Improving Security and Reliability at a Nuclear Station

David Parks - Entergy Grand Gulf Nuclear - Turbine / Generator System Engineer Qualified Design Engineering Instrumentation and Control – USA – dparks@Entergy.com

Mathew King – Siemens Application Engineer – USA – Mathew.King@siemens.com

Oscar Rozo – Siemens Application Engineer – USA – Oscar.Rozo@siemens.com

Leonardo Morales – Siemens Application Engineer – USA – Leonardo.Gonzalez@siemens.com

Eric Stranz – Siemens Business Development Manager – USA – Eric.Stranz@siemens.com

ABSTRACT

The age of almost all nuclear stations practically guarantees that the protective relays are a generation old. The continuation of replacing the broken with the obsolete reaches a practical limit and it becomes necessary to perform a complete protection upgrade. Protection engineers at the Grand Gulf nuclear station decided to take advantage of updating the protection to improve both the reliability and security of the system. The most straightforward way to improve both reliability and security in protection is through the use of a voting scheme. Instead of using a simple one for one replacement philosophy when going from electromechanical to microprocessor, Grand Gulf engineers took advantage of reduced cost and low CT / VT burdens in microprocessor relays. This upgrade improved the reliability and security of the complete generator and transformer protection scheme. This paper details the design used as well as the extensive factory testing to validate the scheme performance under all conditions. While nuclear stations have high requirements for both reliability and security the same can be said of any stations critical to the bulk electric system. This paper provides guidance and ideas for any designer for critical protection systems.

Existing Design and Problem Statement

The Grand Gulf nuclear plant, prior to the upgrade, consisted of more than twenty different protection relays covering the generator and transformer. These protection relays were obsolete electromechanical design and in many cases considered single point vulnerabilities (SPV). Situational awareness was limited and potential for false trips or failures was high. It was imperative a new system needed to be designed to ensure protection security, increase situational awareness and reduce maintenance testing through monitoring.

Entergy requirements

Considerations for the design of a protection system upgrade began early in 2015. The objective was to create a system that eliminated all SPV's, increase reliability, protection security, and minimize routine testing requirements. It needed to also provide easy access to system alarms and fault data to quickly diagnose faults. The protection relays selected had to be flexible to include a large quantity of I/O to implement a voting scheme with the additional CT and VT requirements for protection. The devices replaced the below protection functions:

- A, B, C Differential Protective Relays
- Generator Negative Phase Sequence Relay
- Generator Neutral Ground XFMR Time Overcurrent Relay
- Generator Phase Distance Timer Auxiliary Relay
- Low Frequency Generator Ground Fault Relay
- Generator Ground Fault Relay
- Generator Voltage Balance Relay
- Generator Undervoltage Relay
- Generator Voltage Balance Relay
- Generator Loss of Field Relay
- Generator Power Directional Relay
- Main Generator Auxiliary Time Delay Relay
- Main Generator Auxiliary Time Delay Relay
- Generator Phase Distance Relay
- Generator Volts/Hertz Relay
- Generator Volts/Hertz Relay
- Generator Power Directional Relay
- Main Generator Auxiliary Time Delay Relay
- Main Generator Auxiliary Time Delay Relay
- Generator Under Frequency Alarm Relay
- Generator Under Frequency Trip Relay
- Main Generator Auxiliary Time Delay Relay
- Load Rejection Relay (LRR)
- Unit Transformer Diff Phase Relay
- A,B,C – Main XFMR Differential Phase Relay
- Main Transformer Ground Overcurrent Relay

General Solution Approach

The approach on this project was to not only eliminate any single point vulnerabilities that could cause false trips but to create a much more secure protection scheme. The solution eliminated any legacy, unsupported devices (electromechanical relays) and enabled better metering, monitoring and visualization to aid in troubleshooting and fault diagnosis. Since outages are very expensive in terms of lost revenue and labor hours, the system is designed to minimize device testing by complying with the performance based NERC requirements. To accomplish this, a HMI for situational awareness was used as well as a continuous monitoring solution in compliance with PRC-005-2 testing requirements.

