Defense in Depth For US Electrical Power Systems

Thomas Koshy, Branch Chief
Office of Research
U.S. Nuclear Regulatory Commission

Agenda

- NRC Actions regarding Forsmark Event
- Functional Requirements of offsite Electrical Power Systems
- Communication with Grid Operators
- Industry Actions
- Regulatory Actions
- Functional Requirements of Onsite Electrical Systems
- Functional Requirements of Instrument Bus Power Supply Failures
- Lessons Learned
- Millstone-2 Electrical Event
- Questions

NRC Actions

- Evaluated operating U.S. plants.
- Coordinated with public affairs to respond to media questions on the event
- Issued the following documents to highlight the issue
  - NRC Information Notice 2006-18, Dated August 17, 2006
  - NRC Information Notice 2006-18, Supplement, Dated August 10, 2007

Functional Requirements of Offsite Electrical Power Systems

- Two independent sources of AC power of sufficient capacity and capability to assure that (1) fuel design limits and design conditions are not exceeded as a result of anticipated operational occurrences (2) core is cooled and containment integrity and other vital functions are maintained
- Primary source (preferred source) of offsite power source available in seconds and second source with a time delay
- Offsite power sources together should meet single failure
- Grid analysis that confirms stability and offsite power availability following the loss of a nuclear unit, largest load on the grid, or most critical transmission line.

- **Regulatory Guidance :**
  - 10 CFR 50 Appendix A, General Design Criteria 17,33,34,35,38,41, and 44
  - 10 CFR 50.63 Loss of All Alternating Current Power (Station Blackout)
  - Standard Review Plan NUREG 800, Chapter 8.1 & 8.2
  - Generic Letter 2006-2: Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power
    - Contracts & Communication with grid operator
    - Shared knowledge on contingencies
  - Regulatory Guide 1.93 Availability of Electrical Power Sources (Currently under revision)
  - Regulatory Guide 1.75 Rev 3 Criteria For Independence Of Electrical Safety Systems

