Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies
NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2010)

LESSONS FROM FORSMARK ELECTRICAL EVENT

Thomas Koshy
Chief, Mechanical & Electrical Branch
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission
Thomas.Koshy@nrc.gov

ABSTRACT

The electrical event at Forsmark nuclear station revealed several design and operational oversights that could lead to significant challenges to nuclear safety. The author was a member of the international task group that studied the lessons learned from this event and published "Defense in Depth of Electrical Systems and Grid Interaction" and he shares practical approaches to resolving each of the issues along with selected excerpts from the published report.

The Forsmark incident involved a short circuit in the electrical 400kV switchyard away from the nuclear plant that disabled half of the emergency core cooling systems and half of the information systems in the control room. The half of the systems that survived the electrical transient was also susceptible to the same failure mode. The review of the event identified several electrical vulnerabilities and design weaknesses that have applicability to many electrical power system designs for nuclear stations worldwide. To ensure the defense in depth of electrical safety systems, the following design reviews/or modifications and administrative programs are recommended:

- Evaluate the capability of the onsite electrical system to withstand the range of voltage and frequency fluctuations transmitted through the grid.
- Address islanding/house load operation and its susceptibility to overvoltage excursions.
- Evaluate the suitability of logic/control system failure mode resulting from uninterruptible power supply failure in instrument channels and/or divisions.
- Evaluate the diversity in core cooling systems following loss of all AC power onsite.
- Implement an online contingency assessment program on the transmission system to ensure capability of the offsite power system to provide preferred power for nuclear safety.
- Implement a coordinated maintenance program between the nuclear power plant and the transmission system operator for reducing nuclear safety risk.

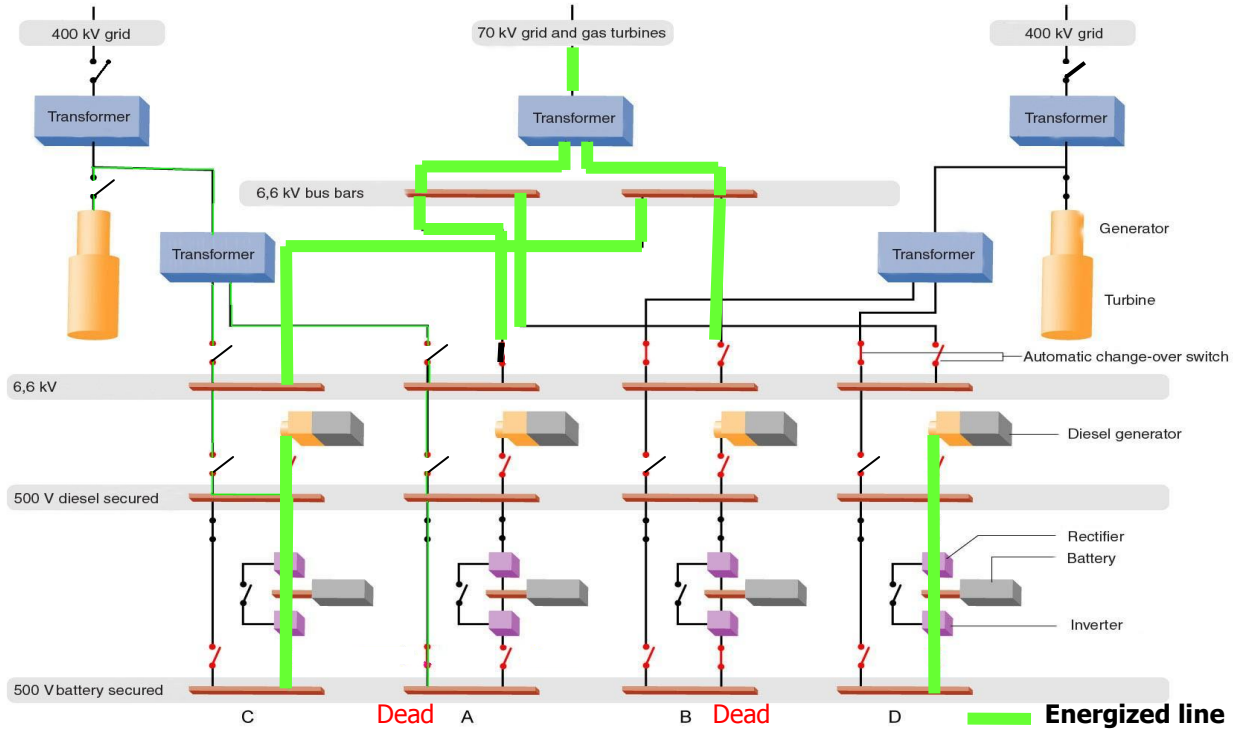
Key Words: Electrical risk, uninterruptible power system, defense in depth, Failure Mode

