448

Refurbishment Strategies based on Life Cycle Cost and Technical Constraints

Working Group
B5.08

February 2011

Refurbishment Strategies based on Life Cycle Cost and Technical Constraints

Working Group B5.08

Members

Peter Leushuis, Convener (NL), Jokin Galletero Lopez (ES), Daniel Garcia Garcia (ES)
Jean-Michel Grellier (FR), Frank Koers (NL), Thomas Küng (CH), Mika Loukkalahti (FI)
Jerzy Pillar (PO), Didier Wiot (BE), John Wright (GB)

ISBN: 978-2-85873-137-4

Table of Content

INTRODUCTION

Many utilities around the world are confronted with the fact that a number of their secondary systems are approaching the end of their technical life. Such systems include a mix of technology from “old” electromechanical and analogue systems to first generation digital systems. Utilities are faced with the decision to either extend the working life of the existing systems, by say upgrading, refurbishment etc or totally replacing them. Drivers for the refurbishment of secondary system(s) include no spare parts, lack of knowledge, missing documentation and the introduction of new functionalities, such as self-check.

The goal of this report is to propose a practical guideline to assist asset managers when making decisions related to refurbishment strategies. The triggers for such decisions are often operational risk or technical constraints and will be typically followed by a Life Cycle Cost (LCC) calculation to determine the financial impact.

Practical examples of refurbishment strategies will be given in chapter 6.2.
The working group distributed a questionnaire to a number of utilities, the results of which are detailed in the appendix.

1 DEFINITIONS

Due to the varying interpretations of the terminology used in this field of Engineering, the working group deemed it necessary to define the following terms for the purpose of the report.

System Level (Bay or Substation)

Replacement: is the process of replacing the majority of the existing infrastructure with the intention of improving the remaining lifetime and the functionality.
Example: replacement of a complete protection cubicle retaining the interfaces to the primary system, i.e. CT's, VT's.

Refurbishment: is the process of major maintenance or minor repair to the existing infrastructure with the intention of improving the remaining lifetime at a minimum cost.
Example: Replacement of a number of protective relays within one or more bay while retaining the existing cubicles.

Retrofit: refers to the addition of new technology or features to older systems with the intention of improving the functional level at a minimum cost.
Example: replacing old electromechanical relays by new digital relays (existing cubicles are fitted with new digital relays) often using the same housing.

Device Level

Replacement: replacing of a device by one of a similar type or functional equivalent.

Repair: restoring of the device functionality after failure

Upgrade: improving of the device functionality or performance (firmware, software or hardware)

The following table shows the approximate / anticipative effects of each type of change that is described in this report.

Table 1: Change options classified by level

		Remaining Lifetime		Functional Level			
	Definitions	Unchanged	Improved	Unchanged	Improved	Risk	Cost
Substation Level	Replacement		X		X	High	High
	Refurbishment		X	(X)	(X)	Medium	Low
	Retrofit	(X)	(X)		X	Low	Low
Device Level	Replacement		X	(X)	(X)	Low	High
	Repair	X		X		Low	Medium
	Upgrade	(X)	(X)	(X)	(X)	Low	High

X = driving force

2 SECONDARY SYSTEM EVOLUTION, LEVELS AND POSITION

This chapter describes briefly the technical evolution of secondary systems, the different levels in a substations and the position of the secondary systems in the network. In order to assess a chosen strategy, decision makers need to understand these items.

2.1 Technology Evolution

Technology evolution, from electromechanical to numerical systems, has brought considerable economical and technical benefits. The price of such numerical devices is comparable or less than electromechanical devices. The numerical systems offer more functionality and information about system status. With modern systems, maintenance intervals can be extended and onsite commissioning can be reduced. The numerical system can be extensively tested at the factory, thereby reducing testing on site. In the next chapter the technical evolution of secondary systems are briefly described.

2.1.1 Classical to Static

Traditional protection schemes consisted of many electromechanical relays all interconnected by hardwiring. The relays were typically housed in multiple protection cubicles, taking up a considerable amount of space in the substations. Classical systems required a considerable amount of installation and commissioning effort. The schemes were inflexible, changes required additional relays and wiring modifications. Due to technology development, electromechanical relays were replaced by static relays. The static relays allowed a reduction in CT requirements and reduced in size, resulting in space saving. However they require a DC supply. The static relays were still one box, one function, hence a considerable amount of hardwiring was still required.

2.1.2 Static to First Generation Digital

With the introduction of multifunctional numerical relays, protection refurbishment started to increase since a number of benefits were obvious:

- Reduced panel space due to multifunctional relays
- Reduced hardwiring; replaced by software coding
- Self monitoring; CB Status
- System monitoring
- Fault recording
- Disturbance recording
- Reduced on site testing since scheme can be simulated in the factory
- Ease of interface to SCADA & DCS
- Possibility to simplify or automate test on site

It is important that the skills of the engineers are in line with the technology. Engineers have to be trained to program and maintain such devices. They can be complicated, and the management of software files and schemes can be time consuming and difficult.

2.1.3 First Generation Numerical to Numerical Today

Some of the most important features of a protection device are reliability, ease of setting and testing. Numerical systems offer a large amount of protection functions in the same box, such as; self supervision, fault recording and programmability Drawbacks of this new technology are; complexity and version handling of software. Hardware depends on the newest PC technology and software bugs (which fortunately are minor).
Issues related to the first generations systems are;

- Possibility and cost of upgrading or renewal of first generation systems (not at the end of their lifetime),
- Ageing of digital systems (especially PC-based ones),
- Update policy for digital systems (step-by-step or only when needed - if this is possible), version handling requirements for tools, PC's, operating systems and vendor software. In early digital products, the upgrade ability was limited. Compatibility between some relay setting tools and early digital products have been problematic. This requires a lot of attention from the user.

2.1.4 Hybrid System (Conventional / Numerical System)

In many substations around the world protection systems are hybrid, i.e. a mixture of different technologies. This mixture of technologies results in the following:

- Engineers require training in different relays and different technologies
- Mixtures of auxiliary voltage levels
- Different environmental operating withstands
- Different ratings
- Different CT / VT requirements
- Mixture of traditional scheme drawings and internal software scheme logic.

Due to the mix in systems; some points need to be addressed, such as;

- Trip relays required or trip breaker direct?
- External or internal trip circuit supervision?
- Can the numerical relay exactly simulate the old scheme?
- Is the old scheme still valid or can it be rationalized?

2.2 Secondary system as a part of the overall system

The secondary system is the heart of overall power system. Auxiliary power, protection, measuring, control and monitoring systems are key elements to the successful operation of the total system. The protection and control system is maybe the most demanding and difficult part of it, as it includes the user / operator interface to the whole installed system for control and support of operation philosophy.

2.2.1 Overall system

The overall system covers all equipment to generate, transmit, distribute, control and ensure electrical power. This is divided into primary and secondary system.
Separation of primary and secondary system:

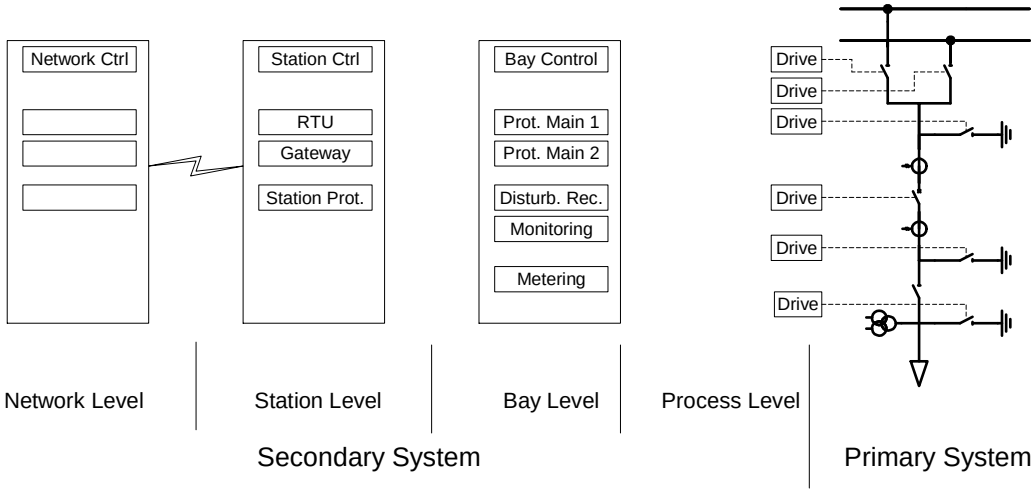


Figure 1 Overview overall system

The primary system covers the high voltage part of the system on which the electrical power of the network is flowing. It covers overhead lines, transformers, circuit breakers, disconnectors, instrument transformers (CT's and VT's), surge arrestors, reactors, etc.
The electrical part for some of the primary devices, like the drives of circuit breakers, transformer / tap changer control boards and disconnectors are considered part of the secondary system

2.2.2 Description of secondary systems

The secondary system covers all electrical parts, which support a utility / grid operator to control and ensure the flow of electrical power. To understand and validate its value the

secondary system itself is subdivided in 4 hierarchical levels:

- Process level
- Bay level
- Station level
- Network / grid level

Depending on the technology used, functionality from more than one level can be allocated in the IED (Integrated Electronic Device) e.g. Station controller controls host of several bay control functions.

2.2.3 Process level:

All secondary equipment to control, monitor and protect single primary devices , such as; motors, contactors relays, energy limiting switches of circuit breakers and disconnectors, transformer / tap changer control box directly mounted at the transformer and secondary wiring between primary equipment and bay cabinets

2.2.4 Bay level

All secondary equipment to control, monitor and protect one bay / feeder / unit.
Bay controller including interlocking and synchronization equipment respective synchrocheck equipment

- Bay protection
- Revenue meters
- Monitoring (online: display of actual operation value, e.g. volt, amp, freq. and power meters)
- Disturbance recording per bay

2.2.5 Station level:

All secondary equipment to control, protect and monitor a substation:

- Station controller (sequencer for control automatic functions)
- Station control system (conventional: electromechanical or numerical: microprocessor / PC based)
- Gateway
- RTU’s
- Station protection (bus bar protection, load shedding functionality, high speed bus bar transfer functions)

- SOE (sequence of event list)
- Disturbance evaluation

2.2.6 Network / Grid level:

Network management system:

- Network control system (main user interface for the grid operator)
- Network information system
- Network maintenance system
- Telecommunication between network and station level.

2.2.7 Purpose of secondary system

The secondary system can be seen as an interface between the primary system and the network management system. Acquisition cost of the protection and control assets is generally less than the price of the primary assets. Still secondary systems need more engineering work than primary system: parameterization, setting and commissioning is time consuming work. On the other hand the failures especially in protection systems (false trips or unselective trips) are very significant and unwanted. Also every primary fault has to be detected by the protection and control systems. With a good secondary system you can detect and isolate the primary faults fast and selectively and obtain the right information about them. However, you cannot prevent primary faults with protection and control systems.
In principle, the secondary system could not totally prevent the risk of damages in the primary system. But it helps to minimize the direct damages of primary equipment failures by interrupting power as well as reducing the consequential damages out of a grid failure e.g. in case of a busbar fault.

2.3 Power system market

The power system industry is working in an environment that requires optimal management of the power system network at all system levels. At transmission level companies must ensure a stable and optimal operation of the grid, whereas in other voltage levels there is growing competition in the market place. The privatization of the power system industry creates the opening for a new electricity market differing in all aspects from the traditional old market. A market where the consumers become customers is due to that new energy supply and traders are appearing in the market. In fact, in the very near future, power system industries all- over the world will see more and more power producer, retailers and network companies.

Therefore, the need to automate the existing substations shall be evaluated by the utilities in order to meet the expected challenges of the future market and the reliability of the existing equipment.
Each utility shall first of all, prepare itself and its network for the challenges ahead. In order to do this, the utility must acquire full knowledge of its automation needs and benefits. The utilities in their effort to automate the existing substation shall focus on two aspects that shall influence the optimum control of its power system management business. These two aspects are economical and technical.

2.3.1 Economical reasons for substation automation

The economical reason plays a major part in justifying existing substation automation (SA). The information about the power system gives the utility the strength to be more successful and competitive in a free market where competition between utilities and the deregulation of the power system industry is being introduced. In this type of environment the information becomes a very strategic requirement in the power system industry market where a fast decision is required. This cannot be obtained from an existing conventional type substation. The changes, which are occurring presently and expected in near future in the power systems industry can be listed as follows.

2.3.2 Changes in the power system market

Major changes have taken place in the power system market and more are expected in the future. The traditional market where Nation/Area-wide power control centres play the role of control and marketing the energy, since there were no other suppliers of electricity to the customer, is disappearing gradually and this trend will continue at a faster rate. Energy service Companies are replacing power system companies and new retailers of energy are being introduced in the market. Also, the privatization/deregulation of the nations electrical networks find interest for even non-national Companies in the market. This gives the chance to have a new power producer and retailers. Such type of market shall be an open type where the consumer is becoming a customer and he can choose his supply contractor, increase the competition in power system efficiency while maintaining system security and reliability. A market having a variable electricity price at present and in the future depending on the market competitions as what can be said Electricity at the Market price.
Activities of transmission and distribution utilities have to separate on open market business (energy market) and regulated business (transmission and distribution). On the energy business there are new functions required for running energy market, while on the regulated field, there are no major changes regarding required functions. There is only the need to provide all necessary data for supporting energy market activities. It is not clear,

who should cover the costs, if this functionality would exceed equipment installed for utility use.
This type of environment requires that the existing substation shall be upgraded to provide the necessary urgent information. This is also in addition that the market must meet the loads needs.
Other additional functions in SA have to be economically proved by other factors, than new energy market situation.

2.3.3 New Nature of Power System Market Requirement

As mentioned previously, the Electricity Consumers in the new market become the customers. These customers will have the choice to get power supply from different suppliers that are geographically spread.
Therefore, new types of power supply agreements shall be introduced in the market. These power agreements shall handle the power supply at different interval of different prices and different suppliers. This is what is called a free market price and place. Suppliers provide daily information of the power transfer capabilities and retailers receive consumption information. This requires huge, accurate, fast information of data for billing the Customers instantaneously. Moreover, the customers also know their daily operational cost in order to properly plan their production to minimize cost and increase their profit. In this case, information is becoming a must and existing substations should look to automation if they are going to a play part in such a market.

3 DRIVING FORCES (TRIGGERS) FOR CHANGE

Reasons for refurbishment, retrofit, replacement and/or upgrade can be various. Driving forces can be extension of the primary configuration, equipment obsolescence, failure risks level, lack of knowledge or maintenance cost. In the next chapters those driving forces are explained.

3.1 Extension of the station

During its lifetime the system is also likely to change, for example, increased fault levels, change in load or system expansion. These will all impact on the protection system design and settings. This action is commonly ignored and has lead to many unnecessary protection scheme operations and under protected primary plant.
Also, an extension in a substation may be a sufficient driver for replacement of existing protection relays, even though they would have some remaining calculated life. If the extension is of significant measure, such a total protection system replacement becomes even more obvious. This gives a benefit on spares handling, ease of use, documentation and periodical testing, as all relays at one substation are of same types and versions. Extension of a substation can also bring along a need to reduce size of new equipment due to space constraints and may give a final push to replace also the old devices. In some cases there is a need to reduce energy consumption with modern IED's due to batteries dimension requirements.

3.2 Equipment obsolescence

Lifecycle management ensures continual operation without substantial interruption due to hardware failures, obsolescence or incorrect application. The value of the protection equipment asset depends on the way its lifetime is managed. Without any particular focus on this process, the peak value of the asset will be at the initial installation stage, after which the asset will start to decrease. The more lifecycle support provided the slower the depreciation of the asset.
For a given technology the cost of spare parts maintenance generally increases with time, its explanation is that new technologies get a better cost/functionality ratio. Fabrication of old technology devices is therefore limited to spare parts: the amount of production decreases and the relative cost of each piece rise.
Also, these types of oldest relays start to become obsolescent and their maintenance may cost too much. Furthermore, the risk of having a too slow operation of a main protection leading to non-selective other trips in the HV networks may give a reason to replace such relays.

The below table illustrates the key milestones of a products life.

Table 2: example of Lifecycle identification *)

Status	Characteristic	Approximate Time
Active	The product or system is in manufacture and subject to continual development (hardware / software changes)	8 years
Legacy	The product or system can still be provided as new, but no new features are developed.	10 years
Pending Obsolescence	The product or part of the system is declared 'Pending Obsolescence' and customers are notified of this event. Key actions are identified.	2 years
Obsolete	The product cannot be obtained as new. A reduced set of services remains available (for example repair but not modify).	5 years
Extinct	No services are available, except commitments related to a specific maintenance contract.	-

*) based on manufacturers data

3.3 Reliability and availability

It is clear that over time the reliability of the protection system goes down bit by bit. At the final stages of their expected lifetime the reliability of protection devices can reduce significantly. Modern relays have better availability and reliability due to self-checking function and this reliability improvement need can be impact for changes in the secondary side of the substation.

The consequences of protection relay failure have the potential to be catastrophic. The following list details a few:

- Disruption in supplies due to incorrect design and settings or due to relay malfunction
- Damage to equipment due to excessive fault current resulting from long operating times.
- Incorrect operation of plant i.e. motors stalling due to low voltages.
- Fire and explosion due to excessive fault current resulting from long operating times.
- Loss of life or serious injury.

