SAFETY EVALUATION - DAVIS-BESSE
ELECTRICAL INDEPENDENCE BETWEEN REDUNDANT SAFETY
FEATURES ACTUATION SYSTEM INSTRUMENT AND LOGIC CHANNELS

INTRODUCTION AND BACKGROUND

Following an inadvertent safety features actuation system (SFAS) actuation at Davis-Besse on December 5, 1980, it was discovered that hardwired electrical connections exist between circuitry associated with redundant SFAS instrument and logic channels 1 and 3. Specifically, the power supply returns (floating commons) for the ±15 Vdc and +24 Vdc supplies within the SFAS cabinets for channels 1 and 3 were electrically connected. Similar connections existed between SFAS channels 2 and 4. The Davis-Besse SFAS uses a 2-out-of-4 "deenergize-to-actuate" logic for the actuation of engineered safety features equipment. Each of four instrument/sensing channels (for each monitored SFAS parameter) provides inputs to each of four logic channels. Each logic channel provides an output when any two or more of its inputs are in a tripped condition. The outputs of logic channels 1 and 3 are combined to form SFAS actuation channel 1 which initiates SFAS equipment in train 1. Similarly, SFAS logic channels 2 and 4 are combined to form SFAS actuation channel 2 which initiates equipment in train 2. Both logic channels associated with an actuation channel must be tripped in order to cause an SFAS actuation. Prior to the SFAS actuation on December 5, 1980, a short circuit within a +15 Vdc power supply associated with SFAS instrument channel 1 resulted in 120 Vac on the shared (floating) return between channels 1 and 3. This caused bistable setpoints within both channels to deviate from their normal values, in some cases exceeding Technical Specification limits. This condition existed for several days prior to the SFAS actuation.

The staff's review of the interconnections between redundant SFAS channels raised the following concerns: 1) An electrical fault on a shared power supply return could potentially cause a spurious SFAS actuation and 2) an undetected

fault (the shared power supply returns are not continuously monitored for fault conditions) coupled with a single failure within a channel unaffected by the fault could potentially prevent a SFAS actuation when needed. The licensee instituted monthly surveillance testing to determine the presence of extraneous voltage on the SFAS commons. However, the staff does not consider this frequency sufficient to identify and correct fault conditions prior to adversely affecting components within redundant SFAS channels. The staff concluded that the Davis-Besse SFAS design does not comply with the requirements of Section 4.6 (Channel Independence) of IEEE Standard 279-1971.

In order to resolve the staff's concerns regarding the common ties between redundant SFAS sensing and logic channels, the licensee proposed to permanently connect the floating commons to the instrument ground. The SFAS was functionally tested successfully in this configuration. With the floating commons connected to the instrument ground, the effects of power supply failures similar to that which occurred prior to the inadvertent SFAS actuation on December 5, 1980 would be limited to a single SFAS instrument or logic channel. The licensee, however, cautioned that grounding the commons would result in significant potential hazards relating to system reliability, that ground faults or stray voltages occurring subsequent to grounding could potentially damage an instrument channel, and concluded that this configuration poses a greater potential for SFAS damage and is considered highly undesirable.

The staff's review of the licensee's proposal concluded that although permanent grounding of the shared floating commons may resolve SFAS channel independence concerns, additional information supporting SFAS connections to the instrument ground system was required since the Davis-Besse plant has had a history of problems regarding the instrument ground system and its relationship to the station ground system. The specific concern was that inadvertent ties exist between these systems at other than the designed common tie point. Given an electrical fault, loop fault current could produce an induced voltage in systems connected to the instrument ground, potentially affecting system operability. The licensee submitted an analysis which demonstrated that safety systems would perform as intended given the worst case station electrical fault

condition with the inadvertent ties present between the instrument and station ground systems. The staff's review of the analysis concluded that the installed instrument-station ground system was acceptable based on the understanding that there were no inadvertent ties between the SFAS instrument ground (i.e., the floating returns) and the station ground, and therefore, that faults could not be postulated that would adversely affect the engineered safety features of the facility. Therefore, the staff requested the licensee to provide additional information demonstrating that connecting the floating power supply returns (SFAS instrument grounds) to the instrument ground system was an acceptable approach to resolving the SFAS channel separation concern, and that the operability of the SFAS will be assured following such a modification.

