329

GUIDELINES FOR SPECIFICATION AND EVALUATION OF SUBSTATION AUTOMATION SYSTEMS

Working Group
B5.18

August 2007

cigré

GUIDELINES FOR SPECIFICATION AND EVALUATION OF SUBSTATION AUTOMATION SYSTEMS

Working Group B5.18

At the time this report was completed, WG B5.18 had the following membership :

Peter Rietmann (Switzerland) – *Convener*

Regular member:

Robert Kirkman (Germany)
Markku Hyvarinen (Finland)
Mika Loukkalahti (Finland)
Giorgio Giannuzzi (Italy)
Thierry Fortin (France)
Steven A Kunsmann (USA)

Corresponding members:

Guilherme Moutinho Ribeiro (Brazil)
Hélène Guéguin (France)
J Singh (India)
Nik Sofizan (Malaysia)
Tomas Johannesson (Sweden)

n° ISBN : 978-2-85873-014-8

Table of content

1 Scope and objectives 7

2 Executive Summary 8

3 Introduction 9

4 Guidelines for specification and evaluation of technical requirements 14

4.1 Basic technical requirements 14

4.1.1. Functional requirements 14
4.1.1.1 System functions 14
4.1.1.2 Supervision functions 15
4.1.1.3 Control functions 17
4.1.1.4 Protection functions 21

4.1.2. Performance requirements 21
4.1.2.1 Message performance 21
4.1.2.2 System performance 22

4.1.3. Environment (thermal mechanical, insulation) & EMC requirements 24
4.1.3.1 General statements 24
4.1.3.2 Relevant standards 25
4.1.3.3 Severity levels 27

4.1.4. Reliability requirements 28
4.1.4.1 Method choices 29
4.1.4.2 Pragmatic approach 31

4.2 Information management 32

4.2.1. Introduction 32

4.2.2. Information target groups 33
4.2.2.1 Operation 34
4.2.2.2 Protection system engineering 34
4.2.2.3 Maintenance 35
4.2.2.4 Network planning 35

4.2.3. Monitoring 35
4.2.3.1 Primary equipment monitoring 35
4.2.3.2 Secondary system 37

4.2.4. Maintenance strategies and support 39
4.2.4.1 Maintenance strategies 39
4.2.4.2 Actions 39
4.2.4.3 Expected benefits 39

4.2.5. Data for asset management 39
4.2.5.1 Examples of calculation and models 40

4.2.6. Information access and security 41
4.2.6.1 Security standards 41
4.2.6.2 Security objectives 43
4.2.6.3 Security measures inside the substation 44
4.2.6.4 Security measures outside the substation 44
4.2.6.5 Requirements and conclusions 45

4.3 System architecture examples 46

4.3.1. Redundancy choices ... 46
4.3.2. Function allocations choices ... 46
4.3.3. General Overview ... 46
4.3.3.1 Process level ... 47
4.3.3.2 Bay level ... 47
4.3.3.3 Station level ... 47
4.3.4. Recommended communication standards ... 48
4.3.5. Abstract System based on IEC 61850 ... 49
4.3.6. Examples for SA System Architectures ... 50
4.3.6.1 Overview ... 50
4.3.6.2 Example 1: Distribution substation ... 51
4.3.7. Example for a transmission substation ... 51
4.3.8. Example for a extra high voltage transmission substation ... 52
4.3.9. Web based solution ... 53
5 Guidelines for specification and evaluation of project management and services ... 54
5.1 Project management ... 54
5.1.1. General Considerations ... 54
5.1.2. Engineering phase ... 55
5.1.3. Commissioning phase ... 57
5.1.3.1 Site erection strategy for refurbishment substations ... 57
5.1.3.2 The erection objectives and constraints ... 57
5.1.3.3 Review of different erection strategies ... 58
5.1.4. Acceptance, quality and type tests ... 59
5.1.4.1 General Overview ... 59
5.1.4.2 Type Tests ... 59
5.1.4.3 Factory Acceptance Test (FAT) ... 60
5.1.4.4 Site Acceptance Test (SAT) ... 61
5.1.4.5 Trial Operation ... 62
5.1.4.6 Quality system ... 62
5.1.5. Documentation ... 62
5.1.5.1 Schedule for submittal of documents ... 62
5.1.5.2 Offer documents ... 63
5.1.5.3 Base design documents ... 63
5.1.5.4 Detailed design documents ... 63
5.1.5.5 Final documentation set ... 63
5.1.5.6 Approval of documents ... 64
5.1.5.7 Software ... 65
5.2 Warranties, after sales services and training ... 66
5.2.1. Contractual aspects - Warranties – penalties ... 66
5.2.1.1 Contractual aspects ... 66
5.2.1.2 Responsibilities and cooperation of different parties ... 66
5.2.1.3 Guarantee period(s) and maintenance ... 66
5.2.2. Training ... 67
5.2.2.1 General Aspects ... 67
5.2.2.2 Focus and Content of the Training ... 67
5.2.2.3 Number of Participants ... 68
6 Considerations for IEC61850 based SA ... 69

6.1 Substation related considerations 69

6.1.1. Single line diagram 69

6.1.2. Process interface 69

6.2 Specification of functions and the related data model 69

6.2.1. Functions 69

6.2.2. Data model 70

6.2.3. Naming convention 70

6.3 Communication related issues 70

6.3.1. Time synchronisation 70

6.3.2. Services 71

7 Weighting of requirements - evaluation and comparison of different substation automation systems 72

7.1 The first stage - specification 72

7.1.1. Technical and functional requirements 72

7.1.2. Basic requirements for the system 72

7.1.3. Options 72

7.1.4. Project management requirements 73

7.2 The second stage - evaluation and comparison of tenders 73

7.2.1. Basic steps 73

7.2.2. Added values 74

7.2.3. Life-cycle cost (LCC) 74

7.2.3.1 Investment cost 75

7.2.3.2 Operating costs 75

7.2.3.3 Maintenance costs 75

7.3 Weighting of requirements 76

8 Conclusions and recommendations 78

A Terminology 79

B Definition of acronyms 82

C References 85

D Applicable Standards 86

E Basic review on Dependability (Reliability definitions and parameters) 88

E.1 Reliability parameters 88

E.2 Reliability Databases 89

E.3 Reliability standards 89

E.4 Methodology guidelines 90

Table of figures

Figure 4.1-1 Control hierarchy levels 17
Figure 4.1-2 Definition of message transfer time 21
Figure 4.2-1 Information Management – Communication Networks...................................... 32
Figure 4.2-2 Data integration for IMS (Information Management System) 33
Figure 4.2-3 Disturbance record with measured voltages and internal signals of the relay.... 38
Figure 4.2-4 Example of transformer monitoring application 40
Figure 4.2-5 Data security requirements – threats – attacks 42
Figure 4.2-6 Data security counter measures 43
Figure 4.3-1 Abstract system architecture based on IEC 61850... 49
Figure 4.3-2 Architecture example for a distribution substation 51
Figure 4.3-3 Architecture example for transmission substation 51
Figure 4.3-4 Architecture example for a extra high voltage transmission substation.............. 52
Figure 4.3-5 WEB based SAS solution 53
Figure 5.1-1 Development process 54
Figure 5.1-2 Remote control migration... 58
Figure 5.1-3 Acceptance test matrix... 59
Figure 5.1-4 Type test content.. 60
Figure E.1-1 Relation between different reliability parameters 88
Figure E.4-1 Modeling selection criteria’s for availability calculation 90

Table of tables

Table 4-1 IEC61850 Message types / performance overview 22
Table 4-2 Typical performance measures at station HMI level 23
Table 4-3 Relevant standards concerning environment and EMC.. 26
Table 4-4 Self diagnostic tasks... 30
Table 4-5 Overview of Security Standards and Guidelines... 41
Table 4-6 Security standards prepared by IEC TC57 42
Table 4-7 SA Architecture Impacts... 50
Table 5-1 FAT tests overview.. 61
Table 7-1 Weighting of requirements – Price 76
Table 7-2 Weighting of requirements – Investment Cost 76
Table 7-3 Weighting of requirements – Life cycle cost.. 77
Table 7-4 Weighting of requirements – Qualitative Comparison... 77
Table D-1 Applicable Standards – IED mapping.. 87
Table E-1 Reliability parameters definition... 88

1 Scope and objectives

The CIGRE Study Committee B5 (Power System Protection and local Control) decided to form a new working group with the task of writing a guide for the specification and evaluation of substation automation systems.

This group intends to deliver “guidelines” i.e. an *applicable and relevant* set of technical, methodological, economical recommendations concerning:

- Technical requirements (part 4) in accordance with the utilities needs and with the industrial offer, for a cost effective and realistic implementation,
- Project management and substation automation related services requirements (part 5) in order to help to manage the Substation Automation project, its operation & maintenance,
- Weighting and evaluation of requirements (part 6) in order to help utilities to focus their needs, to assess their project steps, to evaluate and compare tenders.

This work is mainly based on the analysis of the technology’s state of the art, of utilities needs and of first learning acquired on such systems, taking into consideration utilities as well as manufacturers points of view

It also takes into account the previous and future investigations concerning substation automation:

- It extends the B5/WG07 work concerning substation automation systems features and capabilities
- It establishes a coherent and applicable transition with the upcoming standard IEC 61850 before this norm is finalized and commonly practiced by utilities as well as manufacturers.

2 Executive Summary

Guidelines are focusing mainly on transmission substations

Many utilities are facing the challenge of having to prepare new specifications for substation automation or of having to adapt their existing specification to reflect the latest developments and new possibilities that are available for modern substation automation solutions.

The working group B5-18 was started some years ago with the goal to provide guidelines for the preparation of such specifications and to furnish supporting information and methods for the evaluation of the different offers submitted by the bidders.

The recommendations for preparation of specifications are based on the experiences of utilities and supported by the learning's of the suppliers. Those for the evaluation itself are derived from the experiences of some utilities and backed up by a survey conducted with additional utilities.

A sustainable specification for substation automation shall ideally be prepared in such a way that it is focusing on functionality, performance, reliability, evaluation, project management and services to ensure a fair participation and evaluation of the bidders.

To get a better picture and also feedback from utilities concerning the evaluation of an offer, utilities were asked about their methodologies within a survey. The survey showed that it seems to be an area that is not likely to be shared with others. There might be fears of giving information to the public. So the evaluation part is only based on a few responses.

In order to finalize the report of the WG18, the feedback and the papers from the CIGRE Symposium 2005 in Calgary with the Preferential Subject 2: Specification & Evaluation of S/S Automation Systems have been considered to provide a guideline that covers the areas and problems of the substation automation business as comprehensively as possible.

3 Introduction

A substation automation system shall provide on one hand all the functions that are required for the correct and safe operation of the primary equipment that is contained in a specific substation as well as for the adequate protection and condition monitoring. On the other hand it has to incorporate compatible communication interfaces for the connection of the substation to one or more network control centers.

The scope of functionality of a substation control system depends on the following aspects:

- Size and significance of the substation
- Range of voltage levels concerned
- Operational philosophy (for testing, commissioning, operation and maintenance)
- Availability requirements as criteria related to the substation's criticality and significance in the grid or for consumers.
- Integration of the substation control functions into the user's network management concept, with a varying number of network control levels and a different distribution of functions between network control centers and substation control
- Decoupling of the renewal cycles between substation control, power system management and transmission technology.
- In case of retrofit the integration into the user's existing substation environment in terms of interfaces to the existing equipment and co-ordination with secondary devices for dedicated protection and monitoring that are not substituted by new IEDs that are integrated in the new substation automation system.

Boundary conditions

Specific functionality and boundary conditions of the SA shall be adapted to the requirements, which are related to the particular voltage level and the specific substation layout. Such boundary conditions include:

- Overall single line diagram
- Location of substation buildings
- Control and operation principles
- Protection schemes

Basic technical requirements

The basic technical requirements are the minimal part that is required to describe a substation automation system and shall ensure that bidders have all necessary information to provide a proper offer covering the needs of the buyer.
This basic technical description shall at least cover the following areas:

- Functional requirements
  - System functions
  - Supervision functions
  - Control functions
  - Protection functions
- Performance requirements
- Environmental & EMC requirements
- Reliability / Availability requirements

Information management

In addition to the local functionality at the substation level itself, the substation automation system in most cases also needs to provide information for users outside the substation. Depending on the targeted user, the type and amount of information that needs to be provided varies. Two main areas for information management can be identified:

- Integration of SA with network control
- Provision of data to remote users such as
  - Protection engineers
  - Operational and Maintenance centers
  - Planning and Asset Management centers

System architecture
Typical system architecture is divided into three levels:

1. Process level
2. Bay level
3. Station level

Depending on the actual application area, the SA System might be one with single communication and just a single gateway at the station level or it might be a system with full redundancy.

Considering that the system architecture is based on IEC 61850 one can identify the following main characteristics of an IEC 61850-based system architecture:

- Openness owing to IEC 61850 and other industrial standards like Ethernet, OPC etc.
- Seamless 100Mbit/s Ethernet structure
- Interoperability defined by IEC 61850
- Client-server architecture
- Bay interlocking / automation is independent from station level
- Optional functional redundancy of HMI and station computer
- WEB-based test and diagnosis at bay level (integrated web server)
- IEC 61850-8-1 at the station level
- Interbay communication (GOOSE= Generic Object Oriented Substation Event) at bay level

Impact of IEC 61850
Besides the working group B5-18, the working group B5-11 is also reporting on the impact of the new standard IEC 61850 on the specification of substation automation. To be able to answer the question: "What is the impact of the standard IEC 61850 on the specification of a substation automation system?" it is important to understand the basic features of IEC 61850.

These are:

- coverage of all communication needs in the substation, i.e. of / by both the so-called station bus and process bus
- no specification of functions but the provision of a data model for the functions and their communication needs, i.e. it does not block the future development of functions
- support of free allocation of functions to devices, i.e. it is open for different system philosophies
- definition of Ethernet as layer 1 and 2 of the ISO/OSI reference model, i.e. it provides the wide range of features of mainstream communication
- provision of the Substation Configuration description Language (SCL), i.e. it supports comprehensive consistency in system definition and engineering

The consequences of the features of the IEC 61850 standard therefore are:

- The functions have to be specified same as before, i.e. independent of the use of IEC 61850.
- It has to be decided whether the selection of devices is left to the supplier or is limited by some pre-selection of devices homologated by the utility.
- Availability figures or failure scenarios have to be discussed to get the most appropriate communication architecture.
- The environmental conditions have to be specified very much the same as before but some of these conditions might be decisive criteria for the selection of the communication architecture and, especially, of the communication media, e.g. copper cable or glass fiber.
- If the switchgear including the CTs and VTs already exists, its given type of process interface is important information for the SA specification.
- If the process interface can be selected (conventionally hardwired or serially linked) this might have some important impacts on the optimization process for the solution to be offered.

Project management and services
The project management and service part of a specification covers the parts beyond the technical part.

Engineering Phase
During the engineering phase the following milestones are very important and have to be agreed to between the manufacturers and users:

- finalizing the project time schedule
- defining the interfaces and delivery boundaries to other systems (primary switchgear, separate relays, remote control system) is important, especially if those systems come from different manufacturers than the SA-system. The new IEC 61850 standard will probably help to solve this present problem in SA-projects.
- Completion of single-line diagram, including position of the different objects (c.t.s, v.t.s, isolators,etc), which is the basis for the engineering work
- acceptance of the main pictures at station level such as single-line diagram, event list, alarm list
- acceptance of the lists of events and alarms (including their names) with the indication of the particular signal to be sent (station event list, remote, etc)
- approval of the cubicle layout.

