«SO UPS», JSC

S.1.1-1. Selective Backup Protection for AC HV and EHV Transmission Lines

Jorge Cardenas
GE Digital Energy
Spain

Keywords: *System Integrity, Synchrophasor (PMU), Zone 3, Backup Protection, Node, Super node*

Abstract:

The paper describes a new vision of backup protection, focussed the application on transmission lines (it can be applied also in other areas extending the criteria). One of the major today problems in HV Transmission Systems is remote backup correct operation. The normal practice is the Zone 3 use, but this philosophy presents limitations that have caused several blackouts, because no desired operation caused mainly by line overloads. We can define in the grid Super nodes with the corresponding overlaps, extending the coverage that normally exists for bus protection in Nodes.

As a Super Node is perfect balanced during normal operation (in a first stage we will not considered the charging line effect), differential criteria can be used to detect any internal fault in a similar way as we do with a Node but in this case, using PMU´s as sensors. The main difference is in the operation time that in case of Super node will be time delayed because it is implemented as backup protection.

Introduction:

Overreaching distance relays tripping under load or under relative complex network topologies have played a part in many major blackouts. Here some examples

On November 9th, 1965 in USA, distance relays have been identified as tripping undesirably on line loading during significant system events. A backup distance relay initiated the November 9th, 1965 blackout when it tripped on load on one of five 230kV lines out of the Sir Adam Beck No. 2 Hydroelectric plant on the Niagara River in Ontario. The remaining four lines loaded up and tripped by their respective backup distance relays immediately thereafter. Those relays where set with a load pickup of 375MW to provide stuck breaker protection for breakers at the remote Burlington, Ontario substation. The relays load pickup was significantly below the loading capability of the protected lines.

On August 14, 2003 blackout in USA is the most notable, recent event in North America demonstrating tripping operations by distance relays during overloads.

On November 4th, 2006, distance relays have been identified as tripping on line loading during significant system events. A distance relay on the Wehrendorf end of the Wehrendorf-Landesbergen 380kV transmission line in North Germany operated on load during one of the most severe and largest disturbances ever to occur in Europe. More than 15 million European households lost service and the UCTE system was split into 3 islands. It was concluded that the distance protection operated as designed and might have prevented an even more severe blackout as their operations resulted in the system separating in desirable pieces. [1]

PRINCIPLES OF PROTECTIVE RELAYING

To achieve the objectives specified in the Philosophy of Protection, everyone connected to the system shall agree to install and maintain protective systems that have the following attributes:

1. Reliability - dependably detects and clears all types of electrical failures and still provides essential security against incorrect operations.
2. Selectivity - maintain continuity of service through the isolation of only the faulted parts of the system.
3. Speed - provide operation in the fastest time possible, consistent with 1 and 2 above.
4. Simplicity - install the minimum amount of equipment and circuitry to achieve the above.

Jorge Cardenas, GE Digital Energy, Spain, Email: jorge.cardenas@ge.com, phone: +34661410313

Dependability and Security

Reliability is a product of two factors; dependability and security. For relay system protection, dependability is defined as the ability to trip for a fault within its protective zone while security is the ability to refrain from tripping when there is no fault in the protective zone.

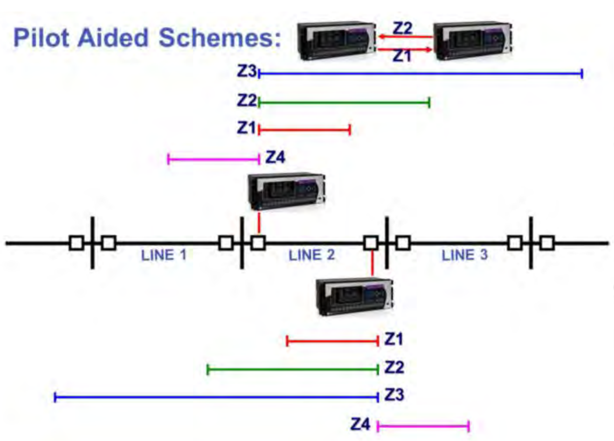
While not practical to use, it could be of interest to illustrate the concepts by looking at the two extremes; 100% dependability and 100% security. 100% dependability would be achieved by a protection system that is in constantly tripped state, hence there is no possibility that there would be a fault that would not be detected. 100% security would be achieved by disabling the protection system entirely so that it could not trip. From this we can see that while high dependability and high security are desirable, they will both have to be less than 100%. Generally, an increase in dependability will decrease security, and vice versa. However, measures to increase dependability may not penalize security to an equal degree and the aim of a protection system design is to find the optimum combination of the two factors in order to provide adequate reliability of the protection system.

Redundancy is defined as ‘the existence of more than one means for performing a given function’. It is obvious that protective relay system dependability can be increased by added redundancy as if one of the systems does not trip for an in-zone fault, a redundant system may. Security on the other hand, is generally decreased by increased redundancy as there are added devices in the system that may trip when not called upon to do so. However, redundancy does not influence dependability and security to the same degree.

Actual protection backup philosophy in HV and EHV Transmission Lines

Backup protection philosophy for line protection basically has not changed since the time that distance protection starting to be used as main protection for Transmission lines. That means, more than 60 years ago.

When Distance Protection is used, worldwide, it is accepted and standardized the protection scheme shown in the Figure 1.



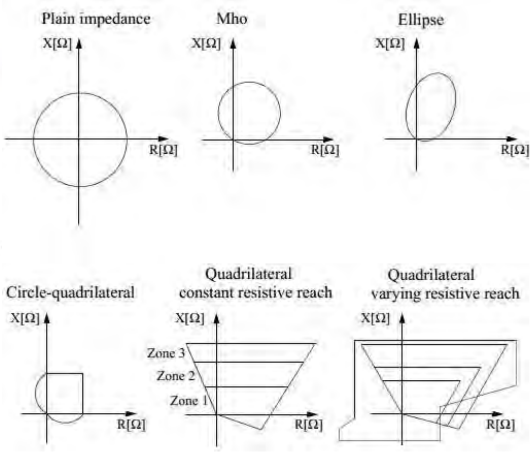


Figure 1. Stepped Distance complemented with Pilot Aided Schemes

Relay characteristics

Now, any faults that occur on the protected transmission line will be detected by the zones of protection on the relay at each end. These relays will then proceed to open the breaker and clear the fault from their own respective end of the line.

Similarly, each relay will also have ground stepped distance zones of protection, which are identical to that of the phase stepped distance zones. The difference being that the ground distance element is used to detect single phase-to-ground faults

This scheme is complemented with a Pilot Aided Scheme (POTT, PUTT, Blocking) to cover 100% of the line with fast trip using Z1 and Z2. Z4 is used as complement for Blocking Schemes on in Hybrid Schemes (POTT with weak infeed detection) and time delayed as busbar backup protection.

Zone 3 (Z3), the third zone of protection is set to over-reach past the end of the second adjacent transmission line. This third zone is used to act as a remote backup for that next adjacent transmission line, in case the protection on that transmission line fails. To act as a backup and if the impedance of Line 1 and 2 are the same, Zone 3 is usually set to extend to 220%, which is the same point as Zone 2 of the adjacent transmission line. Zone 3 must have a time delay that is longer than the operate time of Zone 2 of the adjacent transmission line. This time delay is typically 1 second.

Limitations of Distance Measuring Criteria

(1) With only local measurements, and a small time window, it is difficult to determine fault impedance accurately. For example, if the fault has an impedance ($Z_f \neq 0$), then the derivations of previous lectures are no more exact. The impedance seen by the relay R_1 (fig. 2) for fault F also depends upon the current contribution from the remote end.

(2) There are **infeed and outfeed effects** associated with working of distance relays. Recall that a distance relaying scheme uses only local voltage and current measurements for a bus and transmission line. Hence, it cannot model infeed or outfeed properly.

Consider the operation of distance relay R1 for fault F close to remote bus on line BC (fig. 2).

Due to the configuration of generators and loads, we see that $\vec{I}_{BF} = \vec{I}_{AB} + \vec{I}_{ED}$

Hence,

$$V_{R1} = \vec{I}_{AB} Z_1 + x Z_{l2} \vec{I}_{BC}$$

$$= (Z_1 + x Z_{l2}) \vec{I}_{AB} + x Z_{l2} \vec{I}_{ED}$$

$$\frac{V_{R1}}{\vec{I}_{AB}} = Z_1 + xZ_{l2} + xZ_{l2} \frac{\vec{I}_{ED}}{\vec{I}_{AB}} \qquad (1)$$

Thus, we see that the distance relay at R1 does not measure impedance $(Z_1 + xZ_{l2})$. If there is an equivalent generator source at bus E, then it feeds the fault current. Thus I_{AB} and I_{ED} are approximately in phase. This is known as **infeed effect**. From equation (1), it is clear that infeed causes an equivalent increase in apparent impedance seen by the relay R_1.

From the relay's perspective, the fault is pushed beyond its actual location. This itself does not sacrifice selectivity. In other words, relay R_1 perceives fault to farther away from than its actual location and depending of setting and network topology, fault can be detected or not by backup protection zones.

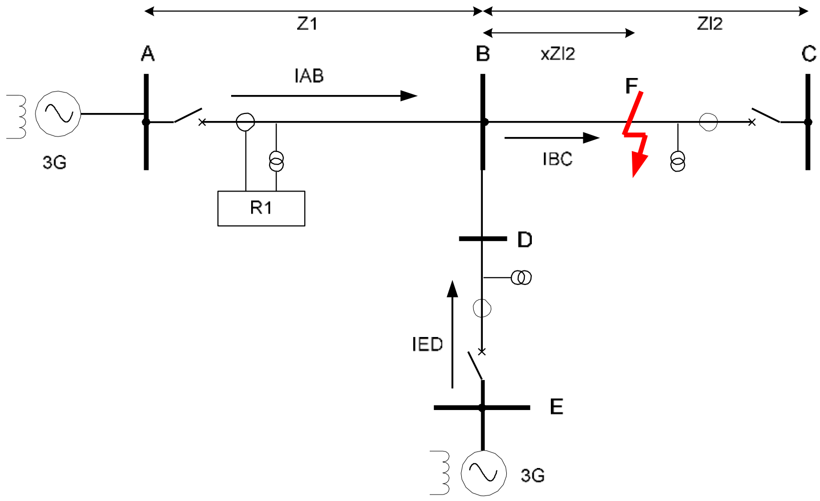


Figure 2. Current Infeed

Back-up Protection

The objective of protection is to remove only the affected portion of plant and nothing else. A circuit breaker or protection relay may fail to operate. In important systems, a failure of primary protection will usually result in the operation of back-up protection. Remote back-up protection will generally remove both the affected and unaffected items of plant to clear the fault. Local back-up protection will remove the affected items of the plant to clear the fault.

Backup protection can, and in many cases does, play a significant role in providing adequate system performance or aiding in containing the spread of disturbances due to faults accompanied by Protection System failures or failures of circuit breakers to interrupt current.

Overreaching or backup phase distance relays providing primary and/or backup functions played a role in the cascading portion of the 2003 Northeast Blackout in USA and have played similar roles in other previous and subsequent blackouts. [2]

Remote Backup Disadvantages

Remote backup often requires longer fault clearing times and that additional circuit element be removed from the system to clear the fault. While the latter usually has no worse effect on the transmission system than does local backup relay operation, it does interrupt all tap loads on all lines that are connected to the substation where the relay/breaker fails to operate.

The primary disadvantage of remote backup protection is that it can restrict the amount of load a circuit can carry under emergency conditions. Generally, relays designated as Zone 3 relays provide this remote backup function for phase to phase and three phase faults; however other relay designations may be used to provide the remote backup function.

Historically from a security perspective, there have been several cases where remote backup relays (Zone 3) have been involved in significantly expanding system outages by tripping due to unexpected loading during some system contingencies. Less obvious are many times that remote backup (Zone 3) relays have unintentionally operated to remove uncleared faults from the system or to halt cascading outages.

Difficult to Study– It is generally more difficult to study power system and Protection System performance for a remote backup actuation. This is because more power system Elements may trip. Tripping may be sequential and reclosing may occur at different locations at different times. For example, tapped loads may be automatically reconfigured and prolonged voltage dips that may occur due to the slow clearing may cause tripping due to control system actuations at generating plants or loads. It is very difficult to predict the behavior of all control schemes that may be affected by such a voltage dip, thus it is very difficult to exactly predict the outcome of a remote backup clearing scenario

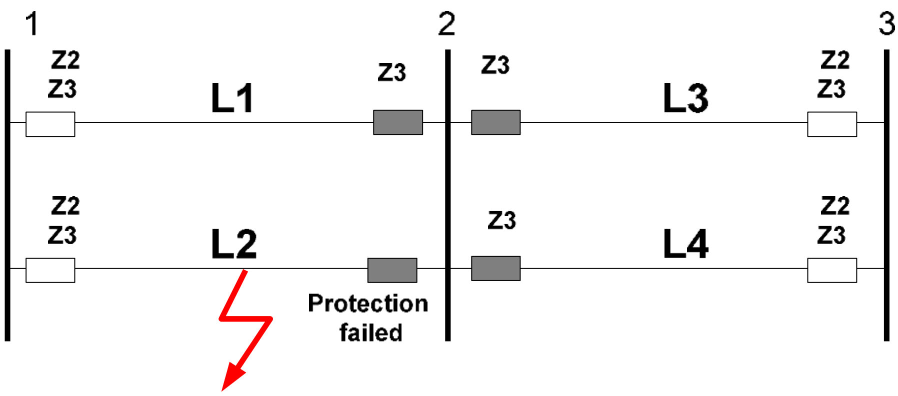


Figure 3. Protection Failed at one end[3]

New Vision of the Problem of Backup Protection

As we have observed, the actual backup protection philosophy has several disadvantages cause mainly by the lack of information in the local backup units and the algorithms used, limited only to work with local information

This is the main reason because we can say that the actual backup protection philosophy has reached its limit and a new vision and paradigm is needed using not only local information, but also remote one.

In the new proposal, Zone 3 is not strictly needed any more (it can be kept “freeze” and ready to be activated if the needed arrives). With is became true “the best solution for a problem is to eliminate the problem, so, we don´t need to think in the solution”. As Zone 3 is the problem if we don´t depend on it, we don´t need to think in all the problems associated with this solution.

Question is: What is the alternative?.

Alternative proposed is a combination of differential protection using information from PMU´s combined with a rational use of the inherent characteristics of the electric network.

The proposal is as follows:

We can define in the grid Super nodes with the corresponding overlaps, extending the coverage that normally exists for bus protection in Nodes.

As a Super Node is perfect balanced during normal operation, differential criteria can be used to detect any internal fault in a similar way as we do with a Node but in this case, using PMU´s as sensors. The main difference is in the operation time that in case of Super node will be time delayed. Doing this, a new protection philosophy based on “three defence lines” can be applied (*):

- Primary protection (as usual, distance, line differential) as the first defence line.
- First Backup selective protection: Differential (Active Power) time delayed with PMU (200 to 300 ms could be sufficient). Other criteria as current differential or directional also could be used. Active Power is preferred because it is inherent non-affected by Line Charging, Inrush current from transformers. Differential criteria works well with none, or reduced infeed during faults as in case with non-renewable (wind and solar) energy sources. This is the second defence line.
- Second Backup Protection: As usual, BF, Zone 3, Overcurrent, etc. (disabled while First Backup is active and automatic enabled if First Backup is non-active or failed). Alternative second (no deterministic) defence line.
- System Integrity Protection: SIPS or equivalent to maintain the stability of the Network as a third defence line. Alternatively, other methods as planned islanding and emergent frequency and voltage control to prevent expansion of an event into a large area power blackout.

Paper develops this new proposal, bringing the user the advantages of using synchrophasors for protection, to solve problems unsolved until now. The enclosed picture can give us better idea of the solution proposed:

As in the example, in case of fault in F1 and breaker 3 fail to open, Area A1 will trip time delayed (breakers 1, 7, 8 and eventually 2). If breaker 4 is open correctly by primary protection, a signal to remove in the PDC the PMU signals from breaker 3 in A2 is given preventing this area to trip. This is a similar technique used in trip for breaker coupler in bus protection (double bus arrangements). In this case, combined with remote breaker open criteria used in line pilot schemes.

(*) Philosophy of “three defence lines” has been successfully applied in China since many years ago, but using another criterion for the second defence line.

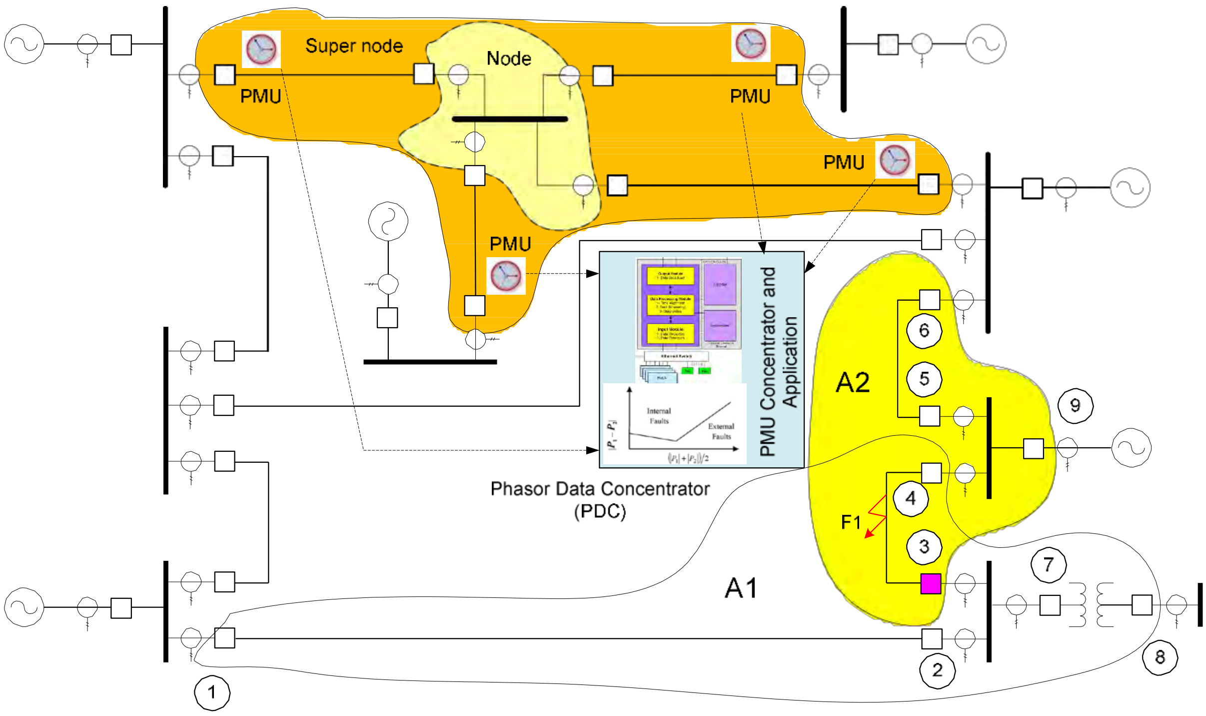


Figure 4. Selective Backup Protection Proposal

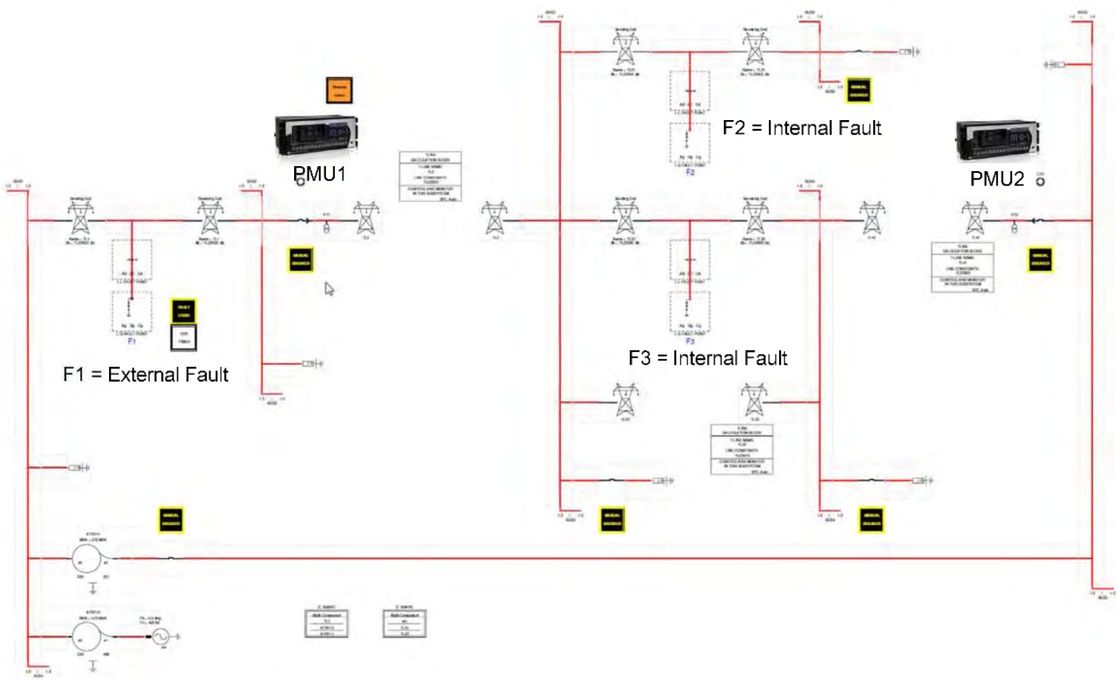


Figure 5. RTDS Model for System under test

Differential Algorithm

In order to minimize the impact of charging current and transformer inrush (during energization), it was decided to analyze a Power Differential Protection [8]. Power differential protection tripping characteristic is based on power differential in function of restraint power calculated for the super node. As the most sensitive in the case of solidly-grounded system the positive-sequence power was selected.
The adequate criteria are as follow:

$$P_{Diff} = |\underline{P}_{1,1} + \underline{P}_{1,2} + \cdots + \underline{P}_{1,n}|/n *$$

$$P_{Rest} = \mathrm{Max}(|\underline{P}_{1,1}|, |\underline{P}_{1,2}|, \ldots, |\underline{P}_{1,n}|)$$

where:

$\underline{P}_1$ – Positive-sequence power in per unit calculated as: $\underline{P}_1 = \underline{U}_1 \cdot \underline{I}_1$
n – n-th PMU of the super node

It was found that under high resistance faults, it was difficult to discriminate internal from external faults (Figure 7).

The above algorithm was combined with a power directional algorithm to discriminate internal from internal faults. Results can be observed in Figure 8. Fault locations in Figure 7 and Figure 8 correspond to fault locations from the model in Figure 5.

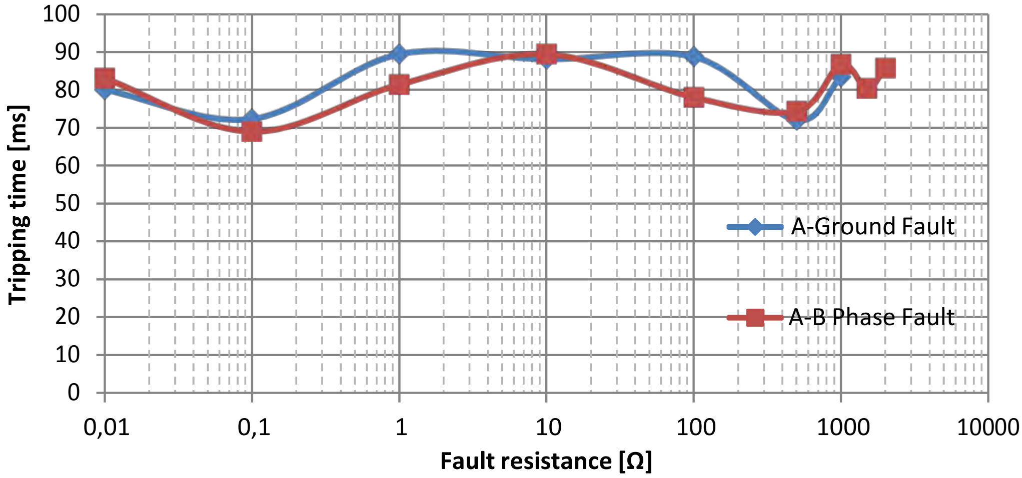


Figure 6. Tripping time of "Backup Protection" contains operating time of RTDS simulator with amplifiers and GOOSE massage sending time between PLC Logic and PMU relay.

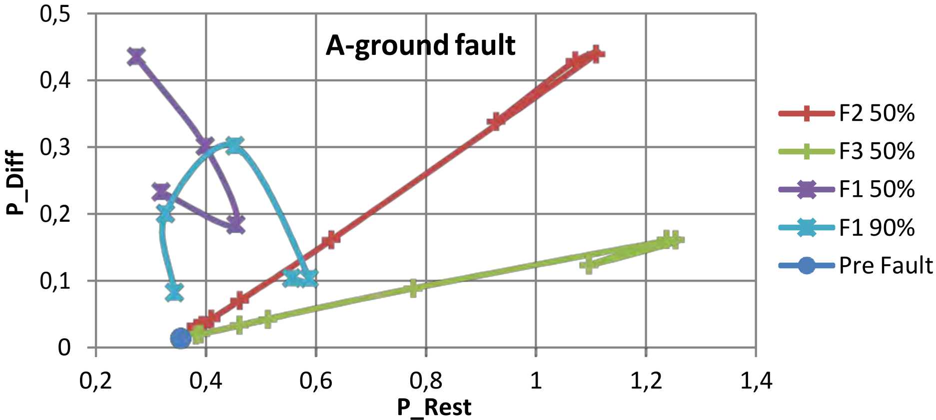


Figure 7. Response with only differential algorithm

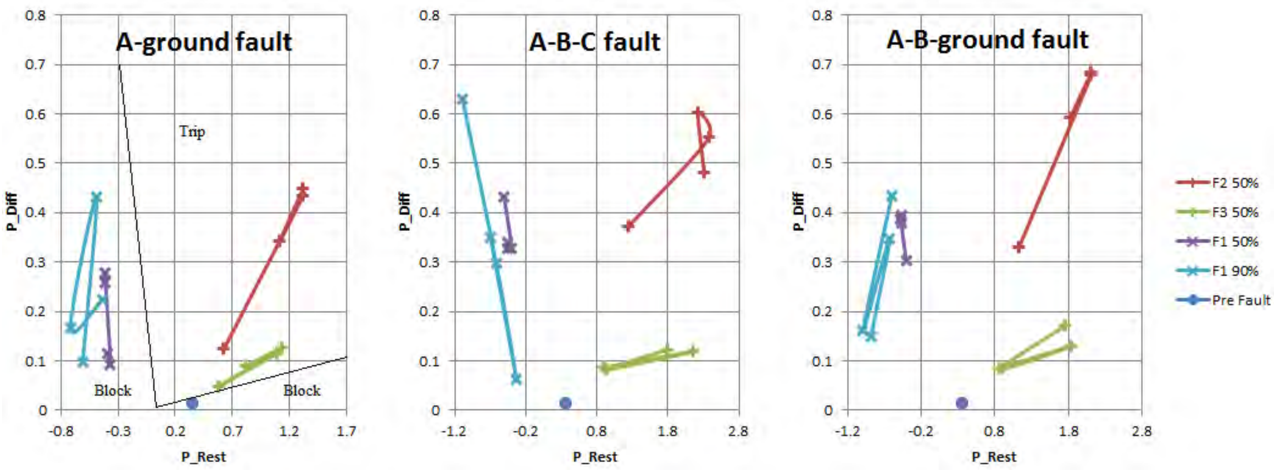


Figure 8. Response with differential algorithm associated with directional criteria

Conclusions

- Power Differential Algorithm combined with power directional criteria give a very good response a correct fault discrimination with any kind of faults.
- Test were made using only two PMU´s sending information at 50 values per second. We can observe the minimum operating time in Figure 6. This time is much smaller than typical delay for Zone 3. For coordination, additional time may be required.
- Research is at early stage, but with promising results. Further work will be needed to define the final structure of the most suitable algorithm and also tests on other more "standard" network models.
- Phasor Measurement Unit (PMU) technology provides phasor information (both magnitude and phase angle) in real time. The advantage of referring phase angle to a global reference time is helpful in capturing the wide area snap shot of the power system. Effective utilization of this technology is very useful in mitigating blackouts and learning the real time behavior of the power system. With the advancement in technology, the micro processor based instrumentation such as protection Relays and Disturbance Fault Recorders (DFRs) incorporate the PMU module along with other existing functionalities as an extended feature. The IEEE standard on Synchrophasors (C37.118) specifies the protocol for communicating the PMU data to the Phasor Data Concentrator (PDC).

Further Reading

[1] Mattias Jonsson: "Line Protection and Power System Collapse". Department Of Electric Power Engineering, Chalmers University of Technology, Göteborg, Sweden 2001
[2] NERC System Protection and Control Subcommittee: "Transmission System Backup Protection", December 2010
[3] Working Group C-6, System Protection Subcommittee IEEE PES Power System Relaying Committee Final Report. Wide Area Protection and Emergency Control
[4] NERC System Protection and Control Subcommittee: "Rationale for the Use of Local and Remote (Zone 3) Protective Relaying Backup Systems", 2005.
[5] IEEE PSRC, WG I 19 "Redundancy Considerations for Protective Relaying Systems", 19 Sept 2008
[6] IEEE PPC37.118.1™/D4.25.0 "Draft Standard for Synchrophasor Measurements for Power Systems", August, 2011.
[7] PSRC WG C2, "Report: Role of Protective Relaying in the Smart Grid", Version 1.1
[8] F. Namdari, S. Jamali, P.A. Crossley: "Power differential protection as primary protection of transmission lines and busbars". IET 9th International Conference on Developments in Power Systems Protection (DPSP 2008).
[9]Patrick Mazza (2005-04-27) (doc). *Powering Up the Smart Grid: A Northwest Initiative for Job Creation, Energy Security, and* Clean, Affordable Electricity.*]. Climate Solutions. p. 7. Retrieved 2008-12-01.*

«SO UPS», JSC

S.1.1-2. Hierarchically Coordinated Protection: An Integrated Concept of Corrective, Predictive, and Inherently Adaptive Protection

M. KEZUNOVIC, P.-C. CHEN, A. ESMAEILIAN, M. TASDIGHI
Texas A&M University
United States of America
kezunov@ece.tamu.edu

KEYWORDS

Cascading event, data analytics, data correlation, distributed generation, geospatial analysis, outage management, power system protection, support vector machine.

1 INTRODUCTION

This paper relates to a new protection paradigm where corrective, adaptive and predictive relaying features are introduced.

The value of *corrective relay operation* can be assessed by looking at the situations when relay mis-operations occur. Analysis of recent historical blackouts has revealed that the power system catastrophic events happened following consecutive cascading events such as transmission line outages, overloads and malfunctions of protective relays [1]-[3]. In general, cascade events can be divided into two time stages. In the first stage, successive events are slow enough to be analyzed as steady-state. If no action occurs to restore the grid to the normal operation condition, and meanwhile several major disturbances occur causing fast transient stability violation, a system collapse will happen. This stage is named as second or irreversible stage. Early prediction and proper control actions during the first stage can prevent further unfolding of cascade events.

When a transmission line is tripped due to the operation of protective relays, a relay mis-operation detection tool can confirm whether the relay operation was correct or the transmission line was healthy and incorrectly tripped [4]. The advantages of such tool could be itemized as higher reliability and redundancy, faster restoration and enhanced critical decision making during disturbances [5]. This tool can also support the reliable implementation of new applications such as transmission line switching (topology) control [6].

The value of *adaptive relay operation* [7]-[10] may be assessed by looking at the situations where adaptive features are desirable. So far, the protection challenges raised by DG integration in the system have been mostly looked at from the distribution side. However, with high penetration of DGs in the network, the protection concerns extend to transmission level also. According to the literature [11]-[12], one of the challenges that high levels of DG penetration create for the power transmission system protection is unintended bulk DG tipping following a disturbance in the transmission system. The interaction of system dynamics with sensitive control and protection measures which are necessary, according to IEEE standards, to prevent or minimize the existence of an inadvertent island, could lead to unintended tripping of DG. For example, if a short-circuit takes place in the transmission grid and its effects on voltage are propagated downstream to the distribution level, it may provoke the disconnection of a large amount of DG. Since these DG plants are tripped, a sudden increase in power flow coming from upstream takes place in this network area. This may provoke cascading operation of distance relays in transmission lines as a result of overload situations.

Fig. 1 shows the impedance trajectory seen by a relay in the vicinity of DG bus when 500 MW of DG is tripped following a three phase fault in the transmission level in New England 39 bus system. As it could be seen, the DG tripping has pushed the impedance trajectory into third zone of the relay in the vicinity of the DG bus and might lead to the relay false tripping.

The value of *predictive relay operation* may be assessed by looking at the situations where occurrence of faults may be predicted based on historical data. Weather factors are primarily responsible for the outages [13]. The severity of weather is predicted to become progressively worse [14]. The operation of electrical systems, particularly in an overhead structure, is very sensitive to the weather conditions. Therefore, it is imperative to come up with corresponding strategies. One of the promising solutions is to have a way of implementing weather-aware protection in a predictive manner. It is shown that the application of weather data may bring additional benefits to the outage management [15]-[16].

The question of how to correlate weather data from various sources with power system data remains a challenge. Such correlation requires the ability to leverage the geospatial nature of predictive information. In this case, utilizing Geographical Information System (GIS) is the key for correlating different layers of data for geospatial analysis. Within the traditional concept of utility, GIS is defaulted as a visualizing mapping tool. Yet, the spatial-temporal information can render not only the geographical visualizations but interpretation of different data layers. The flow of data provides useful knowledge extraction which enables better decision-making process for a utility operator. Further study is needed how this information may be utilized to develop predictive protection strategy

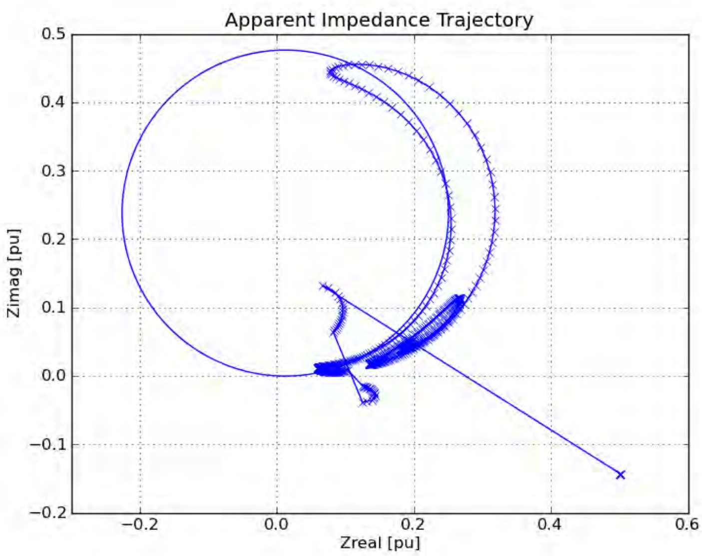


Figure 1: The apparent impedance trajectory for a scenario of DG tripping following a three phase fault clearing

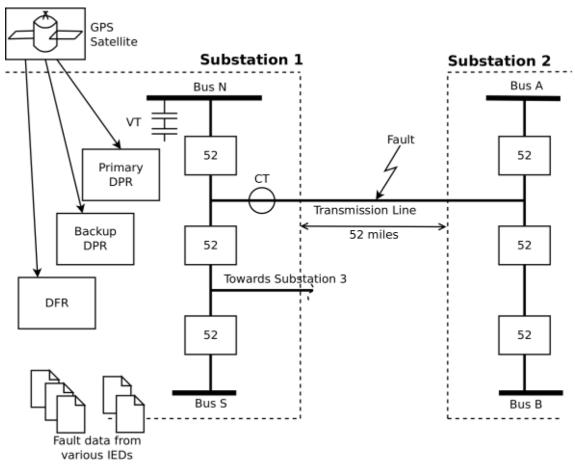


Figure 2: Typical transmission line setup with measurements from both ends

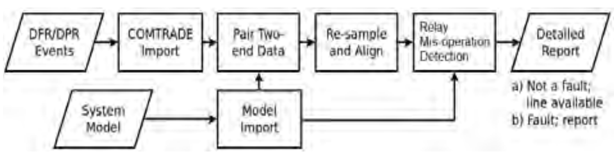


Figure 3: Automated analysis of time-synchronized event data

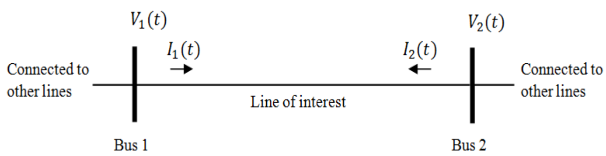


Figure 4: Transmission line with two-end measurements

2 EXAMPLES OF TECHNIQUES USED TO SOLVE THE PROBLEM

2.1 Relay mis-operation detection tool (example of corrective relaying strategy)

Fig. 2 depicts a typical transmission line setup with the event-triggered measurements from both ends. As it can be seen, the line can be monitored by different substation IEDs at both ends (details are only shown in substation 1). When a fault (or disturbance seen as a fault by the protective device) occurs, several IEDs can be triggered and they will capture event measurements. The assumption is that the data samples are synchronized and time-stamped using the Global Positioning System (GPS), and a high-speed communication link between substations and control center is available. The relay mis-operation detection tool implementation is illustrated in Fig. 3. Following is the description of each step.

Step 1. DFR/DPR Events Import: The required IED device data consists of voltage and current samples captured by DFR or DPR. The fault data and system model data are necessary inputs for the tool to run and operate correctly and accurately. The involved DFR and DPR devices varied by vendor, types, and vintage. All data files from different vendors have been converted in unified COMTRADE file format (IEEE C37.111-1999).

Step 2. System Model Import: The system model topology is obtained from the PSS/E (*.raw) file and used for pairing the event files coming from two ends of the same transmission line.

Step 3. Pairing the Two-end Data: There can be multiple IED files created during a disturbance at different substations. Utilizing the network topology from the system model, the IED files from the neighboring nodes are paired to extract the two-end measurement data corresponding to the transmission line between the buses.

Step 4. Re-sample and Align: After the two-end data are paired, they are processed in order to extract data samples for instantaneous voltage and current signals measured at both ends of the line. The extracted data samples are re-sampled and aligned (when the triggering time was not the same) in order to obtain the same sampling rate at both ends as well as synchronized samples.