Subsequent to the staff's request, the licensee requested a meeting with the staff to discuss alternate methods available to resolve the issue. Options considered by the licensee included 1) continuous monitoring of the ±15 Vdc and +24 Vdc SFAS power supply commons for electrical fault conditions, 2) connecting the power supply commons to the instrument ground system as discussed above, 3) physically removing all interconnections between redundant SFAS channels, thus separating the power supply returns, and 4) separating the sensor/instrument channel power supplies from the logic/actuation power supplies, and removing the connections between redundant instrument channel power supplies. The licensee has decided to implement option 4.

EVALUATION

Two figures are provided at the end of this report to aid in the understanding of the material in this section. Figure 1 shows the Davis-Besse SFAS logic configuration and the boundary between instrument/sensor channels and logic/actuation channels. Figure 2 shows the SFAS power supply configuration before and after the modifications. Both of these figures reflect the general Davis-Besse SFAS design, but have been greatly simplified and should not be used to infer design details.

The Davis-Besse SFAS design uses ±15 Vdc and +24 Vdc power supplies. The -15 Vdc supplies provide power to sensor/instrument channel components only. The +24 Vdc supplies provide power to logic/actuation channel components only. The +15 Vdc supplies provide power to both the instrument and logic portions of the SFAS. The SFAS dc power supply design uses a floating ground system, i.e., the power supply returns (commons) are isolated from the SFAS cabinet structure which is connected to the instrument-station ground system. The floating returns for SFAS instrument channel #1, logic channel #1, instrument channel #3, and logic channel #3 are electrically connected (hardwired). Similar connections exist between SFAS channels 2 and 4. These connections between redundant SFAS channels led to the channel independence and single failure concerns identified by the staff. The floating return configuration was selected by design to reduce the number of contacts (and thus the amount of field run wiring) from SFAS relays and control switches needed to actuate SFAS equipment, and to reduce the potential for degradation of SFAS performance given a fault voltage existing between the SFAS dc common and the SFAS cabinet structure.

To provide electrical independence between redundant SFAS instrument channels, four new +15 Vdc supplies will be used to provide power to instrument channel components. New power supplies will be added to SFAS cabinets 2 and 4, and existing +15 Vdc supplies which are currently spares will be used in SFAS cabinets 1 and 3 (these supplies were originally provided for automatic test circuitry which is no longer used). These supplies will provide power to instrument channel components only (amplifiers, current isolation converters, bistable modules, etc., and associated test and calibration circuits). The existing SFAS +15 Vdc supplies that were previously used for both instrument and logic channel components will now be used to provide power to SFAS logic/actuation channel components only. The four instrument channel +15 Vdc supplies will be electrically independent from each other, and each supply will be electrically separated from its corresponding +15 Vdc logic channel power supply. Thus, each SFAS instrument channel will have its own dedicated +15 Vdc and -15 Vdc power supplies. These supplies will share the same floating ground (designated as the "sensor common"). The sensor commons of redundant SFAS

instrument channels are not connected, thus maintaining channel independence. Each SFAS logic/actuation channel will have its own dedicated +15 Vdc and +24 Vdc power supplies which share a separate floating ground (designated as the "logic common"). The sensor common and logic common within each SFAS cabinet are not connected, thus maintaining electrical separation between the sensor and logic portions of the SFAS. All connections which previously tied the sensor and logic commons together and redundant instrument channel supply commons together have been eliminated.

The above modifications can be accomplished by circuit modifications within the four SFAS. The electrical separation of redundant sensor commons will assure that the effects of SFAS power supply failures similar to that which occurred prior to the inadvertent actuation on December 5, 1980 will be limited to a single SFAS instrument channel (i.e., multiple/redundant channels will not be affected). In addition, since the floating power supply return configuration has been retained, the above modifications will not make the SFAS more vulnerable to spurious trips or equipment damage from electrical faults, and connections between the SFAS and the instrument-station ground system have been avoided.

It should be noted that following the SFAS modifications, the logic commons for SFAS logic/actuation channels 1 and 3 will remain electrically connected as will the logic commons for channels 2 and 4. SFAS logic channels 1 and 3 are combined to actuate SFAS equipment in train 1 (powered from division 1). Both channels 1 and 3 must trip to cause actuation. SFAS logic channels 2 and 4 operate in a similar fashion to actuate equipment in train 2 (powered from division 2). Because the logic/actuation channels associated with a given train of SFAS equipment are not electrically independent, an electrical fault condition associated with a shared logic common could be postulated to disable both logic/actuation channels and therefore, to disable the safety functions of one train of SFAS equipment. However, this situation is not considered more limiting than other failure modes (e.g., loss of divisional power), where SFAS equipment in the redundant train is relied on to accomplish required safety functions. Furthermore, since the two logic/actuation channels associated with

