PLANT GENERAL DESIGN &
SAFETY INJECTION SYSTEM INFORMATION
FROM NORTH ANNA IPE

TABLE 2-2
SUMMARY OF DESIGN FEATURES: NORTH ANNA UNIT 1

1.	Coolant Injection System	a.	High-Pressure Safety Injection and Recirculation System with 2 trains and 3 pumps. System provides normal makeup flow with crosstie to Unit 2.
		b.	Low-Pressure Injection and Recirculation System with 2 trains and 2 pumps.
2.	Heat Removal Systems	a.	Power Conversion System.
		b.	Auxiliary Feedwater System (AFW) with 3 trains and 3 pumps (2 MDP, 1 TDP)*.
		c.	RHR System with 2 pumps and 2 trains inside Containment.
		d.	2 pressurizer power operated relief valves.
3.	Reactivity Control Systems	a.	Control rods.
		b.	Chemical and Volume Control (CH) System.
4.	Key Support Systems	a.	DC power provided by 2 trains of batteries.
		b.	Emergency AC power provided by 2 dedicated diesel generators (both self-cooled).
		c.	Component Cooling Water provides normal cooling to RCP thermal barriers.

TABLE 2-2 (Continued)
SUMMARY OF DESIGN FEATURES: NORTH ANNA UNIT 1

		d.	Service Water is normally fed from a reservoir. Lake Anna serves as an alternate supply of Service Water. The SW system provides heat removal from Containment following an accident.
5.	Containment Structure	a.	Subatmospheric (10 psia).
		b.	1.82 million cubic feet.
		c.	45 psig design pressure.
		d.	Reinforced concrete.
6.	Containment Systems	a.	Quench Spray injection initiated at 28 psia with 2 trains and 2 pumps.
		b.	Inside Recirculation Spray (IRS) initiated at 28 psia with time delay with 2 trains and 2 pumps (both pumps inside Containment).
		c.	Outside Recirculation Spray initiated at 28 psia with time delay with 2 trains and 2 pumps (both pumps outside Containment).
		d.	The Inside and Outside Spray Recirculation Systems provide the only form of Containment heat removal after a LOCA.

*MDP - motor driven pumps
TDP - turbine driven pumps

A.7 SAFETY INJECTION SYSTEM

Schematics for this system are shown in Figures A.7-1 and A.7-9. The one line diagrams include the safety injection subsystems and the safety injection actuation logic trains.

A.7.1 SI System Major Components

The Safety Injection System consists of three accumulators, one hydrostatic test pump, three high head safety injection (HHSI) pumps (also called charging pumps), one boron injection tank (BIT), and two low head safety injection (LHSI) pumps. This subsection describes the major SI System components and the flow paths used to achieve the purpose. The RWST is a major component of the QS System, but it has many safety related interfaces with the SI System. Therefore, the RWST interfaces will be discussed with the SI System major components.

Accumulators

The Safety Injection System has three accumulators: 1A, 1B, and 1C. Two of the three accumulators refill the reactor inlet plenum, downcomer, and lower core basket with borated water following a LOCA. The third accumulator is assumed in the accident analysis to be dumped out of the break. The accumulators are considered to be passive components since no electrical signal, operator action, or power is required for their operation. This subsection describes accumulator 1A. Accumulators 1B and 1C are identical except for valve numbering. The accumulators are located on the 216-foot level of Containment inside the crane wall. Figure 52-2 shows a piping diagram for accumulator 1A. Each accumulator is a pressure vessel filled with at least 7580 gallons of 2200 to 2400 parts per million (ppm) borated water and pressurized with nitrogen gas to 599 to 667 psig. The carbon steel vessel is internally clad with stainless steel and has a total volume of 1450 cubic feet. Remote accumulator pressure and level indication is provided in the Main Control Room.

Each accumulator is connected to its respective RCS cold leg through a motor-operated, accumulator isolation valve MOV-1865A and two swing-check valves. The accumulator isolation valve is used to prevent emptying the accumulator during normal plant cooldown and depressurization. All of the accumulator isolation valves are opened during RCS pressurization when the RCS pressure is between 900 and 950 psig. Above 100 psig, power is removed from the valve operators, and the power supply breakers are locked open. This action partially satisfies technical specification requirements for accumulator operability.

During RCS depressurization in support of unit shutdown, the MOVs are energized when RCS pressure is <1990 psig. This is done by unlocking the admin. locks on the power supply breakers (located on the emergency bus 480 V MCCs in the cable vault), removing the locks, and closing the respective breakers. The MOVs are left open until RCS pressure has been reduced to 950 psig. They are then closed, but the valve operators remain energized until RCS temperature is reduced to <350°F.

The accumulator check valves are normally held shut by the higher RCS pressure of 2235 psig. During a LOCA, when RCS pressure drops below the approximately 600 psig, the check valves open and the accumulator discharges into the RCS without any external requirements. A connection is provided upstream of each check valve for accumulator sampling and to permit testing the check valves for seal leakage during RCS pressurization when there is about 100 psi differential pressure across the valves.

Refueling water storage tank

There is one refueling water storage tank (RWST) per unit. It is located in the yard next to the Safeguards Building. The RWST performs the following functions:

1. Provides borated water to the HHSI pumps, LHSI pumps, and quench spray pumps.

2. Provides alternate source of water to the HHSI pumps during abnormal operations.

3. Provides storage water for the refueling cavity.

The RWST is a vertical, cylindrical tank with a usable capacity of 487,000 gallons. It must contain at least 466,200 gallons of 2300 to 2400 ppm borated water during unit operation in modes 1-4. The proper boron concentration is maintained by the Chemical and Volume Control System (CVCS). The RWST is required to be maintained between 40° and 50°F during unit operation in modes 1-4. The maximum allowed temperature ensures that sufficient cooling capacity is available for the QS System to depressurize Containment in the time required in the event of a LOCA. Further information on the RWST may be found in the QS System training module (NCRODP-53). The water from the RWST is directed to the HHSI and LHSI pumps through a common supply header. Water from the supply header enters the LHSI pumps through individual, normally open, motor-operated valves 1-SI-MOV-1862A, and B. Water to the HHSI pumps passes through parallel, normally shut, motor-operated valves 1-CH-MOV-1115B and D. These valves are redundant to ensure that at least one opens on receipt of a safety injection actuation signal or a VCT low level of 5 percent. The supply header then branches

to each of the HHSI pumps through individual, normally open, motor-operated valves 1-CH-MOV-1267A, -1269A, and -1270A.

High head safety injection pumps

The Safety Injection System has three high head safety injection pumps, commonly referred to as "charging pumps." They are located in the charging pump cubicles on the first floor of the Auxiliary Building. During normal operation, at least one pump is operating with the other two lined up for normal charging. When safety injection actuates, all three pumps receive an auto-start signal but only two of the pumps will remain running. The two running pumps will preferentially be powered from different emergency buses to minimize bus loading.

The HHSI pumps are horizontal, eleven-stage, centrifugal pumps. Each pump is designed to pump 150 gpm at 250°F and 2735 psig. Each HHSI pump has a self-contained oil lubrication system. The HHSI pump is driven by a 900 HP, 1800 rpm motor that rotates the pump at 4846 rpm through a speed-increasing gearbox. HHSI pumps 1A and 1C are powered from 4160 V bus 1H. HHSI pump 1B is powered from 4160 V bus 1J. HHSI pump 1C can be used as an alternate pump for either SI train and may be powered alternatively from 4160 V bus 1J. When pump 1C is powered from its alternate source, it has no automatic start features.

To prevent overheating of the HHSI pumps when they are operated at a shutoff head, a mini-flow recirculation line is provided for each pump. The recirculation flow path contains a check valve, an orifice, and an isolation valve MOV-1275A, B, or C. The three mini-flow lines join to form a common header which discharges to the seal water heat exchanger through a common recirculation line isolation valve 1-CH-MOV-1373. The recirculation flow from the seal water heat exchanger is directed back to the suction of the HHSI pumps. During a LOCA, the recirculation line isolation valve is manually shut to maximize HHSI pump flow when RCS pressure decreases below a certain point. The valve is manually reopened if RCS pressure rises above 2000 psig. When RCS pressure is above 2000 psig, the flow through the HHSI pumps is insufficient for pump cooling, and recirculation flow is necessary to prevent pump damage.