Communication with Grid Operators

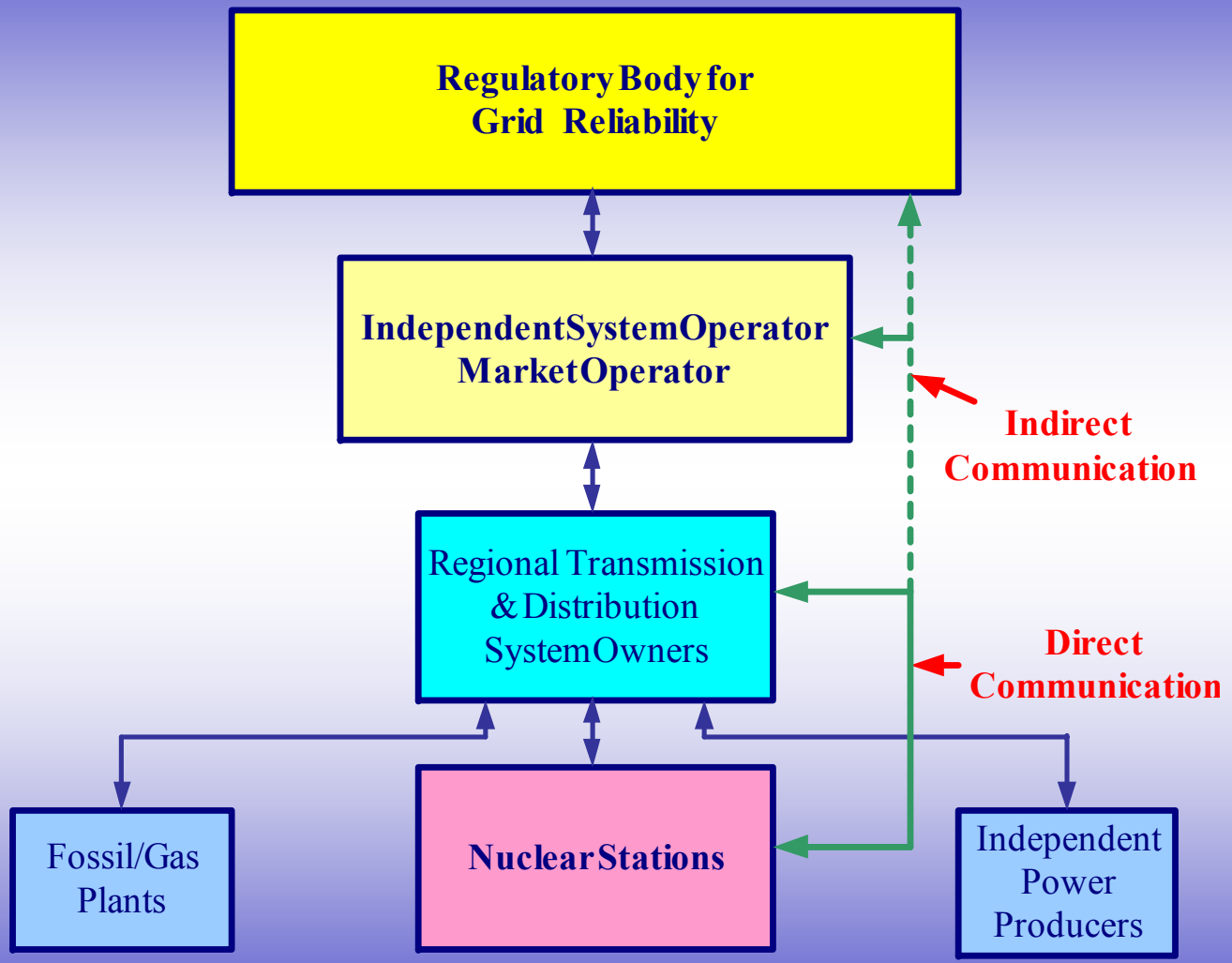


Fig 1

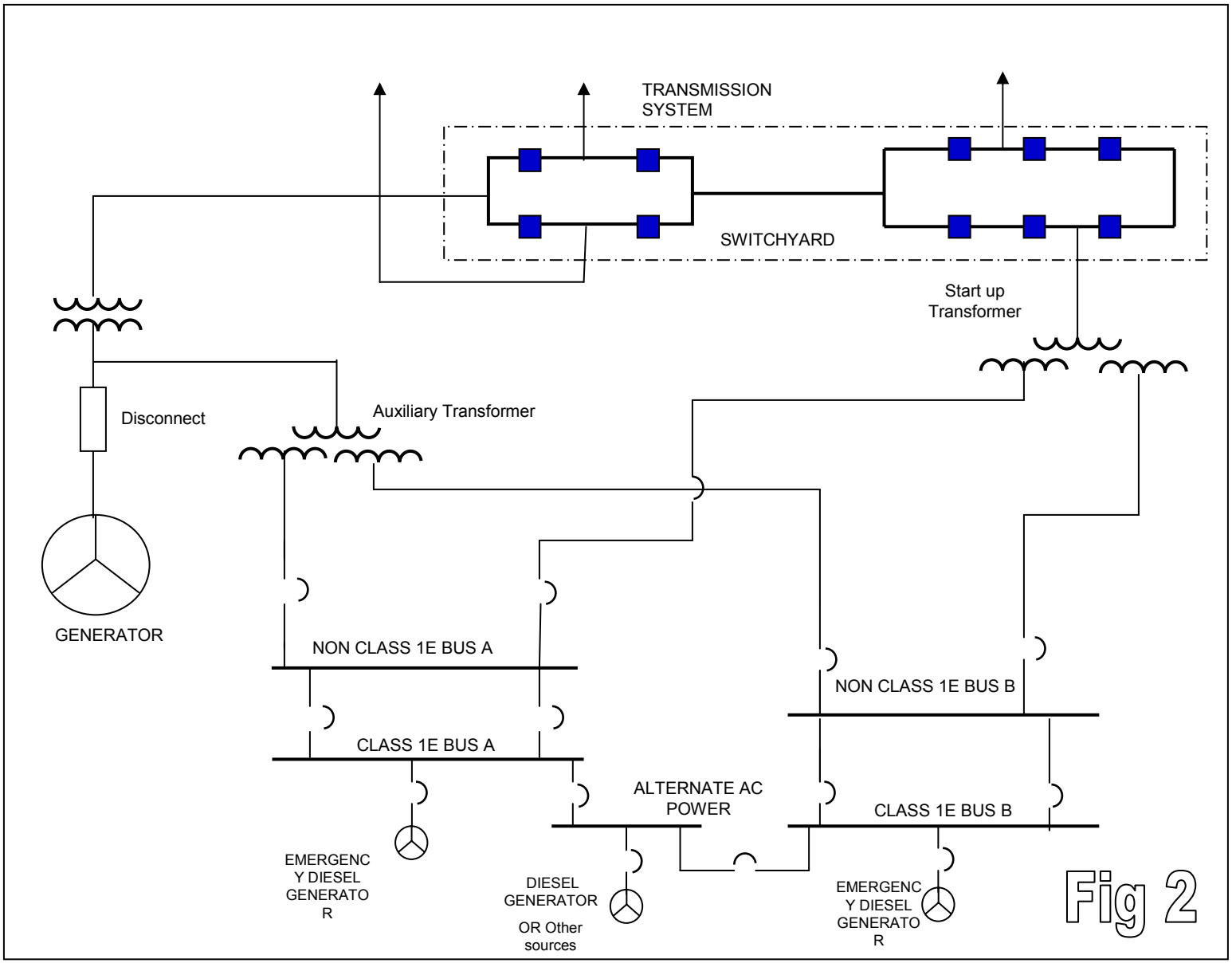
Thomas Koshy/ Office of Research/USNRC

Industry Actions

- Industry-developed procedures on Reliability was endorsed by government regulator Federal Energy Regulatory Commission for mandatory compliance
- Critical Infra-Structure Protection procedures
  - Classification and Special Treatment of critical assets

Regulatory Action

- On March 20, 2008, FERC published a Notice of Proposed Rulemaking (NOPR), 18 CFR Part 40 Docket No. RM08-3-000, which proposed to endorse (with comment) NERC Reliability Standard NUC-001-1, which was intended to address the type of nuclear generator/ transmission system operator interfaces necessary to assure that power is continually available for nuclear plants, not only to allow nuclear plants to meet their licensing commitments for offsite power, but also to improve the reliability of the grid.
- One of the requirements in NUC-001-1 is Requirement R 9.3.6, which states: "Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan."
- "Further, an interface agreement must coordinate responses to unusual conditions on the grid such as loss of ability to monitor grid performance, loss of off-site power, use of special protection systems, and underfrequency and undervoltage load shedding programs."
- Requirement R9.3.6 requires coordination of physical and cyber security systems. The interface agreements also must adopt terms and protocols for communications between the nuclear plant generator operator and transmission entities, coordination and communication during atypical operating conditions or emergency events, investigation and resolution of the causes of unplanned events, compliance with regulatory information requirements, and personnel training (Requirements R9.4.1-.5).
- The full text of this NOPR may be found at: http://www.ferc.gov/whats-new/comm-meet/2008/032008/E-2.pdf


TRANSMISSION SYSTEM
SWITCHYARD
Start up Transformer
Disconnect
Auxiliary Transformer
GENERATOR
NON CLASS 1E BUS A
NON CLASS 1E BUS B
CLASS 1E BUS A
ALTERNATE AC POWER
CLASS 1E BUS B
EMERGENCY DIESEL GENERATOR
DIESEL GENERATOR
OR Other sources
EMERGENCY DIESEL GENERATOR
Fig 2

