Scientific Papers of
the Institute of Electrical Power Engineering of
the Wrocław University of Technology

PRESENT PROBLEMS OF POWER SYSTEM CONTROL

5

Wrocław 2014

Cover design
Piotr PIERZ

Printed in the camera ready form

Institute of Electrical Power Engineering
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
phone: +48 71 320 26 55, fax: +48 71 320 26 56
www: http://www.ie.pwr.wroc.pl/; e-mail: Inst.Energ@pwr.wroc.pl

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
http://www.oficyna.pwr.wroc.pl
e-mail: oficwyd@pwr.edu.pl
zamawianie.ksiazek@pwr.edu.pl

ISSN 2084-2201

Druk i oprawa: EXPOL, P. Rybiński, J. Dąbek, sp.j., ul. Brzeska 4, 87-800 Włocławek
tel. 54 232 37 23, e-mail: sekretariat@expol.home.pl

CONTENTS

microprocessor-based relays,
bus configurations,
bus protection

Casper LABUSCHAGNE*, Normann FISCHER*,
Bogdan KASZTENNY*

SIMPLIFYING AND IMPROVING PROTECTION OF TEMPORARY AND UNUSUAL BUS CONFIGURATIONS WITH MICROPROCESSOR-BASED RELAYS

Breaker substitution, stub bus, and station bypass are temporary substation configurations used to facilitate the maintenance of primary equipment while keeping assets in service and supplying loads. These configurations provide considerable operational advantages but create challenges for protection systems.

Traditional solutions to temporary bus configurations required for electromechanical relays utilize test and bypass switches to ensure the affected relays are provided with the appropriate currents and voltages and the trip signals are routed to the appropriate breakers. In some cases, spare relays, settings changes, and the rerouting of pilot signals and communications have been required. All these manual operations increase the danger of misoperation when making changes, during temporary configurations, or when restoring to the normal configuration. As a result, temporary bus configurations have been carefully considered and often avoided, resulting in underutilization of the network assets.

This paper shows how modern microprocessor-based relays can simplify applications under temporary bus configurations, eliminate the need for any manual reconfiguration, and improve the performance of protection. These benefits stem from the ability to connect multiple current and voltage inputs, the ability to trip multiple breakers, communication between relays, and programmable logic, allowing automatic detection and dynamic response to temporary bus configurations.

1. INTRODUCTION

The current Breaker substitution, also known as breaker transfer, is the temporary usage of a bus coupler in a multiple-bus configuration to substitute for one of the network element circuit breakers, typically for the maintenance of the circuit breaker. The substituted breaker is isolated via disconnect switches and bypassed by the bypass switch to

* Schweitzer Engineering Laboratories, Inc.

connect the network element to the transfer bus, while the transfer bus is energized via the bus coupler. As a result, during breaker substitution, both the bus protection scheme and the network element protection scheme must adapt accordingly.

Stub bus refers to an area of a bus or line that becomes isolated from the original zone of protection, typically by an opened disconnect switch. A typical stub bus scenario occurs in a ring-bus or breaker-and-a-half configuration when a transmission line is isolated via an opened disconnect switch but both line breakers are closed to maintain the integrity of the bus. At the same time, the line may be energized, feeding tapped loads or transferring power between the other two terminals of a three-terminal line. This case also requires both the bus protection scheme and the line protection scheme to adapt accordingly.

Station bypass refers to a situation when two lines of the same voltage level that normally terminate on a bus are isolated from the bus but tied together temporarily via a disconnect switch. Such a configuration changes two lines that are normally protected as individual zones by two protection schemes into a single line protected from both remote terminals, while the local station is effectively bypassed. Depending on the location of the current transformers (CTs), the bus relay may need to adapt to this configuration. More importantly, the two line protection schemes need to be reconfigured to effectively form a single scheme.

During unusual and temporary bus configurations, the breaker failure initiate or trip signals must be rerouted accordingly as well. This is a consequence of tripping circuit breakers that are different than normal upon detecting an in-zone fault. This paper reviews protection challenges and typical solutions related to temporary bus configurations.

2. BREAKER SUBSTITUTION

2.1. BUS SWITCHING SEQUENCES

Consider the double-bus, single-breaker configuration in Fig. 1. Normally, network elements (NEs), such as feeders, transformers, and so on, are connected to either Bus 1 or Bus 2 via disconnect switches, while the bus coupler (BC) is either opened or closed, depending on the preferences related to fault current levels and the selectivity of bus protection. A given network element can be transferred from one bus to another by disconnect switches. Furthermore, one of the two buses can be used as a transfer bus to facilitate breaker substitution. In this switching scenario, the bus coupler is closed first. Then all network elements except for the network element to be transferred are switched to one of the two buses (assume this is Bus 2), while the transferred network element (assume this is NE1) is switched to the trans-

fer bus (Bus 1). Subsequently, the corresponding bypass switch (BP1) is closed. Next, the transferred breaker (CB1) is opened and then isolated by its disconnect switches. At this point, the transfer is complete and the transferred breaker is available for maintenance.

The bus coupler therefore takes over the role of the network element breaker, and the zone of protection now includes the transfer bus and extends to the bus coupler CT opposite to the transfer bus (CTB1 in this example).

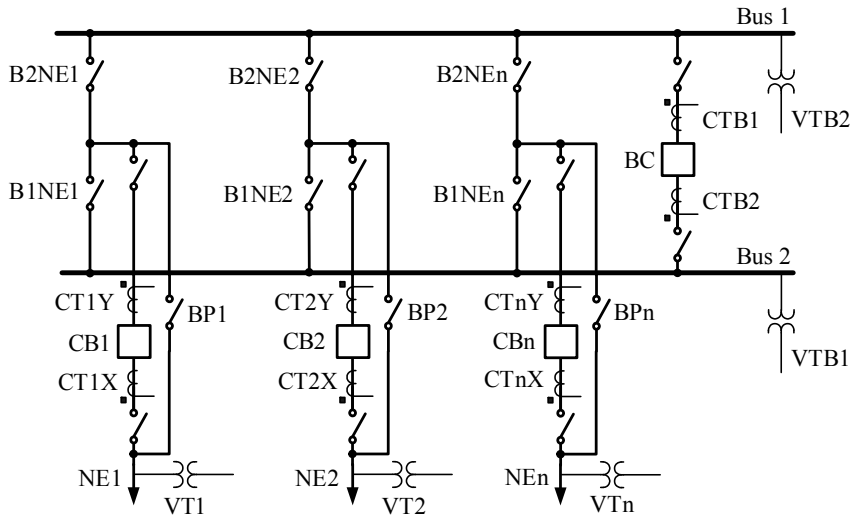


Fig. 1. Double-bus, single-breaker busbar configuration

2.2. BUS PROTECTION CHALLENGES AND SOLUTIONS

Long To protect the two buses shown in Fig. 1 selectively, the bus protection scheme is required to support at least two bus zones (i.e., two independent differential protection elements). The bus protection scheme uses current from the equipment-side CTs (CT1X…CTnX) and current from the bus coupler CTs (CTB1 and CTB2). The auxiliary contacts of the disconnect switches are used to determine which currents to include in which bus zone.

In general, a bus zone is formed by the bus coupler CT opposite to the protected bus and the equipment-side CTs of the equipment connected to that bus. With none of the disconnect switches closed, the Bus 1 protection zone is bounded by the bus coupler CT opposite to Bus 1 (CTB1), and the Bus 2 protection zone is bounded by CTB2, as shown in Fig. 2. This is known as an overlap bus coupler configuration. When a network equipment disconnect switch is closed onto Bus 1 or Bus 2, then that piece of network equipment is included in that protection zone and its CT currents are included in the bus differential element.

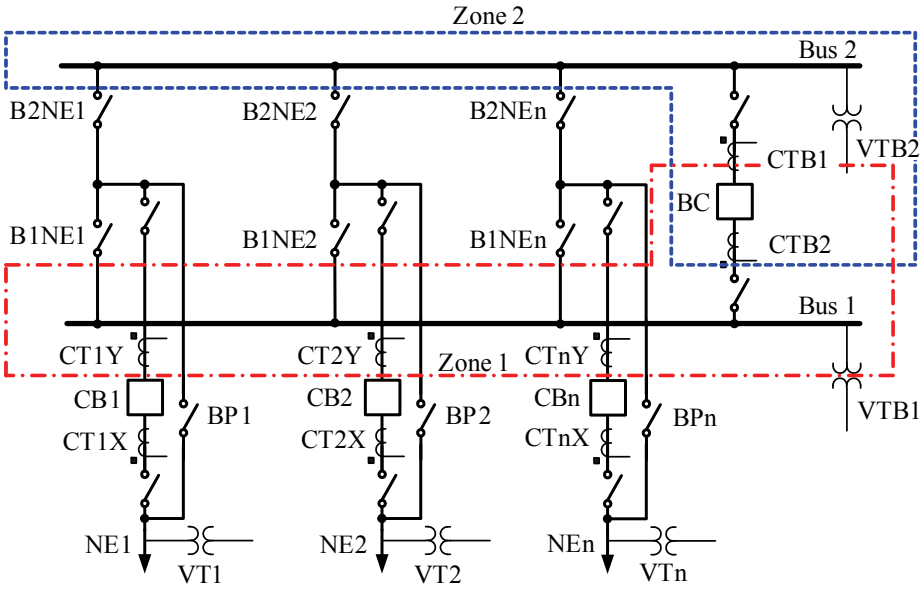


Fig. 2. Double-bus, single-breaker busbar configuration showing the individual bus protection zones

When a bus fault occurs, the bus zone protection element in the zone in which the fault occurred sends a trip signal to all the network element breakers connected to the faulted bus.

Depending on the status of the bus coupler (i.e., open or closed), a trip signal is also routed to the bus coupler.

For a breaker failure, the bus protection scheme trips the entire bus to which the failed breaker is connected at the time and the bus coupler, in a similar way as for a bus fault.

The first challenge for bus protection is when a network element is transferred from one bus to the other. For example, assume that NE1 is to be transferred from Bus 1 to Bus 2. Initially, the B1NE1 disconnect switch is closed and the B2NE1 disconnect switch is open. To begin the transfer process, B2NE1 is closed, both B1NE1 and B2NE1 are closed, and then B1NE1 is opened. When both B1NE1 and B2NE1 are closed, the two buses are paralleled. While the bus protection scheme measures the total current in the transferred NE1 (via CT1X), it does not know how this current splits between the two buses. Therefore, the two zones of bus protection cannot be protected individually (selectively). Instead, the entire bus is protected by a single bus differential element using all the CTs that bound the two buses (CT1X…CTnX) but excluding the CTs internal to the bus (CTB1 and CTB2).

The bus protection system monitors the position of the disconnect switches and assigns currents to the corresponding bus-zone relay elements. However, there may be

a time lag between the change in the disconnect switch status and the current flow in the power system. This time lag can result in a temporary unbalance of the differential elements and an unexpected bus protection operation. To guard against this, an undervoltage supervision element is applied to the bus zone. Therefore, before a bus differential scheme issues a trip signal to the breaker connected to the bus zone, the following two conditions have to be met:

- The differential element must indicate an internal bus fault.
- The phase undervoltage element must indicate an undervoltage condition.

This two-out-of-two trip requirement prevents the protection scheme from operating during a transfer procedure.

Previously, it was mentioned that the bus coupler CTs are excluded when the two buses are in parallel. If the bus coupler CTs are not excluded, the sensitivity of the bus protection scheme is decreased. The reason for this is that the differential element will overrestrain, or even block, due to a current circulating via the bus coupler during a bus fault. Should the fault be a high-resistance fault, the dependability of the relay may be compromised.

Another solution to prevent an undesired bus-zone operation during a transfer operation is to use a check zone, a supervisory differential zone made up of the currents of all the network elements connected to all the buses but excluding the bus coupler element. Generally, this zone is static and does not use the information of the disconnect switches to assign network elements to a zone of protection. For this example, the check zone is composed of all the equipment-side CTs, namely CT1X…CTnX, as shown in Fig. 3. In this case, before the bus protection scheme can issue a trip, both the faulted bus-zone protection element and the check zone must indicate the presence of an internal bus fault. Again, a two-out-of-two condition must be met before a bus trip is issued.

What is interesting about the configuration of the check zone is that it is identical to the differential zone for the case when the two buses are paralleled.

The second challenge for bus protection is when the bypass switch is closed as a part of the breaker substitution sequence while the breaker being substituted is still carrying current. Assume that NE1 is connected to Bus 1, all the other network elements are supplied from Bus 2, and the bus coupler is closed. When BP1 is closed, CT1X does not measure the total current flowing into Bus 1 via B1NE1 anymore, as shown in Fig. 4. It measures an unknown portion of this current splitting between the two parallel branches (CB1 and BP1). At this time, Bus 1 cannot be protected with a differential principle because it lacks current measurement in the B1NE1 path. Upon detecting the closing of a bypass switch, the bus protection system inhibits the corresponding bus protection zone. BP1 inhibits Bus Zone 1 in this case.

Again, a time lag can occur between detecting the status of BP1 and the current redistribution in CT1X, and this can lead to misoperation. In this case, a check zone is not effective because it uses the same current CT as the bus zone, namely CT1X.

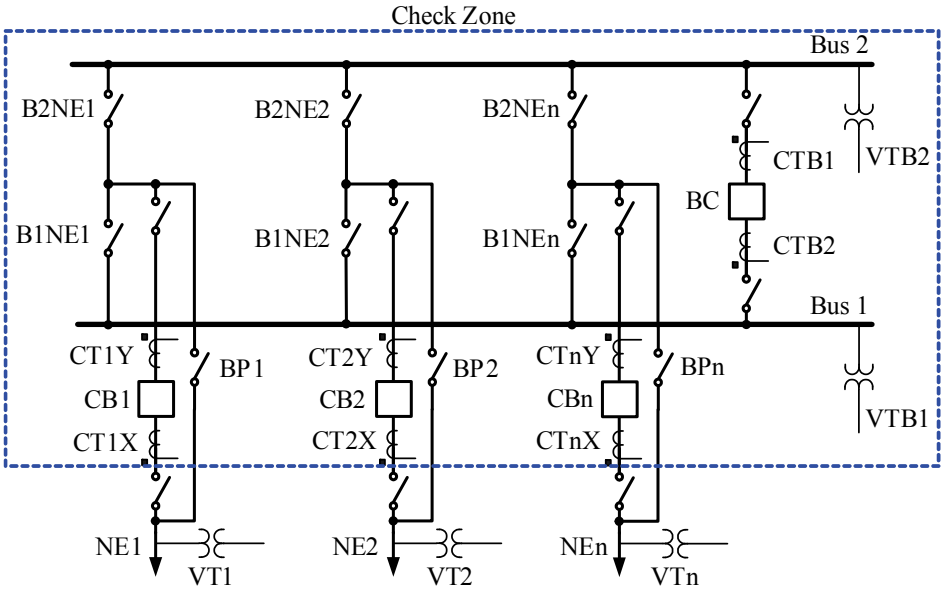


Fig. 3. Check zone for a double-bus, single-breaker busbar arrangement

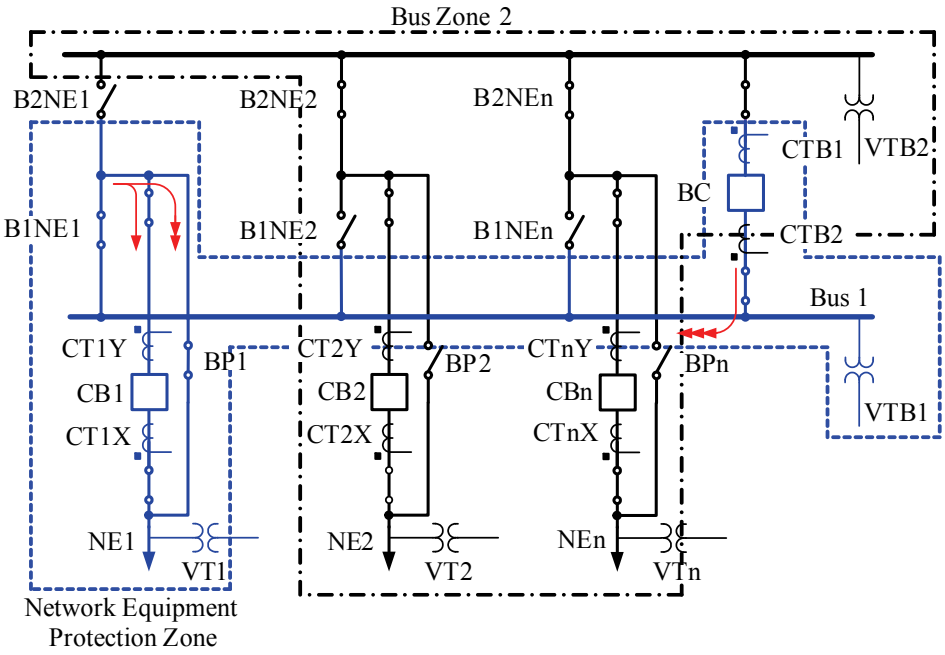


Fig. 4. Distribution of the current between the line CT (CT1X) and the bypass switch and desired protection zones when the bypass disconnect switch is closed

However, undervoltage trip supervision (VTB1) will work to secure the bus protection scheme in this instance.

After the breaker substitution switching procedure, Bus 2 is protected with differential protection and Bus 1 is protected as a part of the NE1 protection zone, which is explained in the next subsection.

If voltage supervision is not available and a check zone option is the only available option, the bus coupler CT (CTB1) needs to substitute the network equipment CT (CT1X) in order to balance the check zone. Although this dynamic adjustment of the check zone makes the check zone dependent on the disconnect auxiliary contacts, it does so only during bypass operations.

2.3. NETWORK ELEMENT PROTECTION CHALLENGES AND SOLUTIONS

Normally, the protection of network equipment uses bus-side CTs (CTnY) and equipment-side voltage transformers (VTs), and the zone of protection overlaps with that of the bus zone at the circuit breaker (CBn). Breaker substitution affects the protection of the network element. With the bypass switch (BPn) closed, the bus-side CTs no longer measure the total current of the network equipment. As a result, the network equipment protection must be switched from the bus-side CTs to the bus coupler CTs (CTB1 or CTB2). By doing this, the network protection not only includes the network equipment but also the bus to which the network equipment is connected during the breaker substitution temporary bus configuration. Depending on the location of the VT, the network protection relay may need to switch from the equipment-side VT (VTn) to the bus VT (VTB1 or VTB2).

Switching the protection current measurement and trip paths from the regular breaker to the bus coupler breaker can be achieved in several ways. Assume the transferred NE is a line.

One solution is to use the same line relay but to transfer the required signal from the bus coupler to the line relay. This method makes use of a set of external auxiliary relays that switch the bus coupler CT, breaker I/O contacts, breaker failure initiate signal, and, if required, the bus VT to the network equipment relay. Figure 5 is a simple sketch of this solution for a breaker substitution.

When the piece of network equipment is placed in the transfer mode, the auxiliary relays are energized and the network equipment relay is supplied by the bus coupler CTs, VTs, and the I/O from the bus coupler breaker. The interlocking in this instance is such that only one piece of network equipment can be placed in transfer mode at a time. This solution requires that the CT auxiliary relays be capable of switching and carrying the full load current of the CTs, as well as fault current.

Advantages of this scheme are that relay settings do not need to be altered during a transfer and the communications signals or channels do not require rerouting. A further benefit of this scheme is that it does not really matter what type of network equipment (feeder, transformer, and so on) is being placed on transfer.

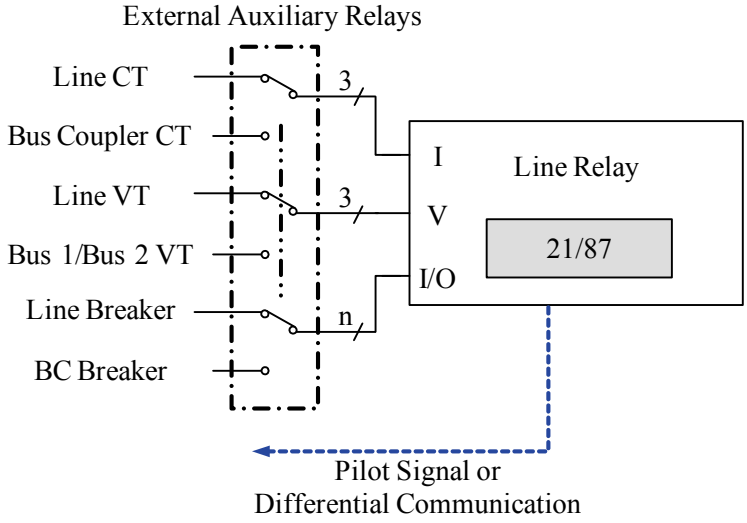


Fig. 5. Breaker substitution scheme where auxiliary relays
are used to route the coupler currents and voltages to the network equipment relay

A disadvantage of this scheme is that it is expensive (cost of the auxiliary relays and scheme engineering). This scheme has a moderate level of complexity, and because the transfer process is done manually, it is prone to human errors. Also, the existence of switching devices in the ac and dc wiring lowers the overall reliability of the scheme and creates safety concerns, especially in relation to switching the CT secondary currents.