The HHSI pumps normally receive water from the VCT through a supply header that contains two series isolation valves MOV-1115C and E. The VCT supply header and the RWST supply header combine into a common HHSI pump suction header. The discharge of LHSI pump 1B can be directed to the HHSI pump supply header through normally shut, isolation valve 1-SI-MOV-1863B. Each HHSI pump is supplied in parallel from the supply header through normally open, isolation valves 1-CH-MOV-1267A, -1269A, and -1270A. LHSI pump 1A can supply each of the HHSI pump suctions through a normally shut, common

isolation valve 1-SI-MOV-1863A and individual, normally open, alternative path isolation valves 1-CH-MOV-1267B, -1269B, and -1270B.

The HHSI pumps can discharge water through individual, normally open, outlet valves 1-CH-MOV-1286A, B, and C. This discharge can pass through a common discharge header isolation valve 1-CH-MOV-1289B to the normal RCS charging header. The discharge from 1-CH-MOV-1286A, B, and C can also be directed through the BIT to the RCS cold legs or to the RCS through normally shut isolation valves 1-SI-MOV-1867C or D, hot legs through a normally shut isolation valve 1-SI-MOV-1869B. The discharge of the HHSI pumps can also be directed through individual, normally open, isolation valves 1-CH-MOV-1287A/B/C to either the RCS cold legs through normally shut, alternate path isolation valve 1-SI-MOV-1836 or the RCS hot legs through normally shut, alternative path isolation valve 1-SI-MOV-1869A.

During normal plant operation, water enters the HHSI pump from the VCT through 1-CH-MOV-1115C and E and through HHSI pump suction valve MOV-1267A, -1269A, or -1270A. The discharge of the HHSI pump passes through the pump discharge valve MOV-1286A/B/C through the RCS charging header isolation valve MOV-1289B, FCV-1122, MOV-1289A, the regenerative heat exchanger, HCV-1310, and into B-Loop cold leg downstream of the accumulator discharge line.

During the injection mode, water from the RWST enters the HHSI pumps through 1-CH-MOV-1115B and D and the pumps suction valves MOV-1267A, -1269A, and -1270A. The discharge of the pumps passes through the pump discharge valves 1-CH-MOV-1286A/B/C to the BIT.

During the recirculation mode, water from LHSI pump 1A enters the HHSI pumps through MOV-1863A and the alternate header via pump suction valves MOV-1267B, -1269B, and -1270B. LHSI pump 1B supplies water through MOV-1863B and the normal header via pump suction valves MOV-1267A, -1269A, and -1270A to the HHSI pumps. During cold leg recirculation, the HHSI pumps discharge through discharge valves 1-CH-MOV-1286A, B, and C and the BIT. Later, one of the HHSI pumps is isolated from the other HHSI pump to provide two independent paths to the RCS. Independent paths provide protection against a long-term passive failure causing a complete loss of core cooling. In the cold leg lineup, one HHSI pump discharges through the alternative discharge valve 1-CH-MOV-1287A, B, or C and MOV-1836. During hot leg recirculation, one HHSI pump discharges through its normal discharge valve and 1-SI-MOV-1869B to the RCS hot legs, while the other HHSI pump discharges through its alternative discharge valve and 1-SI-MOV-1869B to the RCS hot legs.

Low head safety injection pumps

There are two low head safety injection pumps for each unit. The pumps are located in Safeguards Area outside of Containment. During normal plant operations, the LHSI pumps are in standby, lined up to pump borated water from the RWST to the RCS cold legs. On receipt of a safety injection signal, the pumps automatically start and deliver large quantities of borated water to the RCS if RCS pressure is less than discharge pressure, otherwise, they will run on recirculation to the RWST.

Each LHSI pump is a vertical, two-stage, mixed flow enclosed impeller, centrifugal pump. The pump has a capacity of 3000 gpm at a temperature of 300°F and a pressure of 175 psig with a design head of 225 feet. The pump suction is located at the bottom of the safeguards pit at the 210-foot elevation. The pump discharges along the shaft vertically to the 256-foot elevation where the mechanical seals and motor are located. The pump is driven by a 250 HP, 4160 V, induction motor that rotates the pump at 1800 rpm. LHSI pump 1A is powered from 4160 V bus 1H and pump 1B from bus 1J. The pumps are protected from overpressure by relief valves 1-SI-RV-1845A, B, and C that relieve to the Safeguards Area. Their setpoints are 220 psig.

The LHSI pump uses tandem mechanical seals to contain the water within the pump at the point where the shaft protrudes through the discharge head. In the event that the inboard seal fails, the outboard seal is capable of handling the full unit pressure. Seal water flow and cooling is provided water from the RWST. Local flow indication is provided for the combined LHSI pumps seal water supply.

The suction of the LHSI pumps is physically located at the bottom of the safeguards valve pit at elevation 210 feet. Water from the containment sump, in particular, gravity drains into the pump suction pit. The containment sump is only a few feet higher than the LHSI pump suction pits. To provide a full suction for the pumps, each pump is provided with two ejectors to remove air from each pump suction area. The air ejectors use the pump discharge as the high pressure source of water to create a suction on the pump suction space. This not only fills the pump suction bell with water, but also increases the flow of water from the sump to the pump suction pit.

A minimum flow bypass line is provided for each pump to recirculate fluid to the RWST to prevent overheating of the pump while operating at shutoff head and for test purposes. Two motor-operated, isolation valves 1-SI-MOV-1885A & C and 1-SI-MOV-1885B & D are piped in series on the recirculation line for each pump. The recirculation line is automatically isolated when the following conditions are satisfied:

1. SI recirc. mode signal is present (from SI, lock-in relay),

2. RWST level is below 24.9 percent, and

3. Either 1-SI-MOV-1863A or B respectively has opened.

During the recirculation mode, the LHSI pumps take a suction on the containment sump. If the recirculation line isolation valves did not shut radioactive gases from the sump water would be released to the atmosphere through the RWST vent. The valves do not shut until minimal cooling flow is ensured by 1-SI-MOV-1863A or B opening.

The LHSI pumps take a suction on either the RWST or on the containment sump. During normal operations and the injection mode, the LHSI pumps are lined up to receive water from the RWST through motor-operated, isolation valves 1-SI-MOV-1862A and B. During the recirculation mode, these isolation valves are shut and the motor-operated, isolation valves 1-SI-MOV-1860A and B from the containment sump are opened. On receipt of a low-low RWST level, 1-SI-MOV-1860A and B will open automatically if a SI recirc mode signal is present and the respective LHSI pump recirculation valves have shut.

The LHSI pump discharge can be directed to the RCS cold legs, the HHSI pump suction, or the RCS hot legs. During normal plant operations and the injection mode, the discharge of the pumps is lined up to the RCS cold legs through normally open, pump discharge valves 1-SI-MOV-1864A and B and a pair of normally open, isolation valves 1-SI-MOV-1890C and D that are piped in parallel. The motor operators for 1-SI-MOV-1890C and D are normally deenergized with their breakers locked open. On initiation of the recirculation mode, the discharge of the LHSI pumps continues to the RCS cold loops with some portion being directed to the suction of the HHSI pumps through normally shut, isolation valves 1-SI-MOV-1863A and B. This lineup ensures net positive suction head to the HHSI pumps, since water is no longer being provided to the HHSI pumps from the RWST. During the recirculation mode, the discharge of the LHSI pumps is periodically lined up to the RCS hot legs through normally shut, isolation valves 1-SI-MOV-1890A and B. On Unit 1, the outside recirculation pumps 1-RS-P-2A and B can discharge to the LHSI pump discharge headers in the event of failure of one or both of the LHSI pumps. Each outside recirculation pump is normally isolated from the corresponding LHSI pump by a pair of series manual isolation valves. They are operated from outside the safeguards building with a T-handle wrench inserted into the associated remote valve operator (a recessed, square-shaped hole in a round, brass device).

A.7.2 Fault Tree Analysis

The Safety Injection system was modeled as a front line system, providing several safety functions.

D1 - Failure to provide high pressure coolant injection from the RWST using 1/3 HHSI pumps.

D2 - Failure of the Accumulators to inject water into the cold legs. The success criteria for D2 are 2/2 for large LOCA, 2/3 for intermediate LOCA, and 3/3 for core cooling recovery.

D3 - Failure to provide low pressure coolant injection from the RWST using 1/2 LHSI pumps.

Dh - Failure to provide coolant injection flow to the RCS hot legs using 1/2 LHSI pumps in the Containment Sump recirculation mode.

H1 - Failure to provide low head coolant injection from the Containment Sump, using 1/2 LHSI pumps.

H2 - Failure to provide high lead coolant injection from the Containment Sump, using the piggyback recirculation mode.

P - Failure to support feed and bleed cooling by providing 1/3 HHSI pumps injecting from the RWST.

