LESSONS LEARNED FORSMARK EVENT
Presented To IEEEE

Thomas Koshy

Member of the Task Group on Forsmark

Chief of Mechanical & Electrical Engineering

Office of Research, USNRC

Thomas.Koshy@nrc.gov

Agenda

- Safety Systems Overview
- Event Summary
- Risk Insights
- Event Details
- Over Voltage
- Recommendations
- Millstone 2 –Failure Modes
- Preferred Failure Modes
- Solutions to House-load Operational Problems
- Regulations
- IEEE Challenges

Forsmark station

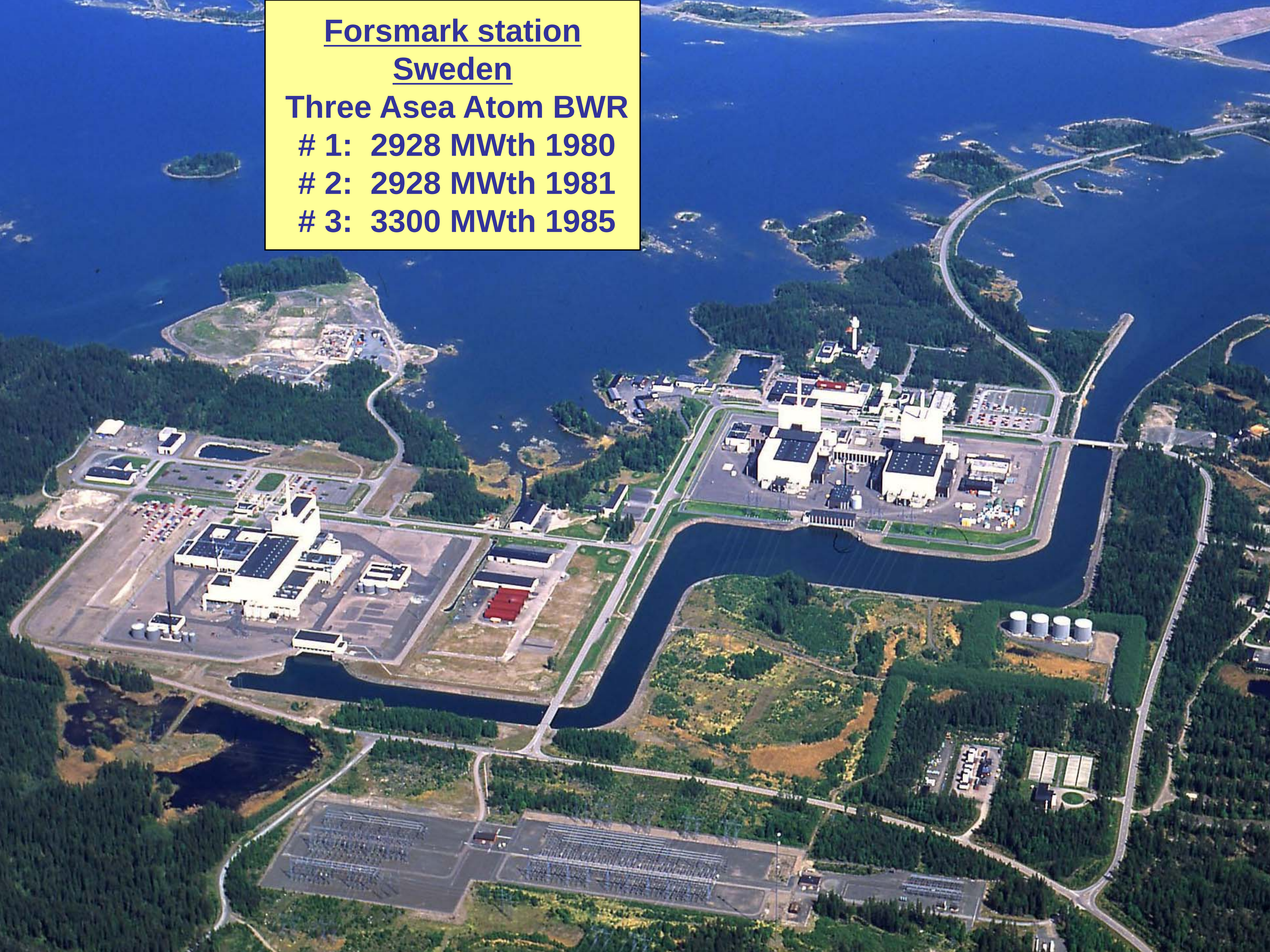
Sweden

Three Asea Atom BWR

 # 1: 2928 MWth 1980

 # 2: 2928 MWth 1981

 # 3: 3300 MWth 1985



Forsmark Safety Systems Overview

- Safety systems are divided into four trains
- Each train with its own emergency diesel generator and capacity to manage 50% of the ECCS loads
- Emergency Core Cooling is all electric

Event Summary

- July 25, 2006; Plant at 100%
- Opened 400 kV disconnect and caused an Electrical Fault
- Generator voltage dropped to 30%
- Unit disconnected from the grid
- Generator over-voltage (OV) 130%
- OV caused 2 of 4 UPSs to fail
- 2 of 4 Emergency Diesel Generators (EDG) failed to connect to the safety buses