Deployment Phase
This part of the specification only concerns substation refurbishment projects that have to deal with more severe erection constraints compared to new substation projects.
The aim is to establish an erection strategy for substation automation systems in existing, energized substations that have the target to:

- Minimize outages,
- Minimize operational constraints,
- Minimize software and site engineering work.

This provides a safe and cost-effective approach. Many tools and methods are likely to achieve the goals, such as:

- configuration flexibility of the system,
- quality of the utility site data inputs (site diagrams, site information).
- various “software” tools, avoiding less efficient and less reliable “hardware” wiring and cabling tasks or minimizing additional hardware and interface costs during on-site erection (temporary interposing relays,..)

Based on feedback from utilities and manufacturers’ proposals, several erection approaches might be considered:

- Fully parallel erection
- Bay level migration
- Remote control migration

Acceptance tests
Acceptance tests are intended to verify that the substation automation system is in conformance with functional, technological and performance specification, that it is free from failures and operates as intended. The Acceptance Test also provides a security for both the customer and the supplier. The tests are also confirming that both parties are in agreement on the functions and facilities, which are included.
The test results are approved and a report signed by a representative of the customer. Signing of the test reports does not absolve the supplier from any of his responsibilities during the guarantee period.

The acceptance tests can be grouped into three different categories:

- Type test
- Factory acceptance test
- Site acceptance test

The main goals of the different acceptance tests are to ensure technological and functional conformance is met and the requested performance is achieved.
It also makes sense to check the status on the quality assurance and project plan. Inspections shall be carried out during tests; based on hold and witness points indicated in the test plan, this inspection will provide information and confidence as to the quality of the tests and reduce the risk of failure during FAT or SAT with all potentially related costs and problems thereof.

Services
Services shall cover all items that are needed by the customer to enable him to run and maintain the delivered system. The areas covered by services are:

- Contractual aspects – Warranties – Penalties
- Training
- Documentation
- Maintainability
- Extendibility

Weighting of requirements
The basis for the evaluation process is established at the customer specification phase. At this stage, the utility is defining the technical and functional requirements for the equipment, system and services, as well as for the project management. Both basic (mandatory) and optional requirements for the system may be set. Already at this stage, it is also important and necessary to determine tangible performance requirements and weighting factors for intangible attributes.
The second stage of evaluation is carried out when utilities are selecting between tendered systems. The selection will be made between those tendered systems that fulfill the mandatory requirements of the specification by taking into account the quality of the supplier and the cost. In a more enhanced evaluation process, the economy over the total system lifetime is calculated, which includes added values as well as a lifecycle cost and risk analysis. Both tangible and intangible aspects must be evaluated. Tangible items can be quantified in financial or technical performance terms. By contrast, intangible issues cannot be quantified. However, they might be used to support decision-making or to prioritize between different solutions.
The costs and benefits are case-dependent and thus it is not possible to provide any numerical values for the weighting factors, but the basic steps of an evaluation process can be described as is done in the following chapters.

Fulfillment of requirements
The first step is to check whether or not the tendered systems are fulfilling the requirements defined in tangible terms. In this phase it would be convenient to have already clarified beforehand (in the specification), which of the requirements are mandatory and which issues are negotiable.

Project-specific items
The second basic issue is the evaluation of project-specific items to see whether it is possible to carry out the project according to the preliminary plan. This includes the analysis of risks, critical time schedules, reliability of the supplier as well as of the project plan for engineering, FAT, erection, commissioning and SAT.

Economy-related items
The third set of issues is economy-related: price and commercial conditions including delivery terms, terms of payment, warranty conditions, etc. The various commercial conditions must be valued so as to equalize the tenders. Present-worth analysis, leveled costing, or some a similar method of putting present and future costs on a comparable basis will have to be used.
The minimum requirement in cost comparison is to calculate the total capital cost instead of the pure quoted price. All costs of design, equipment, software, installation, testing, training, etc. for both the SA system supplier and the customer must be included. In some cases also the investment cost of the communication links outside the substation may have to be included.

In a more comprehensive calculus, the life-cycle cost (LCC) including the investment cost, added values, operation and maintenance costs are determined. In this calculation, the expected life-time of a SA system – especially compared to that of the primary equipment - is one important parameter. Also, the time period for which the cost should be calculated must be stated (this could be different from the expected life-time). Life-cycle cost is in itself a good measure for the overall performance of a substation automation system, if all cost components can be included. The problem is, that the calculation of LCC is more or less estimation with many uncertainties. However, when we are comparing different solutions, absolute figures are not that important.
Added values should at least be calculated for the optional functions and new features offered. This should be straightforward if the tender states separate prices for them, but these functions are more often included in the basic system of the supplier without any additional cost. In this case, a bonus could be added based on the financial evaluation of the added functionality as compared to the evaluation results of more conventional types of solutions.

Qualitative evaluation
The fourth step is the qualitative evaluation of those aspects that are difficult to give an economic value for. One way of avoiding qualitative evaluation is to convert attributes to criteria. In many cases this in not very convenient and it is more practical to use qualitative measures, i.e. to weight the different performance aspects of the systems by means of a scoring system. Weighting factors may be different from case to case, depending on the type, location and importance of a substation. If qualitative measuring is used, it is fair to predefine the selection criteria and weighting factors. Qualitative evaluation can be used to support decision-making, especially if the systems compared have rather similar investment and/or life-cycle costs.

Overall value
The final step is to find the highest overall value taking into account both the economical and qualitative evaluations. The quantitative (economical) and the qualitative values must first be scaled - with a chosen proportion between the scales, providing an opportunity to put emphasis on either one of these aspects - and then perform a scalar or vectorial addition.
While performing the evaluation - either economical or qualitative – it should be remembered that in order to achieve the overall benefits from the utility’s point of view, the cost of substation automation systems - and other related information technology based systems, SCADA etc. - might increase. Effective utilization of data also requires stronger employment of condition-based maintenance and asset management concepts. The main conclusion here is that substation automation systems should not be evaluated as independent units but as a part of the utility's other operations.
Beside those considerations also local rules may have to be considered e.g. in the European Union public owned utilities have to respect the EU regulations and procedures for the tender.

4 Guidelines for specification and evaluation of technical requirements

4.1 Basic technical requirements

4.1.1. Functional requirements

The functional requirements shall address all the needed functions of efficient monitoring and control of the entire system. Depending on the application where the substation automation system will be applied not all monitoring and control functions may be applicable.

All functional requirements can be mapped in one of the following main groups:

- System functions
- Supervision functions
- Control functions
- Protection functions

In the following chapters you'll find a brief description to each function and where applicable additional explanation on where the focus shall be set when compiling the specification.

4.1.1.1 System functions

HMI (local / station level)
The control of the switching objects shall be possible via the bay mimic or via the station HMI. For distribution substations bay control devices with integrated mimic shall be provided. For high and extra high voltage substation a backup mimic that allows in an emergency situation the control also without the control IED or a redundant station HMI is recommended.

Tele-control
The tele-control function provides the serial link to a remote control centre for remote monitoring and remote control. Several lines with different protocols shall be supported. A command authority mechanism shall apply for the control commands. Building of group alarms and pre-calculation of measurements needs to be supported to reduce the amount of signals submitted to the remote control centre. This is especially required when a substation provides huge amount of data but the communication link to the remote control centre has a small bandwidth.

Time synchronization
Events shall be time stamped directly at the source that means in the IED. The system wide synchronization shall be done via a master clock to all IEDs and relevant station level equipment. The time stamping accuracy and resolution shall be ±1ms (Time Performance Class T1 for time tagged events according to IEC61850-5). In case the synchronization source is lost the time derivation shall not exceed 50µs/s.

Data archiving
Archiving of historical events and measurement reports and trend data for long term storage and later retrieval or archiving.

Interfacing, open connectivity
The system shall support open connectivity towards third party IED as well as toward external software tools and packages via DDE, ODBC or OPC interface.

Access rights
To protect the system from unauthorized actions and changes the access to the system and its components shall be controlled by a user authorization mechanism. Meaning each user has to login with a user name and the appropriate password. Advances solutions allow defining for each user an individual profile concerning the access level of the different parts of

the system. If the user forgets to logout himself after leaving the system shall automatically logout after a pre-defined time out time.

System configuration
System configuration is not only needed at the initial stage of a project but also later when it comes to modification and system extension. The system shall include the necessary tools for modification of data bases and pictures for application changes and later system extension.

4.1.1.2 Supervision functions

The supervision functions can be divided into basic functions that are required as an absolute minimum for any kind of application and the enhanced functions that can be selected depending on the need of the particular project. As basic supervision functions are listed below:

Primary equipment monitoring
The primary equipment monitoring covers the supervision of all the primary equipment like circuit breakers, disconnectors and earthing switches positions, tap changer positions in real time.

Measurements
Measurements are taken by the control or protection IED directly connected to the VTs and CTs.

Secondary equipment monitoring
Internal diagnostics and all the secondary equipment has to be supervised concerning the communication status.

Communication supervision
The communication to all protection and control IEDs is constantly supervised. Also the communication to the remote control centre has to be supervised.

Sequence of events
All events are time stamped directly at the source. That means in the IED itself. The events are submitted to the station level where they are stored as historical data's and displayed in chronological order in the event list of the station HMI. The events can also be directly being printed via a matrix printer.

Long term storage of data, reports
The reports shall provide time-related follow-ups of measured and calculated values. The data displayed shall comprise:

Trend reports:

- Day (mean, peak)
- Month (mean, peak)
- Semi-annual (mean, peak)
- Year (mean, peak)

Historical reports:

- Day
- Week
- Month
- Year

It shall be possible to select displayed values from the database in the process display on-line. Scrolling between e.g. days shall be possible. It shall be possible to select the time period for which the specific data are kept in the memory.
It shall be possible to print out the report on request and automatically at pre-selected times.

Short term storage of data, trends
A trend is a time-related follow-up of process data. It shall be possible to illustrate all types of process data as trends - input and output data, binary and analogue data. The trends shall be displayed in graphical form as column or curve diagrams.
It shall be possible to pre-calculate the value before it is stored (direct, mean, sum, or difference) on-line in the window. It shall also be possible to change the update intervals on-line in the picture as well as the selection of threshold values for alarming purposes.

Operation counters for circuit breakers and pumps
The number of operations of circuit breakers, disconnectors and earthing switches shall be recorded. For circuit breakers the operation of pump starts and the operations associated with a circuit trip shall be reported separately. The operation shall be provided with a reset facility and the date of the reset shall be logged in the event list.

Collection of disturbance record files
Collection of disturbance recorder files produced in IEDs with disturbance recorder functionality shall be possible manually on request, automatically per a predefined cycle or automatically upon receiving an event (typically the disturbance recorder start signal) from the IED. The transferred file shall be stored on the hard disk of the station PC for further analysis or submission to a higher level system.
For the IEDs with integrated disturbance recorder as well as for dedicated disturbance recording systems, all recorded data shall be automatically uploaded (event triggered or once per day) to the SA station computer or a dedicated computer and be stored on the hard disc.

Analysis of disturbance recorder files
In case of power system disturbances, protection engineers currently use different kinds of information to find the cause of a disturbance. However, it is becoming more and more important to find these failures in a very short time and to react efficiently with suitable measures in order to restore the power supply as fast as possible.
The substation automation system shall provide all relevant information for faultfinding, analysis, and troubleshooting. Suitable and user-friendly fault evaluation software shall be included in the scope of supply, providing short fault summaries and printouts of the fault history and fault location.
The protection engineer may have his own PC-based system to evaluate all the required information for proper fault analysis, independent of the network control centers.

Metering (local/remote)
The data used for billing purposes are the metering data. The control and protection units usually do not have the required accuracy for metering purposes. Therefore the metering system is an independent, dedicated system with independent, dedicated hardware and software. The metering devices are connected to special metering current transformers (CT) cores and instrument voltage transformers (PT) cores. Metering data can be pre-processed in a station-metering computer (today normally a different system to the station computer for control), and are then transmitted to the metering department.
Technically it is already today possible to integrate power quality information via a LAN / Ethernet / IEC 61850 connection just as with IEDs to all relevant groups. Developments with VTs and CTs and the implementation the process bus may mean no distinction between protection and metering IEDs in the future.

4.1.1.3 Control functions

Mode of operation (local, station, remote)
The following modes of operation are applicable:

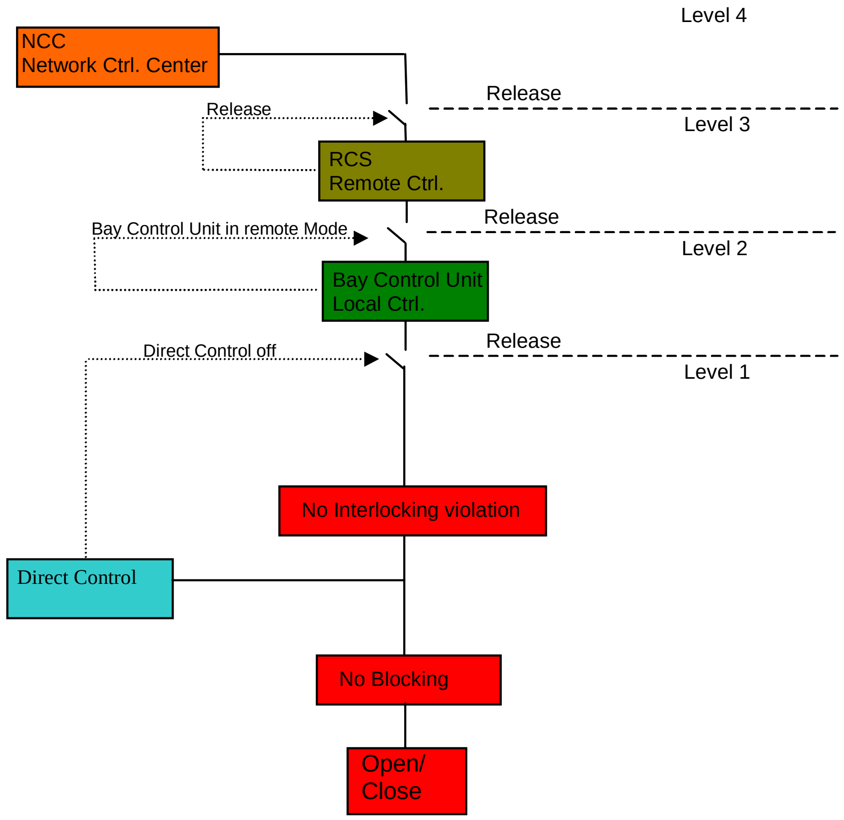

Figure 4.1-1 Control hierarchy levels

Level 1: Direct control from at the bay level

Level 2: Control at the bay level via the control IED

Level 3: Control from the station level

Level 4: Control from the remote control centre

Control of breakers and disconnectors
Control functions for circuit breakers and disconnectors are either used for directing the power flow during normal operation of the substation, or for maintenance of some primary equipment. They enable the operator or an automatic function to control the controlled object to open or close a breaker, disconnector or earthing switch.
For safety reasons the control functions normally include a "Select" step before the “Execute”, to check whether the control action is valid and the correct device has been selected, and to eventually reserve the required resources.
The “Execute” command is subject to miscellaneous conditions that assure that there will be no damage if the control action is conducted.

