
AREVA

Qualification of the Emergency Diesel Generator Digital Excitation System Upgrade for Comanche Peak SES

Presented by

Nissen Burstein and Dan Mikow, AREVA (formerly Framatome ANP, Inc.),

to IEEE PES/NPEC/SC-2 at Meeting 04-01, April 21 and 22, 2004, in New Orleans, LA

Purpose of the meeting

- **Briefing on CPSES Safety Related EDG Exciter Replacement Project**
- **Discuss Digital Portions of the design and approach, including 50.59 Evaluation**
- **Overall Conclusions**

Topics

- Modification Overview
  - Current System Design
  - Modified Design
- What is digital?
  - Safety-related Automatic Voltage Regulator
  - Class 1E SIPROTEC Multifunctional Relay
- Approach to Digital Design and Qualification

Modification Overview

- Current System Design & Problems
  - Why is this modification being performed?
  - Why digital?
- New System Design
  - There is no interaction with non safety equipment, therefore there are no isolation devices necessary
- Differences, advantages of the new design

Modification Overview

Current System Design

- Portec, Static Exciter Voltage Regulator (SEVR)
  - Portec components became obsolete in 1998
  - History of repetitive failures challenging the operability of the Diesel Generators
  - Existing spare components are being depleted
  - Analog system
    - Extensive maintenance is required to maintain reliability
    - No fault recording or diagnostic capabilities
    - Trouble-shooting is very time consuming

Modification Overview

Current System Design (cont.)

The current magnetics associated with the Portec SEVR system supplies more power (5% to + 15%) than is required; therefore, it is necessary to shunt away the excess power.

This is accomplished by SCRs controlled by the Voltage Regulator cards.

A characteristic of a shunt SCR system is that for most failures, excitation will go extremely high, resulting in a trip of the DG.