A second solution for breaker substitution is to use a spare relay, known as a transfer relay, at the bus coupler. This relay is wired to the bus coupler CTs and VTs (if required) and the I/O of the bus coupler breaker. This relay is configured prior to substitution to protect different pieces of network equipment connected to the buses.

When a network element is placed on transfer, then the transfer permission switch from the breaker being substituted initiates an alternate settings group in the transfer relay. This solution requires the communications signals, whether those of a communications-aided tripping scheme or a differential scheme, to be rerouted. A realization of this scheme is sketched in Fig. 6.

This scheme has several drawbacks in that the number of breakers that can be substituted is limited by the number of settings groups available in the transfer relay. Furthermore, this scheme requires a transfer relay for each different piece of network equipment connected to the bus. For example, if a shunt capacitor bank breaker were to be substituted, the transfer relay would need to be capable of providing shunt capacitor bank protection. Even though this approach may work well for line and shunt capacitor banks, it cannot be used when the substituted breaker is a transformer high- or low-side breaker. Owing to these shortcomings, this scheme is not as popular as the previous scheme.

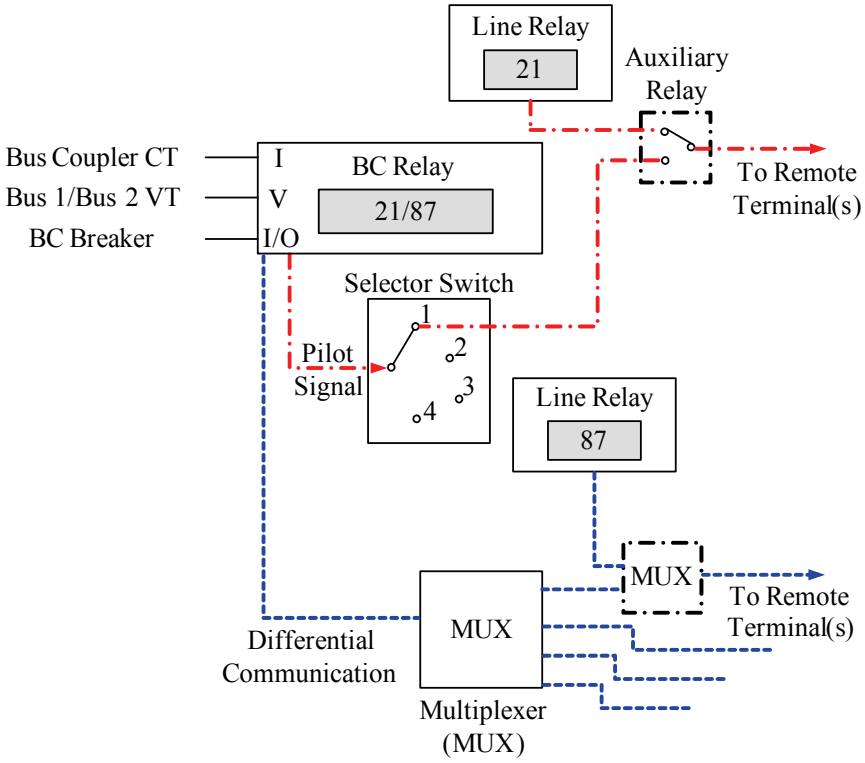


Fig. 6. Breaker substitution scheme in which a transfer relay is used at the bus coupler. This scheme requires the communications channels to be switched

Generally, utilities standardize on one bus to be used as the transfer bus to decrease the errors associated with breaker substitution. This leads to a third and better solution than the two methods described previously in that each new network element has a multi-input microprocessor-based relay with the programmability to internally switch its protection functions from one set of inputs and outputs to another set.

For our example two-bus system, assume that Bus 1 is selected as the transfer bus. This means that both the network equipment bus-side CTs and the bus coupler CTs (in this example, CTB1) are permanently connected to the relay. In addition, both the network equipment breaker I/O and the bus coupler I/O are connected to the protective relay. A sketch of this solution is shown in Fig. 7.

Similar to the first solution, communications signals are not required to switch and the relay does not need to change any settings because it continues to protect the same network element. The relay monitors the position of the bypass switch (BP1) and selects the correct voltages, current, and breaker I/O contacts to use.

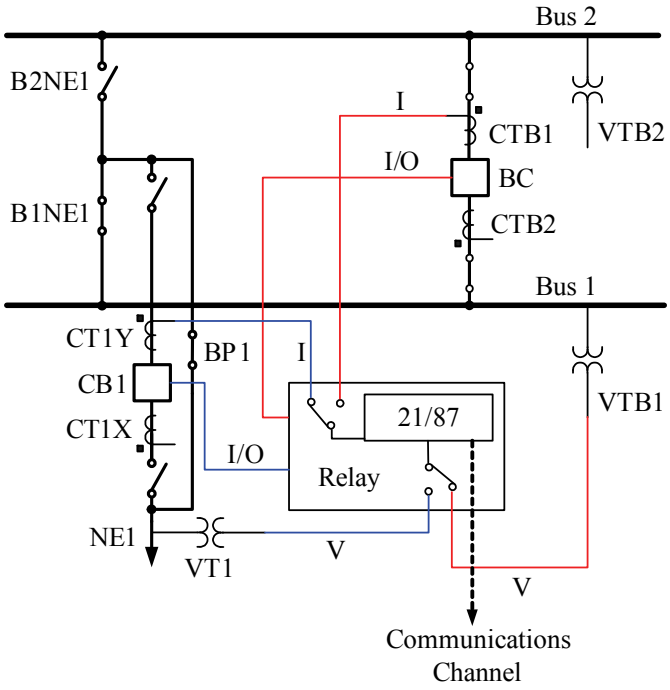


Fig. 7. Breaker substitution scheme using a modern relay
with multiple VT and CT input terminals to facilitate breaker substitution.
The relay selects the appropriate analog and digital quantities internally

Again, a time lag can occur between the current redistribution and the status of the bypass switch. Undervoltage trip supervision is sufficient to prevent misoperation. If required, the relay can measure both VT1 and VTB1 and switch to the bus voltage if VT1 does not represent the network element voltage during the substitution.

Of all the solutions presented here, the third is the preferred solution because of its simplicity and avoidance of any external auxiliary relays and manual reconfiguration requirements. The third solution does not require any manual reconfiguration, thereby eliminating any possible errors during a breaker substitution.

2.4. BREAKER FAILURE CONSIDERATIONS

In a dynamic bus configuration, breaker failure trip signals must be routed based on the present bus connection in order to isolate the fault despite the failed breaker, while, at the same time, not tripping breakers not contributing directly to the fault. In complex bus arrangements, the bus protection scheme is responsible for routing any

bus or breaker failure trip signals because it has access to the status of all disconnect switches and breakers. When breakers are correctly assigned to bus protection zones for all the possible dynamic conditions, breaker failure tripping is straightforward in order to isolate a fault, the bus system must trip the entire bus to which the failed breaker is presently connected (i.e., trip all breakers presently connected to the same bus).

The same rule applies to the breaker substitution situation as well. Using the dual-bus system shown in Fig. 7 as an example, if the bus coupler breaker fails for an NE1 fault while the bus coupler is substituting the network equipment breaker, the bus protection scheme needs to clear Bus 2. In this situation, both buses are cleared and all the network elements are disconnected, unlike during normal operation when a breaker failure clears only one of the two buses. This is a reason to limit the duration of the breaker substitution temporary bus configuration.

In addition to clearing Bus 2, the bus protection scheme must initiate a direct transfer trip (DTT) to all breakers of the NE1 zone (the breaker(s) of the element being substituted). If NE1 is a power line, this can be done by using the NE1 relay to send a DTT to all remote terminals of the NE1 line.

3. STUB BUS CONFIGURATION

Stub bus configuration typically applies to double-breaker connections of network elements. Figure 8 shows a network element connected via two breakers (ring-bus, breaker-and-a-half, or double-bus, double-breaker bus configurations). Stub bus refers to a condition when the network element disconnect switch is opened but the two breakers remain closed in order to maintain the integrity of the bus. At the same time, the network element may remain energized or even serve loads (three-winding transformer, three-terminal line, or tapped line). The opened disconnect switch effectively breaks the original zone of network element protection into two zones. This can cause both selectivity and dependability problems, such as the following:

- The area between the two breakers and the opened disconnect switch (stub bus) needs protection, and the network element protection may lose the ability to protect this area properly.
- The network element should not be tripped for faults within the stub bus.
- The network element must be protected properly, despite the opened disconnect switch.
- Tripping the network element should not include the breakers of the stub bus.
- Breaker failure trips need to be routed to the appropriate breakers.

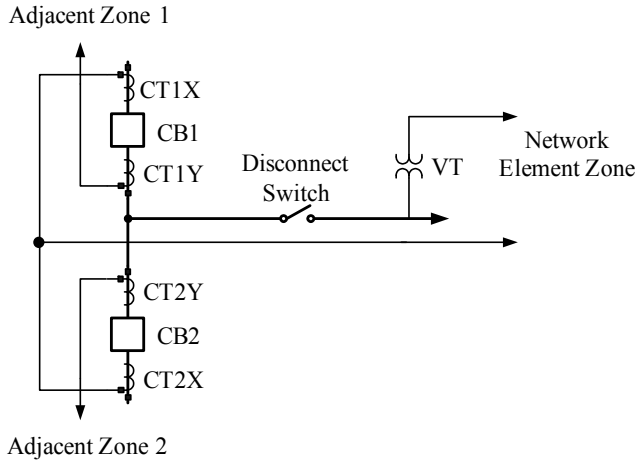


Fig. 8. Stub bus configuration

3.1. SECURITY OF DETECTING THE STUB BUS CONDITION

The stub bus condition is detected based on the position of the disconnect switch. Because protection logic changes considerably in response to the stub bus condition, the stub bus signal must be very reliable. Typically, a spurious assertion of the stub bus logic will cause a false trip. At the same time, the auxiliary contacts of the disconnect switches are known for their relatively poor performance. As a result, it is customary to use both the 89a and 89b contacts when sensing the position and apply discrepancy logic to send an alarm with the intent to rectify any problems [1] [2].

3.2. IMPACT ON BUS PROTECTION

The bus protection system can be used to provide stub bus protection. Assume that Adjacent Zone 1 in Fig. 8 is the bus protection zone. Normally, the bus protection scheme would use CT1Y to terminate its zone of protection at the CB1 breaker. Under the stub bus condition, the bus scheme can dynamically switch from CT1Y to CT2X. This way, the bus zone includes the stub bus. Of course, this operation is convenient when using a low-impedance microprocessor-based bus relay, with both CT1Y and CT2X wired to the relay and switched internally via programmable logic in response to the position of the disconnect switch. However, this solution is not optimal from the point of view of selectivity faults within the stub bus will result in tripping the entire bus. One solution to this weakness is to initiate sequential tripping from the bus zone. First, CB1 and CB2 are tripped. If the bus differential element resets, the fault was in the stub bus area and therefore the other bus breakers are not tripped. If the bus differ-

ential element remains picked up, the fault must be truly on the bus and the entire bus is tripped. A slower bus fault clearing time is a disadvantage of the sequential tripping solution. Another solution is to enable a two-current differential zone within the bus protection scheme, utilizing just the CT1X and CT2X current measurements, and enable this zone under stub bus conditions. This, however, requires the bus relay to support extra zones of protection.

3.3. IMPACT ON NETWORK ELEMENT PROTECTION

The network element relay can be used to protect the stub bus. Typically, a simple instantaneous overcurrent element responding to the sum of the CT1X and CT2X currents or a differential element is used. This protection is enabled only under the stub bus condition. The differential element solution is more secure under CT saturation for close-in faults compared with a simple overcurrent element. When tripping from the stub bus protection, the network element relay trips only CB1 and CB2 and does not trip the other breakers of the network element.

In addition, the network element protection must continue to protect the network element. In this respect, the issues and solutions differ depending on the type of protection.

A. Transformer Protection (87T)

If the network element is a transformer with differential protection (87T), the stub bus is within the 87T zone of protection and therefore there are no concerns with dependability. However, if the transformer is to remain energized and to achieve selective operation, the CT1X and CT2X currents can be dynamically removed as inputs of the transformer differential element 87T upon a stub bus configuration. Some modern transformer relays allow such dynamic assignment of currents. When tripping from the 87T element, the relay should not open the CB1 and CB2 breakers. To complete this solution, the stub bus can be protected using a bus relay or an overcurrent element within the transformer relay responding to the sum of the CT1X and CT2X currents.

B. Line Distance Protection

Line distance protection does not work properly under stub bus conditions with the VT on the line side of the disconnect switch because the voltage and current measurements are taken in portions of the network that are separated by the opened line disconnect switch. When the VT is connected on the bus side of the line disconnect switch, distance protection protects the stub bus. When tripping from Distance Zone 1 under stub bus conditions in applications with bus-side VTs, ensure that no DTT signal is sent to the remote line breakers.

C. Directional Comparison Permissive Schemes

In order to properly protect the line under stub bus conditions, apply echo keying or permanently assert the permissive signal when the line disconnect switch is opened. This permissive signal allows the forward-looking overreaching elements at the remote terminal to trip instantaneously for all faults on the line.

D. Directional Comparison Blocking Schemes

Blocking schemes allow instantaneous tripping if no blocking signal is asserted. Therefore, blocking schemes work correctly under stub bus conditions without any modification.

E. Line Current Differential (87L) Protection

Because stub bus configurations are more often applied to lines rather than transformers, 87L relays typically provide for a built-in stub bus mode of operation. Upon a stub bus configuration, the following occurs:

- The local relay sends zeros as the value of the local current to the remote 87L relay (or relays). This way, the line differential zone of protection provided by the remote 87L relay (or relays) terminates at the opened disconnect switch.
- The local relay substitutes the received currents with zeros. This way, the local 87L zone becomes a stub bus differential zone and terminates at the opened disconnect switch (a differential element using just CT1X and CT2X).
- Received DTT signals are ignored at the terminal with the stub bus (they originate for line faults, and line faults are already isolated from the local terminal by the opened disconnect switch).
- When tripping from 87L under a stub bus condition, DTT signals are not sent to the remote 87L relays (these relays do not have knowledge of a local stub bus condition and cannot decide by themselves to execute or suppress any received DTT signals).
- Some other more sophisticated aspects of 87L operation can be designed into the stub bus configuration (examples are external fault detection or charging current compensation [3]).

F. Loss-of-Potential (LOP) Logic

In applications with line-side VTs, LOP logic that is based on the change of voltage and current can malfunction by sensing a change in the voltage due to faults while not seeing any change in the currents because of the opened disconnect switch. Typically, there are other paths even if weak that connect the VT point with the CT points (parallel lines), making this scenario less likely. However, in general, we can see spurious LOP indications under stub bus conditions.

3.4. IMPACT ON BREAKER FAILURE PROTECTION

Under stub bus conditions, the two local breakers (CB1 and CB2) are isolated from the network element. Therefore, upon CB1 or CB2 failure, DTT signals should not be sent to the other breakers of the network element.

4. STATION BYPASS

Station bypass is an operation that mainly occurs at subtransmission levels where the station bus configuration is relatively simple and no bus coupler or transfer bus is available to allow the substitution of a breaker [4]. These substations may sometimes be referred to as looped substations, meaning a feeder simply loops into or through the substation.

4.1. SWITCHING SEQUENCE

To explain the need for station bypass and the switching sequences involved, consider the bus arrangement in Fig. 9a. If breaker CB2 needs to be taken out of service for routine maintenance and the supply to a critical load must be maintained, a bridge or link has to be created between the source and load. To accomplish this link between Lines 1 and 2 in Fig. 9a, the 89LL disconnect switch is used.

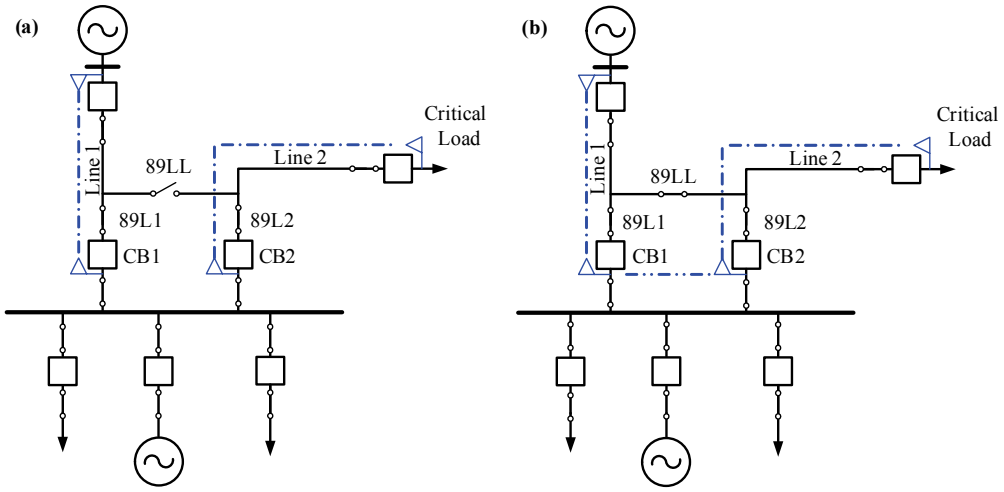


Fig. 9. Normal operating condition with bypass switch 89LL open and two independent feeders (a). Bypass switch closed and circuit transformed from two two-terminal lines to one four-terminal line (b)

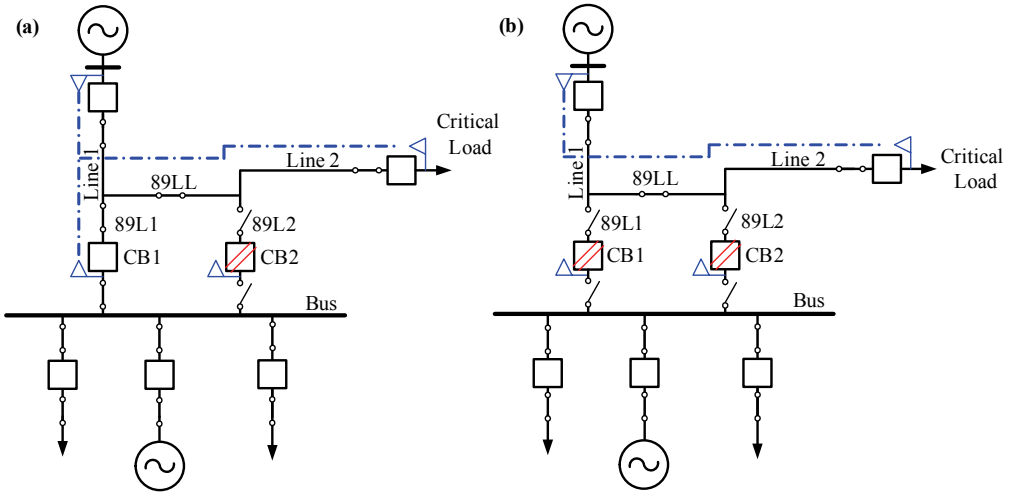


Fig. 10. Breaker requiring maintenance and associated line switch open and the line transformed from a four-terminal line to a three-terminal line (a). Remaining local breaker and line switch opened, and the line transformed from a three-terminal to a two-terminal line and the station bypassed (b)

To place a feeder on station bypass, the following switching sequence is executed:

- Close the bypass switch (89LL in this example), as shown in Fig. 9b.
- Open circuit breaker CB2 and then line link 89L2, as shown in Fig. 10a.
- Open circuit breaker CB1 and then line link 89L1, as shown in Fig. 10b (this step is optional and is dependent on the utility operating philosophy or system condition at the time).

To return the feeder to its normal operating condition, the operating procedure is executed in the reverse order.