A system fault may be a rare occurrence, but unless the protection is maintained and properly serviced then it may not operate correctly. With correct maintenance and application, should a fault occur, the damage and disruption will be minimised. Therefore to maintain optimal performance of the protection equipment, it is very important to manage the life cycle of the protection scheme.

Cost reduction through improved efficiency is the main factor for renovation / refurbishment of an electrical substation. This is achieved through better network operation and reduction in the cost of substation maintenance. In general, for a given technology the cost of spare parts maintenance generally increases with time, the reason is that new technologies with a better cost/functionality ratio progressively replace the old ones.

Another important point to comment on are self-checking capabilities; these can significantly reduce the necessity of periodic maintenance, if such information can be retrieved remotely. Although self-checking cannot prevent or detect all kind of miss-operations, self-checking reduces the complexity of some maintenance because some points are continuously checked by this capability.

The settings in electronic relays may start to change slowly (zone reach in distance relays, current settings, time settings). This increases the risk of having a slow operation of a main protection, or no operation at all, leading to non-selective trips in the HV networks. Thus, this may give a reason to replace such relays.

Due to fast diagnostic of the problems in the system and more information about the power system the modernization of the secondary devices increases the reliability of the substations and shortens the period of diagnosis. This resulted in faster restoration of the substations.

3.4 Lack of competence and documentation

For electromechanical relays one driver for replacement is that the utility may have lack of documentation, lack of competent and skilled relay engineers and technicians as well as lack of suitable tools for testing and repairing.

One problem with digital relays is the version handling with quite limited functionalities in their first versions they are not easy to upgrade into newer versions, at least not without sending the relay back to the factory to do it. However, this is seldom a driver for replacement.

Utilities at present are facing difficulties in documenting all changes and upgrades which are done to the network. In other words, there is no “as built” which reflects the actual site conditions specifically the secondary equipment. There is a considerable amount of time wasted in verifying the existing installation before starting any implementation upgrade or modification to existing installations.

The new IED’s (compatible with IEC 61850) provide self-describing capabilities which can

be used to create system documentation as a part of the current system implementation.
However in certain cases utilities decide to specify / approve one firmware version for the product which they purchase. With this approach they reduce problems that could be derived from having different versions installed. This approach may be recommended for fixed application without need for extra functionalities.

3.5 Maintenance savings

An examination of the capabilities and functionalities available in modern protection and control devices may influence the decision to switch earlier than expected to new schemes to minimise maintenance costs. Self-checking function gives the possibility to reduce the amount of periodical maintenance.
Maintenance strategies strongly differ from utility to utility. Periodical protection test interval times vary usually from 1 year to 6 years, old relays need more maintenance than the new ones. Transmission network protection relays must be secured as good as possible, so the test intervals at transmission level are usually shorter than in the lower voltage levels.
Proper and extensive periodical relay testing consists of testing of the total protection system including relay, measuring circuits, tripping circuits and signalling circuits. Numerical systems are equipped with measuring and tripping circuit fault detection however shelf-check functionality does not cover the complete system. Even with self-check functionality testing is still necessary. The need for complete testing of all settings and zones is not essential due to digital and numerical technology.
During a test there is always a risk that a human failure is introduced. In some cases test has to be postponed due to high load of connections in the network.

3.6 Functional requirements and added value

Early protection schemes may not be considered sufficient anymore and thus the increased performance and functionality capabilities can be a driver for change.
Functional integration capabilities make it possible to group all the feeder functions into a single device thus replacing a collection of elementary elements. This reduces the cost of the spare parts and copes with the new functional needs. Other drivers for change may be equipment standardisation
The new business needs, which require more information, will direct the utilities to upgrade the existing substations. Therefore information is needed about the industrial as well as other types of customers, i.e. computerized load forecast, complicated metering system bulk trading and energy management. The accuracy and the reliability of the data depend on the utilities/traders. Therefore the data availability gives the utility the chance to

be strong in a very competitive field. In the next subchapters the major technical issues that require the upgrading of the existing conventional substation are described.

Examples for need of new functions

In Helsinki Energy (FIN) three most wanted new functions of modern IED's are: self checking function, disturbance and event recording and free programmable integrated functionality. These functions are often also triggers for secondary changes. Self-checking and disturbance recording functions give the possibility to improve reliability and availability of protection system. The possibility to integrate many functions into the same IED gives financial savings, especially at MV level, where separate over-current relay, directional earth fault relay and auto-re-close relay were used before. At HV level modern relays provide options to combine synchro-check and backup over-current relay into differential and distance IED's.

3.7 Data requirement

Information (or data) plays a very essential part in optimal management of the power system. Therefore, more and more data is needed continuously to the master control stations. Data, such as alarms, breaker status, state monitoring, real time acquisition of measurements (voltage, current, active and reactive power, etc.), energy management programs availability and energy metering. This huge data requirement, it's availability and accuracy is a must in the modern power system industry. Therefore, the power control centres in the near future will become Information Technology centres. This requires the existing substation to be upgraded to automated substation to be able to cope with required information.

Not only the network control centre but other parties are interested in more data. Protection engineers need to know if their protection has worked as planned, primary maintenance engineers need preventive monitoring information from the process and network planning need information about the load. There is a need for information to coordinate between engineering, planning, maintenance and operation. Separate maintenance channels connected to the communication bus of the substation automation system or connected straight to the IED's could be a solution for separate needs for data.

3.7.1 Functional demands and performance enhancement

The new modern system offers the addition of new functions to the existing modern equipment, unlike the conventional existing system which might require considerable changes in the secondary equipment to add additional functions. The modern control system provides the chance to obtain a function from different hardware units into the master station software.
Next the new functionality and performance of modern IED's are listed, they are divided into 5 subgroups: Protection functions, Control and automation functions, Fault information, Communication and Monitoring & supervision.

Protection functions

Sensitivity: Better sensitivity and wider range of settings are possible. Choice of characteristics is possible for better protection performance.
Ease of operation: Multiple groups of settings are possible which could be remotely selected or automatically selected. This feature could lead to ease of operations since manual relay setting changes are avoided for transfer bus operation etc.
Accuracy: Almost no drift in pick up values due to digital techniques. Analogue measurements (currents, voltages, PF, etc.) with good accuracy can be measured.
Multiple functionalities (integration): Many functions are built into the relay: auto reclosing, synchrocheck, trip circuit supervision, external trip signals and option to have multiple protection functions in the same box will help to reduce the number of devices and simplify panel wiring leading to higher reliability.

Control & Automation functions

Improved local operation: State-of-the-art HMI application provides higher security of operation, e.g. select and operate functionality
Improved interlocking functionality: Possibility to implement interlocking logics using data available in the control system
Access to more data: Allows implementation of new or improved automation functions
Power system monitoring: Low frequency, low voltage, load shedding, blackout functions may be described with formal language of IEC 61131-3 and easily integrated in any IED
Time synchronization: By using serial or Ethernet communication bus it is possible to synchronise all IED's in the substation

Fault information

Configurable alarms and trip: Alarm and trip/re-close information are programmable and can be assigned to **particular** outputs like contacts or LED's. Group alarms can be customized as per utility practice/ standards.
Fault targets/ indications: Extensive fault data is available on local display
Fault disturbance record: Built in DFR function eliminating separate fault recorders. Separate disturbance recorders are not necessary for recording of current and voltage waveforms. The disturbance data files can be used in simulation of the power system incidence for detailed analysis by using relay test kits.
Power system fault location: Distance to fault location is built in, helps in faster restoration of power supply.

Communication

Communication interface: Integration with Substation Automation through serial or Ethernet communication bus will enable better access to IED -data/information by multiple actors. Fast communication enables chance to get more valuable information from the process.
Maintenance channel: Separate maintenance channel or maintenance channel integrated into Ethernet bus gives opportunity to collect (straight from IED's) protection and disturbance information for protection engineers and condition monitoring data of primary devices for maintenance engineers.

Monitoring & supervision

Supervision: Modern supervision functions provide better availability like IED internal supervision, trip circuit supervision, measuring circuit supervision, auxiliary voltage supervision, etc.
Counters and statistics: Modern IED's can make statistics concerning primary devices like counting number of primary switching device operations, I^2t counters, interruption statistics, etc.
Trends: Measuring capabilities of new IED's could give more information of power quality (e.g. voltage levels, harmonics, sags and swells, flicker), measured temperature trends, measured gas pressure trends, etc.

4 REFURBISHMENT STRATEGY

As mentioned in the previous chapters there are a number of different reasons for replacing an existing secondary protection and control system, namely;

- the risk associated with the existing system is so high that additional steps are required to improve it.
- the additional benefits of a new system are so high that the overall performance of the system improves.
- the costs associated with a new system are lower than the system that is in operation.

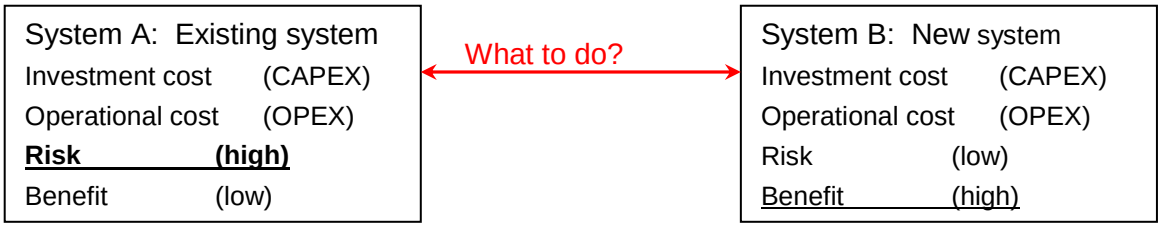


Figure 1: what to do system A or system B?

In the next chapter some of the basics related to risk management and financial models are explained.

4.1 Risk management introduction

Risk management is a methodology whereby in a systematic approach all risk aspects are analysed. With the results of the risk study a strategy can be developed. This strategy can be accepting the risk or reducing / controlling the effect of the risk. Risk management is not only traditional focussed on physical or legal items e.g. disasters, accidents, and environmental aspects such as fire, earthquake etc. but also on network risk, such as blackouts. There is also financial risk management that focuses on the financial risk of a project.
The objective of risk management is to reduce different risks related to a pre-selected domain to the level accepted by the company or society.

In a risk management process different steps shall be followed, namely:

1. identifying all possible risks
2. catalogue the risk in different domains
3. assessment of the identified risk
4. identify the objectives of the stakeholders
5. analysing results assessment and objectives stakeholders
6. risk treatment

4.1.1 Identifying all possible risk

This first step is to identify all possible risk. A complete risk assessment and identification of all possible risks can be very time consuming. It is advisable to start identifying only those items whereby the risk is very high or the probability of the occurrence of this risk is very high. If the result of the risk analysis is unsatisfied, then a deeper analysis of all possible risks might be needed.

4.1.2 Catalogue the risk in different domains

The second step of a risk study is to catalogue the risk in different domains. The domains are not fixed. For example the domains for a protection and control system can be SAFETY, ENVIRONMENTAL, IMAGE, REGULATOR and POWER QUALITY. The reason to catalogue the risk is that in different domains the risk level can be different. It is necessary to calculate the risk in each domain since the risk level within the various domains can vary.

The table below gives a brief example;

Table 3: example identification and catalogue risk

	Description of the risk	Safety	Environmental	Image	Regulator	Power Quality	…
Lacking of knowledge	…	X		X		X	
Lack of spare parts	…				X	X	
Reduced reliability	…	X			X	X	
Reduced availability	Change unwanted power outage	X	X	X	X	X	
Missing manuals	Long repair time		X	X	X	X	
….	…						

4.1.3 Assessment of the identified risk

Once the risks have been identified, the next step is to assess the probability of occurrence and the potential impact.

The standard definition of risk is change multiplied with effect:

Equation 1: risk

$$R_i = L_i p(L_{i)})$$

$$R_{total} = \sum_i L_i p(L_{i)})$$

Where:

L_i potential lost

p probability that the loss will occur

The assessment of the risk is an important step in any risk management study. This step might start a lot of discussions. The figures needed to assess the probability and impact in most cases are not based on large databases. In most cases the figures should be more pragmatically defined. The standard equation of risk is change multiplied by the effect. This means in theory change and effect have the same priority. Sometimes this method of calculations does not give the right feeling of calculating a risk. This might be the case at quantifying risk related to safety. For these items it might be wise to use only the probability in the assessment.
In many cases it is very difficult to find hard figures. In order to establish a common understanding of the risk without detailed investigation it might be helpful to reduce the amount of values that can put in the table. For example:

- Potential lost
  - Very low: less than 10 k€
  - Low: between 10 k€ and 50 k€
  - Moderate: between 50 k€ and 250 k€
  - High: between 250 k€ and 1000 k€
  - Very high: more than 1000 k€
  -
- Risk
  - Very low: less than once every 100 year
  - Low: between once every 100 year and 25 year
  - Moderate: between once every 25 year and 5 year
  - High: between once every 5 year and year
  - Very high more than once every year

4.1.4 Identify the objectives of the stakeholder

The next step in a risk management study is to identify the objectives of the different stakeholders. The stakeholders can be; regulator, the company board, shareholders, society.
The objectives of the stakeholders shall be combined to one overall objective. The objectives can be different in the different domains.

4.1.5 Analysis of risks assessment and objectives of stakeholders

The last step in the risk study is to compare the results of the risk assessment with the identified risk objectives. After the risk is compared, the system that is studied should be classified in one of the three categories, namely:
The risk level is lower than accepted risk, no further measures are needed.
The risk level is higher than accepted, but with some additional measures the risk can be controlled (lower than maximal accepted by the stakeholders).
The risk level is too high and the system should be replaced.

4.2 Financial models

To compare different technical systems with each other it is not longer enough to focus on technical aspects only. The economical aspects related to a project are increasingly important.
Financial experts have developed different financial models. Some of these financial models are better in helping the technicians and/or financial experts in the decision making process. By applying one of the financial models it is possible to compare different projects or technical solutions with each other. The intention of this report is not to give detailed descriptions of the financial models, but to support the engineer. Which model is the most suitable depends highly upon the company policy. This report describes at a high level different financial models. If the reader would like to investigate the models more deeply, background information can be easily founded.

The most used financial models are:

- Total Cost of Ownership (TCO)
- Net Present Value (NPV)
- Internal Rate of Return (IRR)
- Return on Investment (ROI)
- Payback Period (Payback)
- Life Cycle Cost (LCC)

In the next chapters different financial models are explained. As mentioned before this explanation is just a brief introduction of the model.

4.2.1 TCO

Total Cost of Ownership is a methodology whereby different projects with the same benefits can be compared with each other. This methodology can be defined as a systematic quantification of all cost related to a project during the lifetime. For an accurate comparison of different projects it is important that the calculation period is long enough. At least one replacement of a system shall be within the calculation period. It is Important to know that the benefits are not taken into account in the equation.

Equation 2: TCO

$$TCO = \frac{\sum_{t=1}^{t=n} C_0 + C_t}{n}$$

Where:

t the time of the cash flow

n the total time of the project

C_t the net cash flow (the amount of cash) at time t

C_0 : the capital investment ($t = 0$))

The table below illustrates a fictitious project utilizing TCO. In this example, the project investment is 100 k€, and maintenance is expected in years 5, 10 and 15. The technical lifetime of the system is 20 years.

Table 4: Fictive project, TCO calculation

TCO	Expected lifetime 20 year			
Cost	Year 1	Year 5	Year 10	Year 15
Type of cost	Investment C_0	Maintenance C_t	Maintenance C_t	Maintenance C_t
Expected cost	100 k€	5,00 k€	2,00 k€	5 k€
TCO	$\frac{100+5+2+5}{20}$ = 5,60 k€/y			

A major disadvantage of the TCO calculations is that the value of money over time is not taken into account. In this example, it is supposed that the value of money in year 15 is the same as today's money. In other words, inflation and interest rate are not taken into account. Another drawback of TCO calculation is that the benefits are ignored.

4.2.2 Net Present Value

Net Present Value (NPV) is a financial tool whereby it is possible to compare different projects with each other. The basis of NPV is that value of future cost/benefits is calculated back in today's money. For calculating back a defined interest rate percentage is used. This high value of the interest rate is in most cases defined by the regulator or at the corporate level. An often-used interest rate percentage in a NPC calculation is the Weighted Average Cost of Capital **(WACC)**.

With the same formula also benefits can be calculated. The NPV methodology can be combined with other financial models.

Equation 3: NPV

$$NPV = \sum_{t=1}^{n} \frac{C_t}{(1+r)^t} - C_0$$

Where:

t : the time of the cash flow

n : the total time of the project

r : the discount rate

C_t : the net cash flow (the amount of cash) at time t (positive benefits, negative cost)

C_0 : the capital investment ($t = 0$)

Remark: in this equation the cost is calculated as a negative value and benefits as a positive value.

Table 5 is for the same fiction project using the NPV calculated.

