cigre | PARIS 2022

Georgia Institute of Technology

Study Committee B3

Substations & Electrical Installations

Paper ID_10207

Resilient Cyber Secure Centralized Substation Protection

Athanasios P. MELIOPOULOS*, GIT, USA, George J. COKKINIDES, GIT, USA, Paul MYRDA, EPRI, USA, Evangelos FARANTATOS, EPRI, USA, Ramadan ELMOUDI, NYPA, USA, Bruce FARDANESH, NYPA, USA, George STEFOPOULOS, Boston Government Srvs, USA, Clifton BLACK, Southern Company, USA,

Motivation

- Protection systems use numerical, multifunctional, multi-dimensional, communications-enabled relays leading to complex protection systems. Statistics indicate about 10% protection mis-operations many times leading to major system disturbances
- Technologies are needed to eliminate the root causes of P&C unreliability

Method / Approach

The paper discusses a new approach to deal with the above mentioned issues. We introduce:

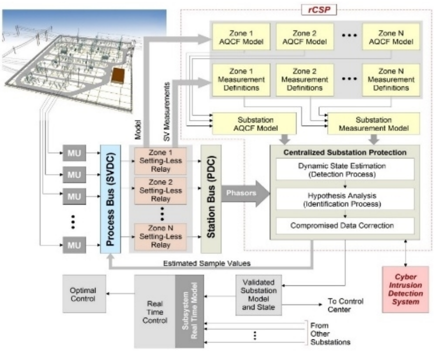
- A state estimation based protection (a.k.a. setting-less protection) that does not require coordination with other protection functions;
- A supervising system to continuously assess the correctness of the data going into the relays via a substation wide dynamic state estimation.
- When data are compromised (hidden failures, cyber attacks, P&C failures) the system identifies the root cause and the compromised data. Subsequently, it takes automatic corrective action to replace corrupted data with estimated values, thus allowing the P&C system to operate normally; at the same time sends messages to operators for repairs.

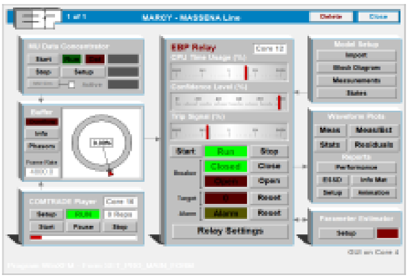
Objects of Investigation

Develop a resilient and secure centralized substation protection system that

- mitigate the main root causes of relay mis-operations
- Introduce the setting-less relay technology which (a) reduces complexity, (b) eliminates the need for coordination among protection functions
- Eliminate the effects of hidden failures and P&C failures by (a) detection of hidden failures and (b) self-healing by identifying compromised data and replacing them with estimated values, while it sends a message to operators with the exact location of the hidden failure for repair.
- Detect and protect against cyber-attacks that compromise data and/or insert malicious commands; both may result in protection mis-operations.

Experimental Setup & Test Results


rCSP
Zone 1 AQCF Model
Zone 2 AQCF Model
Zone N AQCF Model
Zone 1 Measurement Definitions
Zone 2 Measurement Definitions
Zone N Measurement Definitions
Substation AQCF Model
Substation Measurement Model
Model
SV Measurements
MU
MU
MU
MU
Process Bus (SVDC)
Zone 1 Setting-Less Relay
Zone 2 Setting-Less Relay
Zone N Setting-Less Relay
Station Bus (PDC)
Phasors
Centralized Substation Protection
Dynamic State Estimation (Detection Process)
Hypothesis Analysis (Identification Process)
Compromised Data Correction
Estimated Sample Values
Cyber Intrusion Detection System
Optimal Control
Real Time Control
Subsystem Real Time Model
Validated Substation Model and State
To Control Center
From Other Substations



Discussion

- System has been installed in three substations of Southern Company and two of NYPA
- In laboratory factory testing has successfully detected and corrected hidden failures and cyber attacks.

