



VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Toni Puromäki

DATA VALIDATION IN SCADA SYSTEM

Tekniikka ja liikenne
2010

PREFACE

I would like to thank Harri Paulasaari from ABB who gave the possibility to make this thesis and for introductions which he gave me. I would also like to thank Jari Koski from Vaasan ammattikorkeakoulu, University of Applied Sciences who supported me and gave advice for this thesis. Finally, thanks for everyone who feels that he or she has contributed to my thesis.

Toni Puromäki

VAASAN AMMATTIKORKEAKOULU

Sähkötekniikan koulutusohjelma

TIIVISTELMÄ

| | |
|--------------------|---|
| Tekijä | Toni Puromäki |
| Opinnäytetyön nimi | Tiedon oikeellisuuden todentaminen SCADA ympäristössä |
| Vuosi | 2010 |
| Kieli | englanti |
| Sivumäärä | 70 |
| Ohjaaja | Jari Koski |

Tämä opinnäytetyö on tehty ABB Oy:lle, Sähkönjakelun automaatiojärjestelmät - yksikköön.

Työssä selvitetään kuinka tiedon oikeellisuus voidaan todentaa luotettavasti ja mitä mahdollisuuksia todentamiseen on SCADA-järjestelmässä. Työn painopisteenä on teoreettisen osan selvittäminen siten, että joitain osia teoriasta voidaan soveltaa käytäntöön MicroSCADA-järjestelmässä.

Teoriaosuus keskittyy kommunikaatiossa käytettäviin todentamisrutiineihin sekä sellaisiin älykkäiden kenttälaitteiden (IED) luomiin mahdollisuuksiin, joita voidaan hyödyntää monitoroinnissa ja valvomon käyttöliittymän luomisessa.

Viimeinen osa esittelee muutaman tiedon oikeellisuuden todentamisrutiinin käytännön toteutusta MicroSCADA-järjestelmässä.

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Sähkötekniikan koulutusohjelma

ABSTRACT

| | |
|--------------------|---------------------------------|
| Author | Toni Puromäki |
| Title | Data Validation in SCADA System |
| Year | 2010 |
| Language | English |
| Pages | 70 |
| Name of Supervisor | Jari Koski |

This thesis has been made for ABB Oy, Substation Automation Systems.

The purpose of this thesis was to clarify the possibilities for data validation in the SCADA system. The emphasis of this thesis was clarify theoretically basic validation routines that are in use but also other possibilities what could be implemented to the MicroSCADA

The first part deals with SCADA system in general and clarifies abstracts, needs and challenges including in the SCADA. The second part concentrates on data transfer and communication and clarifies how the validation is executed in the protocols. Third part discussed Intelligent Electronic Devices and monitoring systems but also possibilities which these two can create if they are use together.

As a result of the thesis routines are presented which have been chosen to be implemented to the MicroSCADA system.

Keywords: Data, IED, Monitoring, SCADA, data validation

TERMS AND DEFINITIONS

| | |
|-------|--|
| ABB | ABB is a global company in power and automation technologies |
| AC | Alternating Current |
| CB | Circuit Breaker |
| CBM | Circuit Breaker Monitor |
| CT | Current Transformer |
| DC | Direct Current, Disconnecter |
| DFR | Digital Fault Recorder |
| DI | Digital Input |
| DO | Digital Output |
| DPR | Digital Protective Relay |
| DR | Disturbance recorder |
| IEC | The International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IEEE | Institution of Electrical and Electronics Engineering |
| KCL | Kirchhoff's Current Law |
| MADMD | Maximum Allowable Double Measurement Discrepancy |

| | |
|-------|--|
| PLC | Programmable logic controller |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control And Data Acquisition |
| VT | Voltage Transformer |

Table of Contents

| | |
|---|----|
| PREFACE | 2 |
| TIIVISTELMÄ | 3 |
| ABSTRACT | 4 |
| TERMS AND DEFINITIONS | 5 |
| 1 INTRODUCTION | 9 |
| 2 BACKGROUND | 10 |
| 2.1 Knowledge, Information and Data | 10 |
| 2.2 Validation | 12 |
| 2.3 SCADA System | 13 |
| 2.4 Requirements for SCADA | 14 |
| 2.5 Challenges | 15 |
| 3 DATA TRANSFER AND COMMUNICATION | 17 |
| 3.1 Overview | 17 |
| 3.2 Network Topologies | 18 |
| 3.3 Communication | 18 |
| 3.4 TCP/IP Network and IEC 61850 | 21 |
| 3.5 Error Detection in Data Transfer | 22 |
| 3.5.1 Checksum | 23 |
| 3.5.2 Cyclic Redundancy Check | 23 |
| 3.5.3 Hamming Distance | 24 |
| 4 DATA SOURCES AND CONDITIONING | 25 |
| 4.1 Instrument Transformers - Analog Inputs | 25 |
| 4.1.1 Current Transformers | 26 |
| 4.1.2 Voltage Transformers | 27 |
| 4.2 Interferences and Coupling | 27 |
| 4.2.1 Sources | 28 |

| | | |
|-------|---|----|
| 4.2.2 | Coupling..... | 28 |
| 4.3 | Digital Inputs | 30 |
| 4.4 | Filtering..... | 30 |
| 4.4.1 | Analog Signal Filtering of AC Signals | 32 |
| 4.4.2 | Digital Signal Filtering of AC Signals | 33 |
| 4.5 | Intelligent Electronic Devices..... | 34 |
| 4.5.1 | Overcurrent Protection | 35 |
| 4.5.2 | Differential Protection..... | 36 |
| 4.5.3 | Unbalance Protection | 37 |
| 4.5.4 | Earth Fault Protection..... | 39 |
| 5 | TOPOLOGY MONITORING IN REAL-TIME..... | 41 |
| 5.1 | Monitoring | 43 |
| 5.1.1 | Multiple and Redundant Information..... | 43 |
| 5.1.2 | Circuit Breaker Status Monitoring..... | 45 |
| 5.2 | Signal Selection for Topology | 46 |
| 5.3 | Data Validation | 46 |
| 5.3.1 | Check Using Redundant Current Measurements | 48 |
| 5.3.2 | Check Using Measurements Without Redundant Information | 50 |
| 5.3.3 | Check Using Kirchoff's Current Law..... | 51 |
| 5.3.4 | Check of the Feeder Status..... | 53 |
| 5.3.5 | Check of Feeder Currents and Topology Data..... | 56 |
| 5.3.6 | Time-Series Consistency Check..... | 59 |
| 6 | IMPLEMENTATION OF DATA VALIDATION IN MICROSCADA . | 62 |
| 6.1 | Power Balance | 62 |
| 6.2 | Equivalent Breaker - Phase Currents | 66 |
| 6.3 | Primary Measurements | 67 |
| 7 | CONCLUSION | 69 |

REFERENCES

1 INTRODUCTION

In computer sciences data validation (DV) is a commonly used term of ensuring that a program or application operates correctly and reliably. Typically DV consist of certain routines or methods which ensure a correctness of the input signal. Incorrect or invalid data can be replaced by a new one, it can be marked as suspicious or the value is eliminated.

In the power system DV can be done in several automation levels and DV is not unambiguous. The characteristics of the process are miscellaneous in power system so the DV should be built in such a way that it can separate the changes between normal and fault state.

This thesis consists of four parts. The first part represents some typical requirements for Supervisory Control And Data Acquisition (SCADA) system and some typical problems existing. The second part deals with data signals and communications. This part introduces data signals and some communications methods but also how the data is typically validated in protocols. The third part handles Intelligent Electronic Devices (IEDs) in general and discusses some possibilities how these devices can be used in DV. Real-time monitoring and data acquisition are also dealt with in such a way, how to build a reliable monitoring system. The last part of this thesis presents the data validation routines implemented into MicroSCADA.

2 BACKGROUND

This chapter introduces shortly some terms and concepts related to the data validation so that it is easier to understand what the data validation means and why it is important.

2.1 Knowledge, Information and Data

Knowledge is defined by Collins Cobuild English Language Dictionary as:

”Knowledge is information and understanding about subject which a person has in his or her mind or which is shared by all human beings.”(Collins Cobuild 1987, 803)

Based on this definition knowledge can be thought a as consisting of the information e.g. what we can see on computer’s screen.

In the same dictionary the information is defined as follow:

”If you have information on or about something, you know something about it.”(Collins Cobuild 1987, 748)

Based on these two definitions the data can be understood. The definition of the data is:

”Data is information, usually in the form of facts or statistics that you can analyze, or that you use to do further calculations”(Collins Cobuild 1987, 357)

The conclusion is that data does not take a stand on information which information, which it encases. The data transfer is needed if the information is wanted to move from one location to another. If the contents of the data have been inter-

preted and understood, it can be called information. The interpretation can be executed in many ways:

- In the ear the pressure waves are interpreted into the electrical impulses and the brains create the information based on these impulses
- People have been agreed that certain sounds consist of certain words and these certain words transmit the information
- Information between electronic devices consists of bits, bytes and words
- That transceiver and receiver could understand each other their language must be the same. This common language is called protocol. (Nieminen 2008)

The figure 1 clarifies the terms explained above.

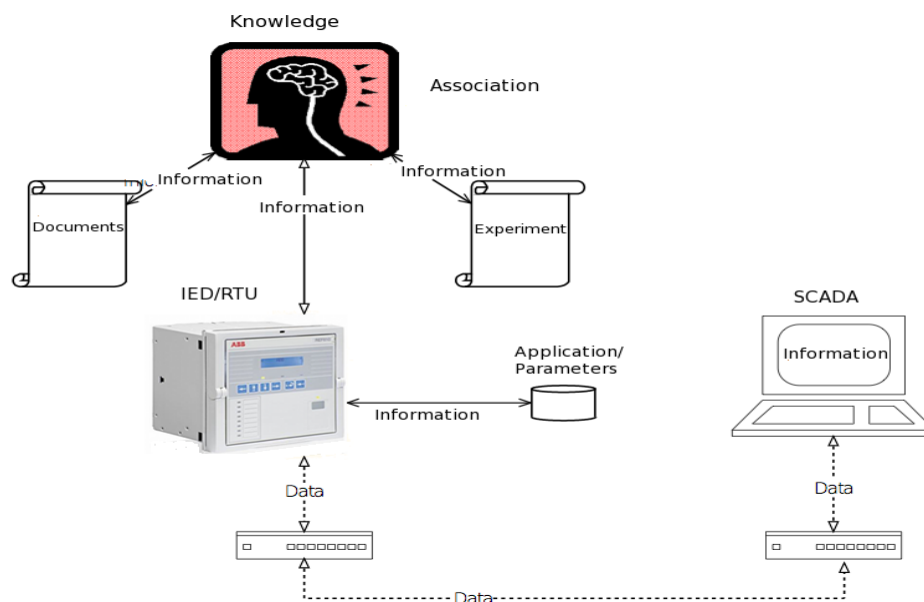


Figure 1: Knowledge – Information – Data. (Nieminen 2008)

Data is typically the result of different measurements and can be the basis for graphs, images, or observations of variables which finally create the functional applications.

In the SCADA system the data is collected from IEDs or RTUs. The SCADA application and IEDs create the information on their screens and the operator associates as understanding of the state of the process.

2.2 Validation

A following statement clarifies the meaning of the validation:

”To validate a statement or claim means to prove
or confirm that it is true or correct; A fairly formal word.”
(Collins Cobuild 1987, 1615)

Consequently, the validation is the process of checking if something meets a certain criterion.

In engineering or as part of a quality management system, validation confirms that the needs of an external customer or user of a product, service, or system are met. The validation is ensuring "Am I building the right product?"

In computer terminology, validation refers to the process of data validation, ensuring that data inserted into an application satisfies pre-determined requirements i.e. stated length, character requirements and other defined input criteria. It may also ensure that only data that is either true or real can be entered into a database. Validation refers to finding out bugs in the hardware but also proving absence of certain critical bugs which may not have workarounds and may lead to project cancellation or product recall. Table 1 defines some typical validation routines used in computer sciences:

Table1: Typical validation routines in computers

| Method | Description |
|----------------|--|
| Range check | This checks that the data lies within a specified range of values. |
| Presence check | This checks that important data is actually there and has not been missed out. |
| Type check | A check that data is of the right type. |
| Length check | Checks that fields have the correct number of characters. |
| Check digits | Used for numerical data. |
| Batch totals | This checks for missing records. |
| Hash totals | This is just a batch total done on a meaningless field. |

2.3 SCADA System

SCADA is an abbreviation from words Supervisory Control And Data Acquisition. SCADA systems are composed of networks, electronic devices, measuring sensors, switching devices etc. The structure of the system enables to control and manage processes locally or remotely, analyze the data, generate alarms and send them to different locations etc. The term SCADA is often used to define the system that are geographically dispersed.

A legacy system consists of a central host or master, one or more data gathering and control units, also known as RTUs, and a collection of standard and/or custom software used to monitor and control remotely located field data elements. Figure 2 shows a typical structure of modern SCADA for electrical transmission and distribution.

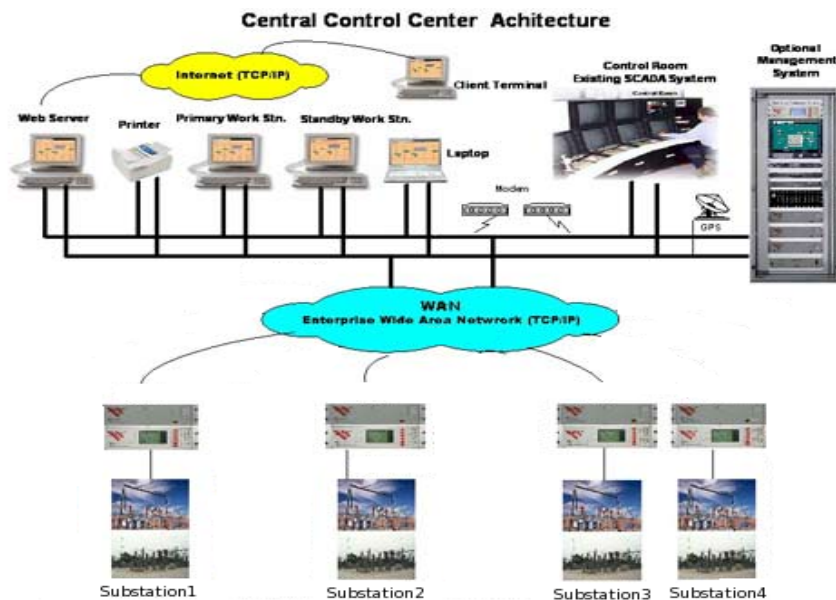


Figure 2: SCADA system example. (Fortune Automation, 2010)

2.4 Requirements for SCADA

The abnormal electrical conditions in the power system are detected and handled by protection relays. The ability to correctly restore power system back to the normal operation heavily depends on both a configuration of the relays and understanding of the power system topology. (Djokic et al, 2005, 2)

End-users and electric utilities are becoming increasingly concerned about quality and reliability of the power system and all disturbances decrease the total quality of the electricity. Automation has replaced a local maintenance staff at the substation and automation has also increased the reliability of the distribution but it cannot make controls and operations without right parameterization and configuration of the applications and devices. In order to handle these things the maintenance staff in the control room must still have a good perception of the power system.