Table 5: Fiction project, NPV calculation

Year		Expected cost	Expected benefits	NPV 6% interest rate
0	Co	-€ 100.000	€ 0	
1	Ct		€ 10.000	€ 10.000
2	Ct		€ 10.000	€ 9.434
3	Ct		€ 10.000	€ 8.900
4	Ct		€ 10.000	€ 8.396
5	Ct	-€ 5.000	€ 10.000	€ 11.881
6	Ct		€ 10.000	€ 7.473
7	Ct		€ 10.000	€ 7.050
8	Ct		€ 10.000	€ 6.651
9	Ct		€ 10.000	€ 6.274
10	Ct	-€ 5.000	€ 10.000	€ 8.878
11	Ct		€ 10.000	€ 5.584
12	Ct		€ 10.000	€ 5.268
13	Ct		€ 10.000	€ 4.970
14	Ct		€ 10.000	6.635 €
15	Ct	-€ 5.000	10.000 €	€ 4.688
NPV				**€ 12.081**

Only those projects that have a positive NPV are worth investing in. Those projects that have a negative NPC should be in principle rejected.

For secondary systems is it very hard to calculate the real benefits. Sometimes utilities choose to calculate only the NPV cost. They assume that the benefits for the secondary systems are the same.

4.2.3 Internal Rate of Return

Internal Rate of Return (TRR) is a methodology to calculate the interest rate for a project whereby the NPV is zero. It is important is that the cost and benefits are known. The same NPV equations are used to calculate the IRR. The difference with the NPV is that the interest rate is a given figure and in an IRR calculation the interest rate is calculated. The advantage of this method is that it is not necessary to know the interest rate.

Equation 3: IRR

$$\text{Initial Investment} = \sum_{t=1}^{n} \frac{C_t}{(1 + IRR)^t}$$

Where:

t : the time of the cash flow

n : the total time of the project

IRR: internal rate of return

C_t : the net cash flow (the amount of cash) at time t (positive benefits, negative cost)

C_0 : the capital investment ($t = 0$)

Figure 3 is an example of IRR calculation. In this example the NPV is calculated with different interest rates. The IRR is the interest percentage whereby the NPV is zero. In this example the IRR is 17.5%.

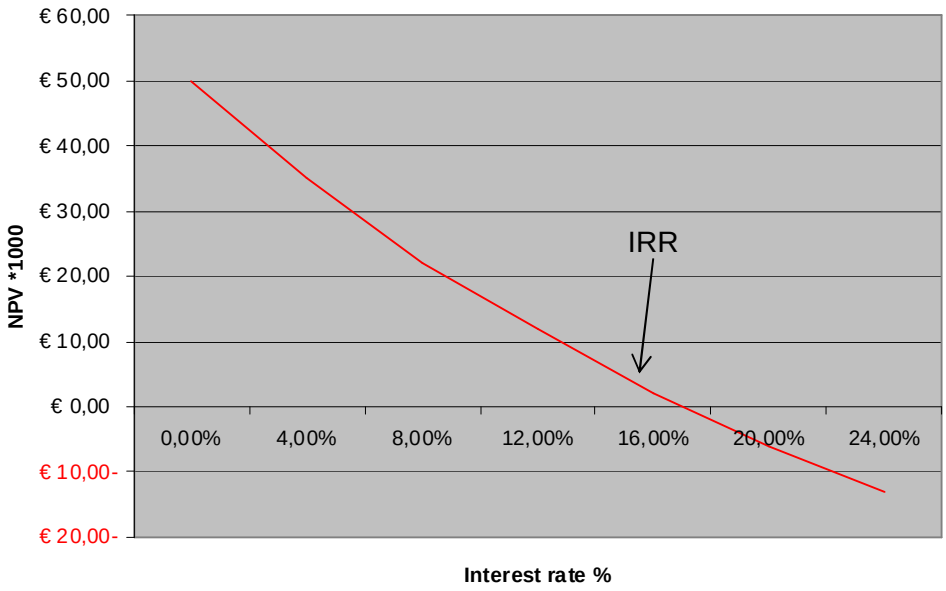


Figure 3: Example IRR calculation

Financial experts are mainly using this tool. The IRR tool is basically not intended to compare different projects with each other. The idea behind this tool is that financial expects can decide if a single project is valuable to invest in (only project with a IRR value lower than the interest rate are worth to invest in). A drawback of this tool is that also the benefits should be known.

4.2.4 Return on Investment

The Return on Investment (ROI) or Ratio of Return (RR) is the ratio between investments and the direct accountable benefits. In a ROI calculation the interest ratio is ignored. It is also possible to combine a ROI calculation with net present values. Besides the ROI calculations with NPV there are other way's to calculate the ROI. In principle the ROI

equation is very simple. The drawback of a ROI calculation is that for protection and control systems it is very difficult to calculate benefits. Normally the period for ROI calculation is over a specific period of time, usually a year. In most cases is the ROI calculation not suitable to compare different projects with each other.

Equation 4: ROI

$$ROI = \frac{V_b - V_c}{V_c} \ (\%)$$

Where:

V_b: Benefits accountable to the investment

V_c: Cost

Other tools such as TCO or NPV give better results. In the standard equation inflation and interest rate are ignored. Normally the ROI is a figure that can be found in annual reports.

4.2.5 Payback Period

Payback Period is a methodology to calculate the period of time that is needed to earn the investment back. In a standard Payback calculation inflation and interest rate are ignored. A Payback calculation can be combined with net present values.

$$Payback = \frac{V_{investment}}{V_{cashflow\ (year)}}$$

Where:

$V_{investment}$: Investment cost

$V_{cashflow}$: Cost minus benefits

For example with an investment of 100 k€ and a yearly benefit of 25 k€ it will take 4 years to have hit the a break even point. In this example the payback period is 4 years.

A Payback calculation gives insight into the time frame that is necessary to earn the investment back. Other calculations models gives in many cases a more balanced result.

4.2.6 Life cycle cost

Figures in TCO calculations are usually based on the real expected cash flow. In a NPV calculation expected cash flow is calculated back into today money. See chapters 5.2.1 and 5.2.2. Life cycle cost calculation is a combination of TCO and NPV calculation. Cash

flow in a LCC calculation is not presented in real expected money but based on a NPV calculation. The time frame for a LCC calculation should be long enough that at least all systems involved in the calculation are replaced. Typical timeframe for a LCC calculation is between 20 and 40 years.

In a LCC calculation it is possible to add risk and benefits as cost in the LCC calculation. Risk and cost shall be calculated in Euro/year. The risk and benefits can be put in the calculations as yearly cost or benefit.

4.3 Summary

	Equation	Positive	Negative
TCO	$TCO = \frac{\sum_{t=1}^{t=n} C_0 + C_t}{n}$	– All costs are calculated – Calculation period can be long – Similar projects can be compared	– Benefits are not taken into account – Interest rate and inflation are ignored
NPV	$NPV = \sum_{t=1}^{n} \frac{C_t}{(1+r)^t} - C$	– Interest rate and inflation is part of the calculation – NPV calculation can be used with other tools	– To determine the interest rate is not always simple – Not the real cash flow is not calculated – For a protection and control system it is difficult to calculate the benefits
IRR	$IRR = \sum_{t=1}^{n} \frac{C_t}{(1+IRR)^t}$	– The value of the interest rate is not needed – Interest rate and inflation is part of the calculation	– This tool is not intend to compare different projects with each other – Not the real cash flow is not calculated – For a protection and control system it is difficult to calculate the benefits
ROI	$ROI = \frac{V_b - V_c}{V_c}$	– Equation is very simple – ROI is calculated over a specific period of time, usually a year	– Interest rate and inflation are ignored – Other tools such as TCO and NPV gives a better result – For a protection and control system it is difficult to calculate the benefits
Payback	$Payback = \frac{V_{investment}}{V_{cashflow\ (year)}}$	– Equation is very simple	– Interest rate and inflation are ignored – Other tools such as TCO and NPV gives a better result – Difficult to calculate the cash flow
LCC	Combination of TOC and NPV	– Gives best and most objectives results – The risks and benefits can be taken into account	–

4.4 Examples

4.4.1 Introduction

In this example, operation risk and financial considerations are analysed in an objective way.

In this example two systems are compared with each other, namely:

system A: that is an existing system in operation for many years. There are technical constrains in this system. For example, the knowledge of how to maintain this system is not in the company and the support of the supplier is below an accepted level.

system B: a new system with new functionalities. The new functionality has many benefits, for example remote diagnosis, extensive self-supervision functionality.

System A: Existing system	
Investment cost	(CAPEX)
Operational cost	(OPEX)
Risk	(high)
Benefit	(low)

System B: New system	
Investment cost	(CAPEX)
Operational cost	(OPEX)
Risk	(low)
Benefit	(high)

Figure 4: system A and B what to do?

The driving force to start a study might be that risk of system a is too high or that it seems that system B has so many benefits that it is recommended to replace system A. Both trigger items points are described in to different examples.

Example 1: system A is in operation and there are problems with this system.
Question, is it from a risk and cost point of view justified to replace this system with a new one with the same functionality?

Example 2: is a new system available in the market, this system has many benefits.
Question, is it from cost and benefit point of view justified to replace the existing system before the end of its technical life?

4.4.2 Example 1: high risk of existing system

In example 1 is an existing system that gives a lot of problems. Advisee is to follow the following flowchart, see Figure 5.

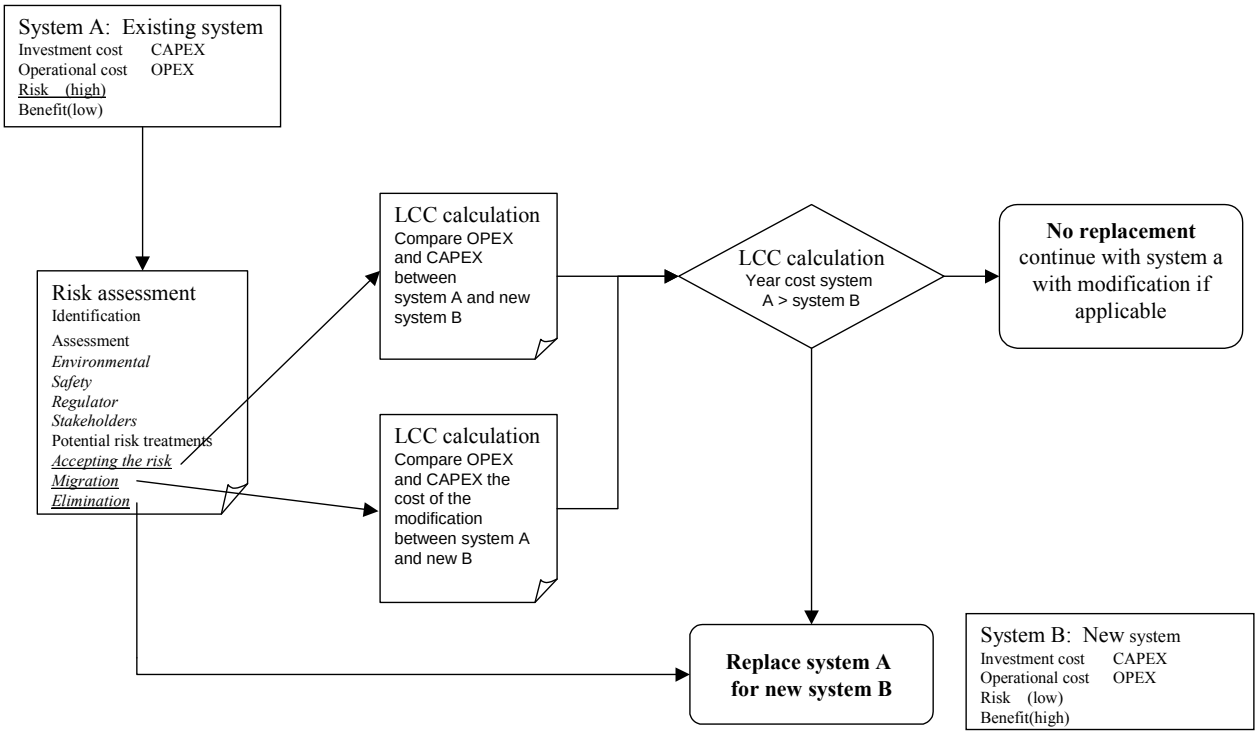


Figure 5: flowchart example 1

Starting point is an existing system A.
The first recommended step is to make a risk assessment. In this risk assessment all risk are identified and compared with the company values. Output of this risk assessment is:

- risk is acceptable, no additional steps are needed
- risk is higher than accepted, but with some additional actions the risk can be controlled (lower than maximal accepted by the stakeholders)
- the risk level is too high and the system should be replaced.

The next step in the study is a LCC calculation. If the outcome of the risk assessment is that the system should be replaced (c) it is in principle not necessary to make a LCC calculation. If the outcome of the risk assessment is that no additional steps are needed (a) or with some modification in the system (b) the risk is decreased and lower than maximal accepted a LLC calculation shall be performed.

If the outcome is that no additional steps are needed is it justified to make a LCC calculation with only the yearly operational cost (OPerational EXpenditures OPEX) and the yearly investment cost (CAPital EXpenditures CAPEX) In this calculation risk and benefits are not taken into account. Based on the outcome of the calculations it might be still possible that from cost point of view advisable to replace system A for system B

If the outcome is that with additional steps the risk is controlled a same LCC calculation shall be made. In this LCC calculation also the cost for the modification shall be included.

4.4.3 Example 2: high benefits new system

Example 2 is a new system with many benefits. It is advisable to assess the benefits of the new system and analyse those benefits from a cost point of view. The best approach in this example is to make a complete LCC calculation. The benefits can be part of the LCC calculations. For example due to improved self supervision the chance of an unwanted outage is reduced. The yearly benefits can be calculated by the value of the benefit divided by amount of years this new system is in operation in the network.

In the table below an LCC calculation made for system A and the new system B. In this example it is supposed that system A is replaced in Year 2 and that benefits of this new system also start at Year 2. Further it is supposed that the economical debit of system A stops in Year 3. See Table 6.

Table 6: example LCC calculation with benefits

Year	Scenario A Without replacing system A	Scenario B Replacing system A in year 2 for a new system
0	Opex cost /year Capex cost /year	Opex cost system A /year Capex cost system A /year
1	Opex cost /year Capex cost /year	Opex cost system A /year Capex cost system A /year
2	Opex cost /year Capex cost /year	Switching cost Opex cost system B /year Capex cost system B /year
3	Opex cost /year[1]	Opex cost system B /year Capex cost system B /year Benefits system B /year
..	Opex cost /year	Opex cost system B /year Capex cost system B /year Benefits system B /year
20	Opex cost /year	Opex cost system B /year Capex cost system B /year Benefits system B /year
	∑ NPV	∑ NPV

If the LCC shows that the overall net present cost of system B is lower than system A than it is from cost point of view is it justified to replace system A before the end of the technical life time. In the LCC is most difficult point is that the expected benefits are in most cases not easy quantifiable.

4.4.4 Overall methodology

Both scenarios can be combined. Also the risk can be translated to cost since risk is change multiplied by effect (the effect can be translated into EURO's). For a LCC calculation the risk and benefits are treated in the same way as OPEX, CAPEX. The difference between risk and benefits is that benefits can be abstracted off the year cost and risk is added cost.

[1] Remark: in this example the CAPEX of system A stops due to end economical investment debit system A

Table 7: overall LCC calculation

System		Risk	Cost	Benefits	Total
A:	Existing system	High € /year ↑	Investment cost (CAPEX) ↓ Operational cost (OPEX) ↑ € /year ↓	Low - € /year ↓	 ∑ € /year
B:	New system	Low € /year ↓	Investment cost (CAPEX) ↑ Operational cost (OPEX) ↓ € /year ↑	High - € /year ↑	 ∑ € /year

5 OPTIONS AND STRATEGIES FOR CHANGE

This chapter is dealing with migration possibilities, general methods and challenges in this process. It is ending with actual experiences from United Kingdom, Finland, Poland, France and Belgium.

5.1 General

It is widely accepted within the industry that most of the installed protection relays are rapidly approaching or have passed their operating lifetime. According to Newton-Evans' '*Worldwide Study of Protective Relay Marketplace in Electric Utilities'* approximately 60% of the relays currently being in operation are electromechanical ones with age of 30-40 years. This number varies significantly from country to country. It is recognised that there is a need for management of the obsolescence of components of such aging devices.
Several methodologies are currently employed to achieve this goal, such as: relay replacement, refurbishment and hardware life cycle management.
A number of possibilities and techniques to improve the transition from aging protection systems to up-to-date modern technology with minimal disruption to the power system are available, namely: maintenance contracts, protection upgrades, spares holdings, refurbishment of existing infrastructure and life cycle monitoring.

5.2 Migration Options

As with all Engineering solutions, it is important to consider the difficulty of the task and the resulting technical / economical advantages. If possible it is better to keep it simple to reduce the design and testing time. However, once it is determined that the current installed equipment is in need of replacement, and then various options are available. These range from `plug and play` refurbishment kits to complete scheme upgrade and replacement. These options will require, to some extent, a combination of additional competences, including full short circuit analysis, protection setting studies/examination, programmable scheme logic design, drawing layouts including AC/DC schematics, understanding of current technologies and protection scheme, commissioning, training and comprehensive project management.
This approach provides the opportunity to modify, improve and update the protection system through the use of modern technology. The following available options depend wholly on utility requirements; primarily, capital expenditure, utility history and legacy practices, system down time availability, complexity or simplicity of the scheme as well as personnel skills and human assets.