Conclusion

Centralized Substation Protection is possible today with present technology and offers many advantages and solutions to known protection gaps. First, it provides the technology to validate the data streaming into relays, thus ensuring the reliability of the protection system. Second, it provides the technology to detect hidden failures, data attacks, and other disturbances and at the same time, utilizing estimated quantities, enables the continuous and reliable operation of the protection and control system in the presence of anomalies such as hidden failures and data attacks

Study Committee B3

Substations & Electrical Installations

Paper ID_10207

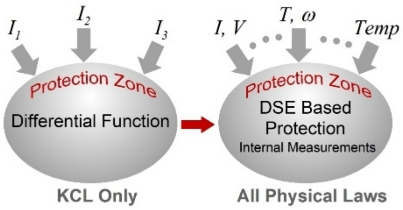
Resilient Cyber Secure Centralized Substation Protection

Athanasios P. MELIOPOULOS*, GIT, USA, George J. COKKINIDES, GIT, USA, Paul MYRDA, EPRI, USA, Evangelos FARANTATOS, EPRI, USA, Ramadan ELMOUDI, NYPA, USA, Bruce FARDANESH, NYPA, USA, George STEFOPOULOS, Boston Government Srvs, USA, Clifton BLACK, Southern Company, USA,

Estimation Based Protection (EBP)

The basic idea of the EBP has been inspired by the differential protection function (no coordination needed), but it is different than differential protection, which is depicted in the figure. In differential protection, the electric currents at all terminals of a protection zone are measured, and their weighted sum must be equal to zero (generalized Kirchhoff's Current Law(KCL)). In EBP, all existing measurements in the protection zone are utilized, i.e. currents and voltages at the terminals of the protection zone, as well as voltages, currents inside the protection zone (as in capacitor protection) or speed, temperature and torque in case of rotating machinery or any other internal measurements

Dynamic state estimation is used to determine that the device (protection zone) matches the model of the protection zone and therefore there is no internal fault. Otherwise an internal fault is asserted and the relay acts.


I_1 I_2 I_3

Protection Zone

Differential Function

KCL Only

I, V T, ω $Temp$

Protection Zone

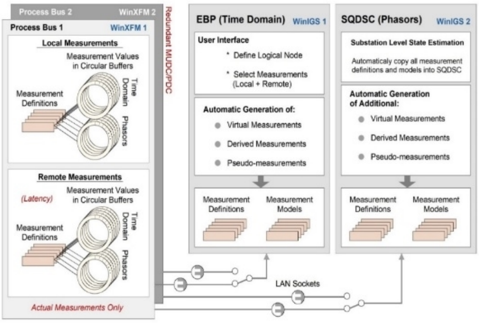
DSE Based Protection

Internal Measurements

All Physical Laws

Process Bus Management

The process bus manages the sample values streaming from the merging units. All sample values are time aligned, the validity of their time tag is assessed, and their physical location (i.e., the physical quantity they represent) is objectified into a mathematical model so that it can be interpreted correctly by upstream users .


Process Bus 2 WinXFM 2

Process Bus 1 WinXFM 1

Local Measurements

Measurement Values in Circular Buffers

Measurement Definitions

Time Domain

Phasors

Remote Measurements

(Latency)

Measurement Values in Circular Buffers

Measurement Definitions

Time Domain

Phasors

Actual Measurements Only

Redundant MUDC/PDC

EBP (Time Domain) WinIGS 1

User Interface

- Define Logical Node
- Select Measurements (Local + Remote)

Automatic Generation of:

- Virtual Measurements
- Derived Measurements
- Pseudo-measurements

Measurement Definitions

Measurement Models

SQDSC (Phasors) WinIGS 2

Substation Level State Estimation

Automaticaly copy all measurement definitions and models into SQDSC

Automatic Generation of Additional:

- Virtual Measurements
- Derived Measurements
- Pseudo-measurements

Measurement Definitions

Measurement Models

LAN Sockets

P&C Supervision by Substation Wide DSE

- As with any relaying scheme, EBP relays are also vulnerable to any false input data, independently of the source of errors, i.e. hidden failures, failures in instrumentation circuits, cyber attacks, missing data, etc.
- The substation-wide dynamic state estimation module operates on the entire measurement set of the substation. The information flow from the EBP relays to the substation wide state estimator is illustrated in the Figure, see block on the right of the figure designated as 'SQDSC (phasors)'.
- The goodness of fit between the measurements and the substation model is computed via the well-known chi-square test which calculates the probability of goodness of fit between the measurement and the substation model. A probability of 0.1 or below indicates existence of an abnormality. This condition triggers the hypothesis testing and the self-healing process.

Hypothesis Testing

- It is initiated when the dynamic state estimation has declared the existence of data abnormality
- A set of hypotheses are created and then tested sequentially: (a) occurrence of a protection failure, (b) occurrence of power fault(s) in a protection zone, and (c) simultaneous occurrence of a faulted protection zone and a protection failure.
- When a hypothesis is tested positive, the process is terminated.

Data Self-Healing

This task is triggered when the substation dynamic state estimation has identified the compromised data via hypothesis testing. For each compromised datum identified, the mathematical model of the substation is used to compute what this datum should be. Then, the values is streamed into the process bus to replace the compromised value.