4.2. BUS PROTECTION CHALLENGES AND SOLUTIONS

The bus configuration shown in Fig. 9a can be equally well protected by a high- or low-impedance bus differential relay. A high-impedance scheme would generally be a more economical choice but poses a challenge in how to handle the CTs associated with the out-of-service breaker(s) (see Fig. 10). This concern is addressed by routing the CTs through the auxiliary contacts of the line disconnect switches 89L1 and 89L2, as shown in Fig. 11. These auxiliary contacts need to be early make, late break contacts [2].

Because the operating procedures and interlocking philosophy are such that line breakers are opened before the line disconnect switches are, there is no risk of ever open-circuiting a CT under load conditions.

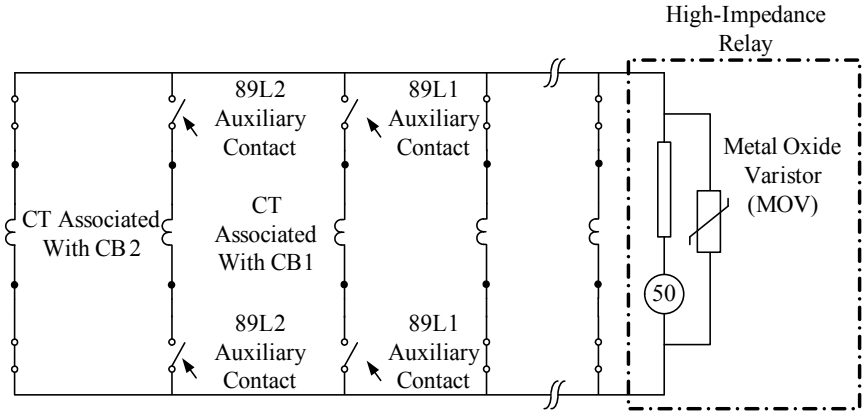


Fig. 11. Routing CT leads through auxiliary contacts
of line disconnect switches enables CT switching
in a high-impedance bus protection scheme

If a low-impedance bus differential relay is used to protect the bus, no physical CT switching is required and the CTs associated with the out-of-service breaker(s) are removed from the differential protection zone dynamically by the relay programmable logic using the status of the line disconnect auxiliary contacts [1], [2]. If the line disconnect switch is closed, the CT is considered in zone, and if the line disconnect is open, the CT is considered out of zone. The low-impedance bus differential approach avoids CT switching. Check zone and undervoltage supervision are not required because, at the time of switching, the currents are zero (the breakers are opened).

4.3. LINE PROTECTION CHALLENGES AND SOLUTIONS

When the bypass link (89LL) is closed, the two independent lines (Lines 1 and 2) are transformed from two two-terminal lines to one four-terminal line (see Fig. 9b).

When one of the local breakers and its associated line disconnect switch are opened, the line is transformed from a four-terminal line to a three-terminal line (see Fig. 10a). Depending on the operating philosophy or system conditions, the other remaining local breaker and associated line disconnect switch may be opened, transforming the line from a three-terminal line to a two-terminal line. Accordingly, the line protection has to be adjusted to effectively protect the reconfigured line. In this paper, we consider both distance and differential protection of the line. Even though these protection methods may seem to have common attributes, their differences validate dealing with the two protection methods separately.

A. Distance Protection

To afford 100 percent protection for both lines during the switching sequence, the settings of the distance relays at all locations need to be adjusted to reflect those of the power system being protected.

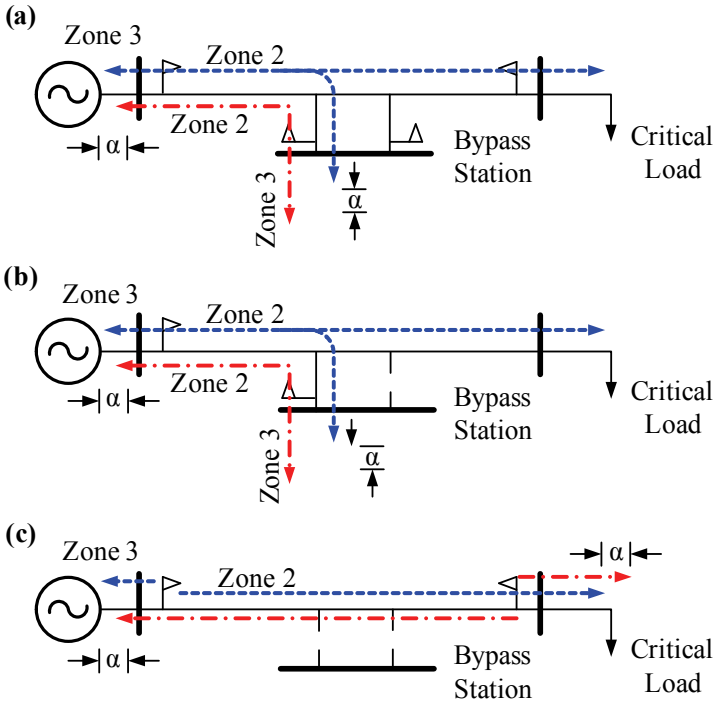


Fig. 12. For the first step of the bypass procedure, the line is a four-terminal line (a). For the second step of the bypass, one local breaker is taken out of service and the line becomes a three-terminal line (b). For the third and final step of the bypass, the second local breaker is taken out of service and the combined line becomes a two-terminal line (c)

During the first step of the station bypass when the line is transformed into a physical four-terminal line, the protection of the lines (Lines 1 and 2) requires the overreaching zone reaches of the remote relays to be set so that each remote relay can see past the other remote terminals, considering infeed from the terminal(s) at the bypass station, as shown in Fig. 12a. The overreaching zones of each of the local relays (relays at the bypass station) have to be such that each relay can see past the farthest remote relay terminal. At the same time, the reverse reach of the local relays has to be checked to ensure coordination with the overreaching zones of the remote relays (α in Fig. 12a should be set so that the reverse-reaching element can see at least 10 percent further back than the forward-reaching zone of the remote terminal). Note that

none of the instantaneous or underreaching zone reaches at any of the relay locations requires a settings change from its normal settings value.

For the second step of the bypass (as shown in Fig. 12b) when one of the local breakers is taken out of service (out of service in this paper means the breaker is open and the associated disconnect is open), no settings at any of the relay locations need to be changed if the settings at the remote relays and at the local relay are such that each overreaching zone can see past the farthest terminal and the reverse zones are set to correctly deal with the extended overreaching zones.

For the final step of the bypass, when both local breakers are taken out of service, no settings changes are required at the local relays if they are configured correctly so as to not initiate a trip to an already open breaker. The remote relays require a settings change in their communications-aided scheme logic because they transitioned from a multiterminal system to a two-terminal system. The overreaching zones do not require change, but the underreaching zones can be extended so that they cover a greater percentage of the combined line. Details of how this is accomplished are discussed in the following paragraphs.

In essence, the bypass of the station can be broken up into the following two parts:

- Adapting the settings and control of the relays at the bypass station (local relays).
- Adapting the settings of the remote terminal relays.

At the bypass station, the whole bypass process can be made less complex and more reliable if the relays have access to the current in the adjacent line and are capable of controlling the adjacent line breaker. As mentioned in Section II, modern distance protection relays are capable of supporting multiple current and voltage input terminals.

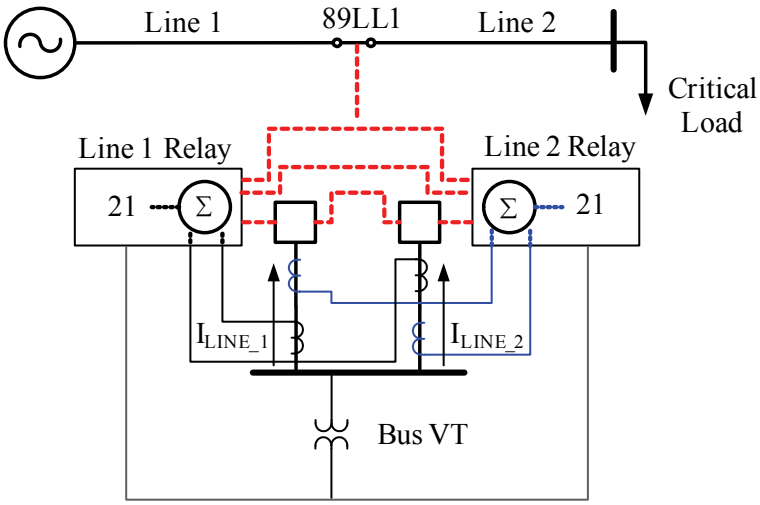


Fig. 13. Suggested setup at the bypass substation to facilitate a more reliable station bypass

When both line breakers are closed and the bypass link closes, the current used by the distance elements should switch from that of Line 1 (I_{LINE_1}) to the sum of the two line currents ($I_{LINE\_1} + I_{LINE\_2}$). This is equivalent to placing a virtual CT measuring the current at the tap created between the two lines by closing the 89LL disconnect switch.

At the same time, any trip or reclose decision made by any one of the line relays will operate both of the local breakers, because the two breakers operate in parallel and are in series with the tap created by closing the 89LL disconnect switch.

Since both local relays are set identically, we can say that at this stage, one relay is a backup for the other relay. In this manner, the four-terminal line can be considered as a three-terminal line, as shown in Fig. 14.

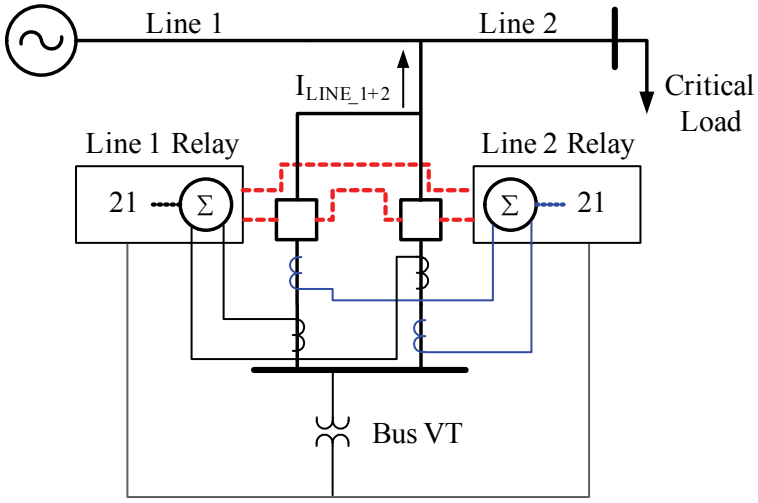


Fig. 14. When viewed from an electrical point of view, the physical four-terminal line can be, in effect, a three-terminal line if the two currents at the bypass station (local) are simply summed together

In the arrangement shown in Fig. 14, the communications schemes in the two relays can be kept separate in that each relay only communicates to its original remote terminal and not to the adjacent line remote terminals. So in order for a line relay to send a permissive signal to the adjacent line relay remote terminal, a cross trigger arrangement is made between the two local relays whereby an output from one relay asserts an input in the adjacent relay, which, in turn, initiates the communications signal if the 89LL switch is closed. This arrangement has a further advantage in that the relays are not required to transition from a two-terminal communications scheme to a three-terminal communications scheme and then back to a two-terminal communications scheme. Also, to enable a three-terminal communications scheme would require a communications channel between the two remote terminals.

Depending on whether the bypass station has an alternative source or not, the weak infeed echo logic would need to be enabled in the communications scheme. This scheme can easily handle any further switching of the bypass station, such as the case in which one of the local breakers is taken out of service, by simply disregarding the current from that breaker. At the same time, the logic is adjusted so as not to issue a trip signal to the out-of-service breaker. When both the local breakers are taken out of service (disconnect switches are opened), both local relays still remain in service, with the exception that the local relays do not operate the local breakers. If both the local breakers are out of service, the communications logic is modified so that the local relays simply repeat or pass through the signals they receive from the remote relays, as shown in Fig. 15. Should one of the relays be required to be taken out of service, an external repeater relay can then be used to simply repeat the signals.

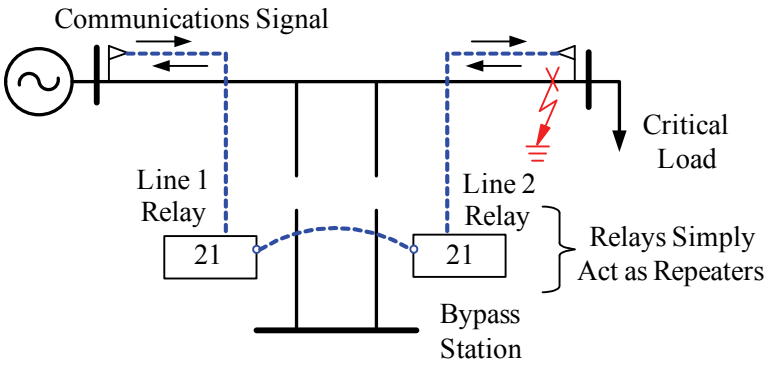


Fig. 15. When both breakers at the bypass station are taken out of service with the line in the bypass mode, the local protective relays can act as repeaters for the communications signal to enable the communications-aided scheme

A further advantage of the scheme is that it can also deal with the case in which the critical load bus may be connected to an alternative power source.

The other issue that needs to be addressed is informing the remote terminal relays about the changes occurring at the bypass substation. This can be done by using the same communications channel as the protection communications scheme and reserving two extra communications bits. One bit is to inform both remote relays that the bypass link has been closed and to adjust their overreaching zones accordingly. The second bit is used to indicate that both local breakers are out of service and that the instantaneous zone reaches can be extended so that a greater part of the combined line can be protected by these elements.

The advantage of the previous scheme is that for each system configuration, a separate settings group can be preconfigured. This means that for each switching configuration of the power system, the lines are appropriately protected. An extra benefit of

the scheme is that it is fully automated by using the appropriate link status to select the corresponding settings group.

B. Differential Protection

Differential elements work on the principle of Kirchhoff's current law. Therefore, for a differential element to effectively protect a piece of apparatus, it needs to see all the currents that enter or leave the protected zone. For the station bypass case under normal operating conditions (Fig. 16a), there are two separate two-terminal lines protected by a pair of line differential relays providing instantaneous protection for both lines. However, when the bypass link is closed, the two two-terminal line protection zones transition to a single four-terminal line protection zone, as shown in Fig. 16b.

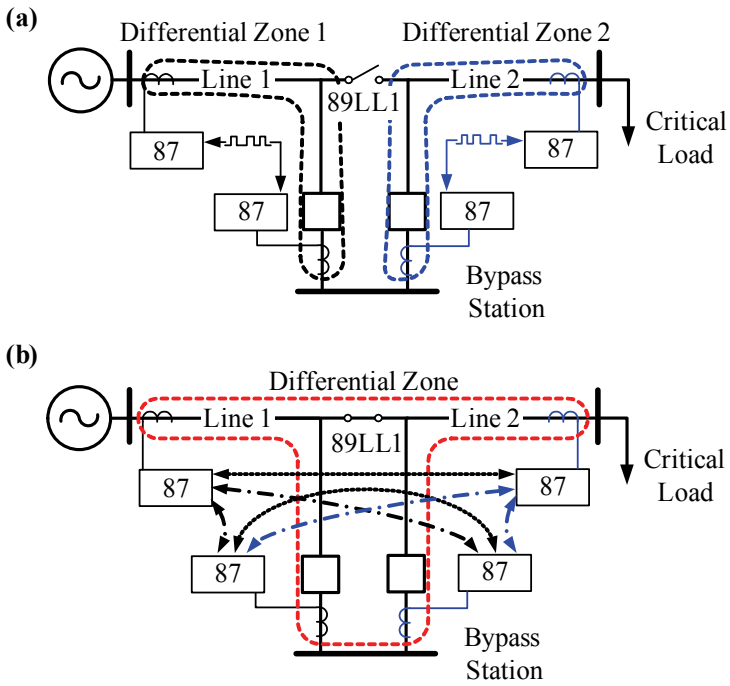


Fig. 16. Normal operation with two two-terminal line differential zones (a). Three-terminal differential zone with the bypass switch (89LL) closed (b)

We could use a brute force method and simply require that each differential relay now have access to all the currents that enter the protection zone, as in Fig. 16b. This requires that communications channels exist between all the stations and that the differential relays be capable of being configured as four-terminal differential relays. One way to ensure connectivity between all four relays is to use Ethernet for 87L protec-

tion over a deterministic transport method, such as a synchronous optical network (SONET).

If all of the above requirements are met, then it is definitely possible and feasible to preconfigure a modern line differential relay to adapt to the changing configuration of the power system by making use of the different available settings groups within the relay. Again, the statuses of the local and bypass disconnect switches are used to enable the different settings groups.

Should all communications channels not be available or should the line differential relay not be capable of being configured as a four-terminal differential relay, then there are more elegant methods available to protect the lines during power system reconfiguration. In this paper, we consider the following two different scenarios:

- Communication is available between all substations, and the relays are only capable of being configured as either two- or three-terminal line differential relays.
- The only communications channels available are those that normally exist between the remote substation and the local substation, no direct communication is available between the two remote substations, and the differential relays are only capable of being configured as two- or three-terminal line differential relays.

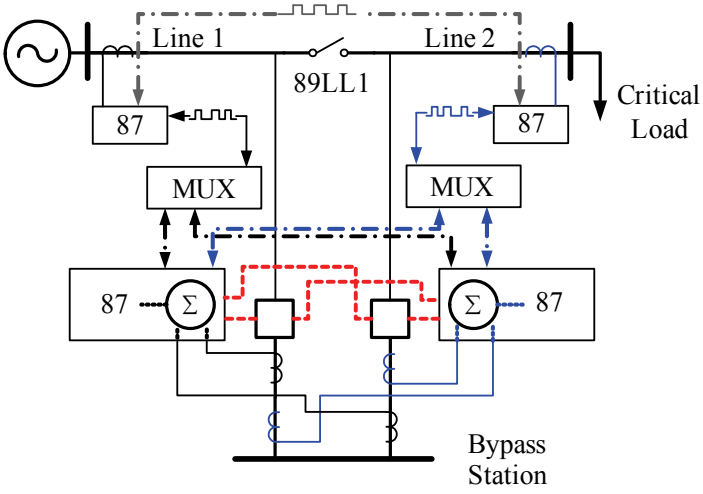


Fig. 17. Setup of the protective relays when there are communications channels between all substations and the differential relays are capable of protecting a three-terminal line

If we consider the first scenario, in which we have communications channels available between all substations, the relays at each substation would be preconfigured to adapt to the changing power system configuration. As shown in Fig. 17, the protective relays at the source substation and the critical load substation have a communications channel between them, and similarly as with the distance protection scheme, the relays

at the bypass substation have access to the current and breaker I/O from the adjacent feeder.

When the bypass link is closed, all relays in the scheme change from two-terminal mode to three-terminal mode and the zones of protection change from two independent zones to one common zone, as shown in Fig. 16b. At the bypass station, one of the relays becomes the main protective relay and the other relay goes into standby mode, as shown in Fig. 18. In standby mode, the relay is fully functional with the exception that it does not run its 87L element. This is because the remote relays expect a single 87L relay at the bypass station to be a part of the three-terminal 87L scheme. This is different than in the distance scheme where the data packets in the communications signals do not contain their origin. However, in the differential scheme, the data packets contain the origin of the packet for the purpose of avoiding cross-connections and loopbacks. Even though both local relays could consume the data from the remote terminals and send the total current of the tap created by the closed 89LL switch, only one relay can be a part of the three-terminal 87L scheme.

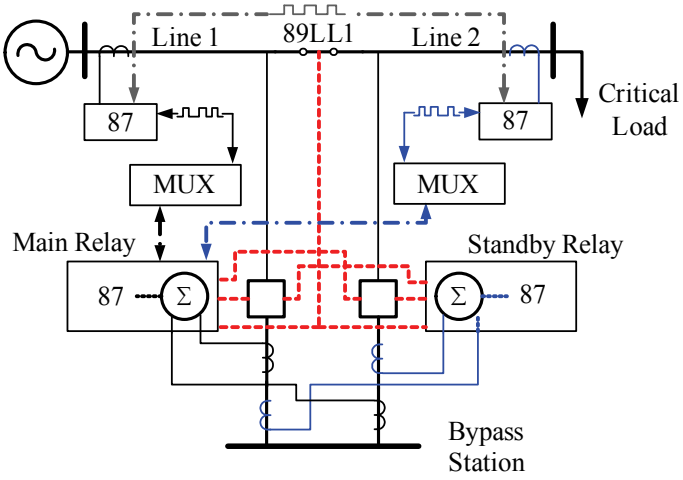


Fig. 18. Configuration of a differential protection scheme when the bypass link is closed and the power system is configured as a four-terminal line. Only one of the bypass station relays is available in the protection scheme, thereby turning this application into a three-terminal line

The scheme is set up such that if the main relay fails or is taken out of service, it automatically transfers the communication and protection to the standby relay and the standby relay is set identically to the main relay; even its transmit address is the same. This means that if the protection transitions from the main relay to the standby relay, the remote relays will not be able to detect this transition, with the exception that there will be a few missing packets because of the time taken for the local relay to begin

transmitting data packets to the remote terminals. In this scheme, all relays are master relays, meaning that each terminal performs its own differential calculation and is responsible for initiating its own trip command.