1 INTRODUCTION

The electrical event at Forsmark nuclear station revealed several design and operational oversights that could lead to significant challenges to nuclear safety. The author, who participated in the international lessons learned task group, identifies the significant issues and provides practical approaches to consider for resolving each of the issues along with the selected excerpts from the international lessons learned report.

The Forsmark Unit 1, a 1,010 megawatt (MWe), 2928MW thermal boiling-water reactor (BWR) plant, located in Sweden, designed by ASEA Atom with two turbine generators was commissioned in 1980. Its principal safety design is four trains with each train sized for 50 percent Emergency Core Cooling System (ECCS) capacity. Any two of the trains provide adequate core cooling for a design basis event. The unit at the time of the event (July 25, 2006) was operating at full power. Unit #2 was connected to the same switchyard and was shutdown during the event. See Fig. 1 for the simplified electrical alignment following the event.

The event, which involved a short circuit in the 400 kilovolt (kV) switchyard just outside the plant area, was the result of a maintenance error. The short circuit at the switchyard caused a grid voltage perturbation resulting in momentary depression of the system voltage and the voltage regulator on the main generator responded to restore the system voltage. The backup protection system disconnected the plant from the grid and the control system aligned the full output of the main generator to supply power to the house loads. At the instant of switching to house load operation, the high voltage output of the generator resulted in a brief but significant overvoltage on the power station's internal electrical network of redundant Essential Power Supply (EPS)—divisions A, B, C and D. Each of the four divisions of the EPS contains an uninterruptable power supply (UPS) system to power the instrument buses at the 500V battery-secured AC bus. The short circuit at the switchyard caused the grid voltage to come down, and the delay in clearing the electrical fault caused the main generator voltage regulator to demand maximum voltage output to correct the voltage drop. When the backup protection system disconnected the plant from the grid, the control system aligned the full output of the main generator to supply power to the house loads. At the instant of switching to house load operation, the maximum voltage output of the generator was experienced by the onsite power system until the voltage regulator reduced the voltage down to a normal rating. The reactor core remained cooled throughout the event.



diesel generators (A & B) to fail to load. See Figure 1. The two UPSs that did not fail were also susceptible for the same failures but survived the voltage spike serendipitously. If all four UPSs had failed, this could have led to a total blackout for the onsite control system. The diesel generators depended on the associated 500V battery-secured power supply for verifying the frequency before the breaker would close to energize the 500V diesel-secured bus. As a result, two trains of power became

fully de-energized at both levels of 500V buses. An unrelated failure in the engine start circuit prevented the backup gas turbines from starting. Two trains of power supply remained unavailable for 22 minutes until they were energized through the alternate feed. A logic deficiency caused the relief valves to stay open when two trains lost power and reduced the rate of core cooling available from the operating channels.