As a result of the technology developments, new requirements for monitoring and control can be defined. The system changes should be tracked and monitored very closely, reliably and events and consequences are needed to analyze automatically so that it enables to react to system changes quickly. This creates pressure to the applications and device vendors. Nowadays the situation at the substation is quite challenging especially for the system integrators because of a wide range of the different devices and vendors. This creates needs to develop controls and monitoring systems continuously.

2.5 Challenges

A power system topology is defined by i.e. the circuit breaker status. The system topology is updated automatically by the operation of the protection relays or in some cases it is made manually. No matter what the convention is, it is possible that topological data does not reflect the real switching status of power devices in the field. (Djokic et al. 2005, 2) If the measurement value is bad it could cause a remarkable error in the long time period. Wrong energy measurement causes errors in daily, monthly and yearly reports.

The operators may also have difficulties to make decisions to restore portions of the power system that may have been automatically disconnected by the intelligent electronic devices (IEDs), especially if the operators do not have a clear way of verifying the system conditions or related topology. (Djokic et al. 2005, 1) The problem with SCADA is not a lack of the data. There is more data available than it is utilized but the problem is how to use it rationally.

Old RTUs are not designed to track the analog measurements in true real time. Only the reporting by exception when certain thresholds are exceeded is implemented. During electrical faults in the network e.g. short circuit fault, analog sig-

nals change very quickly, and only a closer tracking can give the information about the phase relationships and dynamic changes in the signal magnitudes. If the faults are needed to detect with RTUs the external disturbance recorders have to be used. If new IEDs are used, it gives more opportunities to react the faults and get robust information. (Djokic et al. 2005, 1)

One major problem is also the incompatibility of devices and non-existence of a relevant standard that would unify forms of data produced by the variety of devices. The information from devices differs between protocols and for that reason it is not simple to get devices to communicate with each other. In the future a new substation communication standard, IEC 61850, may facilitate this problem.

3 DATA TRANSFER AND COMMUNICATION

This chapter discusses some principles of the data transferring. The first part introduces shortly serial and parallel transmission. These techniques are still in use but it could be said that especially the pure serial transmission is already old fashioned technique in the substation because the needs and demands of communication have increased. The serial transmission cannot transfer enough data as quickly as it is required.

3.1 Overview

Many different communication protocols have been developed in the last decades. Different solutions and devices set up different demands for the signals and communication. The figure 3 shows some protocols which can be used for communication in the electrical transmission and distribution automation systems.

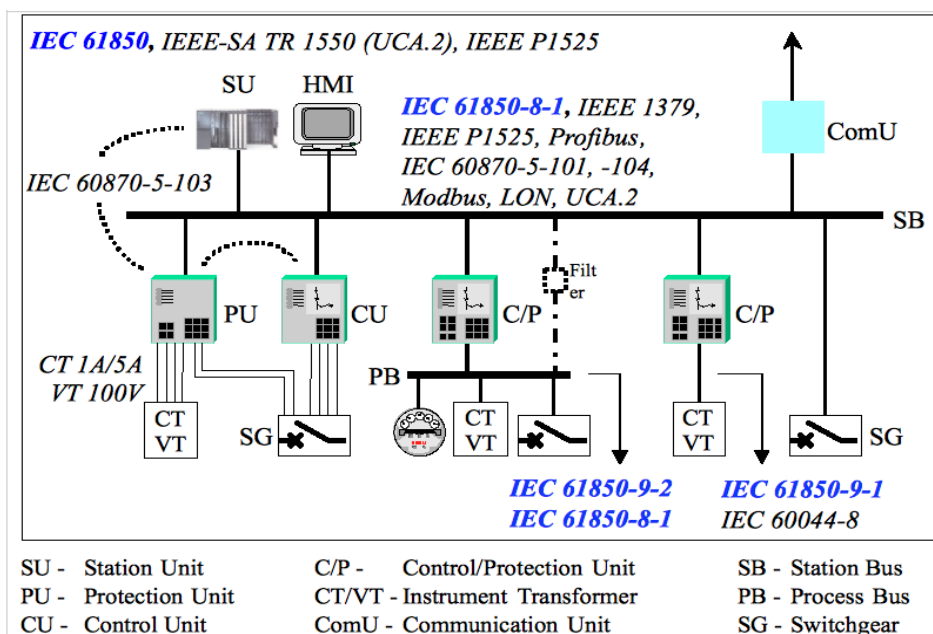


Figure 3. Protocols used for communication in the substations. (Nieminen 2008)

3.2 Network Topologies

The communication network can be built in several ways. Some of the common structures used in the SCADA system are represented in a simplified manner in figure 4.

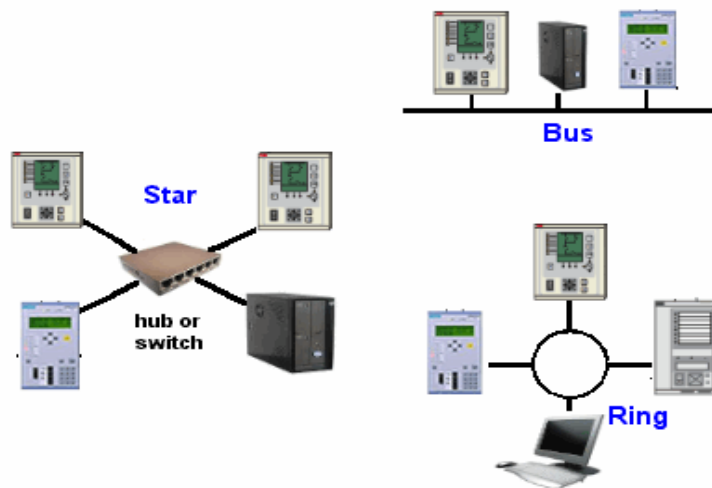


Figure 4: Typical network topologies

3.3 Communication

The traditional solution in digital data transferring is serial or parallel transmission. In serial communication the data is sent one bit at a time from the transmitter to the receiver and in parallel communication several data bits or entire byte are transferred simultaneously over several parallel channels. The figure 5 shows the difference.

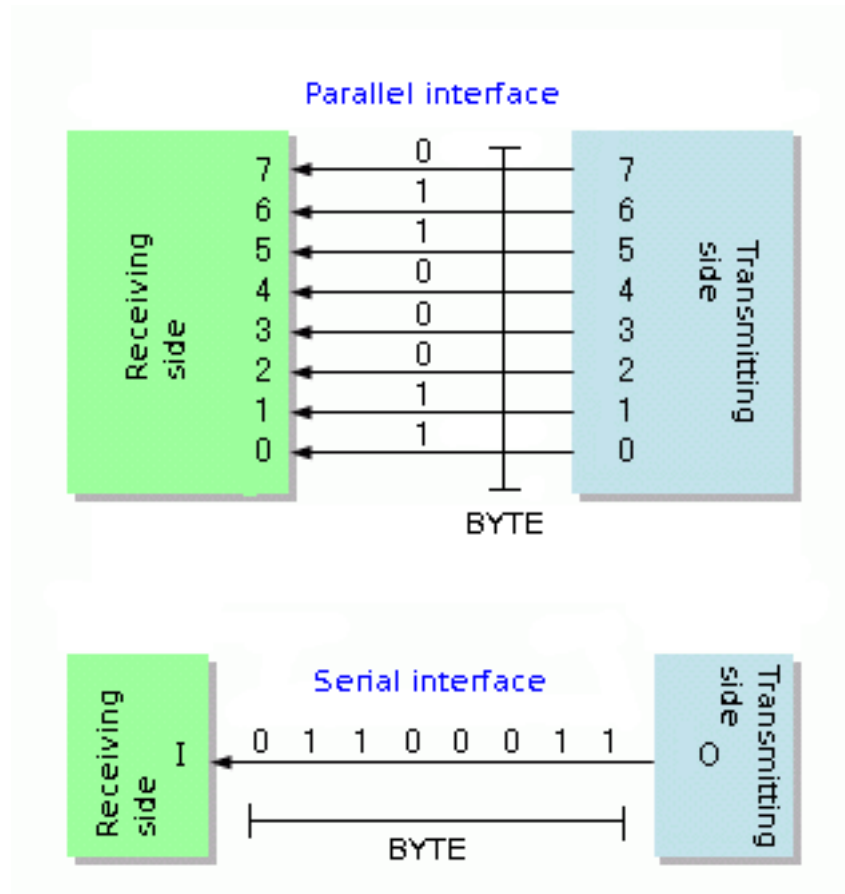


Figure 5. The basic idea of the parallel and serial transmission

Parallel communication is used over short distances, typically inside computers. The parallel transmission is a quick way to transfer data but in a long distance it needs more wires which makes the error handling more challenging and therefore the costs increase.

Serial transmission is usually used to transfer data between two computer systems or systems where the transferring distance is long. The protocols e.g. SPA, used in substation automation is based on a serial mode. Serial transmission can be either synchronous or asynchronous. In synchronous transmission, groups of bits are combined into frames and frames are sent continuously, with or without data, to

the receiver. In asynchronous transmission, groups of bits are sent as independent units with opening/closing flag and no data link synchronization, to allow for arbitrary size gaps between frames. However, start/stop bits maintain physical bit level synchronization once detected. Figure 6 clarifies the situation

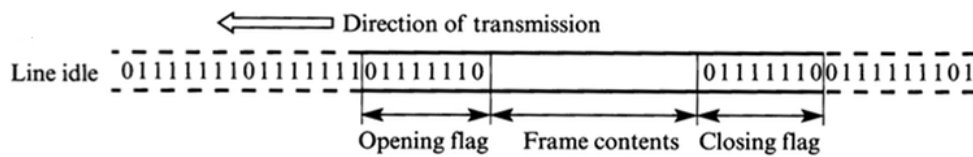


Figure 6. Typical asynchronous frame include opening/closing flag.
(Nieminen 2008)

The SPA bus, which was originally designed as a field bus for a distributed network application, is a typical example of asynchronous serial communication. Its data packet is shown in figure 7.

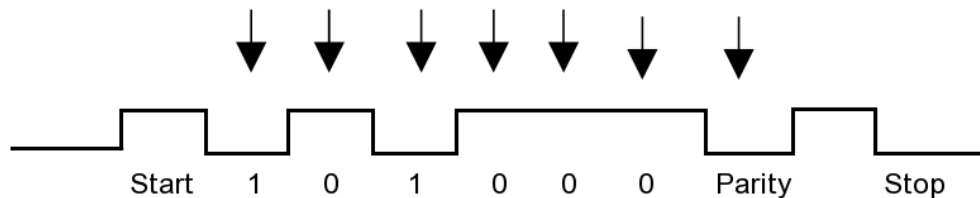


Figure 7. The data packet used in SPA-bus

In asynchronous transmission, the start bit must be included to the packet and that bit notifies when the data arrives to the receiver. After the start bit, there are seven data bit and a parity bits is also added. The parity bit is a mark which is added to ensure that the number of bits with the value "1" in a set of bits is even or odd. Parity bits are used as the simplest form of the error detecting code. The last bit of

the packet is the stop bit which separates the different data packet from each other.

For example, in the SPA bus it is assumed that the slave device has a self-initiated need to talk to the master but the master is aware of the data contained in the slaves and can request required data. In addition, the master can send data to the slave. The request by the master can be performed either by sequence polling (i.e. for event information) or only demand. (SPA-Bus Communication V2.5 2001, 4)

3.4 TCP/IP Network and IEC 61850

TCP/IP is the set of communications protocols used for the Internet and other similar networks. It is named after two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard. TCP/IP network is usually built as a ring which improves the reliability of the network, because a failure in a single network cable or switch do not interrupt all communication.

IEC 61850 is quite a new standard for the design of electrical substation automation. It includes a broad range of services and tools for monitoring, control, and protective relays. The one of biggest benefits with IEDs supporting IEC 61850 is that they can communicate directly with each other over the TCP/IP network. The IEC 61850 includes all layers of OSI model so it also includes the developed error detection techniques. The structure of the standard is shown in figure 8.

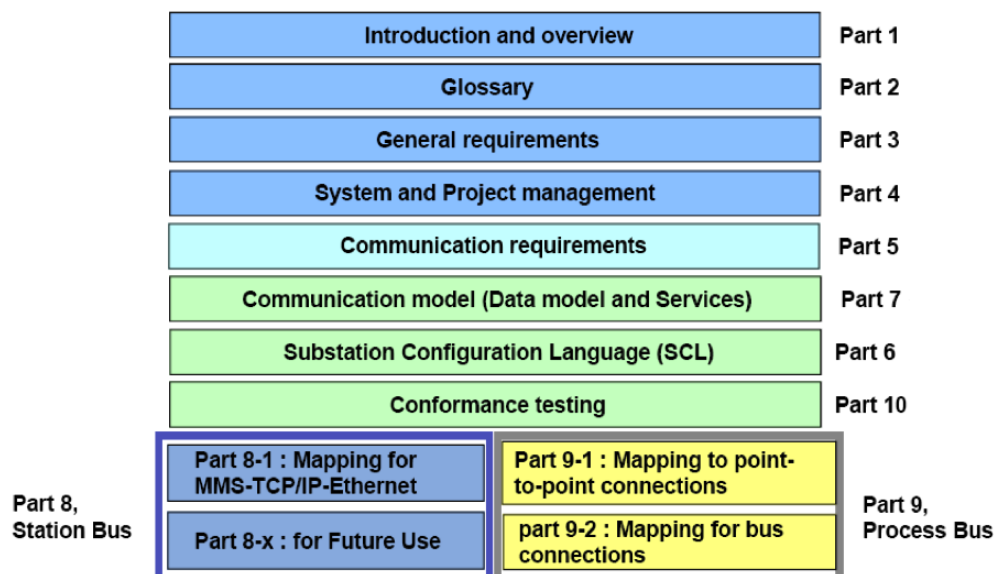


Figure 8. Structure of the IEC 61850. (IEC 61850 Standard)

As it can be noticed IEC 61850 is a very versatile standard and only a small part of it deals with the data transmission. The part 8-1 includes the TCP/IP protocols and this layer includes also the error detection from the messages.