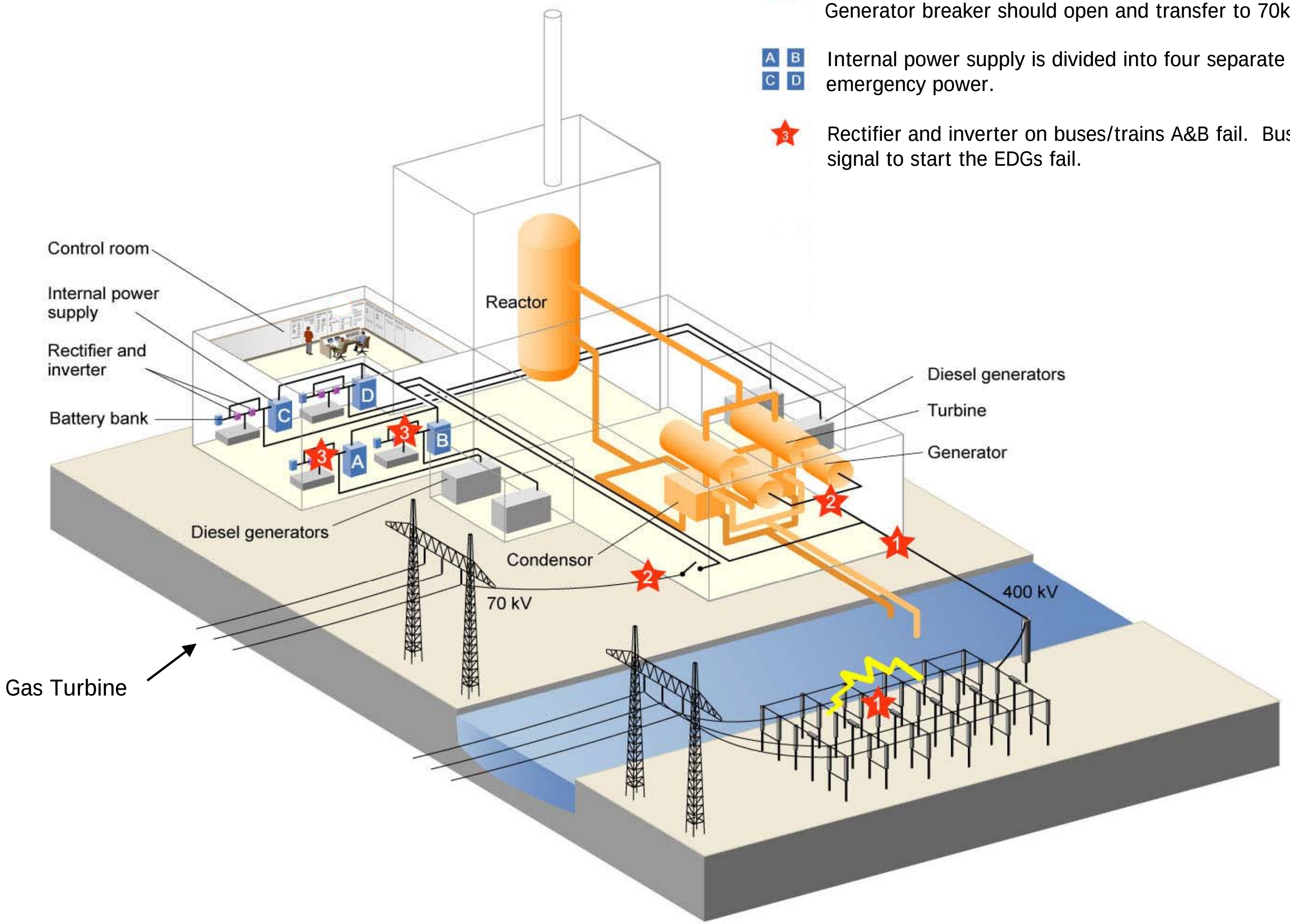
5

Maintenance work in the switchyard causes an arc and a short circuit. Unit 1 is disconnected from the grid and reactor scrams.