The assumption and notes used to develop the Safety Injection system fault trees are contained in Table A.7-5. The assumptions and notes used to develop the safety injection actuation system fault tree follow.

Safety Injection Fault Tree Modeling Assumptions

1. Variations in boron concentration were not included in the failure analysis. Boron concentration is controlled by Technical Specification to a much narrower range than that required by the PRA. In fact, there are no explicit boron requirements of the accumulators in the PRA. This is because the probability of being out of tolerance enough to have any impact is generally considered (in all past PRA's) to be negligible.

2. Variations in water level and pressure were not considered included in the fault tree model. Water level and pressure are constantly monitored by Technical Specifications. These parameters are annunciated if out of specification.

3. The probability of the discharge valve (1-SI-MOV-1865A/B/C) being inadvertently closed at the time of the initiator was considered negligible in comparison to other faults. The following reasons apply:

   a) failure to be fully open is annunciated

   b) the valve is designed to be fully open or fully closed.

4. The loop selected for the break is not important. All valves receive redundant signals to open.

5. Stroke test interval for 1-SI-MOV-1865A/B/C valves is assumed to be 18 months.

6. Failure of the LHSI pump due to failure of seal cooling was not explicitly modeled. The seal cooling for LHSI pumps is self contained and principally passive. The water level on the seal head tank is constantly monitored and annunciated. Failure of seal cooling is considered to be included in the component boundary of the pump.

7. Failure of bearing cooling to the pump was not explicitly modeled. There is no external cooling supplied for the bearings. As long as the pumped stream is within the design temperature of the pump, the bearing temperatures are considered acceptable. Failure of the bearings for all causes is considered to be within the component boundary of the pump for pump failure, although the accident sequence delineation does not allow the pump to operate if the sump water temperature is over the pump design temperature.

8. Motor heating failures and trace heating failures were not modeled explicitly. The LHSI pumps have no external cooling. All pump failures due to loss of the internal cooling mechanisms are considered within the component boundary of the pump.

9. Misposition errors were not postulated for valves which get an open (or close signal) on an SI.

10. 1-SI-MOV-1890A and B are normally closed and have power removed.

11. Failure of one LHSI pump due to dead-heading when the 885 valves are open, was not postulated. This assumption represents the resolution of NRC concern expressed in Information Notice 87-59. If two pumps share a common recirc line, a slightly higher discharge pressure in one pump could deadhead the other pump. At North Anna, each LHSI pump has a 2 inch minimum flow recirculation line feeding into a 3 inch common header. Due to the quarterly measuring of the

discharge head during the pump test and the 2 to 3 inch pipe size increase, the possibility of having conditions where the NRC concern was applicable was considered negligible. Dead heading of the LHSI pumps due to valve blockage in the minimum flow line or misposition of an 885 valve were explicitly modeled. These faults are considered of much higher probability than the NRC scenario.

12. Containment sump valves 1-SI-MOV-1860A/B were considered to have a flow test frequency of 5 years, although they are never flow tested, only stroked. This assumption provides a plugging failure probability of 2.63E-3, compared to a valve fail to open probability of 1.09E-2.

13. 1-SI-MOV-1864A/B and 1-SI-MOV-1890C/D are flow tested every refueling. 1-SI-MOV-1862A/B are flow tested at 400 gpm every month.

14. As 1-SI-MOV-1863A/B are periodically flow tested, and they are normally closed valves, a plugging failure mode for these valves was not included. The general guideline for the fault tree analysis was that if an active failure mode is postulated for an MOV, there is no reason to include a plugging failure mode also. 1-SI-MOV-1860A/B are the exception to that guideline.

15. Restoration error for 1-QS-38 (Unit 1) and 2-QS-33 (Unit 2) was not postulated, because it is often flowed and under administrative control if it is ever closed. Its position is vicariously verified by every LHSI pump test (PT-57.1). The probability of a restoration error and a valve demand before the next pump test is considered to be small compared to the plugging fault. A plugging fault for 2-QS-33 or 1-QS-38 was postulated with a test interval of three months (PT-57.1).

16. North Anna MAAP analysis shows that the maximum sump water temperature at the time of recirculation, for all transients considered in the IPE, is well within the 250°F design temperature of the pump (which is limited by the graphite bearing assembly).

17. Common cause miscalibration of multiple 1845 relief valves is not modeled.

18. It is assumed that LHSI header pressure will not get high enough in a large LOCA to lift a relief valve.

19. In the event that 1-SI-SV-1845B opens, and the operator diagnoses the event and isolates the valve, equipment failures in the alternate injection paths are not modeled. It is assumed that one hot leg injection path or HHSR path will be available.

20. As the mission time for the injection phase of LHSI is one hour, system failure due to inadvertent opening of a relief valve was not modeled. At 180 gpm, the total flow in one hour would be 10,000 gallons. This is not enough diversion from the RWST to cause insufficient inventory. Nor is it enough to cause flooding of the safeguards area.

21. The cross tie between the recirculation spray system and the LHSI system is not used and was not modeled.

22. Operator action to allow injection through 1-SI-MOV-1836, in the event 1-SI-MOV-1867A/B/C/D fail was included for all initiators. The same operator error probability was used for all initiators.

23. The volume control tank must isolate in order to prevent cavitation of the charging pumps, even if both RWST valves open.

24. Cross tie to the other unit's charging will be modeled in the recovery analysis if necessary. Cross tie requires local operation of two manual valves in the auxiliary building. It is estimated that cross tie will require 20 minutes to accomplish. It is not directed by 1-FR-C.1 as is the case for Surry. The cross tie procedure, 0-AP-48 directs both reactors to be tripped in order to perform the procedure. The time and procedural direction for the set-up of cross tie is not certain at this point in the analysis.

25. One charging pump is running at all times. It was modeled as the 1A pump. The 1B pump is modeled as in standby and on the J Bus, and 1C is modeled as racked into the H bus, and in the "auto-after-stop" condition. In this condition, it will not receive any signals, but can quickly be activated from the control room.

26. Charging pump 1A is dedicated to bus H. Charging pump 1B is dedicated to bus J. Charging pump 1C can be powered from the H or the J bus. H is the normal alignment for Charging pump 1C. There are several interlocks on breaker position to prevent crosstie of the buses through the pump 1C. If pump 1C is on the J bus, it must be running. 1C receives no auto-signals on the J bus. Only one pump can be aligned to the J bus at one time. Two pumps (1A & 1C) can be operating on H at one time (during pump test). If a loss of offsite power occurs during this time, both pumps are tripped off the bus, to prevent the diesel from loading onto a loaded bus.

27. Generally, only 2 Charging pumps will receive an autostart signal. If 1C is on the J bus, then only the 1A pump will receive an autostart. If 1C is on J, then by Administrative procedures, 1C is running.

28. The running pump is not stopped on an SI signal; rather it continues to run.

29. A third pump can be started if another pump fails. In order to have a third pump available, pump 1C must be on H.

30. Two Charging pumps are required by Tech Spec and thus one of the three pumps can theoretically be out of service forever. Two pumps can be out of service for 24 hours. This is handled in the fault tree as follows:

    The A pump is assumed to be running. The B and C pumps are both assigned a term for scheduled maintenance (TM) and unscheduled maintenance (UM). Both frequencies will come from plant specific data. All incidences when two pumps are in maintenance at the same time are lumped together, and this event is applied to both the B and C pumps. All maintenance events involving single pumps are similarly lumped and this event probability is applied to the C pump only. Unavailability due to pump tests are applied to the B and C pumps. Because two pumps can be out of service for up to 24 hours, the combination of pump B in TM and pump C in UM is an allowed cutset.

31. Isolation of charging flow (by closure of 1-CH-MOV-1289A/B) is not necessary for success of HHSI. This is not a flow diversion, as the flow goes to the RCS.

32. Service water to the lube oil coolers (1-CH-E-5A/B/C) and the gear box coolers is required when the Charging pumps are in the SI mode. Although SW has been lost at Surry, for up to 4 hours in the charging mode, with continued pump operation, there is no evidence that the pumps could operate in the SI mode without service water.

33. Because of the piping configuration of the service water supply headers, the requirement of service water to the gear box cooler will also assure supply of service water to the seal coolers, although it is not known if seal coolers are required.

34. HVAC in the charging pump cubicles is assumed not to be required for successful Charging pump operation throughout the 24 hour mission time.

35. Minimum flow lines were ignored for LOCAs and all transients with scram. For these events, RCS pressure is below 2250 psi and thus there will be flow into the RCS, thus negating the need for mini-flow line operation, if the discharge MOV (1286A/B/C) is open.

