



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

DEC 24 1980

MEMORANDUM FOR: T. Novak, Assistant Director for Operating Reactors  
Division of Licensing

FROM: P. S. Check, Assistant Director for Plant Systems  
Division of Systems Integration

SUBJECT: CONFORMANCE OF THE DAVIS-BESSE 1 ENGINEERED SAFETY FEATURES  
ACTUATION SYSTEM (ESFAS) DESIGN TO IEEE STANDARD 279-1971,  
AND SHORT TERM CORRECTIVE ACTIONS TO PREVENT INADVERTENT  
SWITCHOVER OF ECCS PUMP SUCTION FROM THE BWST TO THE  
CONTAINMENT SUMP

On December 5, 1980 an inadvertent Engineered Safety Features Actuation System (ESFAS) actuation occurred at Davis-Besse (See Attachment) causing the low pressure ECCS pumps to transfer suction from the BWST (Borated Water Storage Tank) to the containment sump. During the investigation of this event, it was discovered that hardwired electrical connections exist between circuitry associated with ESFAS channels 1 and 3. Specifically, the power supply returns (floating commons) for the  $\pm 15$  Vd.c and 24 Vd.c supplies within the channel 1 and 3 ESFAS cabinets are electrically connected. A similar connection exists between channels 2 and 4. This raised the question as to whether the Davis-Besse ESFAS design is in conformance with Section 4.6 "Channel Independence" of IEEE Standard 279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations."

Section 4.6 (Channel Independence) of IEEE Standard 279-1971 states that: "Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction." The Davis-Besse ESFAS design does not comply with Section 4.6 of IEEE Standard 279-1971 with regard to independence between channels as evidenced by the hardwired electrical connections between ESFAS cabinets which partially contributed to the inadvertent switchover of December 5.

Furthermore, the Davis-Besse ESFAS design does not comply with Section 4.2 (Single Failure Criterion) of IEEE Standard 279-1971 which states that "Any single failure within the protection system shall not prevent proper protective action at the system level when required." A single failure within the Davis-Besse ESFAS system can adversely affect two ESFAS channels (via the electrical connection). Since these channels supply inputs to both ESFAS actuation trains, an inadvertent actuation could result causing both low pressure ECCS pumps to transfer suction from the BWST to a dry containment sump. Inadvertent transfer can result in ECCS pump damage and possible loss of safety function.

8101100 845

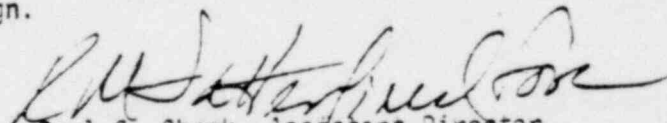
P

During a telecon held at Bechtel's Gaithersburg office on December 18, 1980, the licensee (Toledo Edison Company) maintained that the Davis-Besse ESFAS design is in compliance with IEEE Standard 279. The licensee's basis is that at the output level there are only two ESFAS actuation signals (Train A and Train B) and therefore, a failure of ESFAS channels 1 and 3 (Train A) via the common ground is acceptable since Train B would still be available and similarly, that Train A would be available if ESFAS channels 2 and 4 (Train B) failed. As noted above, however, both trains can be affected by a single failure.

By memo dated June 9, 1980 (P. Check to T. Novak) we informed you of another potential failure mode by which an inadvertent switchover of ECCS could occur at the Davis-Besse facility. On April 19, 1980 while in a refueling mode, an inadvertent safety features actuation occurred due to the loss of two essential distribution panels which were being supplied temporarily from a single power source. This caused the low pressure ECCS pumps to take suction from a dry containment sump. While this inadvertent transfer occurred as a result of modifications made during the refueling operation, it was found that the potential for such an inadvertent switchover may exist during other modes of operation. With Davis-Besse's two battery d.c. power supply system and 2-out-of-4 de-energize to actuate logic, it appears that a loss of offsite power in conjunction with the failure of a 250 Vd.c battery will cause an inadvertent switchover.

As an inadvertent transfer can result in ECCS pump damage and possible loss of safety function, the Division of Safety Technology (DST) is presently evaluating the advisability of continuing to require that switchover be performed automatically. Davis-Besse appears to be particularly susceptible to inadvertent switchovers as demonstrated by operating experience and the number of potential failure modes identified. To preclude the potential for loss of the ECCS safety function, we recommend that Davis-Besse be allowed to disable the automatic transfer feature for the interim period required to complete the DST study. We recognize that this modification would require an assessment of the operator's capability to perform the transfer, and modification of the plant emergency operating procedures. Therefore, the Division of Human Factors Safety (DHFS) should concur in our recommendation prior to its implementation.

The above modification will resolve our concern with regard to inadvertent automatic switchover of the ECCS. We are continuing to assess the adequacy of the Davis-Besse ESFAS design.

  
Paul S. Check, Assistant Director  
for Plant Systems  
Division of Systems Integration

Attachment:  
As stated

cc: See Attached List

Contact:  
R. Kendall  
X29430

DECEMBER 5, 1980 EVENT AT DAVIS-BESSE;  
INADVERTENT AUTOMATIC SWITCHOVER OF ECCS FROM THE  
INJECTION MODE TO THE RECIRCULATION MODE

On December 5, 1980 an inadvertent ESFAS (Engineered Safety Features Actuation System) actuation occurred at the Davis-Besse Nuclear Plant while in a hot shutdown mode of operation. This inadvertent actuation was caused by the tripping of containment high pressure and BWST (Borated Water Storage Tank) low level bistables in ESFAS channels 1 and 3 which satisfied the 2-out-of-4 de-energize to actuate logic. ESFAS levels 1, 2, 3, and 5 were actuated (containment isolation, low pressure injection, high pressure injection, and realignment of low pressure ECCS pump suction from the BWST (Injection phase) to the emergency containment sump (Recirculation phase)).