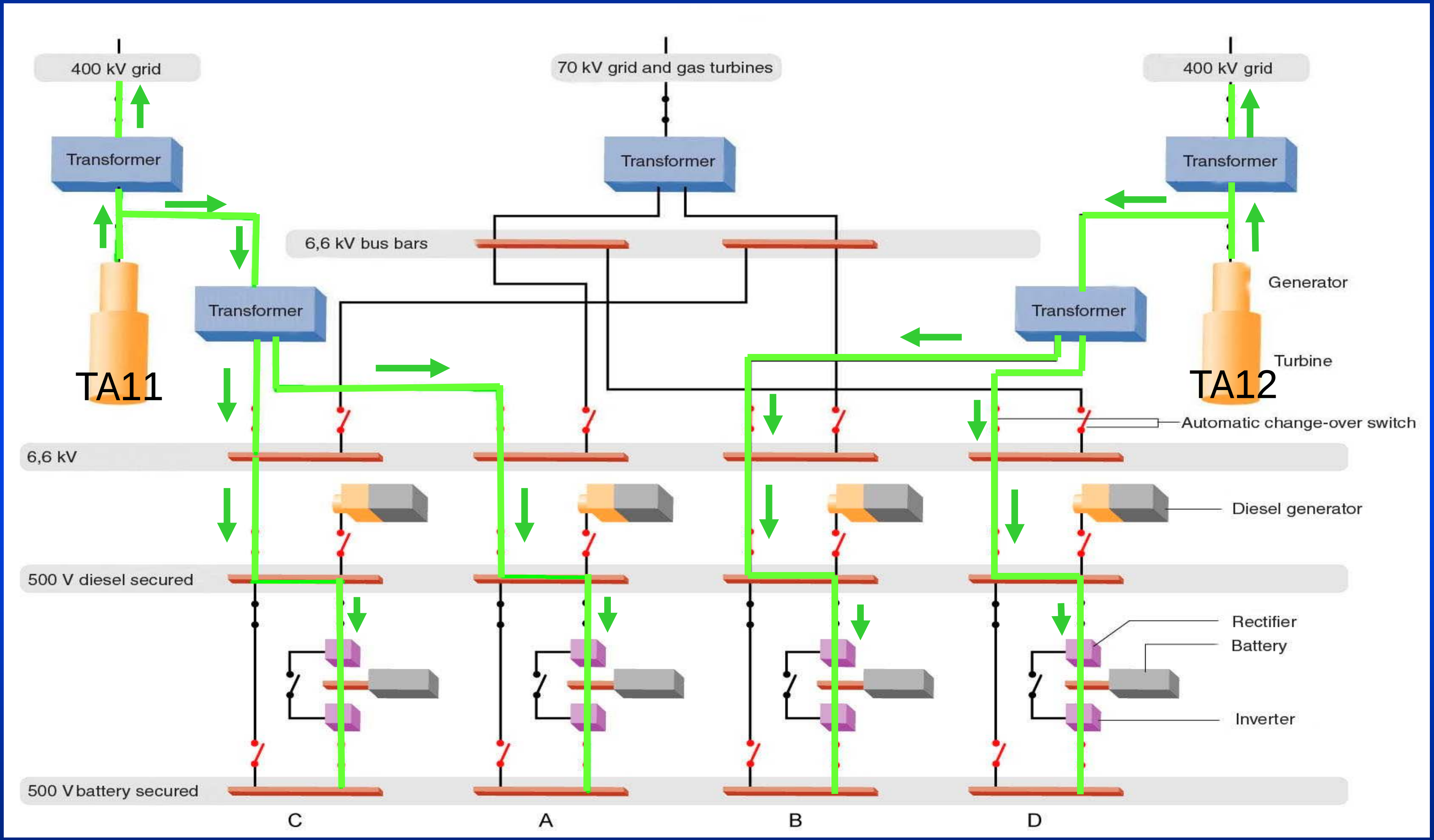
Failure in the generator protection results in generator breaker not opening. Generator breaker should open and transfer to 70kV offsite power.

