control terminal blocks, use a 0-150 volts dc range voltmeter or multimeter to measure the voltage across the two terminals connecting the switch contacts to the coil circuit of Relay RTA in the Train A Engineered Safeguards Relay Rack. A nominal 125 volts (dependent upon battery system voltage) reading should be indicated on the voltmeter. A zero reading indicates an open or short circuit in the interconnecting wiring from the relay racks or closed switch contacts, requiring corrective action. Repeat the voltmeter measurement across the two terminals connecting the switch contacts to Relay RTB coil circuit in the Train B Engineered Safeguards Relay Racks.

Revise appropriate procedures to require the verification tests noted above following automatic or manual reactor trip. Repeat the tests following reclosure of the reactor trip breakers and prior to rod withdrawal.

B. Byron/Braidwood/Marble Hill

Assure the following test sequence is adopted for each train of SSPS, with the plant at shutdown and the SSPS in Normal Operation:

1. Place a Simpson Model 260 multimeter in the 50 VDC range.

2. At the reactor trip switchgear, place the (+) lead on the terminal leading to the SSPS, TB506-4.

3. Place the (-) lead on the terminal leading to the SSPS, TB506-5.

4. The multimeter should read 0 VDC (nominal) with the reactor trip breaker tripped open.

5. This indicates either the reactor trip breaker P-4 contact is properly closed, the blocking diode or printed circuit card A519* is failed open or interconnecting wiring is open. The diode and wiring will be confirmed in the following steps.

6. With the multimeter still connected as in steps (2) and (3), close the reactor trip breaker.

7. The multimeter should read 48 VDC (nominal).

8. This indicates the reactor trip breaker P-4 contact is properly open, and confirms the blocking diode or printed circuit card A519* as well as the interconnecting wiring. End of test.

9. Should step (7) not yield a 48 VDC (nominal) reading, either the P-4 contact is not open, the blocking diode on printed circuit card A519* is open, or interconnecting wiring is open.

10. Initiate corrective action.

11. At the reactor trip switchgear, place the (+) lead on the terminal leading to the SSPS, TB508-7.

12. Place the (-) lead on the terminal leading to the SSPS, TB508-8.

13. The multimeter should read 0 VDC (nominal) with the bypass breaker, associated with steps (4) and (6), tripped.

* Located in the SSPS

14. This indicates either the bypass breaker P-4 contact is properly closed, the blocking diode on printed circuit card A519* is failed open or interconnecting wiring is open. The diode and wiring will be confirmed in the following steps.

CAUTION

DO NOT CLOSE BOTH BYPASS BREAKERS A & B SIMULTANEOUSLY. DOING SO WILL RESULT IN ALL BREAKERS INSTANTLY TRIPPING.

15. With the multimeter still connected as in steps (11) and (12), close the bypass breaker.

16. The multimeter should read 48 VDC (nominal).

17. This indicates the bypass breaker P-4 contact is properly open, and confirms blocking diode on printed circuit card A519* and the interconnecting wiring. End of test.

18. Should step (16) not yield a 48 VDC (nominal) reading, either the P-4 contact is not open, the blocking diode on printed circuit card A519* is open, or interconnecting wiring is open.

19. Initiate corrective action.

The appropriate procedures should reflect a requirement to perform the above tests following automatic reactor trip or any condition requiring opening of the reactor trip breakers. Repeat the tests following reclosure of the reactor trip breaks and prior to rod withdrawal.

C. Farley Unit 1, D. C. Cook Units 1 and 2, Beaver Valley Unit 1, Trojan, Salem Unit 1, North Anna Unit 1

Immediately perform the following for each train of SSPS:

1. Place a Simpson Model 260 multimeter in the 50 VDC range.

2. At the reactor trip switchgear, place the (+) lead on the terminal leading to the SSPS, TB506-4.

3. Place the (-) lead on the terminal leading to the SSPS, TB506-5.

4. The multimeter should read 48 VDC (nominal).

5. This indicates that P-4 contact(s) is (are) properly open, and confirms the blocking diode on printed circuit card A518* as well as the interconnecting wiring. End of test.

6. Should step (4) not yield a 48 VDC (nominal) reading, either P-4 contact(s) is (are) not open, blocking diode on printed circuit card A518* is open or interconnecting wiring is open.

7. Initiate corrective action.

Implement the test sequence in part D for future periodic testing when the plant is shutdown. Revise appropriate procedures to require verification by test of the P-4 contact status following automatic reactor trip or any condition requiring opening of the reactor trip breakers. Repeat the test following reclosure of the reactor trip breakers and prior to rod withdrawal.

D. All Other Non-Operating Plants With An SSPS Which Are Not Identified in Part B or C

Incorporate the following test sequence for each train of SSPS, when the plant is at shutdown and the SSPS in normal operation:

1. Place a Simpson Model 260 multimeter in the 50 VDC range.

2. At the reactor trip switchgear, place the (+) lead on the terminal leading to the SSPS, TB506-4.

3. Place the (-) lead on the terminal leading to the SSPS, TB506-5.

4. The multimeter should read 0 VDC (nominal).

5. This indicates the P-4 contact(s) is (are) properly closed, the blocking diode on printed circuit card A518* is failed open or interconnecting wiring is open. The diode and wiring will be confirmed in the following steps.

6. With the multimeter still connected as in steps (2) and (3), close the reactor trip breakers.

7. The multimeter should read 48 VDC (nominal).

8. This indicates the P-4 contact(s) is (are) properly open, and confirms the blocking diode on printed circuit card A518* as well as the interconnecting wiring. End of test.

9. Should step (7) not yield a 48 VDC (nominal) reading, either the P-4 contact(s) is (are) not open, the blocking diode on printed circuit card A518* is not open, or interconnecting wiring is open.

10. Initiate corrective action.

Revise appropriate procedures to require verification, by the above tests, of the P-4 contact status following automatic reactor trip or any condition requiring opening of the reactor trip breakers. Repeat the tests following reclosure of the reactor trip breakers and prior to rod withdrawal.