Select before operate principle
To operate an object the object to be operated shall first be selected in a first step. On the second step only the operation shall be permitted. The select command normally is sent from the station level or form the remote control centre down to the bay level where the signal is processed and a reply is sent back to the level where the command has been issued. With the second step the execution command the control output of the IED is activated and the switching task started. This increases the security to operate an object as it is not possible accidentally to operate an object with only one bit change.

Command supervision
Command outputs are safety critical, because an unintended operation of a switch may cause physical damage or endanger human beings, which happen to be nearby the switch during operation. To minimize the risk two separate output channels that are connected in series must be used to supply the operating coil current. These channels are often called the Select channel, which selects the switch, and the Execute channel, which switches the load current. Both contacts have to be supervised, so that a relay (contact) failure is detected before any second failure may happen. An often-used solution is reading back the state of a second contact, which is mechanically coupled to the operating contact.
Usually, a contact has to separate each side of the operating coil, so that in normal state the coil is completely isolated. This assures that even a short circuit cannot lead to unintended switching.

Interruption of drive latching in case of runtime exceeding
The command output is usually latches until the switching object reaches his end position. In case the runtime exceeds the defined maximum time (meaning the switching object didn’t reach its end position) the command output contact shall be interrupted for safety reasons.

Breaker position indication per phase
A switch position is normally indicated by two contacts: one is closed if the switch is closed, and a second one is closed if the switch is open. This double indication shows a moving switch in the so-called intermediate position if both contacts are open. For disconnectors and earthing switches it is physically impossible that both contacts are closed at the same time in normal operation, so this must be regarded as an error. The same is true for the intermediate position, if it lasts longer than the switch movement time (often called running time). For circuit breakers in high voltage switchyards often each of the three phases has its own drive. It may then happen that one phase is in a different state than the others. If the contacts of the phases are connected in parallel (logic OR) to get one double indication again, then the 1-1 state may happen, and may be cleared e.g. by an open command. If however this state lasts too long or can not be cleared, then again this is a serious error (pole discrepancy).

Pole discrepancy monitoring and trip function
The pole discrepancy function detects a discrepancy in the pole positions of a circuit-breaker. If at least one phase shows a closed and one phase an open position, a three-phase trip command is issued after a selectable time delay.

Hydraulic pump control and runtime supervision
In order to prevent damage on the pump system, the runtime is supervised. In addition the number of pump starts (e.g. 10 within 24 h) without CB operation leads to a blocked hydraulic system. A blocked pump system can be reset from the BCM after inspection.

Pump-start cascading
Too many simultaneous pump starts, such as e.g. in a busbar protection trip, may put too much load on the station DC batteries. Therefore only one pump is able to start at a time.

Anti pumping
In order to prevent damage on the pump system, the runtime is supervised. In addition the number of pump starts (e.g. 10 within 24 h) without CB operation leads to a blocked hydraulic system. A blocked pump system can be reset from the BCM after inspection.

Operating pressure supervision
The circuit- breaker can only operate if there is adequate SF6 gas pressure and the spring is charged. Should the SF6 gas pressure be too low, both closing and the two tripping circuits are interrupted by independent blocking contacts.
For operational safety reasons the pressure of the pump system blocks the operation on three different levels. If the pressure falls below the O-C-O level, a possible autoreclosure scheme is blocked. Below the C-O level the close operation is blocked in addition, and below the O-level the circuit-breaker trip commands are also blocked.

Voltage regulators
For transformer regulation modern transformer voltage regulator are typically used. It contains tap-changer indication, fully programmable digital and analogue in- and outputs, programmable measuring values, parallel operation and an interface to easily integrate it in the substation automation system.

Interlocking and blocking

Interlocking facilities have to be installed in switchgear to prevent damages and accidents in case of false operation. Interlocking systems shall be provided via hardwire or via station bus for the station interlocking, within the bay itself software interlocking controlled via the control IED is being used.
An override function shall be provided, which can be enabled to by-pass the interlocking function via a key/password, in cases of maintenance or emergency situation.

Station interlocking
To realize the station interlocking two solutions are possible either by a hardwired bus or via station bus. It shall be a simple layout, easy to test and simple to handle when upgrading the station with future bays.
In case of a solution with station bus the tender describes the scenario while an IED of another bay is switched off or defective.

Double operation interlocking
Double operation interlocking prevents from operating two or more switches at the same time. The double operation interlocking is station interlocking that is usually provided via the station bus using an integrated 1 out of n check (software). It considers typically all the switches in the station.

Synchrocheck

The synchronism and energizing check functions shall be distributed to the control and/or protection devices and have these features:

- Adjustable voltage, phase angle, and frequency difference/frequency rate.
- Energizing for dead line - live bus, or live line - dead bus.
- Settings for manual close command and auto-reclose command shall be adaptable to the operating times of the specific switchgear.
- Independent/dedicated synchrocheck relays may be used for manual close command and auto-reclose command

Voltage selection
The voltages, which are relevant for the synchro-check functions, depend on the station topology i.e. on the positions of the circuit breakers and/or the isolators. The correct voltage for the synchronizing and energizing is derived from the auxiliary switches of the circuit breakers, isolator, and earthing switch and shall be selected automatically by the control and protection IED.

Transformer tap control / AVR
Voltage regulation for single transformers or parallel transformers with on-load tap-changer shall either be included in the numerical control unit for the power transformer or located in a separate tap-changer control device which is associated with the power transformer. In the event that a separate tap-changer control device is selected, this shall be an integral part of

the SA system like any bay-oriented control or protection IED. Typical facilities to be provided are:

- Selection of individual groups of transformers to be selected/deselected fro automatic control
- Maintain busbar voltage on the low voltage side of the transformer by a reference value
- Line drop and reactive compensation
- Parallel control

Automatic switching sequences

The automatic sequence control program allows the operator to execute predefined sequences of commands. The operator can activate the switching sequence by giving a single command only. The sequence control function performs a series of single-control commands step-by-step. Each command is supervised and checked by the usual interlocking functions implemented in the associated bay controller, i.e. the blocking criteria, synchrocheck, interlocking logic, etc. Thus, the procedure is identical to manual single step commands and therefore ensures the same degree of secure operation. These switching sequences can also be initiated by remote control. Typical predefined switching sequences are:

- connecting a line or transformer feeder to a specific busbar
- disconnecting a line or transformer feeder from a specific busbar
- busbar changeover.

The available automatic sequences should be described, e.g. sequences related to the transfer bus, changes from bus 1 to bus 2. The automatic sequence can be initiated by the operator.

Dynamic Busbar Coloring

Busbar transfer for a specific feeder. Dynamic busbar coloring gives the operator a quick overview of the state of the substation and shows at a glance whether any specific part of the substation e.g. busbar segment is earthed, energized, or de-energized. This function helps preventing incorrect switching; especially in emergency situations when often time is of the essence. In complex industrial networks the operator has to have a clear precise and fast system overview, infeed sources and consumers e.g. from the utility grid or from the internal generator. Thanks to a better overview the operator is able to respond quicker to any contingency.

Load shedding / Power restoration

There are basically two load-shedding modes:

- Under voltage activated load shedding: this is a response to a decline in voltage on a transmission line and is station oriented.
- Under frequency activated load shedding: this is a response to an out-of-step situation between network sections and is transmission system oriented.

Load shedding tables are predefined in order to set the priority that is allocated to each individual feeder. In addition, the actual load conditions of the feeders are taken into account to determine the optimum load to be switched off. This load shedding approach adapts to the actual situation and ensures that only the minimum numbers of feeders are tripped in order to keep the network in a stable state.
After recovery of the voltage or frequency, a sequential restoration of the power supply can then be made based on the information on the tripped feeders and their priority levels.

If load shedding is required, the criteria for the shedding and the criteria for the choice of the feeders to be shed should be described.
The choice of feeders to be shed shall be shown at station level and shall be modified remotely.
The load shedding functionality shall be realized by combining frequency functions at bay level and priority settings downloaded from the station level to the bay.

4.1.1.4 Protection functions

The protection functions are not described in detail. The basis for an optimal integrated solution is that the protection functions are realized using numerical devices with communication capability. The main requirement of the substation automation system is that it shall be capable to retrieve all information for operation and maintenance from the numerical devices. Typical components to be protected in a substation are:

- lines/cables
- transformers
- busbars
- capacitor banks
- battery circuits
- tripping circuits
- breaker
- reactors

The requirements for the protection functions have to be detailed in the specification if they form part of the SAS tender.

4.1.2. Performance requirements

Concerning performance of a substation automation system two typical performance indices can be measured:

- Message performance
- System performance

The IEC61850 standard gives a good basis for the performance requirements independent of the applied communication protocol as such. The two performance groups are briefly summarized in the following two chapters.

4.1.2.1 Message performance

The definition of the transfer time is explained in figure 4.1.-2. The given performance times are referring to the total transfer time **t** that includes the IEDs internal processing time (ta and tc) as well as the transmission time used over the communication network (tb).

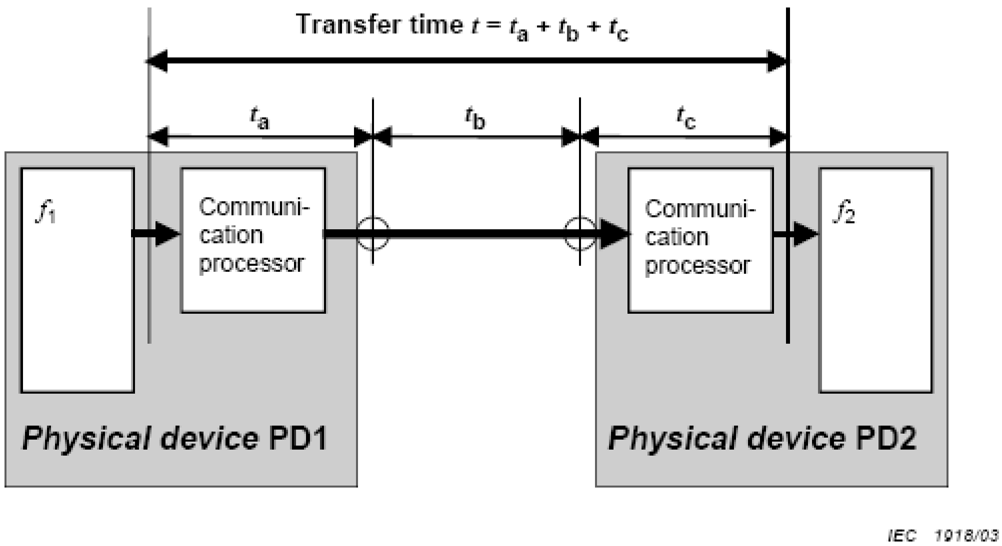

Figure 4.1-2 Definition of message transfer time

Source of picture: IEC61850

Different requirements concerning performance for messages apply depending on the application. Referring to the IEC61850 standard part 5 one can distinguish two typical applications with its different performance classes:

Control and protection
Defining three performance classes for distribution with low requirements (P1), transmission bay (P2) and transmission bay with top performance requirements (P3).

Metering and power quality
Defining also three performance classes where the first one refers to revenue metering with accuracy class 0.5 (M1), second one to revenue metering with accuracy class 0.2 (M2) and the third one to quality metering with up to 40^{th} harmonic (M3).

Message types
Each message type has for each application (performance class) a defined maximum value. The following message types are defined for an SA system:

- Type 1 – Fast message (e.g. GOOSE)
- Type 1A – Trip (e.g. GOOSE)
- Type 1B – Others (e.g. GOOSE)
- Type 2 – Medium speed messages
- Type 3 – Low speed messages (e.g. Reports)
- Type 4 – Raw data messages
- Type 5 – File transfer functions
- Type 7 – Command message with access control

	Performance Class (referring to total transfer time t)						
	No class Applicable	**P1**	**P2**	**P3**	**M1**	**M2**	**M3**
Type 1A	N/A	10ms	3ms	3ms	N/A	N/A	N/A
Type 1B	N/A	100ms	20ms	20ms	N/A	N/A	N/A
Type 2	100ms	N/A	N/A	N/A	N/A	N/A	N/A
Type 3	500ms	N/A	N/A	N/A	N/A	N/A	N/A
Type 4	N/A	10ms	3ms	3ms	1500Hz	4000Hz	12000Hz
Type 5	>1000ms	N/A	N/A	N/A	N/A	N/A	N/A
Type 7	500ms	N/A	N/A	N/A	N/A	N/A	N/A

Table 4-1 IEC61850 Message types / performance overview

Not all message types and performance classes may apply to a specified SA System. Today's solutions based on a station bus and hardwired connection to the process level won't need type 4 messages.

4.1.2.2 System performance

It is expected that a SA System during its life time will have to face different situations concerning the number of events appearing in the substation and the resulting load on the SAS communication network.

In most cases studied, the abnormal or emergency loads on the substation bus will add between 50 % and 100 % to the normal load.

During the normal load situation only occasional alarms and events are occurring at the substation with analogue reporting as load demand changes.

The most important issue when planning the substation communication, are a proper assignment of freely allocatable logical nodes to physical devices and the arrangement of the communication network itself to minimize point-to-point communication requirements.

Combining data objects into object oriented or multi-command messages in a suitable way can result in a noticeable reduction of the total traffic. This will be clearly shown when LAN simulation studies are performed.

When defining the actual network and stacks, it is equally important to combine data objects in such a way that the traffic is minimized.

The main result of the calculations and studies should be to ensure that the requirements on transmission times can be kept for various message types. A LAN simulation program can verify this.

To ensure that the system can handle properly the different situations and to guarantee also the full operation of the system during these critical situations the following parameters shall be measured for the different load situations:

- Exchange of display (first reaction)
- Presentation of a binary change in the process display
- Presentation of an analog change in the process display
- From order to process output
- From order to updating the display

Typical values measured at the station HMI level are listed in the following table:

Function	**Typical values**
Exchange of display (first reaction)	< 1.5 s
Presentation of a binary change in the process display	< 1 s
Presentation of an analog change in the process display	< 1.5 s
From order to process output	< 1 s
From order to updating the display	< 2 s

Table 4-2 Typical performance measures at station HMI level

4.1.3. Environment (thermal mechanical, insulation) & EMC requirements

4.1.3.1 General statements

This chapter details the climatic, mechanical, and electrical influences that apply to:

- Bay level IEDs
- Station level IEDs
- Communications media and interfaces

All these equipments are used for monitoring and control of processes within the substation. The environmental requirements cover the following areas:

- Temperature
- Humidity
- Barometric pressure
- Mechanical and seismic
- Pollution and corrosion
- EMI immunity
- EMI radiation

4.1.3.1.1 Industrial offer

The SAS manufacturers offer different equipment for building a complete SA System. Equipment based on "off the shelf" hardware platforms from the standard industrial range as well as specific substation hardened equipment is found for the different devices and functions.

Concerning bay level functions (protection functions, bay control functions, bay level automatisms, …) the technology and functions performed by those IEDs are typically based on specially designed hardware to fit the harsh substation environmental conditions.