a given SFAS train are arranged in a 2-out-of-2 (logical "AND") configuration (i.e., both channels must trip to cause equipment actuation), a single failure of either logic/actuation channel will preclude the SFAS safety functions of a single train. However, four electrically independent logic/actuation channels are not required to comply with NRC regulations. A four channel design in which dependent logic channels are combined to form two electrically independent actuation channels, such as the Davis-Besse design, is acceptable if properly implemented. Therefore, the electrical connections between redundant logic commons are considered acceptable provided that adequate isolation exists between the sensor and logic portions of each SFAS channel (such that faults within the logic portion can not affect instrument/sensor channel performance), and that faults within the logic portion of the SFAS are detectable.

There are two types of interfaces which occur between the instrument/sensor portions and the logic/actuation portions of the Davis-Besse SFAS. The first and most frequently used interface occurs at the bistable module outputs. Each bistable for each SFAS monitored parameter (containment radiation, containment pressure, reactor coolant pressure, and borated water storage tank level) provides four isolated outputs, one output to each SFAS logic channel. Thus, even the output signal to the associated logic channel is isolated. Isolation is provided by opto-electronic devices housed in the bistable modules. The second interface occurs at the reactor coolant pressure bistable modules used to generate block permissives that allow manual bypass of the reactor coolant low pressure trip functions. Here, relay coil-to-contact isolation is used between the logic channel (+24 Vdc relay side) and the instrument channel (+15 Vdc contact side). The staff concludes that the isolation provided between the sensors channels and logic channels is acceptable to maintain sensor channel independence. All other instrument channel circuits (e.g., indicators, annunciator outputs, computer outputs, etc.) are isolated using relay coil-to-contact isolation or current-to-current converters. The licensee has stated that the physical separation between redundant SFAS sensor and actuation channels, reviewed and approved during plant licensing, has not been compromised as a result of the SFAS modifications discussed above.

The licensee has proposed testing following implementation of the modifications to demonstrate that instrument/sensor channel portions of the SFAS have been effectively isolated from the logic/actuation portions of the SFAS. Specifically, the resistance between the sensor common and the logic common for each SFAS channel will be measured to verify electrical separation. In addition, the resistance between the sensor common and the SFAS cabinet structure, and the logic common and the SFAS cabinet structure for each SFAS cabinet will be measured to verify isolation of the SFAS from the instrument-station ground system. The acceptance criteria for these tests will be a resistance of greater than 10 megohms. The staff concludes that these tests and the acceptance criteria are acceptable to demonstrate adequate isolation. However, the staff recommends that a similar resistance test be performed between redundant SFAS sensor commons to verify that all connections between redundant sensor channels have been eliminated. If the only connections between redundant SFAS sensor channels in the original design were due to the shared dc commons by sensor and logic channels and the subsequent sharing of logic commons in the actuation circuits for SFAS equipment, then this test will reaffirm the effectiveness of the modifications to provide isolation between sensor channels (i.e., this test will verify that no direct connections exist between redundant sensor channels). The licensee has committed to perform the routine monthly SFAS surveillance tests following the modifications to verify the functional performance of SFAS sensor and logic circuits.

Surveillance test procedure ST 5031.03, "Containment Pressure to SFAS Calibration," requires monthly testing for ac voltage potential between each SFAS logic common and the station ground. This test is used to detect power supply or other failures similar to that which occurred prior to the inadvertent SFAS actuation on December 5, 1980. Following the SFAS modifications, this testing will continue, and will be extended to include the SFAS sensor commons (i.e., testing for ac voltage potential between each SFAS sensor common and the station ground will also be performed monthly). The continued monthly testing of the SFAS logic commons is necessary because an electrical fault on one of the floating logic commons may not be easily/quickly detected. The staff has

determined that the monthly surveillance frequency is the minimum acceptable for detecting faults which may have occurred, and taking appropriate corrective actions to ensure that the SFAS is not degraded below an acceptable level.

CONCLUSION

Based on the review of information provided by the licensee in letter #1229 dated December 16, 1985, and an audit review of the field change procedure, including revised electrical schematic/elementary diagrams of the SFAS, the staff concludes that the modifications proposed by the licensee are sufficient to resolve staff concerns regarding independence between redundant SFAS instrument channels and to bring the Davis-Besse SFAS design into conformance with Section 4.6 (Channel Independence) of IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." Therefore, the staff concludes that the proposed modifications to the Davis-Besse SFAS are acceptable pending successful completion of the post-modification tests discussed in the above evaluation. The acceptability of the modifications is based in part on continued monthly testing of the SFAS instrument and logic commons to detect for degraded voltage conditions. In addition, the licensee should perform resistance tests between redundant SFAS sensor commons to verify that all connections between redundant sensor channels have been removed, and the results of these tests should be submitted for staff review.