Step 5. Relay mis-operation detection: The relay mis-operation detection tool core algorithm has been introduced in [17], [18]. Here, we provide an overview of relay mis-operation detection core algorithm implemented as a part of the proposed tool. In Fig. 4, $V_1(t)$ and $I_1(t)$ represents voltage and current measured at one end (Bus 1) of the line at instance t. Similarly $V_2(t)$ and $I_2(t)$ represents voltage and current measured at the other end (Bus 2) of the line. Instantaneous powers calculated at both ends are:

$$P_1(t) = V_1(t) \times I_1(t) \quad , \quad P_2(t) = V_2(t) \times I_2(t) \tag{1}$$

During the normal operation, $P_1(t)$ and $P_2(t)$ will be in phase opposition to each other for the current directions assumed. However, for the faulty phases, when the fault is initiated, they will be in-phase with each other. For un-faulted phases the phase opposition will be maintained even after the fault inception. If a load level change or a fault in neighboring line occurs, the calculated instantaneous powers will remain in opposite direction. Therefore, the method can discriminate load level changes or external faults from internal ones. To represent this feature mathematically, we use signum function which is defined as:

$$\operatorname{sgn}(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases} \tag{2}$$

We calculate $\operatorname{sgn}(P_1(t))$ and $\operatorname{sgn}(P_2(t))$ and plotted the difference for each phase.

$$P\operatorname{sgn}(t) = \operatorname{sgn}(P_1(t)) - \operatorname{sgn}(P_2(t)) \tag{3}$$

Theoretically, before a fault has been initiated, this difference $P\operatorname{sgn}(t)$ should be ±2 and after fault occurrence $P\operatorname{sgn}(t)$ should be 0 on all faulty phases. We used the change of difference of $\operatorname{sgn}()$ to detect fault instant as (3). However, due to transients and noise in the measurements, some outliers exist. To avoid incorrect decisions caused by outliners, a moving window of 5 ms is used to check whether at least 80% of $P\mathrm{sgn}(t)$ are zero, which indicates a fault.

Step 6. Detailed Report: The results of relay mis-operation detection tool are provided in the form of detailed analysis report. As shown in Fig. 3, the outcome of the analysis may be: a) no fault, which means that the tripped line may be available to switch back in; b) fault detected and operation of relay has been confirmed, which means no need for a corrective action.

2.2 Support Vector Machine Based Protection Scheme (example of adaptive relaying strategy)

Recently, supervised learning techniques have attracted attention in various power system disturbance analysis studies such as power swing detection and fault detection and classification. Among these techniques, Support Vector Machine (SVM) is shown to be an accurate and easy to train method. SVM is a learning method based on the statistical learning theory. In this method, the idea is to map the original input space into a high-dimensional dot product space which is called a feature space, and determine the hyper-plane in the feature space to maximize the generalization ability of the classifier. The optimal hyper-plane is found by deploying the optimization theory, and respected insights provided by the statistical learning theory.

Implementing SVM method involves separating the data into two categories: training and testing data sets. These sets include instances each of which contains a label (target value) and multiple features (observed variables). The SVM goal is to create a model based on the training data sets which could predict the labels for the test data sets if the features of the test data sets are given to the model.

In this study a SVM based protection scheme is proposed which enables the relay to detect a DG tripping case from faults. The output of the SVM module and the distance relay pick-up signal together identify the trip signal as shown in Fig. 5. Proper input features for the SVM could be chosen from the principal component analysis [19]. The input feature vector includes the following measurements at the relay installation point: the bus voltage, branch current, active and reactive power flows. The following are the steps of implementing the proposed algorithm:

Step 1. Instances preparation:
Simulation of multiple DG tripping cases with different parmeters: fault location, DG tripped capacity, and DG tripping instant.

Step 2. Feature extraction:
Monitoring and recording the features extracted by principal component analysis (PCA).

Step 3. Training set data preparation:
Randomly choosing the training set out of all the simulated instances.

Step 4. Kernel parameter selection:
Having chosen RBF kernel function, the cross-validation technique is implemented to obtain the proper kernel parameters in training the SVM.

Step 5. SVM training:
Train the SVM based on the obtained kernel parameters.

Step 6. SVM testing:
Test the SVM for the testing data set, i.e. the instances not chosen as training instances.

2.3 Weather Impacts on Outage Management (example of a predictive relaying strategy)

Vegetation contact on distribution lines is one of the most common fault types. The fall of tree limbs and trunks are due to the large wind. An example provided examines the utilization of GIS for outage prediction in the context of faults caused by the lack of tree-trimming. This requires an understanding how typical power system data is correlated with the GIS containing the wind and canopy height data. These sources are used as inputs to generate outage vulnerability assessment for different geographic areas, and then correlate it with feeder data for outage mapping. In general, data used for this types of analysis must be properly chosen and processed for specific application purposes. The data sources will be shown first, and then an example correlation will be demonstrated using a GIS platform named ArcGIS [20].

The power system data used in this example is extracted from the Storm Vulnerability Assessment tutorial from Esri [21]. The components utilized are primary overhead feeders.

The wind forecast data is from National Digital Forecast Database (NDFD) [22]. The data can be accessed through graphical user interface (GUI) (named "tkdegrib") provided by NDFD and then converted to Shapefiles (polygon data format) for further processing in ArcGIS [23].

The canopy height data used in the analysis is the three dimensions Global Vegetation Map [24], [25]. The data format is raster at 1 km resolution using data from the Geoscience Laser Altimeter System (GLAS) aboard Ice, Cloud, and land Elevation Satellite (ICESat) [25]. The average canopy height in each grid cell is recorded.

In the example, the process of data correlation is presented below.

Step 1. Process Vegetation Data
The vegetation data were masked to obtain the grid cells containing the area for just the distribution network.

Step 2. Process Wind Data
The wind polygon data were clipped to match the processed vegetation polygon.

Step 3. Correlate vegetation and wind data and then perform the vulnerability analysis
The data from the wind polygon were spatially joined with the vegetation polygons. This resulted in each cell containing both canopy height and wind data which allows for analysis given a set of rules - e.g., wind speed will be taken into consideration first prior to the canopy height data. Each grid cell is then labeled for prioritizing in the outage search sequences.

Step 4. Identify the system components in each area and output results
It should be noted that one component (e.g. a line) may stretch across multiple polygons or grid areas (i.e. not just inside a single area). While correlating other data layers with power system data layer, the power system must be divided into different areas where components may be separated into multiple pieces to account for this.

By correlating the different data layers, the region with high wind speed and large canopy height data could be identified as the potential outage area.

3 RESULTS AND BENEFITS

3.1 Relay mis-operation detection tool (example of a corrective relay tool)

The relay mis-operation detection tool has been tested against various simulated and field data test cases. The following two examples demonstrate how the tool behaves in the case of a fault as well as relay mis-operation. In both cases, the sampled data are taken from actual IED device in field.

As shown in Fig. 6 (a-c), the instantaneous powers from two ends at phase B and C are in the opposite direction before and after disturbance. While in phase A, the direction has been changed after fault initiation time. As a result, the output of the relay mis-operation detection tool reports "phase A to ground fault". Fig. 6 (d-f) depicts plot of $P\text{sgn}(t)$ with respect to the time for three phases. It can be seen that in phases B and C less than 80% of the total samples are zero. However, more than 80% of the total samples of phase A is zero.

Fig. 7 shows the same type of output plots for a relay mis-operation test case. Fig. 7 (a-c) depicts instantaneous power $P_1(t)$ and $P_2(t)$ calculated based on data captured by DFR units at the two ends of transmission line with respect to time. In this case, the information received by utility shows

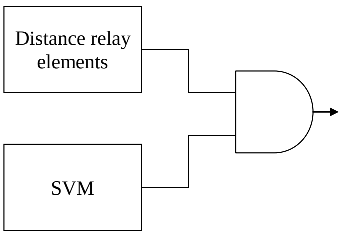


Figure 5: Proposed scheme block diagram

that the fault occurred on a neighboring line. Does not read right due to single phase fault (ag) while the later investigation of the case reveals that the relay mis-operates due to a single phase fault on an adjacent line.

From Fig. 7 (a-c) one can observe that the opposite direction of instantaneous powers from two ends stay the same before and after disturbance. As a result, the output of the tool indicates "no fault" condition. Fig. 7 (d-f) shows plot of $P\mathrm{sgn}(t)$ with respect to time for three phases. It can be seen that less than 80% of the total samples are zero which means no fault has been detected in any of three phases.

3.2 Support Vector Machine Based Protection Scheme (example of an adaptive relay tool)

In this study, the SVM is trained for unintended DG tripping scenarios in New England 39 bus system. To train the SVM, multiple instances have been simulated which include: fault on multiple points along the third zone of the target relay, various DG tripping capacity, and multiple DG tripping instants following the fault. The input vector for the SVM includes the difference of feature values with those of previous cycle. The sampling rate is considered 10 samples per cycle. Considering multiple scenarios for creating the data sets, 25000 instances of DG tripping cases and faults are provided. 15000 instances are chosen randomly as training data sets and the rest as the testing ones.

In the next step, a proper Kernel function and its corresponding parameters should be chosen and determined to train the SVM. For this purpose radial basis kernel function (RBF) is deployed. RBF kernel needs two parameters to be determined: C and γ. The C and γ values, which are best for a given problem, are not known beforehand; so, a parameter search should be done. The values which enable the SVM to predict the testing data sets accurately are desired. As mentioned above, the data is divided into two sets one of which is considered unknown. To examine of SVM performance more precisely, the prediction accuracy for the unknown set has a key role as it could be considered as an independent data set. The cross-validation technique [26] is used as an improved version of the search procedure for determining C = 32768 and γ = 32 for the RBF kernel. It was seen that the SVM reaches the accuracy of 93.7% with the selected kernel parameters. Therefore, the SVM detects the DG

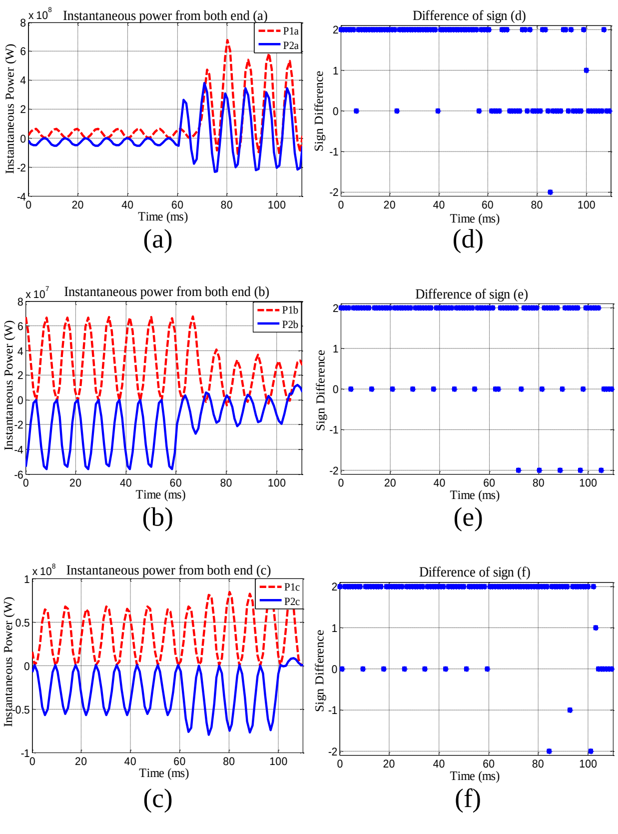


Figure 6: Single phase to ground fault detection and classification

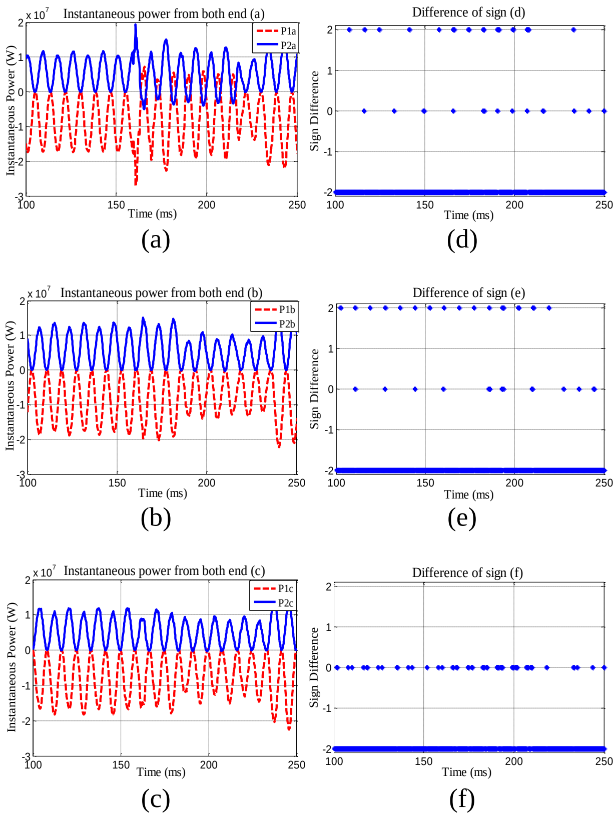


Figure 7: Relay Mis-operation Detection

tripping cases with a high precision which prevents the relay miss-operation and probable cascading failures on such unintended bulk DG tripping cases.

The other advantage of the proposed protection scheme is that it could be implemented in combination with other additional protection schemes such as power swing blocking and that way help maintain the power system protection dependability and security effectively.

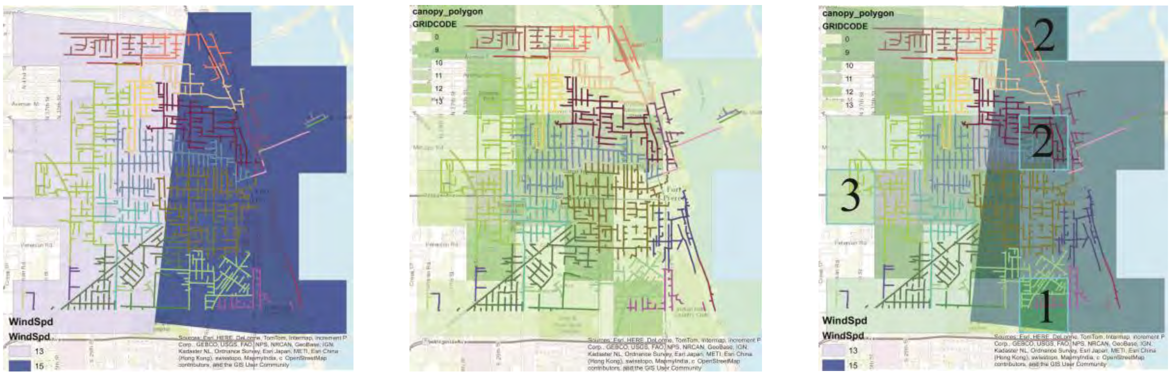
3.3 Weather Impacts on Outage Management (example of a predictive relay tool)

Fig. 8 shows the final results from this example. Fig. 8 (a) shows the power system and wind data layers where the larger wind speed is at the right hand side. Fig. 8 (b) shows the power system and canopy height data where different saturation levels of green color represent different height of canopy. Fig. 8 (c) shows the result of combining each of these layers together. Based on the wind and canopy data, the first three areas should be searched by the dispatched crews are labeled in Fig. 8 (c).

The example discussed here is intended for the prediction purposes but can be also applied to real-time operations stages (search for outages with insufficient outage report information). In the reality, the localized nature of weather conditions (e.g. various types of storms) means that the process for corresponding types of outages may be very different than what is described in the basic example provided here. The rules used to characterize risk or response priority should be based on real conditions and past experience.

The selections of input data are critical for the data correlation provided here. The level of attribute detail provided has critical impacts on the model results. For example, Fig. 9 shows the wind data from reference [27] with the Kriging function in Geostatistical Analyst in ArcGIS. Kriging is a technique for interpolating predicting values of location with no measurement data. In Fig. 9, there are only 4 data points which do not render very effectively adjacent polygons for further analysis. As shown, the area where the network intersects is not reasonably subdivided.

Similarly, the wind speed data downloaded from the live feeds of NDFD [28] contain only 4 data points. The layer file does not contain additional attribute information which can be used for further processing. These data simply visualize wind speeds, and are not readily usable.



(a) (b) (c)

Figure 8: Data layer correlations. (a) Power system and wind data. (b) Canopy height and power system data. (c) All three layers of data

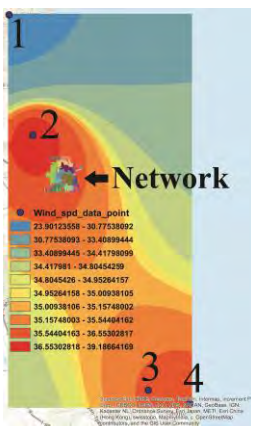


Figure 9: Only 4 data points available from [22] for kriging

4 CONCLUSION

Based on the discussions in the paper the following conclusion can be reached:

- Corrective, adaptive and predictive relay features are feasible
- Such protection paradigm has distinct benefits but requires additional data or equipment
- The test results illustrate the robustness of the solutions
- The practical use of such a protection paradigm is yet to be fully explored
- Future steps are needed to identify other applications that may benefit from such a paradigm

REFERENCES

[1] M. Johnson, "Line Protection and Power System Collapse," Master's Thesis, Department of Electric Power Engineering, Chalmers University of Technology, Goteborg, Sweden, 2001.
[2] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force, Apr. 2004.
[3] R. Baldick et al., "Initial Review of Methods for Cascading Failure Analysis in Electric Power Transmission Systems," IEEE PES General Meeting, Pittsburgh, PA, USA, Jul. 2008.
[4] M. Kezunovic, S. Meliopoulos, V. Venkatasubramanian, and V. Vittal, Application of Time-Synchronized Measurements in Power System Transmission Networks, New York: Springer, 2014.
[5] T. Popovic and M. Kezunovic, "Measures of value: data analytics for automated fault analysis," IEEE Power & Energy Magazine, vol. 10, no. 5, pp 58-69, Sep. 2012.
[6] M. Kezunovic et al., "Reliable Implementation of Robust Adaptive topology Control," HICCS Hawaii International Conference System Science, Manoa, Hawaii, Jan. 2014.
[7] G. D. Rockefeller, et al., "Adaptive transmission relaying concepts for improved performance," IEEE Trans. Power Del., vol. 3, no. 4, pp. 1446-1458, Oct. 1988.
[8] J. D. Codling, et al., "Adaptive relaying. A new direction in power system protection," IEEE Potentials, vol. 15, no. 1, pp. 28-33, Feb./Mar. 1996.
[9] J.-A. Jiang, et al., "A novel adaptive PMU-based transmission-line relay-design and EMTP simulation results," IEEE Trans. Power Del., vol. 17, no. 4, pp. 930-937, Oct. 2002.
[10] J. Upendar, et al., "Comprehensive Adaptive Distance Relaying Scheme for Parallel Transmission Lines," IEEE Trans. Power Del., vol. 26, no. 2, pp. 1039-1052, Apr. 2011.
[11] J. A. Peças Lopes, et al., "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," Elect. Power Syst. Res., vol. 77, no. 9, pp. 1189–1203, Jul. 2007.
[12] R. A. Walling and N. W. Miller, "Distributed generation islanding-implications on power system dynamic performance," IEEE/PES Summer Meeting, vol. 1, pp. 92-96, Jul. 2002.
[13] Executive Office of the President, "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages," Aug. 2013.
[14] A. B. Smith and R. W. Katx, "US billion-dollar weather and climate disasters: data sources, trends, accuracy and biases," Natural Hazards, vol. 67, no. 2, pp. 387-410, Jun. 2013.
[15] M. Kezunovic, et al., "The role of big data in improving power system operation and protection," Int. Inst. for Research and Education in Power Syst. Dynamics Symp. (IREP), Aug. 2013.
[16] P.-C. Chen, et al., "The Use of Big Data for Outage Management in Distribution Systems," Int. Conf. on Electricity Distrib. (CIRED), Jun. 2014.
[17] P. Dutta, A. Esmaeilian, and M. Kezunovic, "Transmission-Line Fault Analysis Using Synchronized Sampling," IEEE Trans. Power Del., vol. 29, no. 2, Apr. 2014.
[18] A. Esmaeilian, M. Kezunovic, "Evaluation of Fault Analysis Tool under Power Swing and Out-of-Step Conditions," 46th North American Power Symposium (NAPS), Sep. 2014.
[19] K. Fukunaga, Introduction to Statistical Pattern Recognitions. New York: Academic Press, 1972.
[20] ArcGIS, Esri. [Online] Available: https://www.arcgis.com/features/
[21] Storm Vulnerability Assessment, ArcGIS for Utilities, Esri. [Online] Available: http://solutions.arcgis.com/utilities/electric/help/storm-vulnerability/
[22] General Information, NDFD, NWS. [Online] Available: http://ndfd.weather.gov/index.htm
[23] National Digital Forecast Database (NDFD) Tkdegrib and GRIB2 DataDownload and ImgGen Tool Tutorial Access Data, NDFD, NWS. [Online] Available: http://ndfd.weather.gov/technical.htm
[24] 3D Land Mapping, Jet Propulsion Laboratory, California Institute of Techonology. [Online] Available: http://lidarradar.jpl.nasa.gov/
[25] M. Simard, et al., "Mapping forest canopy height globally with spaceborne LIDAR," J. Geophysical Research, vol. 116, G04012, pp. 1-12, Nov. 2011.
[26] C. C. Chang and C. J. Lin. "LIBSVM: a library for support vector machines," ACM Transactions on Intelligent Systems and Technology, vol. 2, no. 3, Apr. 2011.
[27] Data Files and Feeds, SECOORA. [Online] Available: http://secoora.org/data/data_feeds
[28] Folder: LiveFeeds, ArcGIS REST Services Directory. [Online] Available: http://tmservices1.esri.com/arcgis/rest/services/LiveFeeds

REDUNDANCY IN DIGITAL SUBSTATIONS

D.L.P. Jenkins *, S. Richards *, S. Vigouroux †

* Alstom Grid, United Kingdom – dylan.jenkins@alstom.com
†Alstom Grid, France

Keywords

IEC 61850, Station Bus, Process Bus, Merging Unit, IEC 62439, Time Synchronisation

Summary

The introduction of the process bus and station bus to modern digital substations has raised many questions and concerns. Protection Engineers are responsible for ensuring that protection and automation systems have an adequate level of redundancy to be considered suitable for critical power system applications.

Many new methods and technologies are now available that offer the means of providing this redundancy; however the temptation to introduce many of these at once could lead to a design that is unnecessarily complex, difficult to test and unreliable in practice as a result.

For example it is now possible to design a process bus architecture whereby protection relays subscribe to multiple sampled value streams from redundant merging units. However the question of whether this is actually necessary is a valid one. In a conventional substation such a design philosophy would equate to protection relays being wired to multiple redundant instrument transformers, which is not common practice nor indeed desirable.

This paper will review the contemporary protection engineering principles that have been used for many decades to engineer redundant systems and then seek to establish how these same techniques can be applied to new digital substation architectures.

Methods and technologies that will be reviewed include:

- Network redundancy protocols such as IEC 62439 Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).
- The architecture of the process bus, station bus and time synchronisation network. For example how merging units are connected to Intelligent Electronic Devices (IEDs) and how connections are made between substation bays to share sampled values and GOOSE messages.
- Where protection and automation functions are distributed across the IEDs, merging units and other devices in the substation.

The objective of this review is not to propose an ideal or target architecture, since the design of suitable solutions depends on the application in question. Instead, it will seek to identify how these methods need to be considered and what trade-offs exist from their use.

Introduction – How Have We Previously Achieved Redundancy?

The principle of redundancy is a long established requirement for substation protection systems in order to achieve reliable power systems.

A definition in the context of protection and automation is the provision of sufficient duplicate components so there is at least two independent protection functions, each of which is sufficiently capable of carrying out the required function on their own. We often refer to these two systems as 'Main 1' and 'Main 2' (see Figure 1) [1].

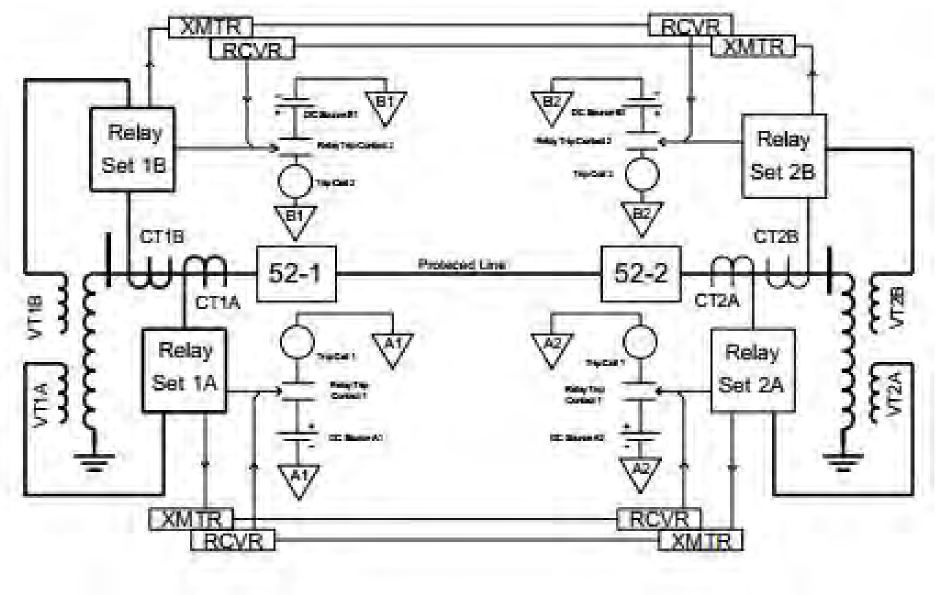


Figure 1 - Fully Redundant Main 1 / Main 2 Line Protection Scheme [2]

This architecture is provided because 100% perfect reliability of any single device is not possible to achieve in the real world, therefore to improve reliability of the complete systems to an acceptable level, we design so that the failure of a component does not disable the overall protection system.

Although redundancy and backup are often confused as the same thing, they are actually two distinctly different properties; a redundant system will provide a duplicate function that is of equal performance to the primary, whereas a back-up system may still provide protection but be of inferior performance. One example of a redundant protection system would be a Main 1 distance pilot scheme with a Main 2 stepped distance scheme. A back-up to Main 1 could be simple overcurrent protection, which does not provide the same level of sensitivity or speed as a redundant Main 2 system [2].

Some designs in a conventional protection system that will achieve this redundancy would include:

- Duplicated circuit breaker trip coils
- Duplicated DC power supplies for IEDs and tripping circuits
- Separate current transformers, or duplicated secondary cores
- Minimising potential for common mode failure between Main 1 and Main 2 systems, such as maintaining physical isolation, and by using different operating principles (this ensures that the two systems are truly 'independent' to one another)

As will be discussed in this paper, we can often accept a lower level of redundancy where back-up is provided and we then assess that this will result in a sufficiently reliable overall protection system.

Sometimes a lower level of redundancy would be accepted where the consequence of failure is less severe. For example, it is common for some distribution systems to provide backup protection, but not redundant Main 1 / Main 2 systems. Such an assessment however is very subjective which is why it is common for different design philosophies to be used between different end users.

Digital Substation Architecture – New Considerations

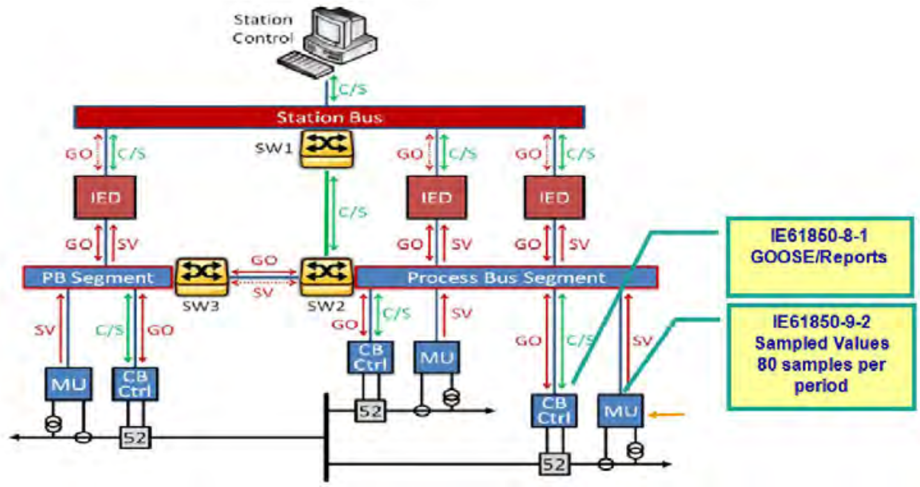


Figure 2 – Digital Substation Architecture

When we look at the architecture of a digital substation, it is apparent that many new technologies are available. However, the overall principle of protection redundancy must be maintained even with this new architecture as it cannot be allowed that the failure of a single device results in the complete loss of system protection. For example IEDs can now send commands to circuit breakers through the process bus rather than with copper connections, but the process bus should incorporate sufficient redundancy so that the failure of a single Ethernet switch does not result in the failure of a GOOSE trip signal being transferred.

As an example of how some Engineers have approached this problem, consider the conceptual design of the first example in Figure 3.

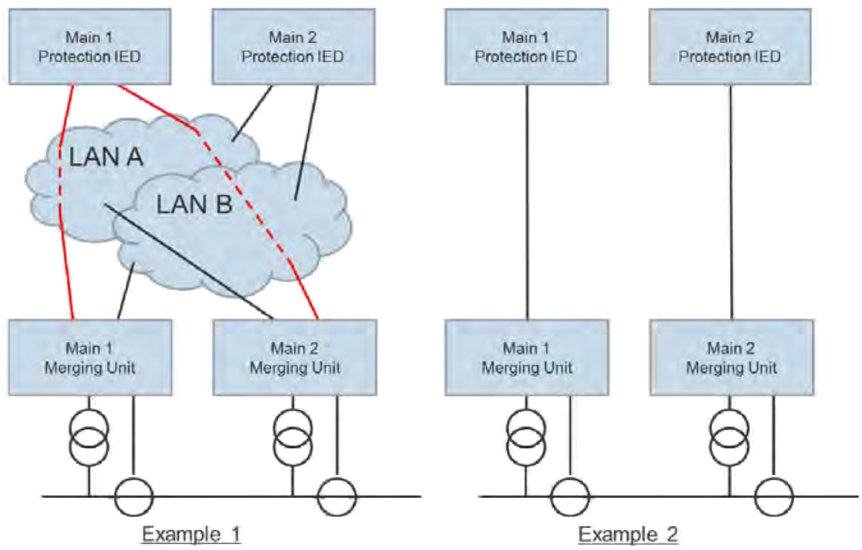


Figure 3 – Options for Protection IED Subscriptions to Merging Units

Because any device can potentially subscribe to any merging unit on the process bus, it is possible for a design architecture like this first example whereby the protection IEDs subscribe to multiple instrument transformer sampled value streams via redundant merging units. However the question of whether this is actually necessary is a valid one. In a conventional substation such a design philosophy would equate to protection IEDs being wired to multiple redundant instrument transformers, which is not common practice nor indeed desirable, as it is accepted that if one of the instrument transformer circuits were to fail that the Main 2 system will provide sufficient backup. Often the sampled values from the merging unit do not need to be shared to other devices, therefore a point-to-point connection could be entirely suitable as shown in the second example of Figure 3. This also aligns with the principle of the two main protection systems being independent of one another.

The architecture of the first example may in fact not be any more reliable than the second when considering a single device failure scenario, and it is also probably more difficult to commission, troubleshoot and maintain. In both cases there is no single point of failure but the first example is significantly more complex. This illustrates a key point that although it is possible to implement more sophisticated designs to add redundancy with new digital substation technology, it does not necessarily mean that it is always appropriate to do so [3].

What then are the key new components to a digital substation that will need to have redundant designs? Referring back to the conceptual architecture in Figure 2 we can see new points of common mode failure that require consideration and will now be analysed in detail:

1. The Ethernet network (both station bus and process bus)
2. The time synchronisation network
3. The functional architecture of protection functions, since these may now be distributed across the substation within different IEDs

Substation Ethernet Network Redundancy

Logically, we can group the two Ethernet networks in a digital substation into two buses; the station bus and the process bus. Though these are separated as logically distinct systems they can be made of different components with varying levels of redundancy. For example the process bus connections between some merging units and IEDs could be point-to-point with no network redundancy whereas others could make use of a redundant protocol like PRP. There may even be components that are used for both the process and station buses, for example in the figure below GOOSE signals are used in both process and station level signal exchange from the protection IEDs.

The types of network redundancy technology that can be used for the substation Ethernet network can be grouped into three categories:

1. No automatic redundancy (point-to-point link)

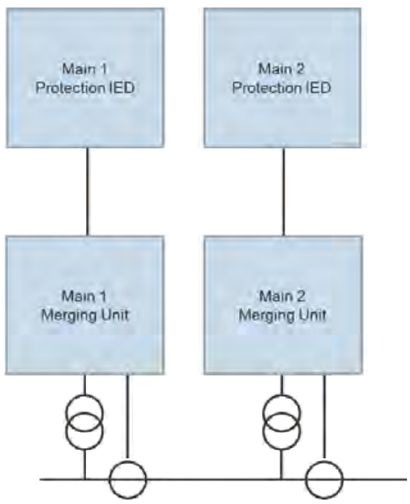


Figure 4 – Point-to-Point Network Connection

In this case the Ethernet connection is a point to point link only. In the event of failure the connection must be manually repaired to re-establish communication. This could take the form of a single Ethernet connection from an IED to a network switch, or a single connection between merging unit and an IED as in Figure 4.

Such architecture relies on back-up devices (Main 2) to provide redundancy to the system, rather than redundancy of the Ethernet network. But this approach could be perfectly acceptable since a failure would have to occur on both the Main 1 and Main 2 simultaneously for the complete system to be disabled.

2. Passive network redundancy

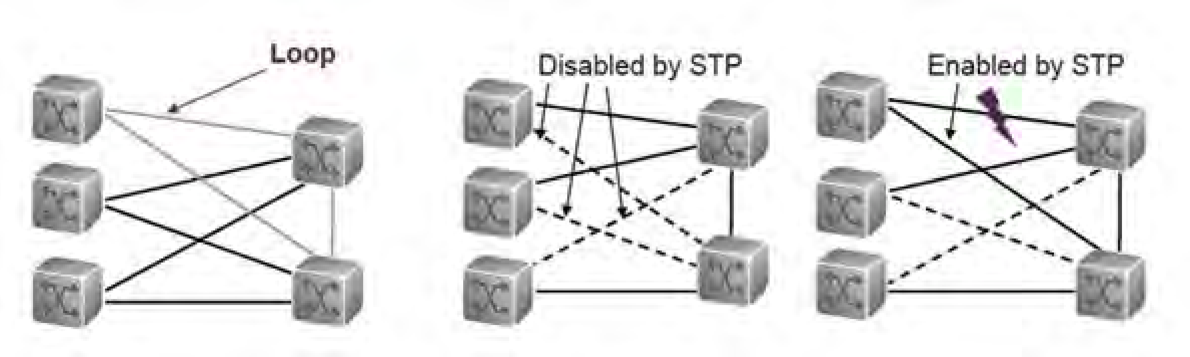


Figure 5 – Spanning Tree Protocol

Some networking technologies offer redundancy but will cause system outages for a certain period of time while communication is re-established. For example Rapid Spanning Tree Protocol (RSTP) which is very commonly used in substation LANs, may take hundreds of milliseconds to reconfigure when a link is broken [4], during which time no signals such as GOOSE can be exchanged between the isolated parts of the network (Figure 5).

Another example of passive redundancy is ‘hot standby’, which is a term used for devices with a back-up network interface that is only activated in the case of the primary interface failing.

The advantage of these technologies is their simplicity; they require very little configuration and training to staff who may be new to networking and digital substation principles. However they are not a suitable choice where system down time is an issue, for example an application that requires a consistent sampled value stream, or a transmission application where a few hundred milliseconds of protection unavailability would pose an unacceptable threat to grid stability.

3. Active network redundancy

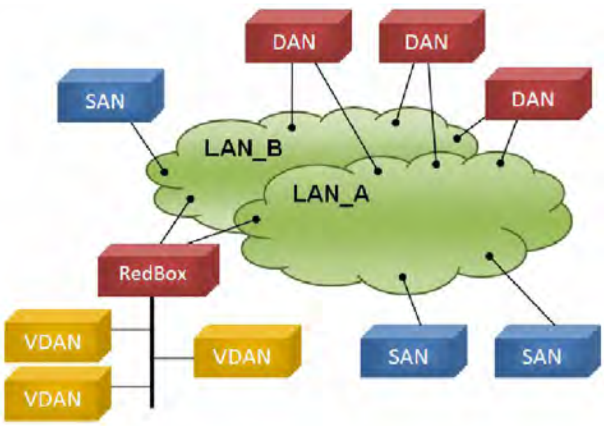


Figure 6 – Parallel Redundancy Protocol

The international standard IEC 62439 defines two network redundancy protocols that can be used for substation Ethernet networks; PRP and HSR [5]. Some other protocols do exist but are not interoperable solutions and not considered in this paper.

These two technologies differ to other protocols in that they are termed as ‘bumpless’ whereby recovery time in the case of failure is zero.

PRP (Parallel Redundancy Protocol) uses a double-star architecture. Two messages are sent to two different networks simultaneously. HSR (High Availability Seamless Ring) as the name suggests uses a ring architecture. Like PRP two messages are sent from each device, but these traverse the same LAN in opposite directions.

Compared to HSR, PRP has the advantages of:

- It can support twice as many devices for the same network bandwidth
- It does not require that all devices in the system support PRP or HSR (devices can be singly attached to only one network if full redundancy is not required)
- Flexibility of LAN structure – since it is possible for the two LANs to have different architectures and use different technology

The disadvantage of PRP is that it requires more investment in network components compared to HSR since the network must be duplicated.

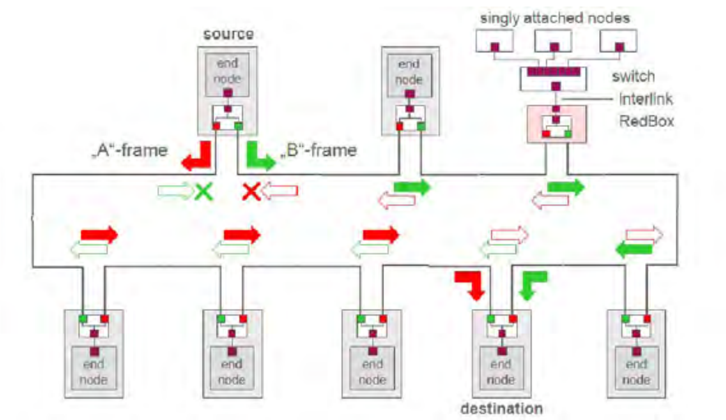


Figure 7 – High Availability Seamless Ring Protocol

It is entirely possible and indeed recommended that PRP and HSR networks are mixed with one another depending on the application. For example ‘LAN-A’ shown in Figure 6 may actually be formed using a HSR ring, or it may use another redundancy technology such as RSTP. It is recommended to not restrict the networking technologies that can be used, so that Engineers may select the optimum solution for the application.

