UNITED STATES DIGITAL SYSTEM FAILURE EVENTS

COMPSIS MEETING
October 25-27, 2006

Presented By:
William E. Kemper, Chief
Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering, and Radiological Research
Office of Nuclear Regulatory Research

OVERVIEW

- Search Criteria
  - Licensee Event Reports 1/2005 - 5/2006*
- Number of COMPSIS events
  - 7 reported events within the search criteria
- Plant Types
  - BWR - 5 events
  - PWR - 2 events
- Affected Systems
  - Core Protection Calculators - 1 event
  - Electro-Hydraulic Control - 3 events
  - Main Generator - 1 event
  - Solid State Protection System - 1 event
  - Others - 1 events

*LER dates are based on the date the event was reported to the NRC

OVERVIEW – cont.

- Effects on Operation
  - Manual Reactor Trip - 0 event
  - Automatic Reactor Trip - 5 events
  - Other (i.e. event detected during a refueling outage) - 2 events

- Root Cause
  - Hardware - 4 events
  - Software - 2 events
  - Communication - 1 event

EVENT 1 - PALO VERDE UNIT 2

Technical Specification Required Shutdown Due to Core Protection Calculators (CPCs) Inoperable

- Background
  - CPCs
    - Consist of 4 separate, redundant channels for the reactor protection system
    - Each channel is a computer system that continuously calculates thermal conditions and thermal limits
    - Provides two trips to the reactor protection system
      - Departure from Nucleate Boiling Ratio
      - Local Power Density

EVENT 1 - PALO VERDE UNIT 2

Technical Specification Required Shutdown Due to Core Protection Calculators Inoperable

- Timeline
  - May 18, 2005 - Westinghouse personnel discovered that the version of the Unit 2 CPC software was not consistent with the system requirement regarding the system response to analog input module error.
  - August 8, 2005 - Westinghouse personnel completed an apparent cause analysis for the issue and concluded the issue was a nuclear safety concern.
    - The version of software that was installed in Unit 2 would not allow certain sensor failures to result in a corresponding trip of the CPC channel.
  - August 22, 2005 - Westinghouse informed Palo Verde of the issue with the CPC software.
  - August 22, 2005 at 1605 Palo Verde declared the CPCs inoperable and commenced plant shutdown on Unit 2.

EVENT 1 - PALO VERDE UNIT 2

Technical Specification Required Shutdown Due to Core Protection Calculators Inoperable

- Problem
  - Common Mode Computer System Failure
- Cause
  - CPC system requirement specification was not properly translated into the CPC software by the vendor.
    - Programming/Human error
- Safety Significance
  - There were no adverse safety consequences as a result of this event.
- Corrective Action
  - The latest version of the CPC software was modified and installed in all four channels of Unit 2 CPC.

EVENT 2 – QUAD CITIES UNIT 1

Automatic Reactor Trip from High Reactor Pressure due to a Malfunction of the Electro-Hydraulic Control (EHC)

- Background
  - The reactor automatically tripped due to a high reactor pressure signal.
  - Trip occurred when maximum reactor pressure reached approximately 1044 psig during the event.
- Timeline
  - June 17, 2005 at 1120 reactor tripped.
- Problem
  - Discrete solid state electronic component failure

EVENT 2 – QUAD CITIES UNIT 1

Automatic Reactor Trip from High Reactor Pressure due to a Malfunction of the Electro-Hydraulic Control

- Cause
  - Failure in one of the Control Valve Input Circuit Cards in the EHC system.
    - Laboratory analysis was unable to identify the specific cause of the failure.
- Safety Significance
  - The safety of this event was minimal. All control rods inserted to their full in position, no reactor relief or safety valves were required to open, and all systems responded properly to the event.
- Corrective Action
  - Card replacement
    - Control Valve Amplifier Card
    - Load Limit Card
    - Pressure Load Gate Card
    - Associated Operational Amplifier Cards

EVENT 3 – FERMI 2

Automatic Reactor Shutdown due to Automatic Voltage Regulator (AVR) Failure

- Background
  - AVR
    - Part of the main generator excitation system
    - Maintains generator output voltage under varying conditions of load within a set tolerance
  - AVR System
    - Uses Closed loop static excitation system
      - 5200KVA excitation transformer
      - Rectifier cubicle (power converter)
        - » Consist of a microprocessor based thyristor unit
      - Excitation control cubicle (AVR)
        - » Consist of two electronic processing units
      - Field Suppression cubicle (de-excitation function)
      - LAN network which is configured with coaxial cabling connections between each interface/termination point and operates using a “ARCnet” signal

EVENT 3 – FERMI 2

Automatic Reactor Shutdown due to Automatic Voltage Regulator (AVR) Failure

- Background cont.
  - November 2004 three thyristor converter units were replaced.
    - Several sub-component boards for each convert unit
      - 3 ARCnet coupler communication boards of a later design
- Timeline
  - On December 4, 2004, the reactor tripped from 60% power.
- Problem
  - Software communication
- Cause
  - Incompatibility of the new ARCnet communication circuit boards with the original design due to excessive noise in the system.

EVENT 3 – FERMI 2

Automatic Reactor Shutdown due to Automatic Voltage Regulator (AVR) Failure

- Safety Significance
  - The AVR has no safety related functions.
  - Although the reactor protection system was challenged, there were no adverse safety consequences as a result of this event.
- Corrective Action
  - ARCNet coupler communication circuit boards were replaced with the original circuit boards.
  - Software changes were made to incorporate a 2-second time delay to eliminate unnecessary noise.
  - A single ARCnet communication alarm was replaced by six separate alarms to better identify the origin of a communication problem.