To implement station level functions (communication functions, local control functions, remote control functions, supervision functions…) two types of hardware are used:

- Standard off the shelf PC devices, workstations or communication nodes (hubs, routers, gateways …)
- Industrial hardware hardened for substation similar as the hardware for bay level IEDs for most critical functions (Gateway, Ethernet Switches for station LAN, …)

No dedicated EMC tests are necessary for "off the shelf" products provided they do not interfere with process. It is however recommended to request from manufacturers their standard EMC test results and the product industrial references.

Some utilities may have particular requirements for the EMC characteristics of the SAS components.

4.1.3.1.2 Normalization

At the same times standardization committees have strengthened the normalization efforts concerning material type tests. As a result, a large amount of tests are now covered by IEC or European norms. For instance the norm IEC 61000-6-5 was published in July 2001. It is now a recognized and approved standard for manufacturers as well as utilities.

IEC 61850 give very few elements on relevant EMC / environment standards and associated severity levels (this norm rather focuses on configuration and communication - digital protocols - standards)

4.1.3.1.3 Utilities strategies

In a lot of utilities budgetary constraints and institutional evolutions have reduced to a large extent qualification and type tests performed internally. EMC, mechanical and insulation tests were time consuming, required dedicated, expensive expertise and materials.

Technological evolutions required a full re-examination and reengineering of these test requirements which were adapted to conventional technologies (electromechanical or static devices, wires…) but less adapted to digital equipments.

- Some test are not required any more (such as long time tests)
- Alternatively new tests are required (such as ELC emissive levels)

Very few material qualification tests remain specific to a utility (compatibility with specific high voltage equipment, power supply specific requirements)

4.1.3.2 Relevant standards

The following table takes into account these various statements to propose a selection of relevant standards coherent with the industrial, normative state of the art:

Reference	Title
Electromagnetic compatibility (EMC)	
IEC 61000-6-5 (2001-07)	Electromagnetic compatibility (EMC) - Part 6: Generic standards - Section 5: Immunity for power plants and substation environments
IEC 61000-6-1 (1997-07)	Electromagnetic compatibility (EMC) - Part 6: Generic standards - Section 1: Immunity for residential, commercial and light-industrial environments
IEC 61000-6-2 (1999-01)	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
IEC 61000-6-3	Electromagnetic compatibility (EMC) - Part 6: Generic standards – Section 3: Emission standard for residential, commercial and light-industrial environments
IEC 61000-6-4	Electromagnetic compatibility (EMC) - Part 6: Generic standards - Section 4: Emission standard for industrial environments
IEC 61000-4-2 (2001-04)	Electromagnetic compatibility (EMC)- Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test
I EC 61000-4-3 (2002-09)	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
I EC 61000-4-4 (1995-01)	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 4: Electrical fast transient/burst immunity test.
IEC 61000-4-5 (2001-04)	Electromagnetic compatibility (EMC)- Part 4-5: Testing and measurement techniques – Surge immunity test
IEC 61000-4-6 (2001-04)	Electromagnetic compatibility (EMC)- Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields
IEC 61000-4-8 (2001-03)	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test
IEC 61000-4-11 (2001-03)	Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests
IEC 61000-4-12 (2001-04)	Electromagnetic compatibility (EMC) - Part 4-12: Testing and measurement techniques – Oscillatory waves immunity test
IEC 61000-4-17 (2002-07)	Electromagnetic compatibility (EMC) - Part 4-17: Testing and measurement techniques - Ripple on d.c. input power port immunity test
IEC 61000-4-29 (2000-08)	Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests
EN 50263 (2000)	Industrial environment

Environmental testing	
IEC 60068-2-1 (1990-05)	Environmental testing - Part 2: Tests. Tests A: Cold
IEC 60068-2-2 (1974-01)	Environmental testing - Part 2: Tests. Tests B: Dry heat
IEC 60068-2-14 (1984-01)	Environmental testing - Part 2: Tests. Test N: Change of temperature
IEC 60068-2-30 (1980-01)	Environmental testing - Part 2: Tests. Test Db and guidance: Damp heat, cyclic (12 +12-hour cycle)
IEC 60068-2-78 (2001)	Damp heat
Instrument transformers	
IEC 60044-1 (2003-02)	Instrument transformers - Part 1: Current transformers
IEC 60044-2 (2003-02)	Instrument transformers - Part 2 : Inductive voltage transformers
IEC 60044-3 (2002-12)	Instrument transformers - Part 3: Combined transformers
Electrical Relays	
IEC 60255-5 (2000-12)	Electrical Relays - Part 5: Insulation coordination for measuring relays and protection equipment - Requirements and tests
IEC 60255-6 (1988)	Electrical Relays - Part 6: Temperature range
IEC 60255-21-1 (1988-09)	Electrical relays - Part 21: Vibration, shock, bump and seismic tests on measuring relays and protection equipment – Section One: Vibration tests (sinusoidal)
IEC 60255-21-3 (1993-09)	Electrical relays - Part 21: Vibration, shock, bump and seismic tests on measuring relays and protection equipment – Section 3: Seismic tests
IEC 60255-22-1 (1988)	1 MHz burst disturbance tests
IEC 60255-23 (1994-10)	Electrical relays - Part 23: Contact performance
Functional safety	
IEC 61508-1 Corr.1 (1999-05)	Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 1: General requirements
IEC 60529 (2001-02)	Degrees of protection provided by enclosures (IP Code)
EN 55022 (2001)	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
EN 55024	Limits and methods of measurement of immunity characteristics of information technology equipment
EN 50 102	Degrees of protection provided by enclosures against external mechanical impact (IK Code)

Table 4-3 Relevant standards concerning environment and EMC

4.1.3.3 Severity levels

The severity levels for various SAS components shall be considered separately, taking into account

- their criticality for the power system
- their location in the substation (bay level or station level)
- The type of integration interfaces

Additional remarks

- Special attention to Cabling quality, not specified in norms
- Special arrangements may be necessary for substation level PCs and network components not fulfilling the required EMC levels, concerning cabling, interposing relays, physical disposal (filtered and close AC power supply units, to reduce disturbances...)

It is recommended to specify and evaluate EMC / environment levels for each type of equipment individually. Dedicated tests to a full bay set of equipments i.e. integrated and wired in a bay cubicle are not recommended:

- because of their complexity,
- because of the big number of configurations to take into account (feeder bay, transformer bay...)
- because individual tests EMC performed on each separate device take into account the cubicle integration related aspects (for example, Electrostatic discharge immunity tests are executed with air, contact and neighborhood)
- some EMC tests are not relevant for cubicles (example : high frequency emission)

Alternatively visual inspections are a convenient and efficient way to check the conformity and quality of equipment integration in cubicles:

- Segregation of communication circuits from disturbed power circuits or CT/VT links
- Earth cabling principles
- Cable physical arrangement

4.1.4. Reliability requirements

Reliability is the probability of a device performing its purpose adequately for the period of time intended under the operating conditions encountered. The reliability assessment of a substation automation system means obtaining failure characteristics of a system. These characteristics are normally frequency and duration of unavailability of a device or a function, or malfunction.

Reliability can only be objectively assessed by quantifying the behavior of the individual items of equipment. The associated reliability data can then be used to predict likely future performance. As importantly, it can be used to judge the merits and benefits, technical and economic, of alternative design strategies and decisions.

Predictive analysis is the core of reliability planning. It must produce an estimate to

- the future performance of the substation automation system
- the benefits of alternative designs, refurbishments and expansion plans
- the effects of alternative operational and maintenance policies
- the related reliability cost/benefit/worth of the alternatives with two previous items

The techniques used in reliability evaluation can be divided into two basic categories: analytical and simulation methods. In addition, qualitative or methods contingency-based methods are used.

Faults are incidental events and thus reliability is mainly based on calculations of probability and statistical mathematics. Probabilistic design methodology provides a way to objectively quantify the relative value of different design arrangements and operational practices. Also, the probabilistic approach makes it possible to understand the sensitivity of the design to system variables, thereby giving the system operator knowledge about where system reinforcements are required to improve performance.

Usually only the manufacturer and perhaps the larger utilities have the possibility to use predictive, probabilistic methods that directly address reliability.

Quantitative or numerical requirements (MTTB, MTTR, etc.) specify only the probability of an incident or durance of a faulty mode operation situation. The allowed consequences in secondary system faults and maintenance situations must additionally be specified. This approach establishes a link between power system dependability targets, and substation automation system design.

It is a task for the customer to specify, as a part of a functional specification, also the functional dependability and failure tolerance requirements.

In customer specification the qualitative functional specification is perhaps more important than the numerical requirements. The manufacturer should execute reliability analysis and calculation of the chosen solution, deliver appropriate documents and must be prepared to verify results with tests.

The following chapters deal with dependability requirement and to a larger extent “RAMS” requirements (Reliability, Availability, Maintainability, Security) in order to make a proper specification and evaluation as required by utilities and to establish an optimized and conforming design concerning manufacturers. The following recommendations shall be applied:

- Choose a convenient **basis of reliability data and calculation**: It shall be non ambiguous and homogeneous (in order to be able to establish comparisons) and clarified with the necessary details (to assess the answers given in tenders).

- Choose a convenient **methodology** taking into account quantitative and qualitative issues: In particular the nature and criticality level of functions to be performed shall be considered to assess reliability values (risks of overestimating the necessary reliability level with negative impact on cost) and faulty modes behavior shall not be omitted

- Choose a **pragmatic approach**: Benefit from “proven in use” design and practices, COTS (components off the shelf) and de facto standards, achievable and testable criteria for both manufacturer and user.

IEC 61508 norm provides recommendations on functional safety, but rather methodological and is not made for a specific application area.

4.1.4.1 Method choices

The following two main tasks have to be worked out by the utility:

- Identification of “unwanted events” or failures with associated gravity or “criticality” levels. Note the classification depends on the policies of the utility.

  Example of failures with high gravity levels: unwanted circuit breaker tripping, delayed busbar fault clearing,...

  Example of failures with less major gravity levels: remote control unavailability, local control unavailability, disturbance recording failure,...

- The assessment of qualitative value associated with these events (functional MTBF) may take into account existing levels of performance with conventional substation systems, provided the utility is able to gather statistical data on the existing protection scheme.

  This phase is necessary to establish links between power system dependability targets, and system design.

At this stage it is necessary to provide all necessary data in coherence with the chosen unwanted events, necessary for the manufacturer (Circuit Breaker failure rates if the unwanted event takes into account the failure of High voltage equipment, power system fault statistics if the unwanted event objective are defined according to a probabilistic approach or based on discrete solicitation hypothesis).

4.1.4.1.1 Requirements concerning Fault tolerance

This point deals with qualitative behavior of the system once a failure in the system occurs the system shall:

- behave in a secure way
- minimize the consequences of the failure
- give indications on the nature and location of the failure to enhance repair time

Key requirements are:

- **Single failure criteria**: The substation shall continue to be operable according to the single failure criteria: If any component fails, there should be no single point of failure that will cause the substation to be inoperable.
- **Advanced self supervision capabilities**: using self diagnostics, most digital IEDs are able to detect internal failures and alert maintenance personnel using alarms. They typically cover the major parts of system hardware.

Example of usual self diagnostics :

Data acquisition system testing	Power supply and ground are connected to the analog input channels of a multiplexer and checked against warning and failure thresholds. The analog acquisition chain is checked: multiplexer, programmable gain amplifiers, ADC converter. The ADC conversion time is checked.
Memory testing	The memories (typically flash ROM) contents are checked
Set point testing	Set points are stored in two different memories (typically EPROM's and RAM). Whenever any set point is changed, the checksum of the set points is calculated from one of the memory (EEPROM) and compared with the one calculated from the RAM.
Watchdog timer	The IED hardware design includes a watchdog timer reset circuit to take the processor through an orderly reset should the program get lost due to a hardware or software glitch

Table 4-4 Self diagnostic tasks

Reliability assessment requires a theoretical approach and the use of mathematical tools. All these methods demonstrate their efficiency to orientate and check design, but quickly reach their limits with large, complex systems, and are poorly describing the dynamic behavior and the sequential aspect of events. Furthermore, people responsible for reliability issues are more familiar with high level management and economic factors than with advanced mathematic probability. The confidence level in digital systems has significantly risen over the past decade and most offered solutions are beyond the specified level. So the major concern of the decision taking staff is not on achieving the specified levels but rather not to put requirements into the specification that are beyond necessary dependability levels.

Therefore requirements shall not omit

- more qualitative criteria (maintenance facilities, faulty mode behavior, rigorous development and design methodology, exhaustive FAT processes) ,
- the use of proven in-use practices and products as much as possible,

Last but not least every dependability requirement introduced in the specification shall be easily checked and assessed , in technical as well as in contractual terms : to achieve this :

- audits
- total visibility on the manufacturers calculation and data
- operational statistics on the system once in operation (failure rates) potentially leading to retroactive corrective actions or contractual penalties

4.1.4.1.2 Hardware and software reliability

In addition to functional dependability considerations it is convenient to address more specifically software and hardware reliability issues

Intrinsic hardware reliability shall be in conformance with the specified quantitative functional reliability requirements and calculations and shall not deteriorate with time. Special attention shall be devoted to the following items because of the potential criticality of these components, and their number:

- Power supply units (a specific requirement is included in IEC 61850–3 concerning power supply)
- CPU
- Bay level controllers

A distinction is established between:

- Bay level hardware (industrial real time PLCs, protections...) : lower failure rates requested, major risks
- Station level hardware (Ethernet, industrial PC, standard hubs...) : higher failure rates, less major risks

Software, including data configuration, is a key element to assess SAS dependability level. However, methodologies and well established standards are not mature; software is not yet in its industrial phase. Therefore it is recommended to rely on:

- Quality assurance and quality system management e.g. ISO 9000, covering sub contractors at all design and project phases
- Preferential choice of proven in-use software components (avoid as much as possible specific development)
- Exhaustive FAT testing strategy to fix bugs

The IEC 61508 norm provide recommendations on SIL (safety integrity level) safety levels for software but this norm is not yet applied by industrial SAS manufacturers. Nevertheless consistent with IEC 61508 most electrical protection IED’s in a substation automation system could be assigned to safety integrity level 3 / 4, most SCADA/HMI’s to safety integrity level 2 and depending on its purpose, most SAS communications networks could be assigned to safety integrity level 2. Fast message type applications would require safety integrity level 3 / 4 be assigned to the SAS communications network.

4.1.4.2 Pragmatic approach

The main target for a network operator is continuous power supply to the customers. It is not allowed that faults in secondary systems, in any reasonable circumstances, are causing interruptions in power supply. Thus, within a substation automation system, there must not occur any such failure or maintenance event, such that the secure operation of the substation should become endangered.

The customer can describe reliability requirements qualitatively (fault tolerance) or use contingency based methods which are on the single failure criteria: design the system so that it can do without any major element and the system can still do its job even if any one unit fails. These methods are often referred to as “N-1” methods. So designed, a system would tolerate failures. The likelihood of two units failing simultaneously is usually remote enough so as to not be a consideration.

One could also take a semi-risk-based approach. Such approaches make a distinction between probable (likely) and extreme (unlikely) faults and are based on the assumption that the rarer an event is the more severe the consequences.

Requirements for fault tolerance should be presented also during maintenance or expansion situations.

Requirements for managing and preventing faults in SAS systems are also a crucial part of reliability engineering.