The application requirement is the determinant factor for what level of network redundancy is required. In some systems there may be a high risk of Ethernet network failure, or a separate ‘Main 2’ system may not be provided, in which case a bumpless redundant network protocol such as PRP might be required. In other cases a simple point-to-point link could be completely sufficient.

Time Synchronisation Signal Redundancy:

One new consideration with the introduction of the process bus is the provision of accurate time synchronisation signals. Process bus applications require sampled value measurements to be synchronised very accurately. If an IED receives sampled values from different sources, for instance voltage measurements from one merging unit and current measurements from another, then protection maloperation could occur if these samples are not properly synchronised. Because of this risk, the same redundant design principles also apply to the time synchronisation network.

Redundant time sources

Currently the most popular means of providing a source of global time synchronisation is using satellite signals from the Global Positioning System (GPS). This is a very accurate and cost effective solution but has some disadvantages, namely it is a single source of failure. In addition to the risk of GPS system failure, there is the potential threat of GPS signals being jammed or spoofed for malicious purposes [6].

However not all applications require time signals to be globally synchronised, so long as all samples are synchronised to the same local clock. For example, in applications that are limited to within the substation such as bus bar protection, there is no risk if communications to GPS satellites are lost as the function can still continue to operate as normal. In such scenarios redundant time sources may not be necessary. This situation is even simpler in cases such as feeder protection where all samples may emanate from the same merging unit, so real time is irrelevant to correct operation.

In the case where the samples being compared are geographically dispersed, such as line current differential, then global synchronisation is very important. If the clocks at either end of the line are not synchronised to one another then a differential current may be wrongly observed resulting in mal-operation, unless the relay scheme offers suitable mitigation.

In such a situation it is necessary rely on back-up protection functions in the case of time source failure or to provide a redundant global time source. One method is to use provide a diverse satellite technology not linked to GPS. Currently the Russian GLONASS system is the only commercially available technology worldwide for such purpose, but in future the European Galileo and other regional systems may provide suitable alternatives. However common mode failure is still possible, for example solar flares can affect all satellite systems equally [7].

An accurate time source can also be provided without a satellite based system by using a Caesium atomic clock (see Figure 8). This is a very expensive solution but has been demonstrated as technically feasible for situations that require extremely high levels of redundancy, as the chance of common mode failure is reduced by providing diversity in the technology used.

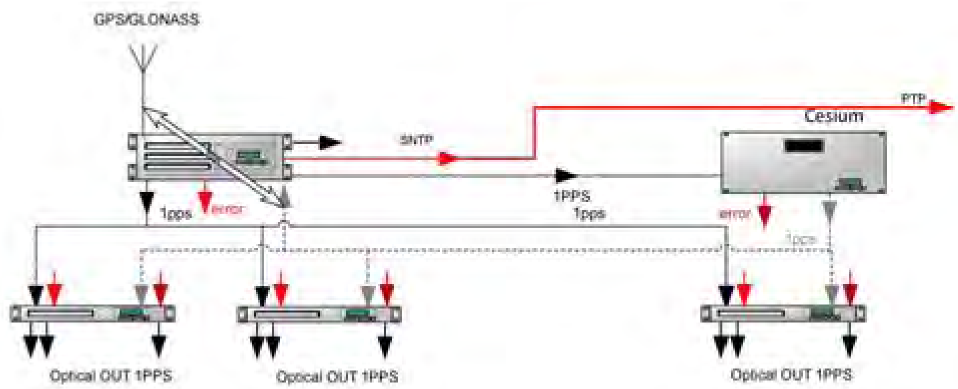


Figure 8 – Redundant Time Source System Example

Redundant time signal distribution

For the distribution of time synchronisation signals there are two main methods; to use separate physical cabling such as 1 Pulse Per Second (1PPS) signals, or to make use of the existing station bus and process bus Ethernet network infrastructure and transmit time synchronisation signals via a packet based technology such as IEEE 1588 PTP.

Packet based technology can offer a lower cost solution if it can make use of the existing process and station buses, but this can require that a great deal of devices in the substation support the IEEE 1588 C37.238 Power Profile to maintain the required level of accuracy of less than 1 microsecond, including 'boundary clock' devices such as bay controllers. At present this can be difficult to achieve but will improve as support for the Power Profile grows.

Signal distribution via physical cabling methods such as 1PPS have been in use many for many years and are well proven. To minimise single points of failure the time signalling for Main 1 protection devices should ideally not be the same as for Main 2. If economically justifiable this would entail the construction of two separate time sync signal distribution networks within the substation so that the failure of one does not affect both systems simultaneously. Where two time sources are provided, this could be achieved with optical multiplexers (Figure 8).

A completely redundant solution using physical cabling can be very cost prohibitive and would normally not be provided if back up protection functions are available that do not depend on time synchronised measured values.

Protection Function Redundancy

The location of the protection functions is not restricted when using digital substation architectures, as devices are not bound to the copper wires of instrument transformers. Measurements can be distributed freely across the substation and shared between different devices and locations on the process bus without additional wiring.

This means that we now have the possibility to economically distribute additional redundant protection functions to any location within the substation that has access to the station and process buses. For example:

1. At the point of measurement acquisition within merging units
2. In passive standby IEDs that are activated in the case of device failure
3. In active standby IEDs that continuously provide redundant backup to one or more protection IEDs

1. Redundant protection functions at the point of acquisition

Merging units in a digital substation take the function of measurement acquisition away from protection IEDs and put this function right up to point where primary measurements are taken. There is the possibility that these devices could also perform additional protection and control tasks.

The argument is that this could increase overall reliability, since if the communication link to the protection IED or the device itself were to fail, the merging unit could continue to operate independently and provide some form of backup protection (for instance an overcurrent protection function as shown in Example 2 of Figure 9 below).

While this is a form of redundancy for specific functions, it is not equivalent to a redundant Main 2 protection system since the performance it provides is less than the performance from a complete protection IED.

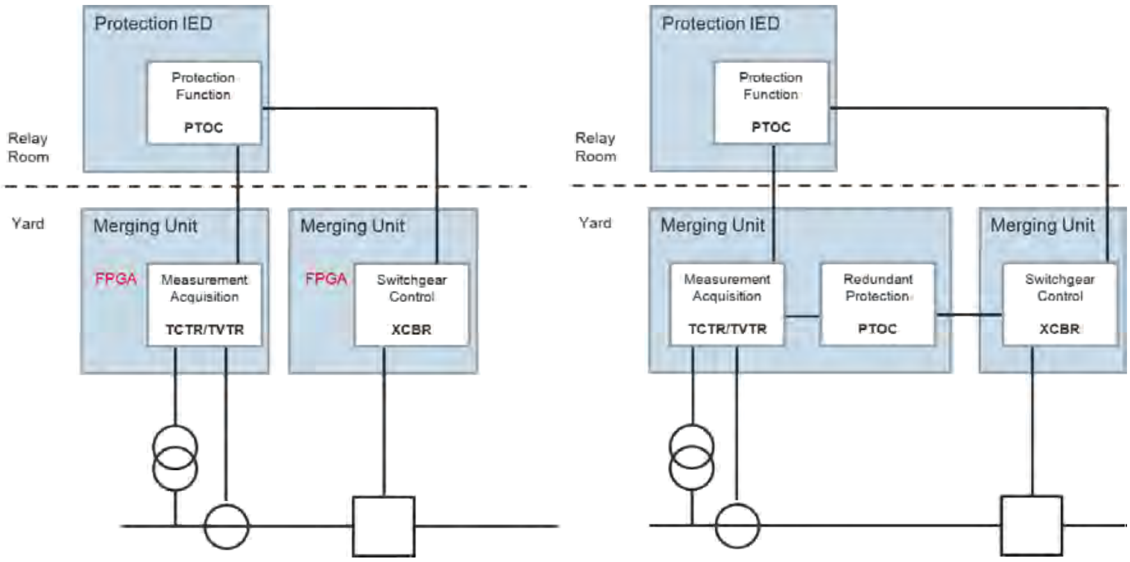


Figure 9 – Protection Functions Inside or Outside Merging Units

Whether this architecture would really provide additional reliability in an outdoor substation where merging units will typically be installed in the yard is open for debate since the design of a device suitable for such an environment, as opposed to the substation control/relay room, can be compromised if it must be sophisticated enough to perform protection functions.

The relay room is a much more climate-controlled environment; to control temperature and humidity utilities typically take a conservative approach at transmission levels, by installing heating in cold/temperate countries, and air conditioning in hot countries.

Devices deployed in outdoor marshalling kiosks in the yard do not have this luxury, in environments of extreme cold occasionally the kiosks may have a heater, but generally no heating or air conditioning is provided. This means that yard devices such as merging units need to withstand greater variations and extremes in ambient temperatures, in addition to making sure that moisture and or pollution in the air produces no degradation. They may also subject to transmitted vibrations when mounted in kiosks attached to the switchgear assembly

Because merging units should withstand these greater environmental extremes than protection IEDs, they need to be designed in such a way as to maximise reliability and to secure the highest possible MTBF (mean time between failures). This is best achieved by good design principles: deploying FMEA (failure mode effects analysis) and secondly by minimising the component count.

Devices that must perform sophisticated protection functions, in addition to measurement acquisition and switchgear control, may need to carry additional components, modules or processing. For example, they may require an additional processor for logic or ancillary tasks whereas a simple merging unit could perform all its functions in an FPGA design (Example 1 of Figure 9).

Given the recommended design for simplicity of merging units and circuit breaker controllers, this will tend to intentionally limit the additional functions that those devices can perform. They are designed to be specifically fit for purpose, as opposed to devices which claim to perform many tasks to the compromise of availability and long service life in their primary function.

In summary, the motivation to keep yard devices simple, and to perform ancillary or complex functions in the traditional location indoor in the bay, remains high. Therefore distributing redundant protection functions to yard mounted merging units may not necessarily deliver a more reliable system in practice, and it could be for the system redundancy to be enhanced that additional redundant IEDs should be installed instead, as will now be discussed.

2. Passive protection function redundancy: standby IEDs

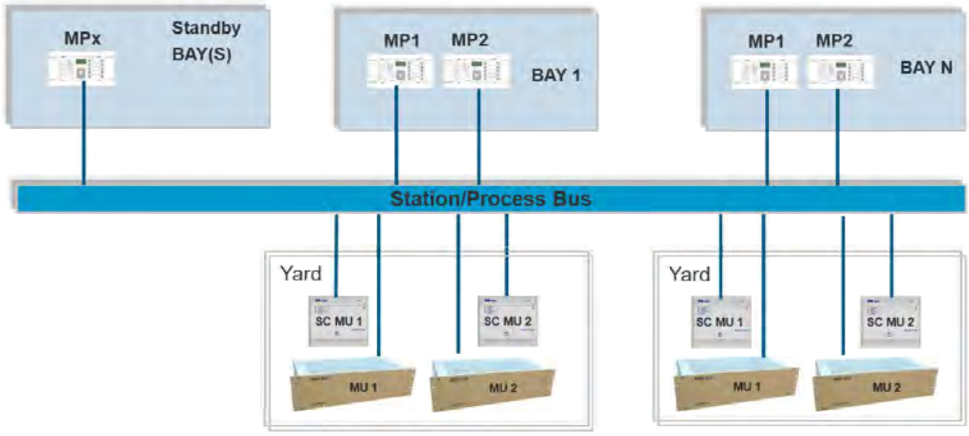


Figure 10 – Example of Standby IED

An interesting possible new redundant protection function architecture is to install an extra IED (MPx), connected to the substation buses, which will be used to replace the functions inside another IED in the case of failure. The replacement of functions can occur without having to physically touch any hardware.

In the example below, if a failure occurs in a Bay 1 protection IED (MP2). We could disable this device and activate a spare that is already installed in the substation.

The following sequence would occur under this scenario:

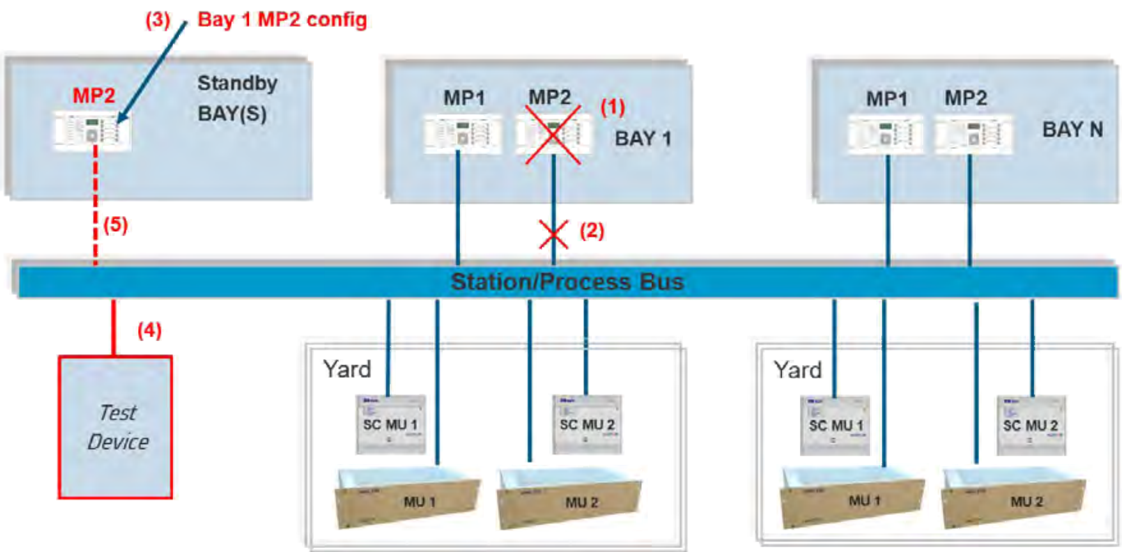


Figure 11 – Standby IED Activation Process

1. During the installation phase a spare standby device is installed in the substation that remains inactive, but can one day be configured to replace functions in one of several bays in the case of failure. The device is connected to the process bus, but does not have any subscriptions enabled.
2. If a failure occurs (Bay 1) we first isolate this device by disabling its process bus and station bus interfaces. This can be achieved by turning off the attached network interfaces in the substation switches.
3. The configuration of the faulted device is retrieved from a central location which is synchronised to the field equipment (to ensure that the settings exactly match) and loaded into the standby redundant IED.

4. The device is placed into the mode defined by IEC 61850-7-4 Ed2 “Test Blocked”. This allows for test signals to be injected into the network to prove that the configuration is correct. GOOSE signals issued by the device will be flagged as “test” so that subscribing switchgear controllers know not to trip during this testing. In this way the protection can be tested all the way up to the switchgear control merging units without having to operate primary circuit breakers or by carrying out any secondary injection.
5. The standby IED is taken out of “Test-Blocked” mode and activated so that it now replaces the protection functions that were disabled from the initial device failure.

This sequence could be performed remotely or potentially even automated in future.

The standby IED allows for reduced downtime in the case of device failure. Rather than waiting for maintenance crew to travel to the substation and replace the faulted IED the protection functions can be restored very quickly and the faulted device can be replaced at the next maintenance cycle. Thus overall reliability of the complete protection scheme can be improved.

The concept of passive protection function redundancy is actually nothing new, and already exists in some conventional substations where a Main and Transfer Bus is provided, particularly in North America. With this architecture (Figure 12) if the protection relay in Bay 1 fails, the source for this bay can be transferred from the Main Bus to the Transfer Bus. The spare line relay then selects the appropriate settings group to replace the faulted IED’s protection functions automatically based on the isolator position statuses.

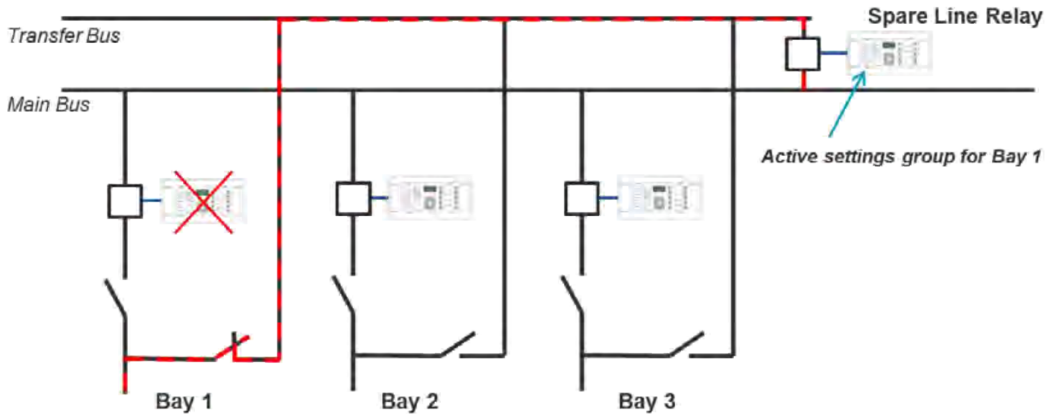


Figure 12 - Passive redundancy in a conventional substation, spare line relay application

3. Active protection functional redundancy: IEDs in parallel

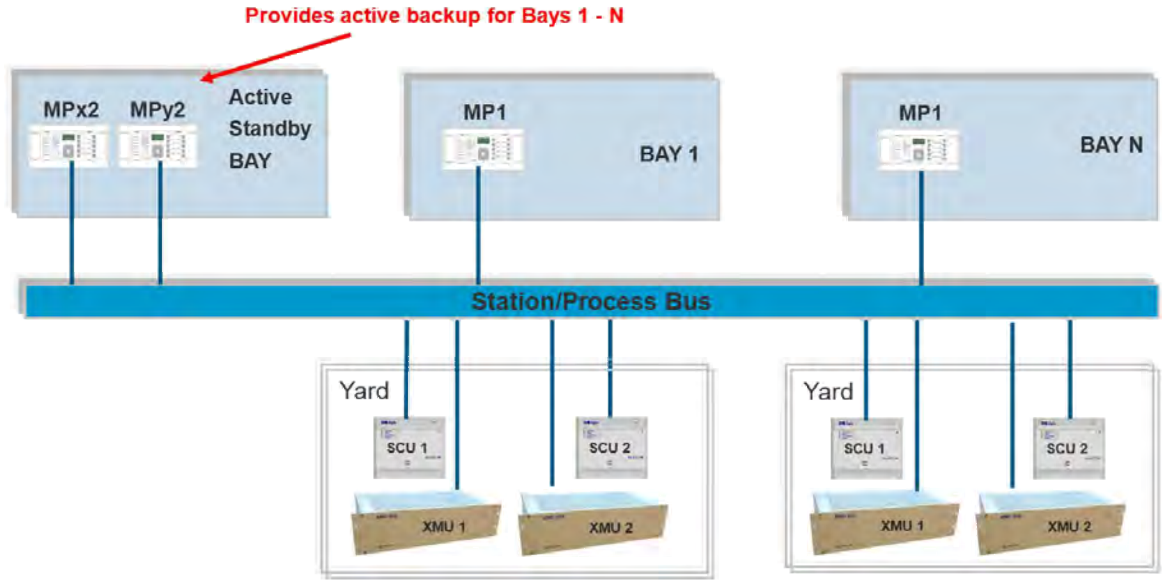


Figure 13 – Parallel Redundant IEDs Example

Taking these same principles a step further, the same redundant IEDs could be configured to actively subscribe to a number of different bays and provide active back-up protection, rather than merely be configured to provide protection in the event of device failure.

For example in Figure 13, the active standby relays may incorporate several independent functions for other bays in the substation. In the event of any relay failure in any bay, protection would still be provided. Such back-up could supplement Main 1 and Main 2 protection in each bay, or could be used in cases where there is no Main 2 protection provided.

In future such principles may lead to more centralised protection system architectures for backup protection. The redundant device could in the most extreme case, provide back-up for the complete substation.

Testing such schemes, where functions no longer reside within a single device will rely more heavily on online simulation and isolation such as the new features provided by IEC 61850 Edition 2. For example, there are now functions that are distributed across the substation that need to be isolated during testing, whereas previously isolation could be achieved by simply turning off devices in a single bay. Clearly, careful work will be required across the industry to make such architectures safe and practical.

Conclusion – Designing the Right Level of Redundancy

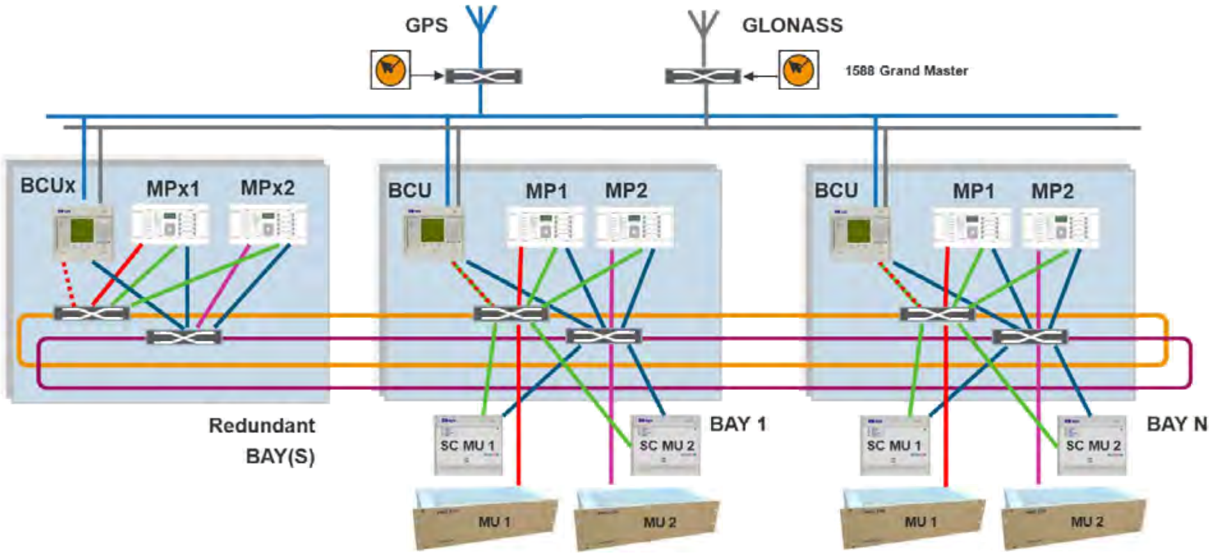


Figure 14 – Example Redundant Digital Substation Architecture

To summarise all the points that have been raised in this paper with respect to redundancy for digital substations, an example of one potential design is now presented. From the figure we see:

- Fully independent Main 1 and Main 2 protection systems, each sufficiently capable of performing independently.
- Two independent process bus LANs. One for Main 1 process information and the other for Main 2. The buses are formed using an active network redundancy protocol (HSR rings) that can selectively share information between bays such as circuit breaker position status for interlocking.
- Redundant PRP connections between the protection IEDs and switchgear control merging units (SC MUs). This shows how PRP and HSR architectures can be mixed; each port is connected to an independent HSR LAN so that every IED actually publishes and subscribes GOOSE to both a Main 1 and a Main 2 switchgear control merging unit. This is in line with the philosophy of a typical hardwired tripping scheme, where operation of any Main protection should result in the operation of both redundant circuit breaker trip coils.
- To maintain simplicity the merging units (MU1 and MU2) publish sampled values to a single LAN and are subscribed to by a single protection IED. For example the MP1 protection relay only subscribes to MU1 and not to MU2. Adequate redundancy is instead provided by duplicating the merging units and protection with independent Main 1 and Main 2 systems.
- All merging unit connections are made via a switch so that measurements can be shared to other bays. These connections are point to point as it is deemed that additional network redundancy is not necessary.
- Two redundant time synchronisation systems are provided, one with a source from GPS and the other from GLONASS to provide some diversity in technology. Each time source system independently synchronises a single Main protection system. In the unlikely event of common mode satellite signal failure (both GLONASS and GPS not being received) the substation relies on backup protection that does not depend on time synchronised values.
- A bay of standby redundant IEDs is provided that can be configured to quickly replace the protection functions residing in any other Main protection IEDs in the event of failure.

It is important to observe that different levels of redundancy are appropriate for different cases. Therefore this example is but one potential solution and is not the optimal for every single case; a trade-off will always exists between cost and reliability.

In conclusion, redundant designs that add additional complexity without meaningful increase in system reliability should always be challenged and above all, the established protection design principles used in conventional substations relating to redundancy are still valid for digital substation technology.

References

[1] *Network Protection and Automation Guide*, Alstom Grid, 2011.

[2] *Redundancy Considerations for Protective Relaying Systems*, IEEE PSRC, WG19 Report, 2007.

[3] R. Hughes, *Against and For Process Bus and Sampled Values*, Retrieved from: https://ideology.atlassian.net, 2012.

[4] M. Pustylnik, M. Zafirovic-Vukotic, R. Moore. *Performance of the Rapid Spanning Tree Protocol in Ring Network Topology*, RuggedCom, Inc

[5] IEC 62439-3, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, Second Edition, July 2012.

[6] Volpe, J.A., *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System,* National Transportation Systems Center, August 2001.

[7] Vladislav V. Demyanov, Yury V. Yasyukevich and Shuanggen Jin. *Effects of Solar Radio Emission and Ionospheric Irregularities on GPS/GLONASS Performance,* September 2012.

«SO UPS», JSC
Russian National Committee
ABS Electro

S.1.1-4. Innovative design of IEDs and functions allow flexible transformer protection applications

H-J. HERRMANN; S. SCHNEIDER
Siemens AG
Germany
hans-joachim.herrmann@siemens.com

KEYWORDS

Protection devices, IEDs, modularity of hard- and software, transformer protection, algorithms, autotransformer, phase shift and special transformers**.**

1 INTRODUCTION

Transformers are very important protective objects in the electric energy system. Therefore different protection principles as well as devices are used in the applications. From the engineering point of view the design of transformers have an influence on protection concepts. For an efficient control of the power flow phase shift transformers are installed in the energy system. These types of transformers have specific requirements on the design of the differential protection. The paper addresses different aspects in the field of transformer protection. It starts with a general discussion regarding basic design of the protection schemes and presents a concept which is used in Germany.

A further focus of the paper is the differential protection. From the practical experiences over some decades two main points are discussed. The first point is the inrush detection. Due to the different magnetic conditions as well as magnetic characteristics of a transformer an overfunction of 2nd harmonic principle is possible. In the new design an additional principle - the analysis of the current wave form analysis (CWA method) - operates in parallel. The second point is the stability during external faults. The transient performance of the current transformers plays an important role. The required transient performance factor (K_{td}) is related to the used algorithm. Due to a new method of the CT saturation detection the factor can be reduced.

An application for an autotransformer scheme with the new design of a modular hard- and software structure will be discussed. Two different differential protection functions are active in parallel in the IED. A phase to earth fault can be detected phase selective in an autotransformer bank design.

A new application area in the differential protection is the phase shift as well as special transformer application. In this field the classical design of differential protection cannot be used. That means the conventional correction of a phase shift in steps of 30 degrees. A flexible angle adaption is necessary. This allows the numerical technology due to a universal design of the transformation matrix for phase-shift correction. The basic changes in differential protection for this kind of application are presented and the differences between the typical applications are shown.

2 TRANSFORMER PROTECTION APPLICATIONS

2.1 Failures in the transformer and protection principles

As an introduction as well as a refresh of the knowledge table 1 addresses typical failures in a transformer and outside of a transformer. The following classification is used: internal electrical failure and non electrical failures as well as external failures. The right column shows possible protection principles/ devices which cover these fault types. As a conclusion different principles are necessary to detect all fault types.

Internal electrical faults	**Protection principles/devices**
Earth fault (isolated and Peterson coil grounded)	Earth fault protection (U0>)
Earth short circuits (solid or resistive grounded)	For all fault types: • Differential protection, • Restricted earth fault protection • Distance protection, Overcurrent protection • Fuses, direct overcurrent release (at smaller transformer (< 1MVA)) • Buchholz protection
2 or 3phase short circuits between the phases	
Interturn faults (short circuit of windings in one phase)	
Insulation breakdown (overload, ageing)	
Electrical faults due to broken terminal connection or contact problems on tap changer	
Non electrical faults	
Drop of oil level	• Buchholz protection • Temperature supervision • Thermal overload protection
Failure in cooling system	
Core burning	
Mechanical breaks in tap-changing gear	
External faults	
Flashover at bushings or supply lead	Identical functions as used for internal electrical faults.
Earth faults	

Table 1: Faults in a transformer and possible protection principles/ devices

2.2 Protection concept of a power transformer

The decision regarding the selected or preferred protection concepts depends on different considerations, like basic protection concept regarding main 1 and main 2 philosophy, practical experiences with the protection and transformer failures over the lifetime, internal guidelines in the utility, repair costs, influence of transformer outage on the system availability, costs of the protection as well as maintenance costs and others. With other words, there is not one standard transformer protection concept for a specific type of transformer. The technical solutions from the utilities are similar, but not identical. For important transformers (coupling as well as power transformer) in the transmission network the following concept is used in Germany (see figure 1).

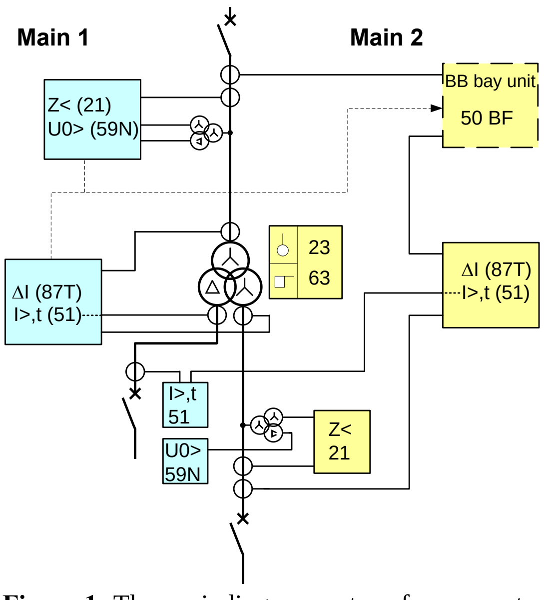


Figure 1: Three winding power transformer protection concept

Redundant protection arrangements are also applied on these transformers. The main protection is current differential protection. Furthermore Buchholz protection is used in all applications. At extra-high as well as high voltage levels, a distance protection is applied as back-up protection. On three-winding transformers, an over-current protection is applied at the medium-voltage side. The earth fault protection detects earth faults when feeding into non-earthed systems and earth-faults when feeding into earthed systems by means of the displacement voltage.
Following CB failure at the EHV side, the breaker failure protection integrated in the bay unit of the busbar protection ensures fault clearance. The differential, distance as well as Buchholz protection trip the CB on the EHV and HV side if back-feed via the medium voltage is not possible.

3 IMROVEMNTS IN TRANSFORMER DIFFERENTIAL PROTECTION

3.1 Inrush detection, Handling of CT saturation, Restraint characteristic

The basic principle of the restraint differential protection is well known since 100 years. But never the less room for improvement always exists. As a feedback from the practice, it's reported, that at an inrush the 2nd harmonic restraint function doesn't work correctly in few cases. The added cross blocked function improves the behavior, but doesn't help in all cases. Similar behavior is also reported in other technical papers. A changed magnetizing characteristic due to new transformer material leads to a lower amount of 2nd harmonics. A reduction of the pick-up threshold increases the risk of an under-function during an internal fault with CT saturation. CT saturation leads to harmonics. Well known is the 3rd harmonic, but a 2nd harmonic is also possible. Figure 2 shows such an inrush current. It looks near ideal. But the harmonic analysis showed in phase L2 a 2nd harmonics lower than 12%. A typical pick-up threshold is 15%.

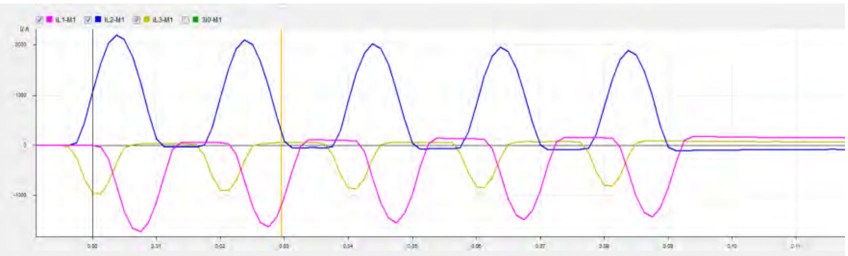


Figure 2: Inrush current of a transformer

Figure 2 illustrates a typical effect during an inrush. In the case of an inrush flat areas exist at the same time in all three phases. The evaluation of such an effect is now implemented as additional criteria. This evaluation principle is called CWA (current wave form analysis). In the present design of differential protection the CWA as well as the 2nd harmonic principle operates in parallel. With a one out of two decision the differential protection function is blocked phase segregated.
Another topic is the stability during external faults with CT saturation. Especial the dc-offset current influences the transient behavior of a current transformer. The used P –type CT's have a closed core. If a fault current with a large dc offset is interrupted by a protection the magnetizing current of all current transformers in the short circuit path moves not to zero. The magnetizing current goes to a remanence point and the CT will be further controlled from this remanence point. The distance to the nonlinear part of magnetizing characteristic becomes closer. An effective countermeasure is the application of CT with air gab. The recommendation is the application of PR-type (max. 10% remanence) instead of P-type. The question is which transient dimensioning factor (K_{td}) is required by the protection. The software realization (algorithm) has an impact. There are three challenges (see figure 3):

a) External faults with a strong CT-saturation on one side (curve A)
b) External fault with CT-saturation and evolving fault (internal fault) occurs (curve B)
c) External failure with a small fault current or load current with a large dc-offset leads to small or slight saturation (Curve C, no restraint current)

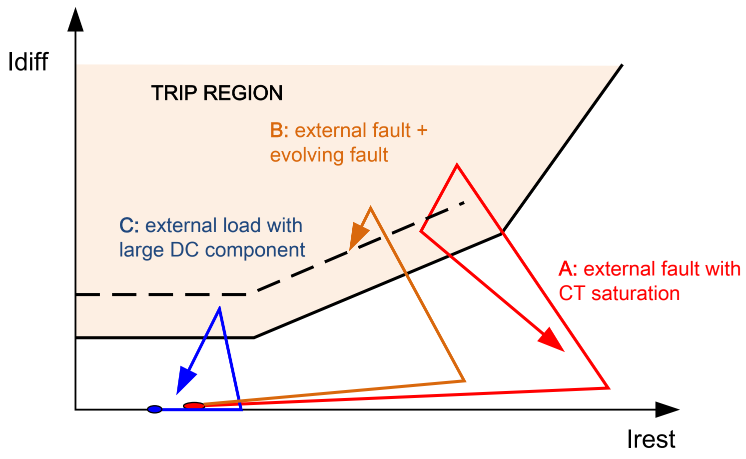


Figure 3: Different fault situation

The functional improvement deals with challenges a) and b). The trajectory of an external fault with CT saturation shows curve A and B in figure 3. The current moves in the first milliseconds after a fault occur from the load point towards the restraint axis. If saturation occurs the trajectory changed the direction and goes into the trip region. After some cycles the fault current is less saturated. The trajectory comes back into the restraint region. In the case of an evolving fault (see B) the trajectory will be stable in the trip region. In the past the evaluation of the trajectory was done with fundamental values. Now instantaneous values (sampled values) are used. With an estimation algorithm the sampled values of the future are predicted under the assumption of sinusoidal values. This method gives in the case of saturation faster a clear decision regarding an external fault. If the current is stable in the trip region an evolving fault is assumed and the trip command is released. Due to this improvement the K_{td}-factor is reduced from 3 to **2**. That means a size reduction of the current transformer. Typical for the behavior of curve C is a large dc time constant in the current and the restraint current doesn't help. If a jump in the restraint current and in parallel a dc-offset current is detected temporally the trip characteristic is increased (see dotted line in figure 3).

Another topic is the calculation of the restraint current. In technical papers different strategies are described. The main question is how to deal with the currents if on one transformer side more than one measuring point is connected (e.g. this is typical in one and a half breaker schemes). Below typical calculation variants for the restraint current are listed.

$$\mathrm{I}: \quad I_{\mathrm{Re}str} = \sum_{k=1}^{n+m} \left| \underline{I}_k \right| \tag{1}$$

$$\mathrm{II}: \quad I_{\mathrm{Re}str} = \frac{1}{m+n} \sum_{k=1}^{n+m} \left| \underline{I}_k \right| \tag{2}$$

$$\mathrm{III}: \quad I_{\mathrm{Re}str} = \left| \sum_{k=1}^{n} \underline{I}_{S1,k} \right| + \left| \sum_{k=1}^{m} \underline{I}_{S2,k} \right| \tag{3}$$

$$\mathrm{IV}: \quad I_{\mathrm{Re}str} = \underset{k=1,2,\ldots n+m}{\mathrm{Max}} \left(\left| \underline{I}_k \right| \right) \tag{4}$$

With: n, m number of measuring points on each side of a transformer

Equation (1) is a standard approach for a universal application independent from the number of measuring points. The current can be the RMS value of the fundamental current or the rectified mean value of the current. The big advantage is the high restraint current and this avoids an overfunction during external faults. Equation (2) has a different scaling of the restraint value. Equation (3) calculates the geometric sum on each side and the absolute value. Equation (4) uses a different approach. The restraint current is the maximum current from the currents of the measuring points. If the current in one measuring point goes into saturation the algorithm jumps automatically to the highest current of another measuring point. CT saturation has a lower impact on the restraint current.

Each equation has different benefits. In a one and half circuit breaker scheme can be the following situation: A transformer with a small apparent power is connected to the diameter and in the diameter flows a large current. If equations (1) is used and due to the two measuring points in the diameter a large restraint is the result. If an internal fault in transformer occurs the protection is less sensitive due to the high degree of stabilization. Equation (4) has for this application more benefits and is now used for transformer differential protection of SIPROTEC 5 family. Compared with equation (1) a modification in the settings of restraint characteristic is necessary (higher inclination values of the straight lines).

3.2 Functional Improvement, example Autotransformer

The slogan perfectly tailored fit of SIPROTEC 5, the new protection family of SIEMENS, means a high flexibility in the application due to modularity in hard- and software. The modern processor technology increases the numerical performance and allows the operation of different functions in parallel. The distance as a back-up protection for the connected line or the line differential protection can be part of transformer differential relay. Via a configurator tool an optimized hardware can be selected. This hardware includes all necessary interfaces (current and voltage input, binary in- and outputs, communication interface) for the used application. A modular hardware design supports the flexibility to change interfaces during the project design phase.