‘Plug and play’ Kits

This involves retrofitting modern protection equipment in existing housing. This has the advantage of no panel rework with minimal scheme wiring changes, resulting in economical capital cost expenditure and minimal system down time. Associated additional costs, such as design work, Computer Aided Design (CAD) and project management are minimised. However, this is applicable only for very small changes, i.e. replacement of a single relay or similar. Otherwise, the work will become more costly than expected.

Panel Door or Rack Replacement

This methodology enables creation of the pre-wired and pre-tested protection scheme remote from the final installation site. This minimises system down time, since the whole panel is replaced simplifying the installation and commissioning stage. Such designs can take the form of complete panel doors, panel sections or cut outs and various rack arrangements. However, this requires extra work at the factory for testing when the wiring goes via other parts of the cubicle that are not present at factory. And all the wiring between panel/rack must then be added at site. Only if the whole panel or cubicle is constructed, full advantage can be achieved regarding pre-tested circuits.

Extension of Existing Installations

This option enables modification to existing relay panels or the addition to existing relay panels. Such installations can include any combination of the designs detailed above, as well as complete panels to expand or modify existing protection schemes and substations.

Complete Scheme Replacement

Complete scheme replacement may result from the fact that the existing protection is no longer adequate or where modification is uneconomical. This is the most expensive solution in terms of initial capital expenditure and system down time. However, it provides the best platform for taking advantage of modern technology.

Protection System Replacement

Often when a protection system is refurbished, economical restraints prevent the associated switchgear from been updated. This is not an ideal situation since at some point the switchgear will have to be replaced, resulting in additional system outages. Remark: some companies prefer to wait until change of primary and secondary part is possible at the same time (e.g. due to limited budget). Reason is to minimize the impact on the services provided to customers.

Control System Replacement

In case of need of improvement of quality and operation measurement data and binary data for SCADA, EMS, equipment supervision, it is sometimes more economic to replace the old RTU or control system than to modify the existing equipment.

Protection Relay Component Replacement

Provided that aging components are identified, available on the market and easy to replace this method is an economic solution.

When migrating from legacy to new systems following issues need to be addressed:

Compatibility of new generation relays to old type panel layouts and operability with old generation trip coils/ lock out relays etc.

Review of electromagnetic environment and ambient condition (high level of dust and humidity)

Wiring and termination practices

DC power supply system, level of DC transients due to switchgear operation, etc. and grounding arrangements.

Since refurbishment process is implemented over a longer period of time, devices of multiple suppliers can be confusing due to non standard way of information presented to operating staff.

Extensive familiarization/ training required to protection and setting engineers for relay configuration, understanding of features etc.

Management of relays software tools and versions along with accessories

Relay setting data management and adoption of settings.

Chemical and environmental pollution

Breaking and closing capacity of solid state relays (SSR) – dI/dt, dV/dt

6 UTILITY FEEDBACK – APPROACH & PRACTICES

6.1 Summary on Questionnaire

Due to the variety of practices employed worldwide, the working group deemed it necessary to consult a wider population. Hence, a questionnaire was prepared and distributed to a number of utilities: Its goal was to capture their experiences in the area of secondary system refurbishment. The main areas under consideration were as follows:

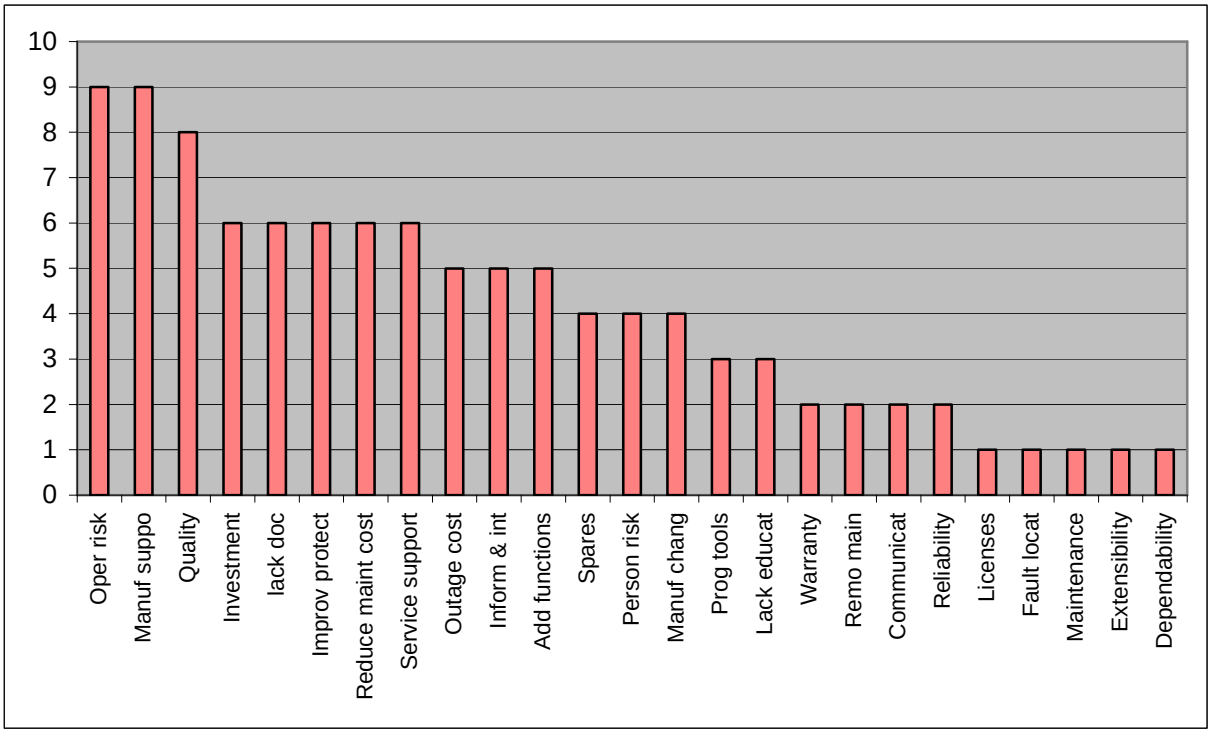
- Criteria used in the decision process
- Refurbishment strategy
- Migration Strategy
- Costing Strategy

In all 12 utilities responded. The results have been consolidated and detailed below:

6.1.1 Criteria used in the decision process

The utilities were provided with a list of criteria and asked to name the ones that influenced the decision process. They were then further asked to rate them in order of importance. Table 8 details the results: a score of 10 indicating the highest influence.

Table 8: Results: criteria used in the decision process



From the results detailed in the table it can be seen that the following issues play an important role in the decision process.

Operational Risk

Continuity of supply is an important consideration for all utilities. Ageing protection systems may present a number of operation risk issues, such as; maloperation or even no operation. It is very important to access the level of risk associated with the current installed base. When investigating operational risk you need to consider reliability, security and dependability.

Manufacturers Support

As protection relays become more technologically advanced, with increasing features, settings and functionality; utilities are becoming increasingly reliant upon the support of the manufactures. This can take the form of after sales service or training.

Quality

The quality of the protection system scores highly on the list. It is important to understand that this extends beyond the physical system itself, it is necessary to have a good quality management system, i.e. document, setting and drawing control along with a robust audit system

Investment / Reduced Maintenance Cost

The economical drivers should always be considered along with the technical aspects to ensure that an acceptable balance exists. Reduction in both maintenance costs and outage times brings considerable financial rewards and reduces operational risks (less down time).

Lack of Documentation

Lack of documentation is a major issue for aging systems. Documents are often misplaced, damaged or not kept up to date. Without such documentation it is very difficult to maintain a system and prolong its life.

Improved Protection (Protective Relay Functionality)

Advances in technology allow protection systems to be upgraded and other functions such as event, disturbance recording and self monitoring to be employed which may have been prohibitive when the original protection system was implemented.

Service Support

It is important to ensure that if a system fails service support is available. This becomes more difficult as the system ages, since experience in such systems may deplete over the years.

6.1.2 Strategies

Refurbishment Strategy

All utilities that responded agreed that the number one driver behind refurbishment strategy is the condition of the currently installed equipment; based on a condition assessment. However, there was considerable variation amongst the Utilities polled as to what level they plan to refurbish at. The following areas were mentioned: network level (many substation), substation level (limited number of substations), bay level, circuit level, relay level (individual relays within a bay).

Migration Strategy

In general the migration strategy can occur at all levels, namely, Sub, Bay, Circuit. It tends to be progressive in nature and driven by the age and condition of the installed base.

Costing Strategy

When polled on costing strategy, all except 2 utilities consider only the life cycle costs, not the initial costs. The two exceptions take into account NPV. When asked “Do you consider savings on account of combining various functionalities in a single numerical device, reducing space/wiring etc to justify higher costs”, the overall response was yes, however, it is voltage dependent.

6.2 Practical Experiences in Some Countries

6.2.1 United Kingdom approach

Case 1 – Rail Industry

It was noted that a considerable amount of distance protection relays were fast approaching replacement for the following reasons:

- Relays were obsolete and no longer supported by the manufacturer
- The Rail Industry had a limited amount of spares
- Current protection scheme unable to deal with current demands i.e. temperature monitoring and regenerative breaking.
- Remote control and monitoring was required

Due to the strategic nature of the rail system and the requirement to reduce outage times to a minimum, a simple and fast solution was required. The current protection schemes

were on hinged doors. To reduce the amount of time on site, a complete new pre-wired door, with flying leads for external connections was built in the factory and tested before delivery to site. It was then possible to simply remove the existing door and wiring to the terminal blocks in the back of the panel and replace with the new panel and test within one day. To speed up any interpanel wiring, cabling between panels was run in but not landed while the system was live, awaiting connection during the outage. This pre enabling works dramatically reduces the system down time.

Case 2 – Distribution Network Operator (DNO)

In order to move with technology a number of DNO`s are embracing numerical relays and taking advantage of the features now available within such devices. This is often a staged process to gain confidence with the following most popular combinations in use:

- Main Protection only, rest of the scheme maintained
- Combine auto-reclose protection into numerical main protection and discard auto-reclose panel.
- Replace all, but have two identical numerical relays, main and back-up
- Complete replacement

Where a considerable amount of relays are to be replaced, then a new front sheet is the preferred solution, since it reduces the outage time. Such schemes can be tested in the factory to ensure the scheme is functioning correctly before delivery to site. Once on site, it is then necessary to test the interface to the system.

To date, the majority of the refurbishment projects have been protection panels only and no switchgear. This is often due to economical constraints. However, in the future this will probably change and complete systems will be replaced i.e. protection plus switchgear.

6.2.2 Finland approach

It seems that some electronic (static) relays and first generation microprocessor relays will need extra maintenance or maintenance in advance. The ageing of some electronic components of these relays is faster than expected. For example, some capacitors, potentiometers and trip relays are not so old. Our company has had 5-6 false trips during the last two years (in medium voltage level) from electronic and first generation numerical relays. It seems that the coverage of the self detection is not very good in these (late 1980's early 1990's) first numerical relays. We have also considered that in the case of an internal error, false trip of the relay is the last possible action. This seems not to be true necessarily. Hopefully, the internal fault detection function of the latest generation numerical relays is as good as manufacturers advertise [claim].

Solution: The manufacturer of the relays has proposed that our company (and the others also in Finland) should start to do preventive maintenance actions: Risky parts of the relays should be changed with the help of repair kits provided by manufacturer (risky

electronic card types, bad capacitors, set potentiometers, trip relays, etc.). It is more economical to do this at the same time of periodical relay testing in the substation. The cost of this job should be about 10 % of the cost of changing the relay to new one. With this they promise 10 years "good" lifetime after the event. This action is reasonable to do for relays which are about 10 to 20+ years old. This preventive maintenance seems to be a reasonable solution at least in Finland, because we have a large amount of electronic and first digital relays assembled in 1970's and 1980's and these devices are made by the same manufacturer. The total change to new relays is impossible in these scales. Other manufacturers and countries also have met this problem.

6.2.3 Poland approach

In 2003 PSE-Operator SA (TSO in Poland) established a new project called 'Remote Control and Supervision of the Transmission Grid'. This is aimed at introducing fully remote operation of the transmission grid in Poland by implementation of the state-of-the-art substation automation systems throughout the network and implementation of a new organization scheme in the areas of power system operation and transmission assets management. This process should lead to unmanned operation of the substations performed by remote control and remote supervision from the centres.
There has been agreed that the primary driving force for this project is common and direct access to the information required by each individual organization unit inside PSE-Operator.
The scope of individual projects (substations' refurbishment) varies and depends on the actual condition of the secondary as well as primary equipment. Beneath are described the most representative examples.

Case 1 – substation replacement

Installation of the state-of-the-art Substation Automation System was included in the scope of comprehensive modernization of a substation. It assures full implementation of current standard functional specifications for substation and overhead HV/EHV lines. Those standard specifications have been prepared by the PSE-Operator's technical staff, published on the web site, and are mandatory for all equipment and services providers. Such a global refurbishment makes it probable to 'forget' the problems with functioning of certain pieces of equipment and substation as a whole, providing decrease of maintenance costs and appropriate environment for the operation of the grid in a new organization scheme.
Usually it concerns running substations with energized circuits. The upgrading process has to provide for an uninterruptible supply to the vital loads. It is provided by applying step by step installation and rolling shut downs of the consecutive bays. It requires from both provider and customer preparation of 'schedule of work' by using an appropriate

method and form, e.g. CPM and Gantt chart, which has to be agreed on by Asset Management Department and Grid Operation Department, especially regarding shut downs of HV lines and power transformers.

As an example, modernization of Mory 220/110 kV substation located in Warsaw suburb area, which is the essential supply node for Warsaw agglomeration. The substation was first energized in the mid 1950's. The primary as well as secondary equipment and substation infrastructure have reached the end of their lifetime and therefore the substation needed a deep refurbishment. One could say that the old substation has been completely destroyed and at the same place a new substation has been built.

The task the contractor was faced with was a real challenge – to perform a substation replacement with minimal shutdowns. To fulfil the above requirements the whole project has been divided into six phases. It started in August 1999 and finished in September 2004.

Modernization has been carried out by keeping the substation's scheme with slight changes to its default operating schedule and there was no need to introduce changes in grid topology, especially highly inconvenient T-connections in the front of the substation.

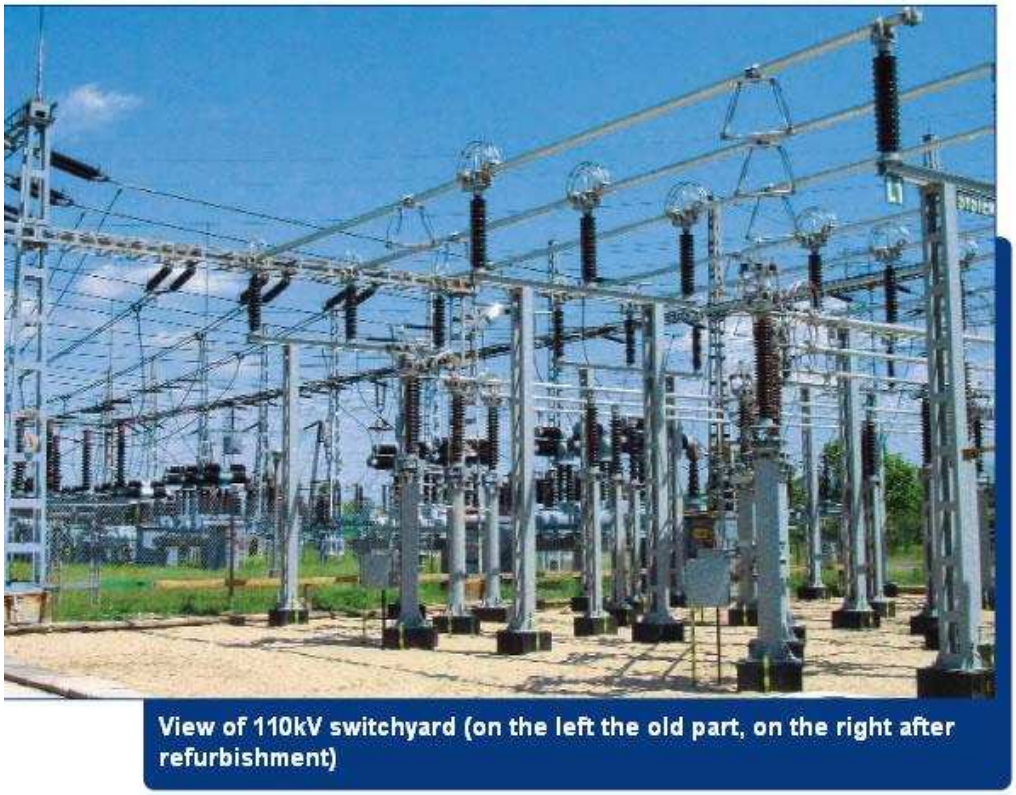


Figure 6. View of 110 kV switchyard

The substation now consists of two switchyards – 220 kV with 15 bays and 110 kV with 25 bays, each switchyard equipped with triple busbar system, three power transformers 220/110 kV, 160 MVA each, auxiliary supply switchgears AC and DC (see Fig.6).