Solution explanation

The existing system at Grand Gulf was typical of generating plants built prior to1990 where individual mechanical relays provided single protection elements to cover the generator and transformer. This meant a total of twenty five relays provided protection for the generator, four relays for the transformer, and three for the overall unit. These relays were pure protection devices and provided no measurements, remote indications, or warnings. Picture 1 below shows the existing generator and transformer protection panels.

Picture 1: Existing generator and transformer protection panels

In the original scheme, each protection relay directly tripped one or more lockout relays which directly tripped the generator main breaker. These relays and circuits were designed without any redundancy and as such all the relay trips are single point vulnerabilities (SPV). This means failure or false trip of a single mechanical relay would trip the generator and because these relays are obsolete, downtime would be lengthy and cost to the plant operator would be extensive. Therefore the two primary design goals of the protection system upgrade project were to eliminate the single point vulnerabilities from each mechanical relay and increase overall security of the scheme.

The first goal was achieved by removing all existing mechanical relays and installing new multifunction digital relays in their place. This eliminated the possibility of obsolete parts for the foreseeable future and ensured the relays are maintainable however the single point vulnerabilities remained. So to eliminate the SPV's and achieve the second goal, multiple digital relays were installed and outgoing trips were arranged in a voting logic. Therefore all these previous vulnerabilities were removed and ensured a single relay failure or false trip would not be able to trip the generator which significantly increased the reliability of the scheme.

Given that the existing electromechanical relays only provided indication via a trip flag, the plant desired to utilize the new protection relays to increase the operational awareness from the protection system. To facilitate this goal, a human machine interface (HMI) was designed to pull data from each of the new protection relays and display this via a LCD screen at the panels. This meant each new relay must be capable of measuring various operands and sending this and indications via a communication port. In addition to the HMI computer and screen, a second computer was installed to maintain the relay

configuration software. This provided both a dedicated IT asset for configuration and analysis tool for pulling and reading fault records from the protection relays.

When selecting the protection relays, significant importance was placed on expandability of I/O points to support the voting logic, flexible protection functions for consolidated protection, availability of communications to support the HMI, and ability to support custom logic functions. These requirements resulted in the selection of four generator and two transformer protection relays from the Siprotec 5 family. The HMI and engineering workstation computers were compact industrial computers using the SICAM and WINCC/SCC software. This was due to their small footprint, processing power, and large support of communications protocols. After removing all legacy relays and installing the new relays and HMI screens, the resulting protection panels are shown below in picture 2.

Picture 2: Upgraded generator and transformer protection panels

Implementation

Reliability is generally understood to measure the degree of certainty that a piece of equipment will perform as intended. Relays, in contrast with most other equipment, have two alternative ways in which they can be unreliable. They may fail to operate when they are expected to, or they may operate when they are not expected to. This leads to a two-pronged definition of reliability of protection systems. A reliable protection system must be dependable and secure. Dependability is defined as the measure of

the certainty that the relays will operate correctly for all the faults for which they are designed to operate. Security is defined as the measure of the certainty that the relays will not operate incorrectly for any fault.

To improve both dependability and security of the Grand Gulf electrical protection system the 1-out-of-2 taken twice logic has been selected. The 1-out-of-2 taken twice logic contains two sets of two independent channels where the two sets are connected one with another according to the diagram below. In order to trip the unit at least two channels from different sets must operate at the same time.