When one of the local breakers is taken out of service, the scheme does not require any settings changes. When both the local breakers are out of service, the scheme has the option to remain in a three-terminal mode or switch to a two-terminal mode. In either case, the relays at the bypass substation do not issue any trip commands and the relays at the remote substations either use the zero current sent to them from the bypass station (three-terminal mode) or work with just the remote station currents (two-terminal mode).

In the second scenario, shown in Fig. 19, where there is no communication between the two remote substations and the protective relay is capable of protecting a three-terminal line, the setup is similar to the one shown in Fig. 17.

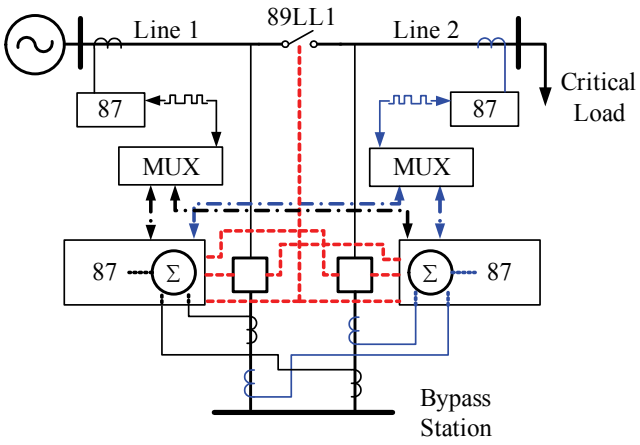


Fig. 19. Setup of the protective relays when communications channels exist only between the remote terminals and the individual relays at the bypass substation

The difference between this arrangement and that shown in Fig. 17 is that when the power system is reconfigured (i.e., the two lines combined to become a single line with four terminals, a three-terminal single line, or a combined two-terminal line), the only relays that see all the currents in the protection zone are the relays located at the bypass bus, as shown in Fig. 20. Therefore, these are the only relays capable of executing the differential calculation and being the master relays. The remote relays simply feed current data to and execute 87L trip commands from the master relays at the bypass substation during the reconfiguration of the power system and therefore merely act as slave devices. These slave devices do not have the ability to make their own tripping decisions, and therefore, the trip decision is communicated to them from the master relays via the communications channel.

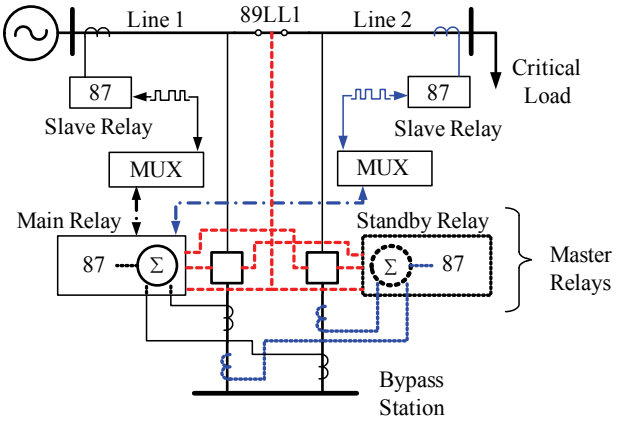


Fig. 20. Configuration of a differential protection scheme when the bypass link is closed and the power system is configured as a four-terminal line and no communication exists between the relays at the remote terminal

Because the remote relays can only act as slave relays, there are a few drawbacks to this scheme. The first is that the relays at the bypass station cannot be taken out of service, even if the line is in a complete bypass mode (i.e., both local breakers are out of service, as shown in Fig. 21).

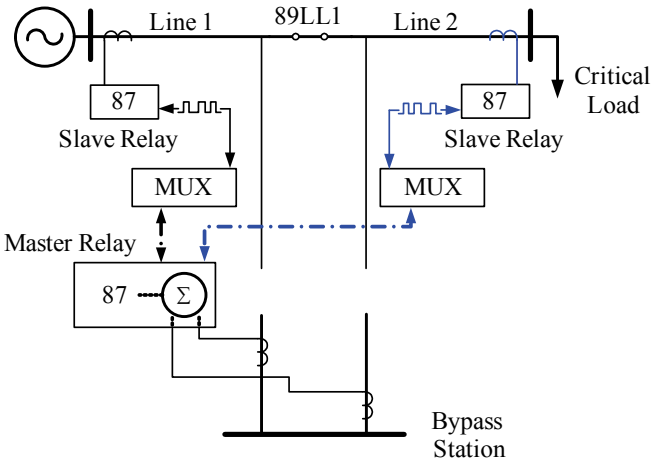


Fig. 21. Final configuration of the power system and the protection system when no communication exists between the remote relay terminals

The remote breakers are tripped slightly slower because they need to wait for the trip command to be sent back from the master relay. This is typically not an issue, however, because of the voltage level at which station bypass is typically allowed.

The advantage of both these schemes is that multiple settings groups can be pre-programmed using different settings for each possible configuration. In this way, the relays can follow the reconfiguration of the power system and afford maximum protection to the power system at all times. The appropriate settings group can be selected using the status of the disconnect switches at the bypass station. In this fashion, the whole bypass procedure can be automated and the possibility of errors during the bypass procedure can be reduced.

5. CONCLUSION

Temporary bus configurations allow greater utilization of power system assets but create challenges for protection systems.

Traditional solutions to temporary bus configurations required that electromechanical relays use test and bypass switches to ensure the affected relays were provided with the appropriate currents and voltages as well as that the trip signals were routed to the appropriate breakers. In some cases, spare relays, manual settings changes, and the rerouting of pilot signals were required. All these manual operations increased the danger of misoperation when making changes, during temporary configurations, or when restoring to the normal configuration. As a result, temporary bus configurations have been carefully considered and often avoided, resulting in the underutilization of network assets.

This paper describes how modern microprocessor-based relays can simplify applications under temporary bus configurations, eliminate the need for any manual reconfiguration or settings changes, and improve the performance of protection. These benefits stem from the ability to connect multiple current and voltage inputs, the ability to trip multiple breakers, communications between relays, multiple settings groups, and programmable logic that allows an automatic detection and dynamic response to temporary bus configurations.

REFERENCES

[1] LABUSCHAGNE C., MOXLEY R., JESSUP E., NEEDS J., *Low-Impedance Bus Differential – Security and Reliability in Complex Bus Arrangements*, Proceedings of the 11th International Conference on Developments in Power System Protection, Birmingham, UK, April 2012.

[2] STEENKAMP L., LABUSCHAGNE C., STOKES-WALLER E., *Tutorial: Complex Busbar Protection Application*, proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[3] KASZTENNY B., BENMOUYAL G., ALTUVE H. J., FISCHER N., *Tutorial on Operating Characteristics of Microprocessor-Based Multiterminal Line Current Differential Relays*, Proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[4] TZIOUVARAS D.A., HAWBAKER W.D., *Novel Applications of a Digital Relay With Multiple Setting Groups*, proceedings of the 17th Annual Western Protective Relay Conference, Spokane, WA, October 1990.

[5] SLEEPER H. P., *Ratio Differential Relay Protection*, Electrical World, October 1927, pp. 827–831.
[6] THOMPSON M. J., *Percentage Restrained Differential, Percentage of What?*, proceedings of the 64th Annual Conference for Protective Relay Engineers, College Station, TX, April 2011.
[7] ZIEGLER G., *Numerical Differential Protection: Principles and Applications*. Publicis Corporate Publishing, Erlangen, Germany, 2005.
[8] MILLER H., BURGER J., FISCHER N., and KASZTENNY B., *Modern Line Current Differential Protection Solutions*, proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.
[9] WARRINGTON A. R. van C., *Protective Relays: Their Theory and Practice, Vol. 1*. Chapman and Hall Ltd., London, England, 1962.
[10] TZIOUVARAS D. A., ALTUVE H., BENMOUYAL G., and ROBERTS J., *Line Differential Protection With an Enhanced Characteristic*, proceedings of Med Power 2002, Athens, Greece, November 2002.
[11] BENMOUYAL G. and LEE T., *Securing Sequence-Current Differential Elements*, proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.
[12] GUZMÁN A., LABUSCHAGNE C., and QIN B. L., *Reliable Busbar and Breaker Failure Protection With Advanced Zone Selection*, proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.
[13] BENMOUYAL G. and ROBERTS J., *Superimposed Quantities: Their True Nature and Application in Relays*, proceedings of the 26th Annual Western Protective Relay Conference, Spokane, WA, October 1999.
[14] FODERO K., HUNTLEY C., and WHITEHEAD D., *Secure, Wide-Area Time Synchronization*, proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.
[15] ADAMIAK M. G., ALEXANDER G. E., and PREMERLANI W., *A New Approach to Current Differential Protection for Transmission Lines*, proceedings of the 53rd Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 1999.
[16] GAJIC Z., BRNCIC I., and RIOS F., *Multi-Terminal Line Differential Protection With Innovative Charging Current Compensation Algorithm*, proceedings of the 10th Developments in Power System Protection Conference, March 2010.
[17] SCHWEITZER E. O., III, FISCHER N., and KASZTENNY B., *A Fresh Look at Limits to the Sensitivity of Line Protection*, proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.
[18] FINNEY D., FISCHER N., KASZTENNY B., and LEE K., *Testing Considerations for Line Current Differential Schemes*, proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

vacuum circuit breaker, double-break vacuum interrupters
SF6 circuit breaker, capacitor banks, transient recovery voltage,
dielectric strength, breaking capacity

Tahir LAZIMOV*
Esam SAAFAN**

TRANSITIONAL PROCESSES AT CAPACITIVE CURRENTS SWITCHING-OFF BY SINGLE AND DOUBLE-BREAK INTERRUPTERS OF VACUUM CIRCUIT BREAKERS

Vacuum circuit breaker technology based on double-break vacuum interrupters has become the most requirements of high voltage circuit breakers that not environmentally harmful. The vacuum interrupter has an excellent ability to deal with the steep rising part of the transient recovery voltage, which makes it faster in the current interruption process. This paper presents results of computer simulations conditioned by capacitive currents switching-offs by using single and double interrupters of vacuum circuit breakers. These results demonstrate that use of double-break circuit breakers leads to notable decreasing of switching overvoltages and allows in the same time to meet the dielectric requirements for high voltage vacuum circuit breakers.

1. INTRODUCTION

According to the dielectric strength, SF6 has better behavior than vacuum. That is why SF6 has generalized as insulating and as arc quenching medium. Under normal conditions, SF6 is an inert, nonflammable, non-corrosive, odorless and non-toxic gas. However, at temperatures over 1000 °C, SF6 decomposes to gases including S_2F_{10} which is highly toxic. Fortunately, the decomposition products recombine abruptly after arc extinction (when the temperature goes down) [1]. SF6 has been labeled as one of the major global warming gases, since the 3rd Session of the Conference of the Parties to the United Nations Framework Convention on Climate Change [2]. Hence,

* Electric Supply and Insulation Chair, Azerbaijan Technical University, AZ1009, Baku, Azerbaijan, e-mail: tahirlazim@gmail.com

** Electrical Engineering Department, Faculty of Engineering, University of El-Mansoura, Box 35516, Egypt, e-mail: esam_ali_saafan@yahoo.com

there is an urgent need to study new generation of high voltage circuit breakers that not environmentally harmful.

Note in this view that working-up of the new generation of high-voltage circuit breakers with carbon and nitrogen dioxides as an arc quenching media begun in the end of the last century had given the negative results [3]. It means that vacuum and SF6 circuit breakers are staying the preferable ones.

As it is known in vacuum circuit breakers (VCBs) the quenching media is a vacuum, so there is no risk for the environment. Another advantage of VCBs is the higher dielectric strength restoration after current zero in comparison with other types of circuit breakers. The problem of using VCB in high voltage applications is related to the high voltage capability of a single gap between electrodes. The breakdown characteristics have very high dependence of electrode area, and the dielectric strength with the contact gap. On this way, in vacuum breakdown, the breakdown voltage is proportional to the square root of the gap length. Thus, a longer gap is necessary for the vacuum interruption. But this technology makes the circuit breaker bigger and leads to the problem of arc control. It appears a high arc voltage noise, which indicates that the vacuum arc is unstable in a long gap [1, 2].

The study of circuit breakers based on the vacuum interrupters in series began in the 1960s. During the past period the patent applications were made by several manufacturers in the USA and Japan but none was applied in the industry because of technical conditions. With the development of large-capacity vacuum circuit breakers, a new round of research is proceeding in the 21st century [2, 4, 5].

So the main purpose of this research is to focus on VCBs only. In this research all capacitor banks switching-off processes were performed by using single and double interrupters of VCBs. A simulation results were performed by using PSCAD /EMTDC program. The transitional recovery voltages are compared in deferent interruption conditions in this research.

2. THEORETICAL BASES OF THE CASE UNDER STUDY

The connection scheme and equivalent electrical network for the case under study (capacitor banks of rated voltage 110 kV switching-offs) are shown in fig. 1. The figure shows the connections of single and double interrupters of the circuit breaker.

The numerical values of the connection scheme parameters for single phase representation used for computer simulation are shown in table 1. Note that, the capacitance value of capacitor bank shown in case of 37 MVAr rated jet power.

While carrying out the present research we had applied a mathematical model described in [6, 7]. The known phenomenon of current chopping was modeled in accordance with [6, 8]. Electrical strength and breakdown voltage of vacuum circuit breakers had been given in the numerical models in accordance with [6, 9].

Table 1. Connection scheme parameters for single phase representation

R_S [Ω]	L_S [mH]	G_L [s]	C_L [μF]	G_C [s]	C_C [μF]
0.2	23	10^{-3}	1.5	10^{-7}	10

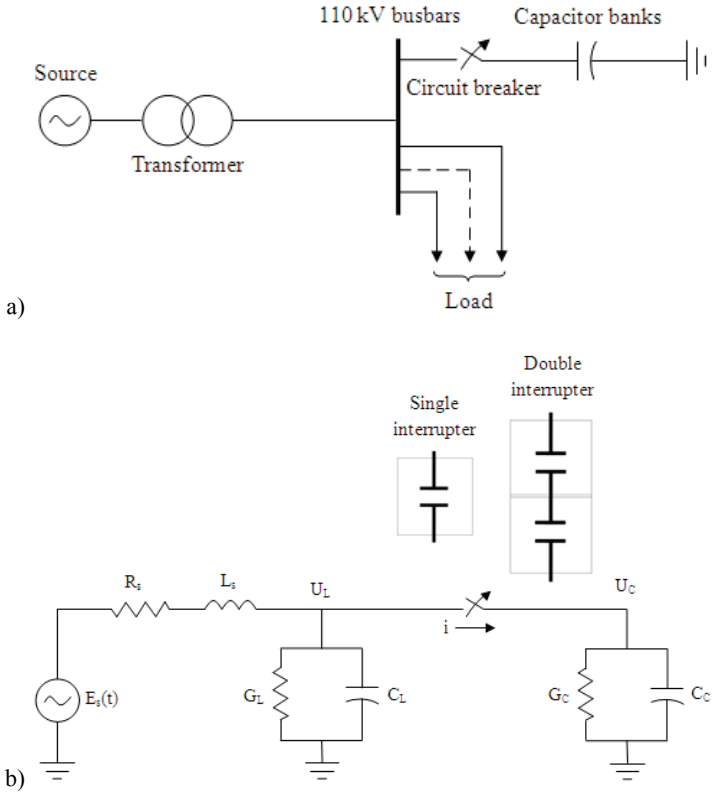


Fig. 1. The scheme and the network under consideration:
a) connection scheme; b) simulated network (index s concerns to the source parameters, l – to the load parameters, c – to the capacitor banks parameters

3. CIRCUIT BREAKER DIELECTRIC STRENGTH

It is known that when the interrupter contacts of circuit breaker starts to separate from each other the breakdown voltage of the gap starts to increase. After the arc has been extinguished, the race between transient recovery voltage (TRV) and dielectric withstand of the interrupter begins. When the TRV exceeds the dielectric withstand of the interrupter a breakdown occurs and creates a conducting path between the two contacts. Then the TRV jumps back to zero and does not start to rise again before the

arc is extinguished. Therefore the dielectric withstand of the circuit breaker is a significant parameter for the switching analysis.

For VCBs the most of authors use linear restoration law [10, 11]. But this law is not quite suitable to the physical nature (decreasing of strength at increasing of inter-contact distances) of vacuum inter-contact gaps [12, 13]. Therefore for modeling the dielectric properties of the inter-contact spaces we used the logarithmic law of dielectric strength restoration in VCBs presented in [14]. This law takes into account both inertia of contact and inconstancy of strength of vacuum gaps. The logarithmic restoration law for dielectric strength is given by the following empirical formula:

$$V_{str}(t) = 191.43 \log\left\{1 - \cos\left[\frac{\pi(t - t_{off})}{T_{full}}\right]\right\} \quad (1)$$

where: $V_{str}(t)$ is the acceptable law of circuit breaker's dielectric strength restoration; X_m is the maximum distance between contacts; t is the time; t_{off} is the initial instant of contact separation; T_{full} is the full switch-off time of vacuum inter-contact gap [5].

4. RESULTS OBTAINED AND DISCUSSION

The aims of these simulations divided into two directions. At first, comparing the results obtained from capacitor banks switching-off by using single and double interrupters of VCBs. In this case the contacts of the two vacuum interrupters are simultaneously separated. At second, it's important to find the interaction relationship between the two vacuum interrupters during the current interruption process and to obtain the best strategy to open contacts. In this direction, the VCB model is obtained by connecting the model of double-break interrupters in series. The voltage distribution between the two vacuum interrupters is simulated under deferent contact parting sequences. Each vacuum interrupter model is represented by the respective contact resistance before contact separation and by the respective dielectric strength restoration after contact separation. We can adjust the initial moment of the dielectric strength model by changing the separation time of the two contacts.

The results of capacitor banks switching-off with rated jet powers of 37-112 MVAr are presented below. The transitional currents and recovery voltages in cases of single and double interrupters of VCB are shown in tables 2, 3, respectively.

As shown the overvoltages values for both cases (single and double interrupters) do not exceed the rated amplitude's triple value which is maximum allowable for

the 110 kV insulation level (tables 2, 3). Comparing the results shown we can state that using of double interrupters of VCB causes less magnitude of overvoltage, inter-contact recovery voltage, and overcurrent. The reductions are equal to 27%, 65%, and 23% for capacitor bank voltage, interrupter voltage, and interrupter current respectively. It means that, double interrupters of VCB have more efficient breaking capability during current interruption process. At the same time the recovery voltage divided symmetrically across the double interrupters. It means that, the recovery voltage is not great influencing the voltage divisors (capacitive and resistive ones) that connected between poles of circuit-breakers.