The upgrade process has resulted in installation of new primary and secondary equipment, like:

220 kV and 110 kV circuit breakers,

- Instrument transformers (voltage, current and combined transformers),
- disconnectors,
- digital protection terminals supporting IEC 60870-5-103 protocol (see Fig.7),
- substation control system supporting all nowadays required functions, including bidirectional communication with control centres, protection terminals and other IED’s in the substation (see Fig.7),
- SDH communication transmission equipment supporting voice and data channels, and transmission of teleprotection commands

–

Figure 7. Protection and Control cubicles layout

Case 2 – substation retrofit

Due to limited funds we installed only specific components of SAS. The scope of the SAS implementation depends on the technical condition of substation components, both primary and secondary circuits. Usually it includes installation of substation control system and replacement of the most exploited and vital components of the protection scheme, e.g. busbar protection breaker failure protection. Sometimes it also involves minor changes in (or retrofit of) primary devices, e.g. disconnector drives. In such a case the focus is on integration of the new components with the remaining secondary and primary devices.

An example of such an approach is the 220/110 kV shared substation. 'Shared' means that the 220 kV switchyard including two power transformers 220/110 kV and their 110 kV

bays are owned by PPGC, while the rest of the substation including 110 kV switchyard, auxiliary supply switchgears (0.4 kV AC and 220 V DC) and substation buildings are owned by distribution company.

On the distribution side there are still static protection relays, there have been done some refurbishment of marshalling panels and control panels (providing local control and measurements). A new digital control system in a centralized architecture supporting DNP 3.0 transmission protocol for external communication has been installed

On the transmission side, electromechanical distance protection relays (used as main protection) have not been touched. The replacement covered electromechanical earth fault relays (used as backup protection) and old TTL-technology based RTU. Digital earth fault relays supporting IEC 60870-5-103 communication protocol and digital substation control and supervision (SCS) system in distributed architecture supporting DNP 3.0 protocol, used for communication with SCADA systems in control centres and IEC 60870-5-103 protocol for communication with protection IED's have been installed. The communication features of the SCS included also implementation of TCP/IP stack, IEC 60870-5-104 protocol and Web Server application to allow communication via enterprise WAN.

On figures 8 – 10 are presented some typical screens of new SCS and current SAS communication scheme. This retrofit process allowed for improved substation observability, quality of measurements and topology information transmitted to SCADA systems. Thanks to the implementation of remote control it was possible to resign from the local manned operation of the substation – service provided by a distribution company.

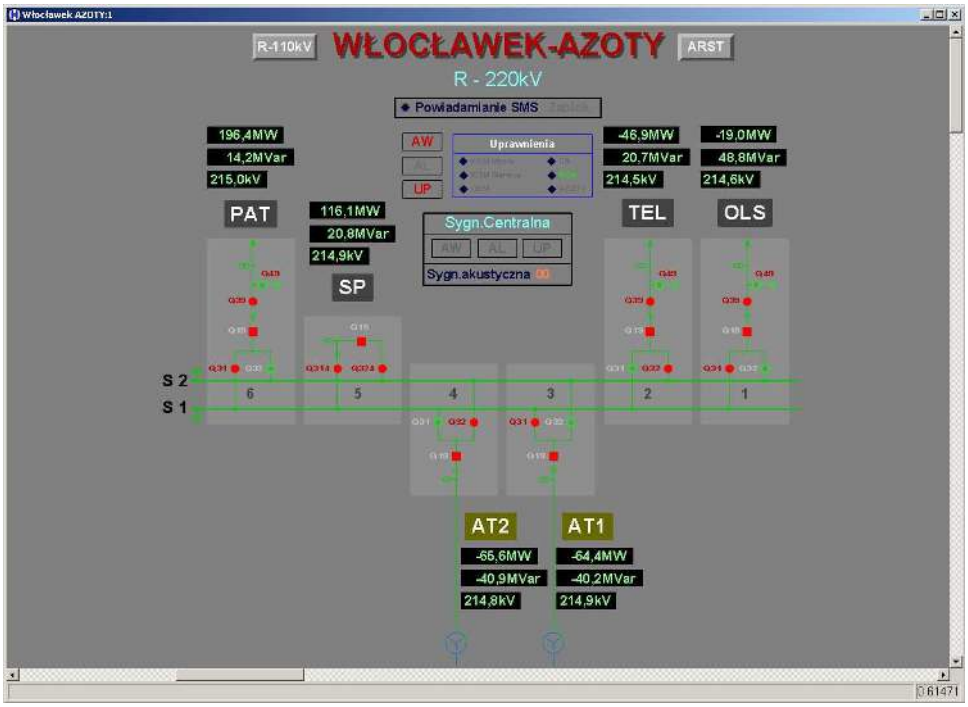


Figure 8: Substation layout on the local HMI

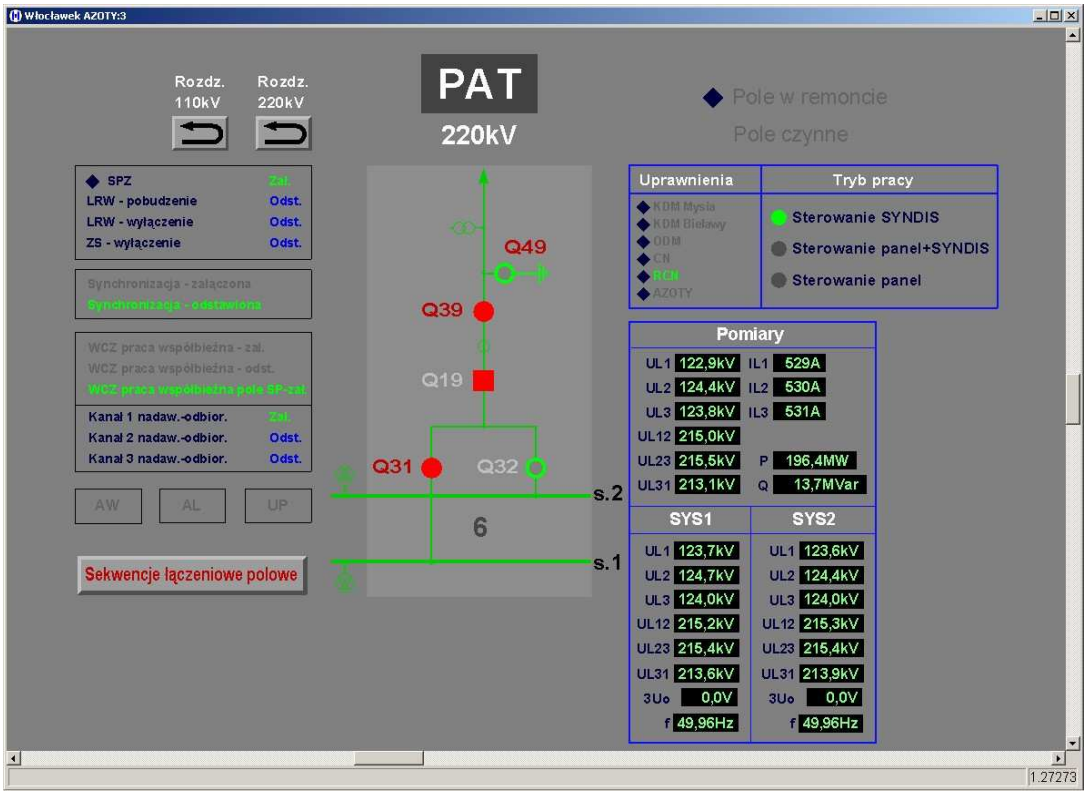


Figure 9: Detailed layout of the feeder incl. protection status, bay measurements, etc.

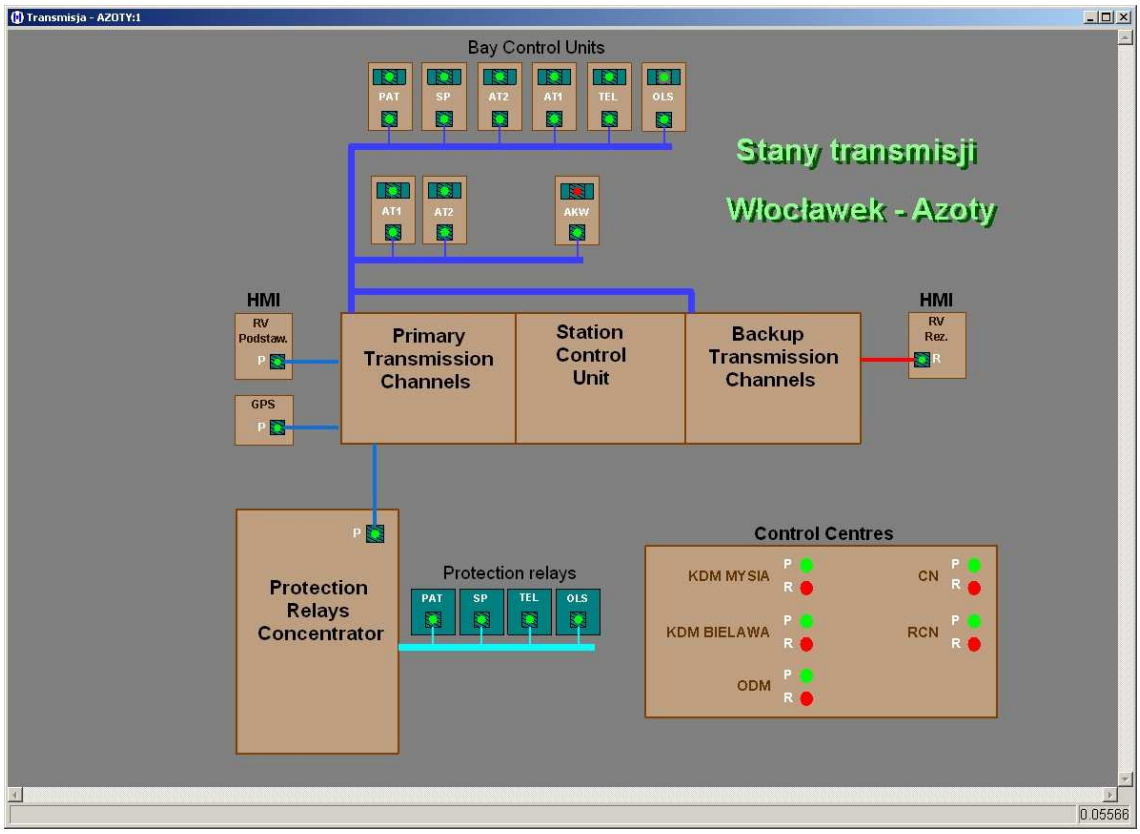


Figure 10: Supervision on data transmission in the Substation Automation System

Certain projects differ depending on the approach to bidding and ordering process. From the view of „openness" there can be public bids – open to all vendors, and limited bids – directed to pre-selected vendors. From the view of completion of projects there are contracts which scope covers certain part or parts of the substation and turn-key contracts covering all works in the substation.

6.2.4 France approach

Is it really necessary and urgent to *refurbish / retrofit / replace*?
This question arises when the protection relays cause incidents, either by failure on request, or by spurious operation on external fault or even without High Voltage cause.
The answer is easy for the old electromechanical equipment, whose measurement relays are not manufactured any more. It is less simple for the analogue electronic equipment for which it is still rather easy to find components for the repairing: indeed, we can wonder whether the equipment is at the end of its lifetime or if its reliability remains sufficient in spite of the incident.
Described below is the method we use which allows us to say which equipment could still

remain in operation for 10 to 20 years plus, on the condition of carrying out some maintenance actions at regular intervals.

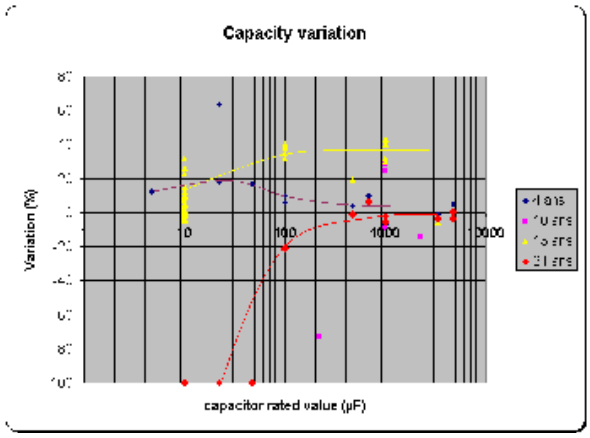


Figure 11: Capacity variation

To achieve this goal, a protection of each type was taken out of the network for thorough analysis.

We started by measuring directly on the charts the characteristics of the components for which ageing phenomena are known.

The aluminium electrolytic capacitors are easily measured without disassembling the chart (measurement at 1 kHz, with a bias voltage of 2V), because their capacities are high and they have a low impedance versus the other components of the chart (of course it must be checked on the chart scheme that there is no other capacitor in parallel). Thus we confirmed the ageing of these components (the smaller they are, the more they age quickly): this led to the recommendation of replacement every 12 years for the values lower or equal to 100µF and every 18 years for the others. We also observed that some capacitor manufacturers had products ageing much more quickly than the average: we recommended their replacement as soon as possible by products of reliable manufacturers.

The photo couplers may age by reduction of the light efficiency of the emitting diode. Measurement on chart of the CTR (Current Transfer Ratio) is possible by making some corrections to the currents of measured input and output: the output is polarized under a constant voltage of 5V and the current is measured under a null input current: this current is the consumption of the other components of the chart which is constant under a constant voltage: it is subtracted from the other measurements. The correction of the input current is done by analyzing the diagram in order to calculate the current leaking in the other components under the input voltage (the photo couplers being used to isolate the inputs, the studied diagram is finally very restricted). No sign of ageing was found, even for those permanently active. The photo coupler manufacturers seem to have controlled this problem. Recommendation: a new sampling will be carried out in 10 years.

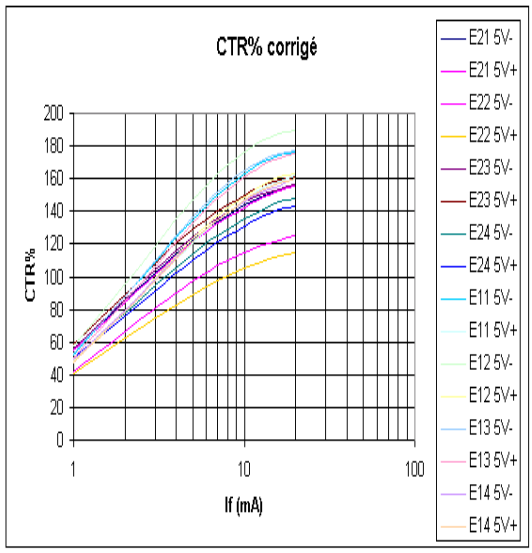


Figure 12: CTR% correction

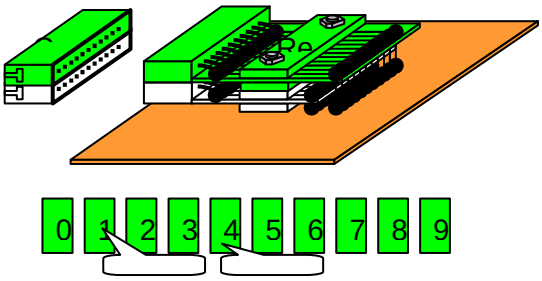


Figure 13: Coding wheels

The coding wheels present a risk of opening of their internal contacts: this defect is difficult to characterize because it is often fugitive (it is sufficient to move the wheel so that it disappears and then reappears later). Using the schemes we analysed the effect of such openings on the behaviour of the protection: measure distorted of x%, spurious trip order on external fault, pickup thresholds modified. We recommended the replacement of the coding wheels when spurious tripping was proved (note: as protections are doubled, the failure is definitely less critical). It was then necessary to propose a replacement system which really eliminates this risk: we replaced the fixed part by a connector base plate and the moving part by a connector block in which a welded wiring reproduce the code (thus there is as many blocks as figures).

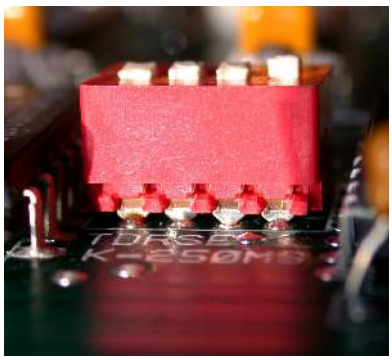


Figure 14: Dip-switches

The dip-switches, which usually do not cause big problems, revealed a series badly manufactured: the plastic block opens and the contacts also: A recommendation of immediate replacement was made, with this difficulty that these components are not dated and not marked; the help of the equipment manufacturer is necessary to know the charts manufactured at the same time as those where we found the problem.