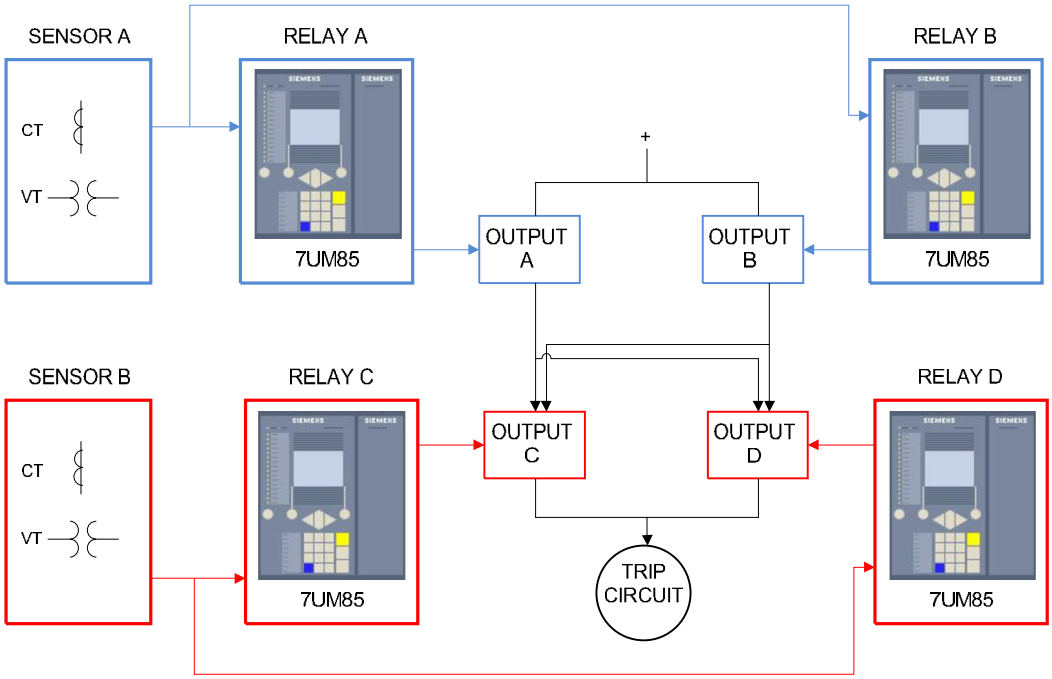

Figure 1 1-out-of-2 taken twice block diagram

The voting principle of a traditional 1-out-of-2 scheme improves the security of the protection system; consequently, if a spurious trip occurs in a relay the other is still capable of developing a safety function. However, the main disadvantage of a single 1-out-of-2 system (non-redundant) is the reduction of dependability. The figure 2 shows the 1-out-of-2 taken twice solution fault tree used in the project resulting in the improved protection security.

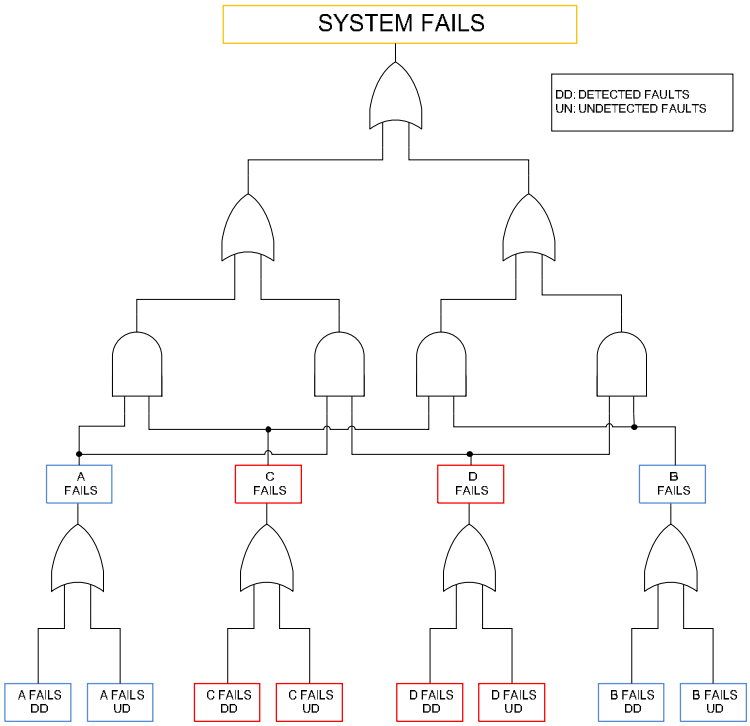

Figure 2 1-out-of-2 taken twice fault tree

Redundancy is a common approach selected to improve the dependability (assurance of trip) of the protection system, and most of the protection systems are designed with high dependability. High dependability means that a fault is always cleared by some relay on the system. The most straightforward way to improve dependability is through the duplication of critical components (redundancy). The figure 3 shows the 1-out-of-2 taken twice solution trip logic used in the project resulting in the improved protection dependability.