3.5 Error Detection in Data Transfer

A number of different routines have been developed for detecting and correcting errors from the messages. The aim of an error detection technique is to enable the reception of a message transmitted through a noisy channel, to determine whether the message has been corrupted. Some of the most typical solutions are discussed in the next chapter.

3.5.1 Checksum

A checksum is a common method where the transmitter calculates a value, (also known as a checksum) that is a part of the message, and appends it to the message. The receiver can then use the same method to calculate the checksum of the received message and compare it with the appended checksum to see if the message was correctly received. The checksum is typically used by upper layer protocols, e.g. the checksum is included to the IP protocol.

3.5.2 Cyclic Redundancy Check

A cyclic redundancy check (CRC) is one of the most used techniques for error detection in data communications. The CRC technique is used to protect blocks of data (frames). The CRC is based on polynomial arithmetic, in particular, on computing the remainder of dividing one polynomial in $GF(2)$ (Galois field with two elements) by another. Using the CRC technique, the transmitter appends an extra n -bit sequence to every frame called Frame Check Sequence (FCS). The FCS holds redundant information about the frame that helps the transmitter to detect errors in the frame. It has to be noticed that FCS can include many other checksums than only the CRC. (Cyclic Redundancy Check. 2009, 1-3) A position of the CRC in frame is represented in figure 9.

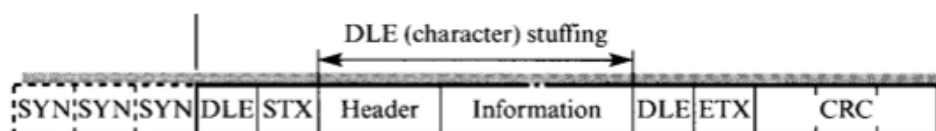


Figure 9. The block where the CRC has been added. (Nieminen 2008)

3.5.3 Hamming Distance

The hamming distance (HD) is a measure for how secure a protocol is against misinterpretation of a packet. $HD=4$ tells us that at least 4 bits can be wrong, the checksum calculations still matches, in order for it to be mistaken as a valid packet. The basic idea is that if more error-correcting bits are included in a message, and if these bits can be arranged in such a way that different incorrect bits produce different error results, then bad bits could be identified. In a 7-bit message, there are seven possible single bit errors, so e.g. three error control bits could potentially specify not only that an error occurred but also which bit caused the error. The mathematical model is not simple and is not discussed further here. (Signal Processing Laboratory 2004).

4 DATA SOURCES AND CONDITIONING

4.1 Instrument Transformers - Analog Inputs

Instrument transformers are used both to protect personnel and apparatus from high voltages and to allow reasonable insulation levels and current-carrying capacity in relays, meters and instruments. The performance of instrument transformer is critical in protection relaying since the relays can only be as accurate as the information supplied to them by the instrument transformer. Standard instrument transformers and protective relays are normally rated 1 or 5 A; 100, 110 or 120 V and 50, 60 Hz.

Where the protective relays operate only on current or voltage magnitude, the relative direction of current flow in the transformer windings is not important. The relative direction, and therefore polarity, must be known where the relays compare the sum or difference of two currents or the interactions of several currents or voltages.

The analog input signal must first be sampled and digitized before it can be used numerically. This converting is made by using an analog to digital converter (ADC). The result is binary numbers representing consecutive sampled values (1 and 0) of the input signal. After converting, the sampled values are transferred to the processor, which executes different numerical calculation on them. These calculations typically involve multiplying the input values by constants and adding the products together. If necessary, the results of these calculations, which now represent sampled values of the filtered signal, are output through a digital to analog converter (DAC) to convert the signal back to analog form. Filtering is dealt with later on. Figure 10 shows the sequence of the ADC-DAC.

All the sampled AC signals immediately after the first analog to digital conversion are usually recorded even if the relay or recording device uses decimated samples for other functions which are desirable (The working group 2006, 20). The figure 10 represent the AD converting process.

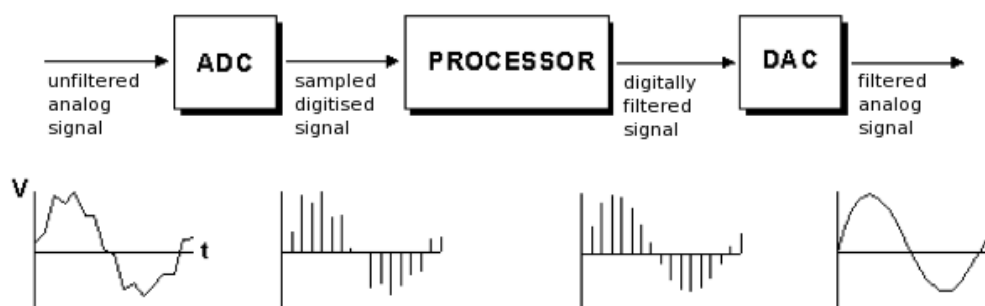


Figure 10: Sequence of the AD-converting.

4.1.1 Current Transformers

A current transformer (CT), like any other transformer, has a primary winding, a magnetic core, and a secondary winding. The alternating current (AC) flowing in the primary circuit (cable) and produces a magnetic field in the core and finally core induces a current flow in the secondary winding circuit. A primary objective of current transformer design is to ensure that the primary and secondary circuits are efficiently coupled, so that the secondary current bears an accurate relationship to the primary current.

A CT reduces high current so that the measurement can be connected to measuring and recording instruments. A CT also isolates the measuring instruments from high voltage in the monitored circuit.

CTs have good frequency response and normally do not require any special attention when operated in their recommended range of one to twenty times rated current and at rated burden or less. Perhaps the only unanticipated degradation in the

input signal will be due to the capacitance of the cables. This can introduce errors in magnitude at several kilohertz and errors in phase angle at several hundred Hertz. (The working group 2006, 17)

In many situations it is easier to measure current than voltage. Current circuits are low impedance paths that are less susceptible to induced signals or noise, whereas voltage circuits are high impedance paths that are more susceptible. (The working group 2006, 17)

In medium and large area substations, the burden on CTs is mainly determined by the cable burden. The reduction of the relay burden with the use of digital relays is useful but usually the cable burden is the greater part of the total CT burden, with either digital or most electromechanical relays. However, some electromechanical relays, such as sensitive ground overcurrent relays, with settings on the order of 0.5 Amp will impose a significant burden to the CT circuits. (The working group 2006, 17)

4.1.2 Voltage Transformers

Voltage transformers (VTs) do not have good frequency response. The capacitance of the cable between the voltage transformer and the relay will further degrade the input signal. But, depending on the frequency, this can be minimal compared to the errors due to the frequency response of the specific VT. (The working group 2006, 17)

4.2 Interferences and Coupling

Usually the measured signals are electrical and therefore include various interferences. The signal power is generally that small that interferences may generate significant errors to the signal transmission line. Interferences might cause several kind of harm for automation devices, like wrong operation, interrupted status val-

ues or other signal errors. In the worst case the whole measurement system might be corrupted.

The problem with interferences can be divided into three groups: the sources of interferences, the coupling of interferences and exposed devices. The closer inspection of these groups is present in the following chapters.

4.2.1 Sources

To eliminate the source of interference is the most effective method to remove the interference. For example, if the sparking has been eliminated from the tripping relay, it also eliminates the interferences from the measurement circuits. Typical interference sources in low and middle frequencies (<100kHz) are:

(Aumala 2002, 144-145)

- Power cables
- Solenoids and relays
- Transformers
- Motors
- The operation of circuit breakers and disconnectors
- Climate

4.2.2 Coupling

Coupling problems can be managed by assemblies and right connection solutions. The practical solution is to take notice of these problems at the same time as measurement arrangements are planned. The good planning is necessary because interferences could couple to the measurement circuits from several sources such as signal conductor. (Aumala 2002, 144-145)

1. Galvanic coupling

Galvanic coupling occurs especially if the same paths are used for high current but also for low current. This kind of solution should be avoided and it is recommended that the different route is used for a device power supply and signal cables. (Aumala 2002, 144-145)

2. Inductive coupling

The inductive coupling occurs via the magnetic field. As the current flows in the cable, it generates a magnetic field around the cable. The change of the current induces voltages to the loops in the circuit. That is why the loops should be avoided. The loop could be possible if the cable is earthed at both ends. (Aumala 2002, 144-145)

Nowadays most signal cables are of twisted pair type and in that way the induced voltage causes less interferences for the cable. (Aumala 2002, 144-145)

3. Capacitive coupling

Capacitive coupling occurs due to the distributed capacitances between circuits. The current flows via the distributed capacitances as the voltage changes. The coupling can be eliminated if the interference source is placed far enough from the signal circuits. This means that instrument cables are not recommended to be assembled to the same cable ladder with high voltage cables. (Aumala 2002, 144-145)

4. Radiation

Radiation is a very complicated event and the radiation sources are increasing. EMC, electromagnetic compatibility, is nowadays a more and more important

case because the electric devices increase all the time and they are at the both time the sources of the interferences but also sensitive for the radiation. The protection from straight radiation is to build the metallic cover around the device and cables which are left outside of the cover should be also covered by earthed shield separately. (Aumala 2002, 144-145)

4.3 Digital Inputs

In the RTUs and IEDs, digital inputs mean typically the digital signals from the external contacts i.e. limit switches of the CB for position indication or internal element status indications of the device e.g. low SF6 gas pressure in CB breaking chamber. Although this input can be a simple contact, it deserves considerable attention because these signals are very important in the analysis process. (The working group 2006, 18)

4.4 Filtering

Filtering is an important part of the signal handling and consequently linked with data validation. This chapter introduces briefly and in a simplified way the basic ideas of the filtering.

As mentioned earlier, interferences cause distortion to the signal. Figure 11 represents the situation, where the interferences have generated distortion in the signal.

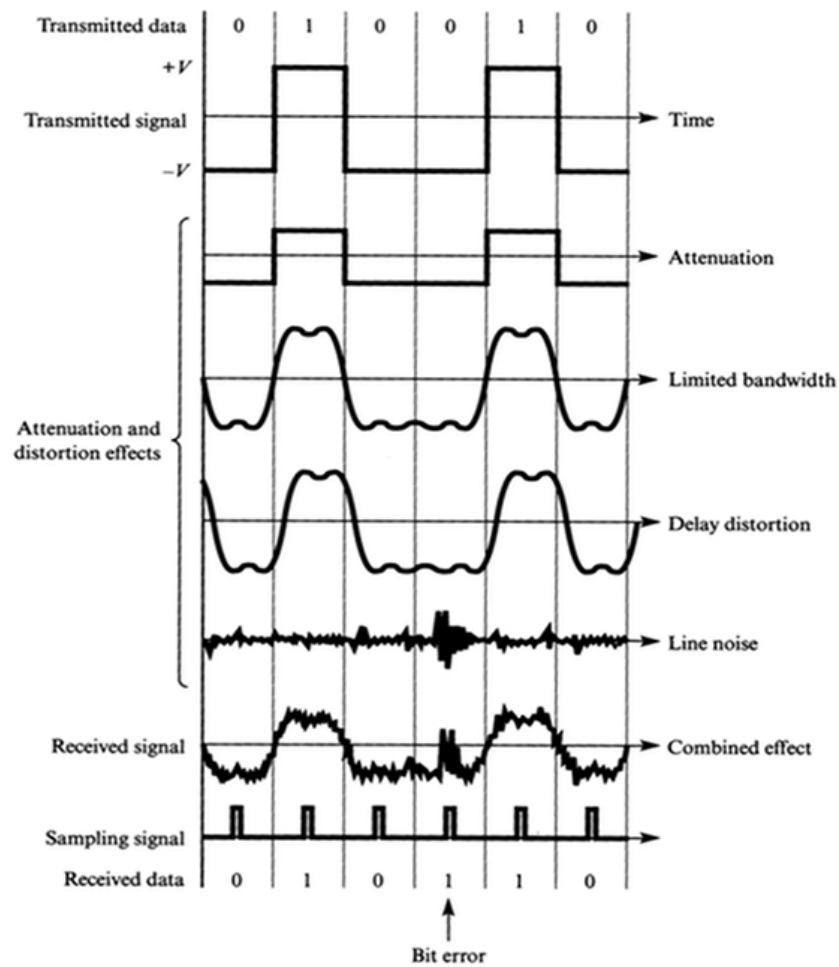


Figure 11: Typical interferences in the voltage signal. (Nieminen 2008)

Filtering means removing unwanted parts of the signal, such as random noise. On the other hand, filtering makes it possible to extract useful parts of the signal, such as the components lying within a certain frequency range. In order to manage these distorted signals, filtering has to be included in the receiver. The filtering of

the applied signals may be both analog and digital, and together with the sampling rate determines the frequency response of the recorded information. (The working group 2006, 19)

There is a great variety of different kind of filters which have been developed over the years to meet the needs of various applications. Despite this variety, many filters are based on a few common characteristics.

One principle is the frequency range of their pass band. A filter's pass band is the range of frequencies through which filter will pass an incoming signal. Signal frequencies lying outside the pass band are attenuated. Next chapter discusses only filtering of AC signals as they are used in IEDs. (Ramsden, 2001)

4.4.1 Analog Signal Filtering of AC Signals

Any digital device, including IED, must include an anti-aliasing feature, usually achieved using an analog filter. Anti-aliasing filtering eliminates higher frequencies that would otherwise overlap the lower portion of the spectrum due to the finite sampling rates of digital devices. (The working group 2006, 19)

One of the used theorems to determine the sampling rate of the device is the Nyquist sampling theorem:

”The sampling frequency should be at least twice the highest frequency contained in the signal.” (Olshausen 2000, 1)

Or in mathematical terms:

$$f_s \geq 2 \cdot f_c \quad (1)$$

Where f_s is the sampling frequency (how often samples are taken per unit of time or space), and f_c is highest frequency contained in the signal. (Olshausen 2000, 1)

Typically the sampling rate in IEDs varies from 4 samples/cycle to 356 samples/cycle. Digital Fault Recorders (DFRs) typically use a sampling rate of 16-128 samples/cycle but some devices permit sampling rates of up to 384 samples/cycle. DFRs typically use higher sampling rates than relays since it is important to get accurate data for further analysis i.e. for the harmonic calculations. DFRs' cut-off filters are set well above 1 kHz which yield comparatively good spectral coverage (The working group 2006, 19).