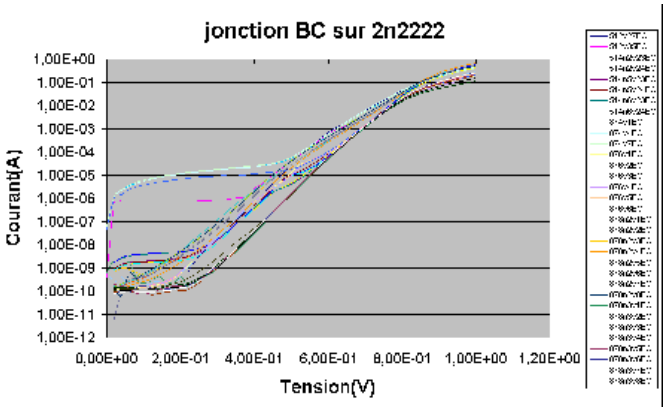


Figure 15: Junctions

Then we continued with measurements on components of which no ageing mode is known (in any case under the rather soft conditions of our equipment): The transistors were the subject of a statement of I(V) curves for their 2 junctions: the exponential characteristic of the junctions allowed to neglect the low values and to measure the variation with ideal exponential for voltages between 0.6V and 1V. This variation allows to calculate the series resistance of the junction: each family of transistors presents a rather constant value, with a value a little higher for the Base-Emitter connection than for the Base-Collector connection. Some specimens far from the mean value were taken for analysis: most probably the cause is a manufacturing defect: bondings badly positioned, silicon

support striped. The diodes were also measured with the same process. We highlighted that certain batches were residues of sorted batches: characteristics beyond 3 standard deviations. A study of the schemes and a simulation showed that the correct operation of the chart remained largely assured in spite of these defects.

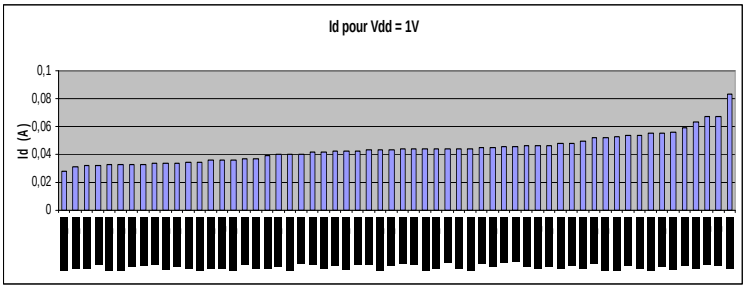


Figure 16: measure

Then we tested the logical components, which present the characteristic to have a measurable junction (without protective series resistance) between the outputs and the power supply pins: Gaussian dispersion, except for a batch, probably also a residue of sorted batch: then it was checked using the chart scheme that the reduced fan-out remained compatible with the load. Finally we tested the operational amplifiers, which present the characteristic to have between the 2 inputs or an input and the GND a measurable junction (without protective series resistance). Substantial but non Gaussian dispersion, due to the fact that several inputs in parallel are often measured: by dividing the current by the number of inputs in parallel, dispersion is then very weak and Gaussian.

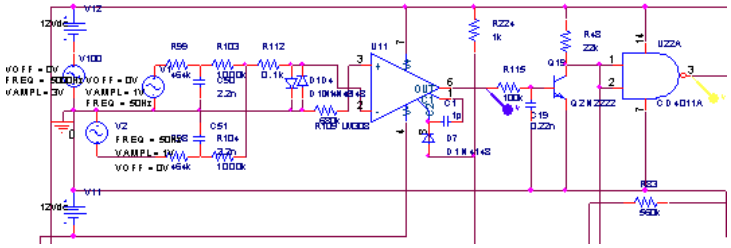


Figure 17: scheme

The recommendation of maintenance was to do nothing. For the repair of broken down charts, an LM308H operational amplifier of the Eighties had a particular characteristic: its output could be clamped by referring the compensating network by a diode to the wished limit voltage: certain diagrams use this property which is not available any more on the recent components: we recommended to make a stock of these components.

In conclusion, with respect to the periodic replacement of the aluminium electrolytic capacitors and a levelling of certain equipment (coding wheels, dip-switches), it is sure that our equipment will last still a long time.

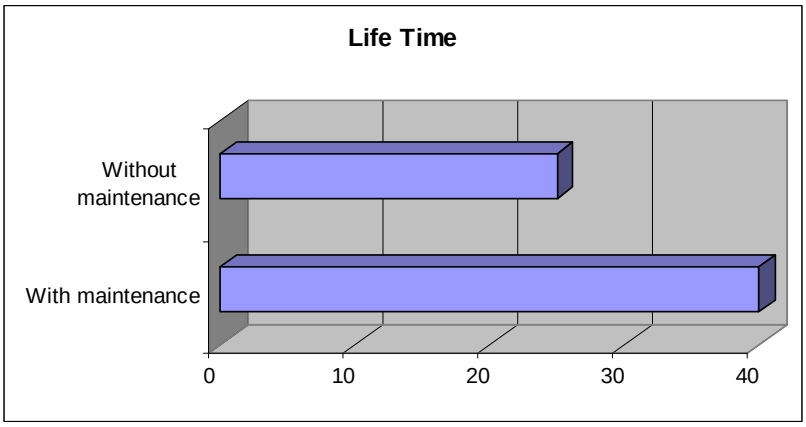


Figure 18: life time

An economic survey which develops the fact of delaying of 10 to 15 years the renewal reveals a very important profitability of this type of maintenance.
The above described approach shows great benefits for the company, although not all companies can follow it. It requires a lot of expertise, appropriately equipped laboratories, etc.

6.2.5 Belgian experience

Elia network includes voltage levels in the range 400kV to 30kV (400kV, 220kV, 150kV, 70kV, 36kV and 30kV). All together, the network is composed of 5000 bays all of which are equipped with Protection and Control systems (cubicle or rack).

Taking into account a life expectancy of 25 years on newly installed protection system, one can roughly estimate that 200 protection systems (cubicles) have to be replaced on a year basis in order to maintain the protection and control systems at a good quality level. This corresponds to a replacement pace of 4 systems per week.

This is a challenging task which has to be tackled with an efficient refurbishment strategy.

Elia protection and control systems are composed of Electromechanical, Static and numerical equipments that have been installed through the years. The next picture gives an idea on the technology repartition per voltage level.

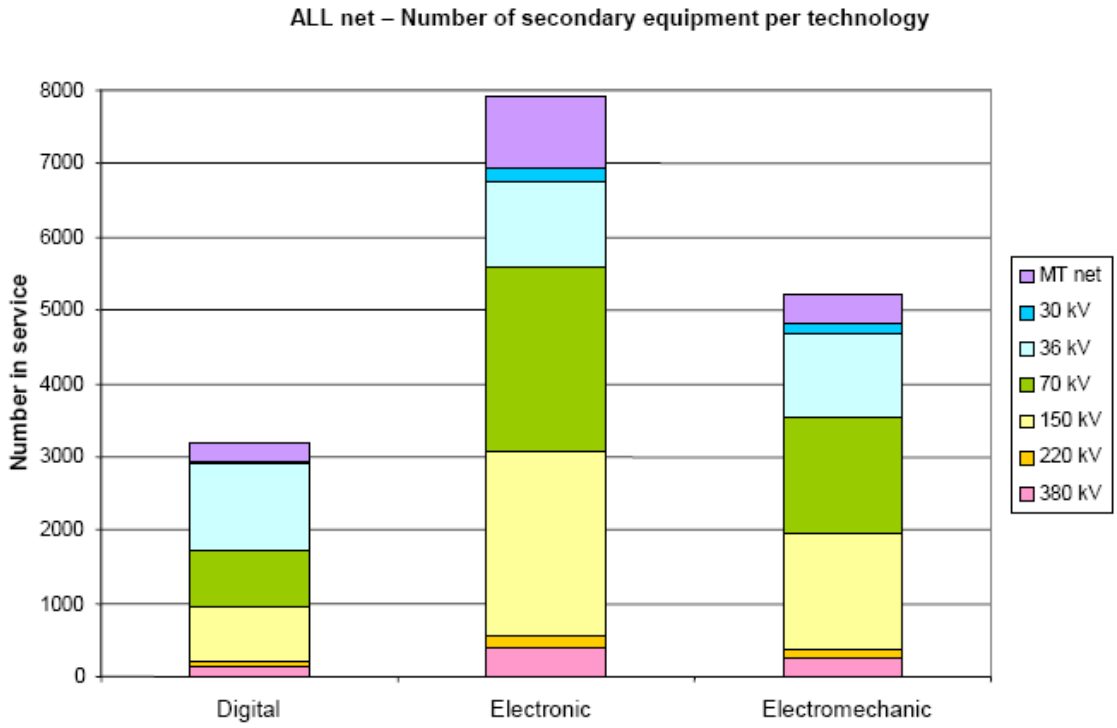


Figure 19: technology

Protection and control devices have been classified in 8 categories, based on their technology and on their Service Level Index (see hereunder).

- Electromechanical : EM1, EM2, EM3
- Electronic(static) : ELO1,ELO2,ELO3
- Numerical : DIG1, DIG2

Service Level Index:

1: good quality and still available on the market

2: good quality, not available on the market anymore but spare parts are still available (stock)

3: bad quality or no spare parts available anymore

A more detailed repartition based on the 8 categories is given in the next picture:

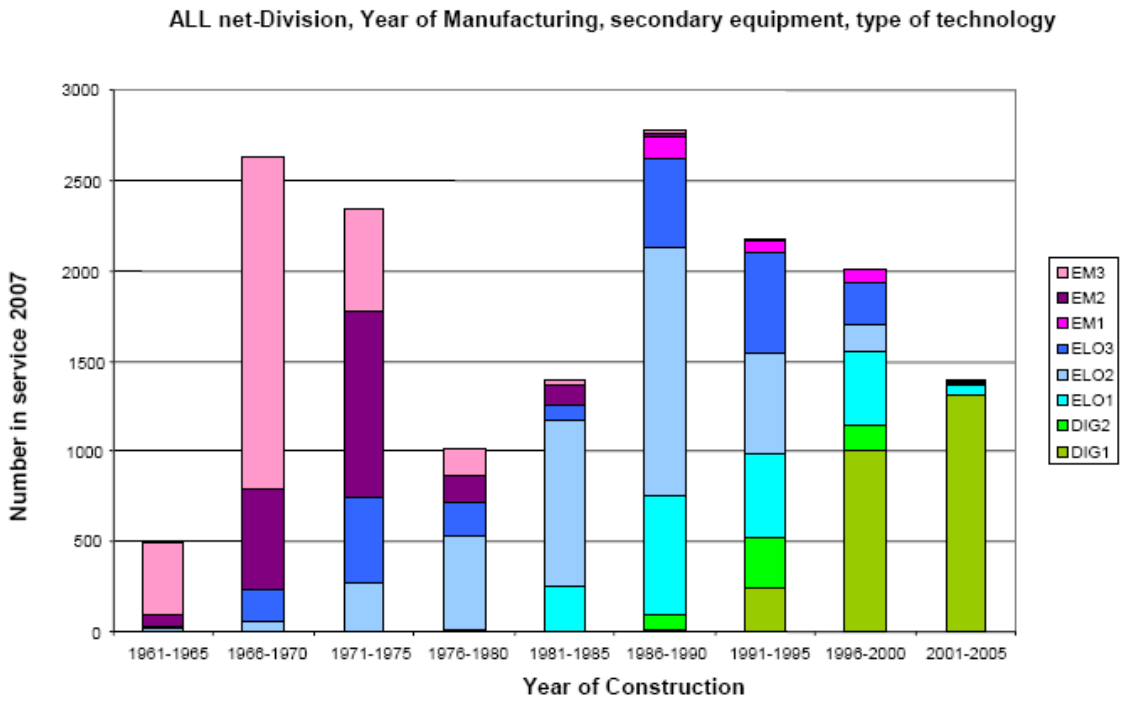


Figure 20: Service level index

EM2 & 3 equipments are expected to have a lifetime of 30-45 years. Those equipments have been mainly installed in the years 1966-75 and are now reaching the end of their lifetime.
In the same way, ELO equipments are expected to have a lifetime of 20-35 years. Those equipments have known their peak of placement in the years 1975-86 and are also reaching the end of their lifetime.

This situation combined with the fact that life expectancy of digital equipment is not known but is expected to be in the range of 20-25 years, has led to a double refurbishment strategy:

1)Investment projects

Maximum replacement of protection and control systems happens through investment projects. Each project (network reinforcement, network development) is used as an opportunity to replace the protection & control equipments which are outdated or which could jeopardize the quality of the system.
As the goal is to replace a maximum of P&C systems, all aspects of the project have been optimized in order to reduce time & costs. This includes Engineering, FAT, SAT, uptime, maintenance aspects.

Practically, this refurbishment strategy makes use of Highly Standardized and modular Protection & Control cubicles at bay level.

These cubicles are characterized by:

- No auxiliary relays and maximum self supervision (maintenance reduction) ;
- Minimum number of IED's to cover all cubicles needs (reduction of spare part costs) ;
- Minimum wiring (reduction of wiring time) ;
- Strict application of international Standards (reduction of approval procedures) ;
- Universal interface to substation level : classical wiring and IEC 61850 connection ;
- Standardized and validated IED's programming (parameters, scheme logics)
- Standardized layouts, wirings schemes and documentation.

For efficiency reasons, the engineering of each new cubicle is based on a library of +- 50 pre-engineered and standardized cubicles covering 400kV to 30 kV applications and requiring a minimum of customization.

2) One-to-One replacements

In the long term, the replacement peak caused by EM and ELO equipments combined with the reduction of the lifetime of P&C equipments and the pressure on investment budgets could be so binding that this strategy alone could prove to be insufficient.

Replacement through investment projects is therefore completed by a "one-to-one" replacement strategy. This strategy is aiming at replacing old equipments (EM3, ELO3) in order to level out the replacement peak through the years.

The one-to-one replacement strategy is based on a so-called "risk model". This models makes use of different information (such as equipment age, substation importance, …) and provides the maintenance engineer with a list a equipment which have to be replaced with a priority ranking.

The following picture shows the impact of different one-to-one replacement strategies on the global quality index of the network.

Without One-to-One replacements:

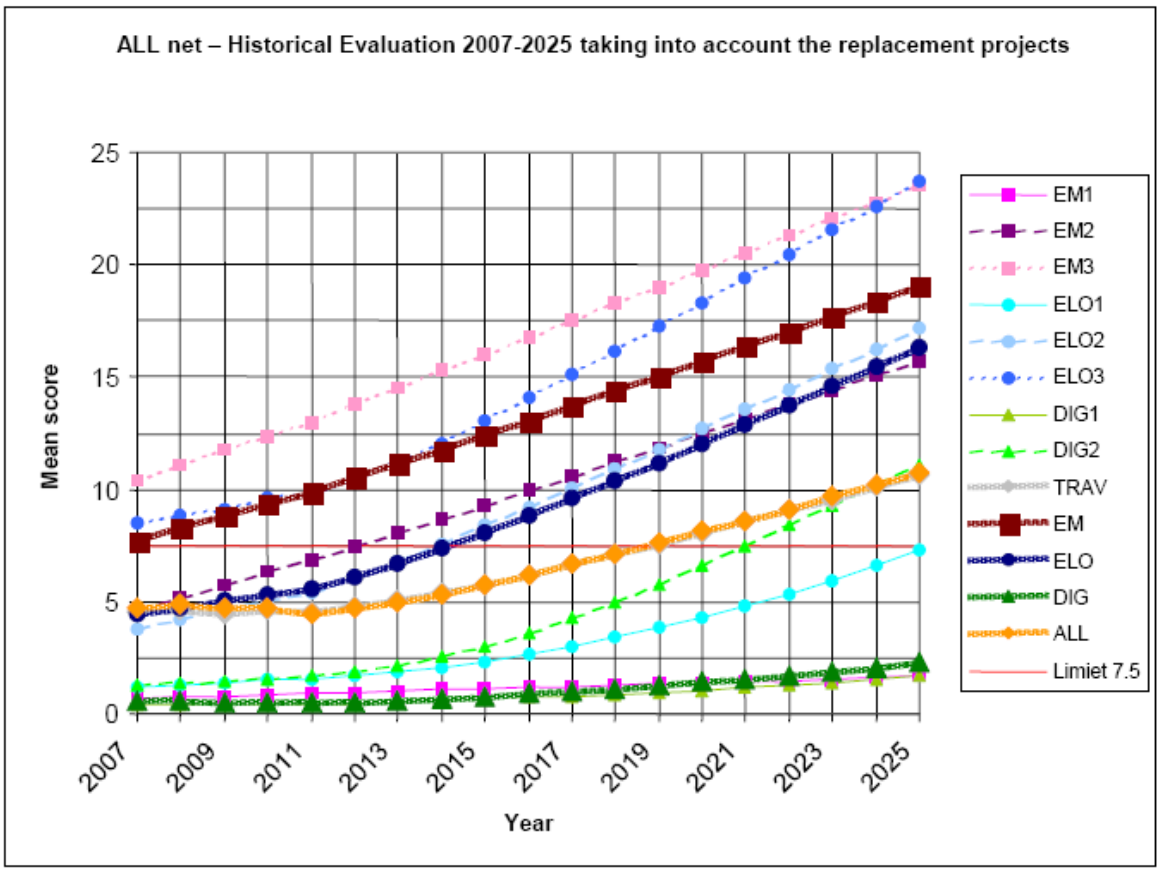


Figure 21: historical evaluation

With one-to-one replacements

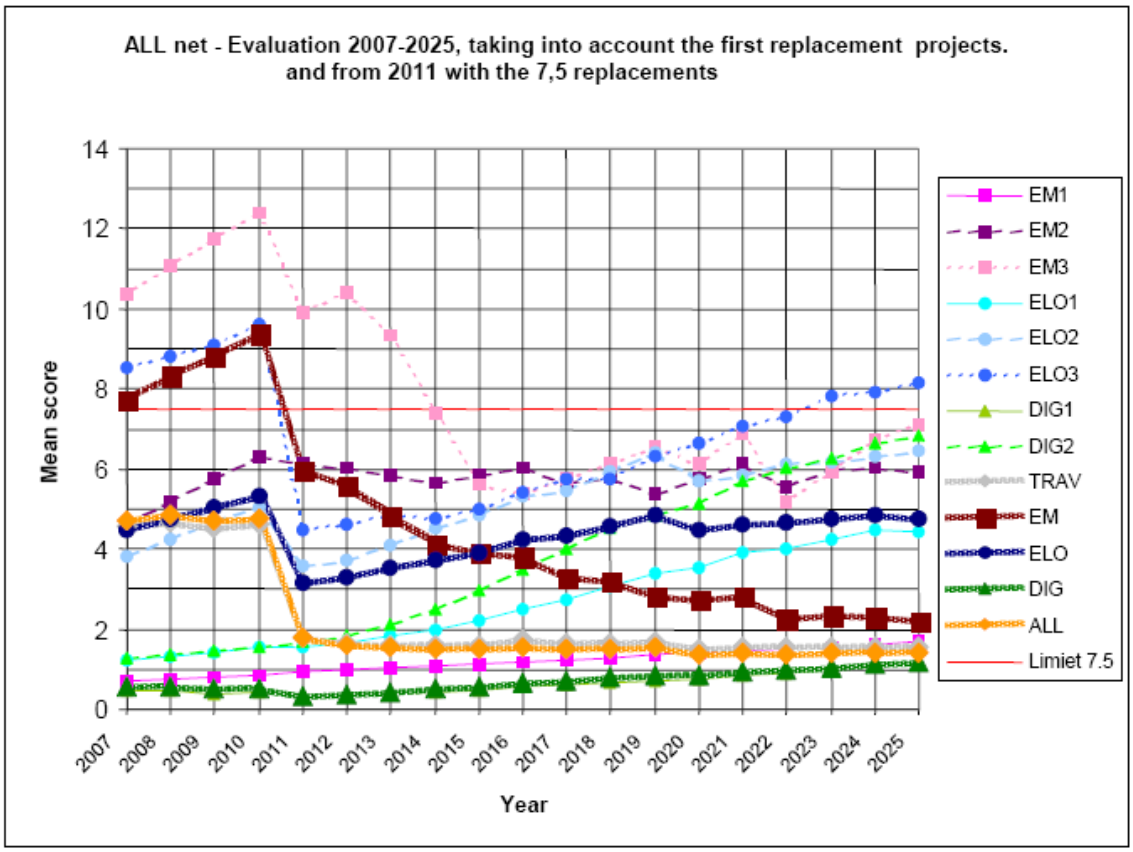


Figure 22: historical evaluation with replacement after 2011

TCO shows that we don't need to buy the cheapest solution, because initial cost is smaller comparing to total cost. It is worth of using more expensive components in order to reduce operational and maintenance costs.

6.3 Conclusions

It is clear to see from the questionnaire that the main driver for change is continuity of supply. This is becoming increasingly important as the supply for electricity increases, since loss of parts of the network may have disastrous consequences. This condition is often exacerbated by ageing equipment on the system. It is also clear that even though new technology and additional functionality in the equipment is not a main driver for change; utilities consider manufacturers support, quality, reliability and advances in technology as being important aspects in providing a secure and reliable electrical power system. However, it is important to understand that such advances in technology may allow the realisation of secondary system designs that were not possible before, hence improving the network reliability and security.

An interesting observation is that it is not possible to clearly define the best strategy for refurbishment, this if often based on a number of factors such as: voltage level, geography, customer preference etc. However, it is clear that some form of refurbishment strategy as oppose to complete replacement has an important role to play when balancing outage times / operational risks against cost.

7 TRENDS

This chapter describes new functions or changes in existing functions that can help end-users in the targets which users are confronted with as a result of system and market trends. This can be input for protection developers to implement this function in the near future as well as for end users to help in the specification process.
This chapter is divided into the following three items

- System trends.
- Self-check contribution to reduce maintenance.
- Remote maintenance.

One of the driving forces for replacement of new protection systems can be the introduction of new technology and/or functionality. This paragraph describes future trends in protection systems. This paragraph can be helpful for end–users and R&D departments to focus their development policy. It is our intention to describe trends, and not be complete.
Technical developments should be mainly driven on changing needs of end users.

7.1 System trends

The following trends in the industry and utilities are recognized:

- increasing network load, networks are operating closer to the technical limits
- unpredicted, changing load flows in the network
- reducing investment and operational cost (total cost of ownership)
- improving reliability
- reducing technical skills within the company (outsourcing of non core activity)
- more information from the status of the network to management, load forecast,… systems etc
- scale and amount of blackouts is increasing
- flexible networks

7.1.1 Increasing network load

The trend is that electrical infrastructure is operating closer to the technical limits. Worldwide there are two trends. There are networks where the load increases in such a way that it is almost impossible to follow the increasing energy consumption, and there are networks where the growth is not so high but where due to the liberalization investments in the network are postponed.
A second trend is that due to the increasing load end-users decided to up-rate their

installed primary components (power transformers, cables, overhead lines). In an up-rating process not the maximum technical value on the rating plate is used. The construction of a component is analyzed in detail. It has been found out that in many cases the maximum technical value of a component is much higher than the maximum value on the rating plate (although this could have an impact in equipment life).
Higher loads in the network and up rating component have an impact on the protection system / settings. In networks that are operating much closer to the technical limits the performance of reliable protection system is essential.

7.1.2 Unpredicted, changing load flows in the network

The amount of decentralized energy produced is increasing. Installing large-scale windmill parks helps countries to fulfil the agreed Kyoto Protocol targets for the reduction of the emission of greenhouse gases. Due to more dispersed energy, network configurations, load flows and short-circuit power are more unpredictable. The conventional applications of transmission protection schemes and methods of calculating protection settings become more and more unsuitable.

7.1.3 Reducing investment and operational cost (total cost of ownership)

The users of protection systems are confronted with a pressure to reduce investment and operational cost. Trend is that manufacturers of protection devices develop one uniform hardware platform, which is suitable for all protection relays. The next step in this development is that protection functions are delivered as a software module. This “protection software module” can be installed in any equipment. The relation between physical hardware and protection functions as a software module will become more vague. This product standardization allows reducing investment in spare equipments and/or modules. Modular designs allow reduction in operation costs as in many cases end users may perform simple repairs at module level replacement on site minimizing downtime.

Another trend in reducing maintenance cost is the enhanced self-check functionality. The trend is that self-check functions are also monitoring major parts of the secondary equipment. Trip-coils supervision and voltage supervision are typical examples. With new functionality the complete primary equipment can be monitored. When these functions are available inspection can be reduced to an absolute minimum.

7.1.4 Improving reliability

There is an increasing focus on power quality. For a modern society the reliability of the electrical infrastructure is an essential part of economical growth. Regulators are introducing quality indexes in their financial structure. The reliability of protection systems is an essential part of the overall network performance.

7.1.5 Reducing technical skills within the company (outsourcing of non core activity)

From published papers it is known that almost 50% of the unwanted protection operations are related to human errors. With adaptive protection settings (fuzzy and neural network technology) using the information from network calculations programs and SCADA systems settings can be automatically calculated. The human expertise of calculating protection settings can be translated into setting algorithms

7.1.6 More information from the status of the network to management, load forecast, systems, etc.

Due to the information society the need for additional network information is increasing. Due to this additional information needs, detailed information regarding the behaviour of the network is increasing. Typical examples of addition information are for example the trend recorders which are incorporated in all of digital protection relays. Due to this additional information it is easier for a protection engineer to explain the cause of a failure. The next step is that additional information from protection and substation systems is also used for management of information, maintenance purposes, load forecasting, etc.

7.1.7 Scale and amount of blackouts is increasing.

Networks are enlarged due to globalization. The coherency between power producing and power consuming are becoming weaker. Interconnecting connections are more than in the past needed for the network flows and stability. The recent major blackouts in Canada and Italy show that tripping off a single transmission line can result finally in a blackout of a complete region. Fact is that the scale, size and frequency of blackouts is increasing.

7.1.8 Flexible networks

The last example of trend is flexible networks. The situation today is that almost every network is designed and operated in one way. With more flexible networks it is possible to

configure a network in such a way that in every situation the most economical configuration is selected. In theory with flexible networks the most cost benefit solution is selected. Smart grids using modern technologies may contribute to security in a cost effective way.

7.2 Self check contribution to reduced maintenance

7.2.1 Self supervision definition

We could define the self supervision, sometimes referred to as self-check or self-test, as the capability of one device to monitor its own health, reporting this failure to upper levels, and pre-programmed or spontaneous response in terms of its outputs (i.e. disable protection outputs).

We will see in the scope of self-supervision some cases where the equipment monitors something more than its own health. These should not be called self-supervision, but it is important as a global system point of view as it gives value to the user.

7.2.2 Scope of Self supervision

Modern protections include modular design approach, to minimize down time and increase availability (through quick problem detection and fast module replacement). This leads to the need of special tests to warranty the right modules were installed in the right slot when repairs are done in the field. This is why diagnostics are more oriented to these modules.

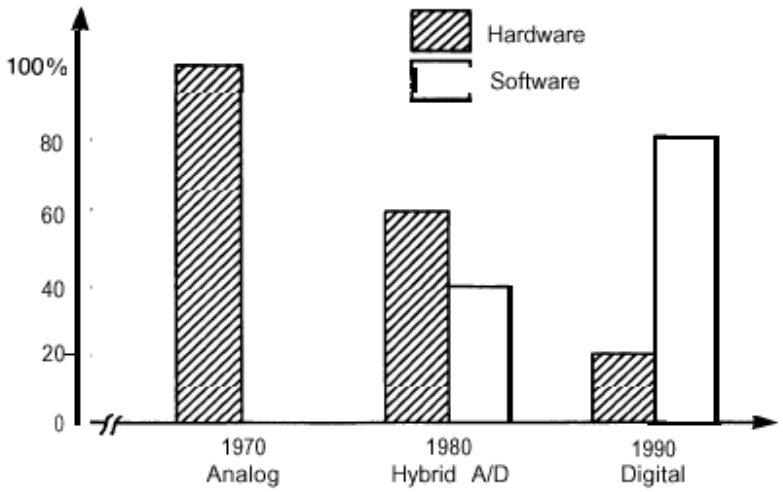


Figure 2: Failures by hardware and software components in percentage. Change over period 1970's – 1990's. [Ref. 4]

On the other hand, modern digital protections implement most of the functions based on software, so more attention is paid to software elements check, both software and hardware. In the next chart it is shown the percentage failures occurred by hardware and software components, being the 90s figure relatively constant and yet valid for present days.
Software should then be considered as another module. In fact module that contributes to higher probability of failure. Therefore, some way of software self-supervision should be also considered. For this purpose, watchdog hardware built in mechanisms in modern processors may help. Other high level “watchdog” or “token passing” mechanisms may be used to complement the latest.
Obviously, the scope of self supervision should include the components with the biggest failure probability for whichever reason.
Software failure modes include not only manufacturer’s bugs but also user programming bugs (i.e. when programming flexible logic schemes).
Hardware failure modes include output relays and circuit supervision even though sometimes failures are due to unavoidable wear out, lighting, overloads, etc. more related to overall application than to the pure IED design or manufacturing quality.

In the appendix 11.3 we describe some hardware and software components that may be monitored based in existing products. [Ref. 5]

7.2.3 Coverage

It is important for the user to know how much coverage the self supervision provides. In many cases it is not practical providing a percentage quantitative number due to lack of data. In other cases manufacturers may give ratios difficult to show against any known standard. Therefore, qualitative coverage information should be given with a clear differentiation of two different states:

Start-up
Typically during start-up tests are done that should be disruptive during runtime.
Modern protection equipments with many built-in functions may require significant start-up time until protection functions are ready to work. In case of electromechanical and static relays start-up time is negligible (it is in the range of less than 1 second for many analogue products), whereas it may become important for digital protections. If functions are enabled in a stepped approach, manufacturer should declare a table of functions availability and time. For example, protection is ready after 30 seconds of start up, communication is ready after 1 minute, etc.

Runtime
These tests are intended to diagnose possible real-time failures due to component aging,

drift, premature failure, verify memory circuit's integrity, internal buses connections, etc.
Self supervision is done typically during background time of circuits; therefore they do not affect relay response. Any effect on product unavailability should be declared. If, for instance, a complete test of a circuit that takes 1 second is done every day, this should be declared, even though the effect in availability is quite low (12 parts per million).

7.2.4 False alarms

Three collateral effects of self supervision may be foreseen:

Fail to detect a failure

Self supervision cannot cover 100% of circuit failures. Even for simple functions like a battery voltage monitor, the circuit that monitor battery may also fail. To minimize the chances of this effect, monitoring or supervision circuit (or software module) should be simple and robust. In theory it should have failure rate one or two levels of magnitude better than the monitored circuit, otherwise it is probably a useless waste of resources.

False alarms

This is probably the worst effect for two reasons. Cost, due to attending something that was not a real problem and loss of detection system credibility that may lead to disabling the function, tampering or worse: reaction time in future opportunities. Probability of a false alarm should be reduced, in the order of 1% false alarms

Disruptive test

Supervision should be done in a way that does not interfere with normal protection functions. Any effect in delaying or even disabling a trip should be considered.
It should be checked supervision sanity.
For instance, circuits with limited number of operations (i.e. an EEPROM memory with, say, 10^5 operations) should not be operated beyond its limits (i.e. continuous read and write test during idle or background time at a rate of 1 per second). Some of these effects are not visible during static, dynamic or endurance tests, therefore they require a deep product review.
Prevention principle should reign as in other critical areas (medicine, law, etc.).
The simplicity principle should also be used to improve overall reliability.

7.2.5 Self action (response from the device)

When either type of self-test error occurs, the IED will react automatically in some way.
For instance, it may signal the error via local HMI (LED indicators, display). It may also indicate such error in an internal variable that may be read via communications.

Depending on error criticality the protection status may change from regular to a predefined “fail safe” status.
A minor error should not disable protection. For example, in case a measurement monitoring device detects measurements out of tolerances, the equipment could use some default calibration parameters that would reduce accuracy to a level still acceptable in a protection scheme. This behaviour provides higher availability than other that would disable completely the protection.
In certain cases, user may bias relay towards security or dependability manually or he may decide to set the relay to react automatically in one way or another. Due to the possibility of human error and the slow human response time, automatic mechanisms are preferred. Leaving decision to an additional setting in a complex IED may increase unnecessary complexity that drives lower usage reliability, therefore settings are not recommended for these kind of automatic responses.
In cases where a critical major error is found, it is recommended disabling all responses, including output contacts, to a secure state, i.e. keep output trip contacts open. When this occurs, user should be able to detect both locally and remotely, this new “protection disabled” status. Modern IEDs include a “ready” normally closed contact that will open in such cases. Normally open contacts are preferred because in case of an auxiliary power outage, it will also go to that “disabled” status signalling something is wrong in the system.

The manufacturer should clearly assess which is the IED response in case of an error and recommended user reaction in such cases.

An example of how this description could be done is included in appendix 11.3

7.2.6 Prevent malfunction

It is important to highlight that anything done either automatically or manually, should be focused to prevent mal function. False trips create major losses in processes and should be avoided. Self check should contribute to an early detection of failures and, very important too, prevent product mal function, mainly false trips. One way to implement this “fail safe” mode is disabling all contact outputs to a secure predefined state. In modern schemes that cooperate via communications in complex protection schemes, such as a multi-voting scheme in an Ethernet IEC61850 based system, should consider a “dead relay” as a non valid vote. Even though this is obvious, the fact that in software logic schemes there is not a conventional schematic diagram that was available in wired connections, may lead to this utilization error.
Disabling a protection is converting a valuable protecting device into a useless black box. Therefore, self check mechanisms should be robust, using safe and clear mechanisms in simple surveillance schemes either software or hardware.

In certain digital IED's there is a digital trend by which the relay works perfectly or disables all functions. This digital behaviour (either works or not) may not be optimum in complex products that include many protection functions. For instance, if a distance protection provides overcurrent backup and a voltage input fails (due an internal product error), it could be considered the possibility of disabling only voltage related functions, while preserving the simpler overcurrent backup ones. This "analogue" or continuous behaviour may combine both security and dependability in a better way, providing maximum availability.

7.2.7 Analyse signalling what information do we need (for efficient maintenance policy)

Too little data on a failure event may be a bad situation to react. Too much data may be even worse, provided that some situations are critical and need immediate user response. It is said that "you can't see the wood for the trees". A sound self supervision scheme should provide enough and relevant data. It should also provide a way to obtain useful information on failure detected, so that the user quickly identifies what failed and knows what to do in such case.

Present policy of many users is carrying a complete IED to an installation once a failure is detected. Unfortunately the many models, many manufacturers and different applications, may make keeping spare IED's or even spare parts to fix quickly one failure in the field impractical.

Manufacturers should provide, as much as possible, standard equipments with modular design and minimum models variation, especially hardware related. Even though updating modern equipments, flash memory based, via communications, may seem easy, sometimes users do not have enough training, laptops, or they do not have the required files in their PCs. For this reason, it would be also recommended a single piece of software valid for all models and simple product upgrade procedures. All this takes into account easy maintenance.