2 LESSONS

2.1 Electrical System Capability to Withstand Voltage and Frequency Fluctuations

During the event, the delay in clearing the electrical fault caused the main generator voltage regulator to demand maximum voltage output to correct the voltage drop. When the backup protection system disconnected the plant from the grid, the control system aligned the full output of the main generator to supply power to the house loads. At the instant of switching to house-load operation, the maximum voltage output of the generator was experienced by the onsite power system until the voltage regulator reduced the voltage down to a normal rating. The overvoltage spike caused by the loss of load on the generator induced a 30-percent voltage rise on the onsite electrical system and failed half of the electrical power system. The typical system and component design is intended to withstand 10 percent over voltage and 10 percent under voltage. These conventional limits may be inadequate for components that are relied on for nuclear safety. Following the deregulation, the electric utilities have split up into separate companies for generation, transmission, and distribution. This separation of companies with legal restrictions on market-related communication has made the utilities even more reluctant to entertain each other's preferences. The US grid regulators have made legal provisions to share adequate information with nuclear stations on grid reliability related information.

Certain regulatory provisions are essential for communicating information necessary for nuclear safety decisions on design, operation, and maintenance. The nuclear station needs to assess the historic record on voltage excursions caused by electrical transients (from transmission network switching actions, generator malfunctions etc.,) and to simulate worst-case scenarios through appropriate modeling techniques to identify the required voltage and frequency protection. Because most of the overvoltages from generator control system failure and switching surges cannot be fully suppressed, an acceptable solution has to match protection and withstand capability with a suitable overlap to ensure the integrity of the safety systems.

2.2 House Load Operation and Overvoltage Transients

Current operating U.S. nuclear stations are designed to trip the reactor on loss of load when the main generator breakers disconnect from the grid and not to revert to house load (islanding) operation. One of the European reactors experienced overvoltage higher than 150 percent as the result of exciter and voltage regulator failure.

In cases where the plant is designed for islanding, the following improvements can be considered for protecting the safety systems. One European regulator has decided to block the house load operation when any fault signals are present in the switchyard. Another approach to solve this problem would be to reduce reactor power in response to a grid disturbance to about 15 to 5 percent (based on the condenser size), transfer plant safety and non-safety loads to offsite power, and continue to dump the steam to the condenser until the grid connection can be reestablished. This approach retains the benefit of resuming full power operation without additional delays and prevents over voltage conditions to the onsite power system. In addition, any of the following operations would significantly mitigate over voltage exposure to onsite safety systems:

- Design a fast-response protection system to prevent the impact of overvoltage to UPS and other safety systems.
- Design UPSs and the downstream control systems to withstand worst-case voltage.
- Interrupt AC power to UPS until fault transients have cleared.
- Isolate the safety system power supplies through a reliable isolation mechanism similar to a motor-generator set.

2.3 Suitability of Logic/Control System Failure Modes

One of the problems identified in the Forsmark event was an undesirable failure-mode-of-logic system that opened relief valves when two of the UPSs failed. This condition increased the duration of reactor coolant system level recovery.

The conventional design principles limit failure-mode analysis to single failures and, therefore, the loss of two trains of the four battery-backed AC instrument bus trains was not considered into the Forsmark design bases. During the event, two UPSs and the respective instrument buses were de-energized. The logic system reverted to the loss-of-power mode (failure mode) due to the de-energized process control system and commanded a relief valve to go open along with two other safety relief valves. This failure mode was undesirable because it reduced the rate of reactor coolant system level recovery while the emergency core cooling system from the two operational trains was injecting water to cool down the reactor core. In addition, the time needed to recover reactor coolant system level significantly increased when the remaining two trains were energized and operational within 22 minutes following the event.

The design basis generally considers single failure as a requirement in safety-related systems. In addition to single failure, common-cause failures such as loss of redundant electrical buses should be considered to ensure that the failure mode does not introduce any unacceptable conditions that challenge nuclear safety. The following discussion will address the details of design precautions and techniques to avoid undesirable failure modes. The discussion and the diagrams are based on two-out-of-three logic for simplification. Figures 2 and 3 demonstrate an acceptable approach to avoid an undesirable failure mode in a reactor protection system and core cooling system. Figure 4 demonstrates an acceptable approach for addressing the failure modes in DC control systems.