The example, protection of an autotransformer bank with a delta winding, demonstrates the performance of system. The single phase transformers are wired together. In that case the detection of the phase to earth fault as well as a phase segregated tripping (activation of the right sprinkler system) is important. In the past two separate differential protection relays were used. Now these functions run in parallel in one device. One differential protection function is the node protection. This function uses three measuring points (two measuring points from high voltage sides and one from the CT on the star point side). The main task of this function is the detection of phase to earth faults. A big benefit is the high sensitivity – fault detection close to the star point- and the phase selective signaling. The second differential protection function covers the delta winding and detects faults in the autotransformer as well as in the delta winding.

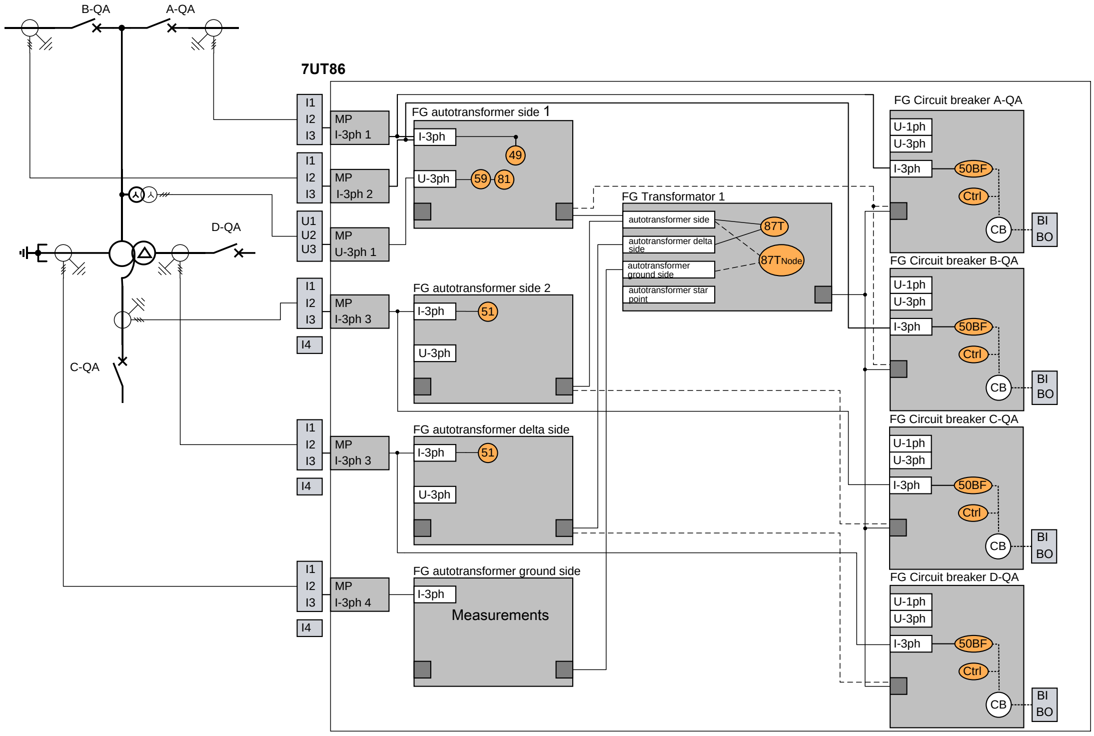


Figure 4: Interfaces and structure of the autotransformer application

Figure 4 shows the application. The autotransformer is connected on the high voltage side of a one and a half breaker scheme. Additional a voltage transformer is used for supervision of frequency and volt-

age. Figure 4 shows the internal structure of the device. This is an object oriented approach. A function group (FG) is a container which includes all necessary interfaces. In the example the function groups on the left side represent the sides of the transformer. In the middle is the FG for the differential protection functions and additional the connection of the interfaces is shown. On the right side are the circuit breaker related function groups. Visible is the interface to the four circuit breakers. In parallel to the control functionality the circuit breaker failure protection operates in this FG. This approach is close to approach of IEC61850 (object orientated functions). The FG autotransformer side routes the signals to the FG autotransformer. In a FG “side” operates also side related functions. This is illustrated with a back-up overcurrent protection (51) or with an overload protection (49), an overvoltage protection (59) and a frequency protection (81).
The allocation of functions to a FG is done with the engineering tool DIGSI 5. All allowed functions for device are stored in a library. Via drag and drop the functions can be allocated to the function group. Due to the known interfaces the tool checks which functions can be loaded into the device. To guarantee the real time performance – trip of a function in the specified time – in the back ground a load model supervises the performance. If the maximum allowed load is exceeded, the model gives an alarm and the engineered functionality cannot be loaded into the device.

Figure 5: SIPROTEC 5 (left front view, right view possible backward view with different modules)

Figure 5 shows the hardware of the device. The hardware modularity is visible. On the left side is the so called base module which contains the CPU, communication interfaces (plug-in modules are used), the power supply, 8 current inputs and binary inputs and output. To fulfill all requirements for the necessary interfaces $^{1}/_{6}$ 19” expansion modules can be added. For the shown application of figure 4 in total 20 current and 4 voltage inputs are required. This leads with the available expansion modules to a device size of $^{2}/_{3}$ 19”. With the configured boards 19 binary inputs and 17 binary outputs are available. Additional two plug-in modules can be added. That means 4 serial interfaces are available for different communication task.

4 IMROVEMNTS FOR PHASE SHIFT AND SPECIAL TRANSFORMER APPLICATION

4.1 Basic concept

Phase shift transformers (PST) are used for regulating the phase-angle shift to control the active power as well as the reactive power flow in a high-voltage power system. The installation is between the power systems or in a parallel line to control mainly the active power flow. Figure 6 shows the basic idea of the power control. A changing of the angle δ influences the active power flow (see the equation in figure 6) between the source and the load side.

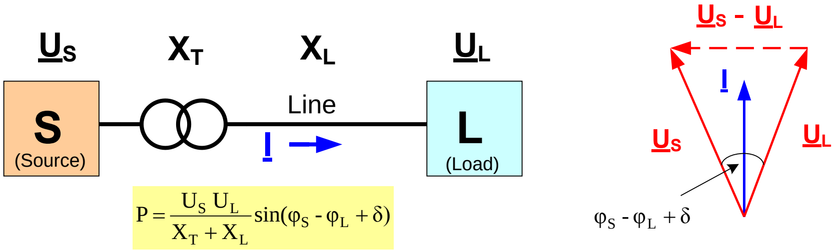


Figure 6: Application of PST, basic principle

In practice two basic designs of PST's are exists. The *single core* design contains all necessary windings on a 3phase transformer core. When the angle is adjusted, the output voltage does not change linearly. To compensate the change of the voltage an additional transformer with in-phase regulation is used. The phase angle shift in a single core design is realized with 90° or 60° phase-angle regulation. The benefit of this transformer type is simplicity and economy. The on-load tap changers (OLTC) are connected to the system and directly exposed to all overvoltages and through faults. The short-circuit impedances of the PST varies depending on position of the tap changer. The *two core design* uses two separate cores (series unit and main unit). A single-tank and a two-thank design is possible. For larger apparent power of the PST the two-tank design is required. The advantage of the two-core design is the flexibility in selecting the step voltage and the current of the regulating winding. The tap changer does not carry the load current. The absolute value of the voltage does not change with the angle change. Figure 7 shows the principle design of both types of PST. The protection concept of the two core design depends on the location of the Advanced/Retard (A/R) switch. If the A/R switch is inside of the delta winding (shown in figure 7) the position of A/R must be considered in the protection solution. That means the phase angle 0° (vector group 0) or 180° (vector group 6) must be considered by the protection. In a single core design each position of the tap changer (phase angle shift and voltage step) must be evaluated.

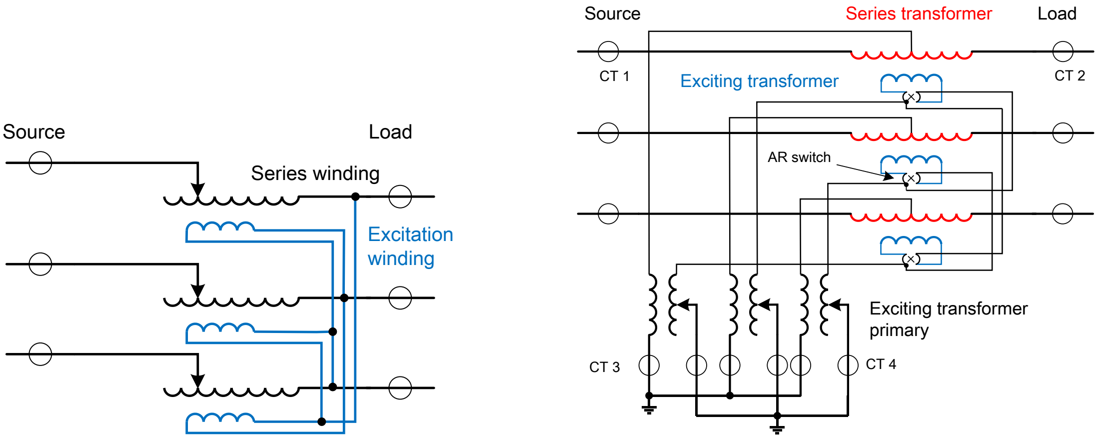


Figure 7: Phase shift transformer (left: unsymmetrical single core design; right: two core design)

Special transformers have a fixed connection of the windings. But the phase shift is not in steps of 30°. For example a phase shift of 7.5° is possible. Special transformers are used as inverter transformer with different windings depending on the inverter design (12 or 24 pulse inverter). The main reason for such a design is the reduction of the ripples in the direct current.

To achieve all the different applications a modification in the transformation matrix was implemented. For standard transformers the different vector groups (phase shift is a multiple of 30°) are used. In the universal approach the phase angle shift of the application can be set and the numerical protection calculates internally the values of the transformation matrix. For the single core application the calculation must be done for each step position of the tap changer. The principal design of the transformation matrix illustrates equation (5).

$$\begin{pmatrix} I^{**}_{L1} \\ I^{**}_{L2} \\ I^{**}_{L3} \end{pmatrix} = \begin{pmatrix} f(\alpha) & f(\alpha-120°) & f(\alpha+120°) \\ f(\alpha+120°) & f(\alpha) & f(\alpha-120°) \\ f(\alpha-120°) & f(\alpha+120°) & f(\alpha) \end{pmatrix} \begin{pmatrix} I^{*}_{L1} \\ I^{*}_{L2} \\ I^{*}_{L3} \end{pmatrix} \qquad (5)$$

f(α)	trigonometric transformation function
$I^{*}_{L1,2,3}$	Magnitude corrected current (correction of CT- and tap changer mismatching)
$I^{**}_{L1,2,3}$	Phase angle shift corrected current

The transformation function has such a design that the transformation parameters for the standard vector groups correct achieved. Due to new design the differential protection function is optimal adopted for different applications. This allows a sensitive setting for PST as well as special transformers.

4.2 Application example

In a single core application a differential protection with two measuring points can be used (see figure 7). The protection reads additional the position from the tap changer. In a tabular form for each tap position the angle shift and the changed voltage is set. According to the tap position the actual voltage is used for the adaption of the current (see I^{*}_{Lx} in equation (5)) and the set phase shift is the basis for the calculation of the transformation matrix parameters. Figure 8 shows as an example the differential and restraint current of a PST under load. The adaption works perfect and the differential current was close to zero at a tap changer position with a phase shift of -8.47°.

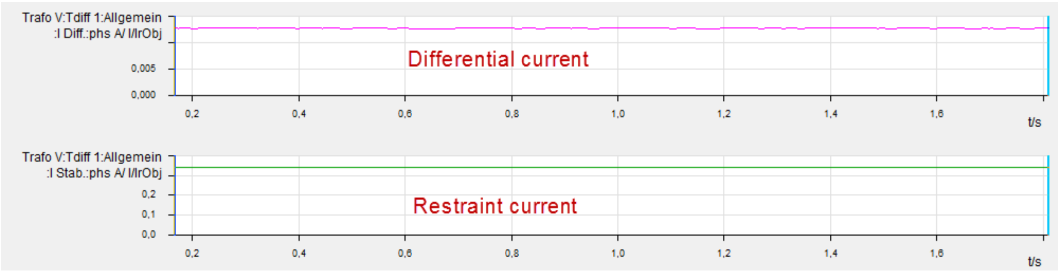


Figure 8: Measured I_{diff} and I_{Restr} of a single core PST

For a two core transformer application it is not necessary to consider the tap changer position. Only the position of the AR switch must be evaluated. That means a changing of the vector group from 0 (0°) to 6 (180°), if the AR switch is activated. To achieve all fault locations a primary as well as a secondary differential protection is necessary. Both functions are integrated in one SIPROTEC 5 device. The primary protection is a pure node protection. According figure 7 the CT1, 2 and 3 are used. The secondary protection uses the following CT triple: CT1, CT2 and CT4. CT4 is connected on the regulating winding of primary excitation transformer. The secondary protection uses two binary inputs to evaluate the position of the A/R switch. For the time where the A/R switch is activated the restraint stage Idiff> of the differential protection is temporarily blocked. This countermeasure is necessary to avoid an overfunction. The fast stage Idiff>> with an insensitive setting is always active.

5 CONCLUSION

In the paper different aspects of transformer protection are presented. After a brief discussion of possible failures and protection functions a typical protection schema was presented. The main protection is the differential protection. For this protection principle as lessons learnt from the practice some improvements are discussed. This was inrush detection, CT saturation detection and the restraint current calculation. Application of phase shift transformer as well as special need a new transformation matrix for the phase shift adaption. The general idea was presented. This universal matrix is now used for all applications.

Modern technology of hard- and software allows a flexible design. This was presented in an autotransformer bank application. New is that two differential protection functions work in parallel. In the past two separate devices were necessary. In last chapter the subject of PST and special transformers was presented. The two types of PST –single and two core design – are brief discussed and some application notes are given.

REFERENCES

[1] Mueller, N., Herrmann H-J. / Protection of phase shift transformers – application examples // CIGRE B5 conference in Belo Horizonte, Brazil (29 August 2013) PS3 paper 311

[2] SIPROTEC 5 Transformer differential protection 7UT82, 7UT85, 7UT86, 7UT87. Siemens AG, manual C53000-G5040-C016-5, 2014.

Actual Trends in Development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

S.1.1-5. Simplifying Teleprotection Communications With New Packet Transport Technology

D. DOLEZILEK, C. GORDON, D. ANDERSON, S. MCCREERY, and W. EDWARDS
Schweitzer Engineering Laboratories, Inc.
USA
dave_dolezilek@selinc.com

KEYWORDS

Generic Object-Oriented Substation Event (GOOSE), software-defined networking (SDN), middlebox, North American Electric Reliability Corporation (NERC), OpenFlow™, protection-class Ethernet network (PCEN), Parallel Redundancy Protocol (PRP), Rapid Spanning Tree Protocol (RSTP), virtual local-area network (VLAN).

1 INTRODUCTION

Availability, reliability, and simplicity are major metrics in the world of teleprotection communications. Protection applications based on exchanging command signals once thrived in the realm of analog signal and dedicated point-to-point communications links. Due to the trend of combining all communications on an Ethernet network (a shared-bandwidth communications medium by design, illustrated in the relevant IEEE standards), protection signals are being published over a network that was never meant to offer message delivery deterministic enough—or deterministic at all—for mission-critical applications.

A new Ethernet packet transport technology, software-defined networking (SDN) and its open-source protocol incarnation, OpenFlow™, promises to revolutionize the ways that traffic engineers design, build, operate, and maintain critical networks. OpenFlow promises improved performance on Ethernet networks via granular control over Layers 1 to 4 of the Open Systems Interconnect (OSI) model. It also promises to give network engineers the ability to abstract teleprotection communications out of the Ethernet world and back into the realm of dedicated virtual circuits without sacrificing simplicity, flexibility, and reliability. OpenFlow-enabled Ethernet hardware further promises the ready availability of inexpensive, nonproprietary hardware that can be modeled and controlled like a software application programming interface (API) and the elimination of the need for most proprietary Ethernet management protocols.

This paper provides a description of the requirements for protection-class Ethernet networks (PCENs) and the benefits of using SDN technology over traditional networking.

2 IMPLEMENTING END-USER REQUIREMENTS FOR PCENS USING TRADITIONAL NETWORKING TECHNOLOGIES

End users of mission-critical communications networks typically prioritize speed, reliability, maintainability, dependability, and security.

2.1 Speed

The transfer time specified for an application is the time allowed for a signal or data exchange to travel through a communications system. IEC 61850-5 illustrates transfer time (shown in Figure 1) as the time duration between the action of communicating a value from the logic processing of one device to the logic processing within a second device as part of an application [1]. Transfer time includes the time to execute the communications processing algorithm in both the source and destination device and the transit time. Designs for PCENs do not influence source and destination device behavior and affect only the message delivery via network middleboxes and links. The designs are concerned with the transit time, t_b, which is the time duration for the message to travel through the communications network.

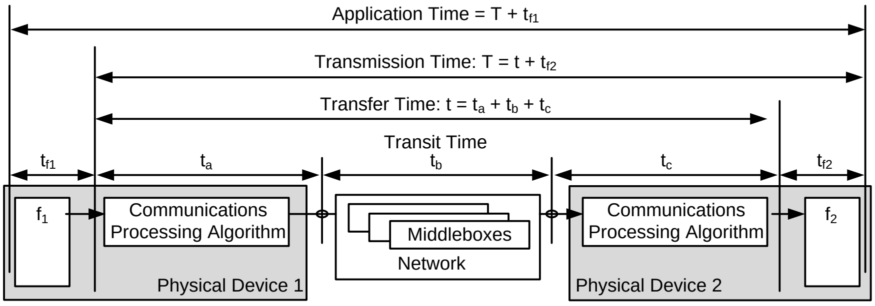


Figure 1: Transmission time and transfer time illustration based on IEC 61850-5 [1]

IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines clarifies many performance and test requirements [2]. Of note, it simplifies the discussion of transfer time requirements by documenting time classes for different types of messages and their associated transfer times, as shown in Table 1. Using the IEC/TR 61850-90-4, network engineers can accurately specify and design local-area networks (LANs) to satisfy a transfer time class without the need to understand the underlying protection and automation applications.

Transfer Time Class	Transfer Time (ms)	Application Example
TT0	>1,000	Files, events, and log contents
TT1	1,000	Events and alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases and status changes
TT6	3	Trips and blockings

Table 1: Transfer time class applications and requirements based on IEC/TR 61850-90-4 [2]

2.2 Reliability, Dependability, and Security

The IEC/TR 61850-90-4 technical report defines latency of communication as the delay between the instant that data are ready for transmission and the moment they have been completely received at their destination(s) [2]. IEC 61850-5 describes the traffic recommendations specific to IEC 61850 [2]. It does not identify the other necessary traffic on the IEC 61850 Ethernet network for maintenance, telephony, video surveillance, and so on.

IEC 60834 requirements for reliability, dependability, and security guide engineering design criteria [3]. Networks must be available to deliver messages (reliability), to accomplish operations (dependability), and to prevent unwanted operations due to error or intrusion (security). From the recommendations for IEC 61850 Ethernet traffic in IEC 61850, it can be seen that Generic Object-Oriented Substation Event (GOOSE) communication used for protection has the highest priority and the shortest maximum delay. Control blocking schemes, via GOOSE or any other method, require a 99.99 percent success rate (dependability), and direct control schemes require a 99.9999 percent success rate of receipt of digital messages (reliability). Direct tripping, via the delivery and processing of a GOOSE or other message, is typically expected to occur within 20 milliseconds [3]. Failure is defined by the absence of the message at the receiving end or, for direct control, a delay in delivery greater than 18 milliseconds. Therefore, IEC 61850 Type 1A, Performance Class P2/P3, as part of a communications-assisted protection scheme, requires that the system meet the 3-millisecond transmission time 99.9999 percent of the time (identified as TT6 in Table 1) and have a delay of no longer than 18 milliseconds for the remainder.

3 IMPLEMENTING THE ETHERNET NETWORK BETWEEN IEDS PERFORMING DIGITAL SIGNALING

The speed, reliability, dependability, and security of mission-critical communications-assisted applications are directly affected by the intelligent electronic devices (IEDs) exchanging signals, referred to as Physical Device 1 and Physical Device 2 in Figure 1. However, the devices that make up the communications network, referred to as middleboxes (illustrated in Figure 1), have as much or more impact on packet delivery and therefore the performance measures of speed, reliability, dependability, and security for these applications. The scope of this paper is to discuss current and new developments in the network technology available to measure and improve the speed, reliability, dependability, and security of the transport of Ethernet packets through the network, with speed measured as the transit time in Figure 1.

From the previously mentioned standards for teleprotection security and reliability comes a number of related requirements for the Ethernet network or middlebox hardware itself.

3.1 Minimal Failure Recovery Times

Applications require fast and seamless communications recovery times both for middlebox hardware and Ethernet link failures. Traditionally, spanning tree algorithms (STAs) in each middlebox share data via Rapid Spanning Tree Protocol (RSTP) (particularly IEEE 802.1D-2004), which publishes Bridge Protocol Data Unit (BPDU) packets to communicate with other Ethernet middleboxes. This exchange provides information used by the STA to identify duplicate paths to a network address and forces one into hot standby because only one link can be active at a time. This same method identifies and logically breaks data flow loops by deactivating links and putting them in hot standby mode. Also, dual active connections to IEDs are not possible. When an IED is physically dual-connected, an STA disables one link and forces it into hot standby mode. When a middlebox failure (bridge death) or link failure (link loss) occurs, an STA executes in each middlebox to optimize a current RSTP network via statuses received within BPDUs published from other middleboxes. Next, each STA determines how to enable hot standby paths to reconfigure the network around the failure. Parts of the network that are affected by this reconfiguration may be unavailable to deliver packets during the transition period or period of network darkness. The ladder topology ensures fast reconfiguration times, but ring topologies take much longer [3]. During reconfiguration after a failed middlebox or link, the ladder topology with standardized and fast STA recovers every non-root bridge failure scenario in less than 15 milliseconds. It even resolves some root bridge failures in this time and resolves others in just slightly longer. However, any ring topology larger than three middleboxes will not reconfigure in less than 15 milliseconds [3]. Test and measurement of a four-node ring of middleboxes with traditional STA performance reveals transit latencies that grow from hundreds of milliseconds to tens of seconds.

3.2 Minimal Network Transit Latency Times

End users typically specify “latency low enough to satisfy the application” and leave the definition and design up to the network engineer. A common error is that engineers will assume that any Ethernet topology will satisfy latency and they will choose topologies based on low cost and convenience such as a ring. However, this ignores the first important step of engineering design where transit times for GOOSE messages and Sampled Values (SVs) messages must be less than 1 millisecond [1]. This transit time of 1 millisecond, combined with the duration of the subscriber communications processing algorithm illustrated as t_c in Figure 2, must aggregate to a transfer time of less than 3 milliseconds, as shown in Table 1. The overall message transit time through networks constructed as small rings and large and small ladder topologies is less than 1 millisecond when a small number of middleboxes exists between the GOOSE producers and consumers. Transit time is so small that it is often not measureable without very precise equipment. However, as rings grow in size, transit time grows as well and will eventually be longer than 1 millisecond when the number of middleboxes in the path between each GOOSE producer and consumer grows large enough. The challenge is that this change in latency is due to the ingress, egress, and switching delays associated with packets passing through each middlebox. When the number of middle boxes in the path cannot be predicted in advance, the system requires thorough testing of every message exchange scenario. An important benefit of the ladder topology is that all possible middlebox configurations are predictable and measurable to match results found during research of the design. Transit latency is calculated by aggregating the ingress and egress port delays on each middlebox plus the switching time within each middlebox the packets pass through. The time for packets to traverse all physical links is added. The physical link time is calculated as the speed of light through fiber over the link distance.

3.3 Per-Link and Per-Host Bandwidth Calculations

End users often require engineered calculations for bandwidth provisioning of application communications traffic, including the bandwidth consumption per host completed during the design stage. Protection engineers must calculate per-link bandwidth using per-host bandwidth calculations to ensure that link bandwidth capacities are not exceeded and thereby reduce the chances of dropped protection-related packets. In the ladder topology, all traffic is segregated so that the only traffic allowed on each ladder segment is the collection of messages required for the IEDs and devices on that segment. This filtering and blocking of all unneeded traffic at the links between middleboxes prevents unnecessary packet processing and link oversubscription and saturation, which can lead to packet transit delays. Ring topologies force all traffic through each and every link, which creates a lot of unnecessary packet processing and eventually leads to oversubscription and link saturation, resulting in unacceptable packet transit delays. However, even with correct bandwidth provisioning in ladder and ring topologies, the nature of shared bandwidth links makes it impossible to guarantee performance. Other topologies are even more unpredictable and nondeterministic. Ethernet provides Class of Service (CoS) and prioritized packet processing, but it cannot provide quality of service, guaranteed latency, or determinism, especially because bandwidth usage varies so widely during both normal and abnormal circumstances.

3.4 System Performance Testing

In order to guarantee performance of the protection system, traffic engineers are tasked with both testing the system under normal loading with real or simulated traffic and under stress by emulating various failure scenarios. For all nonladder topologies, this process is extremely time intensive and manual because almost all PCENs are tailored to specific end-user requirements and there are no test examples available to show the runtime behavior without all physical hardware and links present. Also, the performance characteristics of the systems change each time new traffic or new nodes are added, which also requires new testing.

When these tests are performed on ladder networks, the measured times match calculated transit times, which confirms that the calculation method can be used without testing to simplify the verification process. Also, ladder behavior does not change when new traffic or new nodes are added to other LAN segments. Rings are tested with worst-case traffic conditions, but each link must be measured because they cannot be calculated. Unlike ring behavior, the performance of ladder topologies does not change each time new traffic and new nodes are added.

3.5 Separation of Traffic by Type and Application

Shared-bandwidth networks require that all system application traffic traverse the same links and that different traffic types be logically separated to further ensure the reliability and predictability of the PCEN. In some mission-critical applications, designs still specify that supervisory control and data acquisition (SCADA), synchrophasor, and engineering access communications be isolated onto a physical link separate from protection traffic in order to remove the possibility of protection packets queueing due to collisions. This is done by creating a second, smaller LAN for GOOSE only and separating it from the combined traffic LAN via IEEE 802.1 virtual LANs (VLANs). Traditional Ethernet does not support the separation of Layer 3 SCADA, engineering, synchrophasor, and maintenance traffic because they all share the same Ethertype for IP. When this capability is needed, complex middleboxes with routing capabilities must be added and configured to ensure the separation of Transmission Control Protocol/IP-based (TCP/IP-based) communications.

3.6 Maintainability

Internal end user information technology (IT) staff often know the methods for business IT networks but not the requirements for mission-critical operational technology (OT) for PCENs. Unfortunately, users of Ethernet for OT often become aware of their lack of in-house Ethernet OT networking skill after systems fail in service. At that time, IT staff become involved but are not prepared for building and maintaining PCENs with OT requirements. OT designers and IT staff should collaborate during the specification and design of systems. Also, end users often rely on contractors to build the networks, but they need the ability to maintain the networks themselves in the future and check system statuses, add or remove devices and hardware, or troubleshoot the system. Therefore, end users require that PCENs be as easy to maintain, understand, and troubleshoot as possible. Technologies used to implement PCENs should be nonproprietary to prevent reliance on specific individuals or a single manufacturer for success. Post-implementation concerns should not be understated; simple tasks, such as replacing a middlebox, become extraordinarily expensive and time intensive if the system operation is not well understood. This, in turn, leads to poor reliability and performance of the protection system, which relies on this new and difficult to maintain communications network.

3.7 Cybersecurity

Due to the criticality of PCENs, most end users view cybersecurity as important for overall system reliability. Due to the growing threat surface for multilevel cyberattacks, as well as growing regulatory pressure, cybersecurity should be considered equally important to application reliability and security. PCENs need to protect the availability, performance, integrity, and the confidentiality of information transferred as packets for OT and IT functions. Securing PCENs against growing malware threats over a long period of time is a difficult task that requires constant attention to intrusion prevention systems (IPS) and the added complexity of processor-intensive deep-packet inspection (DPI) devices.

4 INTRODUCING SDN

SDN essentially allows networks to be managed as a single asset, giving network operators extremely granular levels of control over network functionality while simultaneously abstracting the complexity into a more traditional and functional programmatic interface. The effects of the abstraction and granular control are the simplification of the operation of the network, the ability for continuous monitoring in more detail, and holistic, centralized network control over the programming of individual middleboxes.

The fundamental shift in networking brought by SDN is the decoupling of the systems that decide where the traffic is sent (i.e., the control plane) from the systems that perform the forwarding of the traffic in the network (i.e., the data plane). The traditional network deployment process begins with designing the topology, then configuring the various network devices, and, finally, setting up the required network services. For traditional Ethernet PCENs, engineered to optimize speed, reliability, maintainability, and cybersecurity, the application data must flow on links determined by the various distributed STAs in the middleboxes supported by information published in RSTP packets. Messages must be designed with traffic control methods, including IEEE 802.1Q VLANs and media access control (MAC) addresses. In large networks, trying to match the network-discovered path with an application-desired data path may involve changing configurations in hundreds of devices with a variety of features and configuration parameters. All of this happens in addition to the traditional STA network monitoring to avoid loops, improve route convergence speed, and prioritize protection traffic. This complexity in management arises from the fact that each middlebox has the combination of control logic and data-forwarding logic integrated internally. For example, in traditional PCEN implementations, each Ethernet switch must run STAs and the switches exchange data in an iterative fashion to make network decisions. This takes time. Furthermore, the control plane in a traditional network is distributed among the STAs in the middleboxes, and as a consequence, changing the forwarding behavior of a network involves changing the configurations of many (potentially all) middleboxes. With respect to the IEDs, SDN eliminates the need to disable duplicate connections to

IEDs and looping connections in networks. By defining the behavior of these paths, SDN allows them to be actively used simultaneously. Therefore, all Ethernet connections to the IEDs and middle boxes are used as designed and none are forced to hot standby mode.

SDN is a new architecture in networking that simplifies network management by abstracting the control plane from the data plane. Figure 2 illustrates the building blocks of SDN, which are discussed in the following subsections.

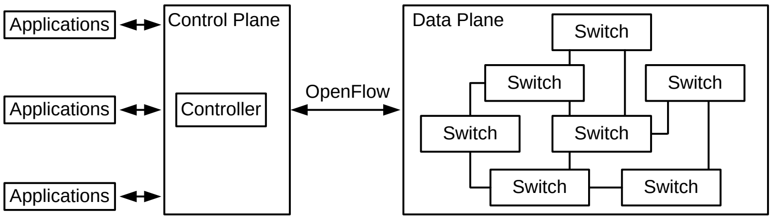


Figure 2: SDN architecture overview [4]

4.1 Control Plane

At the heart of SDN is a controller that embodies the control plane. Specifically, controller software determines how packets (or frames) should flow (or be forwarded) in the network. The controller communicates this information to the network devices, which constitute the data plane, by setting their flow tables. This enables centralized configuration and management of a network. Many free, open-source controllers, such as that of the Linux Foundation OpenDaylight initiative [5], are readily available. Essentially, the controller manages the data flow algorithms and sends rules out to the middleboxes each time the network changes. If the network does not change after commissioning, such as in substation and industrial applications, the rules do not need to change. These rule sets are much faster, more precise, and give more control of packet flow management than iterative STAs.

4.2 Data Plane

The data plane consists of network devices that replace switches and routers. In SDN, these devices are very simple Ethernet packet forwarding devices with a communications interface to the controller to receive flow information. Many manufacturers today provide packet forwarding devices that are SDN-enabled. These devices quickly execute rules for data flow to improve packet transit speed, reliability, availability, and dependability.

4.3 Control and Data Plane Interface

SDN requires a communications interface between network devices and the controller, as is evident from the description of control and data planes. A standardized interface between them will allow a controller to interoperate with different types of network devices and vice versa. The criterion for such a protocol is that is as widely supported as possible, with industry adoption by major switch and router manufacturers. However, it should be noted that any such protocol is simply a building block in the SDN architecture, and there are other open Internet Engineering Task Force (IETF) standards or manufacturer-specific standards that are either already available or are being developed.

5 IMPLEMENTING THE SDN COMMUNICATIONS INTERFACE WITH OPENFLOW

OpenFlow is a protocol developed by the Open Networking Foundation (ONF) to fulfill the need for a communications interface for SDN [6]. OpenFlow enables one or more OpenFlow controllers to define the path of packets through an Ethernet network by manipulating the packet flow tables of OpenFlow-enabled hardware. OpenFlow provides four primary functions to help a controller make packet flow decisions based on packets entering the data plane of OpenFlow-enabled network hardware: matches, actions, counters, and statistics.

5.1 OpenFlow Matches

When a packet first ingresses the port of an OpenFlow-enabled network middlebox, the device examines the packet in an attempt to match fields, as illustrated in Figure 3a, to one or more flow tables that have been defined by the OpenFlow controller(s).

(a)

Physical Layer (OSI Layer 1)				
Logical Port ID	Physical Port ID	Metadata	Tunnel ID	
Data Link Layer (Ethernet, OSI Layer 2)				
Source MAC	Destination MAC	Type/ Length	VLAN ID	VLAN Priority
Network Layer (OSI Layer 3)				
IP DSCP	IP ECN	IP	IP Src Address	IP Dst Address
Transport Layer (OSI Layer 4)				
TCP Source Port	TCP Destination Port			
ICMPv4/ICMPv6 Type	ICMPv4/ICMPv6 Code			

(b)

Physical Layer (OSI Layer 1)				
Forward Logical Port ID	Set Queue ID	Forward Group ID	Set Tunnel ID	
Data Link Layer (Ethernet, OSI Layer 2)				
Set Source MAC	Set Destination MAC	Set Type/ Length	Set/Push/Pop VLAN ID	Set VLAN Priority
Network Layer (OSI Layer 3)				
Set IP DSCP	Set IP ECN	Set IP	Set IP Src Address	Set IP Dst Address
Transport Layer (OSI Layer 4)				
Set TCP Source Port	Set TCP Destination Port			
Set ICMPv4/ICMPv6 Type	Set ICMPv4/ICMPv6 Code			

Figure 3: OpenFlow possible match fields (a) and OpenFlow possible actions list (b)

If the ingressing packet does not match the present flow table, then the device can drop the packet, forward the packet to the OpenFlow controller for inspection, or forward the packet to another flow-table. If the packet matches an entry in the flow table, then the OpenFlow-enabled middlebox may then add one or more actions to the action set for the packet.

5.2 OpenFlow Actions

Various actions can be performed on packets that have matched a flow table, including copying, setting, or otherwise manipulating Ethernet/IP packet headers. The action set of the packet can also be marked to forward to other flow tables, groups of physical redundant or load-balancing ports, or metering groups for rate-limiting functions. See Figure 3b for a list of possible OpenFlow actions. For each packet, the OpenFlow middlebox can also apply actions immediately to the packet, bypassing the current action set altogether, output the packet to a physical port, and perform other action set manipulation functions (such as clearing or updating flow tables).

5.3 OpenFlow Counters

Counters are maintained on OpenFlow-enabled middleboxes for every flow, flow table, port, group, and other point of interest. These counter data are polled by the OpenFlow controller to maintain granular data about the status of the network system as a whole.

Using OpenFlow matches, actions, and counters, an OpenFlow controller exercises complete, granular control over an Ethernet network while maintaining detailed information about the state of the Ethernet system without any additional protocols.

6 IMPLEMENTING END-USER REQUIREMENTS FOR PCENS VIA SDN TECHNOLOGY AND OPENFLOW

6.1 Speed and Reliability

6.1.1 Minimal Failure Recovery Times

Using the OpenFlow controller, logic is developed by network engineers to pre-engineer failover scenarios per middlebox and per link and then update the flow tables in all OpenFlow middleboxes with this precalculated logic. By using advanced failover algorithm techniques, it is possible to automate the calculation of advanced failover scenarios that would effectively reroute traffic with only the loss of the Ethernet frame that is currently on the affected link.

Therefore, appropriate engineering design based on OpenFlow creates networks in which the loss of a network link only directly affects the two OpenFlow middleboxes that are connected to it. Redundancy of links is easily performed by grouping ports together so that, on packet egress, the highest priority port currently “up” is used for the outgoing packet to the next hop or its final destination. In cases where ports are not grouped, it is possible to use logic to send a packet back out the original port from which it ingressed. This is impossible with traditional Ethernet but possible with OpenFlow and serves the purpose of redirecting traffic back into a switch for the purpose of resending it out an alternate port. With OpenFlow, using granular-enough rules, it is possible to ensure the safety of packets traversing links except for scenarios where a link fails while the packet is traversing the link itself or packets are queued in the outgoing port of the middlebox hardware.

6.1.2 Minimal Network Transit Latency Times

While OpenFlow methods alone do not automatically determine the shortest path between hosts, OpenFlow does provide the ability for network engineers to more easily implement network-specific algorithms that provide this, even for large networks. Furthermore, latency can be reduced for GOOSE message packets by implementing action logic in the very first flow table on the OpenFlow-enabled hardware, effectively minimizing the amount of logic to get the packet from one port to another. Furthermore, OpenFlow provides a built-in traffic shaping ability that can prioritize protection traffic without requiring the classical CoS IEEE 802.1Q tags.

6.1.3 Per-Link and Per-Host Bandwidth Calculations

SDN offers distinct advantages when it comes to bandwidth calculations. OpenFlow methods are capable of not just rate-limiting unicast, multicast, and broadcast traffic, but can limit any flow matching a particular flow table entry. OpenFlow is further able to take advantage of a traffic whitelist capability to simply allow only certain specific data types to be forwarded to a host on a strict preset bandwidth. A traffic whitelisting model is able to provide the most protection-based security for the link because it can simply drop unexpected traffic flow that may otherwise cause link or host availability problems. Because OpenFlow hardware can be modeled entirely in software by using emulators such as Mininet [7], bandwidth calculations of expected traffic based on predicted applications can be modeled accurately without the need for physical middleboxes, SCADA hardware, or protection devices. These calculations must next be considered in light of any additional network traffic. OpenFlow's statistical gathering capabilities via counters also provide an easy method of retrieving detailed bandwidth data for real-time data flow analysis. The OpenFlow counter capabilities are granular enough to be able to gather data on both the hosts and the link, even under dynamic conditions.

6.1.4 System Performance Modeling and Testing

Because an SDN system can be modeled entirely in software, the OpenFlow controller, middlebox hardware, and most any traffic type can be modeled on one or more computers without hardware being involved. This technology provides the opportunity to develop tools based on these methods to fully stage, test, and simulate traffic and applications similar to the way power systems are modeled today. This will greatly speed up testing and implementation times and will be able to record more accurate numbers and prevent surprises in the field.