Functional specification may lead to very different architectures and thus different constructive solutions by different manufacturers. Although it is not recommended to specify any architecture, it is difficult for the customer to compare different vendor solutions without any reference architecture. It could be recommended that vendors present several solutions to help the customer to better understand the differences between different architectures.

4.2 Information management

4.2.1. Introduction

Besides the basic requirement for mainly operational purpose, the use of modern solutions for substation automation opens the door also for further enhanced interfaces to support other areas in the organization. It provides data to remote users as Protection engineers, Operational and Maintenance centers, Planning and Asset Management centers. This chapter shall give an overview of what applications may be requested by customers when preparing the specification.

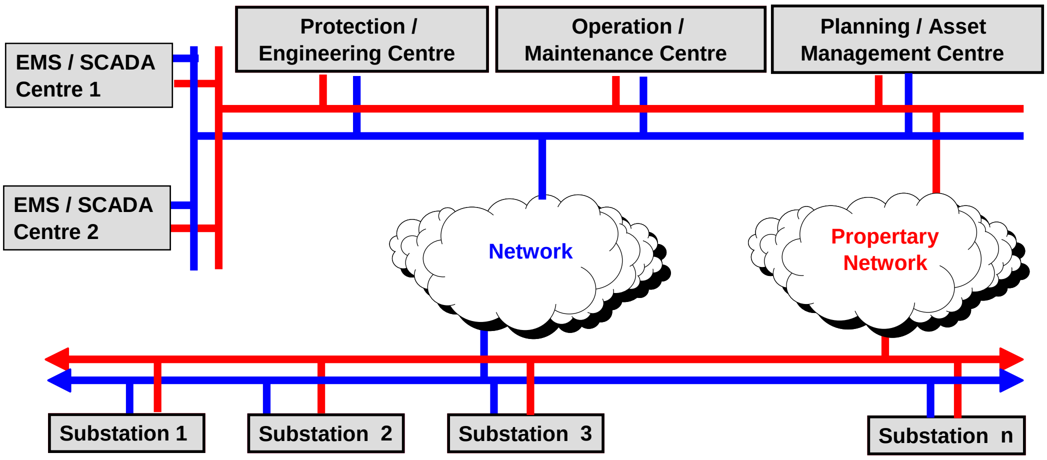

Figure 4.2-1 Information Management – Communication Networks

The use of an extensive information management can provide the following additional benefits.

- Improve components efficiency and reliability through advanced maintenance strategy in a way to reduce O&M costs
- Obtain best performance of existing devices
- Permit to know really “life cycle” of components and optimize upgrading / substitutions
- helps system planning
- performs risk analysis
- gives decision support (load shedding, system restoration, etc.)
- permits fault location
- failure cause analysis
- functional reliability
- predictive maintenance
- equipment life history
- wide area protection
- performs automatic load shedding
- maintain safe and reliable equipment operation
- Operate assets at maximum performance for current conditions
- Extend maintenance intervals without decreasing system reliability
- Defer the cost of replacement or upgraded equipment

In practice the information management is divided into two logical subsystems: The monitoring system and the asset management system.

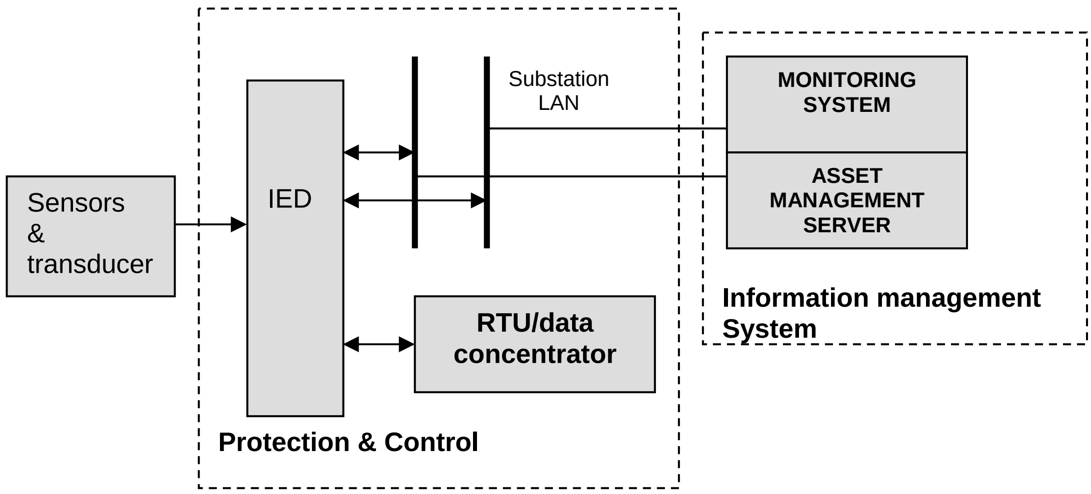

Figure 4.2-2 Data integration for IMS (Information Management System)

The main tasks of the monitoring system are:

- data acquisition from primary and secondary systems
- storage in substation database
- event recorder (main concentrator + bay units) -> depending on technical requirements, can be integrated into protection devices
- fault locator (main concentrator + bay units) -> depending on technical requirements, can be integrated into protection devices
- oscillograph -> depending on technical requirements, can be integrated into protection devices
- basic alarm functions (threshold or rate violation)

Whereas the asset management system focuses on the following functions:

- diagnostic data elaboration and grouping / correlation in way to know components real time status
- intelligent alarms managing
- statistical elaborations and decision supporting
- interface with other remote / local system like HIS, maintenance archives, SCADA, other
- life management and component history

An important evaluation key is the degree of interoperability and integration between single devices in a way to minimize the presence of “single communication islands” in the system.

4.2.2. Information target groups

There are several target groups for the information that substation automation can provide. Main target groups are network operation, protection system engineering, maintenance (primary and secondary circuits), network planning and asset management. Serial communication from bay level to substation level and from substation level to network level is the way for all information.

Operators

- Continuous need of process data (alarm, state, measurement, control), usually no need for mass-data

Protection engineers

- Not time critical need for protection relay and disturbance record data: relay event lists and comtrade format files

Maintenance

- Not necessarily so time critical need for primary component condition monitoring data, can be mass-form data

Network planning

- Need for loading level (currents, voltages) information of network, not time critical, usually yearly max load values needed

4.2.2.1 Operation

Substation automation system works as a remote terminal unit for remote network operating system. At the substation level it can also be a local substation operating system. At the bay level bay units can provide bay level operations and local operational info.

Operational information is usually needed at once, so it is time critical. For operation there are several information groups needed: tele-control commands for switching devices, state information of switching devices, measurement information, alarms from primary systems and from protection and other secondary devices (including metering and communication). Tele-control commands and state information are most important for operational use. Also alarms are important, but there shouldn't be too many alarms transferred to remote operators. It is reasonable to do remote alarm grouping at the substation level or latest at remote control level. Measurement information has a little bit lower importance level when we think about speed and accuracy. In case of remote system or telecommunication faults there should also be a spare system or way to move some basic information (for example some group alarms and basic measurements) to remote control centre.

Operators need also some basic primary fault information, for example type of fault and location of fault. Part of voltage power quality information is also necessary for operators (voltage levels etc).

4.2.2.2 Protection system engineering

Protection engineers need information concerning the operation of the protection. They need relay event lists, indication lists and disturbance records to ensure that the protection operated correctly. The most important thing is to find out what happened if the protection didn't work properly. Also disturbance records give exact information of the type and magnitude of the primary fault. This kind of protection information can be very accurate information and the disturbance record files can be quite big, at least medium sized. Analyzing protection information is not necessarily so time critical. Protection engineers study the disturbance information usually one or several days or weeks afterwards.

This accurate protection relay information should not go to the remote operation system because of the large amount of specified data. The data comes automatically or manually from relays via the substation bus or via separate maintenance channel to substation automation system. Another chance is that the disturbance data is collected directly from relays via the maintenance channel. This data can be collected directly from SA-system or from relays by protection engineers. Substation automation system can include a temporary storage for protection data. Disturbance data remote collection can be fully automated or partly manual.

4.2.2.3 Maintenance

Primary and secondary system maintenance personnel use also the data that operation system or operation personnel give to them. Alarm indications from faulty or almost faulty primary and secondary devices give input for maintenance personnel to start repair actions.

More accurate maintenance information from primary and secondary devices is also collected and will be collected more and more in the future. Condition monitoring (self supervision) of new secondary devices (including relays, secondary circuits, metering, and communication) is already widespread standard. Condition monitoring of primary devices will increase during future years and decades. This maintenance and condition monitoring information of still healthy devices is required to determine the maintenance need of the device in the future. Part of this information can go straight to the network operation system but most of it should go to separate condition monitoring systems used by maintenance personnel. Substation automation system can include a temporary storage for maintenance data. Maintenance data remote collection can be fully automated or partly manual.

4.2.2.4 Network planning

The network planning department needs power flow information (loading levels and voltage levels) and also power quality information. Loading levels of feeders and main transformers are most important for network strengthening investment calculations. Also operational reserve calculations need loading level information. Power quality information (voltage levels, voltage sags and swells, harmonic distortion, interruption statistics…) can also be useful when planning network strengthening in the medium voltage level. Basic network loading information (current, voltage, power) is always transferred to network remote control system. This can be a satisfactory way to collect information for the database useful for network planning. Some of power quality measurements contain so much data, that separate channel from SA-system or from power quality devices to power quality analyzing system should be built.

4.2.3. Monitoring

4.2.3.1 Primary equipment monitoring

A list of equipment that may be considered as part of the primary equipment to be monitored is shown below:

- Transformers
- Load Tap Changers (LTCs)
- Special transformers and compensators (PSTs, SVC, STATCOMs)
- Bushings
- Capacitors banks
- CTs, VTs
- Circuit-breakers
- Disconnectors
- GIS
- Auxiliary services
- Cables

At the substation level, condition based maintenance (CBM) is becoming feasible with new technology. CBM is a wide encompassing term which implies that maintenance, in terms of repairs or replacement is done based on the condition of the component. The term is defined as: An equipment maintenance strategy based on measuring the condition of equipment in order to assess whether it will fail during some future period, and then taking appropriate action to avoid the consequences of that failure.

From the above definition we understand that information needs to be stored about the condition of the equipment and that this information needs to be accessible for future analysis. Additionally it could be stated that the full potential of condition and maintenance information cannot always be realized by using traditional techniques of data handling and analysis. There are often underlying trends or features of the data that are not evident from the usual analysis techniques. Such detail and trends can be important for the assessment of the equipment operation and there are increasing demands from operators and asset managers to fully exploit the capabilities of this data in order to optimize the utilization of high voltage electrical plant.

To keep complete records of the condition of high voltage cables, an information system needs to consider three types of data. First, equipment data such as the identity and location of the component and related information. Second: Activity data needs to be stored on the measurements done, when they where done and which methods were used. Third: Condition data such as the actual results of the measurements and the conclusions drawn on equipment status. Also a fourth category of data, could be defined, that is the Norms, which we here include in the equipment data.

Equipment data consists of static data about the component in question, its type, its location, where it is connected, when it was commissioned, the manufacturer, year of manufacture, technical specifications and so on. An information model must be able to store these data but also be able to represent relations between subcomponents and other components. In other words, the data model must allow run-time updates. In addition to the obvious necessary information such as manufacturer, year of commission, location etc. two groups of data are important. First thresholds and limits that the components have been designed for and are permissible operating conditions, second, data about how the component is connected to other segments of the network needs to be stored.

Activity data consist of information about inspections and measurements made. The data stored includes type of measurement, when it was done, who did it, which sensors were used and so on. Of course, the information model must allow the activities to be related to equipment and vice versa. In addition to obvious data such as time of measurement and the origin of the performance the activity data such as measurement and system type and method of calibration must be stored.

Condition data is the actual measurement results, both in terms of measured quantities, but also the resulting measured value(s) and any conclusions drawn. The condition data is related both to the equipment and to the Activity. Which measurement data that needs to be stored is based on which method is used for the diagnostic. For example for electric PD measurements using capacitive sensors the data is different than from dielectric response measurements at VLF combined with loss factor measurements.

A core component in the 61850 standard is the logical node, which represents a data and functionality, similar to an object in object oriented analysis. The logical nodes are implemented in the IEDs and represent parts of, or complete real world objects. These real world objects need not necessarily be power system components but can also be abstract entities such as measurements. A logical node may be implemented across several IEDs or be contained within one IED. In total the 61850 standard defines 98 logical nodes, organized in 13 groups.

The standard also contains a set of logical nodes related to diagnostics; however these are specialized for switchgear (3 logical nodes) and transformers (two logical nodes). These logical nodes do contain attributes such as for example the acoustic level of a partial discharge in a breaker. Very little information about for instance power cables can be represented by the attributes in the logical node. This is perhaps not surprising given the standards focus on substation equipment.

Activity data is not available in the 61850 logical nodes, which is unsurprising since such information is not suitable to store at the IED level.

The weakest point of the standard is the storage of measurement data. The standard provides a generic measurement object that contains some attributes related to measurements. However, none of these are specifically tailored for diagnostics measurements such as PD or DR. Very likely this is because many different methods exist and a standard that includes all necessary parameters will be too detailed.

Clearly the standards investigated do not have sufficient attributes included to store detailed information about diagnostic measurements. This is especially true for measurement data which, depending in measurement method can be very extensive.

The fact that a specific data point is included, or not, in a standard does not preclude vendors from providing that data in their system. As long as additional data is marked as additional to those specified in the standard and an interface is available to query it the data will be accessible and can be made available.

4.2.3.2 Secondary system

A list of equipment that may be considered as part of the secondary equipment to be monitored is shown below:

- protections
- control
- metering
- communication
- quality of service
- phase monitoring unit

This on-line self supervision data of the modern secondary devices and communication channels from substation to the Network Control Center (NCC) is vital for secondary asset managers. This information provides fast corrective actions before unwanted mal- or miss operations of the secondary devices. Without the self supervision the secondary asset manager is "in the darkness" between periodical maintenance actions.

Example of disturbance record file transfer
Protection engineers need to see if their protection devices have worked as planned. Modern numerical protection relays can produce comtrade-type disturbance recordings (*.cfg and *.dat files). These recordings can be viewed and analysed with analysing software made by any relay manufacturer. Disturbance record files can be read directly from relays via relay maintenance channel or from SA-system via maintenance channel. Direct reading from the relay is third possibility. Additionally internal event lists of the relays can be viewed by relay setting software. To read the internal relay event lists the relay setting software is usually necessary.