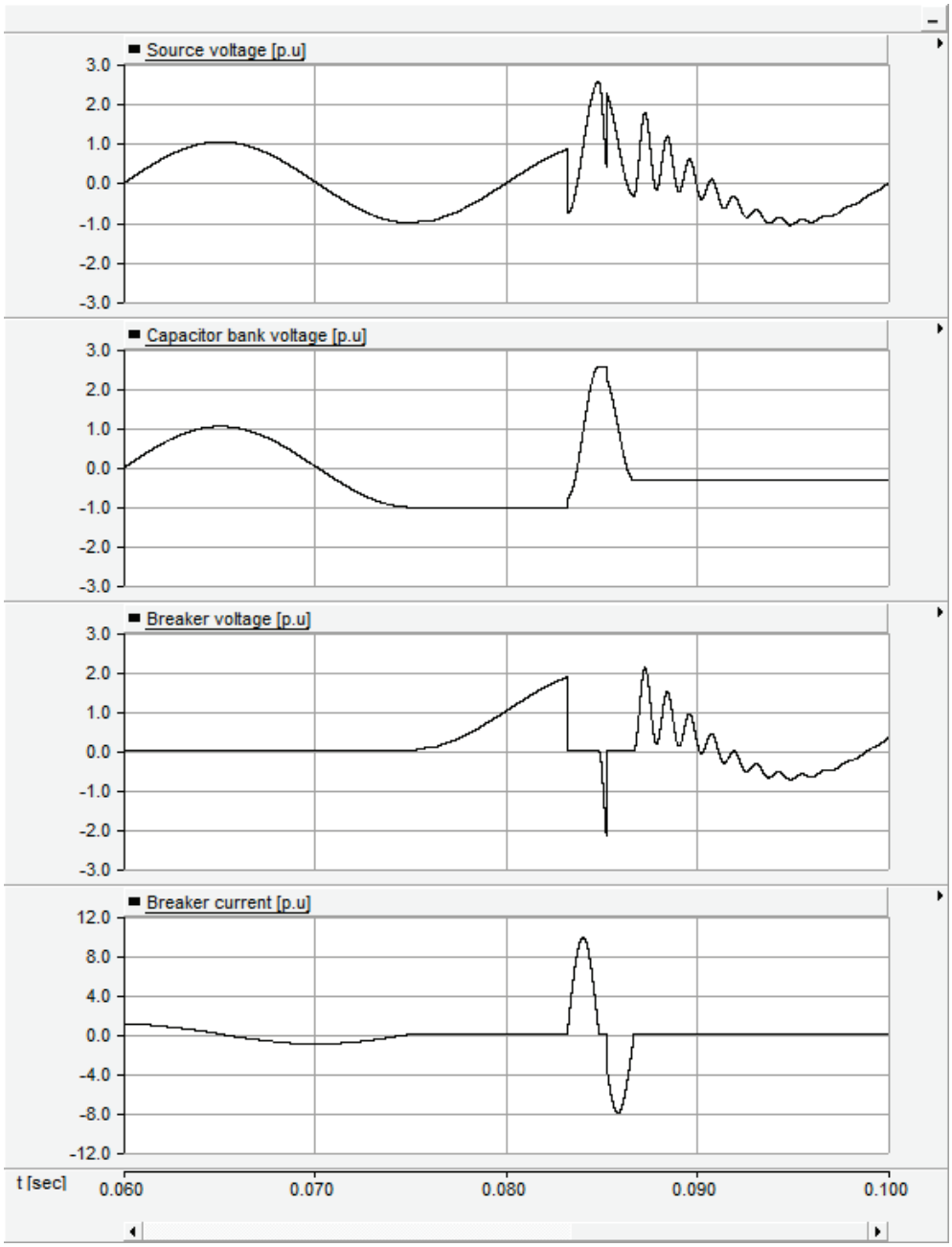
Table 2. Overcurrents and overvoltages in case of single interrupter VCB for range of jet powers

Capacitor bank [MVAr]	Capacitor bank voltage [p.u.]	Breaker voltage [p.u.]	Breaker current [p.u.]
37	2.54	2.16	9.84
56	2.68	2.39	8.68
75	2.75	2.56	7.80
112	2.84	2.69	6.81

Table 3. Overcurrents and overvoltages values in case of double interrupters VCB for range of jet powers

Capacitor bank [MVAr]	Capacitor bank voltage [p.u.]	Interrupter voltage [p.u.]	Breaker current [p.u.]
37	1.85	0.85	7.63
56	2.02	0.88	6.83
75	2.14	0.91	6.19
112	2.34	0.96	5.39

Some calculated transitional voltages and currents taken place at capacitor banks switching-off with jet powers of 37 and 112 MVAr are presented in figures 2, 3, respectively. Note that, the recovery voltage shown in figure 3 for each interrupter in case of double interrupters. As shown in figure 2, for the case of 37 MVAr capacitor banks switching-off, we had only two repeated re-ignitions for both cases (single and double interrupters). But from figure 3, for the case of 112 MVAr capacitor banks switching-off, we had three repeated re-ignitions in case of single interrupter and two repeated re-ignitions in case of double interrupters. It means that, using of double interrupters of VCB may also reduce the probability of repeated re-ignitions.


Source voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Capacitor bank voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Breaker voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Breaker current [p.u]
12.0
8.0
4.0
0.0
-4.0
-8.0
-12.0
t [sec]
0.060
0.070
0.080
0.090
0.100

a)

b)

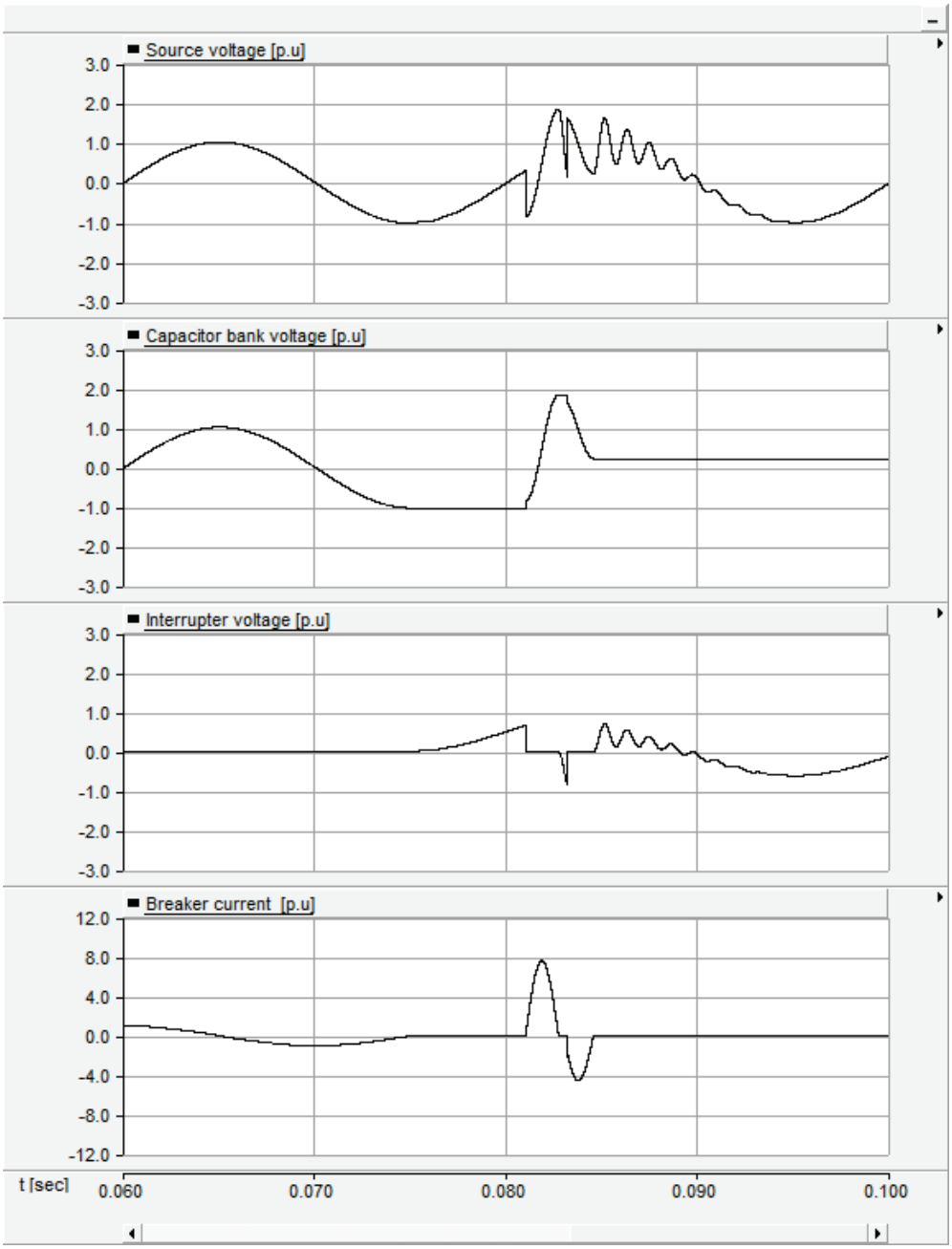
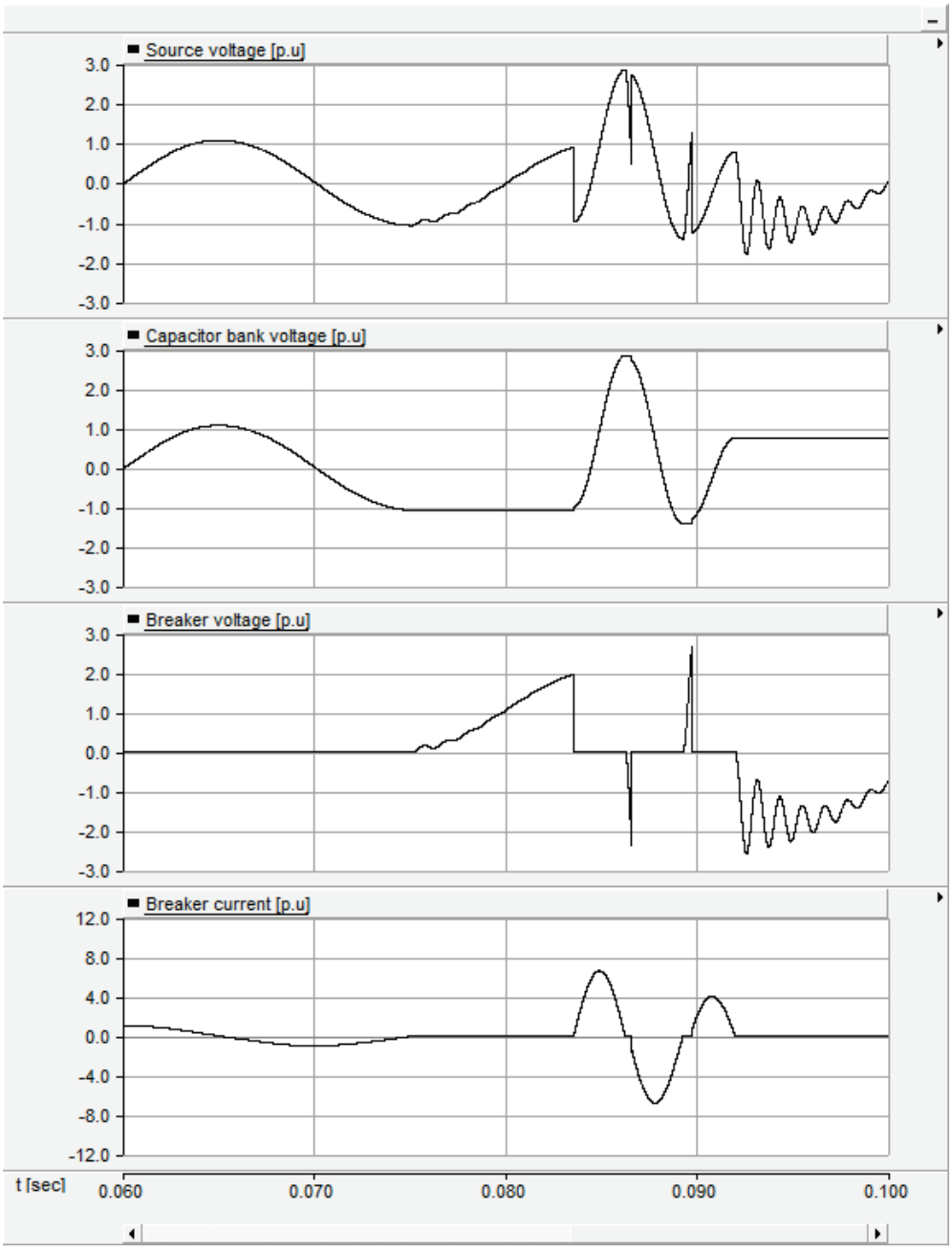
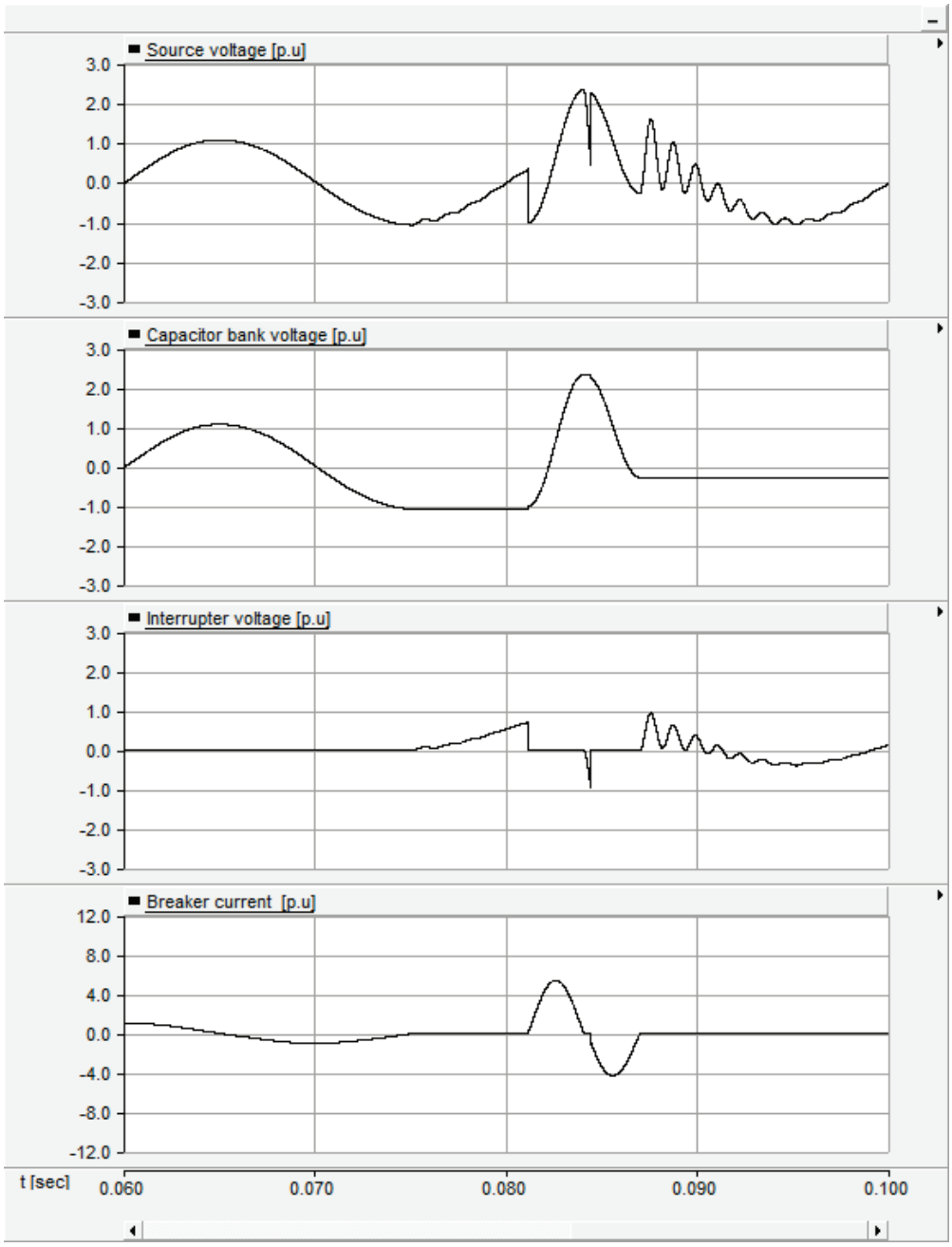


Fig. 2. Transitional voltages and currents conditioned by 37 MVAr capacitor banks switching-off of VCB: (a) single interrupter; (b) double interrupters


Source voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Capacitor bank voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Breaker voltage [p.u]
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
Breaker current [p.u]
12.0
8.0
4.0
0.0
-4.0
-8.0
-12.0
t [sec]
0.060
0.070
0.080
0.090
0.100

a)



b)

Fig. 3. Transitional voltages and currents conditioned by 112 MVAr capacitor banks switching-off of VCB: (a) single interrupter; (b) double interrupters

For the second aim of this research we had found that, if one of the two interrupters switched-off after/before the other interrupter, during this time interval the interrupter which switched-off at first will be withstand the TVR alone. So it's important to mention that, when the contacts of the two vacuum interrupters are not simultaneously separated, the performance is not significantly differing from the case of single interrupter switching-off.

5. CONCLUSION

Use of vacuum circuit-breakers with series interrupters leads to a notable decreasing of overvoltages at switching-off high-voltage capacitor banks. This has taken place because that rate of rise the dielectric withstand of the series interrupters is faster than the same rate of a single interrupter of the equivalent spacing. In other words use of more than one break let to prevent notable decreasing of dielectric strength at contacts separation as it occurs for single-break circuit-breakers. The results indicate that, with the development of large-capacity vacuum technology, it is possible to meet the dielectric requirements of VCBs to use it with applications more than 110 kV.

REFERENCES

[1] Iturregi A., Torres E., Zamora I., Abarrategui O., High voltage circuit-breakers: SF6 vs. vacuum, International Conference on Renewable Energies and Power Quality, Valencia (Spain), 2009.

[2] Xian C., Xiongying D., Minfu L., The Voltage distribution characteristics of a hybrid circuit breaker during high current interruption, Plasma Science and Technology, 2013, vol. 15, No.8, P. 800-806.

[3] Berlin, Germany, CIGRE SC B3 Colloquium, Tutorial, Panel and Annual Meeting, Electra, № 239-Aug 2008.

[4] Homma M., Sakaki M., Kaneko E., Yanabu S., History of vacuum circuit breakers and recent developments in Japan, IEEE transactions on dielectrics and electrical insulation, 2006, vol. 13, № 1, P.85 – 92.

[5] Kulkarni S., Kahane A., Sanvatsarkar U., Prospects of Application of Vacuum Switchgear at Transmission Voltages, proceeding of Gridtech 2013 - 4th International Exhibition & Conference, New Delhi, 2013.

[6] Lazimov T., Akhundov S., Research on influence of high voltage circuit-breakers' characteristics on switching overvoltages and overcurrents, proceedings of ELECO'2003 – 3rd International Conference on Electrical and Electronics Engineering, Bursa, Turkey, 2003, p. 1-4.

[7] Lazimov T., Akhundov S., On numerical modeling of transients conditioned by the chopping of current in circuit-breakers, Power Engineering Problems, 2000, №1, p. 60-64.

[8] Lazimov T., Akhundov S., On numerical modeling of current chopping in circuit-breakers, Power Engineering Problems, 2000, №2, p. 38-43.

[9] Lazimov T., Akhundov S., Modeling of electrical strength of high voltage circuit-breakers, proceedings of the International Symposium SIEMA'2001, Kharkov, Ukraine, 2001, p. 112-114.

[10] Yevdokunin G.A., Korepanov A.A., Over-voltages and their limitation at vacuum circuit-breakers switching, Electricity, 1998, No. 4, P.3-10.
[11] Wong S.M., Snider L.A., E.W.C.Lo., Over-voltages and re-ignition behavior of vacuum circuit-breaker, proceedings of IPST - International Conference on Power Systems Transients, New-Orleans, USA, 2003, P.1-6.
[12] Lazimov T., Imanov S., Saafan E. A., Transitional Recovery Voltages at Capacitive Currents Switching-off's by Vacuum and SF6 Circuit-Breakers, Energy and Power Engineering, Chicago, USA, 2012, vol.6, #5.
[13] Lazimov T. M., Saafan E. A., On velocities of modern circuit-breakers' dielectric strength restoration, Power Engineering Problems. 2010, №2, p. 26-32.
[14] Mammadov H., Lazimov T., Imanov S., Improved model of circuit-breaker's dielectric strength restoration, proceedings of ELECO'09 - International Conference on Electrical and Electronic Engineering, Bursa, Turkey, 2009.

voltage stability estimation,
Thevenin equivalent

Bartosz BRUSIŁOWICZ*
Janusz SZAFRAN*

VOLTAGE STABILITY ESTIMATION OF RECEIVING NODE USING APPROXIMATE MODEL

The paper presents approximate model for determining the voltage stability margin. In the first part, Thevenin model and equations describing this model e.g. stability limit are presented. Influence of load and system impedance changes on variations of node voltage are shown. Second part consist description of approximate model determination methods. For the analysis, the 14-bus IEEE model have been chosen. Basing on this model the impact of configuration changes on the Thevenin parameters of considered receiving nodes have been analysed. At the end, the possibilities of use of approximate model for determining the voltage stability margin are described.