DAVIS-BESSE SAFETY FEATURES ACTUATION SYSTEM (SFAS)
LOGIC DIAGRAM

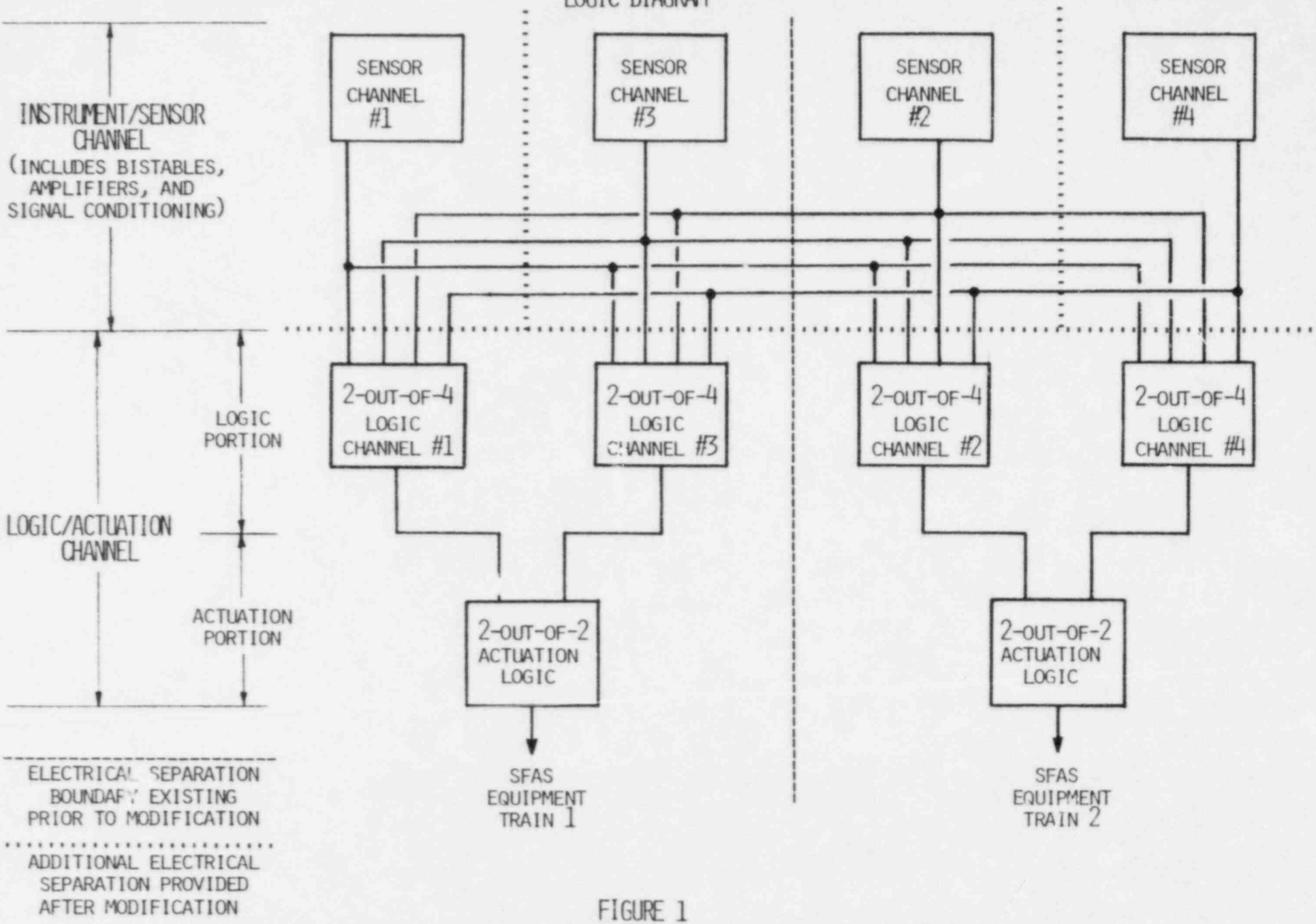
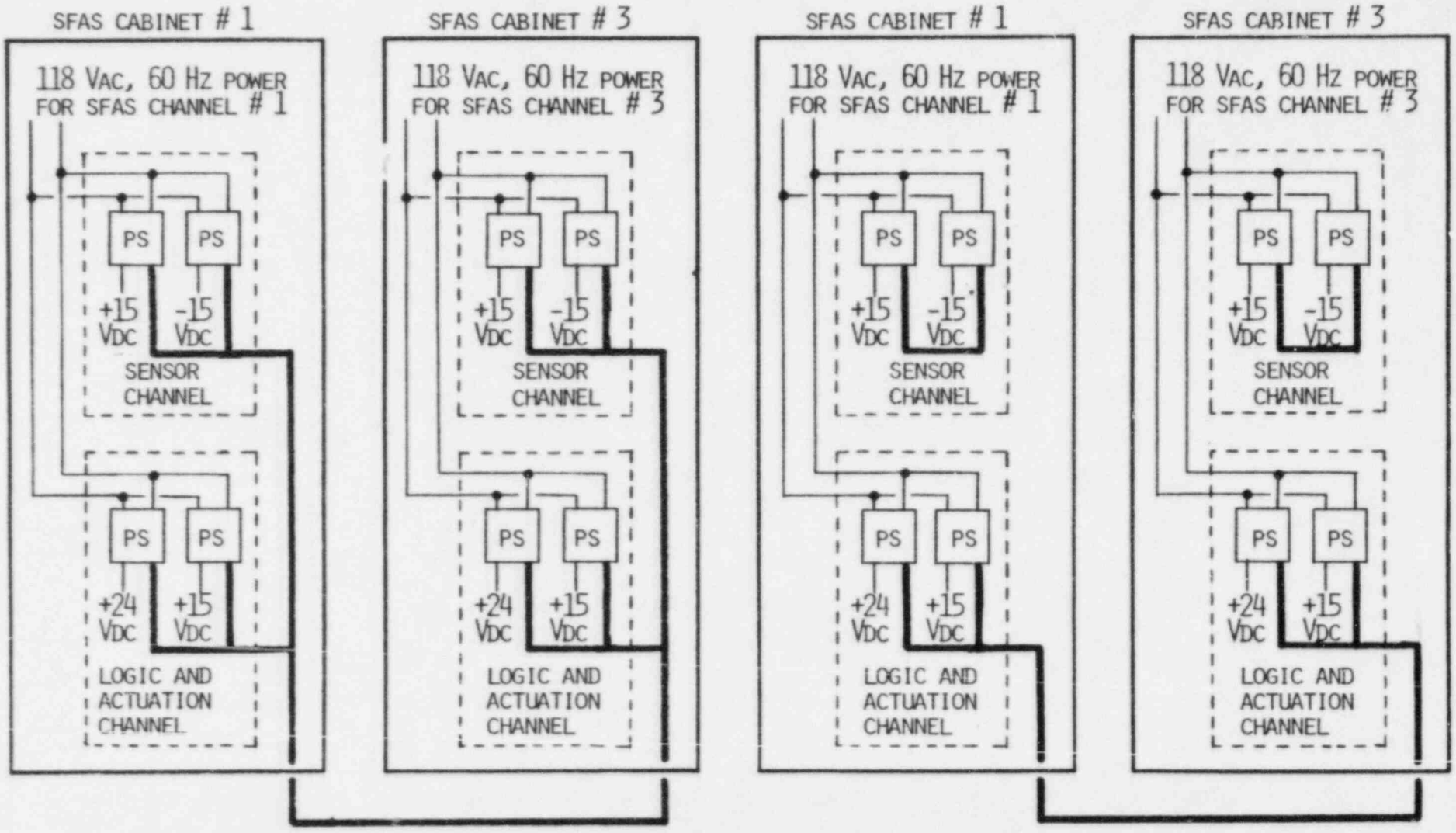


FIGURE 1

DAVIS-BESSE SAFETY FEATURES ACTUATION SYSTEM (SFAS)
SENSOR AND LOGIC CHANNEL POWER SUPPLY BLOCK DIAGRAM
(CHANNELS 1 AND 3 ARE SHOWN; CHANNELS 2 AND 4 ARE SIMILAR)



THE HEAVY LINE REPRESENTS THE FLOATING SFAS POWER SUPPLY RETURNS

FIGURE 2

PS = POWER SUPPLY - ONLY ONE IS SHOWN; AS MANY AS THREE OR FOUR MAY BE PROVIDED