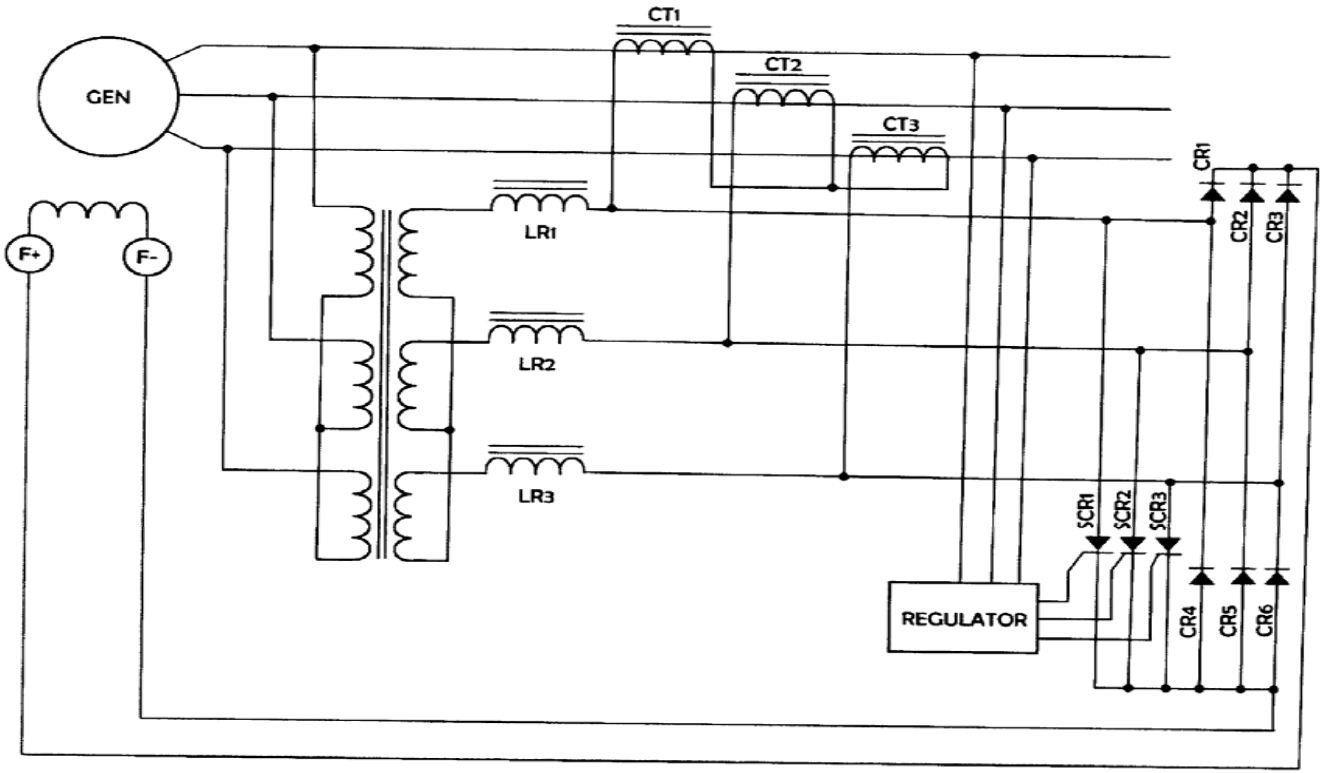
Modification Overview

New System Design

- Siemens Thyripart, static, compound excitation system
  - Component and engineering support through the life of the plant
  - Proven reliability
  - Digital system
    - Fail-safe analog back-up via magnetic portion of system
    - Self diagnostics and fault recording
    - SIPROTEC Multi-functional relay bypassed in Emergency Mode
    - Voltage precision achieved by the magnetics portion is within +/-5% of Tech Spec requirements of >6480V and <7150V
    - MasterDrive ‘tunes’ the generator voltage regulation to within +/-0.5%
      - Boost (increase excitation)
      - Buck (decrease excitation)
    - MasterDrive output monitored with over voltage and under voltage relays to trip MD if undesired voltage levels are sensed.