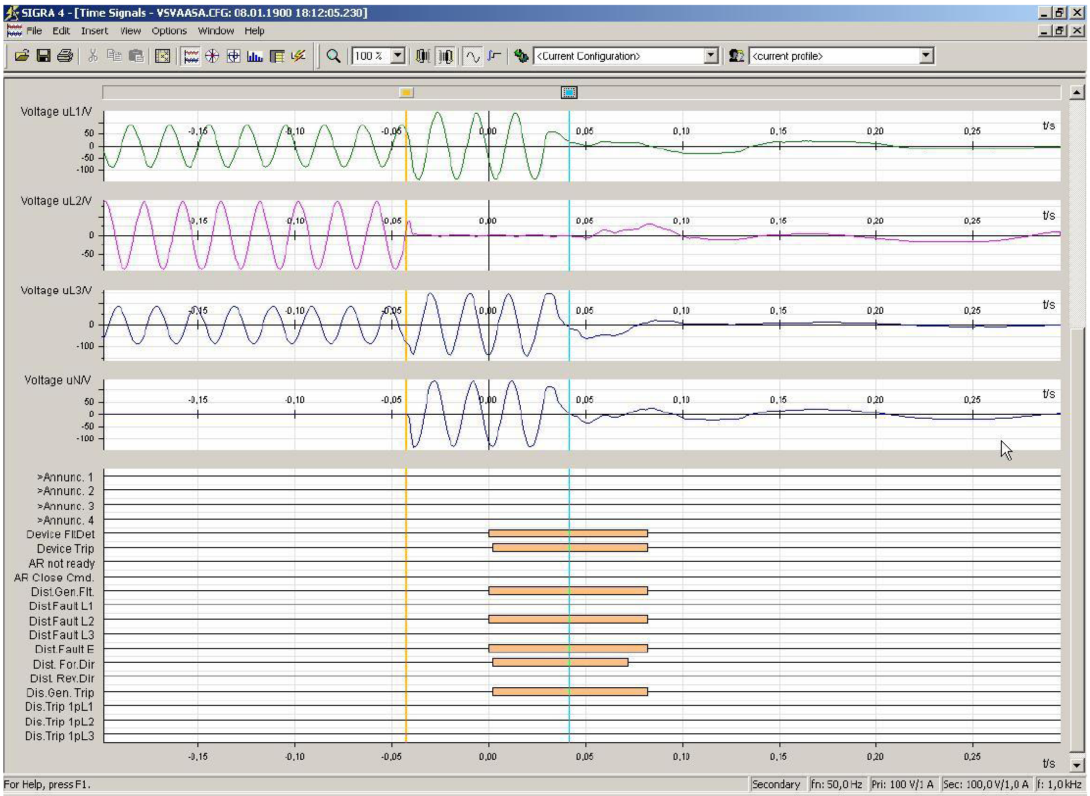

Figure 4.2-3 Disturbance record with measured voltages and internal signals of the relay

4.2.4. Maintenance strategies and support

4.2.4.1 Maintenance strategies

Concerning the maintenance strategy utilities have to make the decision which strategy or strategies are fitting most of their requirements. An overview of different strategies is listed below:

- Special maintenance
- Predictive maintenance
- Periodical maintenance
- Condition maintenance
- On fault maintenance

4.2.4.2 Actions

The actions related required upon the result of measures may have different priorities as:

- urgent (i.e. dielectric faults);
- not urgent, to do in short time (i.e. gas low pressure);
- not urgent, to do in long time (i.e. tank corrosion);

4.2.4.3 Expected benefits

The benefits provided when implementing a proper strategy for maintenance and supports are:

- Reduce inspection costs
- Reduce maintenance costs
- Reduce failure-related repair or replacement costs
- Enhance system reliability: fewer unplanned outages
- Provide better planning for scheduled outages
- Defer planned upgrade or replacement capital costs
- Reduce insurance premiums
- Retain knowledge of most skilled staff (expert system)
- Provide wide access to key knowledge.

4.2.5. Data for asset management

SA system is one information source for asset management data. Simple asset management system can also be called as network information system. The main goal with asset management is to maintain the network information data and to be aware of the value and condition of the owned network. Overall asset management of transmission and distribution network owner includes all the information areas mentioned previously in this chapter. So the data for asset management can come from other systems or the intelligent asset management system can be partly combined with a network maintenance system and/or network planning system. With intelligent asset management system network owners can get for example:

- decision support system for investments and maintenance strategies
- statistical analyses of network data
- component life and history management

Data base concept and management

- Object oriented databases and general structure
- Suggested standards (SQL, XML)
- Backup and redundant configurations
- Data exchanges
- Openness and portability
- Database management

Alarms

- Primary system:

- Secondary system: supervision and auto control alarms

Measurements from primary system

- Water in oil (transformers, LTC, special transformers)
- Combustible gas in oil (transformers, LTC, special transformers)
- Temperature (breaker, transformer, LTC, special transformers, ambient)
- Gas pressure (breaker, transformers, GIS)
- Insulation status (cables, transformers, bushings, CT)
- Partial discharges (electrical and acoustical methods for transformers+ optical for GIS)
- Acoustic (LTCs)
- Motor current (LTC regulator, pumps, fans)
- Bushing leakage current detection
- Moisture in isolation
- SF6 pressure
- Load current & voltage
- Harmonic content
- Sudden pressure alarm
- Oil level
- Transmission line temperature
- Transmission line sag
- Breaker motion (speed and velocity)
- Humidity
- On-load tap changer position On-load tap changer temperature differentialBattery status

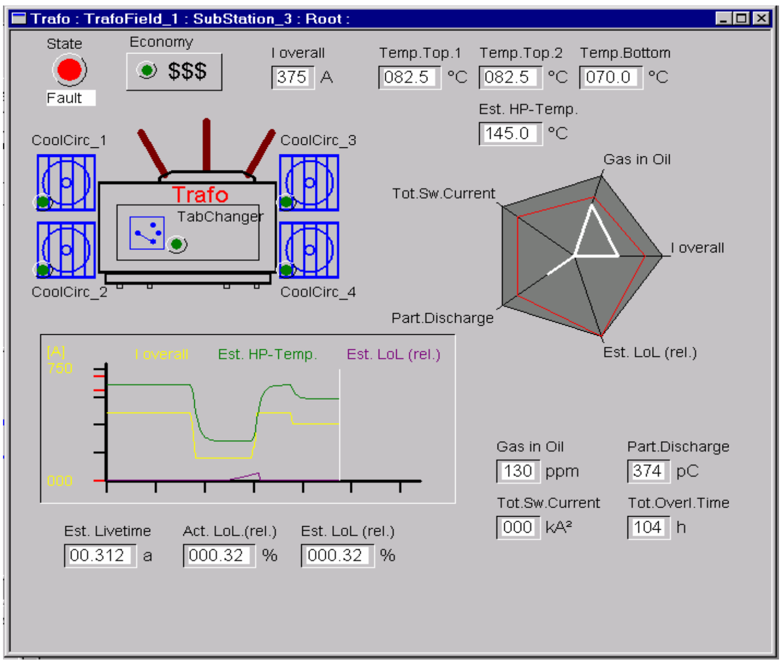

Figure 4.2-4 Example of transformer monitoring application

4.2.5.1 Examples of calculation and models

- SF6 density and leakage
- Dynamic thermal model
- Winding insulation life
- Breaker contact wear
- LTC contacts wear and cooking
- other

4.2.6. Information access and security

The substation automation system is a part of the substation process and therefore the security of the system is very important. The most secure way is to always keep the process systems apart from open systems such as internet and office network systems. Remote control system in many cases really is an isolated system and therefore the security level of it is higher. Other data collecting and access systems to SA-system can be and often are non-isolated systems, modem connections, internet connections or comparable etc. There must be several security levels in SA-system: data monitoring and collecting level, control level, system management level. At the monitoring level the security of the access to the system can be lower than in the higher levels.

4.2.6.1 Security standards

Several standards exist concerning the security. Mainly the following standards may be of interest:

IEC	**International Electrotechnical Commission**
IEC 62351	Data and communication security
IEC 62443	for Industrial Process Measurement and Control – Network and system security
NERC	**North American Electric Reliability Council**
NERC 1200	Urgent Action Standard 1200 – Cyber Security
NERC CIP	CIP-002-1 through CIP-009-1
NERC Security Guidelines	Security Guidelines for the Electricity Sector
ISA	**Instrumentation, Systems, and Automation Society**
ISA SP99	Manufacturing and Control System Security
NIST	**National Institute of Standards and Technology**
	System Protection Profile - Industrial Control Systems
DOE	**US Department of Energy**
	21 Steps to improve Caber Security of SCADA Networks
NISCC	**National Infrastructure Security Co-ordination Centre (UK)**
	Good practice Guide
AGA	**American Gas Association**
AGA Report No. 12	Cryptographic Protection of SCADA Communications
IEEE	**Institute of Electrical and Electronic Engineers**
	Guide for Electric Power Substation Physical and Electronic Security

Table 4-5 Overview of Security Standards and Guidelines

The following table give additional details to the security standard prepared by IEC TC57:

IEC 62351-1: Data and Communication Security – Part 1: Introduction and Overview
IEC 62351-2: Data and Communication Security – Part 2: Glossary of Terms
IEC 62351-3: Data and Communication Security – Part 3: Profiles Including TCP/IP
IEC 62351-4: Data and Communication Security – Part 4: Profiles Including MMS
IEC 62351-5: Data and Communication Security – Part 5: Security for IEC 60870-5 and Derivatives
IEC 62351-6: Data and Communication Security – Part 6: Security for IEC 61850 Profiles
IEC 62351-7: Data and Communication Security – Part 7: Management Information Base (MIB) Requirements for End-to-End Network Management

Table 4-6 Security standards prepared by IEC TC57

Source of table: The exploitation of substations bus solutions at the transmission system operator’s grid, Master of Thesis, V.Tiesmäki 2005 –> Source IEC 62351-1

The figure below indicates the four base requirements for data security (red) including the threats against requirements (yellow) and the concrete attack ways (blue).

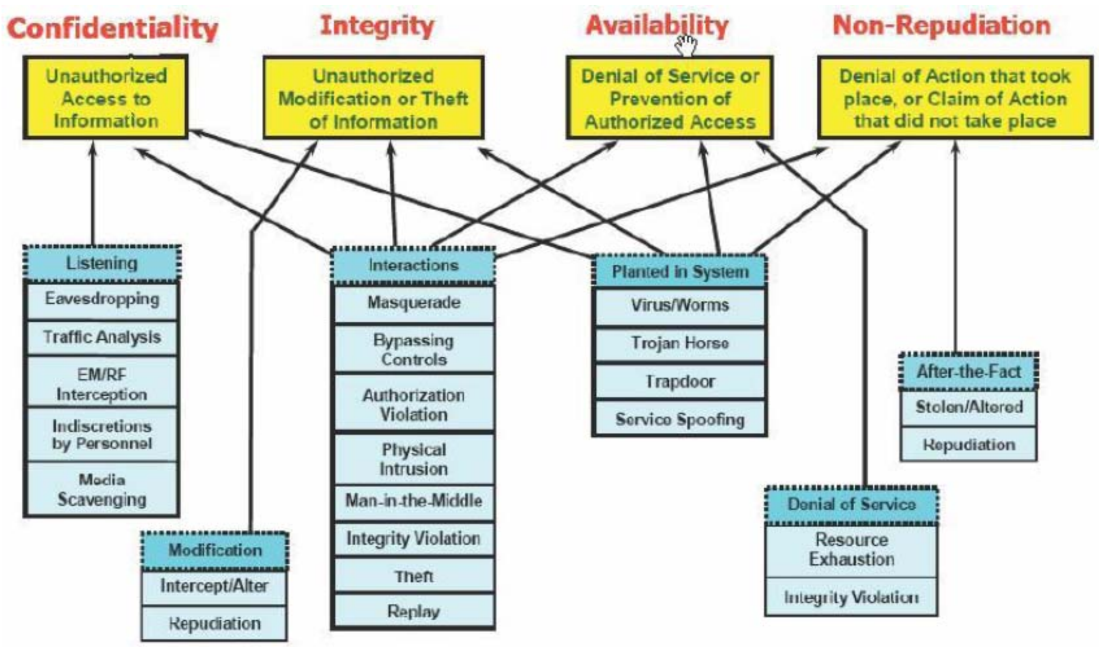

Figure 4.2-5 Data security requirements – threats – attacks

Source of picture: The exploitation of substations bus solutions at the transmission system operator’s grid, Master of Thesis, V.Tiesmäki 2005 –> Source IEC 62351-1

The next figure gives even more details: Four base requirements for data security (red), threats against requirements (yellow), counter-measures against threats (violet), data security management (blue). Basis: NERC recommendation for data security.

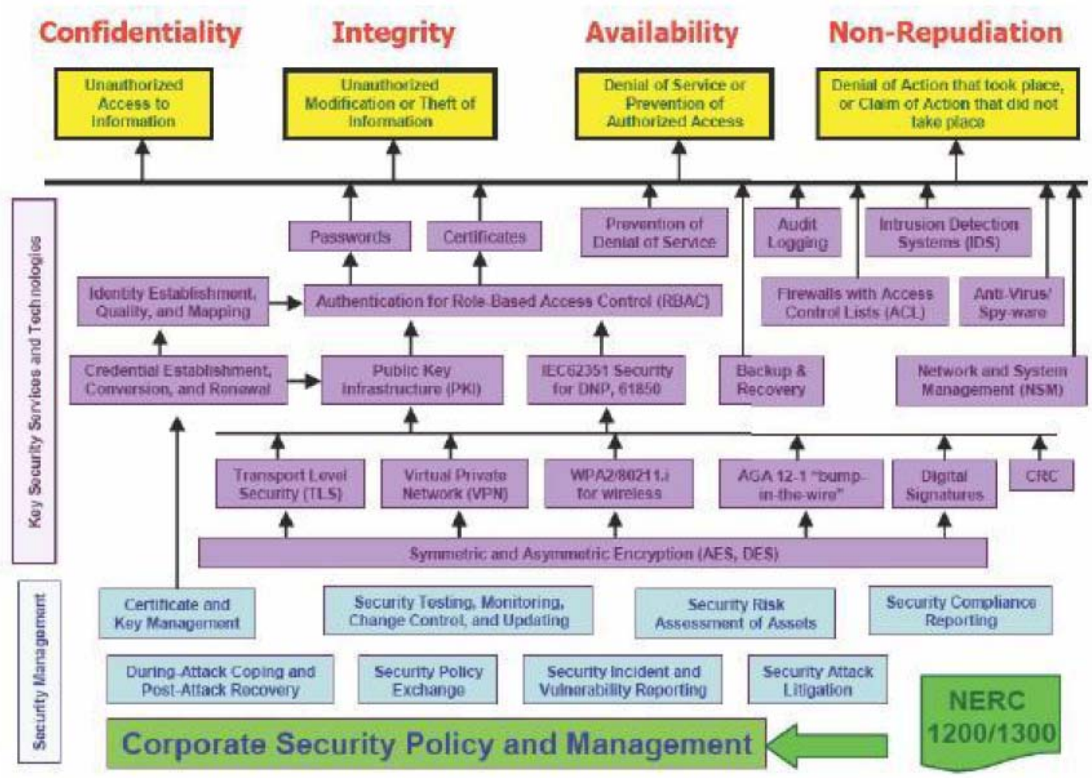

Figure 4.2-6 Data security counter measures

Source of picture: The exploitation of substations bus solutions at the transmission system operator's grid, Master of Thesis, V.Tiesmäki 2005 –> Source IEC 62351-1

4.2.6.2 Security objectives

The main objectives of security are shortly explained below. Besides these main objectives other criteria such as authentication, authorization / access control, audit ability, non-reputability / accountability and third party protection may be considered as well.

Availability
It is essential to have availability of control in order to maintain the normal function of the power grid. For example this allows operators to restore power in case of outages (either by accident or by terrorist intent).

Integrity
But availability in itself is not enough. A hacker might take control of a substation and let the station pass wrong switchgear state data to the operator to trick him to do the remote control. By using this trick a hacker can still perform the actions that were not granted to him directly by the SCADA system.