Internal power supply is divided into four separate buses/trains (A,B,C,D) for emergency power.

Rectifier and inverter on buses/trains A&B fail. Buses A&B loss power and the signal to start the EDGs fail.



6


400 kV grid
70 kV grid and gas turbines
400 kV grid
Transformer
Transformer
Transformer
6,6 kV bus bars
Transformer
Transformer
Generator
TA11
Turbine
TA12
Automatic change-over switch
6,6 kV
Diesel generator
500 V diesel secured
Rectifier
Battery
Inverter
500 V battery secured
C
A
B
D

Event Summary

- Both generator breakers should have tripped immediately
  - Common Cause Failure
- Over voltage tripped two battery charges & two inverters (2/4 UPS shutdown)
  - Common Cause Failure
- 2/4 EDGs failed to energize the safety bus
  - Common design flaw
- Gas turbine failed to start
  - 70kV grid was available
- Loss of control room information
  - Loss of network power A&B

8

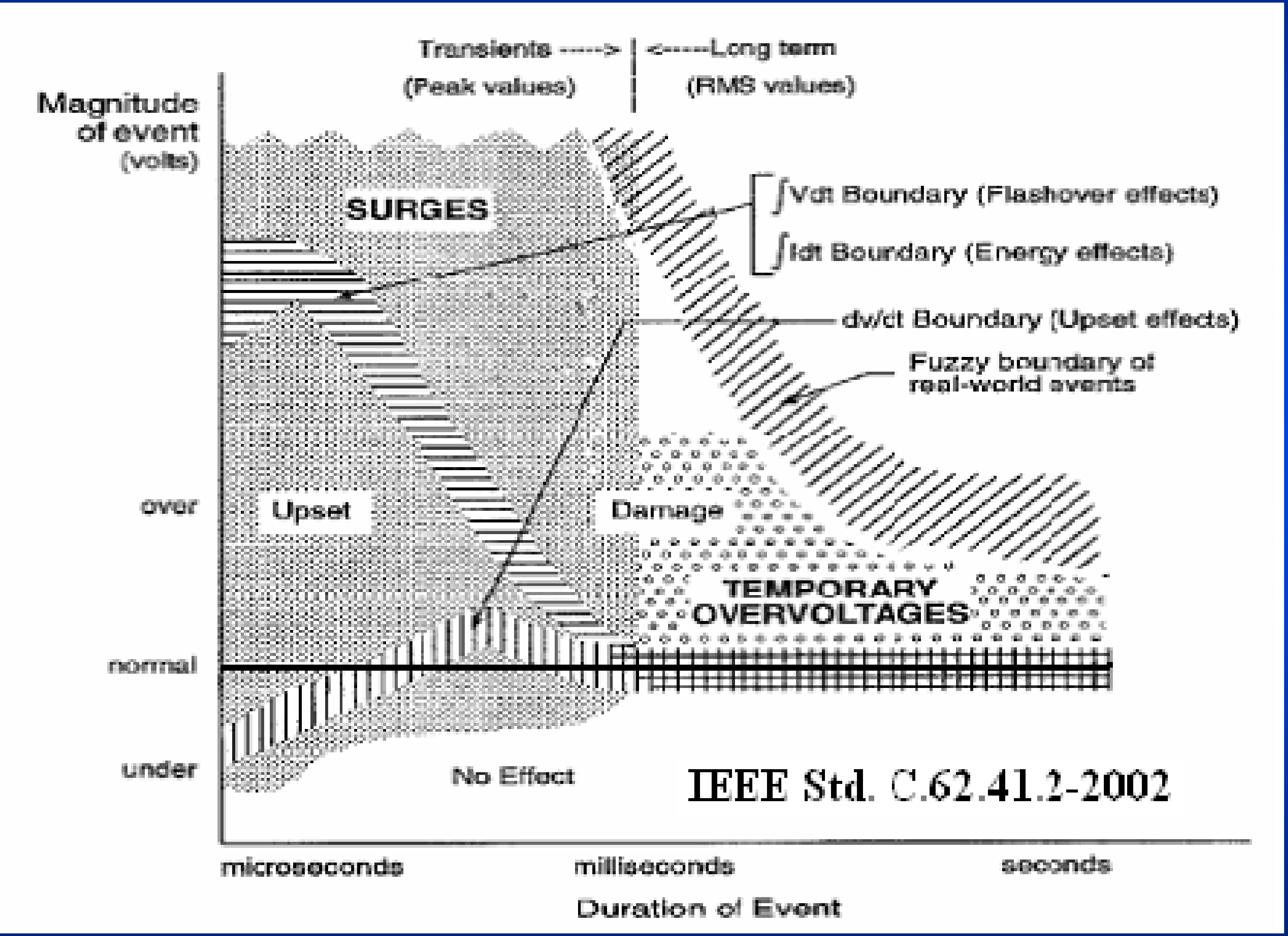
Risk Insights

- Plant Uniqueness that influence risk :
  - No steam/diesel-driven pumps (diversity /defense in depth)
  - 2 Common Cause Failures (UPS, Generator Relay Protection)
  - EDG controls relied on AC power from UPS
  - Failure of power supplies to control room indications
  - Gas Turbine didn't start