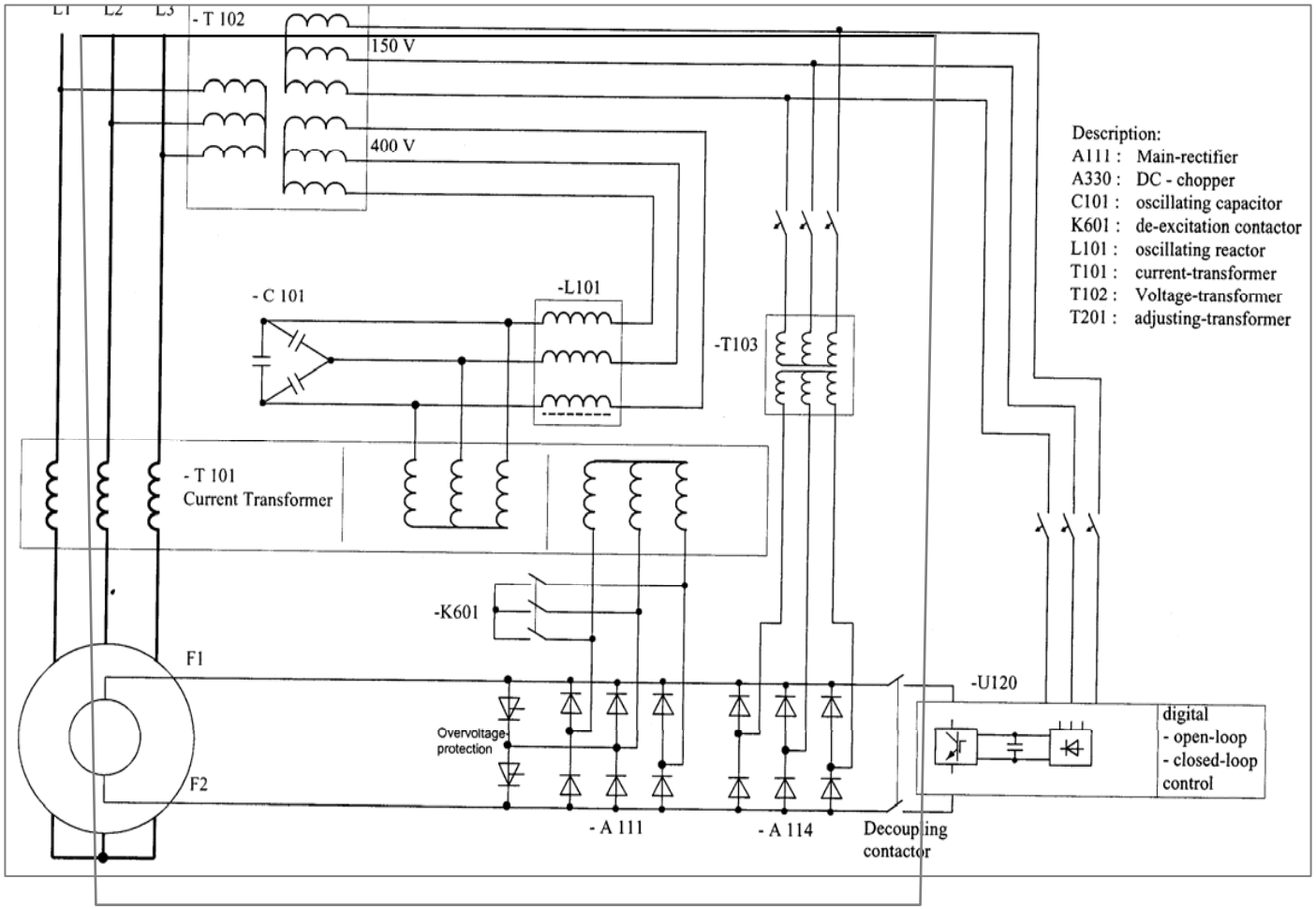
Modification Overview

Schematic of current design



Existing excitation system consists of three, single phase power transformers, two three phase sensing transformers, one 800/5 reactive current transformer, three power current transformers, 3 linear reactors, one three phase power output rectifier bridge with shunting Thyristor (SCRs), normal and standby automatic voltage regulators, a remote gate firing module, power driven pot (PDP), relays and control switches. Most of these components are obsolete and spare parts are no longer available.