EVENT 4 – BROWNS FERRY UNIT 3

Reactor Trip from Main Turbine Trip from Loss of All Speed Feedback

- Background
  - A lightning strike occurred on the TVA 500-kV system that resulted in a phase-to-ground fault on all three phases of the transmission line.
  - The electrical power transient caused speed perturbations on unit 3 that were slightly greater than the maximum rate anticipated by the turbine control system logic.
  - The turbine speed feedback signals, while valid, were designated as invalid by the logic of the EHC system.
- Timeline
  - On November 23, 2004 at 1002, a main turbine trip and subsequent reactor trip occurred from steady state operation at 100% power.

EVENT 4 – BROWNS FERRY UNIT 3

Reactor Trip from Main Turbine Trip from Loss of All Speed Feedback

- Problem
  - Invalid software setpoints
- Cause
  - An incorrect design response of the main turbine EHC logic to initiate a main turbine trip when a condition occurs where no valid turbine speed signals are available.
- Safety Significance
  - There were no adverse safety consequences as a result of this event.
- Corrective Action
  - The +/- 15rpm difference setpoint was changed to +20/-36 rpm.

EVENT 5 – MILLSTONE UNIT 3

Inadvertent Reactor Trip and Safety Injection

- Background
  - During 100% power, the solid state protection system (SSPS) generated a low Safety Injection/Main Steam Isolation signal on train “A”, which
    - Tripped the reactor
    - Closed the main steam isolation valves
    - Started one train of the emergency core cooling system
  - The turbine driven auxiliary feedwater (TDAFW) pump tripped on startup.
- Timeline
  - On April 17, 2005 at 0829 a reactor trip occurred.
    - Safety Injection and main steam line for train “B” was manually actuated
  - 0840 - Reactor coolant system pressure reached 2350 psia and both pressurizer power operated relief valves began to cycle.
  - 0913 - Safety injection was terminated
  - 1019 - Manual restart of the TDAFW pump
  - 1905 - Event terminated

EVENT 5 – MILLSTONE UNIT 3

Inadvertent Reactor Trip and Safety Injection

- Problem
  - Whiskers on I&C Components
- Cause
  - Diode leads on Universal Logic Board were coated with a material susceptible to whisker growth that eventually shorted the card output of the SSPS. (later found to be a tin whisker)
- Safety Significance
  - This event was considered of low significance.
    - Failure of the TDAFW did not prevent manual restart.
    - Motor driven AFW pumps were supplying adequate flow to the steam generators and no loss of safety function occurred.
- Corrective Action
  - Develop and implement a preventive maintenance program for SSPS cards
  - Review measures executed by the vendor of the SSPS cards to assure condition adverse to quality are promptly identified and corrected

EVENT 6 – PEACH BOTTOM UNIT 2

Automatic Trip due to an Electro-Hydraulic Control (EHC) System Malfunction

- Background
  - Due to an EHC circuit malfunction, which was the result of a low main steam line pressure, and an opened main turbine bypass valve, the primary containment isolation system (PCIS) was actuated. (Group I)
    - Reactor level decreased resulting in the actuation of the high pressure coolant injection, reactor core isolation cooling, and the alternate rod insertion (ARI) trip systems.
    - Group II and III PCIS isolations also occurred as reactor level decreased.

- Timeline
  - On December 22, 2004 at 0455 a reactor trip occurred.
  - 0530 - The PCIS Group II and III isolations were initially reset
  - 0540 - The trip and ARI initiation were reset.
  - 0750 - PCIS Group I Isolation was reset.

EVENT 6 – PEACH BOTTOM UNIT 2

Automatic Trip due to an Electro-Hydraulic Control System Malfunction

- Problem
  - Discrete solid state electronic component failure
- Cause
  - The cause of the EHC system to malfunction was due to a failed Pressure Regulator circuit card, supplied by Mechanical Dynamic and Analysis.
  - The circuit card was found to have excess solder which created a short across two traces of the card, causing a voltage drop.
- Safety Significance
  - There were no adverse safety consequences as a result of this event.
- Corrective Action
  - The defective card was replaced and the EHC system was tested to verify proper operation.

EVENT 7 – LIMERICK UNIT 1

Safety Relief Valve (SRV) Position Indication on the Remote Shutdown Panel Inoperable

- Background
  - During a refueling outage, a surveillance test of the SRVs from the Remote Shutdown Panel (RSP) was performed.
  - The red/open bulbs failed for the three RSP Safety Valves when the SRV solenoid was returned to the closed position (de-energize) following the open function (energize).
  - The loss of the indication did not affect the ability of the SRV to be operated.
- Timeline
  - This event occurred on March 19, 2006.

EVENT 7 – LIMERICK UNIT 1

Safety Relief Valve Position Indication on the Remote Shutdown Panel Inoperable

- Problem
  - Discrete fault design
- Cause
  - Fault design for the SRV control circuit at the remote shutdown panel.
- Safety Significance
  - There were no adverse safety consequences as a result of this event.
- Corrective Action
  - An MOV was added to the unit 1 circuit and the SRVs were tested satisfactorily.

QUESTIONS