36. If 1-CH-MOV-1286A/B/C is closed, mini-flow is assumed required to prevent pump dead head and subsequent failure.

37. Monthly testing per 1-PT-14.1, 1-PT-14.2 and 1-PT-14.3 makes the pump unavailable unless the operator takes action to open the discharge valve.

38. MOV test duration per 1-PT-212.1/2/3 or 213.1/2/3 is so short, it was not considered as an impact on system operation.

39. For recirculation from the sump, either LHSI, injecting through either 1-SI-MOV-1863A or B is sufficient to supply flow to two operating charging pumps. Either check valve 1-SI-47 must close or both MOV-1115D and 1115B must close in order to isolate the RWST. The calculation below is used to justify that sufficient hydraulic force is present to close the check valve. If the check valve operates, the head from the LHSI will keep the valve closed and thus, MOV-1115B and MOV-1115D do not have to close.

    Design flow for 1 LHSI pump is 3250 gpm. Runout flow for a Charging pump is 600 gpm. Under piggyback recirc at high RCS pressure, one LHSI pump could supply up to 2050 gpm surplus flow to reseat check valve 1-SI-47 in the event MOV-1115B or MOV-1115D failed to reclose. 1-SI-47 is in an 8" line. Surplus flow of 2050 gpm would result in a back flow of 13.2 ft/sec.

40. The auxiliary oil pump on each Charging Pump was not modeled. The aux. oil pump is constantly running in the standby pumps to circulate the oil. During normal Charging Pump operation, a shaft driven pump provides lubrication. The aux oil pump is needed for initial start, before the shaft driven pump gets up to speed. It was not included for two reasons; either one is sufficient:

    a) Start of the Charging Pump without the aux oil pump, on a one time basis is not damaging, according to the manufacturer. Repeated dry starts would degrade pump life.

    b) Failure of the aux oil pump would be a revealed fault. The probability of an initiator simultaneous with a failed aux oil pump is very low.

41. Failure of trace heating is a revealed fault (through instrumentation) and thus not included in the fault tree.

42. The standby Charging Pump will start upon failure of the running pump on low discharge header pressure. This is a non-SI signal.

43. Resolution of NRC Information Notice 88-23 - "Potential for Gas Binding of SI Pumps" is as follows: HHSI suction piping is periodically vented. Records show a typical gas volume of $.3ft^3$ - $.4ft^3$. This level is consistent and supports the position that the CHPs can tolerate this amount of gas flow through without any pump damage.

44. 1-CH-MOV-1115C/E will not close unless interlocks from limit switches on 1-CH-MOV-1115B/D are satisfied. The limit switches provide more redundancy and reliability than the MOVs. The interlock was therefore not included in the fault tree.

45. RWST failures and suction failures were assumed to fail all pumps by cavitation before operator action could be taken.

46. 1-QS-38 [2-QS-33 for unit 2] is a manual valve on the discharge of the RWST. Its failure represents a single point failure for the HHSI and LHSI system. Three failure modes have been postulated for this valve, plugging, closed for test or maintenance, and failure to restore after maintenance. Each of these are discussed.

    a) Closed for maintenance: No PTs were discovered which require closing of the valve during power operations. Closing of the valve would be on an infrequent, as needed basis to support maintenance activities. The valve could not be closed for more than 4 hours without violating Tech Spec (as it makes both trains of SI unavailable). Therefore, the amount of time the valve could be closed is small and was neglected in the fault tree.

    b) Failure to Restore after maintenance: As the valve could be closed during power operation (for whatever reason), there is a probability that it is inadvertently left closed. The valve is vicariously verified open every three months during LHSI pump test, 1-PT-57.1, which requires recirc flow from the LHSI pumps. For the misposition to cause a system failure, an SI demand would have to occur between the time of valve misposition and the next LHSI pump test (this presumes the valve is closed on a far less frequent basis than 1-PT-57.1 is performed). Assuming 1E-3 for failure to restore, 2E-2 for SI demand per year, and LHSI tests every three months, the probability of a valve misposition and a demand prior to the next pump test is:

    $$(.001 * .02) / 4 = 5E\text{-}6$$

    c) The plugging failure probability for a three month test period is 1.3E-4. Plugging therefore seems to be the dominant failure mode for the valve and was the only one included.

47. Pump trips due to interlocks on the breakers being activated by operator errors were not included in the fault tree. These events are revealed faults and are not present at the time of system demand. Modeling these errors during the mission time are errors of commission and are consequently not modeled.

48. Failures of the lube oil heat exchangers 1-CH-E-5A/B/C are included in the component boundary of the charging pump.

49. Failure of the Boron Injection Tank due to flow obstruction is modeled as a TNK-LF (tank-loss of function) failure.

Safety Actuation Fault Tree Modeling Assumptions

1. Contacts were modeled as part of a relay and not modeled as separate components. For example, a device which starts when a contact is open (energized) will be modeled as a relay which fails to energize. The relay and the contact are actually one component, and there is no significant advantage to separating out the contacts from the relay.

2. SI output signals to MOVs were simplified by only including relays required to actuate the valves to the desired position. Other devices such as limit switches, hand control switches, and torque switches were not included.

3. Modeling of the manual initiation of safety injection and recirculation mode transfer was not included within this fault tree. These human interactions will be included in the SI system fault tree.

4. The SI actuation system has input signals to protect against a LOCA or a Steam Line Break (SLB). All input signals were included within the model. A house event, XHOS-SLB, was included to allow the SI actuation fault tree to be used for LOCA or for SLB initiators. The input signals Related to a SLB were included under an "and" gate with XHOS-SLB. When the house event is equal to 1.0 the SLB signals are allowed to contribute to the SI actuation system unavailability. When the house event is 0.0 then only the LOCA signals contribute to SI system unavailability.

5. Based on a review of SI actuation procedures, SI actuation channels which are bypassed for the purposes of testing are not automatically realigned in the event that SI operation is required.

6. Components for SI actuation train B were generally not shown in system drawings. Train B was drawn in the simplified schematic in a configuration identical to that of Train A.

7. The T_{avg} input signal to SI actuation requires temperature signals from both hot and cold leg RCS temperature transmitters; however, only a single temperature instrument channel was modeled for each pair of hot/cold leg transmitters.

8. Relay K647 is a permissive relay that is energized when SI actuation occurs and must be energized for the initiation of recirculation mode (i.e., it is assumed that K647 must be energized in conjunction with K630).

9. Failure of the SI actuation reset permissives were not modeled as they had been in the Surry model for the steamline break portion of the SI actuation system. North Anna has several different reset permissives installed for the various inputs which cause SI actuation. Due to the numerous possible inputs which can lead to SI actuation, failure of more than one reset permissive would be necessary, and this contribution to system unavailability is assumed to be insignificant.

10. SI actuation lock-in relays (discussed in the reactor protection systems training manual) are not modeled. Failure of these relays would be revealed immediately and prompt operator action is highly probable.

11. No periodic tests specific to the logic which transfers SI to recirculation mode were identified. It is assumed that this logic is tested with one train operable and one in trip.

12. Common Cause Failure of instrument lines has been modeled where appropriate. The basic events are listed below:

1RCTIC-CC-TAVG	CCF of 2/3 Tavg channels
1RCPIC-CC-PRSZRP	CCF of 2/3 Pressurizer pressure channels
1MSPIC-CC-STMDPR	CCF of 2/3 Main Steam line pressure channels
1LMPIC-CC-100	CCF of 2 of 3 containment pressure instrument channels
1MSFIC-CC-MSFLOW	Steam line flow instrument channels
1MSPIC-CC-MSLP	CCF of 2 of 3 steam line pressure instrument channels
1SILIC-CC-RWST	RWST Level Instrument Channel common cause failure - 2/4 channels

two AOVs work together to control the cooldown rate of the RCS. The discharge of the flow control valves feeds into the SI/Accumulator piping and is delivered to the RCS loop 2 and loop 3 cold legs. Each path has a normally shut MOV isolating the RHR from the high pressure RCS during normal plant operations. Makeup to the RHR System is provided by the RCS.

The RHR is manually initiated. An interlock prevents opening the Hot Leg RHR isolation MOVs until RCS pressure is below 450 psig. Only one RHR pump and heat exchanger are required for plant cooldown although both pumps and heat exchangers are normally used immediately following a reactor shutdown, to provide a faster cooldown. Following a loss of offsite power, the stub buses powering the RHR pumps are shed from the emergency buses and must be manually reconnected to restore power to the RHR pumps.