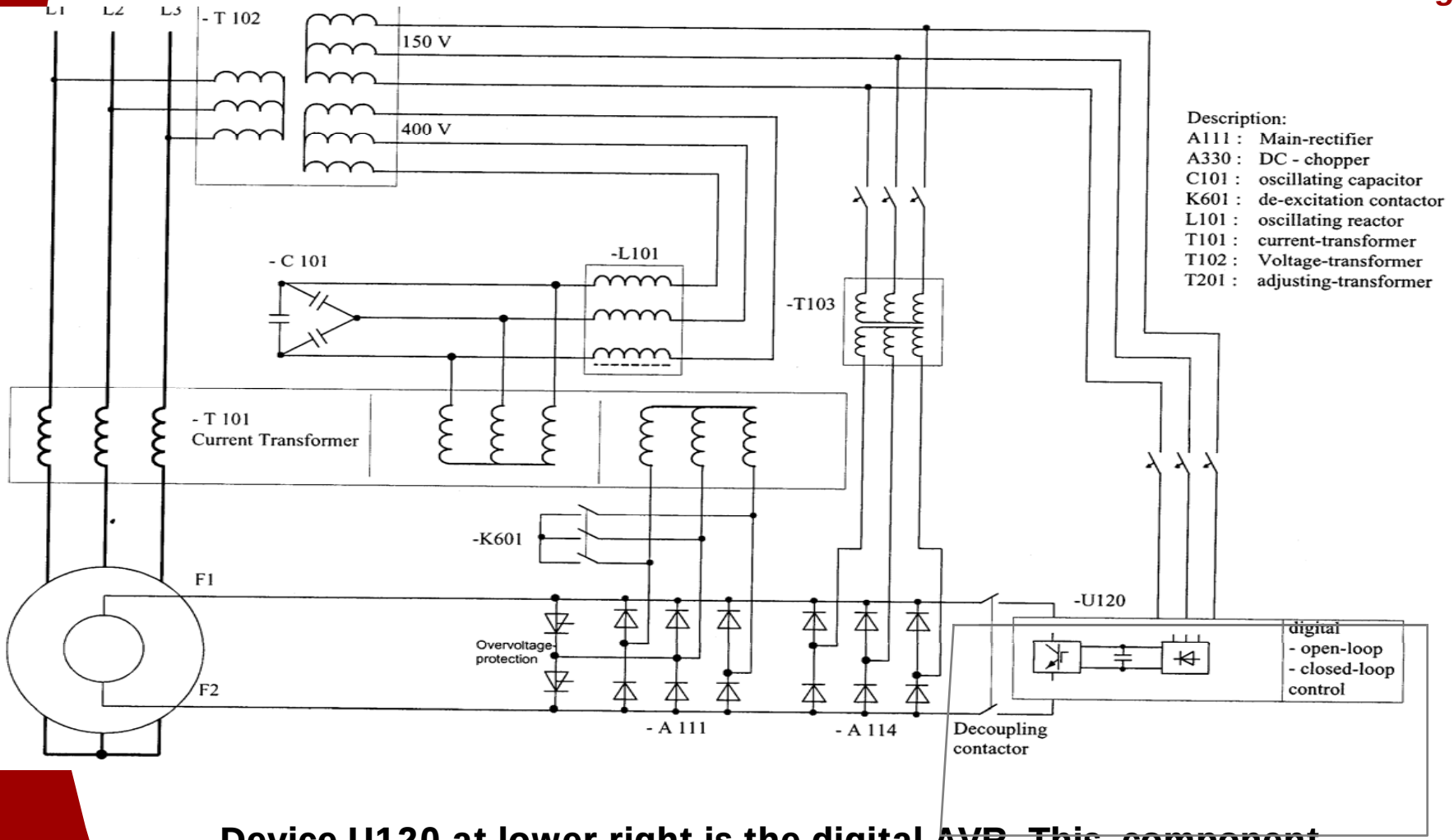
Modification Overview
Schematic of Modified Design



Devices T102, C101, L101, T101, A111, T103, A114 comprise the part of the new design called the "magnetics." These components produce rectified DC field current that is a function of DG no-load and load components capable of regulating DG output voltage to ±4.8 percent.