1. INTRODUCTION

Today electricity is treated as a commodity and like any commodity should meet defined quality requirements. Required parameters are described in European Standard EN 50160 [1]. One of the parameters is the voltage level. To ensure acceptable value of the voltage in some power system nodes voltage regulation should be installed. This regulation affects voltage level and also other parameters of power system node, e.g. voltage stability conditions. Ensuring appropriate quality of energy and power system safety in the same time may be difficult. For the recipient the most important is quality and for power system operator safety. Additional difficulty results from slow changes of power system characteristic from centralized to distribute. Serious problem may be wind generation which cannot be precisely predicted in long term. Increasing energy generation using distributed generation (DG) connected to distribution networks may cause voltage stability problems [2]. In such networks, the problem is also voltage

* Wrocław University of Technology, Department of Electrical Power Engineering, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland, e-mail: bartosz.brusilowicz@pwr.edu.pl

regulation processes and a large number of its activations. This may be caused by changes of direction of the power flow [3].

To ensure appropriate level of voltage and stability margin, these values should to be considered simultaneously. This can be done by global and local control systems. In literature examples of global systems like Wide Area Control System [4] and their implementation [5] can be found. Methods of approximate value of voltage stability margin determination using local measurements are also described. Both approaches global and local possess the advantages and disadvantages, but development of new control and measurements techniques like PMU (Phasor Measurement Unit) increase a number of advantages of local solutions. The main advantages are: greater reliability, lower installation costs and easier integration of control processes with protection devices. This integration will allow adapting protection algorithms and responding more quickly when adverse condition occurs. The development of local automation is a part of the Smart Grid idea.

2. LOCAL MODELS OF RECEIVING NODE

2.1. THEVENIN EQUIVALENT

Steady state of power system, seen from considered node, can be represented by Thevenin equivalent. Assuming the symmetry of generations and loads of power system, such model can be reduced only to positive-sequence components. Such simplifications are also used to value of short–circuit currents calculation [6]. Thevenin equivalent consist of ideal voltage source E and system impedance Z_S (Fig. 1).

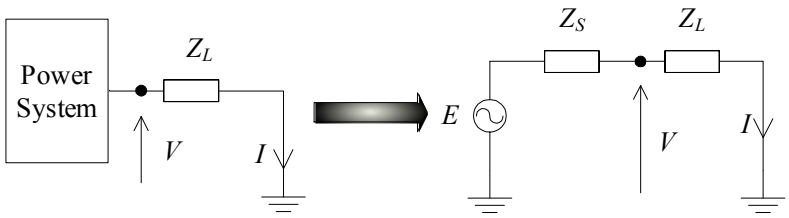


Fig. 1. Power system representation as Thevenin equivalent

Node voltage and apparent power of presented Thevenin model (Fig. 1) can be defined by the following equations [7]:

$$V = \frac{E}{\sqrt{1 + W^2 + 2W\cos\beta}}, \tag{1}$$

$$S = \frac{E^2 W}{Z_S(1+W^2+2W\cos\beta)}, \tag{2}$$

where: V – voltage of node, S – apparent power, $W = Z_S/Z_L$, Z_S – system impedance, Z_L – load impedance, $\beta = \varphi_S - \varphi_L$, φ_S and φ_L – system and load impedance phase angle.

Based on equations that describe model from Fig. 1 value of maximum power transfer (voltage stability limit) can be calculated. Stability limit occurs when the absolute values of system Z_S and load Z_L impedance are equal [8]:

$$|Z_L| = |Z_S|. \tag{3}$$

By transforming formula (1), voltage stability margin calculation equation can be obtained:

$$\Delta W = 1 - \frac{|Z_S|}{|Z_L|}. \tag{4}$$

Factor W can be considered as a load of node ratio. The range of factor W changes from 0 (for idle node) to 1 (voltage stability limit).

Value of node voltage depends on factor W and angles of system φ_S and load impedances φ_L (2). Assuming certain changes of these parameters, curves presenting voltage variations can be plotted (Fig. 2). Ratio W, as noted above, varies between 0 and 1 and β between 50° and 130°.

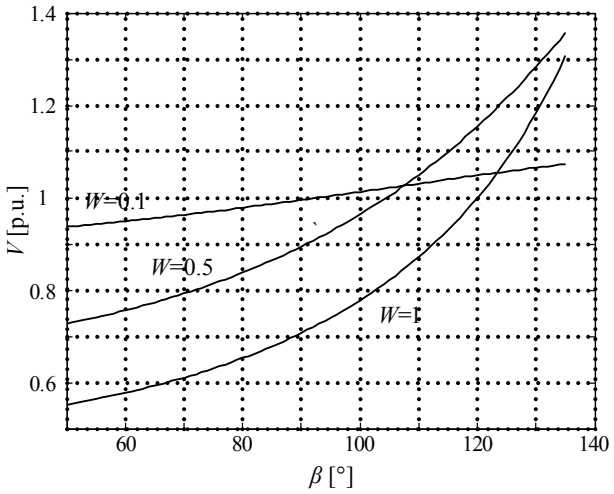


Fig. 2. Variations of voltage depending on W and angle β changes

For one value of angle β, voltage can have different values depending on factor W (Fig. 2). However, one value of voltage can correspond to several levels of W depending on angle β. Basing only on voltage measurements, voltage stability margin of the node cannot be exactly determined. To calculate accurate stability conditions, attaching measurements of other parameters is needed.

Basing on formula (4) and parameters of system and load impedances, distance from operation point of power system node to stability limit can be calculated. Parameters of load impedance Z_L can be measured with high accuracy basing on local measurements. The problem is determination of system impedance Z_S parameters. This value cannot be measured with direct methods.

2.2. THEVENIN CIRCUIT CALCULATION

The simplest way to determine Thevenin model is to calculate parameters using full model of power system. Such model should contain information about whole configuration of power system including parameters of generators and lines. The full models used for power flow calculations represent components of power system as positive-sequence representations. To determine Thevenin equivalent one of the power system nodes should be chosen. Voltage source E is equal to voltage occurring in the idle node. Impedance Z_S is the impedance seen from considered node when all voltage sources are grounded.

Power system configuration and parameters of loads (magnitude and angle) are continuously changed during normal operation. Both of these variations affect the parameters of Thevenin equivalent. Changes of loads can be measured in real time. However, to determine stability conditions according to these changes remaining parameters of Thevenin model should be also updated. These model parameter changes are not measurable directly. Voltage source E and system impedance Z_S are not physical elements. They are virtual equivalents of power system steady state seen from considered node.

2.3. UPDATING OF THEVENIN CIRCUIT PARAMETERS

Thevenin model updating using full power system model requires collecting and analysing a large amount of information about configuration and loads. This method is unsuitable to implementation in automation installed in receiving node, because global information is not available. Better idea is to use local information and measurements or derived from close environment of the node.

One of the methods of voltage stability determination using local measurements has been described in literature [8]. To calculate the Thevenin parameters, local voltage and current measurements are used. Using Kirchhoff's law, Thevenin circuit (Fig. 1) can be described by the following formula:

$$\overline{E} = \overline{V} + \overline{Z}_S \overline{I} \,. \tag{5}$$

Measurable values in the node are voltage V and current I orthogonal components. Unknown are components of serial impedance R_S, X_S and voltage source E_r, E_i. Formula (5) is insufficient to calculate this parameters because there are four unknown values. Two additional independent equations can be obtained by substituting the known parameters obtained for different time. It is important that all calculated parameters should not change between measurements in specific time.

Developments of described method are algorithms that use level of operating point parameters changes caused by load variations. This variations cause node voltage and current changes and consequently apparent, active and reactive power changes. In the literature can be found algorithms using for example: derivative of the node voltage against load admittance dV/dY [9] or derivative of apparent power against voltage of node dS/dV [10]. In the paper [9] have been additionally described use of dV/dY method to block transformer tap changer and to determine the need to load shedding start.

Methods using the local measurements have acceptable accuracy if certain conditions are fulfilled. One is change of the load impedance. It is needed to measure the parameters of working point of two time moments. This may result in a lack of dangerous conditions identification in the case of system configuration change while there is no change of load parameters. Other approach that uses local measurements and information from close environment of node is use of Thevenin approximate model.

2.4. APPROXIMATE THEVENIN MODEL

Approximate Thevenin model can be created basing on separated area of power system full model. In such model analysis of Thevenin parameters changes caused by variations of configuration can be performed. To study this approximate model, IEEE 14-node test model have been used (Fig. 3). The IEEE model has been implemented in ATP-EMTP software.

The IEEE model can be divided into two areas. One with the generators (Area 1) and second with loads only – distribution system (Area 2). Both parts are connected by two important links between nodes 5–6 and 4–9. For analysis nodes 10–14 have been chosen. These nodes are located farthest from generators (considering the electrical distance) and their parameters are most susceptible to changes of configuration. In tables 1–5, changes of Thevenin parameters caused by exclusion of particular line are presented. The greatest impact on the parameters has exclusion of the line directly connected to considered node and disconnection of one of connection between Area 1 and Area 2 (Fig. 3).

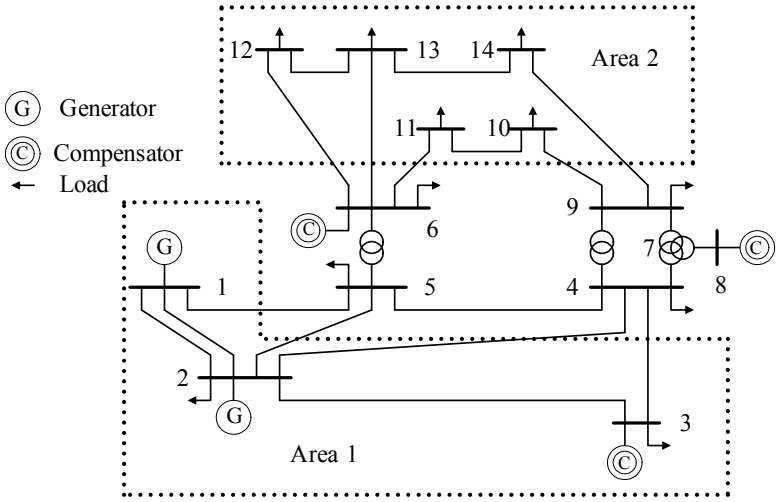


Fig. 3. IEEE 14-node test model

Table 1. Node 10 Thevenin parameter changes

Node 10						
	Full conf.	Excluded line				
		L10–11	L9–10	L6–11	L5–6	L4–9
Z_S [p.u.]	0.296	0.349	0.668	0.346	0.360	0.502
φ_S [°]	68.3	69.6	65.4	69.2	65.9	61.3
E [p.u.]	1.02	1.02	1.03	1.01	1.00	0.91
φ_E [°]	–12.1	–12.1	–12.2	–12.4	–16.6	–18.1

Table 2. Node 11 Thevenin parameter changes

Node 11						
	Full conf.	Excluded line				
		L6–11	L10–11	L9–10	L5–6	L4–9
Z_S [p.u.]	0.329	0.519	0.494	0.475	0.473	0.435
φ_S [°]	66.7	66.4	67.1	65.6	60.9	63.7
E [p.u.]	1.02	0.99	1.03	1.00	0.97	0.92
φ_E [°]	–12.51	–13.12	–11.95	–13.03	–19.43	–17.04

Table 3. Node 12 Thevenin parameter changes

Node 12							
	Full conf.	Excluded line					
		L6–12	L12–13	L5–6	L6–13	L13–14	L4–9
Z_S [p.u.]	0.405	0.597	0.519	0.653	0.423	0.437	0.455
φ_S [°]	63.1	52.6	65.3	55.7	63.1	64.8	63.5
E [p.u.]	1.02	1.01	1.03	0.96	1.01	1.03	0.96
φ_E [°]	–12.27	–12.7	–11.78	–20.92	–12.78	–11.77	–15.56

Table 4. Node 13 Thevenin parameter changes

Node 13								
	Full conf.	Excluded line						
		L6–13	L12–13	L13–14	L9–14	L5–6	L4–9	L6–12
Z_S [p.u.]	0.335	0.484	0.350	0.394	0.381	0.570	0.397	0.347
φ_S [°]	66.9	60.0	66.9	68.0	66.1	59.0	66.4	66.5
E [p.u.]	1.04	1.01	1.04	1.05	1.03	0.99	0.97	1.03
φ_E [°]	–11.39	–12.12	–11.35	–10.56	–11.92	–19.22	–14.65	–11.55

Table 5. Node 14 Thevenin parameter changes

Node 14							
	Full conf.	Excluded line					
		L13–14	L9–14	L5–6	L4–9	L12–13	L6–13
Z_S [p.u.]	0.381	0.519	0.717	0.483	0.538	0.385	0.416
φ_S [°]	65.5	65.7	62.9	62.6	62.5	65.5	63.6
E [p.u.]	1.03	1.02	1.03	0.99	0.93	1.02	1.01
φ_E [°]	–11.62	–11.41	–11.95	–16.94	–16.4	–11.61	–12.09

Based on full power system model presented studies can be made for every node of power system. Obtained information can be used to calculate voltage stability margin in two ways. It is possible to assign specific values of Thevenin parameters to configuration of close environment of the considered node. To limit amount of information, the exclusions that have the greatest impact on Thevenin parameters can be chosen. Information from breakers and switches are used to update Thevenin model (Fig. 4). Basing on such approximate model and local measurements of load, voltage stability margin calculation is possible. Verification of correctness of this model can be made by comparison of measured voltage and calculated using model. If these values are close it can be assumed that parameters of model are selected correctly and voltage stability is calculated with a small error.

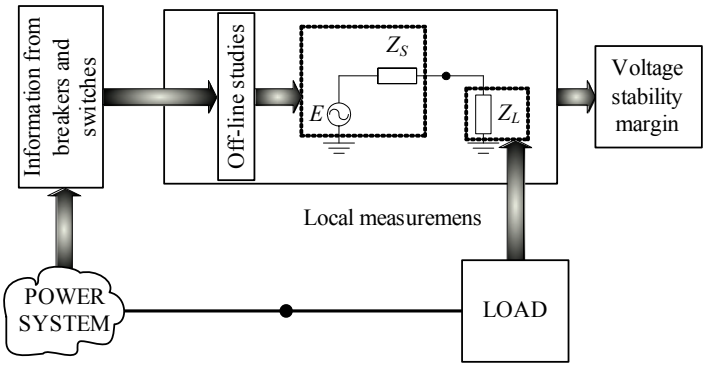


Fig. 4. Approximate model updating

Other use of determined Thevenin parameters is to calculate average value. Such value should be calculated using parameters of states that are not easily identifiable. At node 10 the most dangerous states are: exclusions of the directly connected lines (L9–10, L10–11) and break one of connection between two areas (L4–9). Information about exclusions of direct lines is always available at node. Braking of connection between areas has a major influence on Thevenin parameter changes of all considered nodes. Therefore, information about this occurrence is important and should be forwarded to those nodes. Average values calculated for receiving nodes are presented in Table 6.

Table 6. Average from selected values of Thevenin parameter changes

Avarage from selected values					
	Node				
	10	11	12	13	14
Z_S [p.u.]	0.334	0.428	0.430	0.365	0.416
φ_S [°]	67.8	64.2	63.63	66.47	64.29
E [p.u.]	1.01	0.98	1.01	1.02	1.01
φ_E [°]	–13.7	–15.5	–13.10	–12.38	–13.07

3. SIMULATION RESULTS

According to analysis presented in Chapter 2 it can be seen that variation of system parameters of Thevenin model are small when switching elements "electrically" far distant from considered receiving node are performed. In contrary, these parameters change substantially when switched are elements "electrically close" to given node, mainly connected to this node. These changes can reach over 100 percent comparing to standard configuration. Important is that these switches can be identified locally in

the receiving node. This analysis lead to the conclusion that the problem of estimation of system parameters of Thevenin model could be realised in two ways:

1. When exclusion of elements electrically far distant occurs, an average values of parameters for all configurations (single elements switching) are assumed.
2. When elements electrically close are switched off, given disconnected element is identified and adequate for this situation system parameters obtained from simulation are chosen. These parameters are used to estimate voltage stability margin directly using measured load parameters.

Node 10 of IEEE model has been chosen to perform simulations. This node was selected because during changes of configuration Thevenin parameters have changed the most. Value of system impedance Z_S has changed by about 125%. Two cases have been tested to calculate variations of voltage stability margin. Constant value is assumed average value (Table 6). In the first case correct parameters correspond to full configuration and in second to the most dangerous from among unidentified (exclusion of line L5–6). The simulations have been performed for two power factors tgφ = 0.4 (Figs. 5, 6) and tgφ = –0.2 (Figs. 7, 8). The stability margin values correspond to current configuration have been plotted by line number 1. Assumed average value is switched element plotted by line number 2.

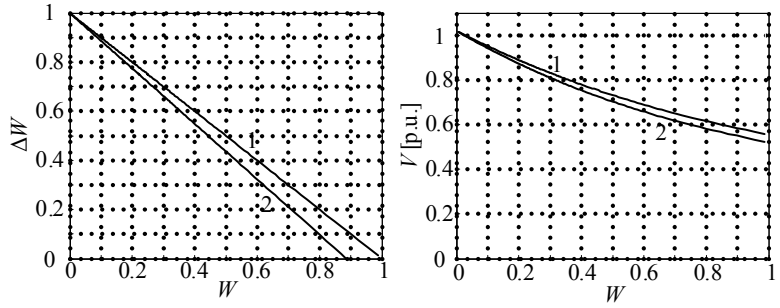


Fig. 5. Changes of stability margin and voltage tgφ = 0.4 – full configuration

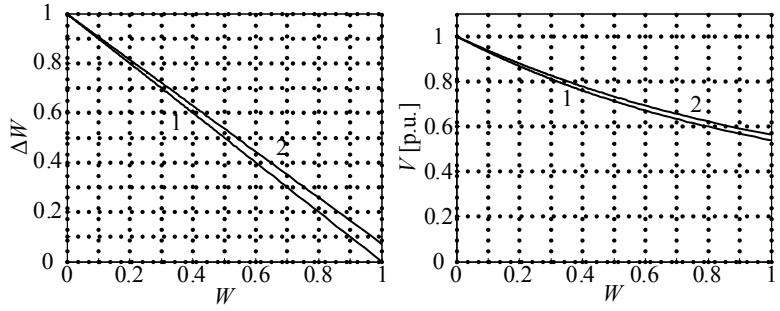


Fig. 6. Changes of stability margin and voltage tgφ = 0.4 – excluded line L5–6

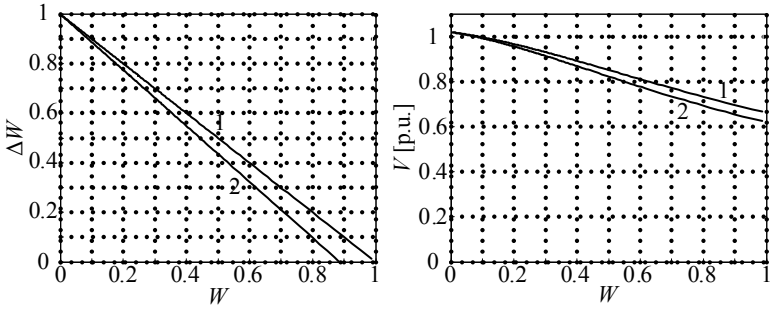


Fig. 7. Changes of stability margin and voltage tgφ = –0.2 – full configuration

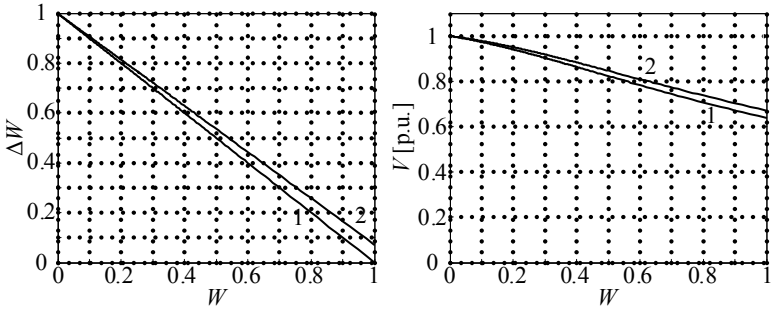


Fig. 8. Changes of stability margin and voltage tgφ = –0.2 – excluded line L5–6

System impedance Z_S for full configuration is less than average value of this parameter. Therefore, calculated stability margin is also less than exact. This is the safe case. The reverse event occurs when the exact value is correspond to exclusion of line L5-6. Calculated stability margin is higher, but we can estimate the error of calculation. In both cases, the difference grow as operating point approach to the stability limit. The values of voltage calculated using approximate model possess similar errors as stability margin estimation.