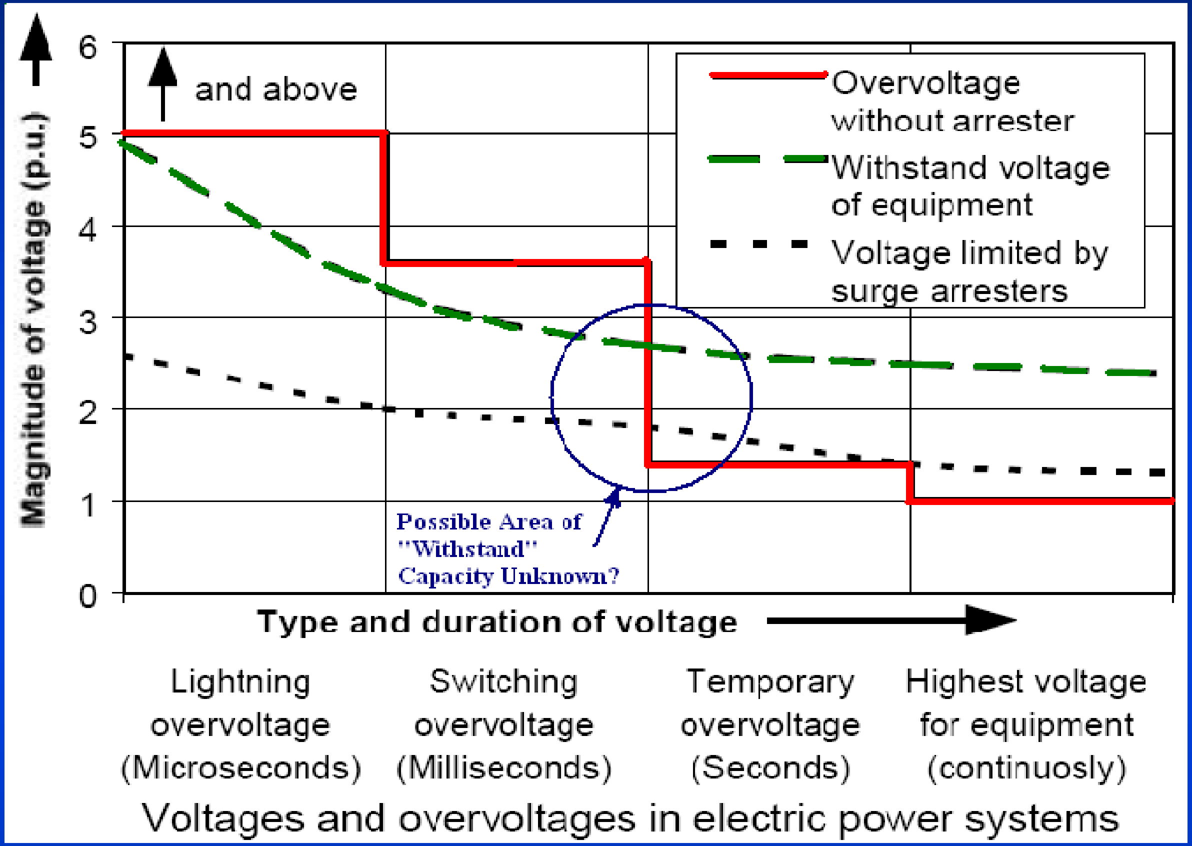
Event Details

- When two Uninterruptible Power Supplies (UPSs) failed during the Forsmark event
  - The pressure regulating valve in the primary system failed open
  - The valve remained open until the bus was re-energized
- Failures beyond single failure that originated from common-cause (IAEA NS-G-1.8 Section 2.11:Common Cause)

Over Voltages



Over Voltage



- Breakers can’t address lightning surges because *they operate too slowly*
- “Surge arrestors” can divert short duration Overvoltage

Over Voltage

- electrical systems NPP nominally designed for operation with +/-10% Voltage
- Voltages *above*120% but *below* lightning protection lightning features are generally beyond *design bases*
- 2006 Forsmark--1 and 2008 Olkiluoto--1 events indicate that Previously assumed “Withstand Voltage” may be as low as:~*130%*

Recommendations

- ***Prevent*** NPP--grid interaction challenges to NPP electrical power systems *(Prevent Grid Challenges)*

- Improve ***Robustness of NPP electrical systems*** to cope with grid, and internal NPP electrical faults *(Electrical System Coping)*

- Improve NPP training, procedures, display capabilities to deal with degraded electrical systems *(Procedures)*

- Improve ***Coping Capability*** of NPP to deal with NPP electrical of power system failures *(NPP Coping)*

- Improve ***capability to recover offsite grid*** to support NPP electrical power systems *(Electrical System Recovery)*

Preventing Grid Challenges

- WANO SOER 99WANO 99--1 and 2004 Addendum offer practical approaches to reduce electrical grid challenge, including:
  - Binding Agreements for communication, coordination of planned activities
  - Jointly planning, coordinating electrical circuit test & Jointly maintenance activities
  - Grid operators: provide NPPs early warning of grid problems
  - NPP operators: provide grid operators early warning of operational NPP limitations that might impact NPP power output
  - Grid procedures must recognize NPP as priority load center Grid requiring efforts to avoid shedding circuits to NPP requiring NPP

Electrical System Coping

- Identify possible voltage surge transients between nominal and existing lightning surge protection.
- Include consideration of combinations of events, such as:
  - Large load rejection →→attempted runback to house load ***AND*** failure of main generator excitation and voltage regulator failure
- Conduct equipment review to determine current Conduct ***Voltage Withstand*** capability for power frequency over--voltage transients (including: *asymmetric cases*)
- Give special emphasis to recently upgraded solid state equipment that may have the least ***Voltage Withstand*** capability
- This includes: UPS units, rectifier circuits, chargers, I&C power supplies