Modification Overview

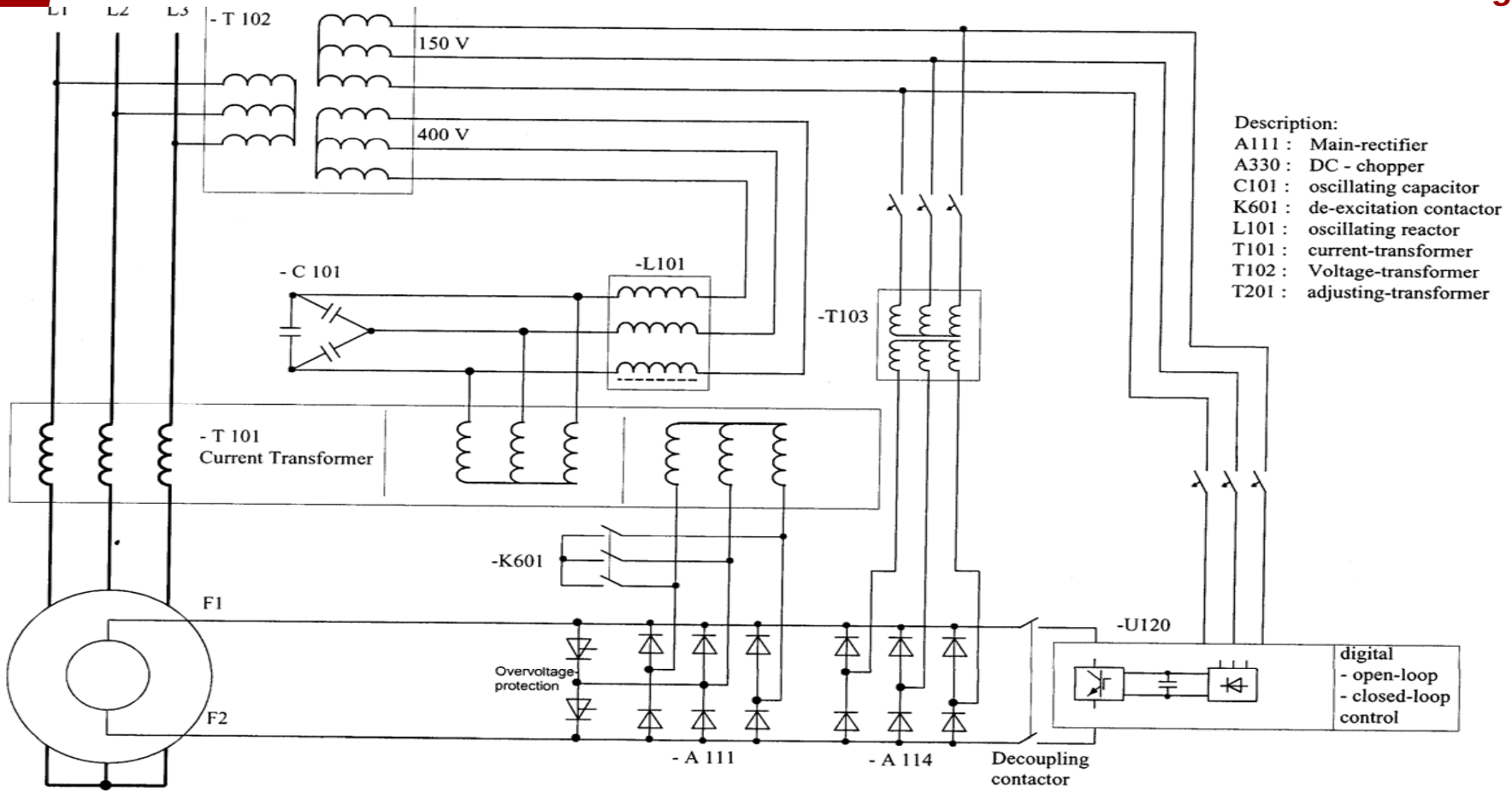
Schematic of Modified Design



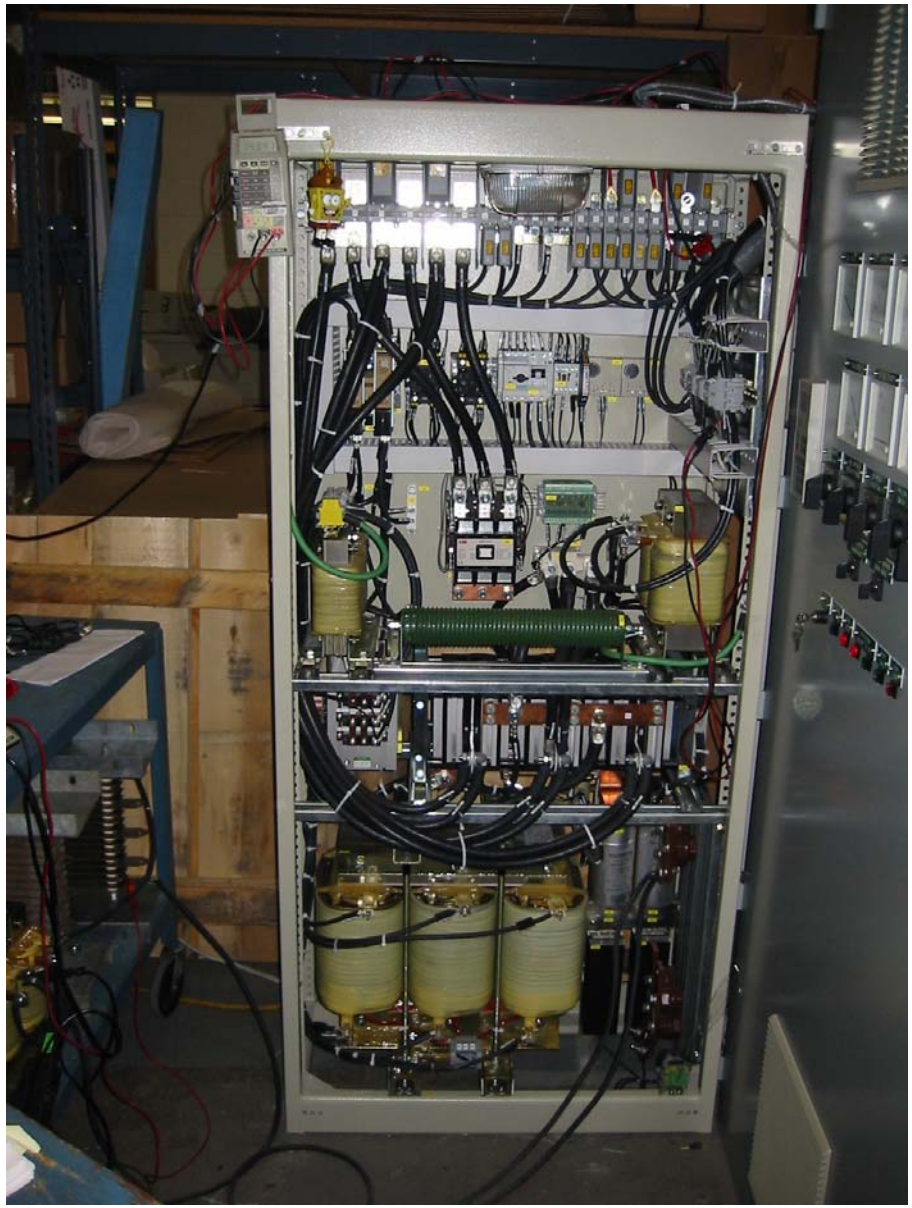
Device U120 at lower right is the digital AVR. This component produces rectified ±DC which boost (+) or bucks (-) output of "magnetics" allowing regulation of DG output voltage to ±0.5 percent, and allow raising and lowering of voltage for such functions as synchronizing to the grid.

Modification Overview

Schematic of Modified Design



In event digital AVR (U120) malfunctions, an over/undervoltage relay disconnects the AVR by opening the decoupling contactor.
Diesel generator continues to operate within Tech Spec voltage limits using the "magnetics" to supply field current but without ability to raise or lower voltage.



This is the rack containing the “magnetics.”

This is the AVR panel. The AVR equipment is here.

These are indications and controls of the new exciter controller on front of the AVR panel.

Safety-Related Digital AVR

- **CGD of Siemens Commercial Product**
  - **Frequency Drive Controller**
  - **Widely used as controller for variable-speed motors (estimated 350,000 applications)**
- **Function Performed**
  - **Provides ±DC current which boost/bucks output of "magnetics" to provide enhanced DG voltage regulation, and ability to raise/lower voltage (+/- 0.5% regulation)**
- **Safety Classification: Safety Related**

Safety-Related Digital AVR (conti.)