6.1.5 Separation of Traffic by Type and Application

The OpenFlow match/action flow-table sequences have the ability to separate traffic types to a highly granular level. As an example, OpenFlow can simply match and forward protection traffic as quickly as possible while assigning a low-priority queue to all other packets not matching protection packet headers. OpenFlow also has the ability to physically separate out traffic by dedicating a group of redundant ports, a port group, specifically to whitelisted protection traffic and can be configured to simply drop all traffic not matching protection criteria on a particular physical link.

6.2 Maintainability

One of the promises of SDN is the decrease in day-to-day operational complexity. Because OpenFlow provides a network-wide snapshot of the system, it is easier to visualize and be alerted to any changes in the PCEN. Some modern OpenFlow controllers, such as Big Switch Floodlight [8], are attempting to integrate graphical user interfaces, with the goal of making operational changes to the network intuitive and interactive rather than a command-line task. Because network operators can update flow tables in real time, tasks that require temporarily re-architecting the network to add, remove, or upgrade hardware or firmware can be scheduled, potentially without packet loss. OpenFlow more easily supports test modes because test hardware on the network can be easily integrated by simply updating flow tables to forward test messages to specific manufacturer MAC addresses. Because network flow rules are kept in a centralized OpenFlow controller, replacing hardware is as simple as pushing out a set of rules to a new OpenFlow-enabled middlebox. Finally, the nonproprietary nature of OpenFlow holds the potential to drastically reduce operation and maintenance (O&M), documentation, and hardware costs for highly reliable PCENs through better ease of use and maintainability.

6.3 Cybersecurity

One of the most explicit SDN benefits is the ability for network operators to know exactly what communications flows should be on the network and what path they take, while giving the ability to deny all other traffic. The ability to manage communications by flow rather than packets improves end user ability to perform long-term network management. The OpenFlow protocol allows for hybrid whitelist/blacklist security models so that teleprotection communications can be detected and forwarded as quickly as possible while other traffic types can be forwarded to the controller for human alerting and approval input. Traffic matching known malware signatures can be immediately discarded. The OpenFlow traffic whitelist capability allows only specific data types to be forwarded to a host on a strict preset bandwidth. The whitelisting model provides the most protection-based security for the link because it can simply drop unexpected traffic flows that may otherwise cause link insecurity.

OpenFlow exceeds the traditional needs for an intrusion detection system (IDS) and IPS because it acts in either a reactive mode (allow wildcard communications, but send copies of flows to a centralized IDS) or a proactive mode (drop all unapproved flows). Because OpenFlow has visibility of OSI Layers 1 to 4, it can act as a traditional firewall with more granular per-header packet blocking capabilities.

7 CONCLUSION

OpenFlow has the potential to be vastly superior to present STA failure-handling methods because flow tables work with precalculated failover methods. SDN does not require enabling hot-standby links previously disabled by STA methods to prevent data flow loops. Also, SDN acts on link loss without disrupting large segments of a network. SDN networks can react much more quickly to disruptions than STA, which requires peer-to-peer RSTP communication with neighboring switches to determine active links.

OpenFlow can emulate the capabilities of traditional CoS tags and automatically prioritize protection traffic without requiring other priority indicators on the packets themselves, thereby reducing complexity for protection engineers. Traffic engineers can implement custom logic in an OpenFlow controller to reduce complex architectures and minimize latency, even under failover conditions. OpenFlow can be used to emulate entire environments purely in software, leading to the much quicker and easier calculation of host and network link bandwidth usage. The OpenFlow whitelisting capabilities can be used to minimize the amount of unexpected, nonprotection traffic between GOOSE hosts and prevent traffic floods that may otherwise render hosts inaccessible. While traditional rate-limiting and MAC address filtering may be used to achieve similar results, OpenFlow is more flexible and does not require manufacturer-specific protocols or features.

REFERENCES

[1] IEC 61850-5, Communication Networks and Systems for Power Utility Automation – Part 5: Communication Requirements for Functions and Device Models.

[2] IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines.

[3] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014. Available: https://www.selinc.com.

[4] R. Bobba, D. R. Borries, R. Hilburn, J. Sanders, M. Hadley, and R. Smith, “Software-Defined Networking Addresses Control System Requirements,” April 2014. Available: https://www.selinc.com.

[5] Linux Foundation, *OpenDaylight*. Available: http://www.opendaylight.org.

[6] *Open Networking Foundation*. Available: https://www.opennetworking.org.

[7] Mininet Team, *Mininet*. Available: http://mininet.org.

[8] Project Floodlight, “Floodlight.” Available: http://www.projectfloodlight.org/floodlight.

C.1.1-6. Implications and Benefits of Standardized Protection and Control Schemes

Alexander Apostolov, Thomas Schossig
OMICRON electronics,OMICRON electronics
USA, Austria

1 INTRODUCTION

The requirements for improvements in the efficiency and quality of protection schemes at the distribution level of the electric power systems highlights the need for development of new methods and tools that can help the industry achieve these goals. That is why it is very important to start a discussion on the opportunities that exist to develop a set of engineering tools based on the development and experience with the use of utility standards and the IEC 61850 substation configuration language.

The first part of the paper describes an object-oriented engineering process for the development and implementation of protection schemes based on five stages in a utility's standardization process:

- definition of distribution system protection philosophy
- definition of a distribution protection scheme type
- selection of approved protection and control IEDs
- design of the protection scheme
- instantiation of the protection scheme as part of a substation protection system

The second part of the paper describes the IEC 61850 Substation Configuration Language (SCL) and the different types of files that it defines - SSD, ICD, SCD and CID. The need for a new SCL file named ISD (IED Specification Description) is introduced. Their use at the different stages of the engineering process is then presented. This covers the different components of the model, such as:

- Substation topology
- Distribution feeders
- Communications infrastructure
- Protection, automation, control, energy management and other functions
- Multifunctional intelligent electronic devices
- Their associations with the primary equipment and the communication system

The paper then identifies some missing components that require extensions to the existing models or development of new models.

The paper later describes the engineering process based on this concept and the use of different standard files to achieve different engineering tasks.

A four stage standardization process defined by CIGRE Working Group B5.27 is described in the paper. The use of IEC 61850 SCL files as envisioned by the working group is described as well.

Standards based engineering offers some significant advantages that are described at the end of the paper. At the same time this approach may require some changes in the organizations and the methods and tools used for engineering. It will also need some initial investment, but the long term savings will result in significant savings in time and money, as well as improved quality of the schemes and the reliability and security of the distribution power system.

2 OBJECT-ORIENTED STANDARDS BASED ENGINEERING OF PROTECTION SYSTEMS

Intelligent (microprocessor-based) Electronic Devices (IED) for data acquisition, protection, measurements and control have gained widespread acceptance and are recognized as essential to the efficient operation and management of substations. Their integration in hierarchical substation protection and controls systems over a substation local area network allows significant improvement in the functionality of the system without any increase in the cost. This integration process in substations using IEC 61850 as the communications protocol is based on object models that require the use of appropriate tools to represent the complex architecture of the substation, the communication system and the multiple functions in the IEDs themselves. A major part of the engineering of a substation automation system is related to the architecture and configuration of the secondary equipment in the substation. This requires the development

of a formalized format that allows the description of all different elements and their relationships. IEC 61850 defines the object models of the different types of primary and secondary equipment, as well as their functionality in the substation.
The object-oriented approach to the engineering of the substation protection system is based on the system hierarchy and contains nested objects with different levels of complexity that can be defined as part of the standardization process.
At the top of the hierarchy is the substation protection automation and control system (SPACS) that contains multiple instances of bay protection, automation and control schemes (BPACS), each defined as a complex object – SPACSO or BPACSO (see Figure 1).
Each BPACS contains multifunctional IEDs, defined in the object-oriented design process as a protection, automation and control objects (PACO) with scheme specific functionality.

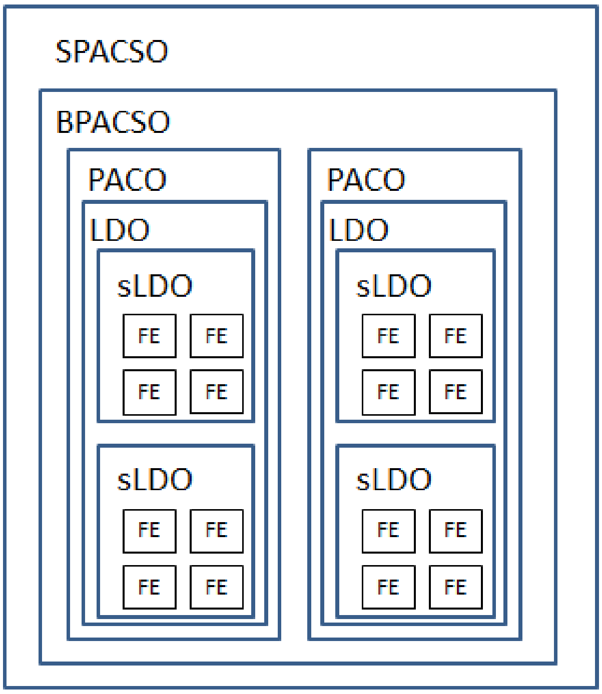


Fig. 1 Object model hierarchy

Each PACO contains multiple logical device objects (LDO) with specific functionality:

- Protection
- Automation
- Control
- Measurements
- Monitoring
- Recording
- Analysis
- Others

Each LDO can contain one to many sub-logical devices sLDO. The sLDO at the bottom of protection system/scheme hierarchy contains the Function Elements (FE), the smallest functional objects that are represented by Logical Nodes in the IEC 61850 model.
A substation protection and automation system also includes different tools for visualization and control of the primary and secondary substation equipment - the substation HMI. The user can navigate through the multiple views of the substation one-line or communications diagrams, or check the status or settings of a specific IED. The development of the HMI and the mapping of the multiple analog and binary signals from the IEDs is a very labor intensive process that also can be subject to errors at different stages of the engineering process.
The standardization process typically defines bay level objects, but more and more utilities are going in the direction of using standard substations, especially at the distribution level of the electric power system.
It is important to understand that standardization, like everything else, has benefits and drawbacks. The analysis of both clearly shows that the benefits are much more than the drawbacks, especially if we consider the long-term benefits against the short-term drawbacks. Even though it will impose an initial cost and resource burden, in the long run it will lead to significant cost savings and improvement in the quality of the secondary systems. The benefits of such an

approach can be further improved if the standardization applies not only to the protection schemes' engineering, but also to IED configurations, settings, logic, etc.
Although some non-monetary benefits might be achieved in the short term, the standardized designs should be applied for a period of time in order to realize the anticipated full benefits, but this period should not be so long that the technology becomes obsolete or too far out of date compared with the latest available.

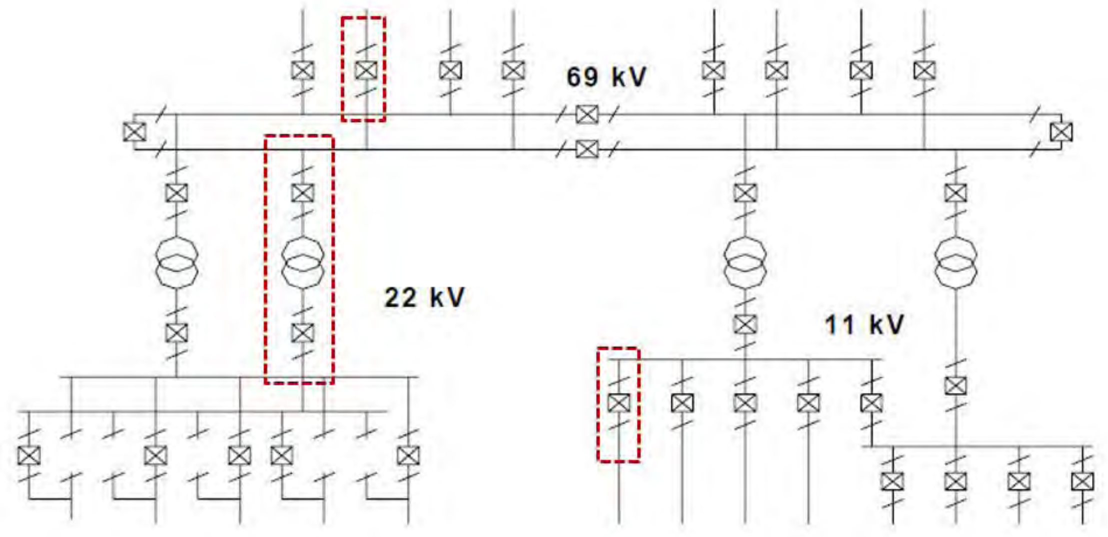


Fig. 2 Substation bay examples

The development of standard secondary schemes is based on:

- Utility standards
- Utility best practice
- National standards
- International standards:
    - IEC
    - IEEE
- Industry best practice:
    - CIGRE reports
    - IEEE Power System Relaying Committee reports

Detailed analysis of the standardization of protection and control schemes, definition of a standardization process, the benefits and challenges of this approach based on the experience and practices of many utilities from around the world is available in the CIGRE Technical brochure 584 "Implications and Benefits of Standardized Protection and Control Schemes" prepared by working group B5.27.
The contributions of this work, combined with the best practices from the established standardization process within a utility provide the foundation for the standardization strategy described in this paper.

2.1 Standard bays

The efficiency of the standardization process can be significantly improved if the design of the substations is based on standard bays.
Standard bay design includes the following elements:

- Bay scheme
- Bay layout
- Bay primary equipment
- Instrument transformers location
- Instrument transformers

The following distribution bay types are commonly used in a utility's distribution system and included in the standardization process:

- HV breaker-and-a-half
- HV single breaker
- MV single breaker
- HV transformer
- MV transformer

The functional and performance requirements in standard secondary systems are defined by the philosophy and criticality of the application.
The overall standard scheme design will be based on the combination of the bay type and voltage level or criticality factor.

2.2 Standard substations

The highest level of efficiency of the standardization process can be achieved using standard substations. It is possible to design standard distribution substations and it is already a common practice in some utilities.
Such strategy will offer significant benefits, since it will support the design of standard container style control houses that can be produced, configured and commissioned in a factory environment.
This will result in a significant reduction of the amount of work that needs to be done at the site, especially if standardized interface between the substation process and the control house is designed and implemented.

3 STANDARDIZATION PROCESS

A standard secondary scheme is defined as a single set of multifunctional IEDs integrated using process and inter-device interfaces in order to provide all required by the application functions, such as protection, control, status monitoring, measurements (including synchrophasors when required), communication, condition monitoring, recording, event reporting, fault locator and power quality.
For each standard scheme a four step standardization process is followed.

3.1 Standard scheme template

This is Step 1 of the standardization process and covers the definition of the functional requirement specification for a standard secondary scheme based on a utility's philosophy and practice.
It is a conceptual description of the scheme. This is typically the formalized description of the application of protection and control philosophy to a specific type of bay as described above. The templates should include all of the necessary components of the documentation of each subsequent stage.
At this stage the functional requirements and integration constraints need to be defined. These are detailed requirements associated with the bay topology, voltage level and criticality, communications requirements, etc., resulting in some interfaces and functions being defined.
This stage should also include primary single-line diagram, secondary functional diagrams, trip matrix, setting and testing philosophies.
Items that are left "generic" at this stage are types of primary equipment or IEDs. They may be considered, but are not specified at this stage.
In addition, the description of the functional specification in the form of an IEC 61850 Substation Specification Description (SSD) file is recommended, thus allowing the automation of the procurement process based on exchange of such files between a utility and its suppliers.
Step 1 of the standardization process is performed by a utility's secondary core group of experts responsible for the engineering of standard schemes at the company level.

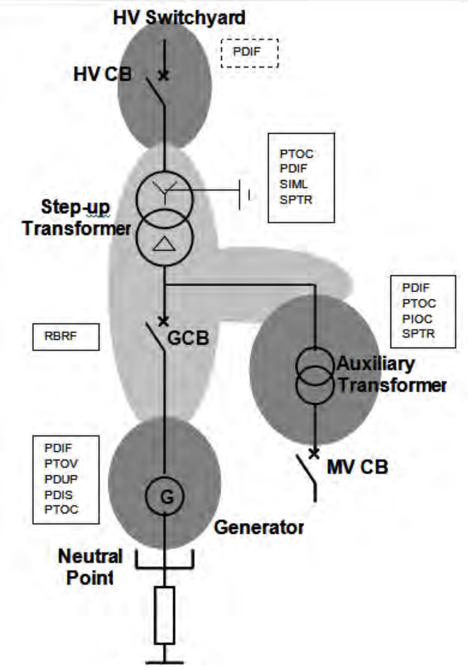


Fig. 3 Standard scheme "Template"

3.2 Defined standard scheme

This is Step 2 of the standardization process and represents a development stage of a standard scheme that defines the primary plant and the hardware interfaces with the specific type of bay covered by the scheme. The CB, disconnectors, earth switches, CT/VT and auxiliary interface specifications, signals list/diagram (hardwired or communications based) are specified at this stage.

The defined standard scheme can be used for the same or similar types of new or existing installations without ANY changes in external wiring, signaling and equipment.

Allocation of functions to generic (abstract) IEDs is also defined at this stage. The required functionality of individual IEDs can be described also using the newly defined IED Specification Description (ISD) file, thus allowing the automation of the procurement process based on exchange of such files between the utility and its suppliers. This will support automatic selection of the IEDs that meet the requirement specification for a specific standard scheme by comparing the ISD file with the existing IED Capability Description (ICD) files.

The definition of the required interfaces (including quality) with the process at this stage also allows the definition of the scheme terminal blocks that are signal specific, but not product specific.

Step 2 of the standardization process is performed by the utility's experts responsible for the engineering of standard schemes at the company level.

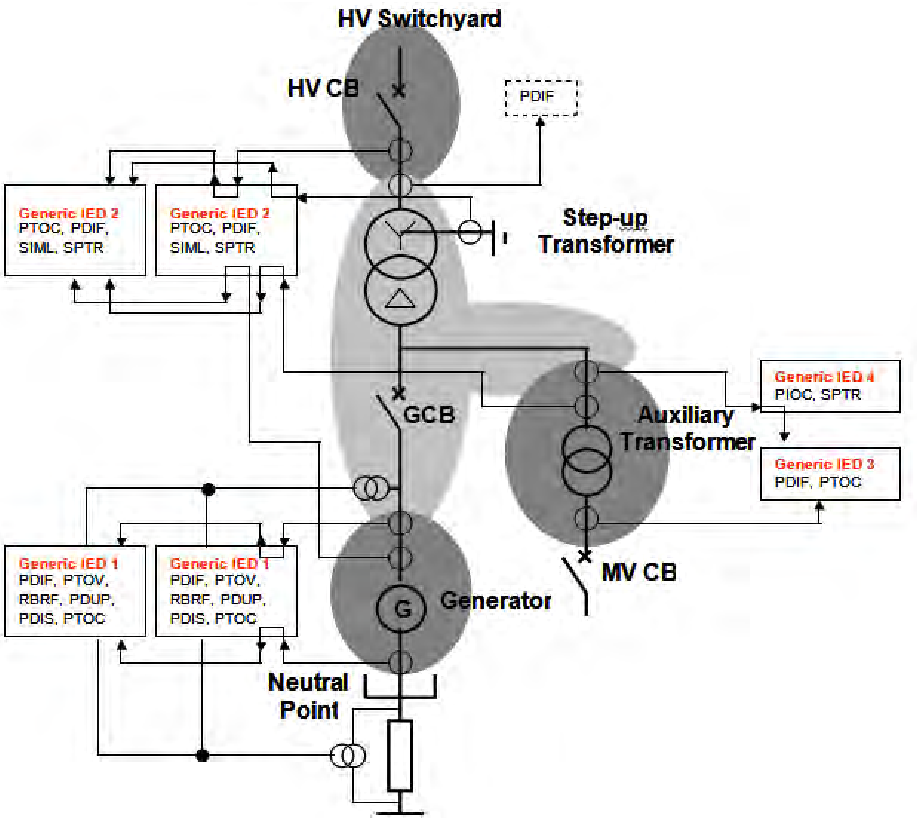


Fig. 4 Standard scheme "Defined"

3.3 Applied standard scheme

Step 3 of the standardization process is what is typically considered by the utility as a "standard secondary scheme".

This includes the use of approved specific IEDs or other secondary equipment. The IED selection should ensure that all functions and functional elements defined for the scheme template in stage 2 are available in the selected IEDs.

The IED HW, SW and parameter-set versions, IED configuration tools, signal list (hardwired or communications based), wiring diagrams, cable lists and standard settings are specified at this stage

The global settings, including programmable scheme logic, of the IEDs are introduced at this level of standardization. However, at this stage there are still no local settings or other site specific configuration parameters.

In case that the utility wants to use a different supplier for the same scheme, it will result in a different scheme template implementation that meets the requirements of the above definitions.

Since at this stage all IEDs and their interfaces are defined, the functionality of the standard scheme is configured using IEC 61850 engineering tools based on the ICD files of the individual IEDs and documented as a Substation

Configuration Description (SCD) file. From this file the individual IED Configuration tools extract the Configured IED Description (CID) files used to configure them for operation in the substation.
Step 3 of the standardization process is performed by the scheme supplier based on the documentation produced in step 2. The development of the standard scheme should also involve at least two members of the utility's group of experts responsible for the engineering of standard schemes at the company level.
The standard scheme should be subject to type testing before it is approved for use by authorized utility representatives.

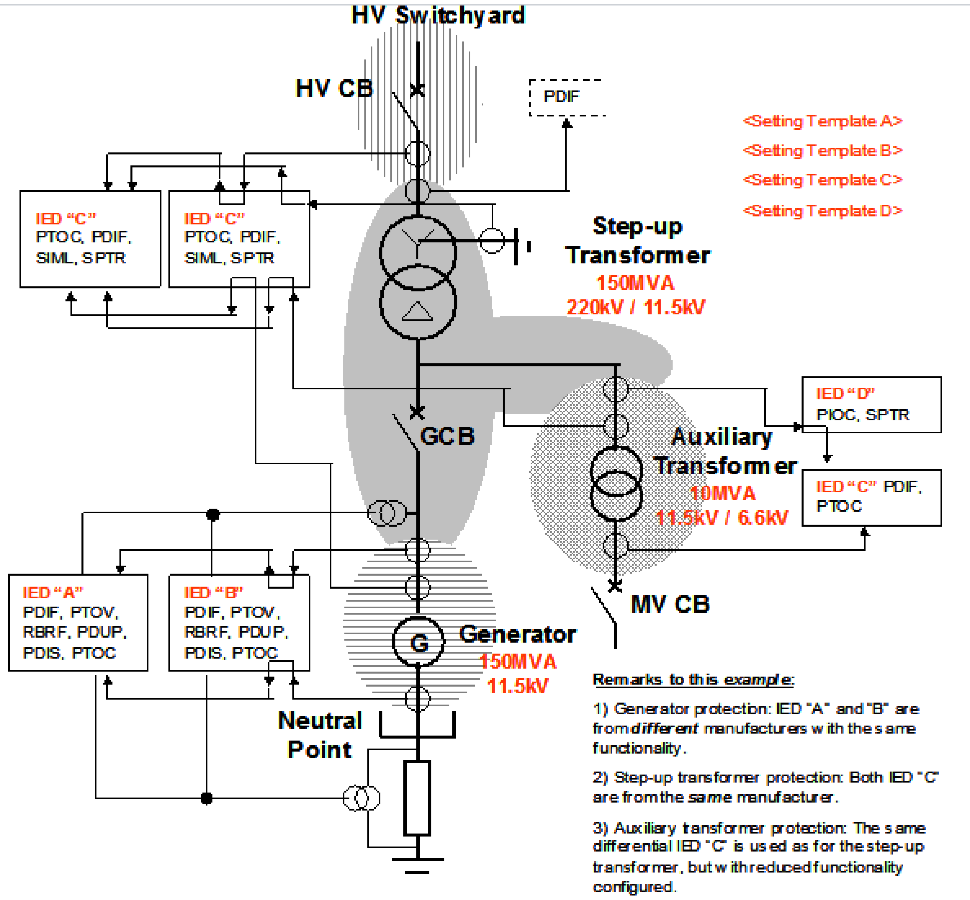


Fig. 5 Standard scheme "Applied"

3.4 Instantiated standard scheme

This is a site specific implementation of the standard scheme (i.e. an instantiated standard scheme from stage 3). Site and application specific settings are implemented at this stage, and all hardware is defined.
While instantiation excludes any modifications besides site specific setting-parameters and site specific naming, specialization on stage 4 offers the opportunity to adapt the standard scheme typically to variations in primary HW-components when used in existing sites.
At this stage the IED specific calculations and setting files as well as specific commissioning, maintenance and testing procedures are applied.
In special cases also other modifications can be considered. This may appear as a deviation from the standardization process, however it takes advantage of the developed standard scheme for a special application that may not justify going back to stage 3 of the process.
Step 4 is performed by the secondary scheme supplier based on setting files and procedures supplied by the utility. Test reports and other documentation produced during the production, configuration and commissioning of the scheme should be reviewed and approved by authorized utility representatives before the scheme is delivered to the site.

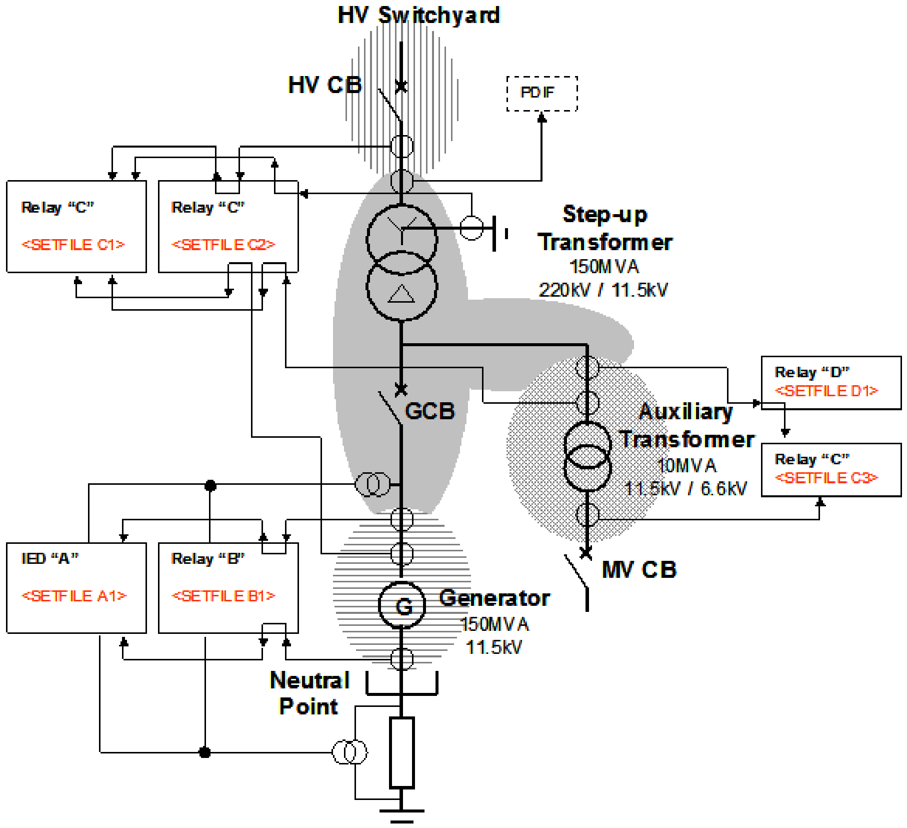


Fig. 6 Standard scheme "Instantiated"

4 IEC 61850 STANDARD FILES

The development of IEC 61850 had as one of its goals the definition of a file format that describes the components of the substation and the protection and automation system in a way that allows most of the engineering tasks to be performed automatically.

In order to allow the modeling and exchange of data between different engineering tools required at different stages of the substation engineering process, that file format has to meet the requirement for interoperability. At the same time the overall engineering process should be designed taking into consideration the fact that during the early stages of implementation of IEC 61850 it may be necessary to use also some proprietary data formats.

Part 6 of the IEC 61850 standard defined the Substation Configuration Language (SCL) and its use to describe the substation configuration, IED's and communication systems in a way that corresponds to the object models defined in different other parts of the standard. SCL is based on UML and XML.

It is used to describe the substation connectivity, IED configurations and communication systems according to parts 5 and 7 of the standard. Description of the relations between the substation automation system and the substation (switchyard) itself is included as well .

SCL was developed to support easier engineering of substation automation systems and application functions. It allows the description of a substation or an IED's configuration to be passed to a communication and application system engineering tool.

Its main purpose is to allow the interoperable exchange of communication system configuration data between an IED configuration tool and a system configuration tool from different manufacturers.

The SCL supports the development of engineering tools that are capable of describing:

- The substation one line diagram representing the different voltage levels, busses, transformers, bays and switching devices. The functional requirements should also be included in terms of allocation of logical nodes to the primary substation equipment.
- The IEDs to be used to perform the required functions based on a fixed number of logical nodes (LNs)
- The communication interface of the different IEDs – specifically their connection to the substation local area network
- The Client-Server and Peer-to-Peer communications for the specific substation automation system implementation

The standard does not define any specific software tools that support the intended engineering process. This is a task that the IED manufacturers, substation automation system vendors or third party providers have to develop based on the requirements of the market using the different types of files defined in the standard.

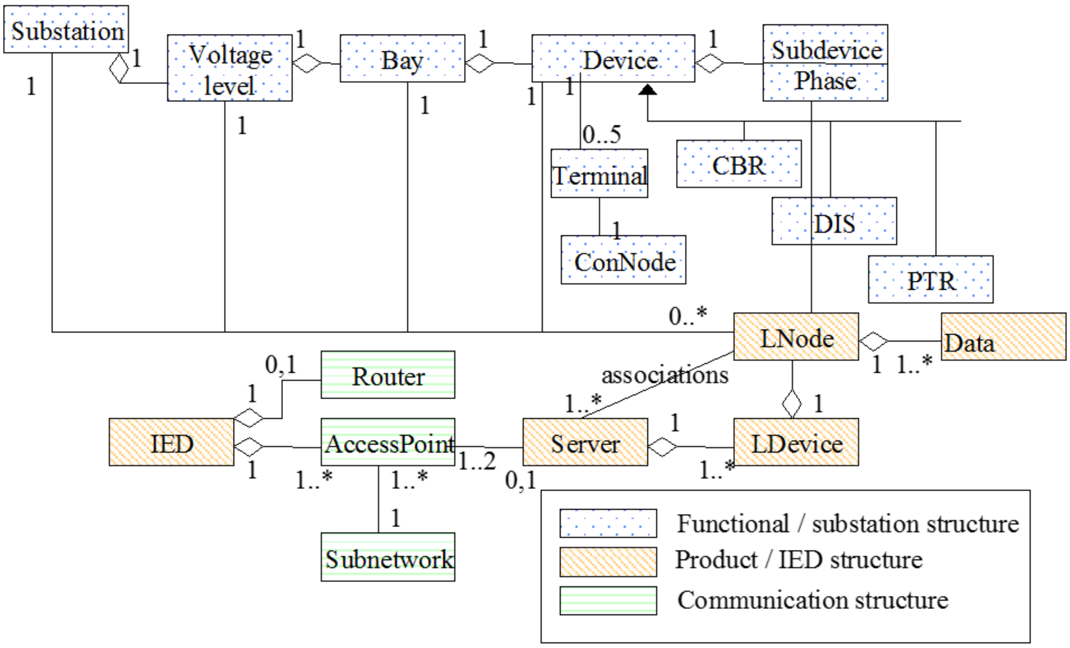


Fig. 7 IEC 61850, Part 6 - System Configuration Language (SCL) - UML

5 SCL FILES

IEC 61850 defines several types of files required to support the intended engineering process. In order for an IED or a system solution by a manufacturer to be compliant with the standard, they have to support the use of the files described below directly from the IEDs or through tools delivered with the system.

5.1 System Specification Description

The description of the system is the first step in the engineering process and until now has not been based on any standardized approach. The IEC 61850 engineering process envisions the use of substation specification tools that allow the user to describe the substation design and associated functional requirements for the substation protection and automation systems.

The data exchange from such a system specification tool and other tools utilized in the process should be based on the System Specification Description files defined in the standard. They have an SSD extension.

The SSD file describes the single line diagram of the substation and the functional requirements represented by logical nodes. The logical nodes can be abstract in the sense that they are not allocated to specific IEDs.

5.2 IED Specification Description

Allocation of functions to generic (abstract) IEDs is part of the engineering process. The required functionality of individual IEDs can be described also using the newly defined IED Specification Description (ISD) file format, thus allowing the automation of the procurement process based on exchange of such files between the utility and its suppliers. This will support automatic selection of the IEDs that meet the requirement specification for a specific standard scheme by comparing the ISD file with the existing IED Capability Description (ICD) files. This file will be included in the next edition of the standard.

5.3 IED Capability Description

The default functionality of an IED in the substation configuration language is represented by the IED Capability Description (ICD) file. It is used for data exchange from the IED configuration tool to the system configuration tool.

This ICD file describes the capabilities of an IED. It contains exactly one IED section for the IED whose capabilities are described. Since it represents the default functionality (i.e. before it has been configured), the IED name in this file is **TEMPLATE**. The file also includes the different logical node types as they are instantiated in the device. The file extension shall be .ICD for IED Capability Description.

5.4 Substation Configuration Description

The configuration of the system is represented by the substation Configuration Description (SCD) file. It contains substation description section, communication configuration section and all IEDs.
The IEDs in the SCD file are as they are configured to operate within the substation protection and automation system. These files are then used to configure the individual IEDs in the system.

5.5 Configured IED Description

The Configured IED Description file includes the substation specific names and addresses instead of the default ones in the ICD. It represents a single IED section of the SCD file described above.

5.6 SCL Files use in the standardization process

The different IEC 61850 System Configuration Language (SCL) files described above can be used to improve the efficiency of the engineering process at all stages of the engineering process.
The table below illustrates which files are used at which stage of the development and implementation of the standard schemes.

	Phase	Bay	PAC Devices	Plant Application / Substation	What it means
A	Standard scheme – template	G	G	G	Totally generic **SSD, ISD**
B	Standard scheme – defined	S	G	G	All HW interfaces fixed **SSD**
C	Standard scheme – applied	S	S	G	IEDs fixed **ICD**, **IID**
D 1 2	Standard scheme: Instantiated Instantiated with small variations	S	S	S	Everything fixed, also settings (= standard scheme applied in reality) **SCD**, **CID**

S = specific; G = generic; B and C can be one step.

6 CONCLUSIONS

A significant part of the engineering of a distribution substation automation system is related to the architecture and configuration of the primary and secondary equipment in the substation. This requires the development of a formalized format that allows the description of all different elements and their relationships.
An object-oriented standardization process based on standard bay types can help improve the efficiency and quality of the protection and control systems.
A four step standardization process takes advantage of the IEC 61850 Substation Configuration Language that allows standard representation of the system design and interoperability between different engineering tools.
IEC 61850 provides an excellent opportunity for the formalization of standards based object-oriented approach to the design of substation protection schemes or systems.
The use of the standardization approach described in the paper requires an initial investment in developing and properly type-testing the standard schemes for each type of bay. But this investment will be quickly paid off by the use of the standard schemes in multiple installations. It will support the development and use of standard testing template that can be executed automatically by advanced testing tools.
Such standard schemes will result in much faster commissioning of schemes with much better quality, thus significantly improving the efficiency of the engineering process.

Protection of Transmission Lines with Series Compensation
New Tools

Francisco A. REIS Filho(1), Eduardo C. SENGER(2), Rodrigo A. BENES. F(3), Giovanni MANASSERO. Jr(2)
Farfilho Consulting Trading and Representations LTDA(1)
USP – University os São Paulo-POLI/PEA(2)
SIEMENS(3)
Brazil
farfilho@farfilho.com.br

KEYWORDS

Transmission Lines, Series Compensation, Wavelets, Travelling Waves, Artificial Neural Networks

1 INTRODUCTION

Properly protecting a transmission line of extra high voltage equipped with series compensation it is still a major challenge for the system protection engineers. The applied conditions resulting from this configuration still present operating conditions not properly resolved that entail great difficulties in determining your settings, and with the risk of an almost certain improper actuation eminent for the reasons to be exposed during the presentation of this work. Another aspect to be considered is that, in many of these applications, the manufacturers of relays available in the market today present the characteristic impedance type MHO or quadrilateral for measurement of these impedances, which implies in some cases to increase the performance of the respective protection zones (mostly the zone 1), compromising their respective times of network stability or reducing significantly your range precisely because of the presence of these capacitors looking to avoid undue performances for faults in parallel circuits and or at the beginning of the circuit.

The present work had, as a main motivation, the results obtained during the tests performed by the company *Farfilho Consulting Trading and Representations LTDA*, hired by IENE, for the coordination and execution of the tests for protection of your 500 kV lines along the RTDS (Real Time Digital Simulator) of FURNAS in 2011. These tests were designed to validate dynamically the adjustments of the protection circuit that interconnects the electric substations Colinas - São João do Piauí as shown in the diagram of the *Figure 1*.

These tests were performed in more than 600 simulations covering all types of fault scenarios in relation to the specific protection to the spark-gaps of banks and whether these systems work or not. The most important conclusion of these tests is that they reduce the range of Zone 1 (around 50%) of the line terminals, due to the overreach of same for external faults in parallel line due to the presence of sub synchronous component *(Tables 1 and 2)*, which made the system protection of these lines virtually dependent only on the adjustments of the zone 2, associated with the system of teleprotection scheme POTT (Permissive Overreaching Transfer-Trip).

In possession of the arguments cited, this work will propose steps to minimizing these operating conditions developed for operation in parallel with the Fourier algorithm common to all manufacturers of digital signal processing techniques, such as the Wavelet Transform [4.3, 4.5], concepts of pattern recognition through analysis of the clusters, and finally of the neural networks to detect the presence or absence of a series capacitor in the fault loop. These conditions detected should occur in a time less than or equal to 1 cycle, and once detected the series capacitor in this loop will be used as the principle of traveling waves (ΔI, ΔV) [4.4] to be able to see the fault with the correct directionality and with the maximum possible range of the protected line. These procedures will increase the reliability and make redundant the currently operating protections in the system with zone 2 added to the relay protection system POTT (Permissive Overreaching Transfer-Trip) [4.1]. Then, these algorithms will be tested on 500 kV circuit presented in *Figure 15*.