Protection relays sample as low as 4 to 20 samples per cycle, to simplify analog to digital conversion and filtering. Some modern relays sample in a range of 32 to 128 samples per cycle or more for recording purposes, providing good spectral coverage. (The working group 2006, 21)

Another aspect of analog filtering is the design of the filter itself. When high order filters are used, their response may not be ideally flat over the pass-band frequencies. This should be considered when a detailed harmonic analysis is performed using records produced by protective relays. (The working group 2006, 19)

The analog filter of digital relays is typically a low-pass filter, allowing the sub-harmonics and dc components to pass through. However, the frequency response of the input magnetic modules at low frequencies may alter the low frequency components (at the level of a few Hz). This should be considered when analyzing sub-harmonics and decaying dc components. (The working group 2006, 19)

4.4.2 Digital Signal Filtering of AC Signals

The primary objective of digital filtering, as any other filters, is to filter out unwanted components of the applied signals, i.e. the dc component. To accomplish this, the filters must include a differentiating portion that ideally should match the L/R constant of the primary circuit. The accuracy of input signal and recorded

data is impacted by the performance of any digital filtering applied to the AC inputs. Digital filtering is applied especially in protection relays, as relays process the sampled data to make appropriate protection function decisions. A proper analysis of recorded data requires understanding any digital filtering applied to the AC input signals. (The working group 2006, 19)

Digital relays tend to record sampled data after digital filtering. Newer digital relays record raw samples prior to digital filtering. This not only widens the resulting frequency spectrum of the recorded waveforms, but also ensures that the stored information does not depend on any proprietary digital signal processing algorithms. Other methods used on a limited basis include converting the sampled waveforms to RMS or other application specific values. (The working group 2006, 20)

4.5 Intelligent Electronic Devices

This chapter discusses IEDs in general and introduces their role in the SCADA system. Finally such important protection function are discussed which could be used for data validation.

Intelligent Electronic Device (IED) is a general term for microprocessor based equipment that is used for maintenance, control, protection and monitoring of the process. Protection relays manufactured these days are primarily IEDs. With available microprocessor technology, a single unit can perform several protective, control, and similar functions. Whereas before the microprocessor technology a single unit would contain only one protection function and if several protection functions were required one would have to combine a number of different units of protection relays. The processing power of digital electronic devices is one of the main reasons to replace these old analog devices. The ease of digital data ex-

change is another very important reason to substitute traditional analog instruments.

Typically there are three categories of input sensors or transducers for IEDs. Two of these are analog – current and voltage, and the other is digital, which reflects the status and change-of-state information for selected equipment operations. (The working group 2006, 23)

IEDs and their implementation in power substations facilitate enhanced data acquisition. The amount of data is increased and all data cannot be utilized, but offering already much better monitoring of the loading and switching status within the substations. Both analog and digital (status) data can be collected from various locations within the substation and processed in certain location. This location can be the IEDs itself or the data can be transferred to various applications. In the future IED will process more data more effectively in the substation. (Djokic et al. 2005 pp. 3 ; The working group 2006, 28)

4.5.1 Overcurrent Protection

Overcurrent protection is used against short circuit faults and heavy overloads. Overcurrent protection functions offer maybe the easiest and the most economical protection for many equipment. Nowadays IEDs include several overcurrent stages which can be adjusted separately. The IED measures the phase current and the protection function is sensitive for the highest of the three phase currents. Whenever the highest value exceeds the pick-up setting of a particular stage, this stage picks up and a start signal is issued. If the fault situation remains on longer than the operation delay setting, a trip signal is issued. The time delay may be a constant or inverse type. Inverse delay means that the operation time depends on the amount the measured current exceeds the pick-up setting. The bigger the fault current is the faster will be the operation.

4.5.2 Differential Protection

Differential protection is widely used to protect generators, transformers and bus-bars. A differential relay measures currents from each phase in two different places. For normal operation or if a fault is outside of the two sets of current transformer, entering (I_1) and leaving (I_2) phase currents is equal. If the fault occurs between the two sets of the current transformers, one or more of the phase currents will increase whereas the current on the other point will either decrease or increase and flow in the opposite direction. The figure 12 shows the idea.

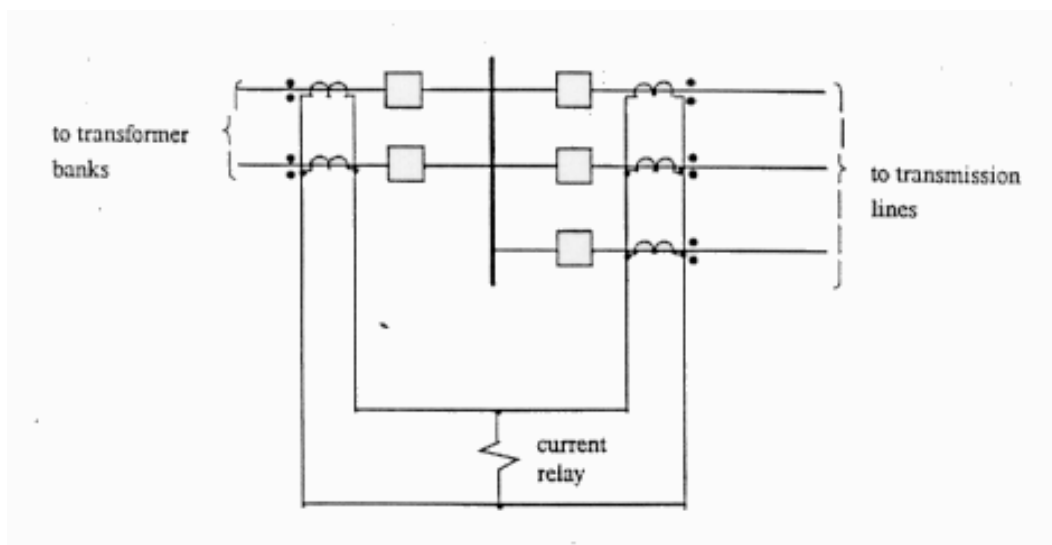


Figure 12: Single line diagram of busbar differential protection

One application of this is high impedance differential relaying based on the conservative premise that the CT's on one side of the protected target perform perfectly for an external fault and the other set of CT's saturate completely. It takes advantage of the fact that the voltage appearing across the relay is limited for external fault to the voltage drop which is produced by the maximum secondary current flowing through the leads from the relay to the saturated CT and its inter-

nal resistance. For an internal fault, the voltage will approach the open-circuited CT voltage

Another solution is a percentage differential relay which solves the problems of poor sensitivity and slow operation. The inputs from the two sets of the current transformers are used to generate a restraint quantity. This is then compared to the difference of these two currents. The operation is produced as a result of the comparison of the difference to the restraint. This desensitizes the relay high external fault currents. The relay should operate if formula 3 is fulfilled

$$|I_1 - I_2| \geq k \cdot \left| \frac{I_1 + I_2}{2} \right| \quad (2)$$

where k is the proportion of the operating coil current to the restraint current and it is typically set between 10 - 40%.

The current required for the relay's operation increases with the magnitude of the fault current. The percentage of increases may be constant or the percentage of increases may vary with the external fault current. The effect of the restraint on internal fault is negligible because the operation quantity is weighted and responds to the total secondary fault current. (Elmore 2004, 169)

Multifunction microprocessor relays do not have a physical operating winding, the difference of the restrain currents being computed mathematically by the algorithm.

4.5.3 Unbalance Protection

Unbalanced protection is based on information that any set of unbalanced three-phase quantities could be expressed as the sum of three symmetrical sets of balanced phasors. There are three sets of independent components in a three-phase

system: positive, negative and zero for both current and voltage. Positive sequence voltages are supplied by generators within the system and are always present. A second set of balanced phasors are also equal in magnitude and displaced 120 degrees apart, but display a counter-clockwise rotation sequence of R-S-T, which represents a negative sequence. The final set of balanced phasors is equal in magnitude and in phase with each other, however since there is no rotation sequence this is known as a zero sequence. (Protection Basics 2007, 79-80) The figure shows the different phasor components.

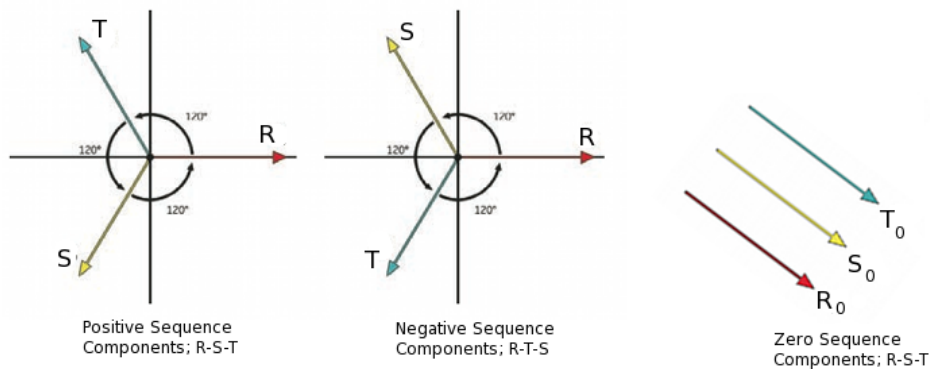


Figure 13: Positive, negative and zero sequence components

The symmetrical components can be used to determine any unbalanced current or voltage (I_R , I_S , I_T or U_R , V_S , U_T which reference unbalanced line-to-neutral phasors) as follows: (Protection Basics 2007, 79-80)

$$I_R = I_1 + I_2 + I_0 \quad U_R = U_1 + U_2 + U_0$$

$$I_S = a^2 I_1 + a I_2 + I_0 \quad U_S = a^2 U_1 + a U_2 + U_0$$

$$I_T = aI_1 + a^2 I_2 + I_0 \quad U_T = aU_1 + a^2 U_2 + U_0$$

where “a” operator shifts a vector by an angle of 120 degrees counter-clockwise.

Under a normal condition, the power system is considered to be essentially a symmetrical system and therefore only positive sequence currents and voltages exist. At the time of a fault, positive, negative and possibly zero sequence currents and voltages exist. Using real world phase voltages and currents along with Fortescue’s formulas, all positive, negative and zero sequence currents can be calculated. Protection relays use these sequence components along with phase current and/or voltage data as the input to protective elements. (Protection Basics 2007, 79-80)

4.5.4 Earth Fault Protection

An earth fault relay is overcurrent relay connected to the star point circuit of a set of 3-phase CTs and it measured the sum of current. Under normal conditions the sum of phase-currents I_1 , I_2 and I_3 i.e. zero current $3I_0$ should be close to zero. Figure 14 shows how these CTs are connected typically to the relay.

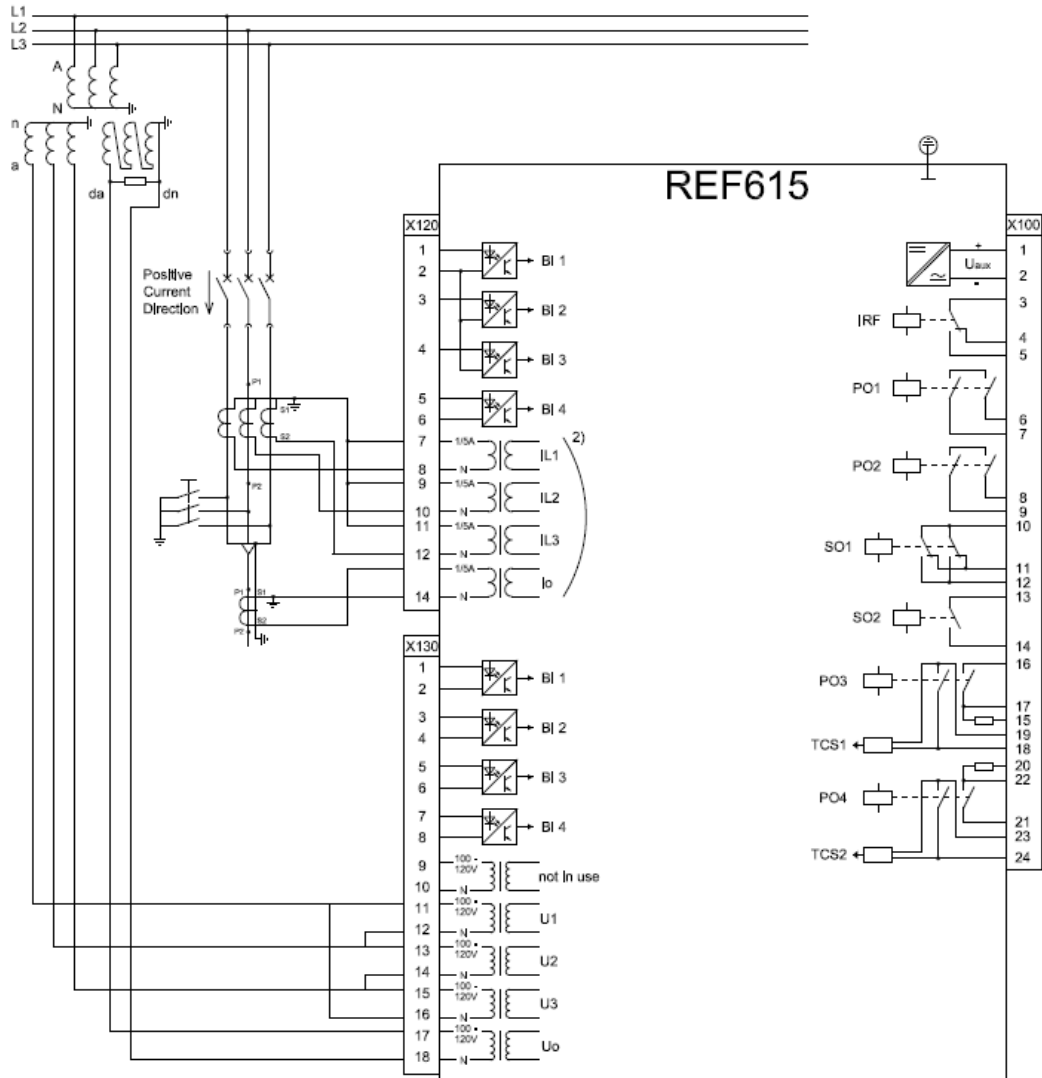


Figure 14: IED with earth fault measurements. (Terminal Diagram REF615)

5 TOPOLOGY MONITORING IN REAL-TIME

In a power system, topology is defined by the connectivity between power system components like transformers, circuit breakers, transmission lines and loads. The reliable information about topology is important for many actions which are executed in the system. Generally, the topology of the network is updated from the status of the switching devices. The common way is to monitor the status of the CB or measurement element and update the topology based on these information. For example, in older systems RTUs and nowadays IEDs are wired to the CB limit switches that operate when the breaker mechanism changes state. (Djekic 2007, 6) The real-time monitoring is typically done through RTUs of the SCADA and the changes in the CB status are reported to the SCADA interface. (Kezunovic 2006, 1)

Today CB status is monitored from the control circuit limit switches as “a” and “b”. These contacts are designed in such a way that an open and close state is easy to determine by verifying the opposite status of the “a” and “b” contact position. By monitoring open/closed status of all CBs, it is possible to create a wide bus/feeder topology configuration of the power system. As it is shown in figure 15, the “a” and “b” contact signals present the voltage across auxiliary switches that specify the open or close status of the CB (Djekic 2007, 6).