- **Digital Attributes:**
  - **Hardware/Software Requirements Specification**
  - **Qualification Plan, Process, & Results**
    - **CGD of EDG Exciter System**
      - **Traceability Matrix**
    - **Seismic Testing**
    - **EMI/RFI Testing**
    - **Environmental Testing**
    - **Failure Analysis**
      - **Common Mode Software Failure**
      - **Unintended Functions**
    - **Software V&V**
    - **Cyber Security Considerations**
  - **Design Control/Configuration Control**
  - **50.59 Evaluation Results for Digital Equipment**

CGD Process for Digital AVR

- CGD of AVR part of the overall dedication of the EDG Exciter System
- Digital AVR CGD meets the requirements of IEEE 7-4.3.2 and EPRI COTS CGD Guidelines for use in Safety Related Applications
  - Commercial Grade Surveys
  - Critical Characteristics
  - Qualification (seismic/environmental/EMI-RFI)
  - Unused/Unintended Functions
  - Common Mode Software Failures
  - FMEA
  - V&V in accordance with IEEE 1012 and RG 1.168
  - Functional Testing
  - Cyber Security Considerations
  - Design Control/Configuration Control
- Detailed requirements traceability matrix ensures customer specifications have been properly addressed, tested, and appropriately documented.
- Comprehensive CGD plan, procedures, and report
- Life Cycle Management Plan
  - FANP Appendix B Vendor
  - Part 21 Reporting

Environmental & Seismic Testing

> Environmental Testing

Operational testing conducted at 130°F ambient temperature conditions for a period of 7 days, high humidity, demonstrated that equipment remained fully operable under worst-case environmental conditions.

> Seismic Testing

Operational tests were conducted at the Trentec laboratory using the CPSES seismic spectra for the Diesel Generator Building. Demonstrated that equipment remained fully operable under worst-case seismic event conditions, including SQURTS levels.

EMI/RFI Testing

Operational EMI testing assessed equipment for emissions and susceptibility, including *low and high frequency conducted and radiated emissions*; *low and high frequency conducted and radiated susceptibility*; *Electrical Fast Transients, Surge Withstand Capability, Electro Static Discharge*. Testing demonstrated that equipment fully met requirements of the new NRC Reg Guide 1.180 and EPRI guidelines for EMI/RFI emissions and susceptibility at nuclear power generating stations.

Testing demonstrated that equipment operation will not be affected by EMI/RFI; nor will equipment emit EMI/RFI which will interfere with other plant equipment operation.

Failure Analysis

- **Overall Conclusions**
  - **System meets single failure criterion and system reliability is at an acceptable level**
  - **FMEA performed and comprehensively documented**
  - **No interface with non safety equipment**
  - **EDG Exciter system capable of providing excitation to the EDG under all known hardware failure conditions and modes**

Failure Analysis *(cont.)*

- **Common Mode Software Failure**
  - **Comprehensive analysis concludes that SWCMF does not impair the Thyripart safety function and there is adequate diversity and independence for the events analyzed.**
  - **IEEE 7-4.3.2-1993, Annex F on Abnormal Conditions and Events was reviewed. The ACEs that could affect the safety functions were identified, analyzed and results documented. All postulated ACEs have been eliminated by rigorous design of the system, or found not to be significant, nor have any impact on system performance. No impact on safety and safety functions.**
  - **Diverse equipment not impaired by postulated SWCMF and is available to effect the needed Reactor Trip and ESFAS Response**
  - **The design of the EDG Excitation System meets the requirements of HICB BTP-19**

Failure Analysis *(cont.)*

- Unintended Functions
  - **Several measures taken to enhance system reliability and prevent unintended functions**

- Unused Functions
  - **Unused functions do not affect the safety functions. The firmware contains software units that are not used.**
  - Only used function blocks have been dedicated. Unused function blocks do not affect the dedicated function blocks.
    - **Unused parameters do not inadvertently actuate and cause undesirable operation**
    - **Operating Experience proves unused functions do not affect dedicated (used) function blocks.**
    - **The unused function blocks can only be enabled by parameterization**
    - **Strict administrative controls over the access to the parameterization of this firmware are designed to prevent unused function blocks from being inadvertently enabled. Controls include:**
      - **Strict procedures that provide explicit guidance on how function parameters will be changed, verified and validated**
      - **Password protection prevents unauthorized access**
      - **Administrative controls in place to ensure that only properly trained individuals have access**
  - **In conclusion, there is no impact on safety functions. Administrative controls are imposed to ensure integrity and configuration control to prevent inadvertent use of unintended functions. By design, Siemens controller functions are independent, and are not automatically activated. Thus, there is no adverse impact of unused functions on the ability of the system to reliably perform its intended functions, including safety functions.**