Procedure Improvements

- WANO SOER 99WANO 99--1 and 2004 Addendum recommend NPP to have procedures for addressing :
  - Degraded voltage
  - Degraded grid frequency
- How well these recommendations have been implemented, information systems to monitor such events, thoroughness of procedures etc.,—***should be evaluated in each country***

NPP Coping Capability

- Recognize ***defense in depth*** requires improving ability to cope with losses of "uninterruptible" electrical buses
- Review RPS and ESFAS logic circuits to identify any undesirable effects from loss of "uninterruptible" electrical buses
  - Examples would include: generation of ADS signal in BWRs or Examples AUTO Switchover to Recirculation in PWRs, PORV openings etc.,
- USNRC (1993) issued USNRC *Information Notice information 93—11* describing concern and to consider evaluations & modifications for US NPPs

NPP Coping

- *For any plants any plants with all-electric Core Cooling:*
  - Evaluate providing a ***diverse means for*** promptly supplying power to core cooling systems
  - This could include:
    - Direct diesel driven pump
    - Dedicated fast start gas turbines

Electrical System Recovery

- WANO SOER 99WANO 99--1 and 2004 Addendum offer practical approaches to improve electrical system recovery:
- Grid procedures must recognize NPP as priority load center requiring highest priority for restoration

Preferred Failure Modes

- Supervisory Controls
  - Design to cause failure mode when parameters cross the operating band (voltage, air pressure, hydraulic pressure, etc.,)
  - Provide alarms for inoperative and bypassed conditions
- Annunciations in Control Room
  - Powered by auctioneered power supply different than logic power (eg: 24vDC multiple power supply units daisy-chained)

Power Supplies

- Provide DC control system (without UPS and inverters) for core cooling systems and AC power with emergency diesel generator back up for powering core cooling pumps & valves
- Provide AC vital bus with UPS back up for trip systems that have fail-safe logic on loss of power eg. Rod drop systems (reactor protection system)

Solutions to House-load Operational Problems

- When grid conditions are undesirable reduce reactor power to approx. 5- 15%
  - Transfer plant loads to offsite power
  - Dump the steam to the condenser
- Prevent over voltage to UPS and other safety systems
  - Design UPSs to withstand worst case voltage
  - Interrupt power to UPS until fault transients are cleared
- Bypass house load operation following a fault / protective relay actuation

Design Review

- Failure Mode and effects Analysis
  - How can each part conceivably fail?
  - What mechanisms might produce these modes of failure?
  - What could the effects be if the failures did occur?
  - Is the failure in the safe or unsafe direction?
  - How is the failure detected?
  - What inherent provisions are provided in the design to compensate for the failure?

Millstone-2 Failure Modes

- 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.

Regulations

- Bulletin 79-27
  - identify the instrument and control system loads connected to the bus and evaluate the effects of loss of power to these loads including the ability to achieve a cold shutdown condition