To achieve defense-in-depth for control systems, the concept of “fail-safe” is generally accepted as the design principle for critical applications where safety is the primary objective. However, the level of analysis for ensuring the fail-safe conditions varies in different plant designs. A component-level analysis followed by combinations of components that have interdependent failures or consequences followed by a system-level analysis would be the recommended approach to confirm the adequacy of reliable control-system performance.

In the nuclear industry, reactor trip systems are generally designed to be fail-safe. The concept extends to all the supporting safety systems that are essential for operating the reactor at power. The critical support systems associated with reactor trip are DC power, vital AC power (supplied by the UPS), and pressurized pneumatic or hydraulic equipment operation. The design should consider the loss or any conditions outside the operating band of any of these critical support systems to constitute a condition to trip the reactor. To avoid spurious reactor trip challenges from isolated instrument failures and malfunctions, the validity of any trip condition could be processed through a logic system that considers two-out-of-three, two-out-of-four, or other suitable logic to validate actual trip conditions. The logic should be designed with provisions to avoid any common mode failures that could fail to initiate a reactor trip on a valid demand.

2.4. Diversity in Core Cooling Systems and Control System Power

The electrical event caused half of the emergency core cooling systems to be unavailable, and the remaining half had the same susceptibility but operated serendipitously. Had the event spread to all trains of equipment, core cooling would have been delayed until power recovery. All control systems were powered through UPSs, and a common-mode UPS failure consequently leads to total loss of control power. It must be recognized that redundancy with identical systems only provides robustness against the possibility of random failures. It provides little or no protection against common-cause failures (e.g., undersized cables, design, manufacturing or installation errors, maintenance errors, etc.).

An approach to deal with common-cause failure problems is to provide diversity. The loss of all AC power at a nuclear station may appear to be extremely rare, but it has happened at certain stations as a result of hurricanes, dust storms, etc. Steam-driven or diesel-engine-driven cooling pumps with a DC battery power for the control system for core cooling could mitigate the effects of a total loss of onsite AC. The U.S. Nuclear Regulatory Commission (NRC) regulation on station blackout 10 CFR 50.63 requires the U.S. design to have coping capability to withstand a station AC blackout, or an alternate AC source independent of the onsite and electrical-grid-supplied AC sources. The new reactor designs are required to have an alternate AC source.

2.5 "On-Line-Contingency Assessment" Program on the Transmission System

The switchyard event was a single contingency that resulted in a plant trip, loss of offsite power, and would have potentially impacted Unit #2 had it been operating. Such significant contingencies should have been evaluated by the nuclear station and grid operators with independent verification to avoid common errors.

To encourage competition and produce competitive pricing in production of electricity, certain countries and regions of United States have deregulated the energy sector. Electrical power, the most flexible energy source, has now become a commercial product with continuously variable prices based on supply and demand. The duly-licensed power marketers in the respective countries enter into contractual agreements to generate or distribute for very short terms as low as hours and long-term contracts into several months for bulk power. The power producers now have the opportunity to sell their uncommitted power to any locations in the market area where it is more profitable. Such hourly changes in markets modify the power-flow pattern based upon market decisions and, consequently, the offsite power voltage and capacity available to the nuclear station. The extremes of market-driven power trading may not be global at this time; however, the expected benefits for the average consumer are providing a strong momentum for deregulation to spread around the globe. The availability and reliability of offsite power has changed in the US over the last decade. The preferred sources of offsite power with an acceptable operating range and high reliability are available at a premium to the nuclear plant operator with a binding contract and technical verification process.