Verification & Validation

- V&V Approach
  - Plan in conformance with RG 1.168 (IEEE 1012)
  - Process
    - Software Critical Functional Requirements Document
    - Software Requirements Matrix
    - Validation Test Plan/Procedure
    - Validation Tests
    - Discrepancy reporting/resolution
  - Results
    - Validation Test Reports
    - Final V&V Reports
- Summary & Conclusions
  - The software meets stated requirements and does not perform any unintended functions
  - The requirements and coding documents are adequate and current

Cyber Security Considerations

- **EDG Exciter system has no external connectivity to LAN or modem, and is a self contained system located in a vital area.**
  - **Strict design control, configuration control and change control process in place**
  - **All direct paths and indirect pathways have been analyzed**
  - **Password protection for parameter change functions via front panel display or via lap top connectivity**
  - **Communication ports for access are key locked**
- **FANP & Siemens Cyber Security program addresses virus checks, malicious code, user authorization, access control and network security**
- **Lap-top access is administratively controlled by CPSES**
  - **Dedicated lap top**

Design Control/Configuration Control

- Software under FANP configuration Control
  - Appendix B vendor with Part 21 responsibilities
  - Software archiving and release, per approved procedures
  - Software changes subjected to the same dedication process as original software
  - LCM for dedicated software in place
- End user functions limited to parameter changes using Station procedures
- Documentation provides hardware and software configuration, including parts ID and software/firmware version of AVR. For dedicated laptop, it provides parts ID, operating system, and resident software modules for AVR maintenance functions and anti-virus software.

10CFR50.59 Evaluation

- **10CFR50.59 screening limited evaluation scope to digital design only.**
- **Evaluation done in accordance with NEI 01-01** *Guideline on Licensing Digital Upgrades*.
- **Evaluation addressed the 8 criteria in 50.59(c)(2), and concluded:**
  - **New equipment serves same function as the existing analog system.**
  - **Consequences of equipment malfunction are the same as equipment being replaced.**
  - **Human-System interface is unchanged.**
  - **No new accidents, failure modes, or malfunctions are created.**
  - **Prior NRC approval is not required.**

SIPROTEC Multifunctional Relay

- **Function: Provides diesel generator protection for Volt-Hertz, Reverse power, Phase balance, Loss of field, Time Overcurrent, Field ground, Stator Temperature, Under frequency, provides Watt/VAR capabilities including data logging, and monitors DC Voltage, as required.**

- **Failure Analysis: For a failure/malfunction originating from relay, upon detection, an internal watchdog alarms and blocks relay outputs; in emergency mode all outputs of the relay are blocked by Class 1E relay. 1E function is to maintain circuit integrity, so that Diesel Generator remains operable despite relay failure/malfunction.**

- **EMI/RFI: relay poses no EMI/RFI challenge to the safety-related AVR or the overall EDG Exciter system**

SIPROTEC Multifunctional Relay (cont.)

- **10CFR50.59 Evaluation determines relay neither results in more than minimal increase in likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the FSAR, nor creates possibility for an accident of a type different than that previously evaluated in the UFSAR.**

- **Impact on EDG Exciter System: The relay has no impact upon the system performing its safety-related function because its diesel generator trip functions are disconnected by an Emergency Start/Run DG signal.**

Overall Conclusions

- **The dedicated commercial equipment, including the digital controller used in Safety Related application ‘CPSES EDG Exciter System upgrade’ is safe, reliable and fault tolerant. The design and qualified equipment meets all regulatory requirements set forth for use of this equipment in a safety significant application.**