2 - Objective

2.1 Theoretical Concepts

The two most important operating conditions as a result of this application on the agenda are as follows:

- Current reversal: this condition, presented in *Figure 2*, occurs when *Equation [1]* is true
- Voltage reversal: this condition, presented in *Figure 3*, occurs when *Equation [2]* is true

In some ways, the conditions presented above can be avoided belong the project and the definition of the level of compensation to be effected in the line, together with the equivalent network and other system informations. The component sub synchronous already present in the current waveforms depends on whether the series capacitor is inserted, or not, in the fault loop. Here is made a brief analysis of a single-phase R-L-C circuit for the two main conditions where the solution of differential equations of R-L (Inductive Loop) and R-L-C circuit (Inductive and Capacitive Loop) have the following main characteristics:

- RL Circuit: DC Component and fundamental frequency of 60 Hz
- RLC Circuit: DC Component, fundamental frequency of 60 Hz and natural frequencies damped oscillatory frequencies

These natural frequencies ω_d are obtained from the roots of the complex differential equation and display the values given by *Equation [3]*.

In the *Figures 4 and 5* are presented both typical waveforms through the modeling of a single-phase circuit in ATP software.

These concepts can be extended to transmission systems, where the lines with distributed parameters modeled by compensation factor that adds to the aspects cited the high-frequency components present in current waveforms, due to reflections of waves that travel to the condition of faults on the line with the presence or absence of these banks. Another important aspect to be seen is the operating excursion impedance vector for the condition of the inductive - capacitive loop. From the modelling performed in MATLAB with typical Fourier algorithms for extraction of the modules and phase of the voltage and current vectors, where we can observe the excursion of the vector impedance for a typical three-phase fault. Unlike the inductive loop featuring a characteristic more well behaved in R-X, that have an oscillatory behavior due to the presence of ω_d frequency, showing a form similar to a logarithmic spiral. This characteristic is responsible for possible underreach or overreach in these protection relays, as shown in *Figure 6*.

2.1.1 Development of Algorithms

2.1.1.1 Algorithm Classification

To clarify, the main problem so far for this type of application is the presence of series capacitors in the fault loop. The intention here is to propose a digital algorithm, operating in parallel with the conventional impedance measurement that detects the presence or not of a capacitor on this loop. Once detected, the same protection system uses the discrimination of directionality concepts of ΔV and ΔI by wave travelling [4.1,4.4], blocking the action of Zone 1 for these conditions. By the concepts already presented this shows that the problem is typically classification, i.e., identify if the fault loop is inductive or capacitive-inductive. The primary tool to be used in the classification will be the Wavelet Transform which is well known in the academic world and widely used [4.3,4.5], where the main objective is to detect the high frequencies to be captured in the current signals. In summary, this transformed form multiplies the input discrete signal by a series of functions well behaved at the time called Wavelet Mother. These do nothing more than answer the urge to filters high - pass and low - pass. Then, after this multiplication, moved this signal by 2, and so on, increasing the resolution in frequency at the expense of reply in time.

These multiplications results in levels with their Wavelet coefficients (Details (D) and approach (A)) indicating the presence of this frequency in the range under analysis. The main difference of this tool, compared to the Fourier transform, is the fact of owning an Escalation Parameter (a) shown in *Equation [4]*, which enables a logarithmic scale for the analysis of the sign in question. This is unlike the Fourier Transform that defines the size of the watch window and displays the same resolution for the entire frequency spectrum of the signal.

In *Figure 7* is presented the block diagram of the algorithm MRA (Multi Resolution Analysis) used for Wavelets analysis.

For the first tests using the above tool modelled on the ATP circuit R-L-C with concentrated parameters using the values obtained from the circuit of *Figure 1* and shown some of the values used in *Table 3* below. In *Table 4* then the Wavelet decompositions are presented and the amount of samples contained in windows, 1/2, 3/4 and 1 cycle of 60 Hz was used for the development of the algorithm in a sampling frequency of 512 samples/cycle or 30720 Hz, which provides measurements of the frequency bands listed in its decomposition levels as shown in the diagram of *Figure 7*.

From here on this kind of algorithm is modeled on ATP a 500 kV double circuit, generating 70 cases in total, being 30 cases to the inductive loop and 40 cases for the inductive-capacitive loop, varying the angles of fault incidence (0 and 90 degrees), the level of compensation of the lines (50 and 70%) and the source impedances, reproducing within the possible operating conditions found in tests performed in FURNAS[4.6].

2.1.2.2 The Neural Network and the Clustering Analysis

The window size and the wavelet level used to detect the presence of a series capacitor was chosen through a bi-dimensional cluster analysis of wavelet coefficient presented in *Figure 10* and to neural network training and testing the data were separated into two sets, where the first strategy was to pick up differences in the high frequencies of the signal due to the presence or not of the capacitor through the wavelet detail levels.

It can be seen by the results obtained that the data is not overlapping; however there is a linear separation, not getting a proper classification. The second strategy is to get the fastest current decay due to the presence of sub-synchronous frequency in the inductive-capacitive signal. To this end, it was used the 8 level approximation component of wavelet transform with the goal of obtaining a filtered signal eliminating the highest frequencies that could interfere with the measurement in this decay. To measure the speed of the decay it was used an approximation of the derivative through the differences between consecutive samples. In the *Figure 11* is shown the cluster analysis based on derived vector module 8 level of Wavelet approximation using Daubechies Wavelet Mother 10 and using a data window of 3/4 of a cycle.

Therefore, in general, the algorithm developed has the following steps:

→ To start the algorithm it was elaborated a criterion of overcurrent that could ensure that the data window was effectively within the fault. With the separation of this window it is calculated the coefficients of the discrete wavelet transform.

→ For the RNA training it was generated two data sets and a network test by varying the angle of incidence of the fault, the level of compensation and the fault of impedance, totaling 36 cases. The circuit used to generate this data was the circuit of *Figure 16* to enable greater ease of variation of the parameters but consistently in order to extract the characteristics of the phenomenon in question.

→ Before submitting the data to the Neural Network, these data above was normalized for better performance of the RNA training algorithm, where the form of normalization chosen was the Division of the data by the absolute maximum value in the table, using the supervised training algorithm of Resilient back propagation type which is based on the original back propagation algorithm. The above only uses the signal to determine the gradient direction to update the weights, resulting in a greater speed in overcoming the local minima of the learning curve where the gradient module approaches zero.

For this condition the RNA showed better performance when had the setting 3-30-1, and the chosen functions for activation of the hidden layer neurons and output layer were hyperbolic tangent and logistic sigmoid function respectively. As a result, the training had an error equal to 10-3 hit in 18 seasons. In the *Figures 12 and 13* are presented the basic structure of the network used and the error curve obtained for the simulated cases.

2.1.2.3 The Directionality Algorithm

Once the presence of series capacitor has been defined in the fault loop, is possible now, block the unit of Impedance on distance protection Zone 1 and use the concepts of Travelling Waves already quite well known, and used on a large scale by some suppliers. In summary, this concept based on superposition theorem uses current and voltage variations that occur in a fault window to generate the signals of ΔI and ΔV due to these variations *(Figure 15)*. These components containing all frequencies contained the signs unless the fundamental component of 60 Hz is literally the first effective incidence of waveforms, regardless of the presence or not of the capacitors in the circuit, as well as the performance of their respective protections. [4.1, 4.4].

This directionality is intrinsic to the phenomenon shown in *Figure 18* where we have polarities with different signs for faults in one direction (forward), and equal polarities in the opposite direction (backward). Another important detail that must be emphasized is their speed in detecting this directionality, i.e. around 4 ms or 1/4 of cycle.

2.1.3 Modeling and Testing

For the modeling and testing of the proposed algorithm, it was made up the 500 kV circuit in MATLAB/Simulink software as shown on diagram of *Figure 19*. The measurement terminal was placed in each terminal and these measurements should be considered important with regards the above. The capacitor Series have two Bank's own intrinsic protections that are quick acting (performance ≤ 1ms) and slow acting (≤ 25ms). For the project, will be consider that having internal faults on the line and when there is action of the quick protections it will be considered as an inductive loop, and for slow protections, as inductive-capacitive loop.

Therefore, in this circuit 10 cases with incidence angle of 0° and 90° on the distances of 25,50 and 75% of the terminal for internal two Phase faults. Then they were generated 04 cases in parallel line to 50 and 75% with the same types of faults. By the characteristics adjusted for the intrinsic protections of banks had for these conditions 03 cases of fast acting protection (RL circuit) and 07 cases of slow protection performance (RLC circuit). The cases of fast acting protections were mainly the DC component of the fault current to shift the same in the time axis. In the *Figure 19* are presented the performances of currents and voltages of the MOV bank as well as the typical voltages and current forms obtained in these simulations as a typical curve MHO to one of simulated cases.

2.2 - Equations

[1] $|Xc| > |XF + XL|$

[2] $|Xc| < |XF + XL|$ and $|Xc| > |XL|$

[3] $$\omega_d = \sqrt{\frac{1}{LC} - \left(\frac{R}{2L}\right)^2}$$

[4] $$\left(W_\psi x\right)(m,n) = \frac{1}{\sqrt{a0^m}} \int_{-\infty}^{+\infty} x(t).\psi\left(\frac{t - n.a0^m \cdot b0}{a0^m}\right).dt$$

Where:

a → Parameter scale

b → Translational Parameter with m and n and Z, a0 > 1 and b0 # 0

2.3 - Figures and Tables

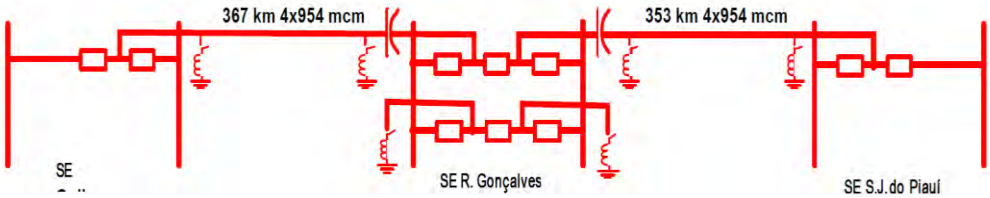


Figure 1: 500 kV System – IENE – SE's Colinas – Ribeiro Gonçalves – São João do Piauí
Note: All reactors are banks of 3x60 Mvar
Capacitive compensation series of 48% in LT COL-RGO and 49% in LT RGO-SJP

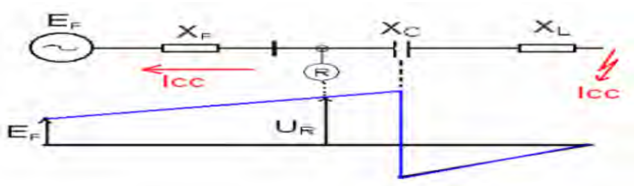


Figure 2: Current Reversal

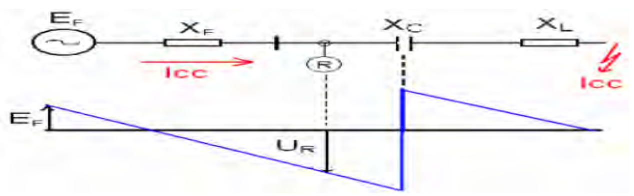


Figure 3: Voltage Reversal

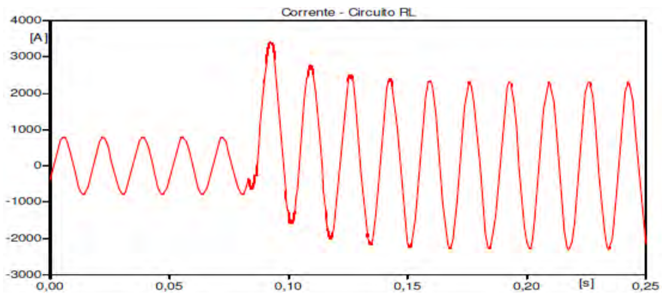


Figure 4: Typical Current Waveform - RL Circuit

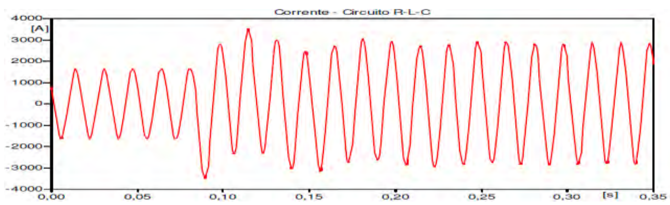


Figure 5: Typical Current Waveform - RLC Circuit

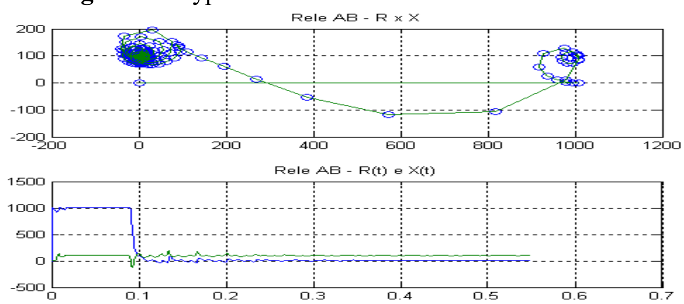


Figure 6: Excursion of Impedance Vector - Inductive/Capacitive Loop

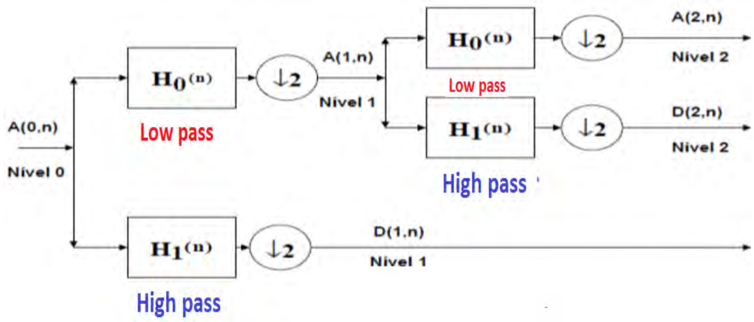


Figure 7: MRA Algorithm - Multi Resolution Analysis

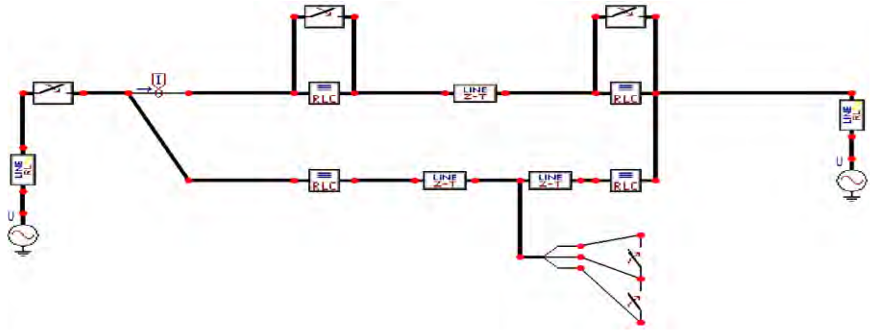


Figure 8: Circuit Modelled in ATP platform

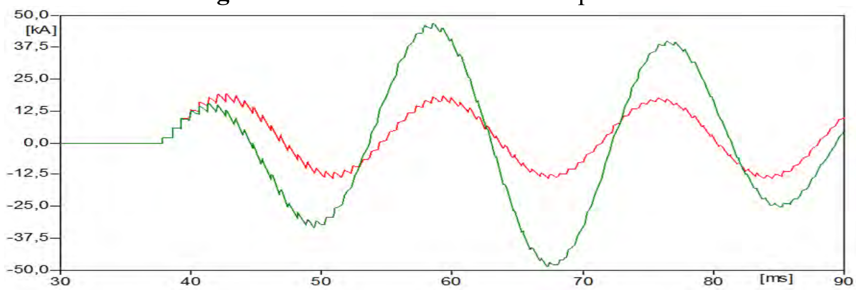


Figure 9: Typical waveforms for fault Loops
Red → Inductive Loop
Green → Induction/Capacitive Loop

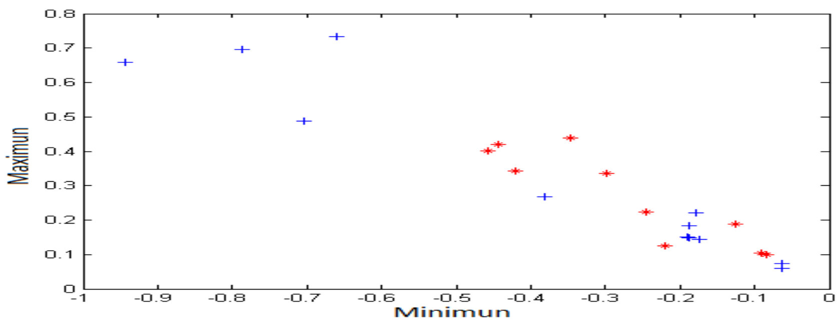


Figure 10: Cluster analysis - Level 5 (Wavelet Detail)

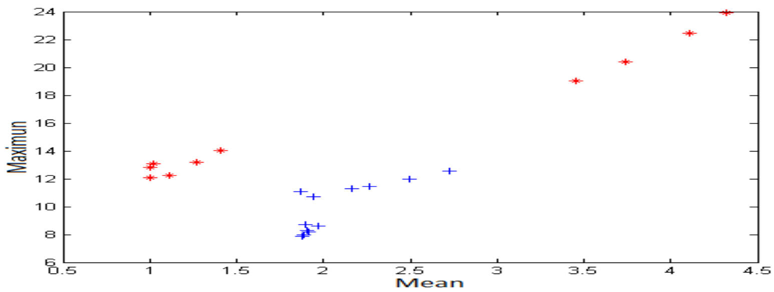


Figure 11: Cluster analysis - derived from Wavelet approximation of level 8

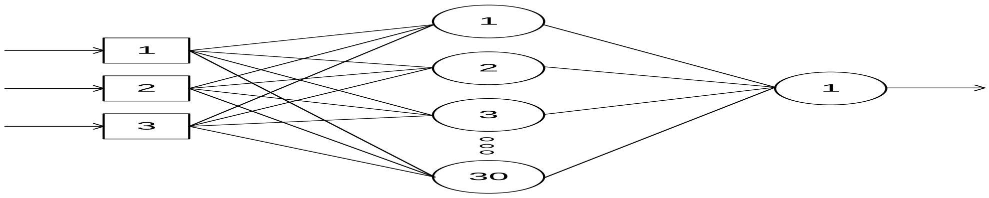


Figure 12: Artificial Neural network

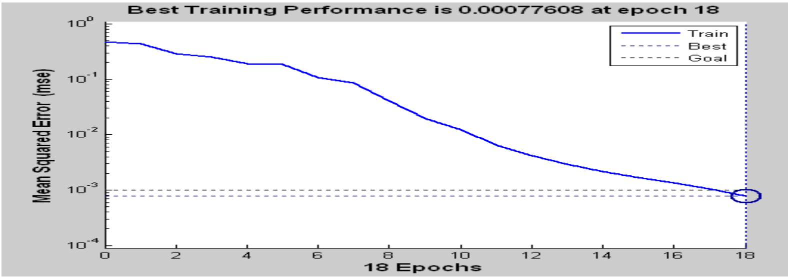


Figure 13: Error Graphic

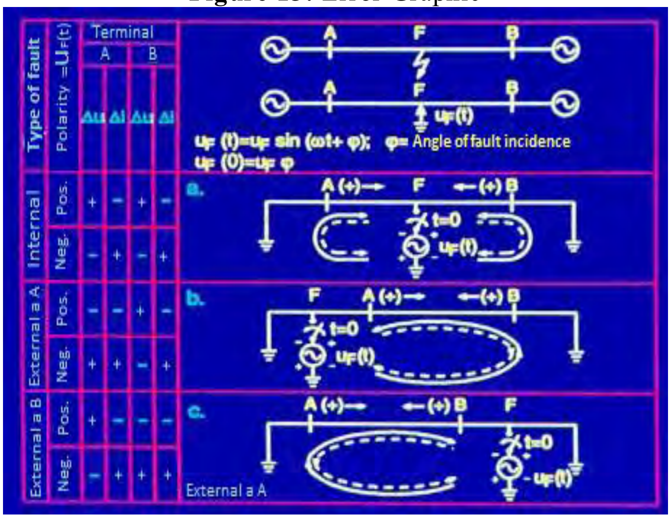


Figure 14: Polarity and ΔI and ΔV polarization

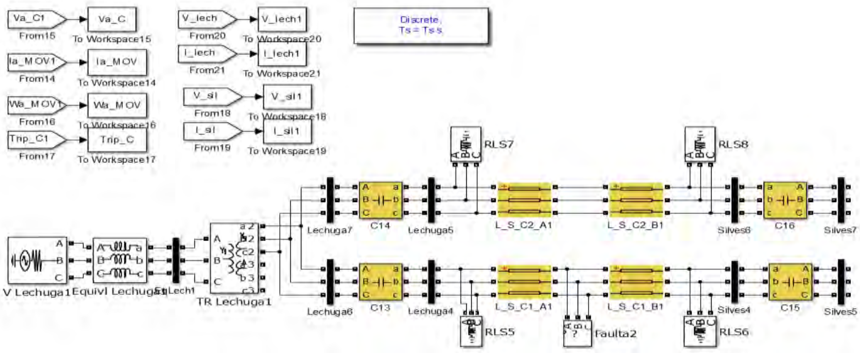


Figure 15: 500 kV diagram for final tests - MATLAB/Simulink Platform

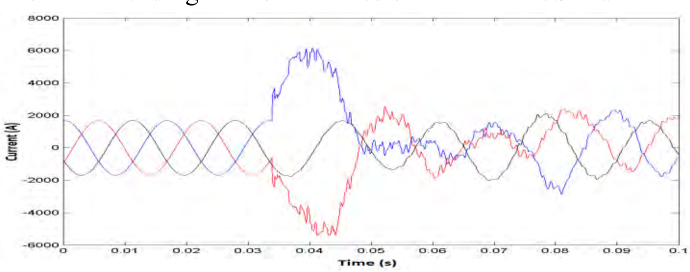


Figure 16: Current Waveforms

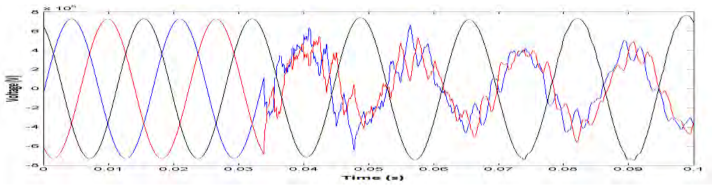


Figure 17: Voltage Waveforms

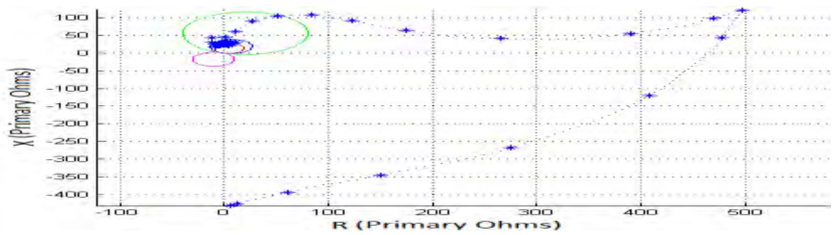


Figure 18: Impedance Diagram

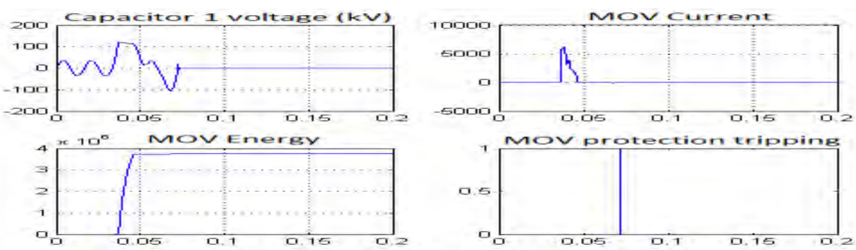


Figure 19: Curves of voltages, currentes and MOV in the capacitor

	Initial Value		Final Value	
	Z1P	Z1N	Z1P	Z1N
Ribeiro Gonçalves	30.67 Ω	26.22 Ω	15.94 Ω	13.11 Ω
São João do Piauí	2.49 Ω	2.22 Ω	2.24 Ω	1.99 Ω

Table 1: Changing settings of the 500 kV line - Ribeiro Gonçalves - São João do Piauí

Settings	Initial Value		Final Value	
	Z1P	Z1N	Z1P	Z1N
Ribeiro Gonçalves	28 Ω	25.78 Ω	14.56 Ω	12.89 Ω
Colinas	13.40 Ω	12 Ω	11.39 Ω	9.96 Ω

Table 2: Changing settings of the 500 kV line - Ribeiro Gonçalves – Colinas

Source (V)	CS (Hz)	Resistance (Ω)	Indutance (Ω)	Capacitance (Ω)	Indutance (mH)	Capacitance (μF)
408248.29	3 Hz	7.106	100.6	0.2515	266.843	10546.79
408248.29	10 Hz	7.106	100.6	2.79	266.843	9507.23

408248.29	58 Hz	7.106	100.6	94	266.843	28.21
408248.29	60 Hz	7.106	100.6	100.6	266.843	26.36

Table 3: Parameters of the R-L-C Circuit for Wavelet analysis

Frequency (Hz)	Level	Window of ½ cycle	Window of ¾ cycle	Window of 1 cycle
15360 - 7680	1	128	170	256
7680 - 3840	2	64	85	128
3840 - 1920	3	32	42	64
1920 - 960	4	16	21	32
960 - 480	5	08	10	16
480 - 240	6	04	05	08
240 - 120	7	02	03	04
120 - 60	8	01	01	02
60 - 30	9	-	-	01

Table 4: Wavelet Frequencies Decomposition(Samples)

3 - CONCLUSION

The results obtained are encouraging with respect to the search for an alternative application for the protection of lines with series compensation. Digital signal processing and pattern recognition new techniques are presented as a good way for solving system protection problems that are still not properly solved.

However, there is still a requirement for greater robustness in its algorithms so that they can become effective in the near future. In case of this developed application, the above should be tested to a larger and more comprehensive number of cases, as well as being analyzed to try to detect the presence of the sub synchronous component with the shortest possible window size.

4 - REFERENCES

[4.1] Reis Filho,F.A : Kotlarewsky, J : Xavier,C ; "Experience in Protection of Lines with Series Compensation" - XI SNPTEE(Portuguese)/1991.(***www.farfilho.com.br***, Folder- Published Works – item 1.3)

[4.2] Reis Filho,F.A : Senger,E.C : Cabral Junior, E ; "Neural Networks and its Applications in Digital Distance Protection for Compensated Transmission Lines "- XIII SNPTEE(Portuguese)/1995. (***www.farfilho.com.br***, Folder - Published Works- item 1.5)

[4.3] Reis Filho,F.A : Ferreira, R. A. Benes; "Saturation of Current Transformers and its Implications in Differential Protection Schemes. Part II. Detection and Performance using the Wavelet Transform and Artificial Neural Networks " - XSTPC(Portuguese)/2010(***www.farfilho.com.br***, Folder-Published Works – item 1.17)

[4.4] Reis Filho F.A ; Master Dissertation/POLI/USP/1992. Title :"Protection Scheme based on the Algorithm of Chamia-Liberman and Comparative Analysis with Distance Relays for Compensated Transmission Lines"(Portuguese,***www.farfilho.com.br*** - Folder-Academic Activities)

[4.5] Reis Filho,F.A ; Doctoral Thesis - POLI/USP/2002. Title: "A Proposed Digital Algorithm for Protection of Utility Interconnection – Industry Operating in Cogeneration Systems"(Portuguese, ***www.farfilho.com.br***,Folder-Academic Activities).

С.1.1-9. Совершенствование измерительных органов релейной защиты методами цифровой обработки сигналов[1]

А.Л. КУЛИКОВ, П.А. КОЛОБАНОВ, В.А. ПЕТРОВА
Нижегородский государственный технический университет им. Р.Е. Алексеева
Россия
inventor61@mail.ru

КЛЮЧЕВЫЕ СЛОВА

релейная защита, измерительные органы, цифровая обработка сигналов, дискретное преобразование Фурье

1 ВВЕДЕНИЕ

Стандарт МЭК 61850 предполагает существенное увеличение числа выборочных отсчетов на период промышленной частоты (N = 80 или 256) при обработке сигналов токов и напряжений [1]. В связи с этим увеличиваются требования по быстродействию к измерительным органам релейной защиты, а также происходит усложнение их программной и аппаратной части.

В современных терминалах релейной защиты и автоматики (РЗА) обычно используется дискретное преобразование Фурье (ДПФ) [2] для оценки комплексных значений аварийных токов и напряжений. Однако такой подход далеко не всегда является оптимальным, с точки зрения производительности и точности получаемого результата.

Авторами предлагаются новые алгоритмы цифровых измерительных органов релейной защиты, обладающие повышенным быстродействием и улучшенными точностными характеристиками в условиях наличия апериодической составляющей.

2 ОСНОВНАЯ ЧАСТЬ

Общие предпосылки

Представим входной сигнал тока (напряжения) $x(t)$ в виде набора дискретных значений $x[k]$. Применительно к целям релейной защиты ДПФ, выделяющее в сигнале действительную и мнимую части компоненты промышленной частоты, можно записать следующим образом:

$$Y_{\mathrm{Re}}[n] = \frac{2}{N} \cdot \sum_{k=1}^{N} x[n-N+k] \cdot \sin\left(\frac{2\pi \cdot (k-1)}{N}\right); \qquad (1)$$

$$Y_{\mathrm{Im}}[n] = \frac{2}{N} \cdot \sum_{k=1}^{N} x[n-N+k] \cdot \cos\left(\frac{2\pi \cdot (k-1)}{N}\right). \qquad (2)$$

Последние два выражения представляют собой, по сути, фильтры с конечной импульсной характеристикой (КИХ-фильтры), которые реализуют подавление помех в сигнале, *придавая ему близкую к синусоидальной форму*.

---

1 Работа выполнена при финансовой поддержке Министерства образования и науки РФ (соглашение №14.577.21.0124 о предоставлении субсидии от 20.10.2014, уникальный идентификатор проекта RFMEF157714X0124)

Выражение (1) называется *«дискретное синусное преобразование»* (ДСП), выражение (2) – *«дискретное косинусное преобразование»* (ДКП). Общий принцип, лежащий в основе ДПФ, предполагает параллельную обработку одного и того же массива данных *двумя* фильтрами (ДСП и ДКП) одновременно для получения комплексного значения.

Однако существует и альтернативный способ нахождения комплексных величин, включающий в себя:

1) фильтрацию входного сигнала *одним* фильтром с действительными коэффициентами, таким, чтобы выходной сигнал был близок к идеальной синусоиде.
2) нахождение действительной и мнимой части по нескольким отфильтрованным отсчетам с помощью так называемых *алгоритмов «короткого окна»*.

Предложенный подход, по сравнению с ДПФ, имеет преимущество в том, что набор поступивших в измерительный орган мгновенных значений токов и напряжений обрабатывается полноценным фильтром только один раз, а второй заменяется гораздо более простым алгоритмом *«короткого окна»*, что означает практически двукратное снижение вычислительных затрат. Разумеется, при этом возникает некоторая задержка по времени начала вычислений, требуемая для накопления в памяти нужного количества отсчетов, однако она обычно невелика при достаточно большой частоте дискретизации.

Обозначим результат фильтрации выборки тока (напряжения) как $X[n]$. Алгоритмы «короткого окна» могут быть реализованы с использованием следующих выражений:

Двухвыборочный алгоритм

$$Y_{\mathrm{Re}}[n] = X[n];$$

$$Y_{\mathrm{Im}}[n] = \frac{1}{\sin\left(\frac{2\pi}{N}\right)}\left(X[n-1] - X[n]\cdot\cos\left(\frac{2\pi}{N}\right)\right) \quad (3)$$

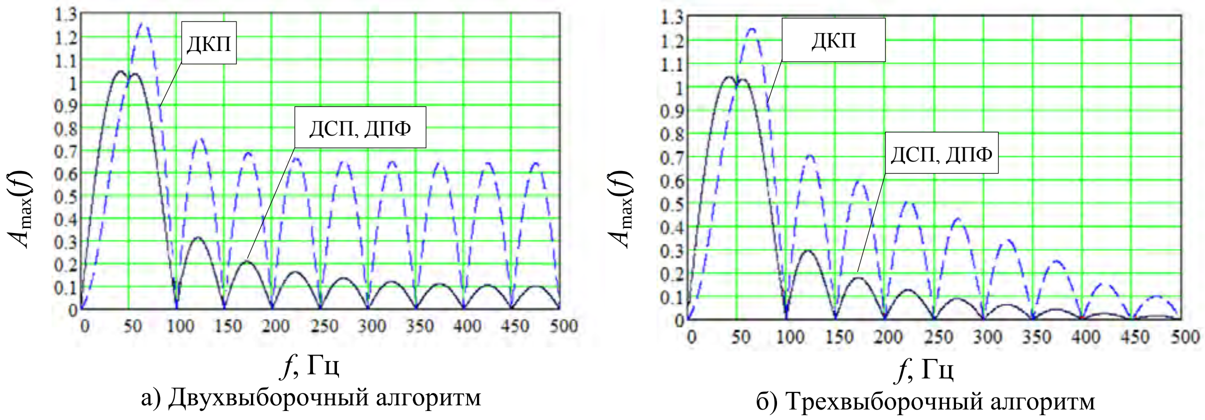
Трехвыборочный алгоритм

$$Y_{\mathrm{Re}}[n] = X[n-1];$$

$$X_{\mathrm{Im}}[n] = \frac{X[n-2] - X[n]}{2\sin\left(\frac{2\pi}{N}\right)}. \quad (4)$$

Сравнительный анализ ДПФ полного периода и алгоритмов на основе упрощенных методов приведен на рис. 1.

Амплитудно-частотные характеристики (АЧХ), приведенные на рис. 1, показывают, каким образом фильтры реагируют на различные спектральные компоненты исходного сигнала. По горизонтальной оси откладываются частоты спектральных компонент исходного сигнала, по вертикальной – коэффициенты амплитудного преобразования *Amax* этих компонент. Нулевое значение коэффициента свидетельствует о том, что компонента выбранной частоты (в данном случае – это все посторонние гармоники, кратные 50 Гц) подавляется фильтром полностью, ненулевое – что она влияет на результат, и чем больше значение *Amax*, тем ее вклад больше.



а) Двухвыборочный алгоритм

б) Трехвыборочный алгоритм

Рис. 1: Амплитудно-частотные характеристики цифровых фильтров в сочетании с алгоритмом «короткого окна» данных

В идеале нам нужна только компонента промышленной частоты (50 Гц), остальные должны быть подавлены полностью, т.е. АЧХ фильтра должна представлять из себя узкую полосу с *Amax* = 1 для частот в районе 50 Гц (с учетом того, что частота в сети может немного варьироваться) однако такое возможно только при физически недостижимом бесконечно большом временном окне. Увеличение временного окна анализа приводит к улучшению фильтрующих свойств, однако с точки зрения РЗА это означает задержку при срабатывании защиты.

АЧХ на графиках были построены для фильтров с временным окном 0.02 с (один период промышленной частоты), в условиях реального сигнала РЗА это обеспечивает хороший компромисс между качеством фильтрации и быстродействием.

Из анализа АЧХ рассматриваемых алгоритмов видно, *что наилучший результат при произвольном входном сигнале обеспечивается с помощью ДСП, т.к. у него минимальные коэффициенты усиления за пределами промышленной частоты*. Однако следует отметить, что на практике такой алгоритм является оптимальным далеко не всегда.

Дело в том, что наличие большого коэффициента усиления фильтра для посторонней гармоники (например, для 125 Гц для фильтров на рис. 1*a*) еще не означает, что результат фильтрации будет искажен – для этого необходимо *наличие* такой компоненты в сигнале.

В частности, при возникновении короткого замыкания (КЗ) в токе может возникнуть ярко выраженная апериодическая составляющая, спектр которой состоит преимущественно из низких частот, которые частично все же проходят через фильтр, искажая замеренное значение.

В то же самое время многие компоненты средних и высоких частот (десятки, сотни, тысячи герц) в сигнале РЗА могут отсутствовать полностью или иметь очень низкий уровень по сравнению с сигналом промышленной частоты.

Поэтому актуальным вопросом, подлежащим разработке в данной статье, является поиск таких алгоритмов расчета, которые обеспечили бы более качественное подавление апериодической составляющей, пусть даже и ценой ухудшения фильтрующих характеристик на более высоких частотах.

Компенсация влияния апериодической составляющей

В общем виде апериодическую составляющую $x_{\text{ап}}(t)$ можно представить следующим образом:

$$x_{\text{ап}}(t) = X_0 \cdot \exp(-t/T_a) = X_0 \cdot \exp(-\gamma \cdot t), \tag{5}$$

где X_0 – начальное значение $x_{\text{ап}}(t)$ при t=0 сек.; $T_a = 1/\gamma$ – постоянная времени затухания;

Наличие апериодической составляющей приводит к ошибкам, которые при расчете амплитуды с помощью ДПФ могут достигать 15% [4].

Основные алгоритмы фильтрации апериодической составляющей в аварийных сигналах тока можно разделить на три вида.

Алгоритмы, настраиваемые на фильтрацию апериодической составляющей с определенным значением постоянной времени затухания. Для этого обычно используется пара ортогональных фильтров вида:

$$Y_{\text{Re}}[n] = \sum_{k=1}^{N} x[n-N+k] \cdot a_k \; ; \; Y_{\text{Im}}[n] = \sum_{k=1}^{N} x[n-N+k] \cdot b_k \; ; \tag{6}$$

где a_k и b_k – коэффициенты фильтра [5], которые подбираются таким образом, чтобы полностью отфильтровать апериодическую составляющую конкретного значения γ.

Вышеуказанные фильтры являются аналогами синусного и косинусного КИХ-фильтров, входящих в преобразование Фурье. Однако здесь также целесообразно перейти к упрощенным алгоритмам с применением выражений (3), (4). В частности, возможно использование одного из следующих вариантов:

$$X[n] = \frac{2}{N} \sum_{k=1}^{N} x[n-N+k] \cdot \left(\cos\left(\frac{2\pi(k-1)}{N} \right) + h_1 \right); \tag{7}$$

$$X[n] = \frac{2}{N} \sum_{k=1}^{N} x[n-N+k] \cdot \left(\sin\left(\frac{2\pi(k-1)}{N} \right) + h_2 \right); \tag{8}$$

где h_1 и h_2 – постоянные коэффициенты, обеспечивающие подавление апериодической составляющей при заданном значении γ. Результаты вычисления коэффициентов h_1 или h_2 при различных значениях γ сведены в табл. 1.