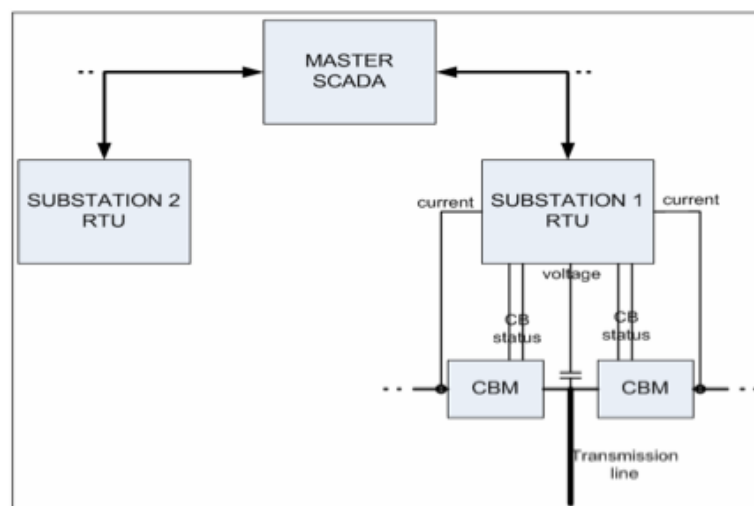


Figure 15: Traditional SCADA topology (Djekic 2007, 6)

The reliability of the contact “a” and “b” indication has been a concern due to relatively frequent errors in the readings of the contacts, that may cause malfunction, or errors in the SCADA communication. (Kezunovic 2006, pp 1) In some cases, the auxiliary limit switch does not show the real circuit breaker status due to mechanical, electrical or wiring problem. Most of the circuit breaker failures that have been detected in the field can be defined to mechanical failures and difficulties related to the auxiliary control circuits. Approximately 25% of the major and minor failures of circuit breakers in service are caused by control circuit failures (Djekic 2007, 4).

Two general issues are associated with determination of the topology, namely the system wide attempt to improve overall network topology determination and the local attempt to improve status determination of a single CB. Locally at the substation level, topology issues include the consideration of the automated analysis of the CB status based on signal measurements from the CB control circuitry but

also the consideration of the topology consistency check based on measurements from substation IEDs. (Kezunovic 2006, 1)

5.1 Monitoring

Monitoring, especially if it is executed in real-time, requires the analog measurements of current and voltages as well as measurement of CB status (Kezunovic 2006, 3). Data acquisition software should run “nonstop” that operator can maintain the process effectively in real-time. There is also applications like disturbance recorders that can be used to detect and analyze faults and such occurrences afterwards but the use in the normal condition are not useful.

The next chapter discusses the possibilities which can help to define the system topology reliably.

5.1.1 Multiple and Redundant Information

If one signal is available from several sources, comparison can basically be performed quite easily and decide if the signals match. Table 2 shows an example situation where the redundant signals exist and how the redundancy could be detected. (Djokic et al. 2005, 9)

Table 2: Description of the types of signals for DFRs, DPRs, and CBMs.
(Djokic et al. 2005, 4)

| Digital Fault Recorder | Digital Protective Relay | Circ. Breaker Monitor |
|-------------------------------|---------------------------------|------------------------------|
| “A” and “B” contacts | “A” and “B” contacts | “A” and “B” contacts |
| Phase currents | Phase currents | Phase currents |
| Relay trip signal | Relay trip signal | Trip and close initiate |
| Recloser timing signal | Recloser timing signal | Trip and close currents |
| Breaker failure initiate | Breaker failure initiate | “X” and “Y” coils |
| Comm. scheme signals | Comm. scheme signals | DC supply |

As it can be noticed, the redundancy exists and comparison is possible to execute. In the case that the signals do match, the level of the confidence for data is pretty high. If these signals differ from each other, a 2-out-of-3 voting logic may be implemented to select a more reliable outcome. (Djokic et al., 2005, 9) However, this kind of solution is very rare in SCADA system.

One benefit of the correlation between analog measurements and CB status signal is an ability precisely to define the sequence of events related to fault clearing. This improves the analysis of operation of a single circuit breaker but also enables the analysis of operation of multiple circuit breakers. (Kezunovic 2006, 8) If the feeder includes several CBs, it is possible to monitor these CBs at the same time by combining their statuses and set the state as one equivalent circuit breaker.

The correlation also helps in a situation when a dynamic change in the substation topology needs to be verified using analog measurements. This can be significantly facilitated if both the CB limit switch changes and phasor changes are measured with a common time reference. This assures that a given measurement scan is “aligned” in time avoiding possible confusions about the sequence of events (Kezunovic 2006, 8).

Determining power system topology very accurately in that way using SCADA information only is not always possible. Utilizing data from different IEDs that are connected to a given circuit breaker improves robustness in determining the topology but it may also need special solutions and an application for the data acquisition and integrating such an application with the existing SCADA system is not trivial (Djokic et al., 2005, 9).

5.1.2 Circuit Breaker Status Monitoring

The mentioned IEDs enable monitoring of the functional tasks of the circuit breaker: clearing the faults and changing the topology of the power system. In either case, an automatic controller or an operator initiating the circuit breaker operation, the final outcome of a circuit breaker changing its state or remaining in the same one depends on the function that the circuit breaker was supposed to support. For example, the voltage and current signals should change if there is a fault on the transmission line, the relay should determine the fault location and fault type leading to a decision to trip (or not to trip), and if there is a trip or close command tasks, the CB control circuit monitor records the behavior of the control circuitry. The whole sequence can tell if the circuit breaker is operating correctly, and if not, what are the possible reasons. (Djokic et al., 2005, 9)

One possible solution is the CB Monitor which would be permanently connected to the substation CBs. CBM records detailed information about each CB operation

in real-time, regardless of whether the operation is initiated manually by the operator or automatically by the protection and control equipment and stores them in COMTRADE file format. The idea of the system is that after the data is collected, it is automatically processed to extract the information of interest, which is then distributed to various users (Djekic 2007, 3).

5.2 Signal Selection for Topology

There are a large number of quantities and signals that could be monitored for circuit breaker and topology monitoring purposes. There are also many methods to measure or calculate those parameters. Traditionally calculations are made by some other program than SCADA. For SCADA the signals for monitoring should be chosen in such a way that it gives enough information to make conclusions about the circuit breaker and system condition and operations without calculations. It is important to have a complete set of quantities/signals to be able to perform quality analysis and give reliable circuit breaker status information. (Jakovljevic et al., 2)

Data is collected from circuit breakers in a substation, and the system combines the data to make deductions about the system topology and operation performance that could help in increasing the system reliability. More precise and reliable assessment of system topology may be achieved by integrating redundant data from SCADA system and monitoring system (Djekic 2007, 4).

5.3 Data Validation

As it was mentioned earlier there is more information available than is utilized. After the suitable signals have been determined a minimum requirements for the signals and records have also to be defined. The signals may suffer from various interferences along transferring so the certain error handling routines have already

been included in the protocols. These methods can be said to be constant and it is not possible or even needed to configure these routines

The situation is different in database applications and other programs which utilize some imported data. It is important that applications operate on clean and right data. In order the applications to operate as planned some minimum requirement for the imported data must be defined. In order to meet these basic requirements, it is up to user or routines in the program to confirm that data is valid. Validation could involve some checks that can be performed on the record immediately after data has been recorded or like the databases the routines are typically executed in certain time interval, for example once a day. Databases enable also to build validation routines very accurately and one widely used method is to validate the imported data statistically. This kind of application is very complex and typically it needs an external mathematical.

In power systems the condition monitoring are regularly executed by measurements and condition state of device is analyzed based on this data (Lindh 1997, 89). In the condition monitoring the state of the device is validated by:

- Alarm limits, if the limit is exceeded or variation of the measuring value
- Trend monitoring. If the values are changed in long time period it indicates the load changes or changes in the use. A simple solution is that quantity peaks generate alarm, and the manual condition analyzes can be executed.

It is possible to use these methods in SCADA but it has to be known how the limits can be set reliable.

5.3.1 Check Using Redundant Current Measurements

There could be assemblies which contain circuit breakers with two current transformers in their bushings. The redundant measurements of current are acquired from RTU or some other IED monitoring the feeder. In these cases, it needs to be decided what the value for current is in the feeder but it also must be made possible to combine these two measurements. Ideally, both values should be equal. The decision which one of the two measurements is right is simple if both measurements are the same but becomes a little more difficult when values are different. (Jakovljevic et al., 3-4) The algorithm flowchart is represented in figure 16.

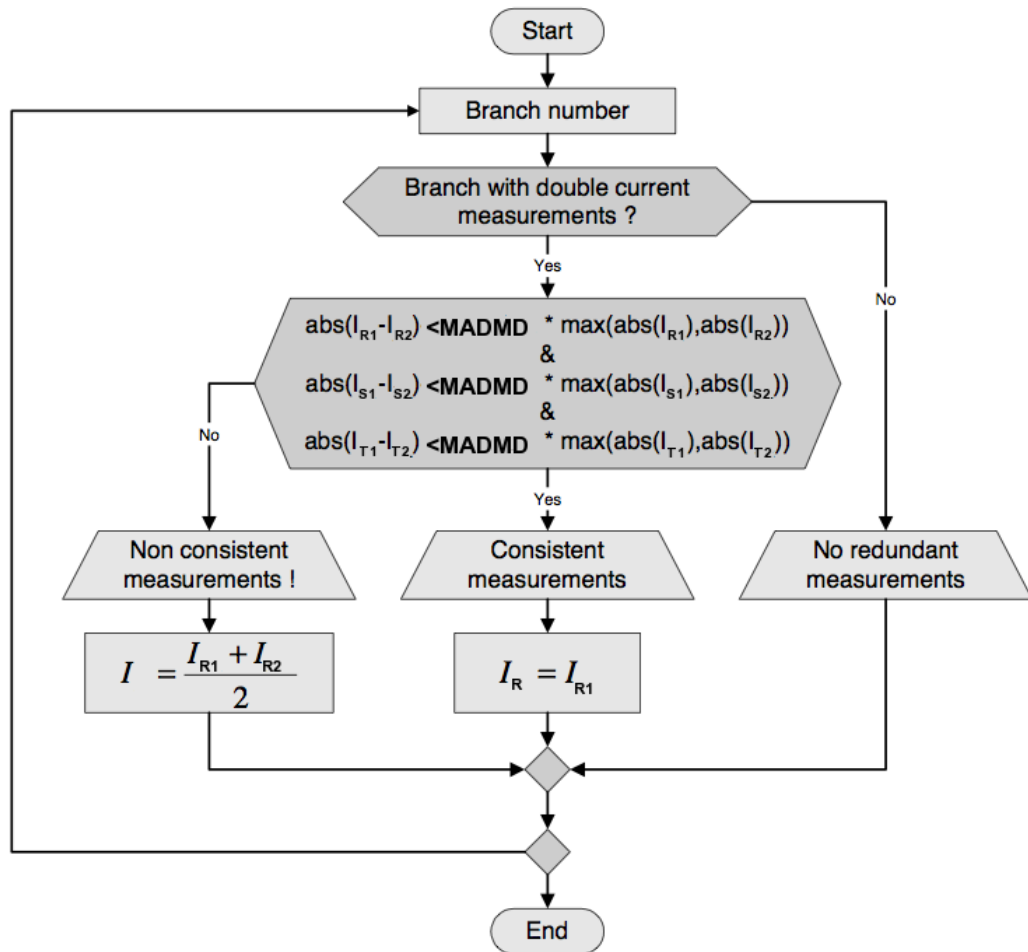


Figure 16: Algorithm for checking the feeder current consistency.

(Jakovljevic et al., 4)

This algorithm can handle all the feeders in the station. First, it determines if there is a redundant measurement of current in the feeder. In the feeders where redundant measurement exists, consistency check can be proposed. The criterion is that the absolute value of the difference between the phasor currents should be less than certain percent of the absolute value of the larger current. In this case the percent is defined by variable *MADMD* (Maximum Allowable Double Measurement Discrepancy). This criterion has to be satisfied for all three phases. The pre-

sumption is that there will be no discrepancy in the phase angle without a discrepancy in the magnitude. (Jakovljevic et al., 4)

If the criterion is satisfied, the current in the feeder will be selected one of the measurements (since they are the same to the precision determined by *MADMD* variable). (Jakovljevic et al., 4)

In the situation when none of the phase current criteria is satisfied, an alarm is generated. The current in a feeder is determined as an average value of the two current measurements. An alternative to this conclusion would be to mark the current in this feeder, and upon additional checks, to reject one of the measurements (if it is bad data). (Jakovljevic et al., 4)

5.3.2 Check Using Measurements Without Redundant Information

1. Current

The validating method introduced in chapter 5.3.1 can be applied although there are not two measurements in the feeder. The validation routine bases on the highest measured phase current (I_{\max}) and two other phase currents (i.e. I_R , I_S) are compared to I_{\max} current. If the measured value in the two phases (I_R , I_S) drops smaller than certain percent value of the I_{\max} the alarm is generated. This percent value could be i.e. 15% of I_{\max} ($0,15 * I_{\max}$). (Yliaho 2008)

It is good to notice that this kind of method is much more effective if the breaker statuses from the certain feeder is also considered

2. Voltage

This same method works with voltages and validating process can be very similar as it was with current. The maximum measured voltage (U_{\max}) is picked and two other phases are compared for U_{\max} and if limits are set right, that kind of function works quite reliably. (Yliaho 2008)

5.3.3 Check Using Kirchoff's Current Law

This type of check can be performed for all the nodes where two or more feeders meet and the measurements of current exist in all those feeders. Kirchoff's Current Law (KCL) can be stated in words:

”At any node in an electrical circuit, the sum of currents flowing into the node is equal to the sum of currents flowing out of the node”.

Or in mathematical terms:

$$\sum_{k=1}^n \bar{I}_k = 0 \quad (3)$$

The algorithm is shown in figure 17.