The RHR System is dependent on AC power for motive power for the pumps, and the DC buses for control power to the RHR pumps and the heat exchanger throttle valves. Additionally, the RHR System requires the Instrument Air system for motive power to the heat exchanger throttle valves. The RHR System is dependent on the RCS water level to avoid air binding of the pumps.

Prior to placing the RHR System in service, RCS pressure must be below 450 psig and RCS temperature must be below 350°F. Following a loss of offsite power, the stub buses which power the RHR pumps are automatically shed and must be normally reloaded as the main bus by the operator to restore power to the pumps.

3.2.19.2 RHR System Logic Model

The success criterion for the Surry RHR System requires RHR flow to be provided from one of two pumps through one of two heat exchangers to the RCS following reactor shutdown and cooldown to 450 psig, 350°F. This criterion translates into the following top event in the RHR System fault tree:

- Failure to provide cooled RHR flow to the RCS.

3.2.20 Safety Injection Actuation System Model

The Solid Station Protection System (SSPS, SI actuation system) automatically initiates the Safety Injection Systems, following an indication of the need for primary coolant makeup, and automatically initiates the switchover of the suction of the low pressure injection pumps from the Refueling Water Storage Tank (RWST) to the Containment sump and the switchover of the suction of the high pressure injection pumps from the RWST to the low pressure injection pump discharge upon low RWST level.

3.2.20.1 SSPS Description

The North Anna SSPS is composed of two independent trains used to automatically actuate the low and high pressure injection systems and the motor driven AFW Pumps.

The portion of the SSPS which supports recirculation is composed of four independent RWST level sensors, each feeding two separate two out of four relay matrices. These two relay matrices automatically actuate the components required to perform the switchover to the recirculation mode of the low and high pressure systems. The SSPS is dependent on the AC vital instrumentation buses and the DC buses for operation of the relay logic network.

3.2.20.2 SSPS Logic Model

The SSPS was modeled as a support system to be linked into the components which are activated by the SI signals.

3.2.21 Service Water System

The Service Water System is common to both reactor units and is designed for the simultaneous operation of various subsystems and components of both units. SW System provides long term cooling after a loss of coolant accident (LOCA) and supplies cooling water to the following safety-related components during normal plant operations:

1. Component Cooling (CC) heat exchangers;
2. Recirculation Spray (RS) heat exchangers;
3. Control Room/ESGR air conditioning chiller condensers;
4. charging pump seal coolers, gear reducers, lube oil coolers; and
5. Instrument Air compressors.

The SW System also serves as a backup source of water to the Auxiliary Feedwater System.

The sources of cooling water for the SW System are the SW reservoir and Lake Anna. These two, independent sources of water form the ultimate heat sink for the North Anna Power Station.