ONE LINE DIAGRAM FOR SINGLE UNIT NUCLEAR STATION

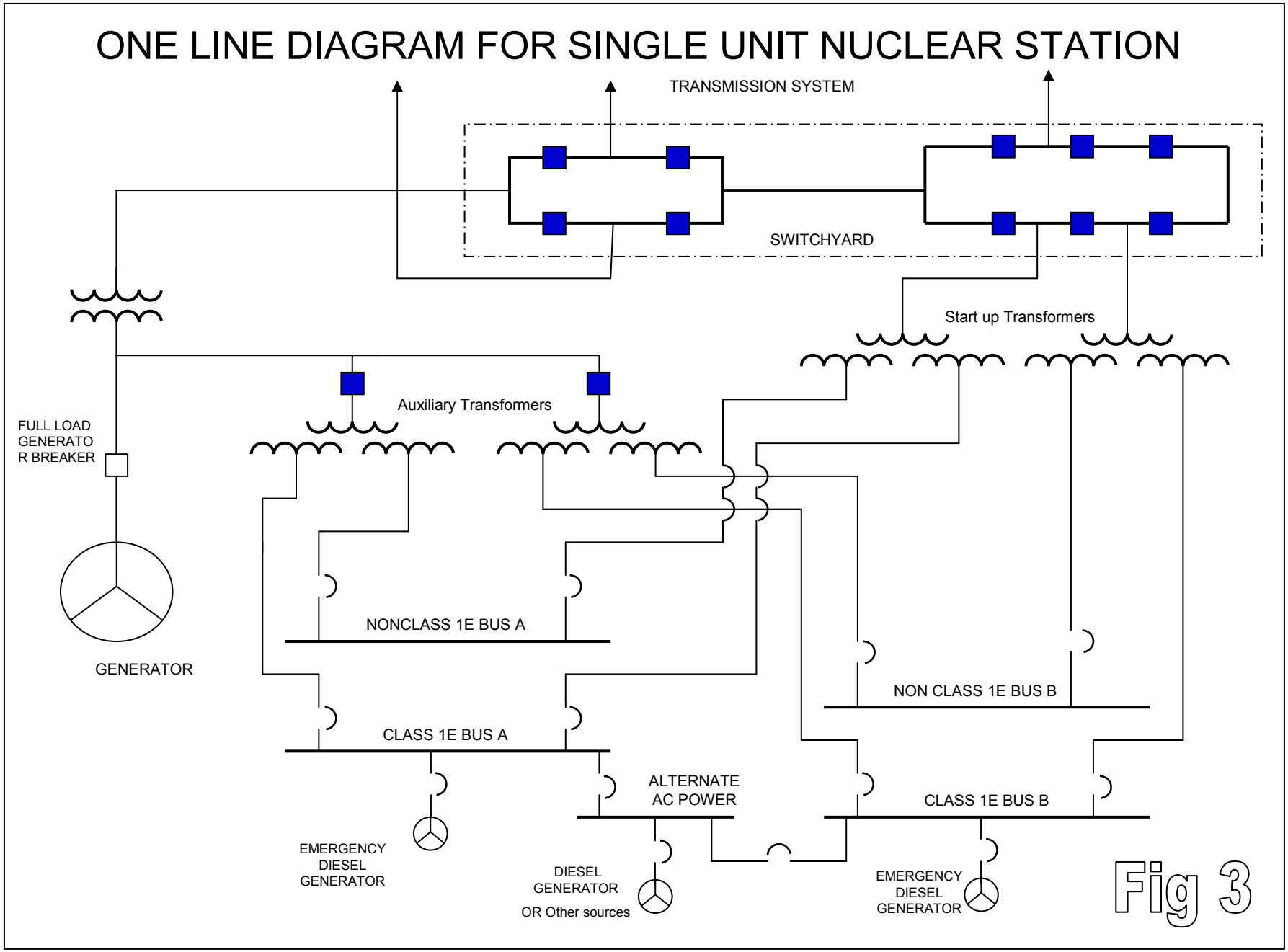


Fig 3

Functional Requirements of Onsite Electrical Systems

- Two independent sources of AC power of sufficient capacity and capability to assure that (1) fuel design limits and design conditions are not exceeded as a result of anticipated operational occurrences (2) core is cooled and containment integrity and other vital functions are maintained
- Onsite power sources together should meet single failure
- Provisions to minimize loss of electric power coincident with or as result from loss of generation, loss of grid, or loss any onsite source