CIGRE | PARIS 2022 Georgia Institute of Technology

Study Committee B3

Substations & Electrical Installations

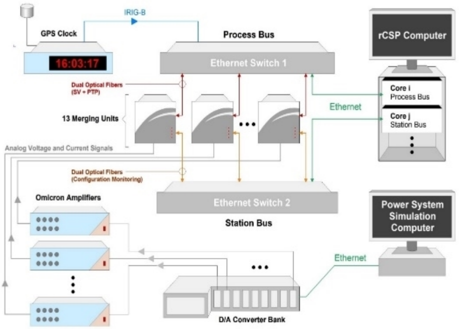
Paper ID_10207

Resilient Cyber Secure Centralized Substation Protection

Athanasios P. MELIOPOULOS*, GIT, USA, George J. COKKINIDES, GIT, USA, Paul MYRDA, EPRI, USA, Evangelos FARANTATOS, EPRI, USA, Ramadan ELMOUDI, NYPA, USA, Bruce FARDANESH, NYPA, USA, George STEFOPOULOS, Boston Government Srvs, USA, Clifton BLACK, Southern Company, USA,

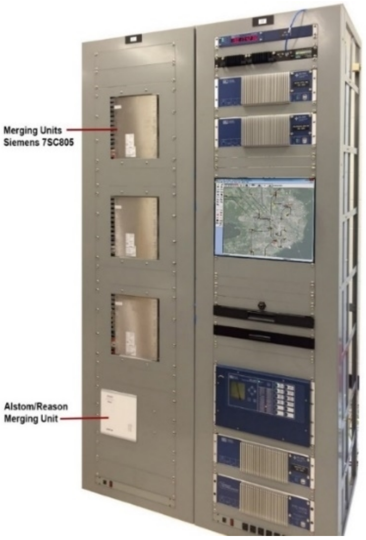
Laborator Testing (Factory Testing)

- rCSP has been tested in the laboratory with hardware in the loop
- Laboratory setup is given in Figure below
- Laboratory setup enables real time operational testing of rCSP.



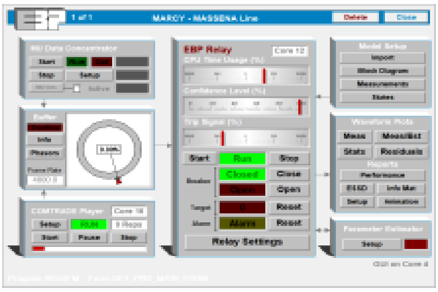
Field Installation

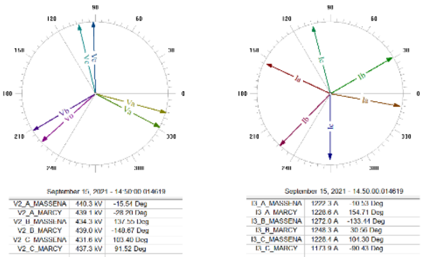
- rCSP has been installed on three Southern Company substations. One installation is shown below.



EBP Relay Interfaces / Relay Performance

- EBP relay is a new paradigm for protection which provides useful information about the protection zone health in addition to the protection function.
- EBP relay user interface (first figure below) allows the user access to many visualizations of protection zone operation (second figure below)
- Performance is quantified with the confidence level that the protection zone is healthy. A single visualization shown in the paper captures the health of the protection zone.





September 15, 2021 - 14:50:00.014619

V2_A_MASSENA	440.3 kV	-15.54 Deg
V2_A_MARCY	439.1 kV	-28.20 Deg
V2_B_MASSENA	434.3 kV	137.55 Deg
V2_B_MARCY	439.0 kV	-148.67 Deg
V2_C_MASSENA	431.6 kV	103.40 Deg
V2_C_MARCY	437.3 kV	91.52 Deg

September 15, 2021 - 14.50.00.014619

I3_A_MASSENA	1222.3 A	-10.53 Deg
I3_A_MARCY	1228.6 A	154.71 Deg
I3_B_MASSENA	1272.0 A	-133.44 Deg
I3_B_MARCY	1248.3 A	30.56 Deg
I3_C_MASSENA	1228.4 A	104.30 Deg
I3_C_MARCY	1173.9 A	-80.43 Deg

Conclusion

- The technology exists today to supervise the protection and control system of the substation and verify that input data to protective functions are valid.
- Hidden failures and other failures of the P&C system can be detected and their effects corrected.
- Cyber-attacks that alter data are detected and their effects can be corrected by quarantine compromised cyber assets for further disinfection.