The analysis of stability conditions of receiving node should consist information about stability margin and also node voltage. These values are close connected. Assumed is often that minimum acceptable voltage value is V = 0.8 [p.u.]. For inductive load (tgφ = 0.4) this value occurs for W = 0.3. For this value stability margin estimation errors are less than 10%. For capacitive load (tgφ = –0.2) voltage value V = 0.8 [p.u.] correspond to W = 0.6. errors of stability margin estimation are about 15–30%.

In the second case when electrically close elements are disconnected (line L9–10 or L4–9) parameters of system model (receiving node 10) changes substantially (see Fig. 3 and Table 1). When disconnection of the line is identified, fix parameters obtained from simulation can be taken. By measuring load parameters voltage stability margin and voltage values can be calculate with proper accuracy. Calculated node voltage and

measured voltage can be compared, this will increase the confidence of estimated values when the difference is small.

4. CONCLUSIONS

1. A simplified method of analysis and estimation of voltage stability margin is presented in the paper.
2. Basis of this analysis is model of given part of power system. For all receiving nodes and all possible single switching processes Thevenin equivalents is calculated.
3. Simulations made for one of IEEE model reassured known fact that substantial changes of the system seen from given node are caused by switching the elements close electrically to this node.
4. Switching of elements electrically distant to given node have a small influence on Thevenin model parameters at this node.
5. Considerations and made simulations allowed to assume an average model for far distant switching. This allows to calculate voltage stability margin directly when load parameters were measured.
6. Knowing all parameters of Thevenin model, calculation of voltage and compare it with measured value is possible. Small difference of these voltage can reassure correct assumptions, modelling and calculations.
7. In case of switching electrically close elements to considered node it is possible to locally recognize what happened and substitute parameters known from modelling and simulations. Voltage stability margin can be calculated directly as well as voltage which could be compared with measured value.
8. Generally the approximated method is simpler than known ones and is independent on the type of load.

REFERENCES

[1] EN 50160, *Voltage characteristics of electricity supplied by public electricity networks.*

[2] ARAUJO F.B., PRADA R.B., *Distributed generation: Voltage stability analysis*, [in:] Proc. 2013 IEEE Grenoble PowerTech, 16–20 June 2013, pp. 1–4.

[3] ZOKA Y., YORINO N., WATANABE M., KURUSHIMA T., *An optimal decentralized control for voltage control devices by means of Multiagent System*, [in:] Proc. 18th Power Systems Computation Conference, PSCC 2014, Wrocław, Poland, August 18–22, 2014.

[4] TAYLOR C.W., ERICKSON D.C., MARTIN K.E. et al., *WACS-Wide-Area Stability and Voltage Control System: R & D and Online Demonstration*, [in:] Proc. of the IEEE, Vol. 93, Iss. 5, May 2005, pp. 892–906.

[5] SANGWOOK H., LEE B., KIM S. et al., *Voltage stability monitoring using PMU data in KEPCO system*, [in:] Proc. IEEE PES Transmission and Distribution Conference and Exposition, New Orleans, LA, USA, 19–22 April 2010, pp. 1–5.

[6] IEC 60909-0, *Short-circuit currents in three-phase a.c. systems – part 0: Calculation of currents.*
[7] WISZNIEWSKI A., *New Criteria of Voltage Stability Margin for the Purpose of Load Shedding*, IEEE Transactions on Power Delivery, Vol. 22, Iss. 3, July 2007, pp. 1367–1371.
[8] VU K. BEGOVIC M.M., NOVOSEL D., SAHA M.M., *Use of local measurements to estimate voltage stability margin*, IEEE Transactions on Power Systems, Vol. 14, Iss. 3, 1999, pp. 1029–1035.
[9] WISZNIEWSKI A., REBIZANT W., KLIMEK A., *Intelligent voltage difference control maintaining the voltage stability limit*, [in:] Proc. 43rd CIGRE Session, Paris, France, B5_107_2010, Aug. 2010.
[10] BRUSIŁOWICZ B., REBIZANT W., SZAFRAN J., *A new method of voltage stability margin estimation based on local measurements*, [in:] Proc. of the International Conference on Advanced Power System Automation and Protection APAP 2011, Beijing, China, Vol. 3, 16–20 October 2011, pp. 2443–2447.

smart power grid, digital security,
smart metering, security policy

Robert CZECHOWSKI*

SECURITY POLICY FOR LOW-VOLTAGE SMART GRIDS

Smart Grid is both a concept and a way to mitigate infrastructural deficiencies and counteract the effects of the growing demand for electrical energy. One of the ways ensuring an increase in power grid's management efficiency is utilization of the latest communication solutions by use of IT technologies. Such solutions ensure reduced energy consumption and evened 24-hour loads, decreased losses and – thanks to automated energy balancing – increased transfer security. Such solutions will directly translate into increased efficiency of the entire power grid. The present article contains an introduction to smart power grids, perspectives for their development in Poland, as well as an extended discussion of related issues concerning security on the organizational level.

1. INTRODUCTION

Development of ICT (*Information and Communication Technologies*) networks cooperating with virtually every industry sector observed in the recent decades has seen an increased use in comprehensive management in electrical energy transmission and distribution system. This development is headed to increased integration of this grid with a power system where the said grid performs more and more functions integrating the system, i.e. the SCADA (*Supervisory Control and Data Acquisition*) system supervising the technological process, PLC (*Power Line Communication*) transmission, or encryption and transmission of control commands by use of open communication standards such as PRIME (standard according to Prime Alliance). Thereby, utilization of smart solutions, predominantly those within Smart Metering, performs an increasingly important role in ensuring security and reliability of a power system, distribution grids and management of smart devices included in the "last mile", the so-called low voltage grid [1].

* Wrocław University of Technology, Department of Electrical Power Engineering, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland, e-mail: robert.czechowski@pwr.edu.pl

The amazing development of information technology and telecommunications will create new tools that can be used in the energy sector, from centralized process management, data mining to encrypted data transmission by use of PLC and cryptographic algorithms such as AES (*Advanced Encryption Standard*).

Modernization of distribution grids and replacing the traditional electricity meters with smart meters, which is the technical aspect of the modern grid, is not all. A key role that cannot be omitted in such investments is also ensuring electrical security of said grids, which will requires familiarity with many issues that are all but unknown to electrical power engineers such as security specialists. Implementation of automatic metering devices will allow for the structure of a traditional grid to resemble modern ICT (*Information and Communication Technologies*) grids. Implementation of smart power grids will require cooperation of not only electricians, who will perform the existing installation tasks, but all new specialists in widely understood information technology, from network administrators, ICT security specialists, data base and warehouse administrators, to analytics of the layer managing the processes and business layer.

The new infrastructure constructed according to the new Smart Grid concept will grant the distribution grid operators not only metering or statistical data that can be used by a given supplier to improve the quality of services or increase the income, but also new challenges related to security, which will be evident in the search for specialists and conducting specialized training courses. Integration of power and information systems will, in a couple of years, surely necessitate modernization of curricula at electrical departments in technical universities, including publishing appropriate handbooks. Changes will also include the outlook of hazards each big grid has to face, and security policies which will have to be verified in terms of new design assumptions and potential dangers [2].

If advanced automation of grids and systems is entrusted entirely to external IT companies, it will lead to nobody from the power supplier's side being fully familiar with these often complex power grids and systems, be it electricians or IT technicians. Moreover, there will be a problem of access to the structure and confidential information of the so-called third party (discussed later in this article), which poses an additional threat to the whole system due to dependency on an independent service provider. It is obvious that such a state cannot adversely affect the power infrastructure security and the power sector's subjectivity. The two above issues can be resolved by investing in own personnel through creation of an AMI (*Advanced Metering Infrastructure*) specialized team consisting of electricians and IT technicians or even better – specialists in both these areas.

Basic functionality of the AMI will ensure metering of all endpoints and intermediary points in the first and second lines, and automation of communication with them. Intrusions and tampering with such functionality usually have very little effect on the entire power system's performance. One would have a problem with not only tampering with and lowering readings of the meter, but also having to face the risk of depriving many clients of electrical power through mass disconnection of meters' power (switching the relay in the meter) [3].

Next to the completely basic functions of disabling and real-time reading, the AMI has many other functions like control of collection while changing time-zones or displaying prices according to which the automation systems can engage or disengage specific receiver through integration with e.g. the HAN (*Home Area Network*). Tampering with such functions on a large scale may lead to the power system's overload or cause problems to any given consumer by exposing them to costs they would not incur without interference of third parties [2].

One of the main hazards is the possibility of cybercriminals or cyberterrorists' interference, people who seriously impede the continued operation of computer systems and networks, or various electronic systems, depending on the scale of damage [3].

Increased automation and communication within smart grids certainly comes with many benefits, but it is not devoid of flaws, either – due to the availability of the ICT technology in a new, hitherto unknown (for such solutions) branch of industry, there will surely be individuals willing to test their skills and abilities, which will translate into these grids' increased vulnerability to attacks. Ensuring years of proper functionality of such grids, their safety and protection from cybercriminals or hackers attack becomes a serious problem [4].

Resources protected in smart power grids are: access to management software, inventory of computer equipment, company's data, personnel (including a list of ICT/AMI specialists), documentation of metering equipment, like e.g. access to the ERP (*Enterprise Resource Planning*) system and company's critical data: data concerning contractors, commercial information, data endangering the positive image, ways of unauthorized access, the so-called Information Security Policy [5].

In summary, attacks on smart power grids can be divided as follows:

a) by the attack location in the power supplier infrastructure:
   - attack on AMI devices (main meters),
   - attack on the data transmission medium, intermediate devices (active and passive),
   - attack on the operator's datacenter (extortion of passwords and access to services by use of various techniques, even bordering on social engineering, attack on access control servers, databases, warehouses and permissions);
b) by the target and scale of a potential attack:
   - attack on a single client [6],
   - attack on the functionality of the entire system or its significant portion [7].

2. DEVELOPMENTAL PERSPECTIVES OF SMART GRIDS IN POLAND

A smart power grid is a solution which proper functioning necessitates implementation of an important mechanism related to energy security, which is management

of demand and protection of one's own infrastructure. Supplying energy by use of a smart grid is related to transfer of information allowing for both continued monitoring of demand, and controlling this demand by influencing energy receivers. This will allow for flexible shaping of the demand and adapting the supply to the daily demand. In connection to the increasingly utilized energy-efficient building solutions, devices and technological processes, it leads to a large-scale increased energy efficiency and limiting one of the most serious risks which are: unsustainable energy balance and low energy efficiency.

Thanks to utilization of telecommunication measures, Smart Grid is a way to mitigate infrastructural deficiencies, current imperfections and challenges power grids, in the present form, have to face. Presently, a power grid is characterized by:

- not being able to store energy,
- having to balance production and reception,
- significant technical limitations,
- dependency of the entire economy on the energy supply and prices,
- natural monopoly.

Alteration of this model by increased investments (mainly exchanging meters and modernization of the "last kilometer" with concentrators) will ensure decreased energy usage, balanced daily loads, decreased losses, and translate into significantly increased transfer security. Moreover, the psychological factor of awareness of wasting energy or possibility of using it with decreased costs will make consumers lower their energy demand themselves. It is estimated to be 2–10%.

Table 1. Summary of estimated benefits in Poland until 2020 (* in millions of zloty) [9]

No.	Benefit	Financial dimension of the benefit*	Total*
1	Reading cost reduction	2300	**9480**
2	Savings on unproduced electric energy	2400	
3	Postponed construction of an additional electric power source	1500	
4	Postponing certain investments aimed at increasing a power grid bandwidth	600	
5	Reduction of balance differences including technical and commercial losses	2400	
6	Decreased customer service cost	280	

Estimating the tangible benefits related to reduction of the aforementioned costs to be around 9.48 billion zloty, with implementation costs around 9 billion zloty, it should be recognized that implementation of smart metering systems in Poland is

Next to the completely basic functions of disabling and real-time reading, the AMI has many other functions like control of collection while changing time-zones or displaying prices according to which the automation systems can engage or disengage specific receiver through integration with e.g. the HAN (*Home Area Network*). Tampering with such functions on a large scale may lead to the power system's overload or cause problems to any given consumer by exposing them to costs they would not incur without interference of third parties [2].

One of the main hazards is the possibility of cybercriminals or cyberterrorists' interference, people who seriously impede the continued operation of computer systems and networks, or various electronic systems, depending on the scale of damage [3].

Increased automation and communication within smart grids certainly comes with many benefits, but it is not devoid of flaws, either – due to the availability of the ICT technology in a new, hitherto unknown (for such solutions) branch of industry, there will surely be individuals willing to test their skills and abilities, which will translate into these grids' increased vulnerability to attacks. Ensuring years of proper functionality of such grids, their safety and protection from cybercriminals or hackers attack becomes a serious problem [4].

Resources protected in smart power grids are: access to management software, inventory of computer equipment, company's data, personnel (including a list of ICT/AMI specialists), documentation of metering equipment, like e.g. access to the ERP (*Enterprise Resource Planning*) system and company's critical data: data concerning contractors, commercial information, data endangering the positive image, ways of unauthorized access, the so-called Information Security Policy [5].

In summary, attacks on smart power grids can be divided as follows:

a) by the attack location in the power supplier infrastructure:
   - attack on AMI devices (main meters),
   - attack on the data transmission medium, intermediate devices (active and passive),
   - attack on the operator's datacenter (extortion of passwords and access to services by use of various techniques, even bordering on social engineering, attack on access control servers, databases, warehouses and permissions);
b) by the target and scale of a potential attack:
   - attack on a single client [6],
   - attack on the functionality of the entire system or its significant portion [7].

2. DEVELOPMENTAL PERSPECTIVES OF SMART GRIDS IN POLAND

A smart power grid is a solution which proper functioning necessitates implementation of an important mechanism related to energy security, which is management

the introduction of mobile phones for public use in social telephone communication patterns. The changes in communication system both individual consumers and public institutions. That is why the subject of Smart Grid can and should attract the interest of:

- individual energy receivers (consumers and households),
- entities included in shaping and realization of energy policy and energy planning (energy companies and industry institutions, local government).

There are certain concerns of some consumers related to implementation of smart software. The fear of energy consumption monitoring in flats or houses is so significant that it initiated protests in some countries, like in Holland [12]. However, the very same clients, when purchasing first mobile phones (by which they are under even greater surveillance), not realize the danger related to disclosure and processing of data stored by these phones.

Implementation of Smart Grid will allow for lowering the costs that sooner or later appear during a grid downtime, yet their complete removal is not possible. By use of smart grids, the risk of failure and scale of losses are lowered. That is because the solution allows for demand and supply to be addressed locally, not centrally, which has no negative effect on higher order grids. However, it requires a change of principles in functioning of the market and grid management. From this point of view, construction of smart power grid is essential for development of the economy. Quick development of smart grids will allow for:

- new technologies for electrical and heat energy generation, including renewable energy sources, like small gas turbines, small CHP(*Combined Heat and Power*) plants, fuel cells, wind energy, heat pumps,
- utilization of distributed generation resources (distributed sources, energy storage),
- ICT technologies allowing for developing new methods and systems of grid control, monitoring and security,
- production of end-use energy receivers allowing for integration with Smart end-use Devices,
- new proactive ways of energy market regulation enforcing a change in the present, unfavorable regulation principles of distributed sources,
- change in the way the end-users use energy due to increased awareness (e.g. climate policy, energy security, rising energy costs, energy saving) [8].

In the modernized Smart Grid model, the energy consumer no longer plays just the passive role of power recipient, but consciously and actively manages energy and its usage in their household (building). Grid management by the consumer, and further reshaping it – prosumer, will incorporate conscious saving by use of heating devices (with the greatest power) during the evening hours or outside the peak hours. As the target form, the consumer becomes a prosumer – a micro-scale energy producer. Investment in knowledge about Smart Grid and development of this tech-

nology and related solutions should translate into better energy usage and resultant savings (thereby, lower energy bills), as well as into a possibility of income from energy sales – in case of presumption and so-called distributed generation. Even if consumers will not transfer their generated energy surplus to the operator grid, such solution will translate into a decrease of energy drawn from the operator anyway, which will decrease the demand during peak hours. Development of smart power grids requires a conscious and active receiver and consumer of energy, also contributing to the growth of information and low-carbon society, and in the perspective of local government entities – to the growth of energetically sustainable local Smart Communities [3].

The main features of real-time Smart Management:

- bidirectional energy and information transfer,
- decentralized energy generation through micro-stations,
- communication between market entities,
- monitoring of the mains supply,
- monitoring of the peak power,
- monitoring of the infrastructure,
- ongoing energy metering,
- load reduction,
- data registration and visualization,
- gathering data on energy usage by particular receivers,
- sending control signals to devices,
- their remote configuration.

The following definition of a smart power grid is widely accepted: an electrical grid able to harmoniously integrate behavior and actions of all users connected to it: generators, receivers and those who perform both these roles – in order to ensure sustainable, economic and reliable power while retaining a level of security appropriate for the process.

In order to ensure security in widely understood transmission of electricity, it is necessary to utilize an advanced AMI metering infrastructure which is an integrated collection of elements:

- smart electricity meters,
- communication modules and systems suing the existing electrical grid for transmission,
- concentrators and recorders allowing for bidirectional communication through various media and technologies between the central system and selected meters,
- communication modules and systems interchangeably using the power suppliers transmission medium with another one which directly allows for most commonly wireless connection with the operator's datacenter.

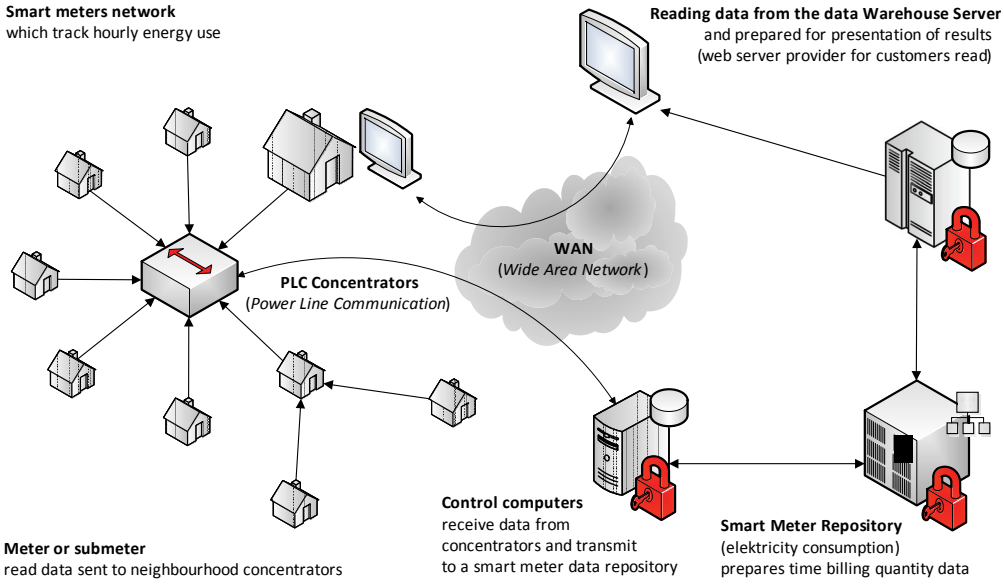


Fig. 1. Paths of information flow in smart grid

One of the main elements of the Smart Grid's functionality is the SM (*Smart Metering*) system – a system allowing for metering, gathering and analysis of energy usage. It consists of energy meters, communication media and software. The system is based on:

- metrology – data gathering and processing,
- telecommunication and computer networks – data transfer,
- computer science and information hardware technology – data processing, storage and presentation.

Intended targets for smart metering:

- creation of a demand management system,
- rationalization of electricity consumption,
- development of a competitive electricity market due to implementation of settlements according to an actual usage profile,
- facilitated switching of suppliers,
- ensuring information on current energy usage in order to allow for energy savings and increased efficiency of its use,
- limited environmental impact of energy,
- introduction of an obligation to use electronic meters allowing for transmission of price signals to energy receivers,
- introduction of nationwide standards related to technical features, installation and reading of electronic electricity power meters [13].

Implementation of a smart grid system presents an opportunity to demonopolize the electric energy market, to regain civil control over the energy sector. However, Smart power grids cannot operate without telecommunication networks.