- **Regulatory Documents:**
  - 10 CFR 50 Appendix A, General design Criteria 17,33,34,35,38,41, and 44
  - Standard Review Plan NUREG 800, Chapter 8.3.1 & 8.3.2
  - Regulatory Guide 1.93 Availability of Electrical Power Sources (Currently under revision)
  - 10 CFR 50. 65 Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants

Onsite Electrical System

- Performance Indicator Program- Reactor Oversight Program
  - The NRC and the nuclear industry have jointly implemented a replacement to the Safety System Unavailability Performance Indicators, called the Mitigating System Performance Index (MSPI).
  - Safety System Functional Failures - The number of events or conditions that alone prevented, or could have prevented, the fulfillment of the safety function of structures or systems in the previous four quarters.
  - Emergency AC Power Systems - The sum of the unavailability of the emergency AC power plus the unreliability for the emergency AC power system during the previous twelve quarters.
    http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/cornerstone.html

Instrument Bus Power Supply Failures

Current US Design

- Provide DC control system for core cooling systems and diesel generator back up for core cooling systems
- Provide AC vital bus with battery back up for trip systems that have fail-safe logic on loss of power

- Regulatory Guide 1.93 Availability of Electrical Power Sources.
- Standard review Plan NUREG 800, Chapter 7