Табл. 1: Значения коэффициентов h_1, h_2 фильтрации по выражениям (7), (8); N=20

Алгоритм (выражение)	h_1, h_2						
	γ=20 1/сек.	γ=40 1/сек.	γ=60 1/сек.	γ=80 1/сек.	γ=100 1/сек.	γ=120 1/сек.	γ=140 1/сек.
(7)	-0,01393022	-0,03537456	-0,06356735	-0,09748136	-0,13592737	-0,17765841	-0,22146289
(8)	-0,06225592	-0,12179187	-0,1773189	-0,22780965	-0,27254991	-0,31115033	-0,34352339

<u>Алгоритмы, ориентированные на фильтрацию апериодической составляющей из диапазона значений постоянной времени затухания.</u>

В общем случае постоянная времени затухания аварийных сигналов тока γ является величиной случайной и зависит от параметров компонентов электроэнергетических систем (особенно ЛЭП), характера замыкания (металлическое или через переходное сопротивление) и ряда других факторов. В таком случае цифровая фильтрация аварийных токов, рассмотренная ранее, становится неэффективной ввиду существенных ошибок.

Для подавления апериодической составляющей аварийного тока в диапазоне значений постоянной времени затухания авторами предлагается использовать следующий фильтр

$$X[n]=\frac{2}{N}\sum_{k=1}^{N}x[n-N+k]\cdot\sin\left(\frac{2\pi(k-1)}{N}-\varphi\right); \qquad (9)$$

со специальным подбором значения фазового угла φ (табл. 2).

Табл. 2: Расчетные значения фазового угла φ

T_a	γ=20 1/сек.	γ=40 1/сек.	γ=60 1/сек.	γ=80 1/сек.	γ=100 1/сек.	γ=120 1/сек.	γ=140 1/сек.
N=20	π/2,45	π/2,55	π/2,65	π/2,77	π/2,91	π/3,09	π/3,24
N=36	π/2,3	π/2,43	π/2,5	π/2,61	π/2,74	π/2,88	π/3,03

Важно, что предложенный алгоритм фильтрации с использованием (9) обеспечивает подавление апериодической составляющей (рис. 4,б), например, в диапазоне значений γ от 0 до 120 1/сек. с погрешностью, не превышающей 5 % при настройке на γ=40 1/сек.

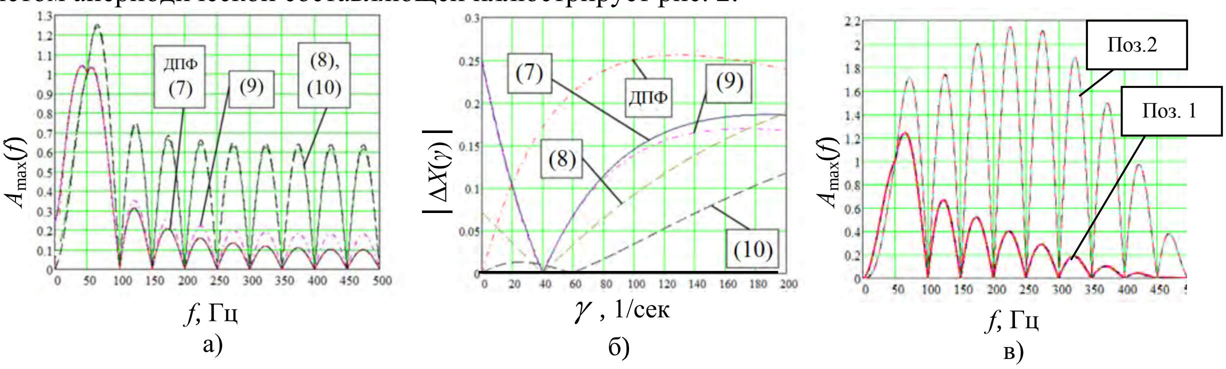
<u>*Универсальные алгоритмы цифровой фильтрации с возможностью подавления апериодической составляющей.*</u> Например, в работе [6] предлагается использование трех последовательных комплексных отчетов $\underline{Y}[n]$, $\underline{Y}[n–1]$, $\underline{Y}[n–2]$, полученных, например, с помощью двухвыборочного алгоритма (3) для реализации дополнительного цифрового фильтра, который полностью подавляет апериодическую составляющую:

$$\underline{Y}_f[n]=\frac{\underline{Y}[n-1]-\underline{d}[n]\cdot\underline{Y}[n-2]}{\underline{a}-\underline{d}[n]};$$
$$\underline{a}=\exp\left(j\frac{2\pi}{N}\right);\ \underline{d}[n]=e^{-\gamma T}=\frac{\underline{Y}[n]-\underline{a}\cdot\underline{Y}[n-1]}{\underline{Y}[n-1]-\underline{a}\cdot\underline{Y}[n-2]}, \qquad (10)$$

где $Y_f[n]$– результат модифицированной квадратурной обработки цифровых отчетов аварийного тока с компенсацией апериодической составляющей.

Применение дополнительного цифрового фильтра существенно увеличивает вычислительные затраты. В соответствии с [3] получаем, что введение дополнительной фильтрации требует вычислительных затрат эквивалентных 88 операций действительного сложения, однако он очень хорошо действует в условиях наличия апериодической составляющей.

Характеристики цифровой фильтрации мгновенных значений аварийного тока с учетом апериодической составляющей иллюстрирует рис. 2.



а) б) в)

Рис. 2: а) и в) АЧХ фильтров; б) Нормированные ошибки фильтрации апериодической составляющей при N=20 ;поз. 1 – косинусный фильтр с коррекцией (12); поз. 2 – синусный фильтр и коррекцией (12).

<u>Замер комплексного сопротивления с использованием дифференциальных уравнений линии</u>

Напряжение и ток, полученные по вышеприведенным алгоритмам, также могут использоваться для реализации замера комплексного сопротивления. Однако также существует вариант, позволяющий уйти от классического деления напряжения на ток – использование дифференциальных уравнений линии.

Входное напряжение и ток в этом случае должны быть подвергнуты синусной квадратурной фильтрации по формуле (1). Используя отфильтрованные результаты, необходимо продифференцировать все входные токи по времени. Хорошие результаты получаются при введении аппроксимации вида

$$\frac{di[k]}{dt} = \frac{i[k+1]-i[k-1]}{2\cdot\Delta t} \tag{11}$$

Известно, что дистанционная защита должна контролировать шесть контуров: три контура фаза-земля ($A0$, $B0$, $C0$) и три контура «фаза-фаза» (AB, BC, CA), при этом на отдельный вход терминала может быть заведена сумма фазных токов параллельной линии $3i_{02}$.
<u>Для контура «фаза-фаза»</u> общий вид дифференциального уравнения линии в этом случае будет:

$$u_{\phi 1}[k]-u_{\phi 2}[k] = R1\cdot(i_{\phi 1}[k]-i_{\phi 2}[k]) + L1\cdot\left(\frac{di_{\phi 1}[k]}{dt}-\frac{di_{\phi 2}[k]}{dt}\right) \tag{12}$$

где $R1$ и $L1$ – сопротивление и индуктивность прямой последовательности, которые требуется найти, $\phi 1$ и $\phi 2$ – индексы фаз. Введем обозначение:

$$u[k] = u_{\phi 1}[k]-u_{\phi 2}[k] \tag{13}$$

<u>Для контура фаза-земля</u> общий вид дифференциального уравнения

$$u_{\phi}[k] = R1\cdot\left(i_{\phi}[k]+k_{RE}\cdot 3i_0[k]+k_{RP}\cdot 3i_{02}[k]\right)+L1\cdot\left(\frac{di_{\phi}[k]}{dt}+k_{XE}\cdot\frac{d3i_0[k]}{dt}+k_{RP}\cdot\frac{d3i_{02}[k]}{dt}\right) \tag{14}$$

Значение $3i_0[k]$ определяется суммированием значений фазных токов:

$$3i_0[k] = i_a[k] + i_b[k] + i_c[k] \tag{15}$$

Коэффициенты k_{RE}, k_{XE}, k_{RP}, k_{XP} вычисляются предварительно и вводятся в терминал. Формулы для их нахождения:

$$k_{RE} = \frac{R0-R1}{3\cdot R1},\ k_{XE} = \frac{X0-X1}{3\cdot X1};$$
$$k_{RP} = \frac{Rp}{3\cdot R1},\ k_{XP} = \frac{Xp0}{3\cdot X1}, \tag{16}$$

Коэффициенты $u[k]$, $i[k]$ и $Di[k]$ рассчитываются так:

$$i[k] = i_{\phi}[k]+k_{RE}\cdot 3i_0[k]+k_{RP}\cdot 3i_{02}[k],\ u[k] = u_{\phi}[k]$$
$$Di[k] = \frac{di_{\phi}[k]}{dt}+k_{XE}\cdot\frac{d3i_0[k]}{dt}+k_{RP}\frac{d3i_{02}[k]}{dt}. \tag{17}$$

Индекс ϕ означает фазу (A, B или C).

Для $k+1$- го отсчета имеем аналогичные математические соотношения. Используя полученные значения, можно найти замер комплексного сопротивления по формулам:

$$R1 = \frac{u[k]\cdot Di[k+1]-u[k+1]\cdot Di[k]}{i[k]\cdot Di[k+1]-i[k+1]\cdot Di[k]}; \tag{18}$$

$$X1 = \omega\cdot\frac{u[k]\cdot i[k+1]-u[k+1]\cdot i[k]}{i[k]\cdot Di[k+1]-i[k+1]\cdot Di[k]}, \tag{19}$$

где ω – круговая частота. Графики зависимости $R(t)$ и $X(t)$ для различных методов приведены на рис. 5

<u>*Натурные эксперименты с цифровой фильтрацией аварийных токов.*</u>

Проводились эксперименты по цифровой фильтрации аварийных осциллограмм с ярко выраженной апериодической составляющей (рис. 3). В качестве экспериментальной базы были выбрана ВЛ 220 кВ Арзамас-Сергач филиала ОАО «ФСК ЕЭС» - Нижегородское ПМЭС. Частота дискретизации составляла 1800 Гц (N=36), а параметры ВЛ и аварийной осциллограмм сведены в табл. 3.

С учетом удельных параметров ВЛ 500, 220 кВ были подобраны коэффициенты для реализации фильтрации по выражениям (7) - (9) с подавлением апериодической составляющей: h_2= –0,21749667; h_1= –0,05055037; $\varphi = \pi/2{,}57$.

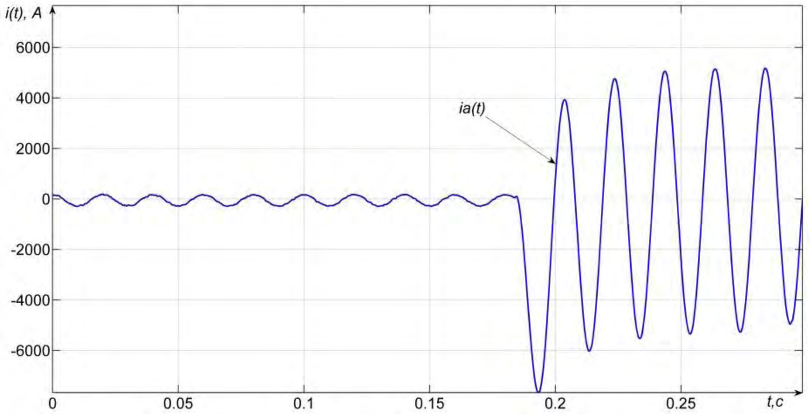


Рис. 3 – Аварийная осциллограмма тока поврежденной фазы ВЛ 220 кВ Арзамас-Сергач

Табл. 3: Параметры ВЛ и характеристики осциллограмм токов короткого замыкания, привлекаемых для натурных экспериментов

Марка провода	Длина ВЛ, км	Оценка T_a, сек.				
		Оценочные значения T_a по параметрам ВЛ (T_a при металлическом КЗ) [7]				Оценочное значение T_a по осциллограмме
		R_0, Ом/км	X_0, Ом/км	T_a, сек.	γ, 1/сек.	
АС-300/39	109,4	0,098	0,429	0,014	72	0,02 сек. 51 1/ сек.

На рис. 4 показано поведение различных алгоритмов при коротком замыкании на примере замера комплексного сопротивления.

Как можно видеть, замерная величина не сразу приходит к установившемуся значению, т.к. в течение 0.02 с после начала замыкания в окне фильтрации оказываются отсчеты доаварийного режима, что эквивалентно появлению дополнительных, ярко выраженных посторонних компонент в спектре сигнала в достаточно широком диапазоне частот. Преимуществом в подобной ситуации обладают фильтры, основанные на синусном, т.к. их коэффициенты амплитудного усиления посторонних частот в среднем самые низкие.

Что касается алгоритмов, использующих косинусный фильтр и его модификации, то, несмотря на то, что они немного лучше подавляет апериодическую составляющую, их поведение в случае реального КЗ нестабильно (ломаные линии на рис. 4), и может привести к кратковременным ложным срабатываниям релейной защиты.

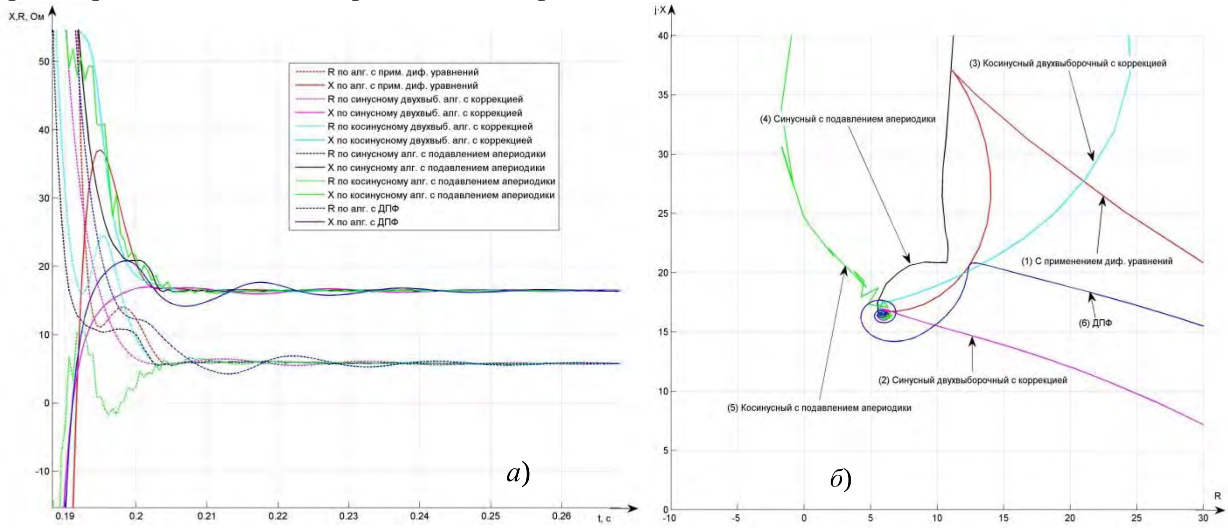


Рис. 4 – Графики зависимости $X(t)$ и $R(t)$ для различных алгоритмов (*а*), и годографы сопротивлений (*б*)

Компенсация влияния переходного сопротивления

Общий принцип используемого при определении места повреждения (ОМП) алгоритма компенсации влияния переходного сопротивления приведен на рис. 4*а*.

Для компенсации влияния переходного сопротивления необходимо измерять напряжение в месте установки защиты тогда, когда ток в переходном сопротивлении $\underline{I}_К$ переходит через ноль [9, 10]. Чтобы найти его фазу, используется опорный ток $\underline{I}_{оп}$, причем он выбирается так, чтобы разность фаз β (иначе называемая углом коррекции) между $\underline{I}_{оп}$ и $\underline{I}_{К}$ не зависела от ЭДС в схеме замещения и величины переходного сопротивления.

В роли $\underline{I}_{оп}$ могут выступать функции токов обратной $\underline{I}_2$ и нулевой $\underline{I}_0$ последовательностей, а также чисто аварийного тока $\underline{I}_{ав} = \underline{I}_1 - \underline{I}_{н}$, где $\underline{I}_{н}$ – ток предшествующего нагрузочного режима. В [9] показано, что расчетные выражения этих функций зависят от вида замыкания и поврежденных фаз. Например, при однофазном замыкании фазы *A* в качестве $\underline{I}_{оп}$ могут использоваться непосредственно сами токи $\underline{I}_{ав}$, $\underline{I}_2$, $\underline{I}_0$.

Угол β определяется степенью неоднородности сети, т.е. непостоянством отношения X/R у различных ее элементов. Для упрощения выкладок можно приблизительно принять X/R = const, чему соответствует $\beta = 0$.

На рис. 5*а* представлена векторная диаграмма при замыкании на защищаемой линии. Предположим, что опорный ток строго совпадает с током в месте установки защиты. Отрезок *OA* представляет собой измеряемое в месте установки защиты сопротивление. Через точку *A* проведем прямую 1, параллельную опорному току $\underline{I}_{оп}$. Через точку *O* проведем прямую 2 под углом φ_L к действительной оси, тогда отрезок *OB* будет представлять собой сопротивление линии до точки КЗ $\underline{Z}_{комп}$, а отрезок *BA* – погрешность $\Delta\underline{Z}_{пер}$, вносимую переходным сопротивлением. По сути, длина отрезка *OB* есть расстояние до места повреждения в относительных единицах. Для сравнения на рисунке также приведен отрезок *OC*, которому соответствует относительная длина защищаемой линии и ее полное сопротивление $\underline{Z}_{лин}$.

Такой алгоритм, дополненный токовыми пусковыми органами во избежание неселективной работы предлагается использовать в качестве первой ступени дистанционной защиты, и его применение позволяет обеспечить достаточно высокую чувствительность при КЗ через переходное сопротивление [11].

Но следует отметить одну немаловажную деталь: данный алгоритм, в отличие от двумерного замера комплексного сопротивления, формирует одномерный результат (длину), и поэтому сильно чувствителен к наличию апериодической составляющей в первичных токах и напряжениях.

Рассмотрим короткое замыкание с ярко выраженной апериодической составляющей в самом начале смежной линии, где первая ступень ДЗ действовать уже не должна. Как уже показывалось выше, обычный фильтр Фурье частично пропустит апериодическую составляющую, в результате чего замеренное комплексное значение получается колеблющимся во времени.

В случае классической дистанционной защиты двумерное комплексное сопротивление во время переходного процесса в электрической сети даже при плохой фильтрации аварийного сигнала необязательно попадет в уставочную область, т.к. для этого требуется одновременное уменьшение замерных *R* и *X*.

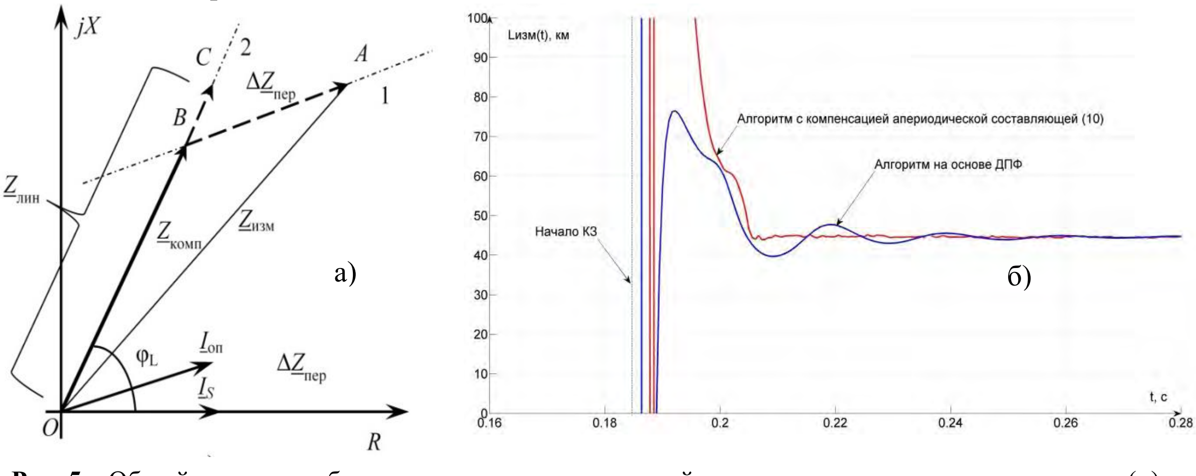


Рис. 5 – Общий принцип работы алгоритма с компенсацией влияния переходного сопротивления (*а*) и его динамические характеристики во времени (*б*).

В то же самое время для алгоритма с компенсацией влияния переходного сопротивления, который сильно зависит от правильности определения фазы опорного тока, подобные колебания могут привести к тому, что измеренная длина может оказаться в диапазоне срабатывания и потребуется дополнительное загрубление защиты. Поэтому для обеспечения правильной работы такого алгоритма придется ждать завершения переходного процесса длиной в несколько периодов промышленной частоты.

Применение методик подавления апериодической составляющей благоприятно сказывается на динамических свойствах алгоритма, позволяя сильно уменьшить длительность осцилляций (рис. 5*б*), и, соответственно, задержку в срабатывании.

3 ЗАКЛЮЧЕНИЕ

Использование новых упрощенных алгоритмов цифровых измерительных органов на основе сочетания подавляющего апериодическую составляющую фильтра с фильтрацией «короткого окна» позволяет практически в два раза снизить вычислительные затраты и улучшить динамические свойства цифровых измерительных органов релейной защиты.

ЛИТЕРАТУРА

[1] Implementation guideline for digital interface to instrument transformers using IEC 61850-9-2.

[2] Шнеерсон Э.М. Цифровая релейная защита. — М.: Энергоатомиздат, 2007. — 549 с.

[3] Маклеллан, Дж. Х., Рейдер, Ч. М. Применение теории чисел в цифровой обработке сигналов. – М.: Радио и связь, 1983. – 264 с.

[4] Yong Guo, Deshu Chen. Simplified algorithms for removal of the effect of exponentially decaying DC-offset on the Fourier algorithm // IEEE Transactions on power delivery, Vol. 18, No. 3, July 2003. pp. 711-717.

[5] Lobos, T. Nonrecursive methods for real-time determination of basic waveforms of voltages and currents // IEE Proceedings, Vol. 136, No. 6, November 1989. Pp. 347-351

[6] Chen Ching-Shan, Liu Chih-Wen, Jiang Joe-Air. Application of Combined Adaptive Fourier Filtering Technique and Fault Detector to Fast Distance Protection // Transactions on Power delivery, Vol. 21, NO. 2, April 2006. pp. 619-626.

[7] Rebizant W., Terzija V. Asynchronous generator behavior after a sudden load rejection.// PowerTech Conference Proceedings, IEEE Bologna, 23-26 June, 2003.

[8] Rebizant W., Szafran J., Wiszniewski A. Digital signal processing in power system protection and control. New York: Springer, 2011. 316 p.

[9] Висящев А.Н. Приборы и методы определения места повреждения на линиях электропередачи. — Иркутск: Изд-во ИрГТУ, 2001. Ч1.

[10] Аржанников Е.А., Лукоянов В.Ю., Мисриханов М.Ш., Определение места короткого замыкания на высоковольтных линиях электропередачи, 2003. — 272 с.

[11] Куликов А.Л., Колобанов П.А., Обалин М.Д. Применение методов определения места повреждения в цифровой дистанционной защите линии электропередач // Известия ВУЗов. Электромеханика. - 2014. - №1. - С. 83-87.

ОАО «СО ЕЭС»
CIGRE Российский Национальный Комитет
АБС Электро
ВНИИР

С.1.1-10. Обучаемые модули микропроцессорных защит линий электропередачи

Ю.Я. Лямец, М.В. Мартынов, А.А. Нестерин
Исследовательский центр «Бреслер»
Россия
usmf_th@mail.ru

КЛЮЧЕВЫЕ СЛОВА

Релейная защита, обучение, модели, условное отображение.

1 ВВЕДЕНИЕ

В настоящее время наблюдается высокая интенсивность исследований, направленных на совершенствование алгоритмов релейной защиты и автоматики (РЗА). Следует отметить американскую компанию SEL, шведскую ABB, китайскую NARI и др. Поиск эффективных алгоритмов РЗА ведется в чебоксарском релестроении. Этим вопросам также посвящены труды иных отечественных школ релейной защиты.

В докладе представляются методы объединения информации для решения задач РЗА. Информация о состоянии защищаемого объекта, представленная в объектном пространстве соответствующей размерности, отображается на плоскостях замеров, которыми оперируют модули РЗА. Разработанные методы обучения позволяют объединить всю имеющуюся информацию в одном алгоритме для достижения максимально возможной чувствительности РЗА при гарантированной селективности.

2 СОВМЕСТНОЕ ОБУЧЕНИЕ МОДУЛЕЙ

Режим работы защищаемого объекта определяется его объектными параметрами. Варьируемые параметры защищаемого объекта служат координатами объектного пространства C (рис.1) . Режим задаётся точкой в этом пространстве [1,2], координаты которой определяют вектор объектных параметров $\mathbf{x}$. Например, в трёхмерном пространстве параметров защищаемой линии электропередачи $\mathbf{x}=\left[x_f, R_f, \delta\right]^{\mathrm{T}}$, где x_f – расстояние до места повреждения, R_f – переходное сопротивление в месте повреждения, δ – угол передачи. Множество режимов задаётся областью $G \subset C$ (рис. 1). Посредством преобразования $\mathbf{z}_i = F_i\left(\mathbf{x}\right)$, выполняемого имитационной моделью объекта, режим $\mathbf{x}$ отображается в соответствующую точку $\mathbf{z}_i$ на *i*-ой плоскости замеров. Всё множество режимов $\mathbf{x} \in G$ в объектном пространстве G отображается на *i*-ой плоскости областью $S_i = F_i\left(G\right)$ замеров $\mathbf{z}_i$.

Альтернативным β-режимом работы защищаемого объекта называется режим, в котором защита не должна срабатывать ни при каких условиях. Контролируемый α-режим – режим, в котором релейная защита призвана срабатывать. Задача обучения релейной защиты – не допустить срабатывания в β-режимах работы и обеспечить срабатывание в максимально возможном числе α-режимов.

Область срабатывания модуля защиты определяется как собственная α-область $S_{\alpha\alpha} = S_\alpha \setminus S_{\alpha\beta} = S_\alpha \setminus S_\beta$ – разность отображений областей G_α и G_β (рис. 2). На первой плоскости A_1 определяются безусловные отображения $S_{\alpha 1} = F_{\alpha 1}(G_\alpha)$, $S_{\beta 1} = F_{\beta 1}(G_\beta)$, их пересечение $S_{\alpha\beta 1} = S_{\alpha 1} \cap S_{\beta 1}$ и собственная α-область $S_{\alpha\alpha 1} = S_{\alpha 1} \setminus S_{\alpha\beta 1}$. Условные отображения применяются, начиная со второго этапа обучения релейной защиты.

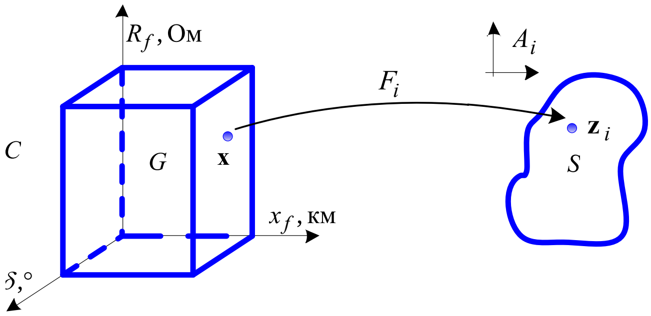


Рис. 1: Иллюстрация процесса отображения области режимов G на i-ую плоскость замеров

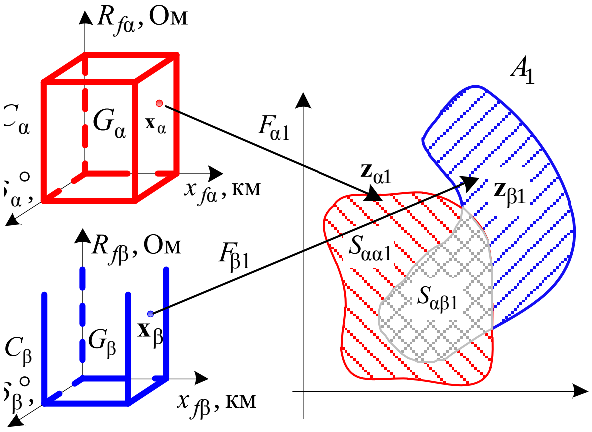


Рис. 2: Иллюстрация процесса отображения области режимов G на плоскость замеров A_1

Условия отображения на второй плоскости A_2 и последующих плоскостях связаны с выделением тех α- и β-режимов, которые не удалось отличить друг от друга на плоскости A_1 (рис.3). Соответствующие операции $F_{\alpha 1}^{-1}$ и $F_{\beta 1}^{-1}$ представляют собой обратные преобразования взаимной области $S_{\alpha\beta 1}$, а именно $G_{\alpha 1} = F_{\alpha 1}^{-1}(S_{\alpha\beta 1})$, $G_{\beta 1} = F_{\beta 1}^{-1}(S_{\alpha\beta 1})$ и теперь уже условных отображений на (плоскость A_2) $S_{\alpha 2}^{\text{усл}} = F_{\alpha 2}(G_{\alpha 1})$, $S_{\beta 2}^{\text{усл}} = F_{\beta 2}(G_{\beta 1})$, где в общем случае обнаружится своя взаимная область $S_{\alpha\beta 2}^{\text{усл}} = S_{\alpha 2}^{\text{усл}} \cap S_{\beta 2}^{\text{усл}}$ и остающаяся после её исключения область срабатывания второго модуля $S_{\alpha\alpha}^{\text{усл}} = S_{\alpha 2}^{\text{усл}} \setminus S_{\beta 2}^{\text{усл}}$. Если бы оказалось, что области $S_{\alpha 2}^{\text{усл}}$ и $S_{\beta 2}^{\text{усл}}$ не пересекаются, это означало бы, что на плоскостях A_1 и A_2 все α-режимы из объектной области распознаются без изъятий. Обученные модули объединяются согласно логической схеме по рис. 4.

Но в общем случае наращивание группы распознающих модулей потребует продолжения в той же последовательности. Соответствующие преобразования показаны в табл. 1. Рекурсия, организуемая формулами табл. 1, доводится до последней плоскости A_n, а далее может быть возвращена на плоскость A_1 или же повернута в обратном направлении.

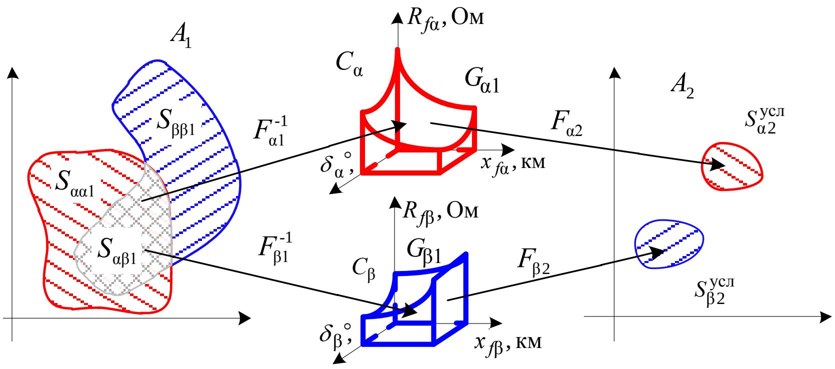


Рис. 3: Условное отображение режимов на вторую плоскость замеров A_2

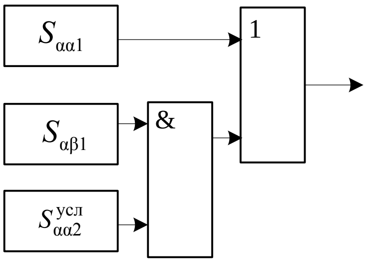


Рис. 4: Логическая схема последовательной распознающей структуры

Табл. 1: Преобразования при наращивании группы распознающих модулей

Действие	Математическое выражение
Определение областей α- и β-режимов, не распознанных на плоскости A_{i-1}	$G_{\alpha,i-1} = F_{\alpha,i-1}^{-1}\left(S_{\alpha\beta,i-1}^{\text{усл}}\right)$, $G_{\beta,i-1} = F_{\beta,i-1}^{-1}\left(S_{\alpha\beta,i-1}^{\text{усл}}\right)$
Отображение объектных областей $G_{\alpha,i-1}$, $G_{\beta,i-1}$ на последующей плоскости A_i	$S_{\alpha i}^{\text{усл}} = F_{\alpha i}\left(G_{\alpha,i-1}\right)$, $S_{\beta i}^{\text{усл}} = F_{\beta i}\left(G_{\beta,i-1}\right)$
Выделение взаимной области отображения режимов $S_{\alpha\beta i}$	$S_{\alpha\beta i}^{\text{усл}} = S_{\alpha i}^{\text{усл}} \cap S_{\beta i}^{\text{усл}}$
Выделение области срабатывания *i* модуля	$S_{\alpha\alpha i}^{\text{усл}} = S_{\alpha i} \setminus S_{\alpha\beta i}^{\text{усл}}$

3 РАСПОЗНАВАНИЕ СЛОЖНОГО ПОВРЕЖДЕНИЯ ЭЛЕКТРИЧЕСКОЙ СЕТИ

В докладе рассмотрен способ распознавания сложного повреждения электрической системы. Его особенность заключается в разложении сложного противостояния групп режимов на элементарные противостояния. Противостоянием называется ситуация, в которой необходимо разграничить α- и β-режимы [3]. Предложенный метод показан на примере распознавания повреждения какой-либо фазы электрической сети, скажем фазы *A*, вследствие какого-нибудь неполнофазного замыкания на землю. Информационную базу распознающей структуры релейной защиты в данной задаче составляют три тока, наблюдаемые в текущем режиме электропередачи. Имитационная модель приведена на рис. 5. Варьируемые параметры приведены в табл. 2. Заметим, что при двухфазных земляных КЗ варьируется на одно переходное сопротивление больше, чем при однофазных КЗ. Фиксированы напряжения источников: $E_s = E_r = U_{\text{ф,ном}} = (500/\sqrt{3})$ кВ, длина линии $l = 280$ км, первичные параметры линии прямой и нулевой последовательностей в Ом/км: $X_1^0 = 0{,}302$, $R_1^0 = 0{,}12$, $X_0^0 = 0{,}696$, $R_0^0 = 0{,}27$. Предельное значение $R_{\text{пред}}$ переходных сопротивлений в α-режимах определялось из условия распознавания всего множества G_α, иначе говоря, из условий $G_\alpha \equiv G_{\alpha\alpha}$, $G_{\alpha\beta} \equiv 0$.

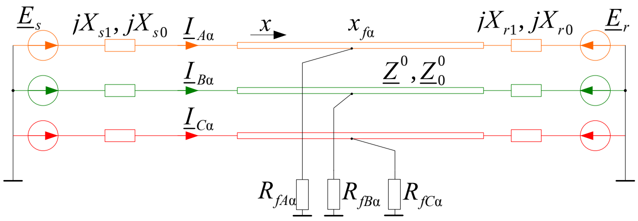


Рис. 5: Имитационная модель электропередачи

Гальваническая связь с землей одной из фаз электрической системы, в данном случае фазы A, – сложное событие. Сложность обусловлена, во-первых, существованием трех разнотипных α-режимов: однофазного КЗ $K_{A\alpha}^{(1)}$ и двухфазных КЗ $K_{AB\alpha}^{(1,1)}$, $K_{CA\alpha}^{(1,1)}$, а во-вторых, их противостоянием с тремя β-режимами: однофазными КЗ $K_{B\beta}^{(1)}$, $K_{C\beta}^{(1)}$ и двухфазным $K_{BC\beta}^{(1,1)}$. Создание информационного портрета структуры, распознающей сложное повреждение объекта, начинается с разграничения противостоящих элементарных событий. В данной задаче насчитывается девять таких пар, обозначаемых по типу $K_{A\alpha}^{(1)} \mid K_{B\beta}^{(1)}$ с разделительной чертой между обозначениями соответствующих α- и β-режимов.

Табл. 2: Варьируемые параметры имитационной модели по рис. 5

Параметры α- и (или) β-режимов	Диапазоны изменения
$x_{f\alpha}, x_{f\beta}$	0…l
$R_{fA\alpha}, R_{fB\alpha}, R_{fC\alpha}$	0… $R_{\text{пред}}$
$R_{fB\beta}, R_{fC\beta}$	0…∞
$\delta = \arg\left(\underline{E}_s / \underline{E}_r\right)$	-60°…60°
X_{s1}	140…160.0 Ом
X_{r1}	100…110.0 Ом
X_{s0}/X_{s1}	0.4…0.5
X_{r0}/X_{r1}	2.5…3.0

Каждое элементарное противостояние разрешается отдельным распознающим модулем, а вся распознающая структура насчитывает девять модулей, группируемых по три логическими операциями «И» (рис. 6).

Информационный портрет распознающей структуры по рис. 6 представлен в табл. 3-4. Определен замер, разрешающий автономно часть элементарных противостояний между α- и β-режимами. Таким замером оказалось отношение между токами обратной и нулевой последовательностей $\underline{I}_2 / \underline{I}_0$. С его помощью удаётся разрешить четыре противостояния $K_{A\alpha}^{(1)} \mid K_{B\beta}^{(1)}, K_{A\alpha}^{(1)} \mid K_{C\beta}^{(1)}$, $K_{AB\alpha}^{(1,1)} \mid K_{B\beta}^{(1)}$, $K_{CA\alpha}^{(1,1)} \mid K_{C\beta}^{(1)}$ из девяти (табл. 3, показан пример для одного элементарного противостояния $K_{A\alpha}^{(1)} \mid K_{B\beta}^{(1)}$). Остающиеся пять противостояний не удается разрешить на основе какого-либо одного замера.

Применяется метод последовательных условных отображений, и с его помощью определяются дополнительный замер $\underline{I}_1(\overset{*}{\underline{I}}_2 + \overset{*}{\underline{I}}_0)$, включение которого в общую группу с первым замером $\underline{I}_2 / \underline{I}_0$ позволяет решить остающуюся часть задачи. В совокупности с первым замером он позволяет разрешить все пять остающихся противостояний α- и β-режимов $K_{A\alpha}^{(1)} \mid K_{BC\beta}^{(1,1)}$, $K_{AB\alpha}^{(1,1)} \mid K_{BC\beta}^{(1,1)}$, $K_{AB\alpha}^{(1,1)} \mid K_{C\beta}^{(1)}$, $K_{CA\alpha}^{(1,1)} \mid K_{B\beta}^{(1)}$, $K_{CA\alpha}^{(1,1)} \mid K_{BC\beta}^{(1,1)}$ (табл. 4, приведён пример разрешения одного противостояния $K_{A\alpha}^{(1)} \mid K_{BC\beta}^{(1,1)}$).