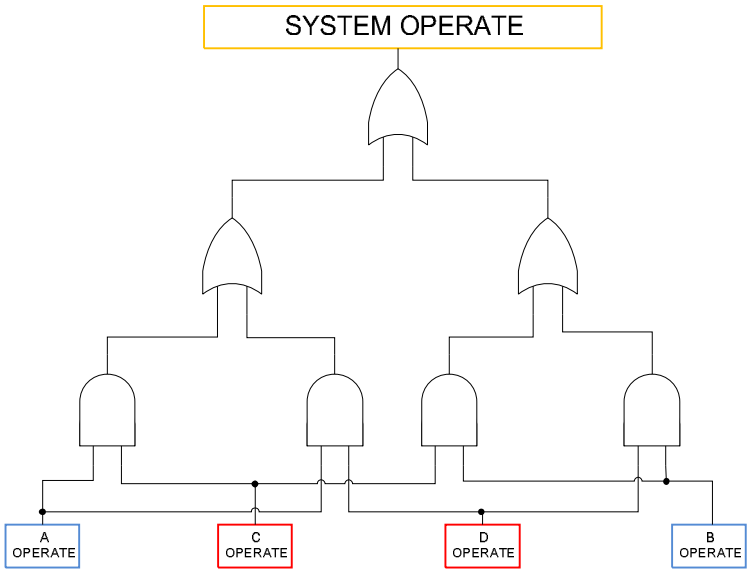

Figure 3 1-out-of-2 Taken Twice Trip Logic

The 1-out-of-2 taken twice scheme implemented at Grand Gulf protection system maintains a balance between security and dependability with the intention of increasing the reliability.

Redundancy of 100% Stator Protection

The following figure shows the 100% Stator Protection basic principle. An external low-frequency alternating-voltage source with 20 Hz injects a voltage of max. 1% of the rated generator voltage into the generator neutral point. If a ground fault occurs in the generator neutral point, the 20-Hz voltage drives a current through the fault resistance. The protection equipment determines the fault resistance from the driving voltage and the fault current. The basic principle described also detects ground faults at the generator terminals including the connected parts, for example, voltage transformers.

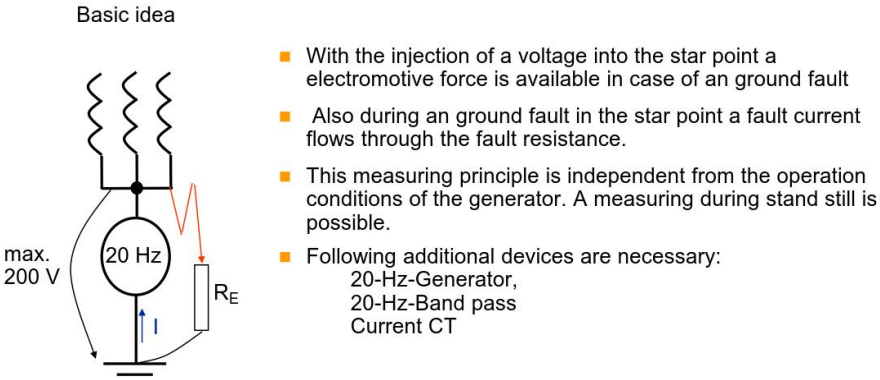

Figure 4: 100% Stator Ground Fault Basic Principle

To ensure the reliability and security of the 100% Stator Ground fault (100% SGF) protection system follows that of the other generator and transformer protections each relay provides the same function. External devices are needed to perform 100% SGF, and In order to keep similar reliability and security for the external devices, a Primary-Backup Failover switch was implemented for the 20 Hz generator and band-pass filter. The figure below shows the general scheme of Primary-Backup Failover switch.