Self supervision should lead to easy failure detection. This should provide enough information on module failure (either hardware or software), for a quick replacement that will lead to fix field repair. If the product should be taken to user laboratories or manufacturer facilities, it should be preferred "draw out" types that leave case and wiring in place.

For an efficient maintenance, it should be considered the possibility of a remote diagnostic and possibly remote product fixing via communications. This leads to the "tele-charge" concept that may increase user productivity avoiding travelling on site, many times to

remote locations in harsh environments. This nice concept should be complemented with enough access security to prevent product tampering by hackers or inadvertent manipulation by authorized users.

Taking into account overall costs, each user should find his own optimum point for periodic intervals.

For meshed distribution lines with frequent faults occurrence, a reactive approach where user will service an equipment that failed when detected a wrong behaviour, could be followed without major problems.
For high responsibility high voltage critical short transmission lines with low frequency of faults occurrence, that reactive approach would be unacceptable. In many cases, redundant schemes with different manufacturers, models or protection principles, may help. Nevertheless, the common mode failures make it still important the periodic testing. In case a common battery with a single fuse may be a weak point even when complex hardware or software IEDs protection schemes are used.
Period testing should preferably be done with modern automatic test sets that cover a significant part of the IED functionality. The trend is to carry out complex and comprehensive testing during SAT (Site Acceptance Tests), while periodic tests are limited to simpler tests. This was a good approach in the past when simple, reduced number of functions equipments was used and testing tools were quite simple. Nowadays, computer programmable test sets may allow quick and productive comprehensive testing during both FAT and periodic testing.

Self check supervision should be done:

- Simple, sound and reliable
- Oriented towards increased overall availability
- Described clearly by the manufacturer
- Comprehensive
- Following “fail safe” principle
- Clear information to detect what failed and how to react

7.3 Remote maintenance

7.3.1 Remote setting

When protection relays work normally during normal system faults, it is enough to check relay operation with the fault information and relay recorded data.
However, in case of the complicated system faults where it is suspected a relay mal-

operation, we need additional information like SOE (Sequence of events) records, disturbance records, fault reports, relay settings, etc.

In the case of some relays, the data can only be retrieved at the substation. In case of remote operation system, we can get the recorded data from a maintenance centre. So we can do the relay operation analysis faster.

The settings change of protection relay occurs as a result of the change of a system constant and the reconsideration of the system operation. At some utilities, setting values are changed on the system change by using a remote operation function from a dispatching centre. For utilities that have frequent system changes, it is very effective that engineers don't have to go to the substations.

When implementing settings changes via the remote operation, the security must be paid attention not to have unjust access from outside. Special setting change that accompanies facility fault occurs suddenly regardless of the time, most of them caused by the natural phenomena such as the earthquake, the heavy rain, the windstorm, the snow damage. Engineers have to go to the substation through dreadful weather. Therefore, if the setting change by remote operation can be applied, it is possible to secure the safety of engineers in addition to fast system restoration.
The technique to judge the degradation tendency of the relays is introduced by comparing a relative error of measuring current/voltage data. Concretely, in case of dual protection relaying, the sampled current/voltage data are compared with each other at the same time and we can manage the degradation tendency of the analogue input part.

In cases when flash memories are used for relay, utility is able to rewrite a sequence. For example, if utility wanted to change a policy of reclosing for line protection, utility can be able to rewrite a reclosing logic by using remote personal computer. The maintenance engineer of utility and the technical engineer of manufacturer go to a substation and repair software now. However, the engineer of utility could repair software by using remote operation from a maintenance centre.
The labour will be saved by the decrease of the opportunity to go to a substation both of the utility and manufacturer. The major challenges are:

- That the available hardware allows software upgrades.
- The way of testing on-site changes done
- To secure the reliability and the security of the communications channel.

7.3.2 Measures for security

In the communication network, when information is transmitted, it goes via various courses. Therefore, the bugging of the information, the interpolation, destructions by the unauthorized network user and so on are worried about. To prevent from an invasion into these networks, the security measure becomes necessary.

Incidentally, whatever measure is implemented, we can’t get a perfect measure. If LAN connects with the protection relay electrically, we do not know when to be attacked.

The security measure implementing at the utility that applies remote operation is as follows.

The remote operation communication network is separated from other communication network physically and prevented from unauthorized user's accessing unjustly from other network.

Compulsion control commands lead to mal-operation. As for the control order about a protection scheme, it doesn't make operation conclude only in remote operation. Only if both conditions by remote operation command and another command are met, would actually control the equipment. Even if the remote operation network is invaded, the unauthorized operation to the protection relay cannot be achieved.

It is effective to implement some security measures. The best security measure must be taken after considering the cost, the effect and the damage of the measures. Therefore, the company that adopts remote operation must have clear security policy beforehand.

8 CONCLUSIONS

In this report we have dealt with the various forms of secondary system change. Several driving factors for change have been described as well as practical refurbishment strategies in several countries. Cost constraints and technical factors have a major influence in these business decisions. The authors have sent a survey that has been answered by different actors (utilities, consultants, etc.) of several countries. Several conclusions might be extracted from the experience shared between the authors of this paper:

Definitions

There is no standard terminology for change (refurbishment, repair, replacement) across different users. The meaning of these terms is related to the context (i.e. component / system level). The authors have provided definitions for this paper.

Driving forces for change

In certain cases, one could wonder whether there is or not an urgent need for change. This report describes ways to quantify such need.
The need to minimize down time makes it interesting sometimes replacing both secondary and primary systems in the same field service.
Main drivers for change have been identified as quality of service, cost of implementation and risk associated with change or with no change.
New functionality is rarely identified as one of the major drivers for change by users.
Cost is the driving factor for change as many factors may be eventually translated into cost. Some clues of how to calculate the overall costs are given in this paper.

Refurbishment strategies

Refurbishment strategies are many times conditioned by the need to continue supplying electricity to certain users.
There are several methods to calculate total life cycle costs. All of them have a common ground and take into account the initial acquisition costs as only one component of the many ones that one has to take into account in electrical projects.
There are numerous strategies for change. They depend of factors such as geography, voltage level, technology, customer know-how and mix of products installed.
Several countries have described their experiences facing product aging, failures, etc
All migration and general change strategies may represent some risks. New digital equipments may need to take into account EMC (electromagnetic compatibility) and environmental conditions that were not an issue in electromechanical technologies.

Practical experiences

From each experience we may learn best practices, taking into account that not all practices may be applicable sometimes in all situations due to different contexts.
Manufacturers may play a key part in contributing to a seamless and successful refurbishment, replacement strategy.

Trends

Self checking modern IED's capabilities may help to reduce the need of commissioning and reduce overall maintenance time and cost.
Self check may help to improve installation reliability by detecting early failures that could derive, if not properly addressed, into major system unavailability.

9 REFERENCES

1. Distance Protections: What Limits of Use for Heavy Loaded Very High Voltage Lines? J.M. Grellier, J.L. Chaneliere, FR 306, Madrid Colloquium 2007
2. Protection Relay Life Cycle Management, Christopher Smith, John Wright, Steve Pickering, March 2008
3. Guidelines for Specification and Evaluation of Substation Automation Systems, CIGRE WG B5.18, August 2007
4. “Digital relay software quality”, Elaine Y. Wintraub GE Protection and control – Charles R. Heisking , Associated Power Analyst, Philadelphia, 1993
5. “G60 Generator Management Relay UR series instruction manual”, GEK-106411A version 3.3X, GE Multilin, March 2003. Latest manual version available on the link: http://www.gedigitalenergy.com/app/ViewFiles.aspx?prod=g60&type=3

10 APPENDIX

10.1 Maintenance strategy. Example 1.

Beneath there is given an example of maintenance strategy applied by utility operating transmission and distribution network.

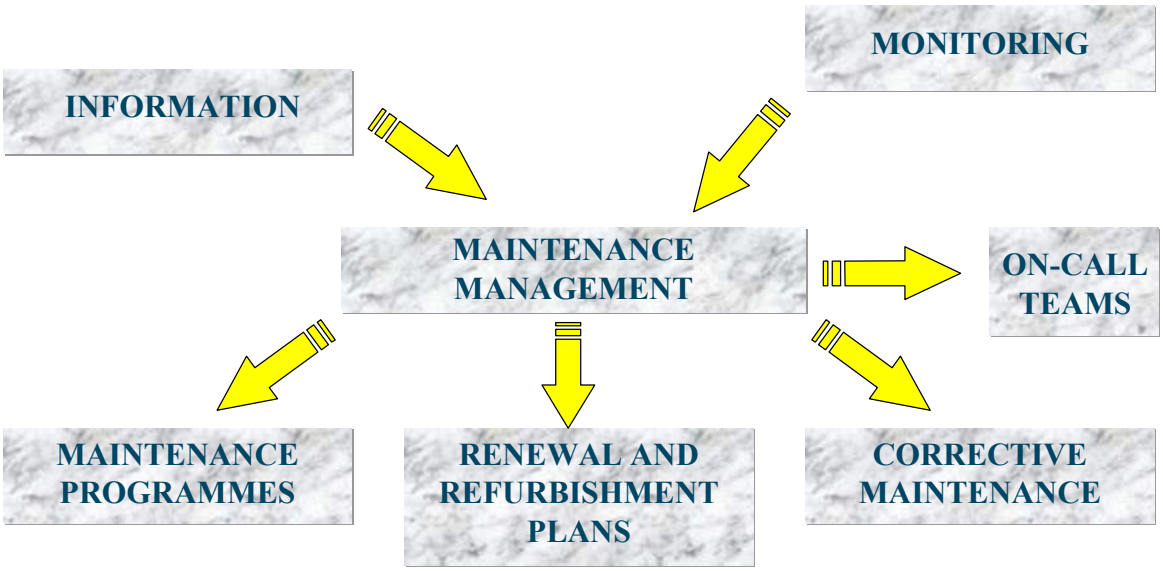
1. guarantee tests before 2 years of usage
2. 3 years periodical testing for electromechanical relays, for electronic (static) relays and for the first version of numerical relays
3. 6 years periodical testing for new numerical relays with coverable self supervision function.
4. yearly measurements of internal electronic voltage levels for electronic relays without self supervision
5. preventive maintenance (replacing risky parts and cards with new ones) for some electronic and first generation of numerical relays after 15-20 years of lifetime

From manufactory point of view six years test interval is quite long for the new digital relays. The end-user cannot rely that the internal self-supervision is able to detect all major internal faults. With the first and the second generation of the numerical relays the self-supervision could detect not more than 80 % of internal faults. The self-supervision of modern generation numerical devices is proved; statistics of the self-supervision is not available. However experiences with internal self-supervision of the latest generation are encouraging.

10.2 Maintenance strategy. Example 2.

As a general comment, one of the domination parts of the operating costs is the maintenance and all relating costs. In order to optimize the service strategy, all relevant cost portions have to be considered. Different maintenance strategies such as time based, corrective, condition based or reliability centred maintenance have different impact on life cycle cost. The decisive parameters have to identify and their influence on the overall cost has to determine, so individual calculations are necessary for the practical application of these principles. The duly investigation on the life cycle cost and a tight asset management reduces the overall cost and contributes to the economical benefit of the operating utility.

Basic Organization Chart



10.2.1 Example of maintenance measures

Next, example of maintenance measures for protection systems determined by the used technology is described:

ELECTROMECHANICAL AND ELECTRONIC ANALOG SYSTEMS

Checking of operating characteristics

Operating levels

Response times

Checking of operating logics

Interaction with operating components

Interaction with other equipment

Records control

Checking of the signalling

To the control centre through the RTU

To external event and signals recorders

To mimic board and alarm panel

Checking of established settings

Checking based on theoretical setting list

ELECTRONIC DIGITAL SYSTEMS

Checking of operating characteristics related to System

Operating logics

Operating levels

Response times

Control of operating logics
Interaction with operating components
Interaction with other equipment
Records control
Oscillographs collected and checking of recorded signals
Control of the analogue-digital converter response
Measurement of in-service values
Measurement under controlled injections (inputs)
Control of established settings
Checking based on theoretical setting list

Furthermore, other secondary system maintenance areas can be:

REMOTE CONTROL UNIT DIAGNOSIS
Inquiry for self-diagnosis
Light indications
Internal alarms configuration (data base)
Either field or remote supervision – Remote loading
Check of voltages at the equipment own electric power sources
Check and adjustment of analogue measured values
Check of the orders limiter unit
Check of digital inputs and outputs
Check of redundant nodes switching

Remote Maintenance Applications:
REMOTE SUPERVISION: Remote supervision of substations and remote control equipment. State, values reading, active alarms, internal alarms and Chart Recorder values collected.
REMOTE LOADING: Remote configuration of control equipment. Tracking and change of internal operating values and data base full loading.

10.2.2 Functional requirements and added value

Earlier protection schemes may not be considered sufficient anymore and thus also the increased performance and functionality capabilities can be a driver for change.

Functional integration capabilities make it possible to group all the feeder functions into a single device thus replacing a collection of elementary elements. This reduces the cost of the spare parts and copes with the new functional needs. Other drivers for change may be equipment standardisation

The new business needs, which require more information, will direct the utilities to upgrade the existing substations. Therefore information is needed about the industrial as well as other types of customers, i.e. computerized load forecast, complicated metering system bulk trading and energy management. The accuracy and the reliability of the data depend on the utilities/traders. Therefore the data availability gives the utility the chance to be strong in very competitive field. In next subchapters the major technical issues that require the upgrading of the existing conventional substation are described.

Examples for need of new functions

In Helsinki Energy (FIN) three most wanted new functions of modern IED's are: self checking function, disturbance and event recording and free programmable integrated functionality. These functions are often also triggers for secondary changes. Self-checking and disturbance recording functions give possibility to improve reliability and availability of protection system. Possibility to integrate many functions into same IED gives financial savings especially in MV level, where separate overcurrent relay, directional earth fault relay and auto-reclose relay were used before. In HV level modern relays provide option to combine synchro-check and backup overcurrent relay into differential and distance IED's.

10.3 Examples of self-check functions

10.3.1 Hardware

Output relays

The main processor does not have any way of checking if an output relay operated unless there is a feedback. This feedback may come from voltage and/or current supervision schemes.

Tripping or closing circuits

The tripping (or closing) circuits work like a series connection in a reliability block diagram approach. It includes several components that may fail, like battery, wires, relay output contact, breaker trip (or close) coil, breaker auxiliary contacts (52a and/or 52b), possibly burden resistors. Some equipment has the capability to monitor the integrity of the COMPLETE circuit. Therefore this should be called, trip circuit supervision, avoiding the term self supervision.

AC circuit

Protections typically have 1 to 12 ac inputs, including current or voltage type inputs. Most times they come from conventional VTs and CTs. Other times they come from more modern sensors that provide low level signals (i.e. Low power transformers, Rogowski coils). In these circumstances they provide analogue low level signals that must be converted to digital for signal processing. Some protections used spare analogue multiplexed channels in their internal analogue to digital conversion circuit, to double check signals sanity by comparing the main voltage reference with another secondary reference.

Power supply

Power supply is a critical component of an equipment and it suffers more electrical stress than other low voltage internal circuits. Therefore some ways of voltage monitoring could be used to detect consumption, voltage, temperature or other parameters that may help to predict or detect a failure. Obviously it is better prevention than detection.

Batteries

Some equipments use batteries to store information when main auxiliary voltage is not present. Due to limited battery life, it should be monitored to detect a low voltage before it actually losses its complete function to store this information.

Communications

Due to the importance of communication in both controllability and monitoring capabilities that affect product availability, some ways of supervision should be used.

Some supervisions may be done at the physical layer to detect failures such as fibre optic broken (this may be especially useful in redundant fibre optic schemes).

Other supervisions may be done at upper levels. Some protocols use a “live signal” periodic message to the master station that may help to detect a ready communication system that relays not only on physical wires or fibres, but also in the complete IED communication function. In this sense, modern protocols such as DNP 3.0 and IEC61850 provide naturally schemes for this function. For other simple protocols, such as Modbus, this function may be implemented in the user application based on simple read/write simple functions.

10.3.2 Software

In this category it may be include supervisions that affect to software, firmware or hardware that cooperates to implement the software functions, such as:

- Hardware Watchdog.
- Software Watchdog.
- CRC (cyclic redundant check) checking in non volatile memory circuits logs.
- CRC main program checking
- Virtual logic token checking
- Memory utilization

The manufacturer should clearly describe:

- Which component is being tested.
- When and how often is it tested.
- Which message is provided.
- Description of the problem
- Effect and criticality
- What should the user do
- What does the relay do automatically
- Supervision effect on product availability

10.3.3 IEDs response and recommended actions

Major self-test errors also result in the following:

- The critical failure indicator relay is de-energized
- All other output relays are de-energized and are prevented from further operation
- The faceplate Ready LED indicator is turned off
- A “protection out of service” event is recorded
- Internal “critical error” flag set to logic level 1.

Recommended action:

Contact factory for service.

Minor self-test errors result in:

- Faceplate “minor error” LED indicator turned on.
- Internal “minor error” flag set to logic level 1.

Recommended action:

Keep reset key pressed for 5 seconds. Switch auxiliary power off and on. If not cleared, please contact factory for service.