Confidentiality
Confidentiality means in this context that nobody has access to data that he is not entitled to. This is especially important in a trading market model to prevent unfair trading or even fraud. But to keep the power grid operational availability and integrity are far more important.

Non-Repudiation
Non-Repudiation means in this context that nobody has access to data without successful authentication attempt. The reaction upon unsuccessful authentication attempts is typically locking of accounts and delaying of login.

4.2.6.3 Security measures inside the substation

The most commonly applied security measures applied inside the substation are typically the following:

- Password protected parameter setting
- Password and user dependent access to control system
- Secure line / encrypted for remote access

4.2.6.4 Security measures outside the substation

It is very important to prevent anyone to access directly to the intelligent electronic devices: access to substation information system could cause serious damage locally (at substation level) but also in generating a chain reaction to destroy (i.e. by Trojan horses' intrusion) the entire grid information infrastructure. In fact, often:

- Operational and corporate systems and networks are not physically separated
- It is not difficult to gain the necessary knowledge to navigate in the operational systems

Vulnerable HW and SW devices:

- Remote terminal units and/or communication gateways
- IEDs
- Meters
- Power quality instruments
- Monitoring instruments
- Operating systems (Windows, Linux, Unix, Solaris, …)
- Field buses
- Wan Standard Protocols, especially objected oriented (ICCP, CIM, …)
- Proprietary vendor software / protocols
- Improper use of X-Windows system (by default open system)
- Relays

Depending on the system design it is important to evaluate:

- Private Network vs proprietary solutions (internet, intranet)
- Network paths
- Host/servers security and recovery / backup actions
- Firewall functions by routing and authentication mechanisms
- Monitoring of WEB based remote accesses and interfaces

The system administrators role is fundamental to manage:

- Hierarchy of access and different login figures (protection engineer, …)
- Information sharing
- Password levels (i.e. view, control, engineering, system management)
- Remote accesses
- Propagation and blocking of access rights

Some typical access measures can be chosen:

- UserID and password combination (alphanumeric at least six characters length)
- Deactivation of vendor/factory superuserID
- Invalidation of a password after some days
- Request to change passwords after some days
- Block the access after some wrong retries
- Detect and block unauthorized modem access
- Detect and block unsecured Internet access

On the other side, it is important to finalize an efficient compromise between transmission network performances and security requirements, introducing

- Encryption
- Firewalls
- Intrusion detecting
- Antivirus coordination

4.2.6.5 Requirements and conclusions

One can conclude that security mechanisms are needed, standards are on the way, but it is still a relatively new area where more experiences and learning is required. Not all requirements mentioned in the listed standards may make sense for substation automation applications. It is recommended to define reasonable security architecture with the help of available standards and in line with the utilities' regulations concerning security.

4.3 System architecture examples

4.3.1. Redundancy choices

It is recommended to avoid prescriptive redundancy requirements Redundancy is not a functional requirement. This decision belongs to the manufacturers. It depends on the particular system design or hardware reliability. If the utility concludes that the standard IEDs and design can not achieve the functional reliability requirements of the utility then a redundant architecture based on the standard product shall be the most cost effective answer.
It increases the overall system complexity and hence the fault risk. It increases the number of components, the acquisition cost and the maintenance costs (failure rate spare parts repairs…)

4.3.2. Function allocations choices

For the same reasons it is recommended to avoid prescriptive requirements concerning the functional allocations or integration levels. The function integrations are the result of theoretical calculation and optimizations from the manufacturer, of his know-how and feedback from previous projects. Interfering with this standard implementation shall be detrimental on the global system dependability or on the project cost.

Some common practices concerning function allocations:

- In most systems main protection relays (lines distance protections, differential relays) remain segregated from the bay controller. This is not only due to reliability considerations but to maintenance, setting constraints (complexity of testing, or setting if all functions are integrated on the same hardware platform) and to qualification practices (utilities prefer to integrate existing qualified, “registered” protections in the digital bays rather than qualifying new “boxes”. Protection requires more advanced and longer qualification procedures.)

- Functional autonomy at bay level. For EHV stations each feeder is protected and supervised independently from other feeders

- The prohibition of the implementation of two functions in one IED in order to avoid common failure modes (example main 1 and main 2) may be used in the specification

4.3.3. General Overview

The architecture is mainly driven by the nature of the project. Usually the least restrictions apply for completely new systems whereas for refurbishment projects the kind of refurbishment is driving to a certain extent the requirements concerning the system architecture. Typical scenarios concerning refurbishment can be:

- Only secondary refurbishment
  - Only protections IEDs
  - Protection and conventional control
  - Protection and control IED's

- Primary and secondary side
  - Complete replacement
  - Step by step (bay by bay replacement)

Independent of the chosen architecture common for all modern solutions are that always the following three levels can be defined:

- Process level
- Bay level
- Station level

Depending of he functions corresponding requirements are set to the communication. Communication, openness and reliability/availability have to be considered.

4.3.3.1 Process level

The process level describes the connection to the primary equipment like the switchgear. There are two possibilities how these connections can be realized: Conventional connection or connection using a process bus. Today in most cases the conventional connection is still applied as open solutions with a standardized process bus (IEC61850-9-1) are not yet widely available on the market. But with the release of the IEC61850 standard and the introduction of products supporting alos process bus to the market it is just a question of time until the process bus will widely be applied to solutions. The characteristics of the two types of process connection are:

Conventional connection based on copper wiring

- connection to the switching object
- connection to the VT's and CT's

Connection with actuators and sensors

- connection via the process bus

In the case of the process bus certain functionality is moved out of the bay level devices towards the process level. Merging units are used to merge signals from several secondary converters into one communication link and time tag outgoing samples with 1 PPS.

4.3.3.2 Bay level

Generally it is state of the art to have a decentralized architecture taking as much as possible the functionality near to the primary process. In this respect, the following functions can be allocated at bay level:

- bay control
- bay protection
- bay event list
- bay fault recorder
- bay interlocking
- bay test and diagnosis
- bay metering

4.3.3.3 Station level

According to the decentralized philosophy the following functions can be allocated to the station level:

- link to NCC
- station interlocking
- HMI
- Fault record
- Event record
- Archiving
- Central automation
- Databases (with interfaces for data exchanges)
- Station oriented protection (e.g. busbar protection)
- Gateway
- Monitoring
- Test and diagnoses

4.3.4. Recommended communication standards

Since the IEC61850 standard has been released and more and more suppliers are supporting it and as well as more and more experiences are made the only recommendation for communication within substations is IEC61850. Currently many vendors support part 8 for the communication between the bay level and the station level as well as for the communication between bay devices. Part 9 covering the process bus is still in an initial phase.

There are still existing products that may only support previous standards. These products are still accepted at the present time. Besides IEC61850 the following other standards for communication that are listed below may still be required to be supported:

Bay level to station level communication:

- IEC 60870-5-103 for bay level to station level

Station level to network level communication:

- IEC 60870-5-101
- IEC 60870-5-104
- DNP 3.0 subset 2

For the communication between the station and the network level other proprietary protocols may still be required to support the connection to installed SCADA systems.

Many other de facto IT standards are under laid to support communication and information exchange on different levels of the system. Below is a list of commonly used standards in a state-of-the-art substation automation solution:

- Ethernet / Fast Ethernet
- TCP/IP protocol suite
- OPC
- HTTP Hyper Text Transfer Protocol , S-HTTP Secure Hyper Text Transfer Protocol , SSL Secure Sockets Layer
- SOAP Simple Object Access Protocol
- HTML Hypertext Markup Language, XML Extensible Markup Language

4.3.5. Abstract System based on IEC 61850

The connections are logical communication links

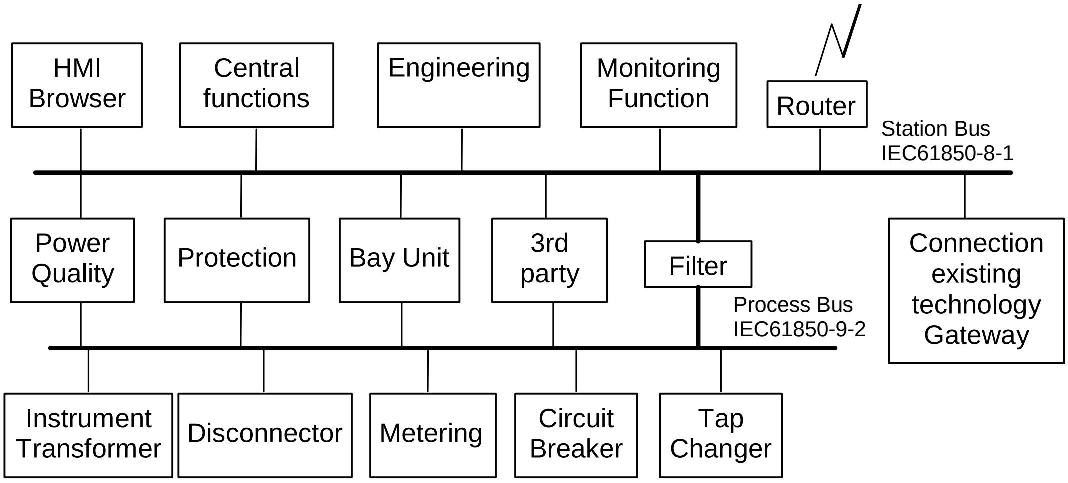

Figure 4.3-1 Abstract system architecture based on IEC 61850

A system architecture based on IEC 61850 can be described with the following main characteristics:

- IEC 61850-8-1 at the station level
- Seamless 100Mbit/s Ethernet structure, backbone with 1 GBit/s
- Inter-bay communication (GOOSE= Generic Object Oriented Substation Event) at bay level
- Redundancy through independent inter-bay communication, bay interlocking / automation is independent from station level (no more bottlenecks)
- Functional redundancy of HMI and station computer
- Client server architecture
- Communication masters for integration of legacy IEDs via e.g. IEC103, DNP3.0, etc.
- Web based test and diagnosis at bay level (integrated web server)
- Openness due to IEC 61850 and other industrial standards like Ethernet, OPC etc.
- Interoperability defined in IEC 61850

4.3.6. Examples for SA System Architectures

4.3.6.1 Overview

Based on the SC B5/WG07 report the table of SA architecture impacts has been extended with the characteristics of the three example architectures.

Influence factor	**Impact on SA architecture**	**Example 1**	**Example 2**	**Example 3**
Size of the substation: • Number of voltage levels • Number of bays • Number of busbars	Number of LAN's: a single Ethernet segment for both substation and bay level, or several segments, one for substation level and others for bay level.	1 Voltage level Small number of bays	2 Voltage levels Medium number of bays	3 Voltage levels Large number of bays
Reliability and availability requirements depending on: • The voltage level, • The substation criticality in the network	• Redundancy or not of LANs • Redundancy of bay level and/or station level controllers and HMI • Integration or not between control and protection • Redundancy of protections	No requirements	High requirements especially for remote control	Highest requirements, no single point of failure
Utility's industrial strategy: • Bay per bay Refurbishment • New substations	• Choice of modular and flexible architectures • Interfaces with existing conventional devices • Choice of configuration tools easy to manage	Not relevant	Not relevant	Not relevant
Cost over the system life cycle	• Number of devices • Redundancy	Low initial costs	Medium initial costs	High initial costs
Operating procedures of the country or the utility.	• Remote control interface using proprietary communications • Integration of protection from other manufacturers	Local and remote control	Local and remote control Local control independent of remote control	Local and remote control Local control independent of remote control
Topology of the substation: • Transfer busbars • 1 or 1 1/2 Circuit breaker arrangement	• Number of cubicles • Number of bay computers • Functions of automation at bay and substation level	Not relevant	Not relevant	Not relevant

Table 4-7 SA Architecture Impacts

4.3.6.2 Example 1: Distribution substation

An architecture example for a distribution substation is shown in figure 4.3-2. The typical characteristics from an operational point of view are that the substation is usually unmanned the controlled from remote. To provide most economic solution concerning space and cost multifunctional bay level IEDs for protection and control are used (BCPU = Bay Control and Protection Unit).

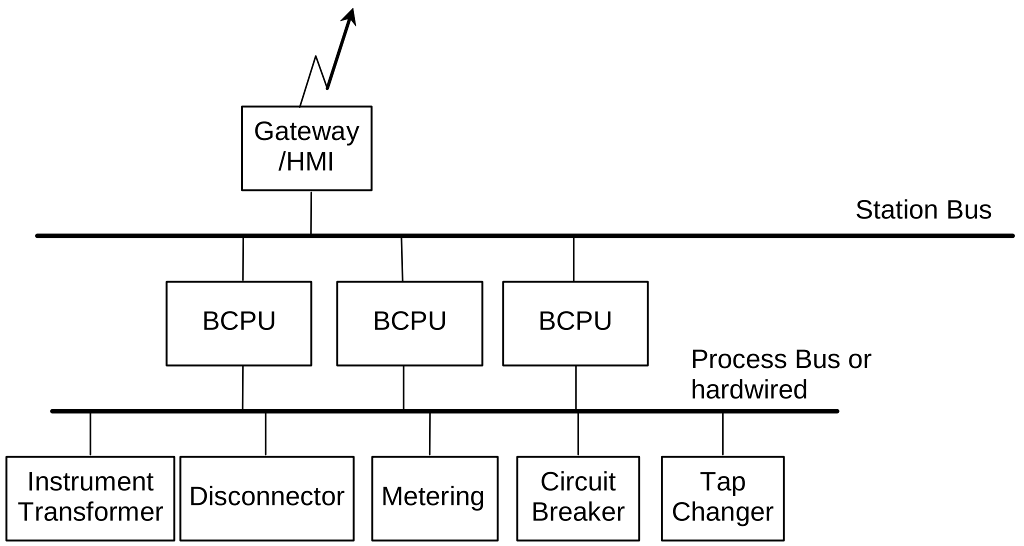

Figure 4.3-2 Architecture example for a distribution substation

4.3.7. Example for a transmission substation

An architecture example for a transmission substation is shown in figure 4.3-3. The typical characteristics from an operational point of view are that the substation is usually unmanned and controlled from remote. To increase the system availability demanded for this kind of application and to ensure high reliability for the important remote link a dedicated IED for the gateway functionality is provided. Protection and control is also distributed into separate devices to ensure independency and high availability.