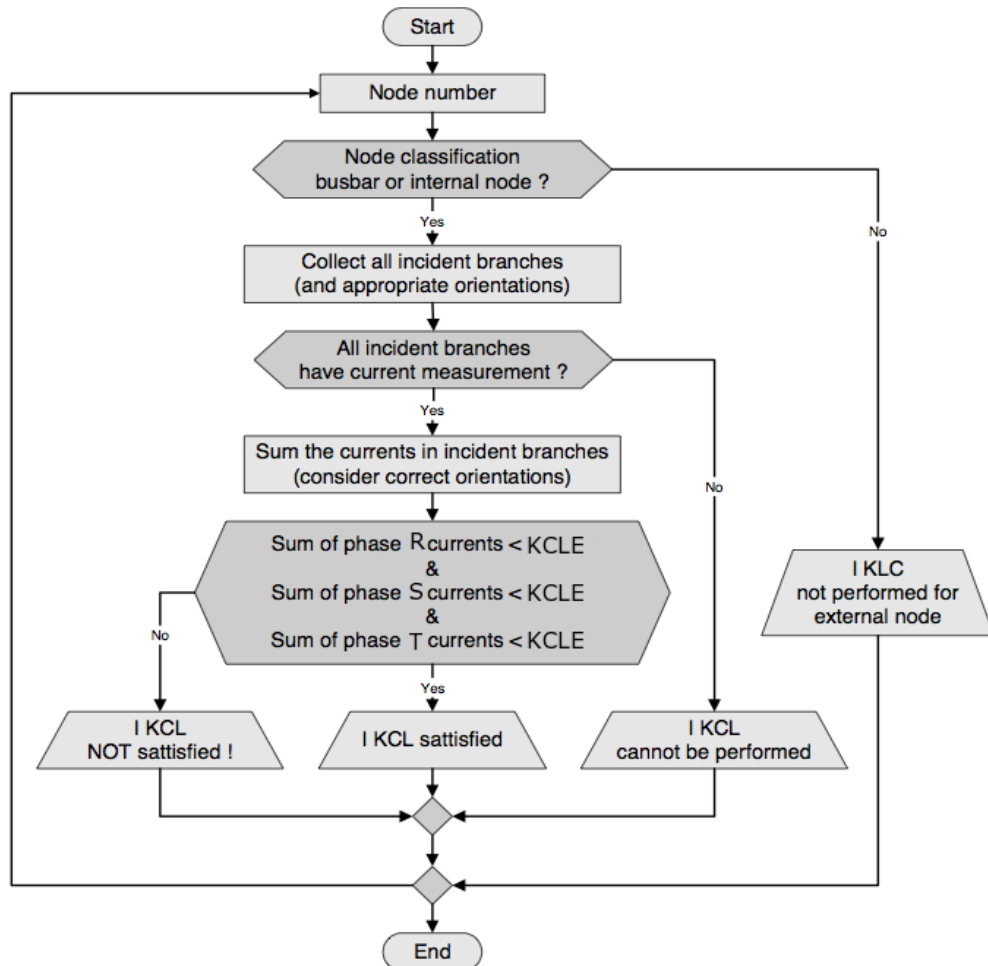


Figure 17: Algorithm for the check of Kirchhoff's Current Law (Jakovljevic et al., 4)

First, the node classification is checked. Only the busbars and substation internal nodes are taken into consideration. First Kirchhoff's law is not performed for external nodes since they split one feeder (that connects two substations) into two parts and usually there is no current measurement available at least on one side. (Jakovljevic et al., 4)

For busbars or internal nodes, the incident feeders need to be determined and a check is performed to see if all of them are equipped with RTUs or IEDs measuring the currents. (Jakovljevic et al., 4)

For the internal nodes, there is enough information to check KCL. Currents in the node incident feeders are summed considering orientation of each current (leaving or entering the node). Then the First Kirchhoff's law condition can be checked for each phase separately. Ideally the sum of currents should be zero, but naturally, certain error should be allowed. This is defined with the variable *KCLE*. (Jakovljevic et al., 4)

5.3.4 Check of the Feeder Status

The determination of feeder switching statuses can be accomplished considering all the switching devices (switching elements) in particular feeders. Typically there is either one circuit breaker with one disconnecter or one circuit breaker with truck (or disconnecter) and line disconnecter in a feeder (branch) of the medium voltage substation.

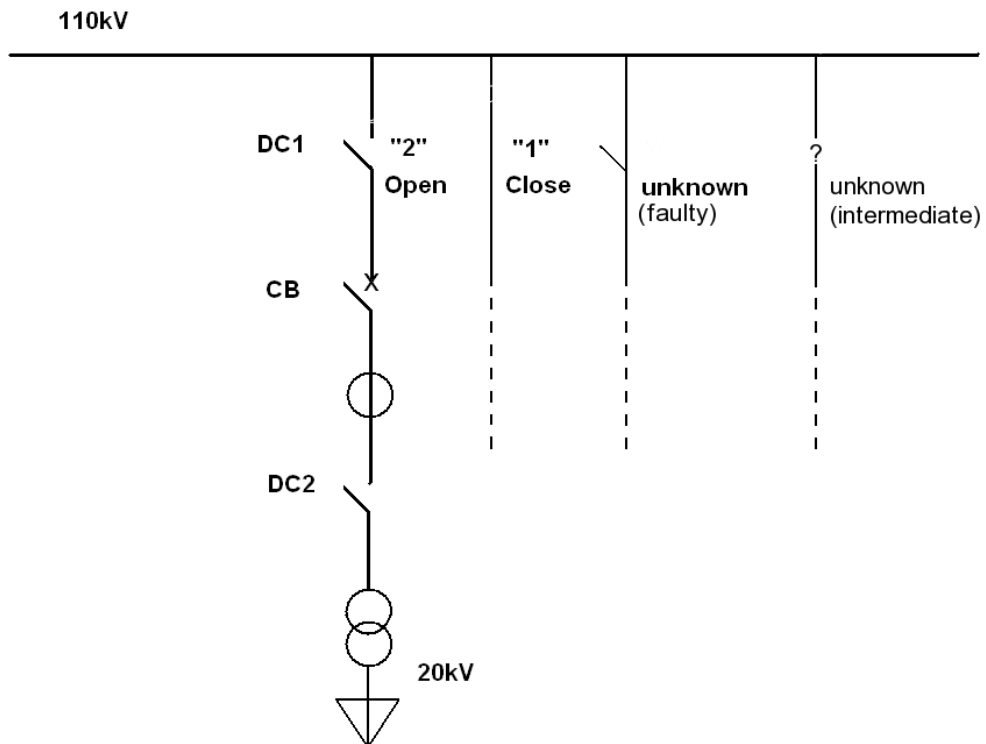


Figure 18: The feeder with one circuit breaker and two disconnectors. The different switching statuses of the one device are also shown.

As it has mentioned earlier, the feeder status in the topology can also be determined based on the status of CB. For feeders with three switching devices, applied logic is shown in the table 3.

Table 3: Applied logic for check of the feeder status in the case of one circuit breakers (CB) and two disconnectors (DC).

| | | | | | | | | |
|----------------------|--------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| DC1 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 |
| CB | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 |
| DC2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 |
| Feeder Status | 3 | 4 | 4 | 5 | 4 | 5 | 5 | 6 |
| Position | Close | Open | Open | Open | Open | Open | Open | Open |

1 = Close, 2 = Open, other = Unknown

The function checks switching devices statuses of the feeder. The function consist of two if-commands. First, if all status values are "1" (closed) then feeder status is "3" and equivalent circuit breaker status is also closed. Next, there is a situation when all switching devices are open ("2") then feeder status is "6" and the equivalent circuit breaker is "open". The equivalent circuit breaker is defined "open" every time as one of the switching devices has a value which differs from "1". It is possible to define different indications for the feeder (Bad, Unknown etc.) if the one of switching devices statuses in certain feeder differs from "1" or "2".

The routine of checking the feeder (branch) status can be shown as in figure 19.

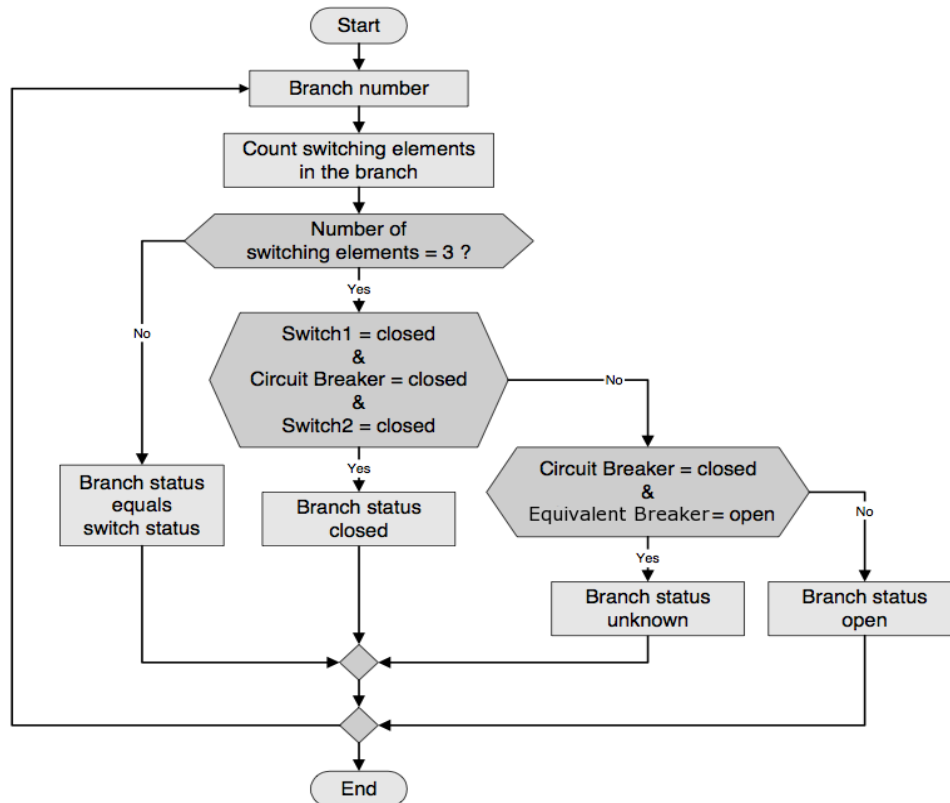


Figure 19: Algorithm for feeder status determination. (Jakovljevic et al., 5)

5.3.5 Check of Feeder Currents and Topology Data

Consistency checks between feeder current values and feeder statuses (topology data) are more accurate than checking the current or status value alone. Checks can also be executed for each phase separately. As it has noticed, there are several possible combinations of feeder current values and feeder statuses. Each possibility reflects different situation and has distinct impact on the conclusion. If there is an exact value for the statuses (open or close) it can be found correspondence between feeder current and feeder status. Consistency could be fulfilled for two basic cases:

- 1) when the equivalent circuit breaker is “close” and there is some current in the feeder (branch)
- 2) when the equivalent circuit breaker is "open" and there is no current in the feeder (branch) (Jakovljevic et al., 5).

In the case the equivalent circuit breaker is “open” but there is some current in the feeder inconsistency can be found out and the alarm can be generated. Due to some transient processes in the circuit breaker or delay of updating of the topology, it is possible that the current has some value greater than zero even after the circuit breaker has changed "open" status. (Jakovljevic et al., 5) The flowchart is shown in figure 20.

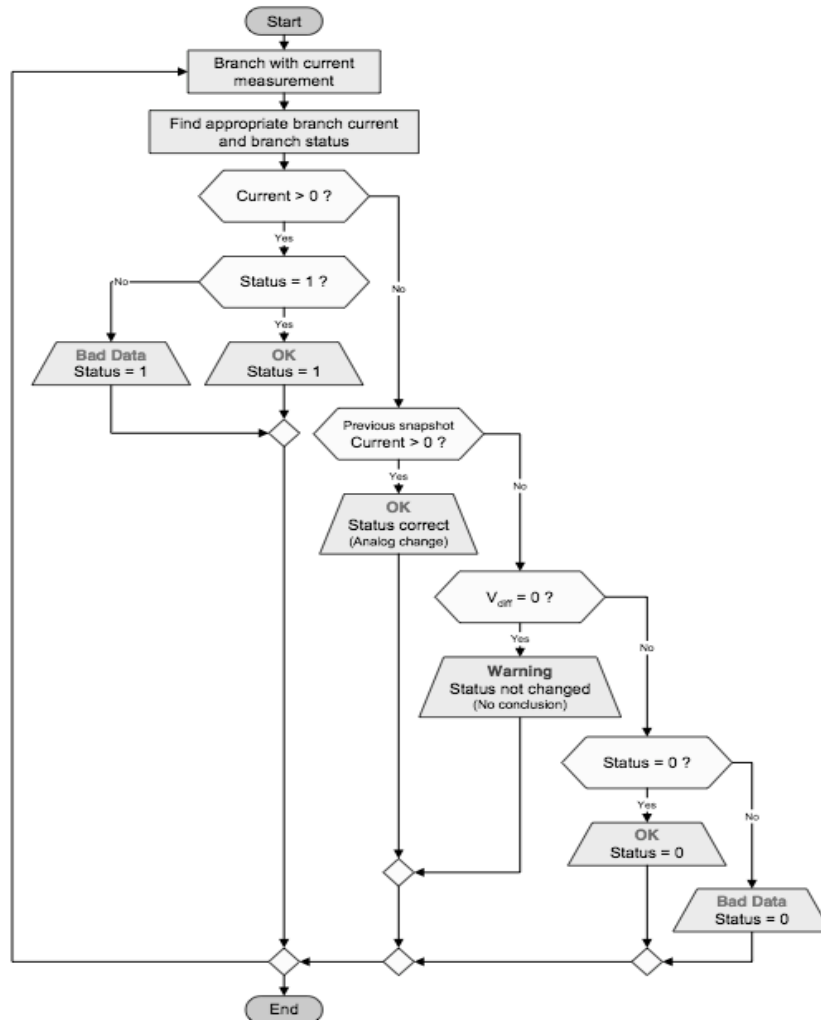


Figure 20: Algorithm for feeder status determination. (Jakovljevic 2003, 42)

The case when the equivalent circuit breaker is closed and there is no current in the feeder is not necessarily inconsistent because it is possible that there is not any load in the feeder. As well if there is no voltage difference between feeder terminals, feeder current will be zero even if the switching device is closed. In order to investigate that, the voltage measurements at the feeder terminal nodes could be validated. When both feeder terminals are equipped with voltage measurements,

absolute value of the difference between voltage phasors can be validated. If the validated voltage difference is greater than some already preset value, bad topology data exists. Then the alarm is generated and it is more reliable to change the value of feeder status to "bad" rather than to "open". (Jakovljevic 2003, 43)

When the actual voltage difference is small, the situation is considered normal since the voltage difference is insufficient to create noticeable current through the feeder even when the feeder switching device status is "close". The consistency is fulfilled. (Jakovljevic 2003, 43)

The last situation is when the equivalent circuit breaker is bad. The consistency check can not generate respective result. Actually the feeder current value can be checked and if it is greater than zero, it is possible that one of the disconnect switches in the feeder had erroneous status (undefined or fault) reported (which caused "unknown" feeder status). (Jakovljevic 2003, 44)

5.3.6 Time-Series Consistency Check

The validation routine can be executed also by checking a change from the previous state to the current state. Then the analog set of measurements and topology data is examined together. Their values are compared between the present and the last recorded value. This routine needs a database or some other reservoir where the previous state information is available. (Jakovljevic et al., 5)

The assumption is that only a change in topology can cause a change in analog measurements. What is a normal change of an analog measurement should be taken conditionally since there is always fluctuation in the power flow even in the normal operation of power network. Any change in analog measurement less than some already preset value is actually not considered a change. (Jakovljevic et al., 5-6)

The analog and topology changes since the last snapshot are detected. The routine examines the consistency of four possible combinations. One combination is when there is a change in both topology and analog measurement. The other one is when there is no change in those two. Both combinations inflict validation. (Jakovljevic et al., 6)

The third case is a change in topology without a change in analog measurement. This can happen for example when the equivalent circuit breaker changes from "closed" to "open" and there was no current in the feeder before it was opened (i.e. no load). The feeder status can also change due to topology data error. Since the true reason for the topology change is unknown, it is recommended to take caution due to possibly bad data. (Jakovljevic et al., 6)

The last case is a change in some analog measurement with no change in topology. This is more complex case than the previous one and it is more likely that the bad data is causing it. It is possible that due to some remote fault, sudden change in the power flow caused a change in analog measurements and no activity is necessary. On the other hand, rechecking the suspicious data can discover some local instrument malfunction. (Jakovljevic 2003, 46). The flowchart of time series checking is shown in figure 21.