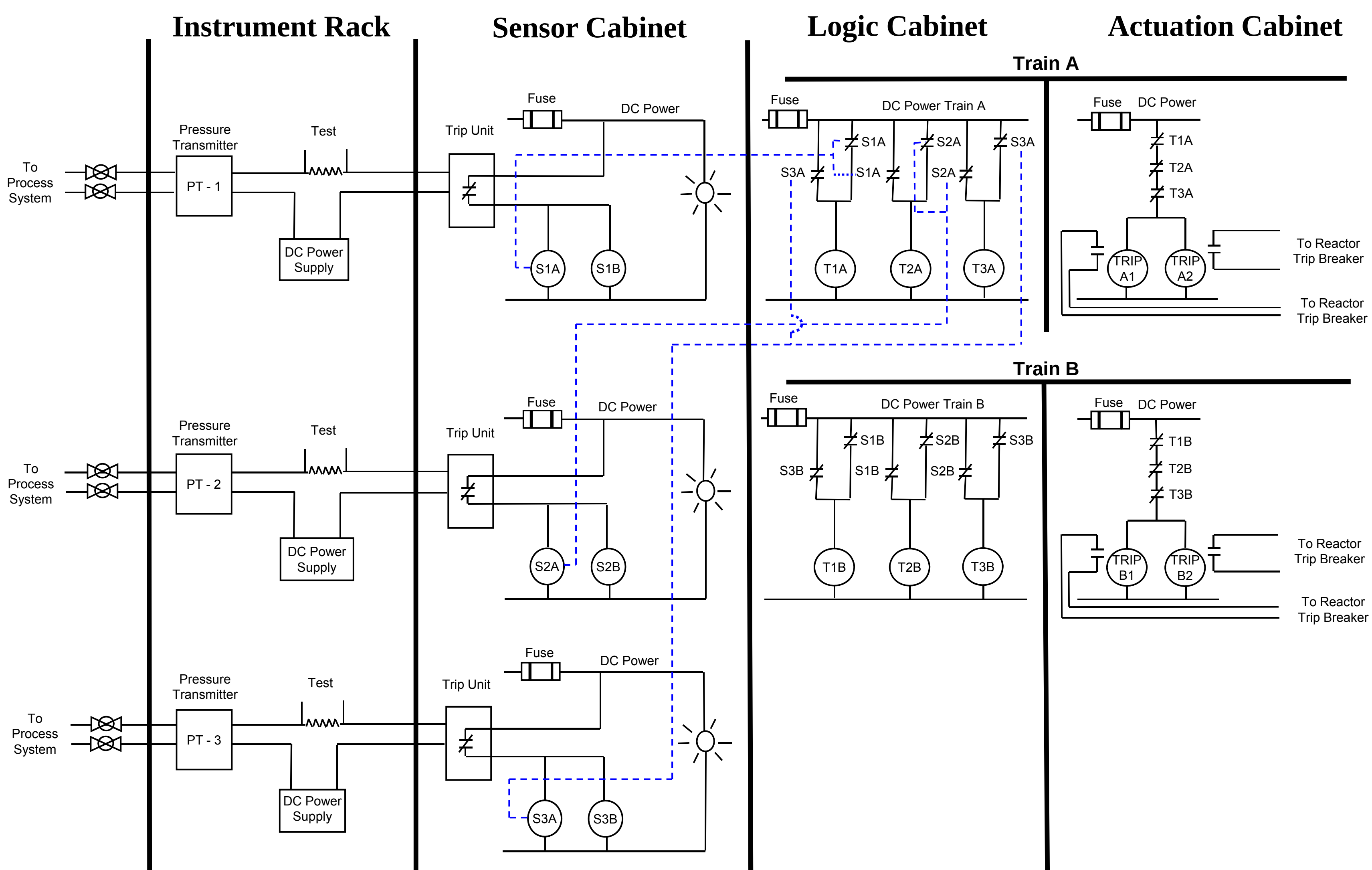
Regulations

- Generic letter 89-018
  - pointed out the incorrect reliance on fail-safe design principles and cautioned the industry regarding the automated safety-related actions with no preferred failure mode.
  - The need for extra precaution to avoid (a) failure to actuate when necessary and (b) a failure that actuate the system when not required

IEEE Challenges

- **ANSI/IEEE Standard 352-1987** (Under Revision)
  - To assist in selecting design alternatives with high reliability and high safety potential during early design phases
  - To ensure that all conceivable failure modes and their effects on the operational success of the system have been considered
  - To list potential failures and identify the magnitude of their effects
  - To develop early criteria for test planning and the design of test and checkout systems
- **Develop UPS qualifying guidance to include 150% overvoltage**

Simplified Fail-Safe Reactor Trip System with a Two-out-of-Three Logic



Loss of power causes actuation

Loss of power causes logic actuation

Loss of power causes actuation

Loss of power causes reactor trip signal

Simplified Core Cooling System with a Two-out-of-Three Logic