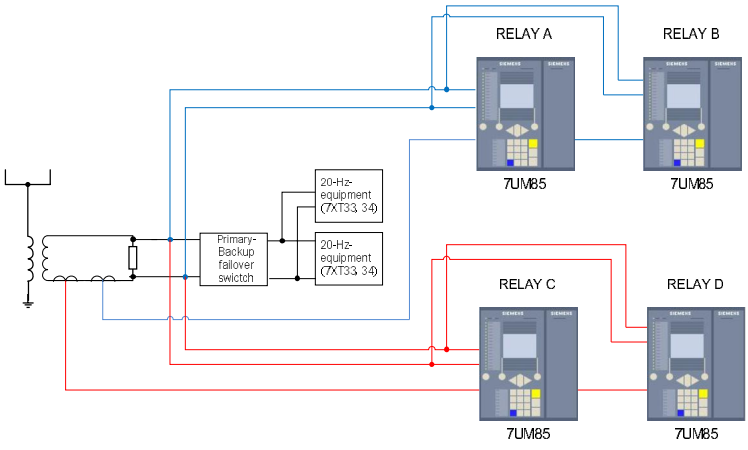

Figure 5 100% SGF Failover switch scheme

Load Rejection Relay System

As part of the existing protection system, a load rejection relay (LRR) was being used to detect large load rejections and stabilize the turbine by the turbine controller before trip speed is reached and the turbine over speed monitor responds. This rejection relay was a analog relay which along with being obsolete was a risk due to its analog components vulnerability to wear and degradation over its lifetime. Therefore it was determined to replace this relay along with the other mechanical protection relays. However since this relay provided a very specific protection function not standardized or readily available, it was necessary to use the plc function of the 7UM85 to recreate it.

The primary operating principle of the function is to detect a negative step in output power (MW) of the generator. This negative step must be greater than a set threshold and occur over a defined time when the generator is above a set power level. Depending on the magnitude of the step, a pulse length of configurable length is released to the hydraulic controller and secondary oil system. The speed of the function is critical to allow the pulse to act upon the secondary oil system much faster than the speed controller. Therefore response times must be on the order of a couple of cycles to be effective. Blocking of the function is provided by active supervision of the secondary VT system to provide additional security from erroneous simulation of negative power jump when VTs fail or are disconnected.

To implement the load rejection function, the built in continuous function chart (CFC), a very power programmable logic controller (PLC) inside the SIPROTEC relays was used. By using the already existing power measurands and CFC calculation blocks, the delta power jump can be easily calculated. This delta power indication was then fed into combination logic and timing CFC blocks to determine the timing and blocking functions. To achieve the fast response time required, the fast based high priority CFC charts were used for measurement calculation and processing along with parallel staggered calculation engines. This allows for a measurement windows of 3 cycles and a resulting response time of 20-60 msec.

To ensure the reliability and security of the load rejection protection system follows that of the other generator and transformer protections, each 7UM85 relay provides the same LRR function. The LRR output contact of each 7UM85 relay was then combined in the same one out of two taken twice logic as before but an additional failure over measure was taken. If any condition occurs that takes down one of the two sets, the output contacts are re-arranged and the resulting logic transforms to one out of two tripping.

PRC-005-2 Continuous Monitor (Performance Monitor)

The six protection relays used in this project are designed to communicate their measured values and status points to the Protection Monitor System (PMS) which resides on the same hardened computer as the HMI. The PMS is fitted with communications, soft PLC functionality and algorithms associated with PRC-005-2 performance based continuous monitor. Current and Voltage signals measured by protection relays are continuously monitored by this system and verified via comparison to a redundant protection relay. The PMS alarms for unacceptable errors or failure between the two devices. This system is designed within compliance of NERC PRC-005-2 Table1-1 and 1-2.

Since a continuous monitor solution was used on this project the six year interval testing defined in the periodic time based requirement of the standard is now extended to every 12 years in compliance with the performance based monitoring requirements.