In the current economic environment in spot pricing and power trading, the reliable power to the nuclear stations could become a second priority because of the ever-changing profile of power flow. To promptly address such variations and to preserve robustness, interactive software with a backup should be continuously run by the transmission system operators to analyze grid contingencies and to implement remedial actions through manual and automatic actions based on the emergency nature of the problem. The transmission authority should have legal authority to remove grid loads and to demand power generation from standby units to maintain the stability of the grid and to provide preferred power to nuclear stations. The US electrical grid regulators have mandated regulations to grant sufficient authority

to the grid operators to take necessary actions to ensure the stability of the grid and provide preferred power supply for the nuclear stations. See Ref. 3 for the nuclear regulatory bases.

2.6 Coordinated Maintenance Program between Plant and Transmission System

The Forsmark electrical event began with a maintenance error. A maintenance error on the transmission and distribution system is a primary cause for unanticipated outages. To maintain a high reliability of the grid, it is prudent to manage these maintenance activities. In addition, because nuclear power plants (NPPs) require reliable offsite power sources, it is necessary to limit transmission system outages and, hence, coordinated maintenance planning is the only solution.

It is necessary to have a coordinated maintenance and outage management program to manage the operational risk exposure to the NPP and the grid resulting from planned, unplanned, or emergent work activities. The coordinated maintenance and outage management program should include NPP maintenance and outage activities that could affect the grid as well as grid maintenance and outage activities affecting the NPP. The coordination of testing, calibration, and maintenance of onsite and offsite power supply systems and related components is essential for providing reliable power sources to the NPP. The outages or maintenance on generation and transmission and distribution systems should be included in the coordinated maintenance planning process with nuclear station oversight because the outage of any one of these systems could affect the NPP's offsite power sources and, hence, challenge nuclear safety.

A planned schedule to manage equipment outage, maintenance, surveillance, and testing is essential to reduce the risk exposure to the grid system and NPP as well as to limit the unavailability of essential systems (risk-significant components). The absence of coordination on such activities could lead to unanticipated transients, outages, or even system collapse. Communication with nuclear stations and other affected parties should remain active during these activities to confirm the completion of the scheduled activities or further remedial actions to prevent unanticipated transients.

Maintenance planning and scheduling with a minimum of monthly, weekly, and daily planning is expected to occur to address all anticipated activities such as equipment outage, maintenance, surveillance, and testing. This coordination needs participation from all the parties that are affected by the aforementioned activities.

The corrective and preventive maintenance activities should be coordinated to limit challenges to nuclear safety. It involves refraining from grid activities while risk-significant NPP components are degraded or under maintenance/surveillance. These grid activities include any maintenance, surveillance, or testing in the transmission or distribution system that could affect the NPP and its offsite power sources. Moreover, NPP procedures should include steps to perform safety analyses to assess the impact of routine or emergent maintenance and outage activities on the NPP and grid and, subsequently, to communicate the results to the grid operator. The USNRC regulation on maintenance rule (10 CFR 50.65) requires licensees to assess and manage the risk before they perform maintenance activities.

3 CONCLUSIONS

The recommended actions presented in this paper or other suitable alternate actions are important to be considered to ensure the defense-in-depth of electrical safety systems. The capability of the onsite electrical system to withstand the range of voltage and frequency fluctuations, the suitability of logic/control system failure mode, diversity in core-cooling systems, a contingency assessment program

on the transmission system, and a coordinated maintenance program between the NPP and the transmission system operator are important elements for preserving nuclear safety.