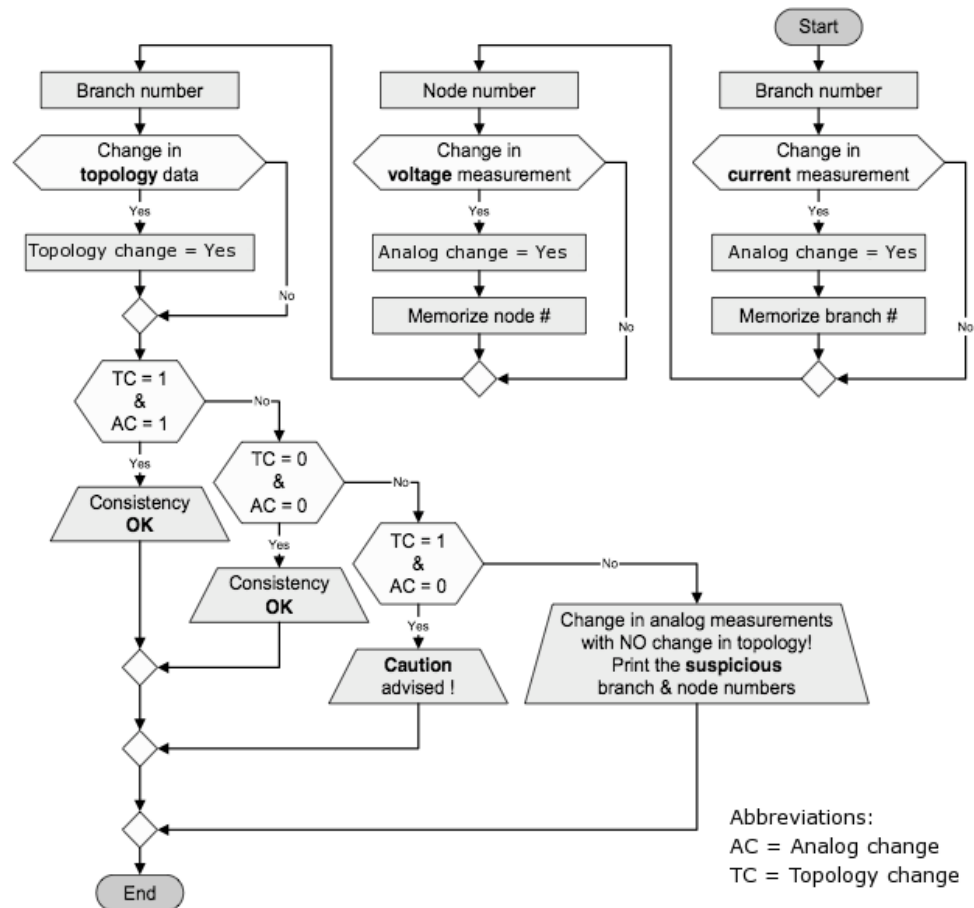


Figure 21: Consistency check based on time series. (Jakovljevic 2003, 45)

6 IMPLEMENTATION OF DATA VALIDATION IN MICROSCADA

The last part of the thesis introduces the solutions of the validation routines which were chosen to the MicroSCADA. A user interface was made with the Scil programming language which has been especially developed for MicroSCADA programming. The user interface was built so that it is easy to check validation states from the different location in the substation.

6.1 Power Balance

The first validation routine checks how big the difference is between entering and leaving power flows in the substation. Based on the Kirchhoff's first law, the difference between these powers should be close to zero. The substation was figured out by a simplified rectangle and the rectangle changes its color depending on the magnitude of the power difference. The percent value of the difference is calculated by formula 4

$$100\% \cdot \left(1 - \frac{P_{out}}{P_{in}}\right) \quad (4)$$

where, P_{out} is power leaving from the substation and P_{in} is power entering the substation.

The supposition is that power cannot flow from low-voltage level to higher. If the power flows from the lower voltage level to the higher voltage level, the alarm is generated. The difference between alarm states are defined by constant parameters which can be changed but it must be made straight to the code. The alarming colors change depending on how big the difference of the powers is. The colors are defined as follows:

- 30% \geq P the color is green
- 30% $<$ P \leq 50% the color is yellow
- 50% $<$ P \leq 100% the color is red
- 100% $>$ P the color is red

The states are shown in the figure 22.

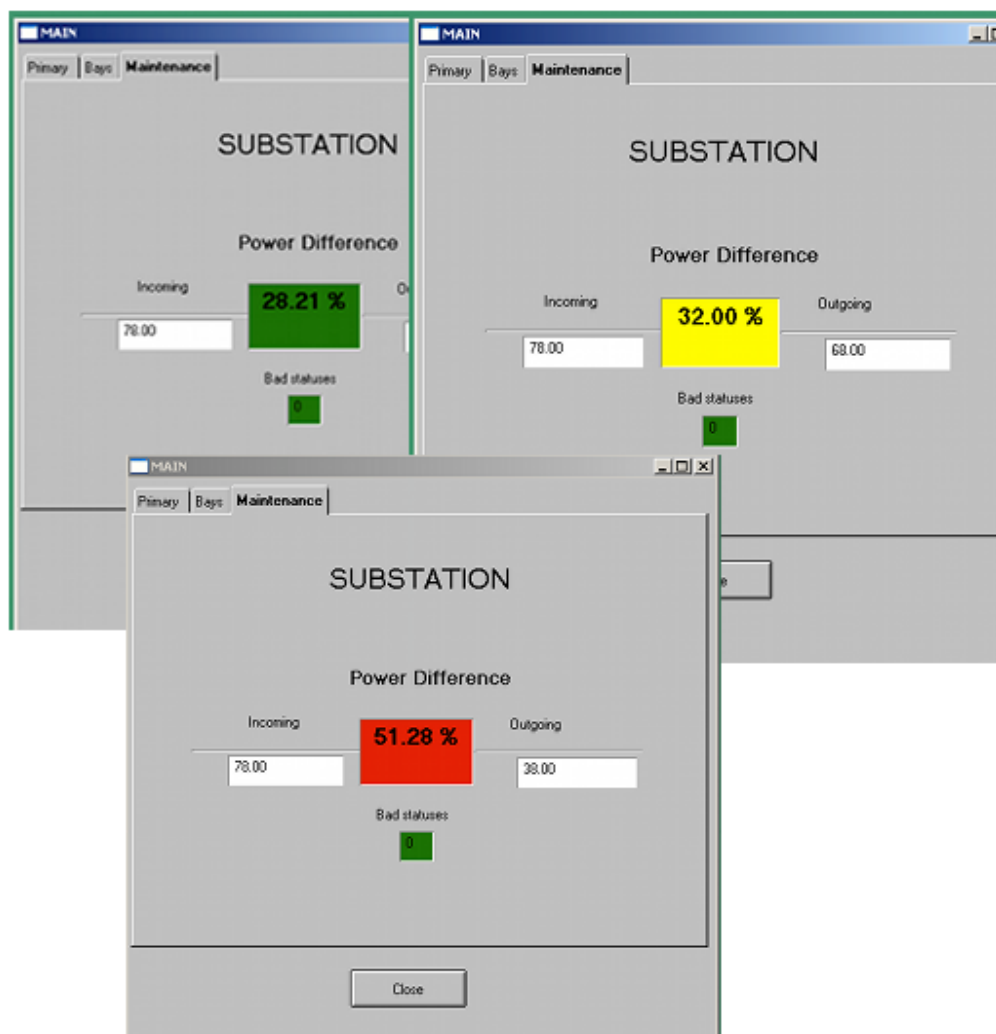


Figure 22: Different alarm states and percent values

As it was noticed earlier the powers should flow from the higher voltage level to lower and if this is not satisfied, the red alarm and text "BAD" is generated. The figure 23 shows the situation. The second situation, when the alarm text "BAD" is generated, is if the power difference is more than 100%.

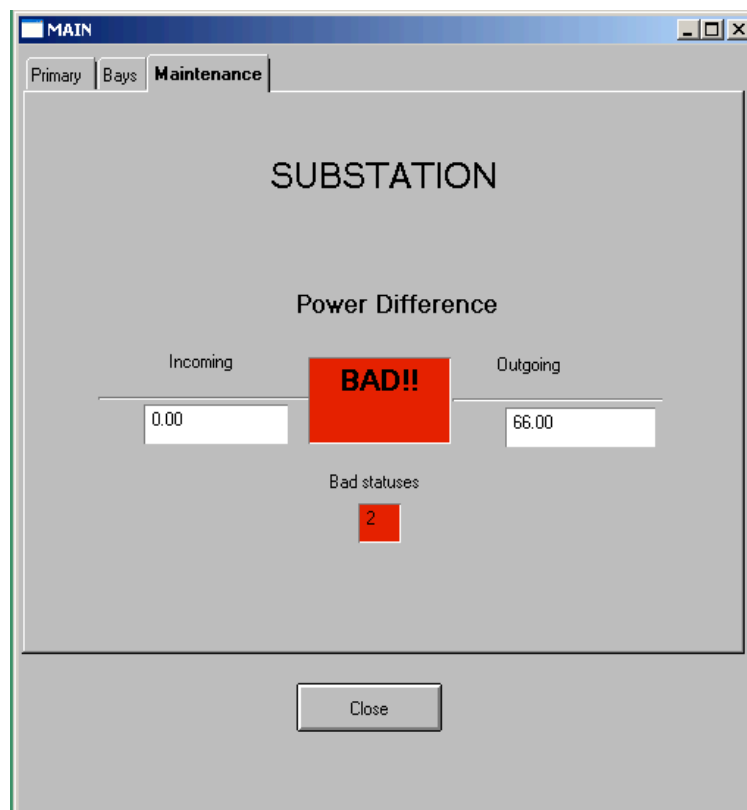


Figure 23: The value is over 100% or power flow is not valid.

Respect states for the measurements are used in the MicroSCADA. These states are defined by Object Status (OS) attributes. The status defines if the measurement is fault, obsolete, etc. If the OS attribute gets the value 0, the measurement is valid. The OS attributes of the powers, used in this window, are collected from the database and if the OS attribute is different than zero, it is defined as "Bad". If there is one bad status in the power measurements, the indication is defined to be

as yellow, and if there is more than one "Bad" status, the color is red. If there is not any indication the color is green. The different situations are shown in figure 24.

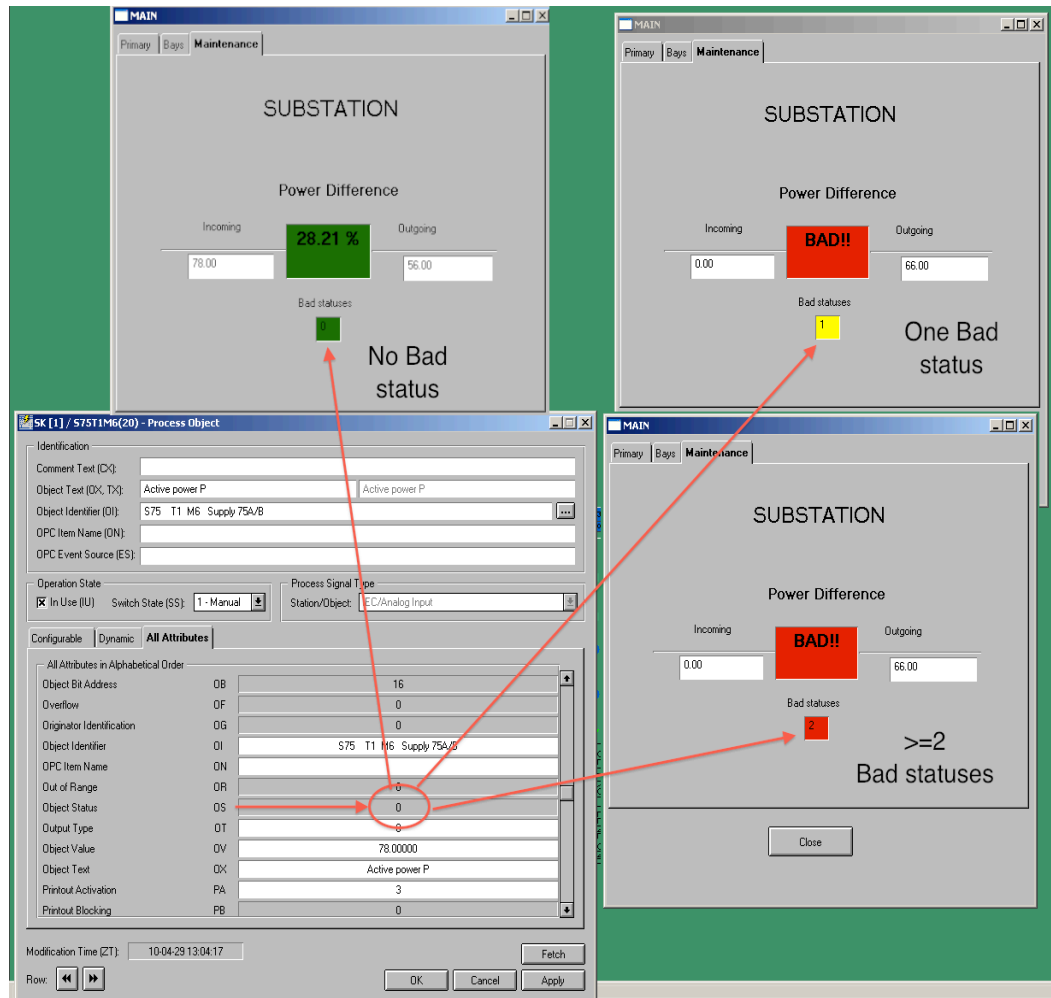


Figure 24: Zero, one and over two "Bad" statuses

6.2 Equivalent Breaker - Phase Currents

The second validation routine is to check the switching state and phase currents in the certain bay. The routine combine the switching devices in the bay and compare this status in the phase currents. The combined switching devices are called equivalent breaker. The combination is built based on information that in MicroSCADA the Object Value defines the state of the switching device. In this routine the status are handled so that