Human Machine Interface (HMI)

The protection system is utilizing Ethernet technology for communication of information from devices to the HMI system. The devices are connected and communicate through the network using the communications protocol IEC-61850 MMS. This protocol brings real time data from the protection relays to the PMS software where it is compared and normalized and then sent to the HMI for complete situational awareness of the electric system.

Dynamic/Static Reports and Fault Records

The microprocessor based protection relays used in the project are fitted with a Network Interface Card (NIC) that is capable of redundant communications schemes. These NIC cards are also configured with IEC-61850 MMS communications. The IEC-61850 MMS communications are a key component for use in the HMI and PRC-005-2 performance based continuous monitor.

MMS is a communications protocol that utilizes a so called “Report” mechanism to push measured values and status information upon value change rather than wait for polling time intervals. These reporting mechanisms can be defined to behave in different ways. One configuration option is to utilize Static or Dynamic reporting. Static reporting is a pre-defined set of variables assigned to a data set which are assigned to a report. If any change is required at the PMS or HMI to include new signals from the protection relays a new configuration file would need to be loaded to the protection relay to represent this change.

Dynamic reporting was selected to be used in this project due to its flexibility. Dynamic Reporting utilizes the PMS or data concentrator to create data sets and reports for the end devices. The data concentrator simply updates the IED’s dynamically with this data set and report configuration. This eliminates the need to reload devices every time a new variable is needed. In Nuclear facilities small changes require extensive amounts of documentation, procedures and planning. Dynamic reporting helps to minimize these changes.

The IEC-61850 MMS protocol also includes an in built file transfer mechanism for Comtrade fault records. Where this is an optional piece of the IEC standard the selected relays have this capability and this feature was implemented as part of the project. All Comtrade fault records generated on the protection relays are auto-collected by the PMS utilizing this file transfer mechanism.

Security

Security was a significant concern when designing the system employed at Entergy Grand Gulf. Specifically the protection system is completely isolated from remote connected networks and not configured or connected to any wireless access points to prevent outside access. The network Ethernet switches spare or unused ports have been disabled to prevent transient connections from infiltrating the system. The hardened computers used in the project have a physical key access as well as role based security for a two factor authentication as described in FERC Order No. 706, Paragraph 572 .Relay alarms are generated when devices are being programmed as well as non-volatile user event log generation for settings changes, invalid login attempts etc. In addition, the protection relays have complex password and role based access functionality to further secure the system. The solution implemented met the strict Entergy procedure and NEI-08-09 cyber security requirements needed for implementation.

Testing

The purpose of the testing was to ensure functionality of the voting scheme and the generator and transformer protection relay settings according to the final coordination study for correct operation of all possible power system conditions and disturbances such as generator faults.

In order to optimize the factory acceptance tests (FAT) and reduce commissioning time the factory testing was split into protection only type testing and voting scheme testing. Here all protection element coordination times for all relays were tested simultaneously and verified independently. The voting scheme was tested independently of protection coordination tests.

For the protection element coordination tests, the setup of the FAT was to connect the current inputs of the relays in series through the test switches to simulate the same current in all relays. The relay voltages were connected in parallel to the test switches. The protection test consists of testing function by function on all relays at the same time and monitoring the operation time of each relay separately. Using a test set the trip operation time of each relay is monitored separately. During cold commissioning, all protection element settings were verified to the coordination study and therefore individual protection element injection testing was not necessary. The voting scheme was tested by isolating individual relays via test switches and performing single function tests. All possible trip combinations and relay failures were performed. See figure 6