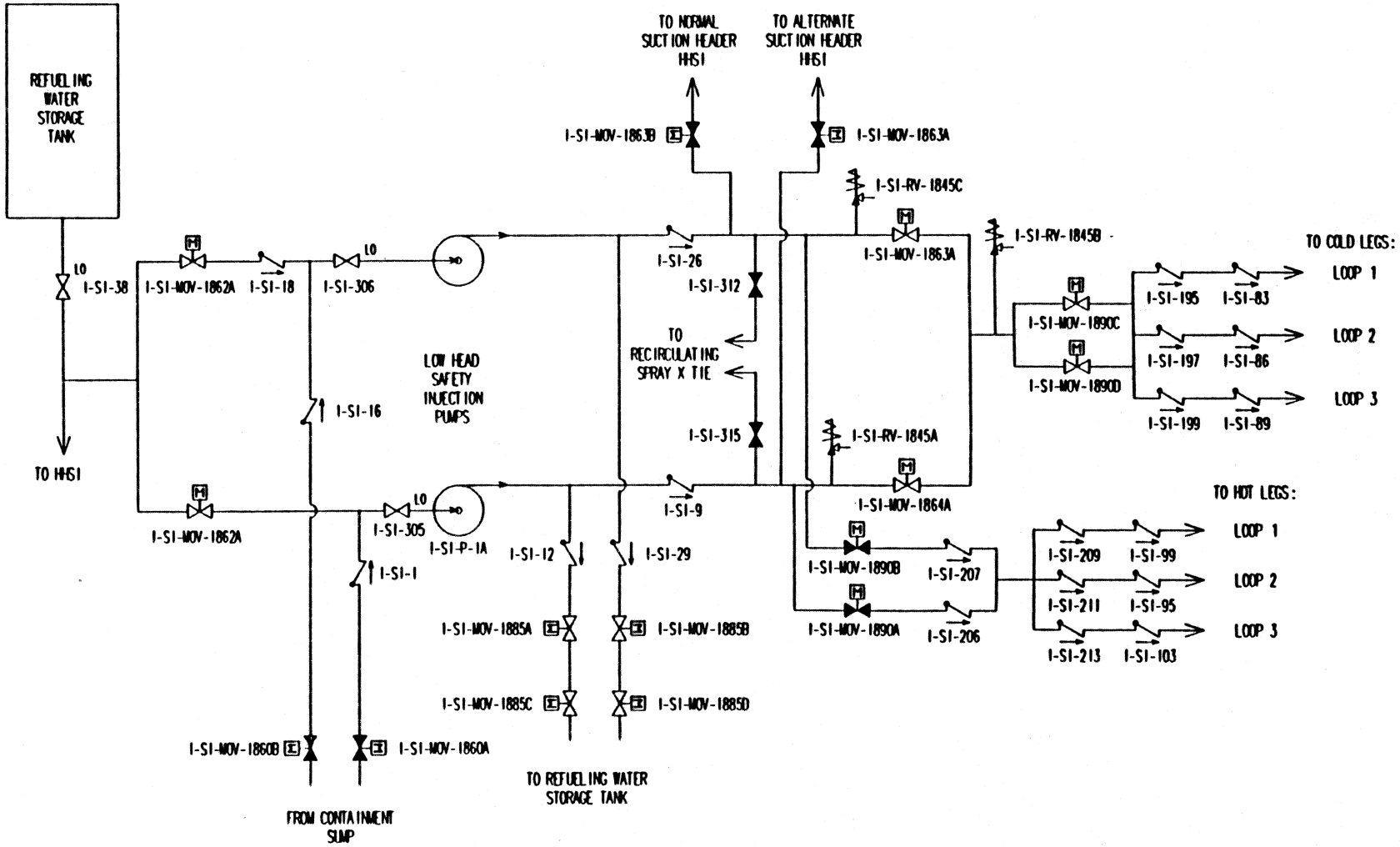


FIGURE A.7-1
LOW HEAD SAFETY INJECTION

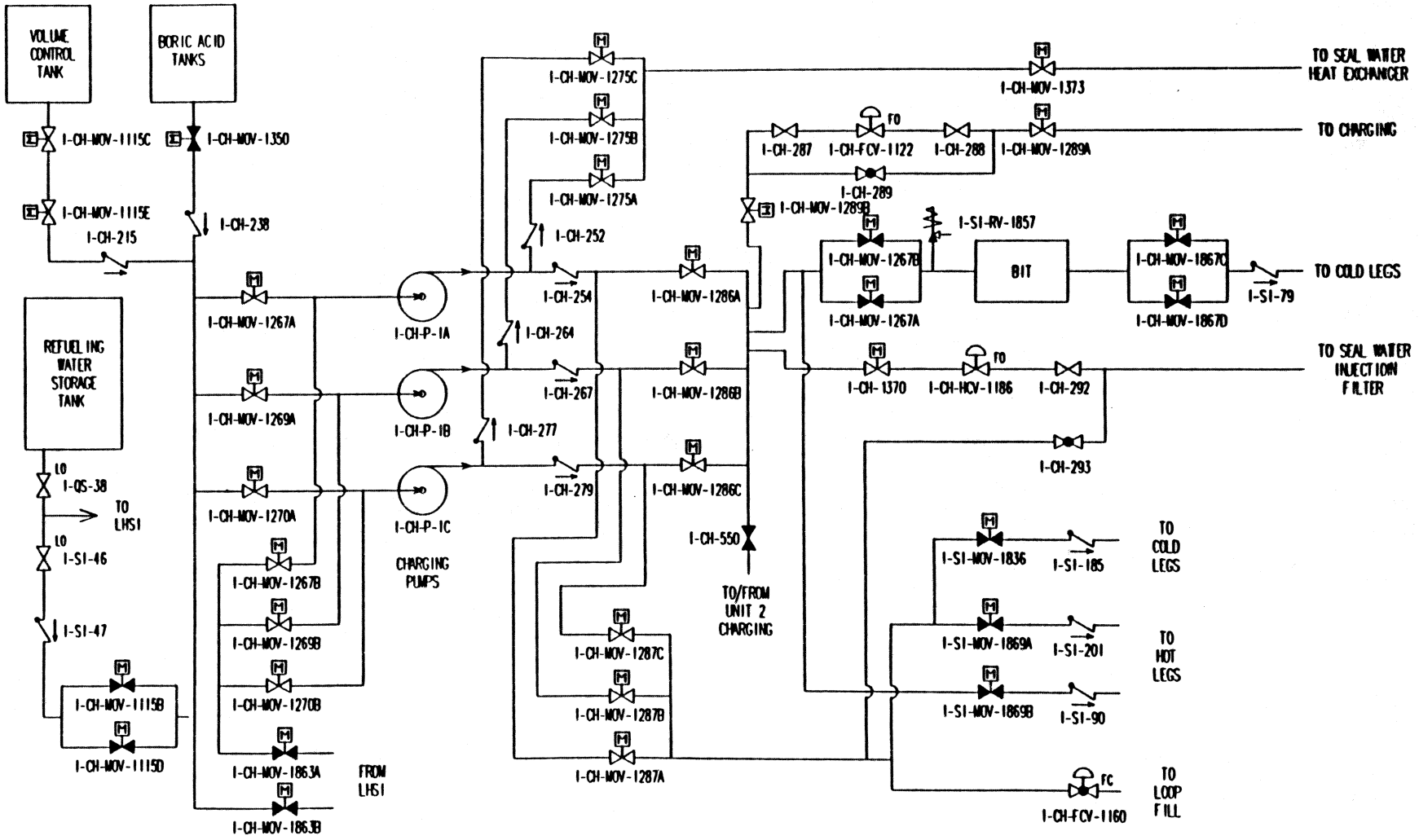


FIGURE A.7-2
HIGH HEAD SAFETY INJECTION

TABLE A.7-4 (Continued)
SAFETY INJECTION ACTUATION DEPENDENCY MATRIX

COMPONENT	MOTIVE FORCE	CONTROL POWER	AUTO ACTUATION	COMPONENT COOLING	ROOM COOLING	INTERLOCKS
1-MS-PT-1496 Main Steamline Pressure	None	120 VAC Vital Bus 1-IV 1-EP-CB-4D	None	None		
RMT Logic & Output Relays Train A	None	120 VAC Vital Bus 1-I 1-EP-CB-4A	RMT Input Signals Train A	None	Emergency Switchgear Room Cooling	
RMT Logic & Output Relays Train B	None	120 VAC Vital Bus 1-III 1-EP-CB-4C	RMT Input Signals Train B	None	Emergency Switchgear Room Cooling	
1-LM-PM-100A RWST Level	None	120 VAC Vital Bus 1-I 1-EP-CB-4A	None	None		
1-LM-PM-100B RWST Level	None	120 VAC Vital Bus 1-II 1-EP-CB-4B	None	None		
1-LM-PM-100C RWST Level	None	120 VAC Vital Bus 1-III 1-EP-CB-4C	None	None		
1-LM-PM-100D RWST Level	None	120 VAC Vital Bus 1-IV 1-EP-CB-4D	None	None		