4 REFERENCES

1. "Defense in Depth of Electrical Systems and Grid Interaction Final DIDELSYS Task Group," November 2009. Published by the Nuclear Energy Agency: Committee on the Safety of Nuclear Installations, France. http://www.nea.fr/html/nsd/docs/2009/csni-r2009-10.pdf
2. NRC Information Notice 93-11, "Single Failure Vulnerability of Engineered Safety Features Actuation Systems." http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1993/in93011.html
3. NRC Generic letter GL-2006-02 "Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power" http://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/2006/gl200602.pdf

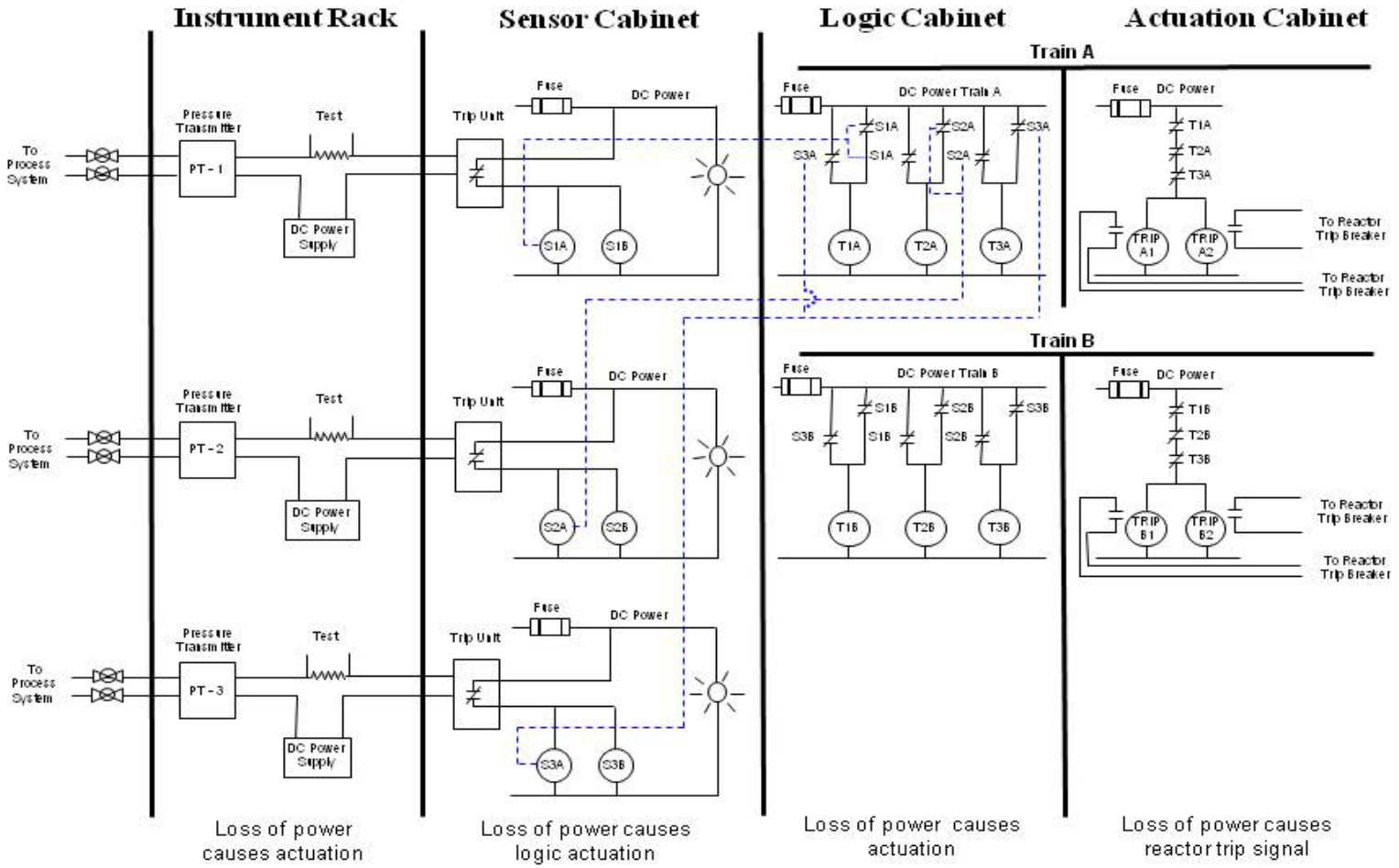


Figure 2. Simplified Fail-Safe Reactor Trip System with a Two-Out-of-Three Logic.