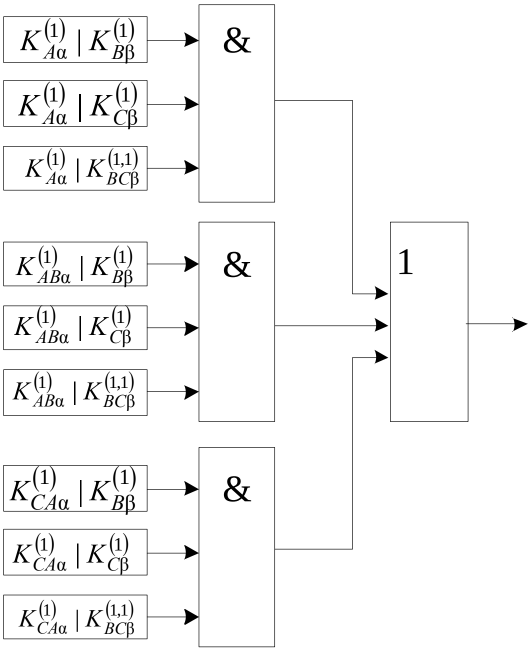


Рис. 6: Структура, распознающая причастность фазы *A* к замыканию на землю

Табл. 3: Противостояние режимов, разрешаемое на одной плоскости

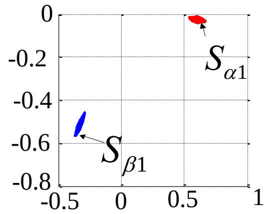
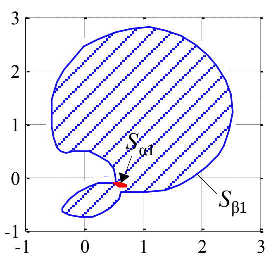
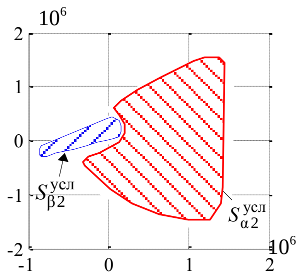
Режимы		Замер $\underline{I}_2 / \underline{I}_0$, о.е.
α	β	
$K_A^{(1)}$	$K_B^{(1)}$	

Табл. 4: Пример распознавания противостояния $K_{A\alpha}^{(1)} \mid K_{BC\beta}^{(1,1)}$ на двух плоскостях

Режимы		Замеры	
α	*β*	$\underline{I}_2 / \underline{I}_0$, о.е.	$\underline{I}_1(\overset{*}{\underline{I}}_2 + \overset{*}{\underline{I}}_0)$, А^2
$K_A^{(1)}$	$K_{BC}^{(1,1)}$		

4 ЭКВИВАЛЕНТИРОВАНИЕ ЭЛЕКТРИЧЕСКОЙ СЕТИ

В докладе рассмотрена задача эквивалентирования сложной имитационной модели электрической сети. Актуальность задачи подчеркивается тем обстоятельством, что имитационная модель объекта призвана обучать его защиту, однако использование сложной многопараметрической модели наталкивается на значительные вычислительные трудности, связанные с необходимостью расчёта разветвленной электрической сети во многих режимах её работы. Возникает задача эквивалентирования исходной модели простейшей моделью с минимальным числом варьируемых параметров. Такая возможность предоставляется методом эквивалентного генератора, но необходимо справиться с проблемой задания его параметров. Допустим, электрическая сеть по рис.7*а* имеет исходную модель по рис.7*б,* где $\underline{E}_1,\underline{E}_2,\underline{E}_3$ – ЭДС систем *ЭС1, ЭС2, ЭС3, РС* – реле сопротивления. Красным цветом обозначены участки КЗ в зоне, синим – вне зоны. $\underline{I}_s,\underline{U}_s$ – ток и напряжение в месте наблюдения, $\underline{Z}_1,\underline{Z}_2,\underline{Z}_3$ – сопротивления систем, $R_{f\alpha}$ – переходное сопротивление в α- режимах КЗ в зоне, $R_{f\beta1}$, $R_{f\beta2}$ $R_{f\beta3}$ – переходные сопротивления в β-режимах КЗ вне зоны, $x_{f\alpha}$ – расстояние до места повреждения при КЗ в зоне, $x_{f\beta1},x_{f\beta2}$, $x_{f\beta3}$ – расстояние до места повреждения при КЗ вне зоны на соответствующих участках, l_1,l_2,l_3 – длины линий электропередачи, $l_{зн}$ – длина защищаемой зоны. Ставится задача представления сети относительно конца защищаемой зоны эквивалентными генераторами α- и β-режимов (рис. 8). Значения параметров сети приведены в табл. 5, диапазонов изменения параметров – в табл. 6. Исходная модель призвана обучить эквивалентные модели.

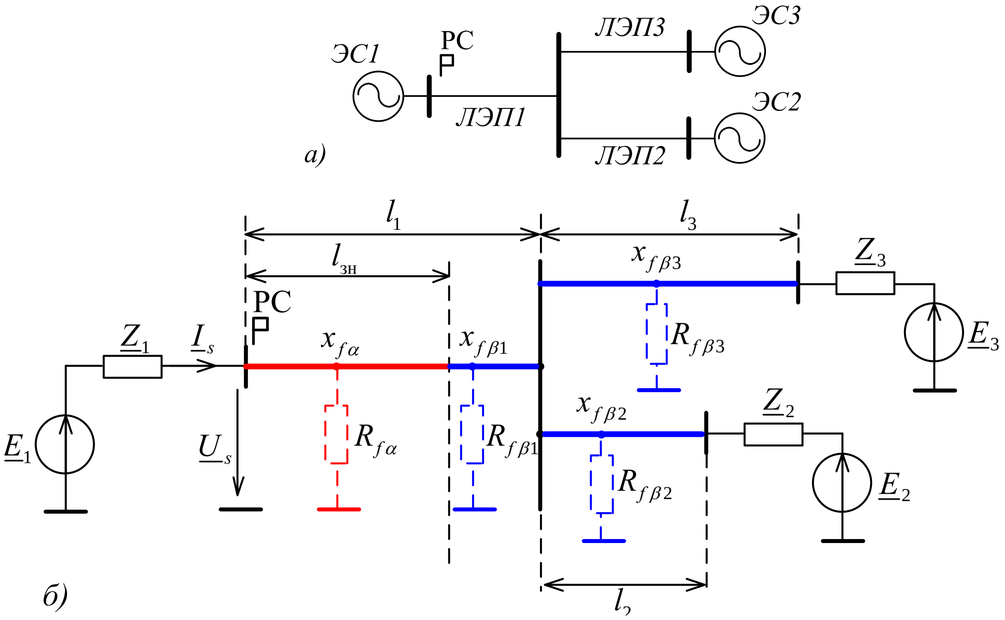


Рис. 7: Исходная сеть и её модель

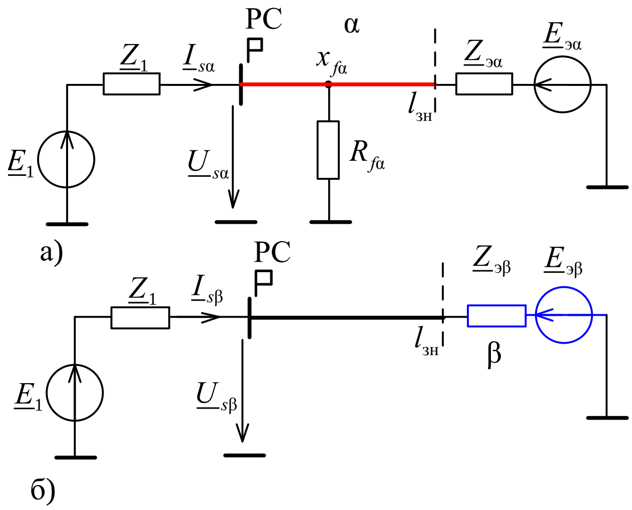


Рис. 8: Эквивалентные модели сети: *а* - в α-режимах, *б* - в β-режимах

Эквивалентная модель строится на основе клеточной структуры [4]. Области отображений разбиваются на N^2 ячеек. Те пары, составленные из ячеек разных плоскостей, которые несут информацию о режимах эквивалентируемой части сети, выявляются следующим образом. Для каждой ячейки ΔS_{1pq} (рис. 9) на первой плоскости $\underline{Z}_{э\beta}$ $(i=1)$ определяется множество отображающихся в ней режимов ΔG_{1pq}. Эти же режимы отображаются на плоскости второго параметра $\underline{E}_{э\beta}$ в подобласти $S_2\left(\Delta G_{1pq}\right)$, которая содержит подмножество своих ячеек, образующих общие коды с ячейкой ΔS_{1pq} первой плоскости (табл. 7). Подобная операция проводится для всех ячеек области S_1, и каждой ячейке на плоскости $\underline{Z}_{э\beta}$ ставится в соответствие подмножество ячеек плоскости $\underline{E}_{э\beta}$. Как следствие, эквивалентная модель задаётся набором ячеек на плоскостях $\underline{Z}_{э\beta}$ и $\underline{E}_{э\beta}$, а кроме того граничными линиями L_1 и L_2.

Табл. 5: Значения параметров электрической сети

Параметр	E_3/E_1, о.е.	δ_1, град	δ_3, град	l_1, км	l_2, км	l_3, км	$l_{зн}$, км	$\underline{Z}_1$, Ом	$\underline{Z}_3$, Ом
Значение	1,05	0	-10	100	100	200	85	$1+j10$	$1+j7$

Табл. 6: Диапазоны изменения параметров электрической сети

Параметр	E_2/E_1, о.е.	δ_2, град	Z_2, Ом	$\arg \underline{Z}_2$, град	$R_{f\alpha}$, Ом	$R_{f\beta}$, Ом
Диапазон	0,95…1,05	-30…30	1…10	70…90	0…100	0…∞

Табл. 7: Коды ячеек подобласти $S_2\left(\Delta G_{1,10,10}\right)$

p_2	21	21	21	21	22	22	22	22	22	23	23	23	23	23	24	24
q_2	2	3	4	5	2	3	4	5	6	2	3	4	5	6	4	5

Задача решается путем отображения эквивалентных параметров на двух комплексных плоскостях $\underline{Z}_э$ и $\underline{E}_э$. На рис.9 дана иллюстрация для параметров β-модели.

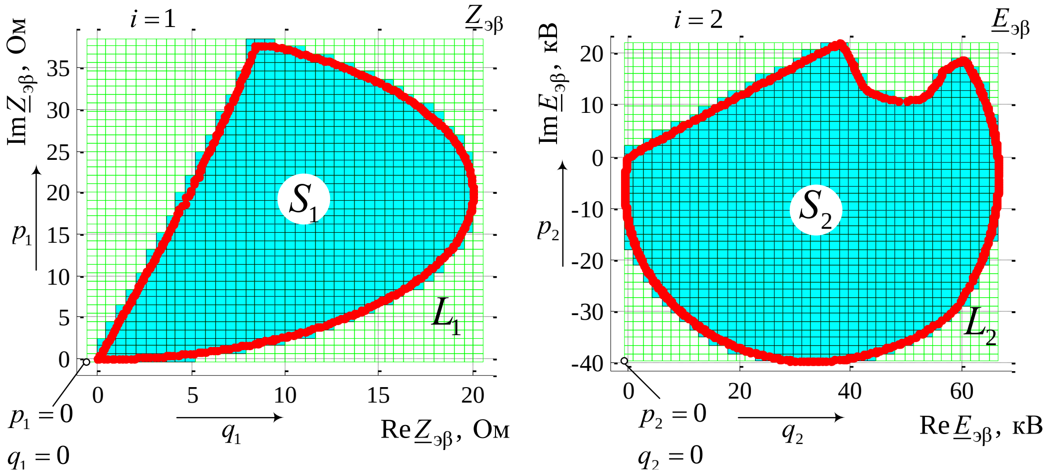


Рис. 9: Разбиение прямоугольников, охватывающих отображения эквивалентных параметров $\underline{Z}_{э\beta}$ и $\underline{E}_{э\beta}$, на $N^2=1600$ ячеек

На рис.10 показана область срабатывания реле сопротивления, обученного от эквивалентной модели сети при дроблении областей отображения её параметров на $N^2=100$ и $N^2=1600$ ячеек. Как видим, с увеличением числа ячеек модель всё более освобождается от избыточных режимов, приближаясь по своим информационным свойствам к исходной имитационной модели.

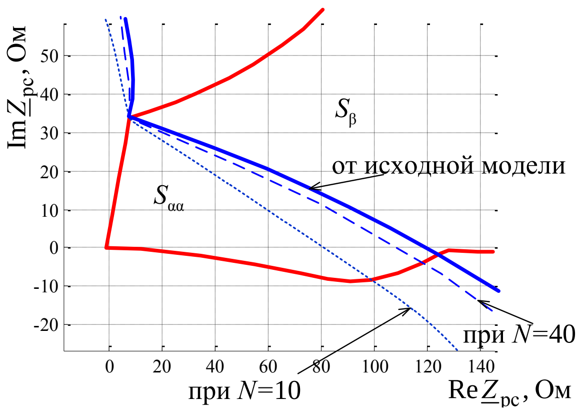


Рис. 10: Отображение на плоскости $\underline{Z}_{рс}$ множества режимов исходной и эквивалентной моделей

5 ЗАКЛЮЧЕНИЕ

1. Применение последовательного условного отображения при обучении модулей релейной защиты позволят повысить её чувствительность при гарантированной селективности. Методы условных отображений создают теоретическую базу для разработки алгоритмов обучения многомерной релейной защиты, оперирующей совокупностью замеров, каждый из которых отображается на соответствующей уставочной плоскости.

2. Информационная интерпретация повреждения защищаемого объекта становится весьма наглядной в форме противостояния совокупности α- и β-режимов. При построении информационного портрета особенно эффективно разделение сложного противостояния на элементарные пары противостоящих режимов с обучением каждого распознающего модуля, разрешающего одно из противостояний, на минимально возможном числе уставочных плоскостей.

3. Задание параметров эквивалентной имитационной модели областями на комплексных плоскостях позволяет воспроизвести в простейшей модели все режимы сложной исходной модели.

ЛИТЕРАТУРА

[1] Лямец Ю.Я., Кержаев Д.В., Нудельман Г.С., Романов Ю.В. Граничные режимы в методике обучения релейной защиты. ч.1,2,3. – Изв. вузов. Электромеханика, 2009, №4. – С.24-30; 2010, №2. – С.53-59; №4. – С.53-58.

[2] Лямец Ю.Я., Нудельман Г.С., Подшивалина И.С., Романов Ю.В. Эффекты многомерности в релейной защите. – Электричество, 2011, №9. – С.48-54.

[3] Лямец Ю.Я., Нудельман Г.С., Романов Ю.В., Мартынов М.В., Воронов П.И. Распознавание противостоящих режимов электрической системы. – Нелинейный мир. – 2011. - т.9, №9. – С. 600-606.

[4] *Пат.* 2247456 РФ. Способ релейной защиты энергообъекта / Лямец Ю.Я., Ефимов Е.Б., Нудельман Г.С. // кл. H02H 3/40, 2002.

С.1.1-12. Системы автоматизации подстанций на основе мощных многофункциональных микропроцессорных устройств.

В.И. КАПУСТИН, С.Д. ГОРЕНКОВ
ООО «Сименс»
Россия
victor.kapustin@siemens.com

КЛЮЧЕВЫЕ СЛОВА

Новая концепция релейной защиты и автоматики, полное дублирование, комбинация защиты, автоматики и измерений в одном устройстве, новое поколение устройств релейной защиты, МЭК 61850, простота обслуживания, повышенная надежность, сниженные капитальные затраты, сниженные затраты на обслуживание.

1 ВВЕДЕНИЕ

Существующая в России нормативно-техническая документация (НТД) описывает требования к выполнению комплексов РЗА, опираясь на исторически сложившееся разделение функций вторичных систем на релейную защиту, автоматику, управление, сигнализацию, оперативную блокировку и измерения для ведения и контроля технологического процесса. К настоящему времени в России уже сформировался подход к выполнению комплексов РЗА на микропроцессорных устройствах (терминалах) различных производителей, который практически полностью повторяет идеологию распределения функций по отдельным устройствам, использовавшуюся в электромеханических и микроэлектронных устройствах РЗА. Для обеспечения аппаратного и функционального резервирования при выполнении комплекса РЗА любого присоединения используется несколько микропроцессорных терминалов. Обмен необходимой информацией между функциями РЗА одного присоединения, реализуемыми в разных терминалах, выполняется с использованием «поперечных» связей, которые организуются либо по «меди» с использованием дискретных входов/выходов терминалов, либо передачей GOOSE-сообщений по стандарту МЭК 61850. Функции управления, сигнализации, оперативной блокировки и измерений, необходимые для ведения и контроля технологического процесса, реализуются, как правило, на контроллерах присоединений и измерительных преобразователях автоматизированной системы управления технологическими процессами (АСУ ТП). Обмен необходимой информацией о положении коммутационных аппаратов присоединения, состояния их приводов между терминалами РЗА и контроллерами АСУ ТП организуется также либо по «меди», либо передачей GOOSE-сообщений по стандарту МЭК 61850. На наш взгляд, такие комплексы РЗА имеют следующие недостатки: необходимость использования довольно большого количества терминалов и шкафов, в которые они устанавливаются; наличие довольно значительного объёма «поперечных» связей между терминалами РЗА и контроллерами АСУ ТП. Все это удорожает стоимость таких комплексов и усложняет их эксплуатационное/техническое обслуживание. Используемая идеология распределения функций РЗА по отдельным устройствам (терминалам) также имеет свои недостатки: релейная защита и автоматика (АПВ, УРОВ) в таких комплексах, как правило, выполняется в разных терминалах. Функции АПВ и УРОВ реализуются, как правило, в терминалах управления и мониторинга соответствующего выключателя и не предусматривается резервирование (дублирование) этих функций. Между тем, вывод из работы (отсутствие по каким-либо причинам) функций АПВ и УРОВ на находящемся под рабочим напряжением защищаемом присоединении приводит к различным режимным ограничениям в прилегающей сети.

Появившиеся в последнее время на рынке новые мощные многофункциональные микропроцессорные устройства РЗА, например, серии Siprotec 5 производства SIEMENS AG, позволяют реализовать все функции РЗА и вторичных систем любого присоединения 110-750 кВ в одном устройстве. Для выполнения всех требований существующих НТД по аппаратному и функциональному резервированию предлагается использовать два устройства с полным дублированием всех основных функций. Это позволяет резко сократить количество устройств (терминалов) и шкафов, снизить стоимость комплекса вторичных систем и избавиться от большинства недостатков существующих в настоящее время комплексов РЗА и вторичных систем.

2 ОСНОВНАЯ ЧАСТЬ

Идеология построения систем РЗА на мощных многофункциональных микропроцессорных устройствах предполагает группировку и привязку функций РЗА отличную от принятой в настоящее время. Все основные функции вторичных систем можно разделить по группам:

1. Функции релейной защиты (РЗ);
2. Функции автоматики АПВ и УРОВ (А);
3. Функции управления и мониторинга выключателя (УМВ);
4. Функции управления коммутационными аппаратами (разъединители, заземляющие ножи) и оперативной блокировки (КА/ОБ);
5. Функции измерения для контроля технологического процесса защищаемого первичного оборудования (ИЗМ).

В первую группу РЗ входит весь необходимый набор основных и резервных защит, который зависит от типа защищаемого присоединения (линия, трансформатор, автотрансформатор, шины, ошиновка и т.д.). Во вторую группу А входят АПВ (ТАПВ, ОАПВ) и УРОВ, которые запускаются при работе функций РЗ присоединения и самостоятельно воздействуют на конкретный выключатель защищаемого присоединения или выключатели смежных присоединений. В третью группу УМВ входят функции оперативного управления конкретным выключателем защищаемого присоединения как от автоматизированного рабочего места оперативного персонала АСУ ТП (АРМ ОП АСУ ТП), так и «по месту» (с лицевой панели терминала). Здесь же выполняется контроль положения выключателя и состояния его привода управления (контроль цепей соленоидов управления, контроль готовности, исправности привода, контроль плотности элегаза и т.д.). Функции, входящие в четвертую группу КА/ОБ, реализуют управление разъединителями, заземляющими ножами и оперативную блокировку ячейки выключателя, логично привязываются к конкретному выключателю. Пятая группа ИЗМ выполняет измерение в классе 0,5 (0,2) электрических величин I, U, f, P, Q защищаемого присоединения, логично привязывается к защищаемому присоединению. При наличии у защищаемого присоединения только одного выключателя может быть включена на трансформатор тока (ТТ) этого выключателя.

Предлагаемые в настоящей статье решения дают возможность реализовать функции всех пяти групп присоединения всего на двух устройствах (терминалах), предусматривают полное дублирование всех основных функций РЗ и А. Функции РЗ присоединения и функции А всех выключателей присоединения всегда реализуются вместе в одном устройстве. Релейная защита взаимодействует только со своей автоматикой всех выключателей присоединения. Таким образом, функции АПВ и УРОВ всегда дублируются, при этом практически полностью отсутствуют «поперечные» связи.

Построение комплекса РЗА и распределение функций по устройствам зависит от типа распределительного устройства, в котором располагается защищаемое присоединение. В комплектных распределительных устройствах с элегазовой изоляцией (КРУЭ) в шкафах местного управления ячейкой (ШМУ), в настоящее время, как правило, устанавливаются микропроцессорные устройства – контроллеры управления. Именно в них предлагается выполнять функции управления и мониторинга выключателя ячейки (УМВ), функции управления коммутационными аппаратами и оперативную блокировку ячейки (КА/ОБ), а также функции измерения (ИЗМ) без резервирования. Все остальные функции РЗ и А реализуются с полным дублированием в терминалах РЗА, которые устанавливаются в помещениях релейных залов. Такие устройства РЗА обеспечиваются необходимым количеством дискретных входов/выходов для независимой реализации функций автоматики всех выключателей защищаемого присоединения. Если проектом предусматривается установка микропроцессорного устройства – контроллера управления ячейкой в шкафу управления выключателем на ОРУ (с обеспечением микроклимата и надёжного питания), распределение групп функций по устройствам выполняется так же, как и для КРУЭ. Если, по соображениям надёжности, такой контроллер на ОРУ не устанавливается, то функции УМВ, КА/ОБ и ИЗМ добавляются к терминалам РЗА в ОПУ за счет расширения аппаратной части модульной конструкции. Далее приводятся схемы распределения функций вторичных систем при использовании терминалов РЗА без отдельных контроллеров управления.

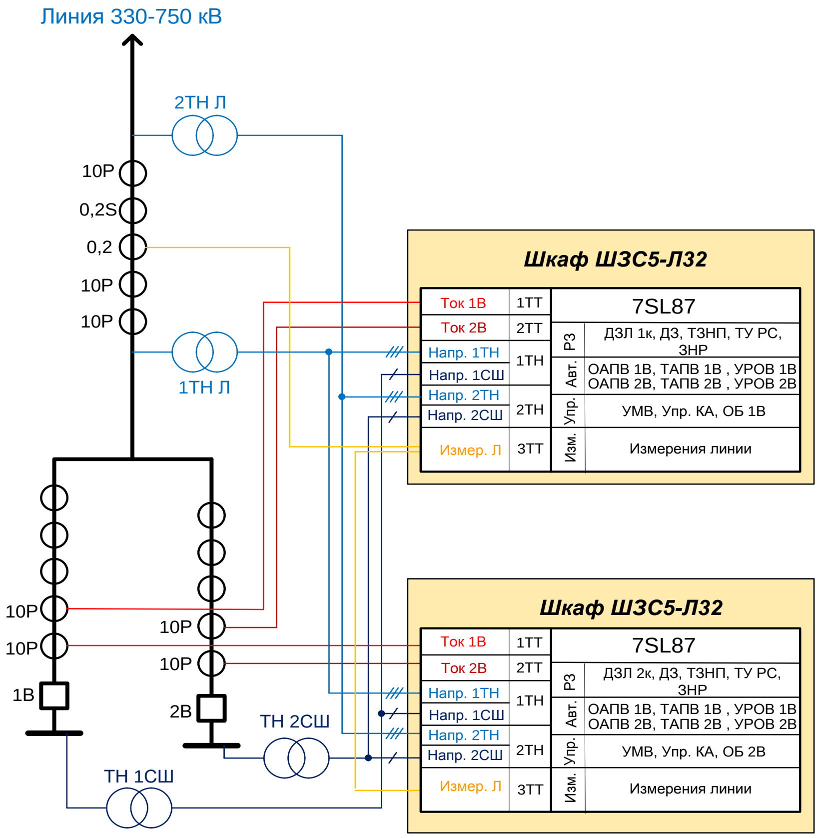


Рис. 1: Схема распределения функций вторичных систем линии 330-750 кВ.

В схеме на Рис. 1 показано распределение функций вторичных систем для линий 330-750 кВ при отсутствии отдельных контроллеров управления ячейками в шкафах управления выключателями. Каждый терминал установлен в отдельный шкаф, терминалы и шкафы абсолютно идентичны по всем параметрам. Все функции релейной защиты РЗ, автоматики А и измерений ИЗМ дублируются, кроме УМВ и КА/ОБ, которые для первого выключателя выполняются в первом терминале, для второго выключателя – во втором терминале. Устройства Siprotec 5 также позволяют выполнять автоматическое резервирование (переключение) цепей напряжения в самом терминале. Для реализации необходимого алгоритма переключения цепей напряжения используется свободно программируемая логика.

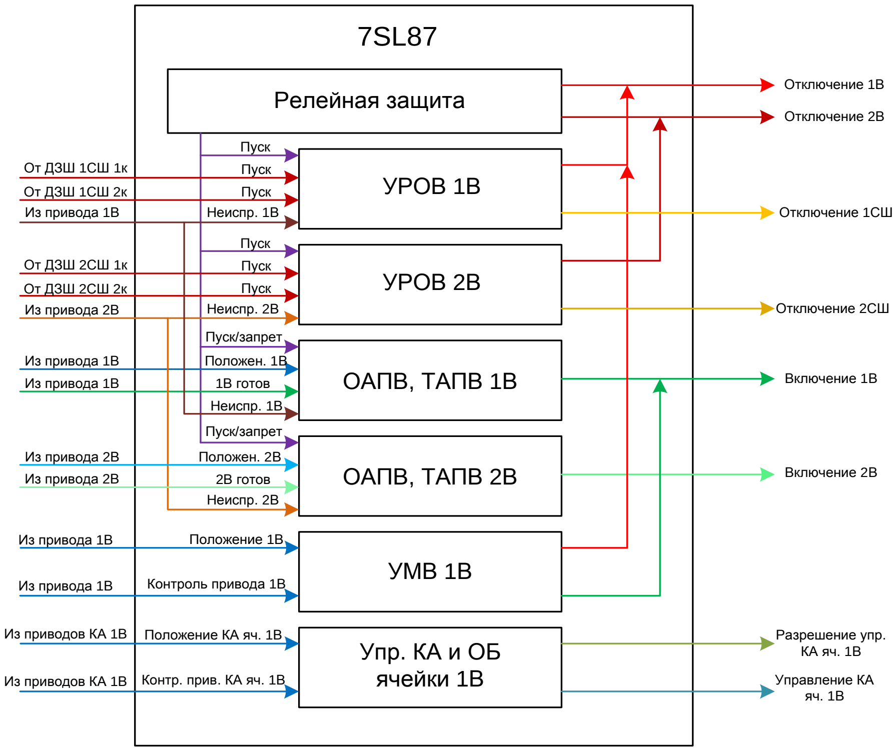


Рис. 2: Схема взаимодействия функций внутри терминала и с внешними устройствами.

В схеме на Рис. 2 показано взаимодействие функций внутри терминала и с внешними устройствами. Схема приведена для одного терминала, схема второго терминала полностью соответствует приведённой за исключением того, что два последних функциональных блока реализуют УМВ 2В и КА/ОБ ячейки 2В. Все функции релейной защиты РЗ полностью дублируются, функции автоматики А (ОАПВ, ТАПВ со всеми видами контролей отсутствия/наличия напряжения/синхронизма/улавливания синхронизма и УРОВ) также дублируются для обоих выключателей. Обмен сигналами между функциями РЗ и автоматики А всего защищаемого присоединения выполняется внутри терминала. Для исключения потерь функций автоматики присоединения (АПВ и УРОВ) в каждый терминал дискретными сигналами по «меди» из приводов выключателей заводится информация о положении обоих выключателей, готовности и состоянии их приводов (4 сигнала для каждого выключателя присоединений, не оборудованных ОАПВ и 8 сигналов для каждого выключателя присоединений, оборудованных ОАПВ). При выводе из работы по каким-либо причинам одного из терминалов все функции РЗ и А для обоих выключателей присоединения сохраняются в полном объёме, теряется только возможность управления с АРМ ОП АСУ ТП одним из выключателей и управление коммутационными аппаратами его ячейки. На этот случай предусмотрена возможность «местного» (функция автоматики исправного терминала) управления этим выключателем.

При построении комплексов РЗА для трансформаторов и автотрансформаторов используются те же принципы, однако здесь имеются некоторые отличия.

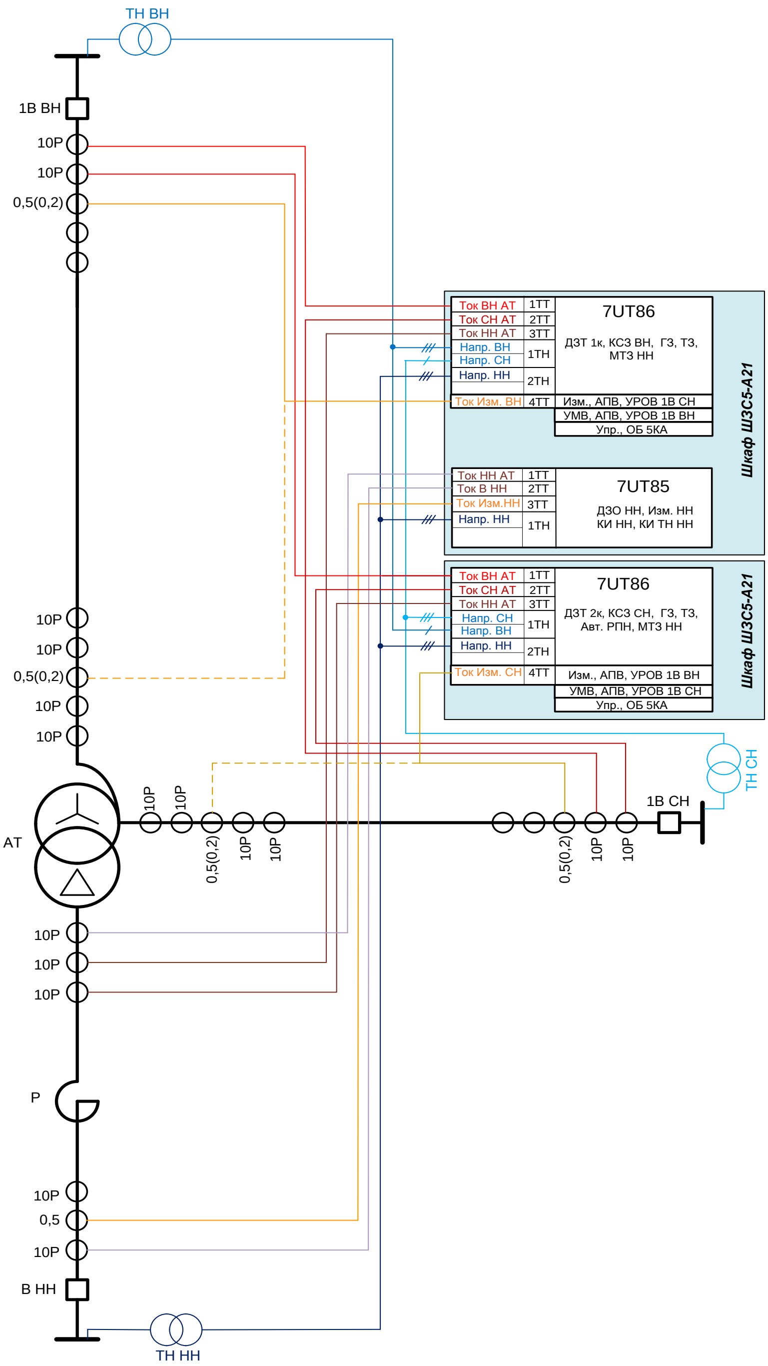


Рис. 3: Схема распределения функций вторичных систем автотрансформатора 220/110 кВ.

В схеме на Рис. 3 показано распределение функций вторичных систем для автотрансформатора 220/110 кВ при отсутствии отдельных контроллеров управления в шкафах управления выключателями 110, 220 кВ. Все основные функции релейной защиты РЗ и автоматики А здесь также всегда дублируются, даже если отсутствует требование к дублированию дифференциальной защиты автотрансформатора (ДЗТ). В первом терминале выполняются резервные защиты стороны ВН (ДЗ и ТЗНП), во втором терминале – резервные защиты стороны СН. Терминалы 7UT86, в которых реализуются основные функции релейной защиты РЗ и автоматики А, по набору функций не полностью идентичны. Во втором терминале дополнительно реализуется функция автоматического регулирования напряжения (управления устройством РПН) автотрансформатора. В первом шкафу устанавливается, вместе с терминалом 7UT86, второй терминал, реализующий функции дифференциальной защиты ошиновки низкого напряжения (ДЗО НН), контроля изоляции ошиновки низкого напряжения АТ (КИ НН), контроля исправности цепей трансформатора напряжения стороны низкого напряжения (КИ ТН НН), измерения стороны НН автотрансформатора.

При подключении трансформатора, автотрансформатора по сторонам ВН и/или СН через два выключателя функции автоматики (АПВ, УРОВ), УМВ, КА/ОБ соответствующих выключателей из терминалов основных защит переносятся в терминалы дифференциальной защиты ошиновки соответствующей стороны (ДЗО ВН, ДЗО СН), которые имеют токовые цепи соответствующих выключателей. Терминалы релейной защиты трансформаторов и автотрансформаторов при этом реализуют только функции РЗ, а каждый терминал релейной защиты ошиновки помимо функций РЗ реализует также функции автоматики (АПВ и УРОВ) обоих выключателей, функции УМВ, КА/ОБ и ИЗМ контролируемой ячейки. Функции АПВ и УРОВ также дублируются в обоих терминалах ДЗО соответствующей стороны для обоих выключателей.

Предлагаемое построение комплексов РЗА линий, трансформаторов и автотрансформаторов автоматически решает проблемы с обеспечением разных режимов работы АПВ и УРОВ среднего выключателя полуторной схемы при отключении этого выключателя от защит прилегающих присоединений.

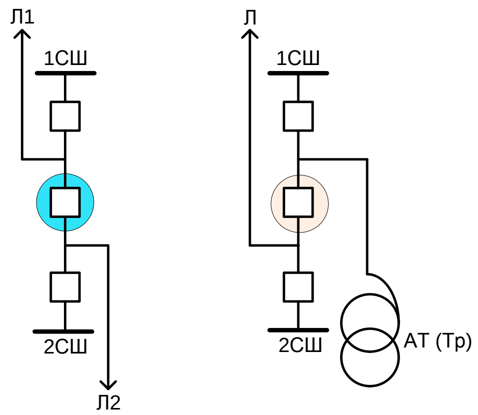


Рис. 4: Подключение присоединений в полуторной схеме.

Функции АПВ имеются в каждом из двух терминалов РЗА обоих присоединений, на средний выключатель, который является общим для этих присоединений, воздействуют независимые функции АПВ обоих присоединений. Алгоритм работы АПВ среднего выключателя зависит от того, защиты какого присоединения отключали выключатель. Так как АПВ каждого присоединения запускается/блокируется только от защит своего присоединения, очень просто решается вопрос обеспечения разных режимов работы АПВ по условиям контроля напряжения/синхронизма, выдержке времени бестоковой паузы, по виду (ОАПВ или ТАПВ) при работе защит смежных присоединений для общего для них выключателя. УРОВ среднего выключателя так же имеется в каждом смежном присоединении. Пуск УРОВ каждого присоединения так же выполняется только от защит своего присоединения, что позволяет выбирать разные уставки по току контроля для УРОВ линии и УРОВ Т, АТ, обеспечивая отстройку от ёмкостного тока в УРОВ линии и необходимую чувствительность УРОВ защит Т, АТ при КЗ за токоограничивающим реактором стороны НН.

3 ЗАКЛЮЧЕНИЕ

Предлагаемая идеология построения систем РЗА на мощных многофункциональных микропроцессорных устройствах позволяет реализовать функции вторичных систем различных присоединений всего на двух одинаковых терминалах, установленных в двух независимых шкафах, и дает следующие преимущества:

- сокращается стоимость вторичных систем;
- сокращается эксплуатационные затраты на содержание таких систем;

- сокращается площадь помещений, необходимых для размещения комплексов РЗА;
- сокращается стоимость сооружения помещений для оборудования РЗА;
- сокращаются эксплуатационные затраты на содержание этих помещений в течение длительного срока эксплуатации;
- полное дублирование основных функций РЗ и автоматики (АПВ, УРОВ) повышает надёжность функционирования всего вторичного комплекса и исключает возможность введения различных режимных ограничений в прилегающей сети при выводе из работы по каким-либо причинам одного из терминалов;
- обеспечивается удобство вывода одного комплекта из работ для технического обслуживания и тестирования, при этом функции РЗ могут быть протестированы вместе с функциями автоматики;
- однотипность комплектов упрощает их техническое обслуживание;
- основной и значимый для функционирования обмен информацией между отдельными функциями РЗ и автоматики выполняется внутри терминалов без использования «поперечных» связей между терминалами, что повышает надёжность и упрощает эксплуатационное обслуживание;
- в полуторных схемах подключения присоединений просто и логично обеспечивается реализация разных алгоритмов работы АПВ, возможность выбора разных уставок по току контроля УРОВ среднего выключателя при действии защит смежных присоединений;
- из-за отсутствия «поперечных» связей между дублирующими комплектами, второй (дублирующий) комплект вторичных систем можно выполнить на устройстве другого производителя;
- при выполнении функций управления и мониторинга выключателя, управления коммутационными аппаратами, оперативной блокировки на «полевом» уровне в шкафах местного управления (ШМУ) КРУЭ или в шкафах управления (ШУ) на ОРУ, они могут быть реализованы даже на оборудовании третьего производителя.

ЛИТЕРАТУРА

[1] Siprotec 5. Distance Protection, Line Differential Protection and Breaker Management for 1-Pole and 3-Pole Tripping // Manual, SIEMENS AG.

[2] Siprotec 5. Transformer Differential Protection // Manual, SIEMENS AG.