The ESFAS level 5 (automatic switchover of ECCS pump suction to the containment sump) actuation logic at Davis-Besse consists of two actuation trains. Train A receives inputs from ESFAS channels 1 and 3 and Train B receives inputs from ESFAS channels 2 and 4.

Just prior to the inadvertent ESFAS actuation of December 5, 1980, the licensee was attempting to isolate an electrical short affecting ESFAS channels 1 and 3. Channel 3 was de-energized to investigate the problem. Upon re-energization a channel 3 indicating lamp failed to illuminate. While attempting to replace this lamp, a ground occurred between the lamp and the module chassis causing the loss of a channel 1  $\pm$  15 Vd.c power supply. Since channel 3 had not been reset, the 2-out-of-4 logic initiated the inadvertent ESFAS actuation.

Subsequent investigation revealed a hardwired electrical connection between circuitry associated with ESFAS channels 1 and 3. Specifically, the power supply returns (floating commons) for the  $\pm 15$  Vd.c and 24 Vd.c supplies within the channel 1 and 3 ESFAS cabinets are electrically connected. A similar connection exists between channels 2 and 4.

The bistables (BWST low level, containment high pressure, etc.) within a given ESFAS channel are powered from the  $\pm 15$  Vd.c regulated supply for that channel. This voltage is required to maintain parameter setpoints at the desired value as dictated by the Technical Specifications. Voltage perturbations, therefore, can adversely effect (change the value of) these setpoints. This occurred during the 12/5/80 event at Davis-Besse. Because of the electrical interconnections between ESFAS channels at Davis-Besse a single failure (voltage perturbation) can simultaneously affect two ESFAS channels (bistable trip setpoints) at the input level. In addition, since the output from each bistable is used as an input to all 4 ESFAS actuation logics, a single failure via the common ground and the 2-out-of-4 logic arrangement can affect both ESFAS trains. In the case of level 5, this could cause both trains of low pressure ECCS pumps to transfer suction from the BWST to a dry containment sump.

During a telecon held at Bechtel's Gaithersburg office on December 18, 1980, the licensee (Toledo Edison Company) maintained that the Davis-Besse ESFAS design is in compliance with IEEE Standard 279. The licensee's basis is that at the output level there are only two ESFAS actuation signals (Train A and Train B) and therefore, a failure of ESFAS channels 1 and 3 (Train A) via the common ground is acceptable since Train B would still be available and similarly, that Train A would be available if ESFAS channels 2 and 4 (Train B) failed. As noted above, however, both trains can be affected by a single failure.

By memo dated June 9, 1980 (P. Check to T. Novak) we informed you of another potential failure mode by which an inadvertent switchover of ECCS could occur at the Davis-Besse facility. On April 19, 1980 while in a refueling mode, an inadvertent safety features actuation occurred due to the loss of two essential distribution panels which were being supplied temporarily from a single power source. This caused the low pressure ECCS pumps to take suction from a dry containment sump. While this inadvertent transfer occurred as a result of modifications made during the refueling operation, it was found that the potential for such an inadvertent switchover may exist during other modes of operation. With Davis-Besse's two battery d.c. power supply system and 2-out-of-4 de-energize to actuate logic, it appears that a loss of offsite power in conjunction with the failure of a 250 Vd.c battery will cause an inadvertent switchover.

As an inadvertent transfer can result in ECCS pump damage and possible loss of safety function, the Division of Safety Technology (DST) is presently evaluating the advisability of continuing to require that switchover be performed automatically. Davis-Besse appears to be particularly susceptible to inadvertent switchovers as demonstrated by operating experience and the number of potential failure modes identified. To preclude the potential for loss of the ECCS safety function, we recommend that Davis-Besse be allowed to disable the automatic transfer feature for the interim period required to complete the DST study. We recognize that this modification would require an assessment of the operator's capability to perform the transfer, and modification of the plant emergency operating procedures. Therefore, the Division of Human Factors Safety (DHFS) should concur in our recommendation prior to its implementation.

The above modification will resolve our concern with regard to inadvertent automatic switchover of the ECCS. We are continuing to assess the adequacy of the Davis-Besse ESFAS design.

mod: [unclear]  
[unclear]

Paul S. Check, Assistant Director  
for Plant Systems  
Division of Systems Integration

Attachment:  
As stated

DISTRIBUTION:  
Central File  
ICSB Reading File

cc: See Attached List

Contact:  
R. Kendall  
X29430

ICSB RKendall:cc 12/24/80	ICSB MSrinivasan 12/24/80	ICSB RSatterfield 12/24/80	ADPS PCheck 12/24/80
---------------------------------	---------------------------------	----------------------------------	----------------------------

cc: D. Ross  
G. Lainas  
F. Rosa  
O. Parr  
T. Speis  
R. Satterfield  
J. Olshinski  
M. Srinivasan  
T. Dunning  
R. Reid  
K. Wickman  
G. Holahan  
P. Shemanski  
D. Garner  
N. Villalva  
J. T. Beard  
A. Thadani  
E. Adensam  
J. E. Knight  
G. Vissing  
E. Rossi  
D. Thatcher  
M. Chiramal  
R. Kendall  
W. Kennedy  
D. Beckham

REGULATORY DIVISION FILE COPY