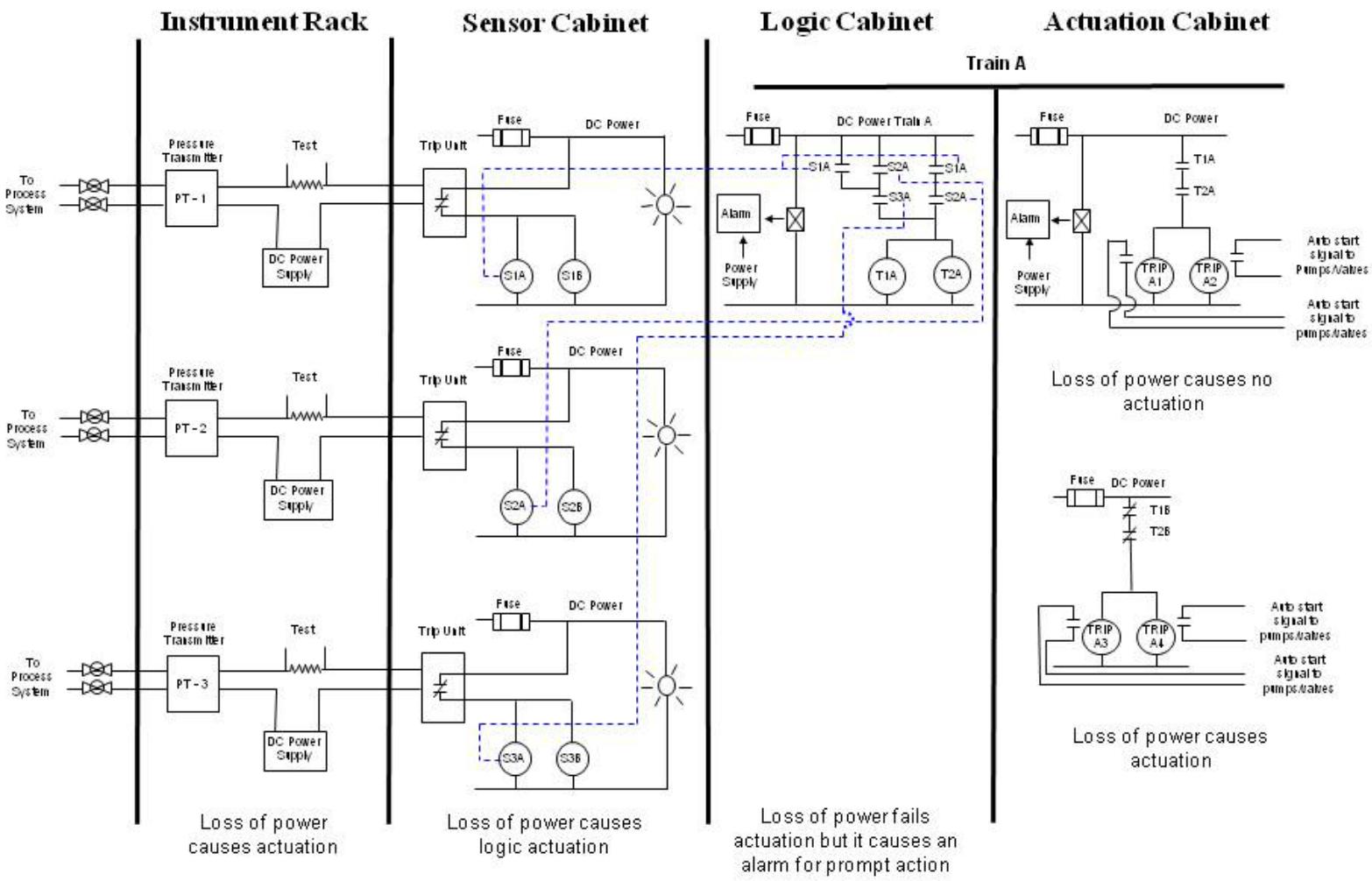
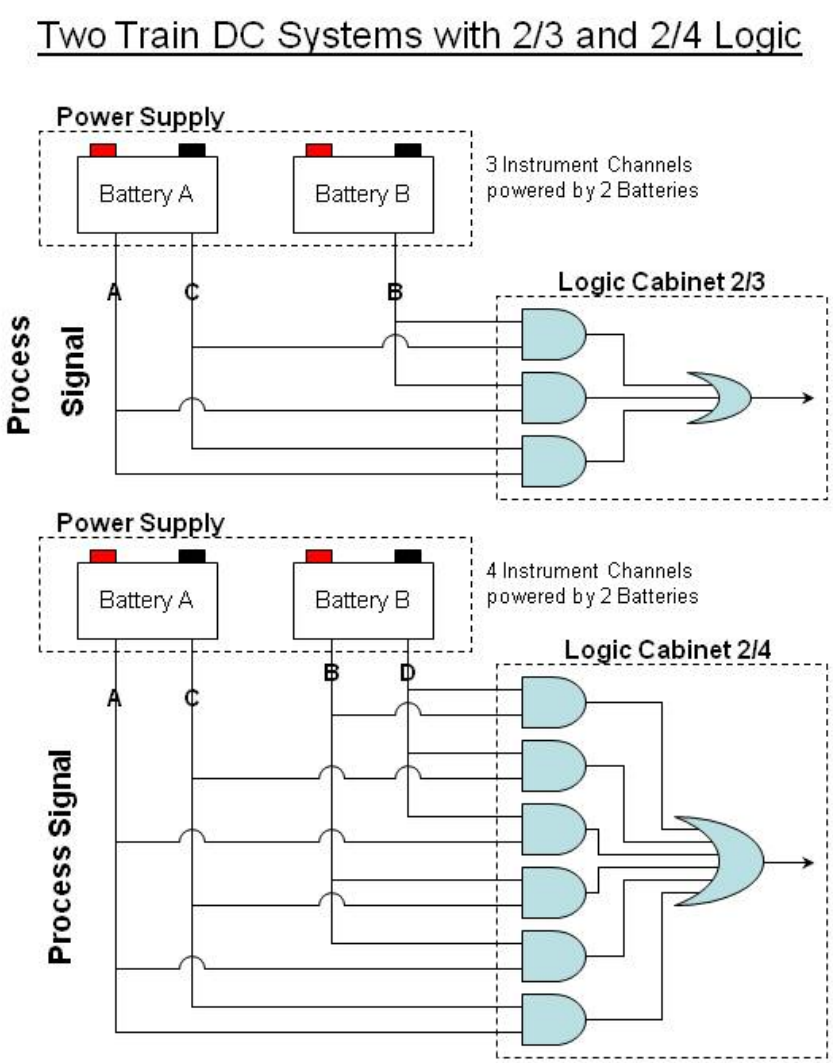


Figure 3. Simplified Core-Cooling System with a Two-Out-of-Three Logic.



Source Power:

UPS – Susceptible for common-mode failures from over voltage or under voltage

DC – Comparatively more reliable

Two train DC System with 2/3 logic has the following vulnerability

- When Battery Bus A is lost the logic could create a false output or prevent logic from any output

Solutions:

(1) Fail-Safe Logic

(2) Logic Reverts to 1/1 logic when Bus A fails

Two train DC System with 2/4 logic has the following vulnerability

- Loss of Bus A or B can cause a false output

Solutions:

(1) Fail-Safe Logic

(2) Logic Reverts to 2/2 logic with the available pair of signals

Figure 4. Two-Train DC Systems with 2/3 and 2/4 Logic.