1 = Close

2 = Open

other = Unknown

In the process picture in figure 24 the two switching devices are handled as a one equivalent breaker and the value for equivalent breaker is calculated from statuses of both switching devices. Earthing switch does not have any effect in the equivalent breaker i.e. it is not considered. The calculation is simplified sum of the statuses so that if $Q1=1$ and $Q0=1$ then feeder status is 2 and equivalent breaker status is close. According to fundamentals of the electrical circuits there can be current in the feeder only if equivalent breaker is closed (feeder status is 2). This state is indicated by green "OK" text. If the equivalent breaker is something else than 2 and there is current in phases the yellow "Bad" text is generated. The figure 25 shows the indications

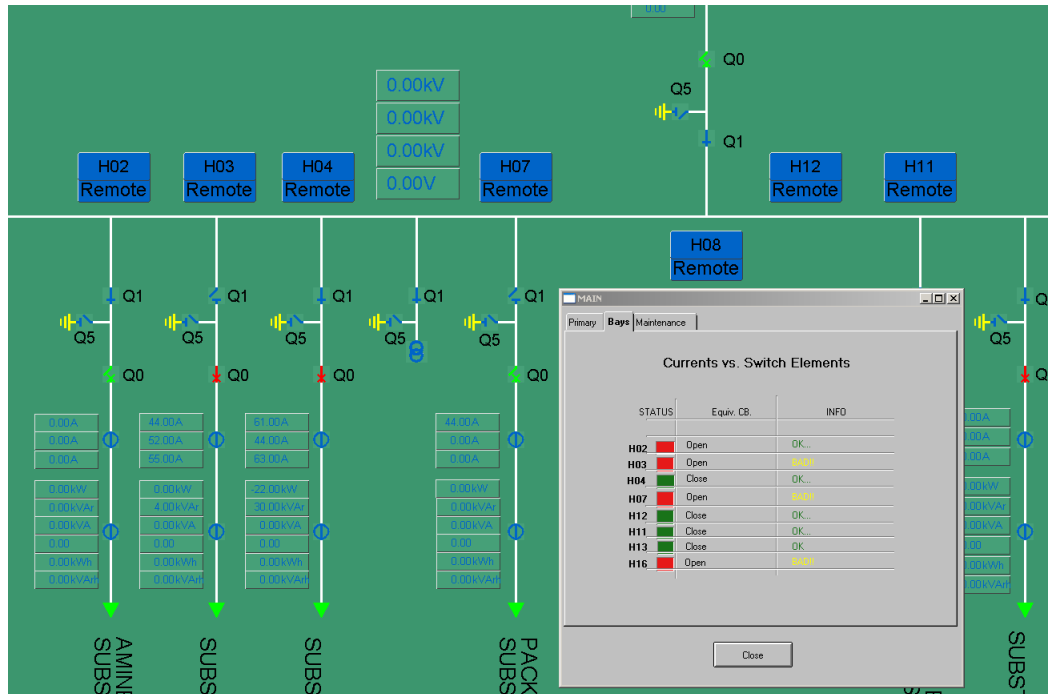


Figure 25: Indication are shown by text and colors

6.3 Primary Measurements

The third validation routine concentrates on primary measurements from active power (P), reactive power (Q) and phase currents (I1, I2, I3). The window indicates the value of the measurements and as it has been done before, the “Bad” statuses are indicated by colors. There is also an info square in the window which tells if the measurement is “OK” or if the measurement includes a bad status, the info square turns to “FAULTY VALUE”. The figure 26 shows the window.

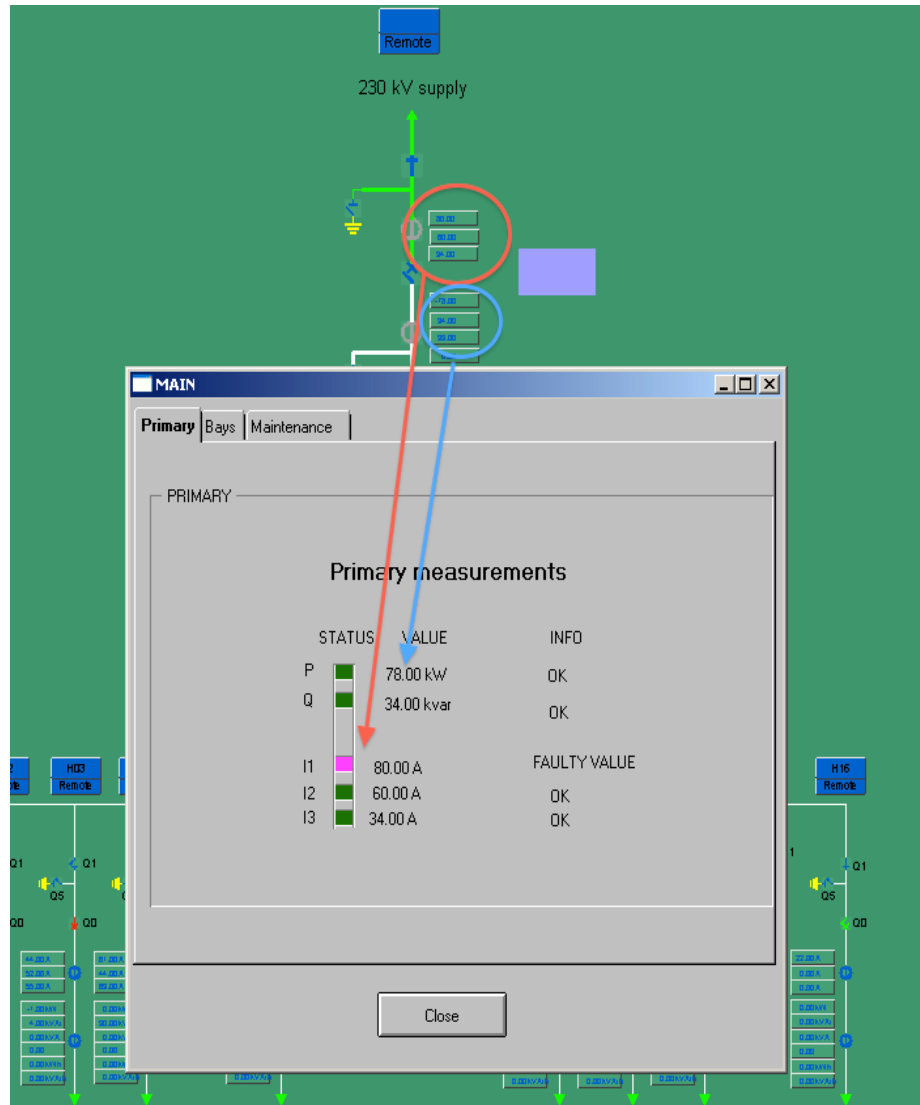


Figure 26: Primary measurements are shown by text and colors

7 CONCLUSION

If reliable validation routines are needed, a good knowledge on the primary process but also the SCADA system itself is required. The different SCADA systems handle signals in different ways e.g. a significance of the status signals can vary depending on the program. This same variation has to be noticed in protocols. For example, open value of the circuit breaker may differ between protocols or if this same signal is transferred between SCADA applications and the open status might change to close in the end.

It is possible to improve data validation in SCADA system with fairly simple methods. The simple program, as it has been introduced in the thesis, gives a notice to the operator and if there are "Bad" values in the SCADA database. In some cases suspicious data can be noticed and reported by the IED which makes it easier to start locating the source for bad or suspicious data. Data validation in the SCADA system is an interesting issue and only "the sky is the limit" to create routines for validation. However, there are also many challenges. It is not easy to build such a program which notices intelligently and reliably faulty or suspicious changes in the process. The program created in this thesis does not notice that, the updating intervals can differ between measurement values in the database. For example, the values that are used in formula 4, can vary to such a range that the wrong alarms are generated. Essentially, the calculation works well if the measuring is happening in real-time but this is not the case always. There can be a large power difference between entering and leaving power even if there are no faults in the process. If the measurement updating is not in real-time, one solution is to compare the measurement values with to values calculated from the database history. Then, of course, a special history database is needed and the estimation calculations have to be done in the history database. That kind of estimation is not

simple and if it is in use, the calculation has been executed by external mathematical program.

REFERENCES

Aumala, Olli. 2002. Mittaustekniikan perusteet. 11. painos. s. 144-145. Espoo. Otatieto.

Collins Cobuild. 1987. English Language Dictionary. First Edition. Williams Collins Sons & Co Ltd.

Cyclic Redundancy Check. 2009. [referred 28.4.2010]The paper is also available on website: <URL:<http://www.hackersdelight.org/crc.pdf>>

Djekic, Zarko. 2007. Automated Circuit Breaker Monitoring, Part 2. [online]. PSERC Publication 07-38. Project Report for the U.S. Department of Energy's Consortium for Electric Reliability Technology Solutions.[referred 20.2.2010]. The paper is also available on website:<URL:<http://certs.lbl.gov/pdf/auto-circuit-breaker.pdf>>

Djokic, T; Kezunovic, T; Kostic, T. 2005. Auto mated Monitoring and Control Using New Data In- tegration Paradigm[online]. Presented at 38th Annu- al Ha- waii International Conference on Systems Sci- ence, Waikoloa, HI. [referred 28.2.2010]. The paper is also available on website:<URL:http://www.pserc.org/cgi-pserc/getbig/publicatio/2004public/kezunovic_hicss05paper.pdf>

Elmore A. Walter. 2004, Protective Relaying Theory And Application. Second Edition. ABB Power T&D Company Inc. pp. 169

Fortune Automation, Inc. 2010. SCADA System Architecture <URL:<http://www.fortuneautomation.com/products-scada-system.html>>

IEC 61850, IEC Standard for communication networks and systems in substations. 1st Edition. Geneva, Switzerland

Jakovljevic, Sasa. 2003. Data Collecting And Processing For Substation Integration Enhancement[online]. Texas A&M University. Master of Science Thesis. [referred 7.3.2010]. The paper is also available on website:<URL:<http://repository.tamu.edu/bitstream/handle/1969.1/93/etd-tamu-2003A-20030324081.pdf?sequence=1>>

Jakovljevic, S; Kezunovic, M. Advanced Substation Data Collecting and Processing for State Estimation Enhancement[online]. PSerc consortium, an NSF I/UCRC, and Texas A&M University. [referred 7.3.2010]. The paper is also available on website: <URL:<http://citeseerx.ist.psu.edu/>>

Kezunovic, Mladen, 2006. Monitoring of Power System Topology in Real-Time[online]. Proceedings of the Hawai'i International Conference on System Sciences, HICSS 39, Kauai, Hawaii, Symposium on Electric Power Systems Reliability, IEEE [referred 15.3.2010]. The paper is also available on website:<URL:http://www.pserc.org/cgi-pserc/getbig/publicatio/2005public/kezunovic_hicss39_paper_09-09-05.pdf>

Lindh, Tuomo. 1997. Scheme for distribution automation and energy management applications in industrial power systems[online]. Lappeenranta University of Technology. Master's Thesis.

[referred 28.12.2009]. The material is also available on website : <URL:http://www.lut.fi/fi/technology/lutenergy/electrical_engineering/research/electricitymarkets/publications/Documents/Diplomityöt/dtyo_lindh.pdf>

Nieminen, Juha. 2009. Communication Bus Systems, Vaasa University of Applied Sciences, Electrical Engineering. Lecture material.

Olshausen, Bruno A. 2000 "Aliasing", PSC 129-Sensory Processes.[referred 2.3.2010]. The paper is also available on website: <URL:<https://redwood.berkeley.edu/bruno/npb261/aliasing.pdf>>

Protection Basics 2007: Introduction to Symmetrical Components[online]. GE Energy .The paper is also available on website: <URL:<http://www.gedigitalenergy.com/smartgrid/Dec07/7-symmetrical.pdf>>

Ramsden, Ed. 2001. An Introduction to Analog Filters. The article is also available on website: <URL:<http://www.sensorsmag.com/sensors/electric-magnetic/an-introduction-analog-filters-1023>>

Signal Processing Laboratory 2004. Digitaalitekniikan perusteet, Hammingin koodaus[online]. Helsinki University of Technology.[referred 20.4.2010]. The material is also available on website:
<URL:<http://wooster.hut.fi/digis/luento3/hamming.html>>

SPA-Bus Communication Protocol V2.5. 2001 Technical description, Version C, [online]. ABB Oy Substation Automation [referred 15.1.2010]. The paper is also available on website:<URL:[http://library.abb.com/global/scot/scot229.nsf/veritydisplay/811733b652456305c2256db40046851e/\\$File/SPAcommprot_EN_C.pdf](http://library.abb.com/global/scot/scot229.nsf/veritydisplay/811733b652456305c2256db40046851e/$File/SPAcommprot_EN_C.pdf)>

Terminal Diagram, REF615 Feeder Protection, Configuration FE05&FE06(E&F). 2009[online]. ABB Oy Distribution Automation [referred 10.5.2010]. The paper is also available on website:
<URL:[http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/82be2df3e1f8f09bc12575cc00352621/\\$File/2RCA021838.pdf](http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/82be2df3e1f8f09bc12575cc00352621/$File/2RCA021838.pdf)>

The working group for use of disturbance recorders 2006. Considerations for Use Of Disturbance Recorders [online]. The System Protection Subcommittee of The Power System Relaying Committee of the IEEE Power Engineering Society. [referred 4.3.2010]. The paper is also available on website:
<URL:<http://www.pes-psrc.org/Reports/C5-Final%20Report.pdf>>

Yliaho, Jaakko 2008. SCADA Systems for Electrohuila, HIS600 Data Validation. ABB Oy Substation Automation Systems. Revision B