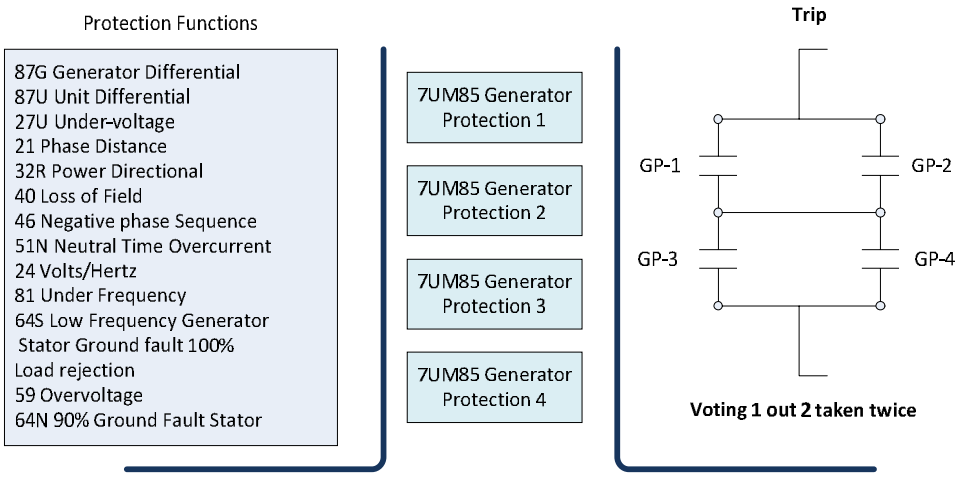

Figure 6- Generator Protection Scheme and Functions

The benefit of testing all generator and transformer protection relays with the final settings provided by the coordination study during the factory acceptance test (FAT), is the significant amount of time reduced during the cold commissioning. This was because the cold commissioning time was optimized and only required hardware testing of the relay binary inputs, binary outputs and analog injections. The relays ability to show valuable information on the front display such as current and voltage per function and digital inputs/outputs status also improved the time duration of the test.

Relay differential protection were tested the same way as the generator protection by verifying the voting scheme and trip operation time. It is important to mention that the relay 7UT87 was configured with two 87 differential functions running in parallel on the same relay.

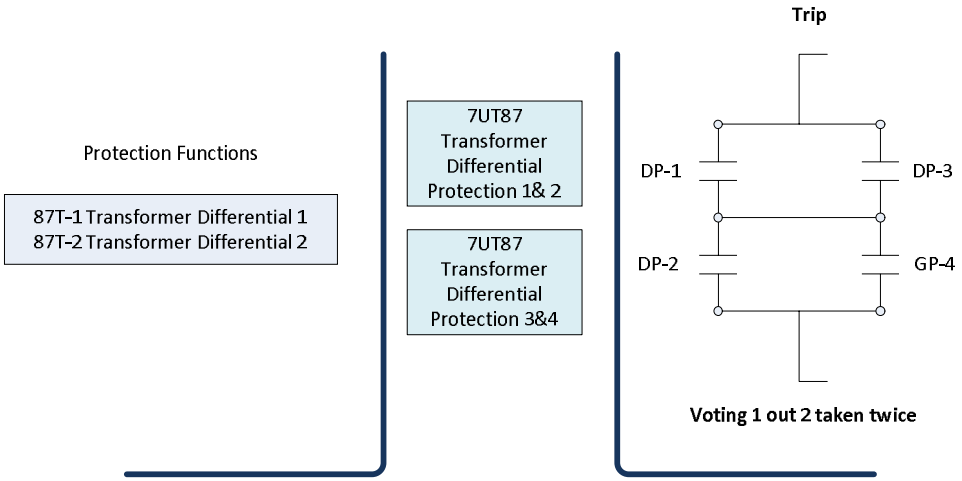

Figure 7- - Differential Protection Functions used per Relay

Conclusion

The project discussed in this paper went live July 2018. By replacing the mechanical relays and incorporating a voting logic, the single point vulnerabilities were eliminated and the reliability of the protection system was substantially increased. The operational value and return on investment was substantial. Some of the additional protection upgrade benefits are:

- Increase of Dependability and Protection Security
- 40 Components reclassified as non-Single Point Vulnerabilities
- Extension of NERC PRC-005-02 preventive Maintenance tasks
- Availability of Sequence of Event Data
- Time Synchronized protection via GPS
- Situational Awareness via relay display and HMI

References

NERC PRC-005-2 https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-005-2.pdf

FERC Order No. 706 Paragraph 572 https://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf

Power System Relaying – Fourth Edition – Stanley H. Horowitz, Arun G. Phadke

Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems- Yang Xu