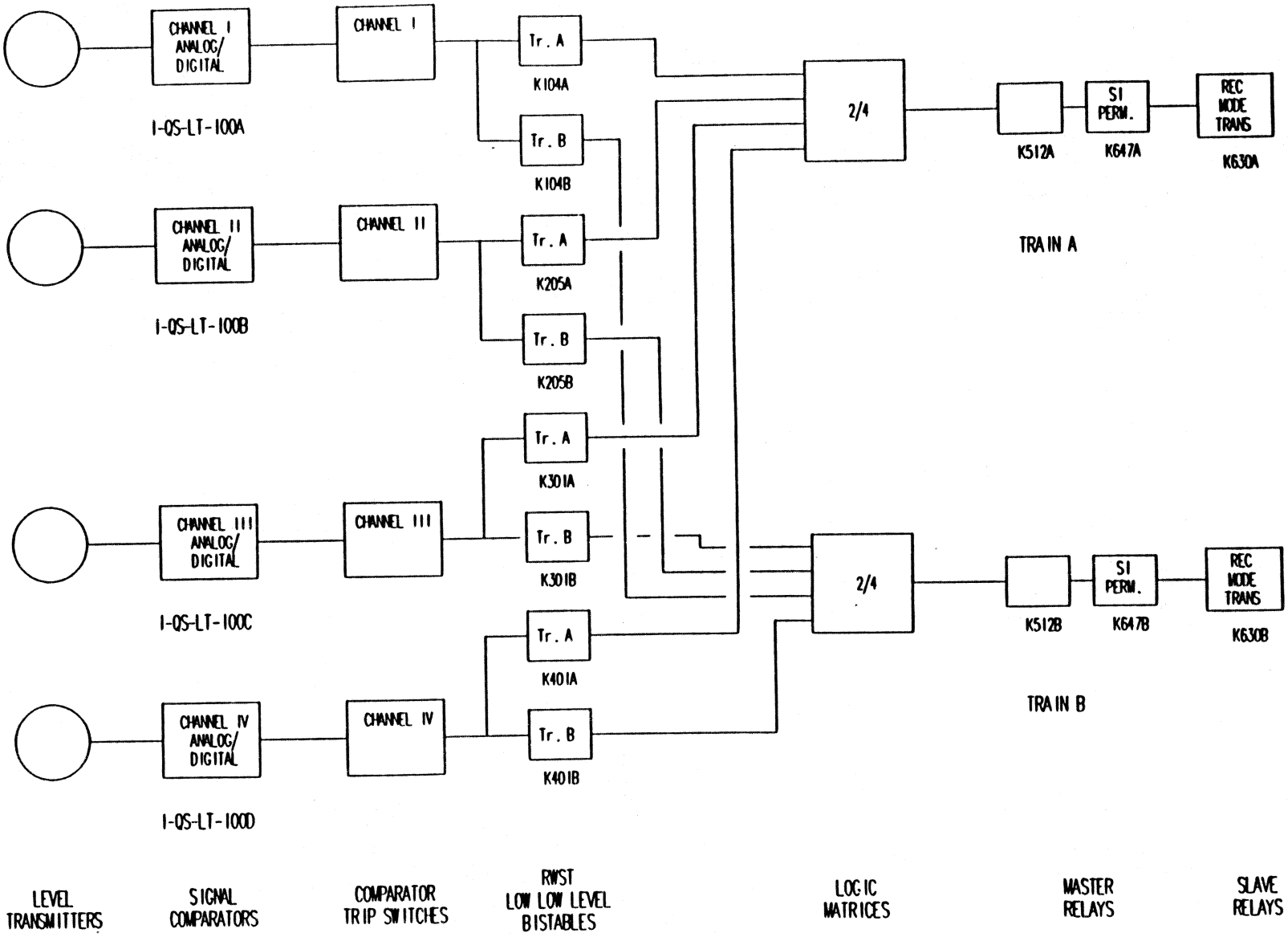
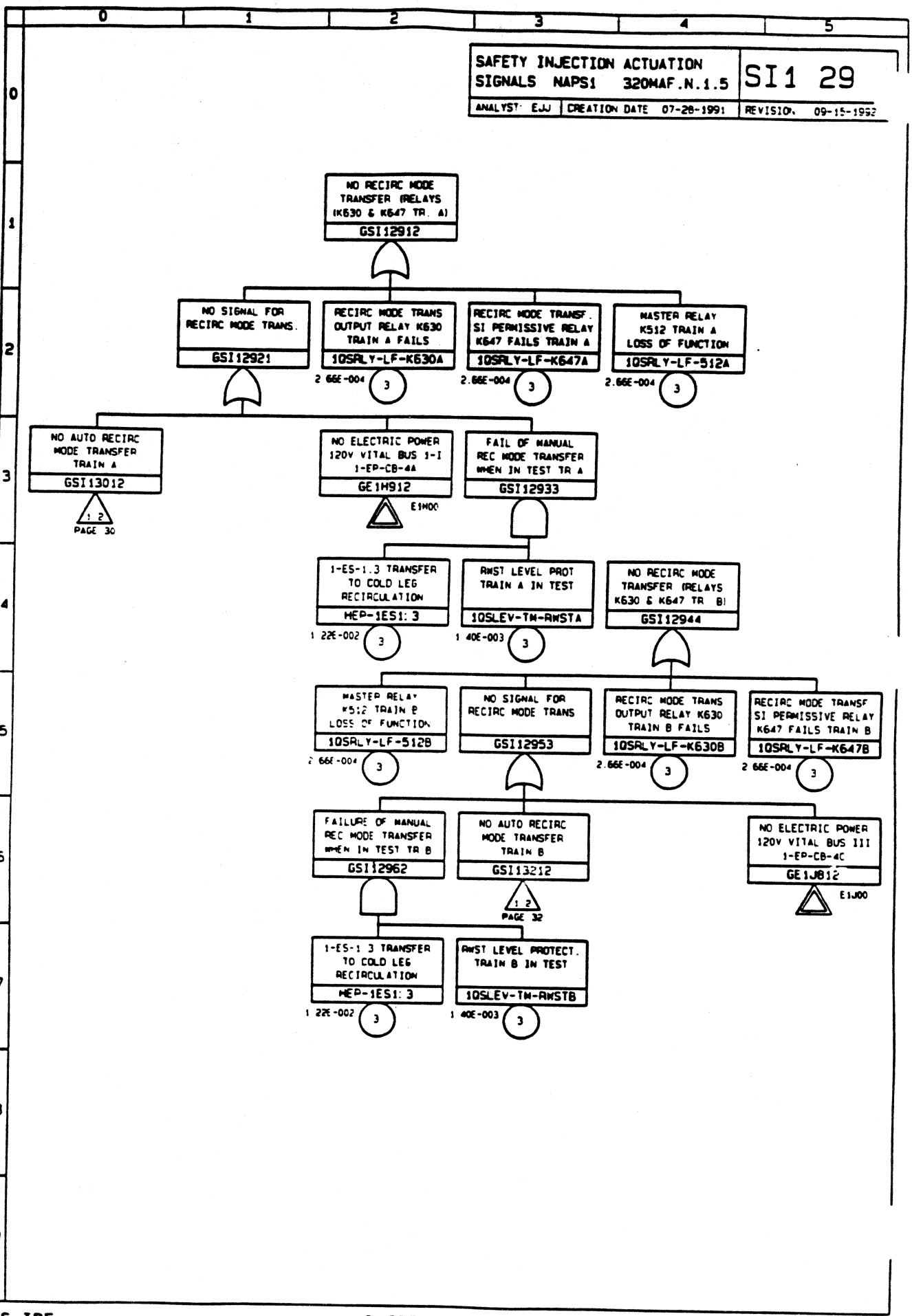
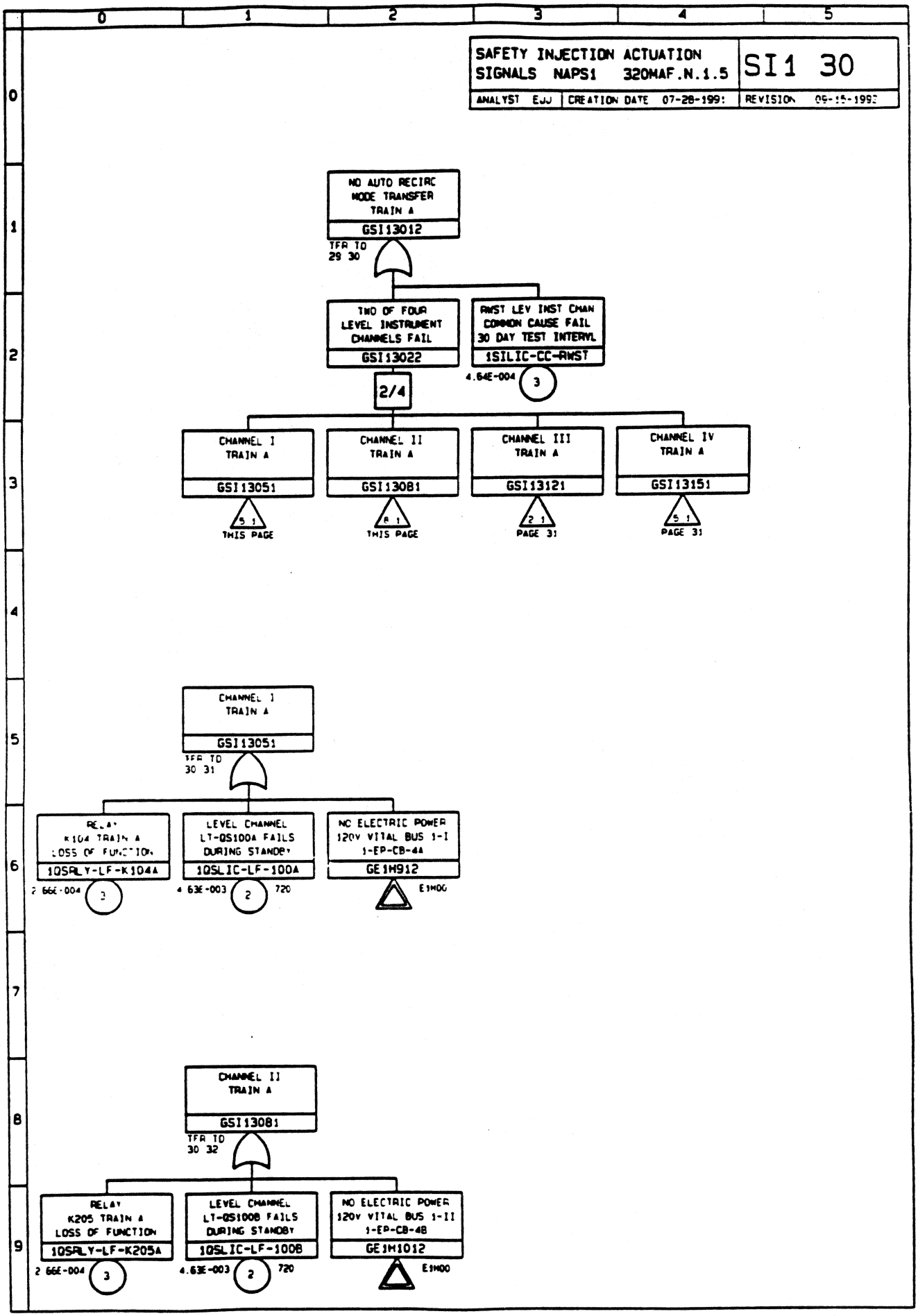


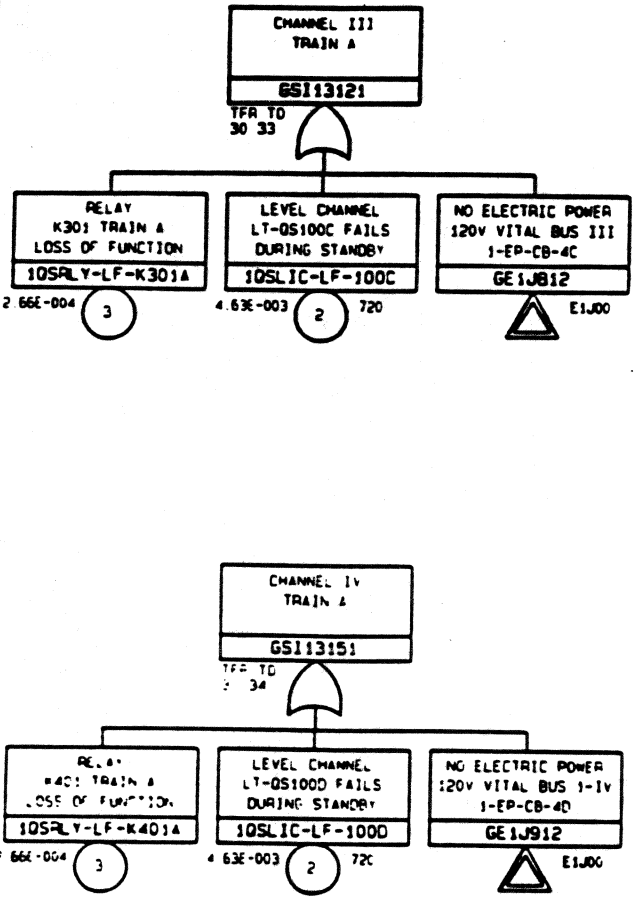
FIGURE A.7-4
RECIRCULATION MODE TRANSFER