3. HAZARDS AND SECURITY OF THE SMART GRID

3.1. INTRODUCTION TO SECURITY

The subject of smart grids has long been taking the leading position in programs and publications related to grid development. Smart grids indicate wide application of innovative solutions, from automated electricity meter readings to full utilization of databases' functionality. These solutions will relate to new innovative uses in most of the already existing technologies, in electrical, IT grids and within the energy market. Smart grids are not only a modern infrastructure , but new products and services offered for the benefit of the customer, which will allow for more efficient management of the power grid. The role of the operator is to ensure a modern, energetically efficient and productive infrastructure allowing service and energy providers for unhindered competitive activities in the conditions of growing participation of distributed generation and the active role of energy consumers [14].

Unlike typical acts of mechanical sabotage, an attack on an electronic energy distribution grid can be carried out with little resources, in a coordinated and very precise way. Moreover, it can be initiated via a public network from remote places and performed in the form of a coordinated attack from multiple places at once. Several places can be attacked simultaneously, which can more quickly contribute to discovering weaknesses of the entire security system [1].

In order to maintain a high level of security, it is necessary to observe predefined procedures and security policies. A grid of meters and concentrators is starting to look more and more like a traditional corporate network, which means that similar security measures can be put in place, including systems for intruder detection, access control and event monitoring. Especially vulnerable to packet data attacks are concentrators which, connected to Ethernet switches, utilize the commonly used TCP/IP protocol [1].

Transformation of the current grid structure into a smart grid necessitates a series of novel security solutions borrowed from already used ones. Typical problems of modern computing include hacking, data theft, and even cyberterrorism, which will sooner or later also affect power grids.

Introduction of smart power grids through installation of remote reading meters, electronic grid elements, construction of new information systems consisting of data on energy usage causes energeticists many new security-related problems. A complex multi-layered security system requires an overall concept of providing information security.

Security in Smart Grid can be divided into three groups:

a) by the continuity and security of services:
   - ensuring continued electrical energy supply at a contractually guaranteed level, binding the supplier and customer (it also concerns cases of bidirectional energy transfer – smart grids with the participation of prosumer),
   - ensuring confidentiality of information on clients and security of statistical data generated by them, such as "consumption amount", time of the greatest energy demand or its total absence,
   - security related to energy distribution management process, and telemetry and personal data protection in datacenters;
b) by security class:
   - protection from unauthorized access to digital data transmission media and physical security of devices in intermediate stations,
   - protection of end-use telemetric devices from unauthorized access, transmission disruption or complete lock of their activities,
   - analytical optimization models and decision-making processes;
c) by policy:
   - data access policy – user authorization, permission management,
   - management security policy – investment processes' principles and rules,
   - system security policy – reaction to incidents, managing confidential information like passwords, cryptographic keys.

Introduction of smart software will contribute to intensified attacks on that grid due to the appearance of a new attack target with a very specific, hitherto unknown architecture which will be a challenge, especially for specialists in computer networks and hosting. ICT systems containing crucial statistical or personal data in one place are particularly exposed to attacks, which will be performed over a computer database on the grid operator's center. If some grid security measures are broken at that time, especially devices responsible for communication and access to concentrators there will not be a possibility to replace them. The learning and dissemination of an effective method to break the security algorithms will not only undermine the entire system, but also entail more expenditures [15]. This happens because there is no technical possibility to easily and cheaply replace these devices software in terms of increased security during access authorization to data and device control. The only possibility of continuous care for a high level of security of these devices is firmware update, and utilization of authentication and encryption based on ID, serial number, password or hash unique to that device and known only to the operator. Based on a given meter's ID, the grid operator can generate a unique code (intended solely for communication with that device only) allowing for further authorization.

Unsecured smart grids implemented today might result in a disaster in the future. A person able to bidirectionally transmit data in metering and billing systems can, to a degree, control pre-payment meters and their internal power disconnection mecha-

nisms. Moreover, they can change the tariff assigned to a meter, and make other changes inconvenient to the consumer and expose them to additional expenses.

Utilization of standard information technologies in power systems is a certain benefit, but it also makes these systems vulnerable to capture. It especially concerns communication standards like PRIME, a fully open, low voltage power line communication standard, available free of charge. The main reasons for arising vulnerabilities in a secured infrastructure are:

- implementation errors,
- closed and poorly tested software,
- errors in system design and security management,
- utilization of obsolete or poorly tested technologies,
- disregard of information security issues.

Utilized solutions have to ensure enough security so even despite a successful attack on one of the grid component, subsequent security breaks do not entail escalating loss of trust in further equipment or services. When designing a secure power grid, one should assume that it will sooner or later be under an attack by a cybercriminal who is familiar with widely used security measures of ICT systems and has enough practical skills to be able to bypass them and properly authorize his or her access to the Smart Grid [1].

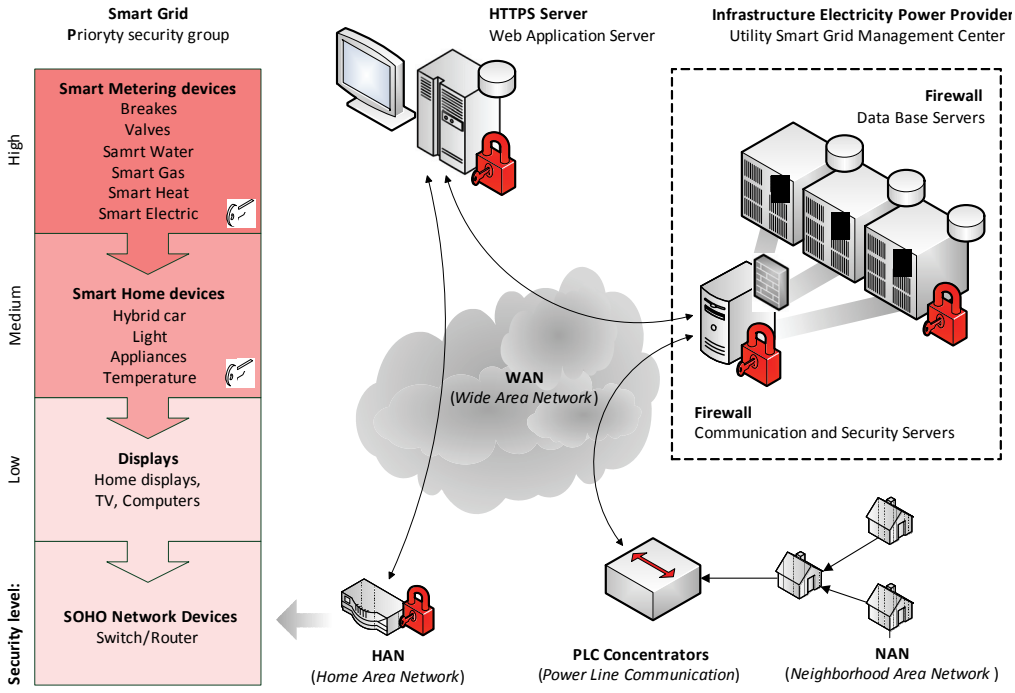


Fig. 2. Smart Grid security model

Such actions may be done via uploading malicious software. That is why proper certifications and advanced authentication methods are required. Unfortunately, these aspects are often disregarded by beginner installers and system administrators, which puts the system at risk of serious consequences already at the initial implementation phase. As indicated by experience from very well secured systems (even the banking ones witch specifics make them considered most secure), not even the best security measures are unbreakable. Using any security means is definitely better than not using one, even if they fail to prevent, they at least significantly impede and limit unauthorized access to the smart grid unauthorized people with average skills and knowledge. It is worth noticing that even average security measures significantly prevent form a successful attack by people who should not have such access at all. It is much more difficult to defend yourself against people with much experience who have previously performed successful attacks of that nature, on grids with similar structure and operating principle. In case of an attack by an "proficient specialist", successful defense depends on multiplicity of mechanisms with various principle of operation, which will ensure enough time for the intrusion prevention or intrusion detection systems to kick in. These systems will be discussed widely in further author works.

3.2. THREAT CLASSIFICATION

Some users are concerned with lack of control over gathering, processing, accessing and using sensitive personal data. The problem, of course, is a little more extensive to this and also concerns unauthorized gathering, acquiring, using and disclosing information obtained by inference from the so-called metadata. That is why it is necessary to implement a comprehensive security strategy for information transfer, personal and telemetry security. Smart Grid and Smart Metering, which simultaneously identify specific devices and their utilization, can disclose clients' profiles and pose new threats to their privacy, such as:

- identity theft,
- disclosure of personal behavioral patterns,
- gathering and grouping consumers by behavioral patterns,
- possibility of disclosure of controlled devices located in a given house or apartment,
- real-time usage monitoring – danger of revealing a consumer's absence in a house or apartment,
- manipulating energy prices transferred to a meter; e.g. transferring a significantly lowered price of energy during peak hours and displaying it for many consumers can cause even a significant shift in behavior in terms of energy usage, a significant increase in energy consumption by many consumers deceived that way might be dangerous to the grid.

3.3. THREAT SOURCES

The growing energy telecommunication grid is increasingly vulnerable to actions that could disrupt its operation. It is possible to both intercept important information, especially of administrative nature, related to energy commerce, and perform an attack to block the functioning of a given grid portion or service (like access to the database server). What may be particularly dangerous is a potential blockade of real-time information transferring grid functionality related to security and control. Intrusions to the grid can also be performed by authorized users from within the system.

The most common threats to information systems include [2]:

- blocking access to a service,
- hacking into an information system's infrastructure,
- data loss,
- data theft,
- confidential data disclosure,
- information falsification,
- software code theft,
- hardware theft,
- damage to computer systems.

Making an ICT power grid available for the needs of external users is a potential source of threat. It is necessary to separate information transferred for the needs of the power sector to the eternal traffic. Moreover, the administrative and office traffic should also be separated from traffic related to remote supervision over energy facilities. The most commonly encountered problems related to incorrect grid architecture design and its management are:

- lack of proper security architecture,
- errors in information security management,
- software errors,
- human errors and intentional actions,
- insufficient security monitoring.

Lack of clear separation of these grids could potentially cause an intrusion into a power plant control system or a distribution system by way of access through the administrative network, or cause actions blockade and deletion of data from the SCADA system. The causes of such threats are found in:

- vulnerabilities of operating systems which are potential targets for hackers attacks,
- unsatisfied employees, e.g. a fired employee might attempt hacking for revenge or sabotage, incorrectly installing antivirus software and planting malicious software that will cause damage within the smart grid.

4. SECURITY POLICY

4.1. INTRODUCTION TO SECURITY

Systems performing security-related functions consist of such elements as: sensors, programmable devices, communication systems, actuators and power. Abuse related to ICT systems security and failures are becoming increasingly commonplace, possibly resulting in enormous financial losses, lost reputation, high repair costs and even business failure [1].

Smart Grids are of ever more significant strategic value in terms of energy security. A smart grid is a modernization of existing power grids, but it will be subject to the same elementary requirements put forwards for computer networks. In order to ensure basic security, all of the below conditions have to be met:

- confidentiality – ensuring the information is available only to authorized individuals,
- integrity – ensuring accuracy and completeness of information and processing methods,
- availability – ensuring that the authorized individuals have access to information and related assets when it is needed.

In case of violation or failure in meeting the above key norms of AMI systems security infrastructure management, the following rules should be observed:

- each change system configuration requires verification for compliance with security policy,
- failure to observe the system's security policy norms should cause it to be physically disconnected from the grid,
- decision to connect or disconnect the system should me bade by authorized individuals.

Moreover, one should follow a principle of assigning permissions for applications, grid active devices and database systems with regard to permission hierarchy of people managing the entire power system. Access to the resources should only be limited to people allowed to have it. One should also determine:

- the level of acceptable risk,
- access control mechanisms,
- access authorization and identification mechanisms,
- recording changes made within the system: regarding configuration and data modification.

Moreover, it becomes increasingly important to ensure data verification, reliability and security. In order to decrease the amount of incorrect data, grids are secured from attempts to hack and manipulate data hackers should have no access to. Security policy procedures that hamper the work of normal application users are constantly added to. It is not difficult to predict the consequences of such a security policy. Security of

a system protected this way becomes more and more unattainable. That is why user authorization or access control that differs from statistical passwords becomes the increasingly important [1].

A power system can be considered as one of the most critical systems of strategic importance in functioning of the entire country. Inactivity or destruction of such a system would weaken national security or economic and social wellbeing of the society and its neighbors, both in the physical world and cyberspace.

Protection of the most important infrastructures includes:

- physical security encompassing all predictable threats regarding human errors, systems protection from physical destruction or tampering e.g. with the circuitry, and natural disasters,
- cyber security, a security policy which, apart from the organizational concept of security supervision, includes legal regulations, research work, training courses, etc.

Presently, the functioning of a power grid and efficient control of its operation depend on various computers, computer networks, software and communication technologies, from the point of view of efficient control. While creating one's own security policy, it is a very good practice to place oneself in the role of an attacker. It allows for avoiding the most common mistakes, at the designing stage. Unauthorized interference of a cybercriminal with a computerized power infrastructure may lead to enormous losses resulting both directly (e.g. inability of the enterprise to perform daily operation) and indirectly (e.g. failure to carry out contracts on time, loss of company good image) from power shortage of particular consumers [16].

4.2. SECURITY POLICY MODEL

A critical and often neglected component of this process is a security policy which usually takes the following form: threat model – security policy – security mechanisms.

Security policy is understood as a document which clearly and concisely states the intended tasks of security mechanisms. It results from our understanding of the threats and is a key influence on the construction of our systems. A security policy often takes the form of certain statements regarding which users can have access to which data. It plays the same role in both specifying the requirements of the security system and assessment whether these requirements have been met, similarly to system specification in regards to overall functionality. Indeed, a security policy can be a part of system specification and, just like specification, its main role is to maintain communication.

Security policy model is a concise expression of security properties that are to be present in a system or a generic system type. It is a document in which the entire environment or customer management agrees on security goals. It can also be the basis for a formal mathematical analysis. Security goal is a more detailed description of security

mechanisms ensured by specific implementation and their relation to the security goals list. Finally, there is also third the use of the term "security policy" which refers to a list of configuration settings of a security-related product [17].

4.3. MONITORING SYSTEMS

A significant number of secured systems is related to environment monitoring. The most obvious example are electricity consumption meters.

We focus mainly on attacks on communication means (although damaging meters is also somewhat of a concern), but many other monitoring systems are very vulnerable to physical damage. Water, energy and gas consumption meters are usually located within rooms belonging to consumers who may have reasons to cause incorrect meter readings. Such devices are also at a great risk of tampering. In both metering and monitoring systems, we have to provide evidence in order to prove tampering. The opponent could gain the upper hand by not only falsifying communication (e.g. by repeating old messages) but also falsely stating that someone else has done it.

Monitoring systems are also important due to having much in common with systems designed for protection of intellectual property of software and other digital media. They also make for a slight introduction to a wider range of issues related to denial of service attacks, dominating in the industry revolving around electronic threats and beginning to be a serious concern for companies dealing with e-commerce [18].

5. CONCLUSION

5.1. POWER GRID FAILURES

Power grids with transformer stations as nodes and high-voltage lines as edges (in graphical representation) often fall to local failures. Still, in most cases damage resulting in failures of individual stations or transmission lines does not have any significant impact on the functioning of the entire grid. The role of the station (or line) that has been damaged is temporarily taken by a neighboring station (accordingly parallel), and the entire system operates properly. From time to time, however, there are such failures in a power grid where a single failure triggers a cascade of further events and causes transformer stations in large geographical areas to shut down, resulting in enormous financial losses [19].

5.2. CYBERTERRORISM

It is quite a challenge to protect each and every one of extensive distribution systems, with cyberterrorism becoming a particularly serious problem. These days, destroying important objects (factories and power plants, but also computer databases)

does not require significant power or resources. Examples show that a single person with proper knowledge and access to computer technology is able to perform a successful attack on a power grid. Additionally, cyberterrorism is cheap, it does not put the perpetrator in immediate danger and can be catastrophic in results. By disrupting the operation of banking computer systems, a cyberterrorist could cause a collapse of the world economy. By introducing false data into systems managing a military, power and fuel infrastructure, they could initiate explosions of pipelines, demolition of water intakes and destruction of nuclear power plants [19].

5.3. DATA SECURITY

From the perspective of data security, The Internet technologies have to abide by the same rules that apply to processing any data. On one hand, generally accepted and still applicable requirements for security-related applications, on the other – requirements regulated by law.

The law of the Republic of Poland encompasses many more or less precise regulations regarding availability, confidentiality and integrity of data process on The Internet. The most numerous ones are confidentiality provisions which not respected results in many sanctions. That is why data security is often limited to confidentiality, protection from unauthorized access. Protected must be encompass content (information, data), possibly other computer system assets which open or close the way to content of shared or otherwise compiled resources. Therefore, practical data security, also in line with provisions of law, includes any and all means and actions undertaken to achieve a predetermined goal [20].

REFERENCES

[1] FLICK T., MOREHOUSE J., *Securing the Smart Grid. Next Generation Power Grid Security*, Elsevier, Inc., 2011.
[2] WILCZYŃSKI A., TYMOREK A., *Rola i cechy systemów informacyjnych w elektroenergetyce*, Rynek Energii, 2 (87), 2010.
[3] BILLEWICZ K., *Samrt metering*. *Inteligentny system pomiarowy*, Politechnika Wrocławska, Instytut Energoelektryki, Wydawnictwo Naukowe PWN, Warszawa 2012.
[4] BALL P., *Masa krytyczna*, Wydawnictwo Insignis, Kraków 2007.
[5] BILLEWICZ K., *Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach*, Instytut Energoelektryki, Politechnika Wrocławska, Wrocław 2012.
[6] Electronic Privacy information Center, Concerning Privacy and Smart Grid Technology, *The Smart Grid and Privacy*, dostępne w: epic.org/privacy/smartgrid/smartgrid.html, 27.11.2014.
[7] PARKS R.C., *Advanced Metering Infrastructure – Security Considerations*, SANDIA REPORT, Sandia National Laboratories, November 2007.
[8] Urząd Regulacji Energetyki, *Inteligentne sieci – szansa na zwiększenie efektywności energetycznej*, data publikacji: 28.10.2009.
[9] Ministerstwo Gospodarki, Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej, *Analiza w zakresie ekonomicznej oceny zasadności wprowadzenia inteligentnych form pomiaru zużycia energii elektrycznej w Polsce*, dostępne w: *Bezpieczeństwo gospodarcze/Energetyka/Inteligentne sieci*, 2012.

[10] Ministerstwo Gospodarki, *Polityka energetyczna Polski do 2030 roku*. Załącznik do uchwały nr 202/2009 Rady Ministrów, Dokument przyjęty przez Radę Ministrów w dniu 10 listopada 2009 roku.
[11] Ministerstwo Środowiska, *Pakiet wyzwań – Polska wdraża pakiet klimatyczno-energetyczny – podsumowanie*, Warszawa 2013.
[12] Urząd Regulacji Energetyki, *Inteligentne sieci – Rynek, konsument i zasada zrównoważonego rozwoju*, Warszawa 2012.
[13] Ministerstwo Gospodarki Departament Energetyki, *Perspektywy rozwoju systemu inteligentnego opomiarowania w Polsce*, 28.10.2009.
[14] CZYŻEWSKI R., BABŚ A., MADAJEWSKI K., *Sieci inteligentne – wybrane cele i kierunki działania operatora systemu dystrybucyjnego*, Acta Energetica, nr 1, 2012, 30–35.
[15] A.T. Kearney GmbH, Raport Technologiczny, *Infrastruktura Sieci Domowej (ISD) w ramach Inteligentnych Sieci* (*HAN within Smart Grids*), 2012.
[16] ŻURAKOWSKI Z., *Safety and Security Issues in Electric Power Industry*, 19th International Conference SAFECOMP 2000, Rotterdam, The Netherlands, October 2000.
[17] ANDERSON R.J., *Inżynieria zabezpieczeń (Model polityki bezpieczeństwa)*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.
[18] ANDERSON R.J., *Inżynieria zabezpieczeń (Systemy monitorujące)*. Wydawnictwo Naukowo-Techniczne, Warszawa 2005,
[19] Fronczak A., Fronczak P., *Świat sieci złożonych*. *Od fizyki do Internetu*, Wydawnictwo Naukowe PWN, Warszawa 2009.
[20] ANDERSON R.J., *Inżynieria zabezpieczeń* (*Bezpieczeństwo danych)*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.