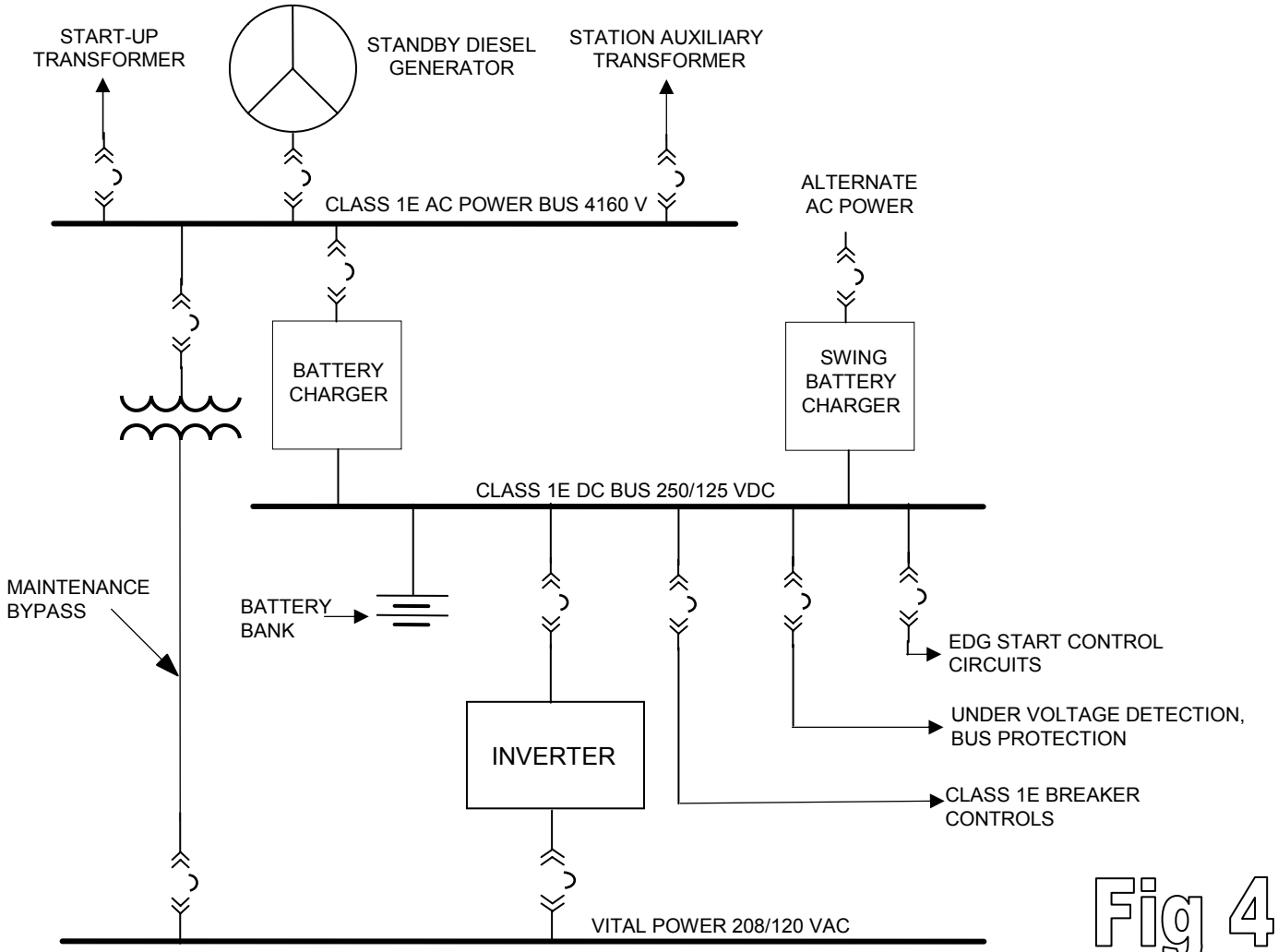

START-UP
TRANSFORMER
STANDBY DIESEL
GENERATOR
STATION AUXILIARY
TRANSFORMER
CLASS 1E AC POWER BUS 4160 V
ALTERNATE
AC POWER
BATTERY
CHARGER
SWING
BATTERY
CHARGER
CLASS 1E DC BUS 250/125 VDC
MAINTENANCE
BYPASS
BATTERY
BANK
EDG START CONTROL
CIRCUITS
UNDER VOLTAGE DETECTION,
BUS PROTECTION
INVERTER
CLASS 1E BREAKER
CONTROLS
VITAL POWER 208/120 VAC

Fig 4

Lessons Learned

- New Reactor Design Challenges
  - 130 to 140% of rated voltage postulated when the main generator goes into islanding (The voltage spike would depend on the maximum regulator output)
  - Voltage regulator on the main generator cannot instantly reduce the voltage spike to the normal voltage levels for onsite safety and non-safety systems
  - Direct DC control systems for EDG and core cooling systems could avoid dependence on UPS

Lessons Learned

- Design modifications should have specific verification steps to ensure proper function of all attributes
  - Phase sequence sensitivity, UPSs
  - Failure mode on loss of power
- All AC sources need periodic maintenance and surveillance testing to confirm availability
  - The operational readiness of alternate AC sources

Millstone-2 Electrical Event

- On July 6, 1992 , during a refueling outage, the licensee identified several undesirable failure modes of a two-out-of-four logic following an event. The plant was designed with two sensor cabinets and one actuation cabinet for each of the two trains. *(Information Notice 93-11)*
  - When power was lost to either one of the vital buses it caused safety injection and sump recirculation actuation.
  - When two of the sensor cabinets in a train lost power it caused the containment sump outlet valves to open
  - Loss of DC power to one actuation train caused power operated relief valve in the other train to open
- The logic was modified to limit certain combinations of two-out-of-four logic to prevent this problem.

NRC Guidance on Control Systems

- Bulletin 79-27 “Loss of Non-Class 1E Instrumentation and control Power System Bus During Operation” – Evaluate the effects of loss of power to control systems
- Generic letter 89-18 “Systems Interactions in Nuclear Power Plants” – concerns regarding automated safety related actions with no preferred failure modes

Questions