SAFETY INJECTION ACTUATION SIGNALS NAPS1 320MAF.N.1.5
SI1 29
ANALYST: EJJ
CREATION DATE 07-28-1991
REVISION 09-15-1992
NO RECIRC MODE TRANSFER (RELAYS K630 & K647 TR. A)
GSI12912
NO SIGNAL FOR RECIRC MODE TRANS.
GSI12921
RECIRC MODE TRANS OUTPUT RELAY K630 TRAIN A FAILS
10SRLY-LF-K630A
2.66E-004
3
RECIRC MODE TRANSF. SI PERMISSIVE RELAY K647 FAILS TRAIN A
10SRLY-LF-K647A
2.66E-004
3
MASTER RELAY K512 TRAIN A LOSS OF FUNCTION
10SRLY-LF-512A
2.66E-004
3
NO AUTO RECIRC MODE TRANSFER TRAIN A
GSI13012
1 2
PAGE 30
NO ELECTRIC POWER 120V VITAL BUS 1-I 1-EP-CB-4A
GE1H912
E1H00
FAIL OF MANUAL REC MODE TRANSFER WHEN IN TEST TR A
GSI12933
1-ES-1.3 TRANSFER TO COLD LEG RECIRCULATION
HEP-1ES1: 3
1.22E-002
3
RWST LEVEL PROT TRAIN A IN TEST
10SLEV-TM-RWSTA
1.40E-003
3
NO RECIRC MODE TRANSFER (RELAYS K630 & K647 TR B)
GSI12944
MASTER RELAY K512 TRAIN B LOSS OF FUNCTION
10SRLY-LF-512B
2.66E-004
3
NO SIGNAL FOR RECIRC MODE TRANS
GSI12953
RECIRC MODE TRANS OUTPUT RELAY K630 TRAIN B FAILS
10SRLY-LF-K630B
2.66E-004
3
RECIRC MODE TRANSF SI PERMISSIVE RELAY K647 FAILS TRAIN B
10SRLY-LF-K647B
2.66E-004
3
FAILURE OF MANUAL REC MODE TRANSFER WHEN IN TEST TR B
GSI12962
NO AUTO RECIRC MODE TRANSFER TRAIN B
GSI13212
1 2
PAGE 32
NO ELECTRIC POWER 120V VITAL BUS III 1-EP-CB-4C
GE1J812
E1J00
1-ES-1.3 TRANSFER TO COLD LEG RECIRCULATION
HEP-1ES1: 3
1.22E-002
3
RWST LEVEL PROTECT. TRAIN B IN TEST
10SLEV-TM-RWSTB
1.40E-003
3
SI100 LGC NUPRA 2.0 VPWR

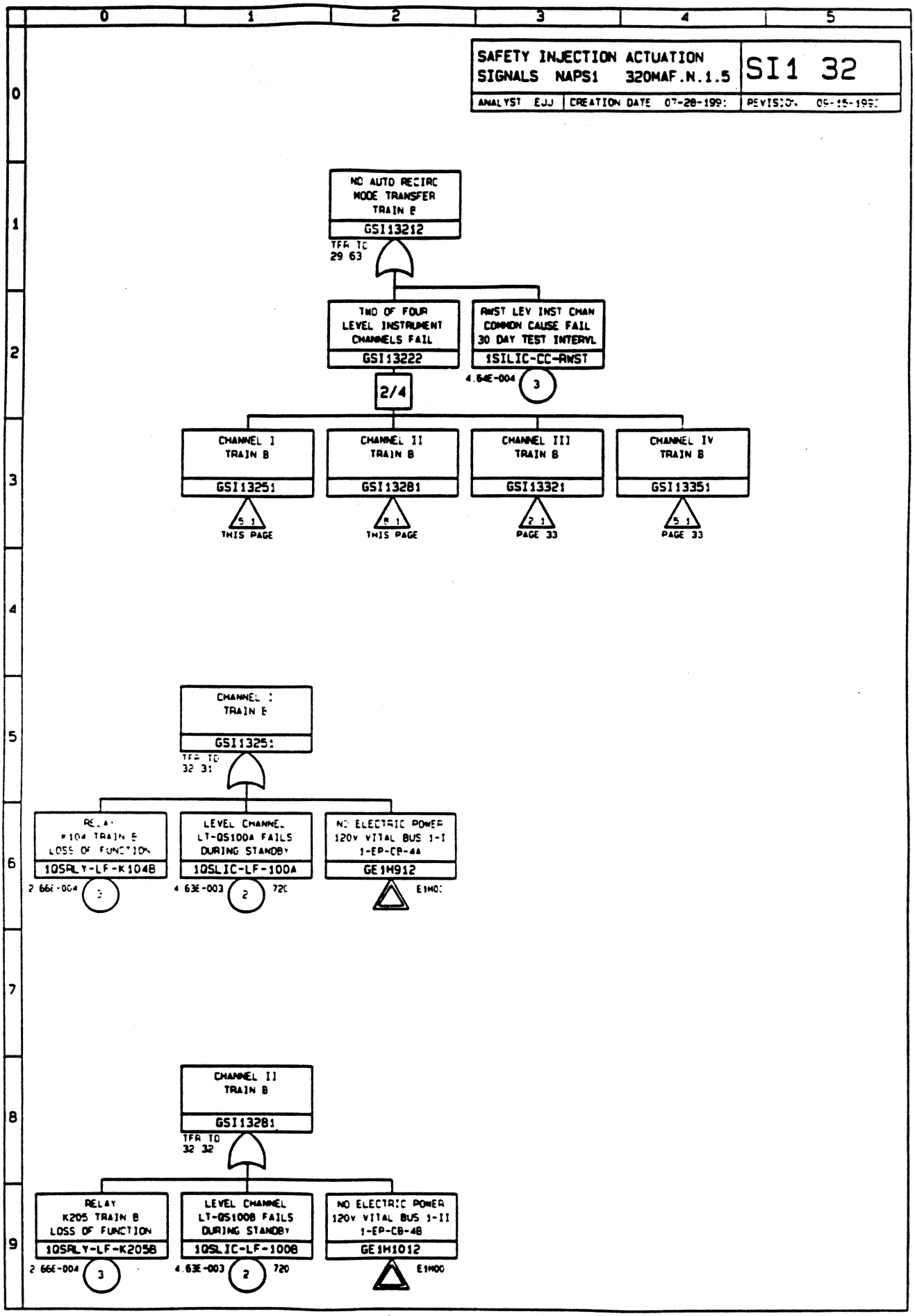


S1100 LGC NUPRA 2 0 VPWR

SAFETY INJECTION ACTUATION SIGNALS NAPS1 320MAF.N.1.5		SI1 31
ANALYST EJJ	CREATION DATE 07-28-1991	REVISION 09-15-19



S1100 LGC MAPAI 2.0 VAX


SAFETY INJECTION ACTUATION SIGNALS NAPS1 320MAF.N.1.5
SI1 32
ANALYST EJJ
CREATION DATE 07-28-199:
REVISION 09-15-199:
NO AUTO RECIRC MODE TRANSFER TRAIN B
GSI13212
TFR TO 29 63
TWO OF FOUR LEVEL INSTRUMENT CHANNELS FAIL
GSI13222
RWST LEV INST CHAN COMMON CAUSE FAIL 30 DAY TEST INTERVL
1SILIC-CC-RWST
4.64E-004
3
2/4
CHANNEL I TRAIN B
GSI13251
CHANNEL II TRAIN B
GSI13281
CHANNEL III TRAIN B
GSI13321
CHANNEL IV TRAIN B
GSI13351
5 1
THIS PAGE
2 1
THIS PAGE
2 1
PAGE 33
5 1
PAGE 33
CHANNEL I TRAIN B
GSI13251
TFR TO 32 31
RELAY K104 TRAIN B LOSS OF FUNCTION
1QSRLY-LF-K104B
2 66E-004
3
LEVEL CHANNEL LT-QS100A FAILS DURING STANDBY
1QSLIC-LF-100A
4 63E-003
2
720
NO ELECTRIC POWER 120V VITAL BUS 1-I 1-EP-CB-4A
GE1M912
E1M00
CHANNEL II TRAIN B
GSI13281
TFR TO 32 32
RELAY K205 TRAIN B LOSS OF FUNCTION
1QSRLY-LF-K205B
2 66E-004
3
LEVEL CHANNEL LT-QS100B FAILS DURING STANDBY
1QSLIC-LF-100B
4.63E-003
2
720
NO ELECTRIC POWER 120V VITAL BUS 1-II 1-EP-CB-4B
GE1M1012
E1M00
S1100 LGC MUFRA 2 0 VPWR

SAFETY INJECTION ACTUATION SIGNALS NAPS1 320MAF.N.1.5	SI1 33
ANALYST EJJ	CREATION DATE 07-28-1991	REVISION 09-15-19