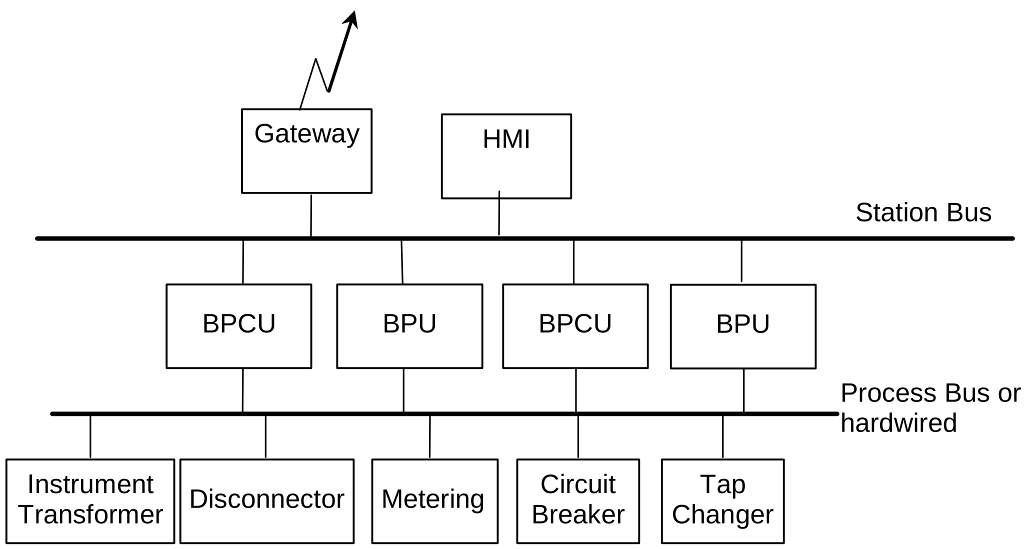

Figure 4.3-3 Architecture example for transmission substation

4.3.8. Example for a extra high voltage transmission substation

An architecture example for an extremely important substation e.g. extra high voltage transmission substation is shown in figure 4.3-4. The typical characteristics from an operational point of view are that the substation is usually unmanned and controlled from remote. To provide the highest level concerning availability all important functions are designed fully redundant, meaning redundant HMI and Gateway at the station level and main 1 and main 2 at the bay level for protection.

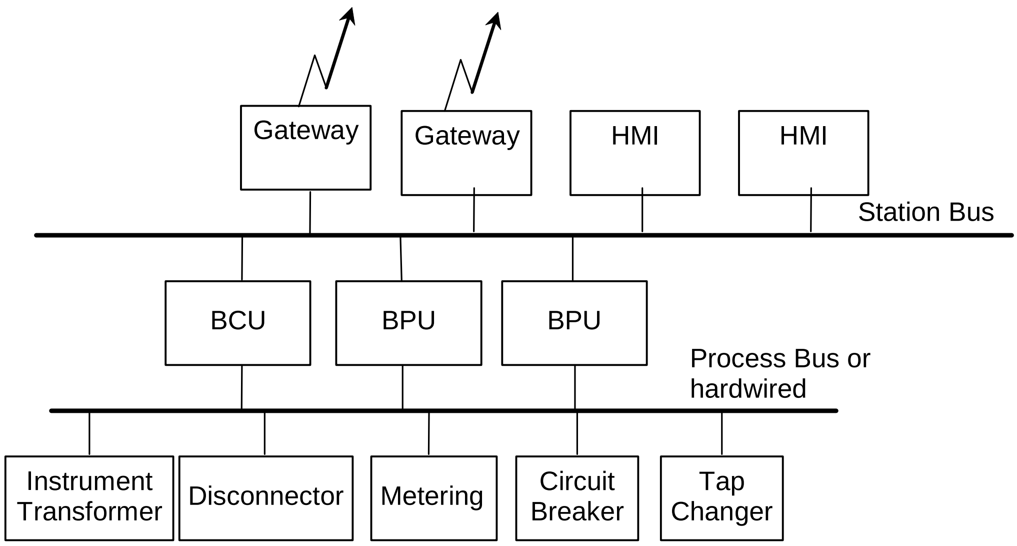

Figure 4.3-4 Architecture example for a extra high voltage transmission substation

4.3.9. Web based solution

Here we are looking beyond the substation and towards the communication between substations or between substations and the network control centre. Today's most common way is to use gateways at the station level that converts the substation protocol to a network protocol. In future when technology at the network level changes and the bandwidth of the utilities communication networks is extended direct connections without gateways may be considered and WEB clients placed anywhere in the corporate network may be allowed to access the substation equipment of any substation for maintenance, service and analysis. Crucial point here is that the necessary security measures are taken to ensure a safe and reliable system.

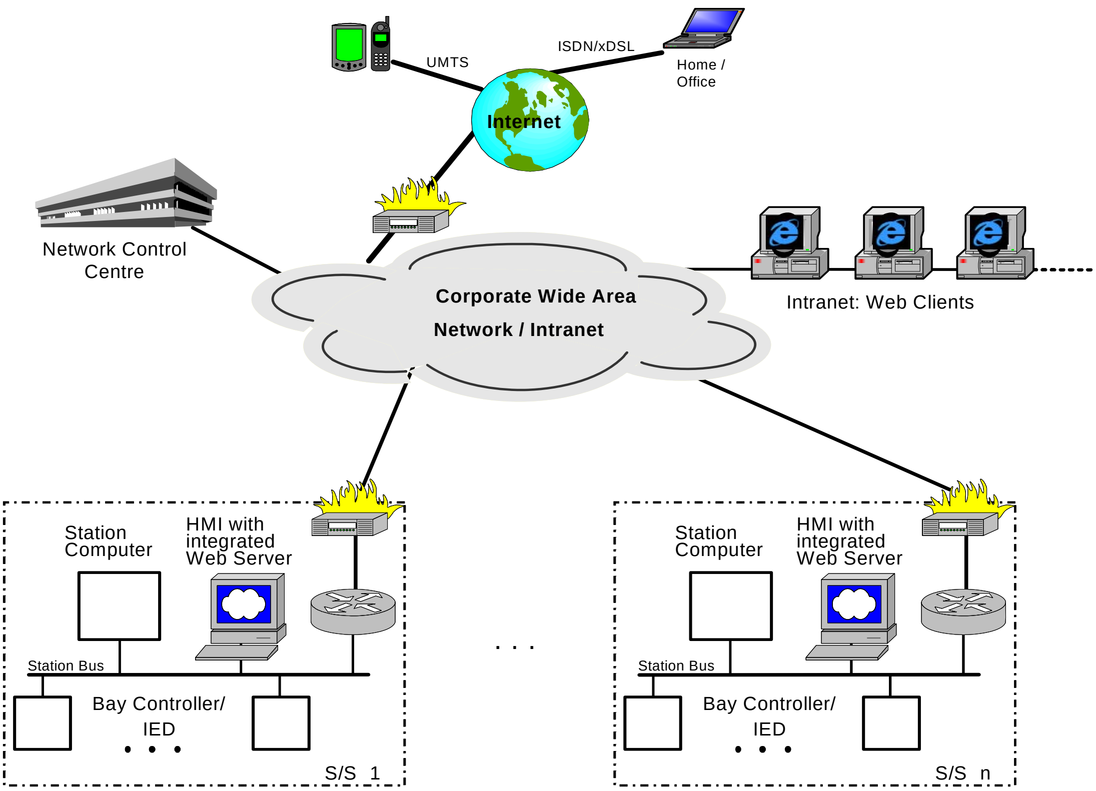

Figure 4.3-5 WEB based SAS solution

5 Guidelines for specification and evaluation of project management and services

Basically this chapter covers all aspects except the technical requirements.

5.1 Project management

5.1.1. General Considerations

After the SAS delivery contract has been signed, the project will proceed according to the following consecutive steps:

- Engineering including project design, parameterizing, constructional and wiring design
- FAT
- Commissioning
- SAT
- Trial operation
- Final takeover
- Warranty period
- After sales services
- Decommissioning

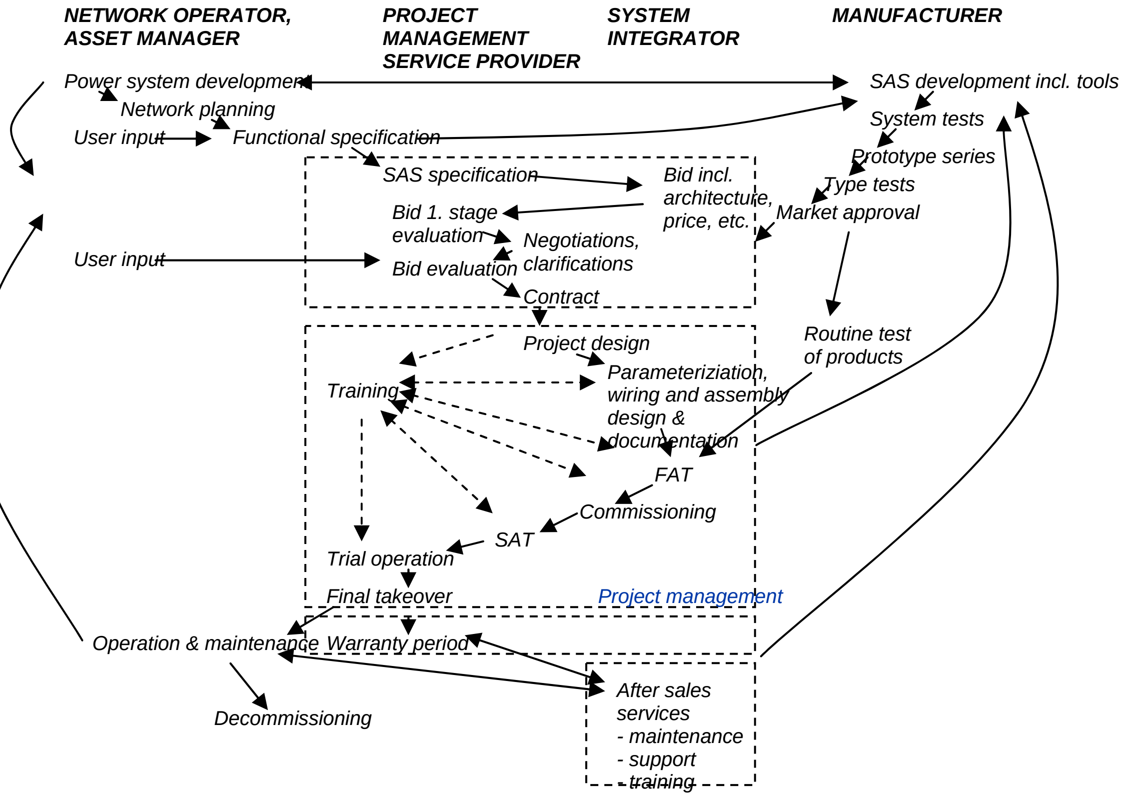

Figure 5.1-1 Development process

Source of picture: IEC61850

It is typical that in a SAS project there are many parties involved: the end-customer with different disciplines, the project management service provider of the end-customer, the system integrator and the factory. At the time of the procurement, it is very important to specify who is responsible for the total installation including the interface to the primary system and the interface to the NCC. Also, agreement between parties of co-operation, information exchange, time-schedule, subcontracting etc. is needed.

The quality assurance is a common task of the system integrator / manufacturer and of the customer of the SAS with different areas of responsibility. If two or more parties are involved then the responsibilities of each party shall be defined at the time of procurement.

The need for several services (training, maintenance, parameterizing, spare parts) is determined by how much in-house work the customer shall do, and how much the customer relies on the manufacturer.

Recommended structure of the project management, Recommendation on assessment of

- time schedule,
- terms of payment,
- subcontracting,
- liability,
- approval process,
- proceeding for the integration of third party equipment,
- scope of supply

5.1.2. Engineering phase

The engineering includes:

- the definition of the necessary hardware configuration of the SAS as the composition of IEDs with various connections to the environment
- the adaptation of functionality and signal quantities to the specific operational requirements by use of parameters
- the documentation of all specific definitions (i.e. parameter set, terminal connections etc.)

The engineering process creates the conditions for adapting a SAS to the specific substation and the operating philosophy of the customer.

Project design is the definition of the technological concept to solve the required SAS tasks including the choice of structure and IED configuration as well as the determination of interfaces between IEDs and the PE. The basic design is already determined at the time of procurement; at this stage the final design with all the details is specified.

Parameterization is the generation of the parameter set for the SAS.

Documentation is the description of all project and parameterization agreements about the features of the SAS and its link to the PE according to the required standards. It includes also the wiring diagrams and constructional diagrams.

Parameter categories

Configuration parameters define the global behavior of the whole SAS and its IEDs. The generation and modification of the configuration parameters should be carried out off-line, i.e. separately from the operation of the SAS. The configuration parameters usually include *system* and *process parameters*.

Operating parameters define the behavior of partial functions of the SAS. They shall be changeable on-line during the normal operation of the SAS via remote access through a gatekeeper (e.g. HMI) running the necessary software to access the IEDs, HMI or integrated service interface of the IEDs. The operating parameters usually include process and functional parameters, for example limit values, target values, command output times, delay times etc.

Usually the customer has a big role in defining the operational parameters (process and functional parameters) and thus his role in this phase is crucial.

Requirements for the engineering tools

The parameterization tool shall be able to run on commercial hardware with a commercial operating system. (also after 20 years)

The parameterization tool of a manufacturer shall be strictly backwards compatible, i.e. it shall be possible to parameterize all SAS of the same family supplied by the manufacturer using the most recent parameterization tool.

The parameterization tool should be able to be used for all applications of a SAS of one product family.

In most cases, the engineering tasks are included in the system integrator's offer for the SAS project. In all cases, however, the system integrator has to offer customer training for the use of the engineering tools so that the customer may maintain and expand the SAS installation (could be service agreement based also). The system integrator should support this process with consultative services, training and regular information regarding updates and extended functionality of the SAS installation and the engineering tools.

The scope and limits of the purchase should be specified in detail, especially when there are third parties, such as primary switchgear supplier, involved in a project. Responsibilities and cooperation of these parties particularly during the planning stage, the different testing phases, installation and commissioning should be clearly specified in a contract. Care has to be taken that, in the end; the customer will get a properly operating unity and full documentation. Things will go much more smoothly, if the division of tasks and responsibilities are agreed by all parties in a multilateral contract.

5.1.3. Commissioning phase

5.1.3.1 Site erection strategy for refurbishment substations

This part of the specification only concerns substation refurbishment projects that have to deal with the severe erection constraints compared wit new substations projects.

5.1.3.2 The erection objectives and constraints

The aim is to establish SAS erection strategies in existing, energized substations:

- Minimizing outages of the primary system
- Minimizing operation constraints
- Minimizing site engineering work

and therefore it is safe and cost effective.

Many tools and methods are likely to achieve these goals such as:

- configuration flexibility of the system,
- quality of the utility site data inputs (site diagrams, site information).
- various "software" tools, avoiding less efficient and less reliable "hardware" wiring and cabling tasks or minimizing additional hardware and interface costs during on site erection (temporary interposing relays,..)

The main constraints are listed below:

- Power system constraints: nowadays, in a deregulation context utilities are forced to drastically reduce outages in frequency and in duration. This is especially the case for EHV voltage levels or for power plant substations. Therefore migration has to be done on a "bay per bay" approach over a sometimes very long period, depending on the network load and on the substation strategic location

- Substation Operation constraints: during site work, operation people may have to accept to have two control points (the conventional mimic panel for the bays remained in conventional technology and the new MMI computer for the digital bays) or two event recorders.

- Remote control operation constraints: the data coherency with the remote control centre has to be ensured during the whole migration, hence the switch from an old to new bay induces changes in remote control information. Site work shall avoid disturbing remote supervision and control.

- System engineering constraints: migration from old to new SAS introduces architecture changes : for example:
    - centralized functions from the conventional system such as autoreclosure relay or phasing relay (to close circuit breaker with zero phase angle by checking frequency slip) become distributed functions at bay level in the digital system.
    - Interbay exchanges between old and new digital bays must be temporally created during migration. Some of these exchanges will be realized at the end on the fiber optic LAN instead of peer to peer copper wires.

- Site work constraints: the main problem corresponds to the lack of free space in substation building and in bay kiosks. In that case, it is difficult to put the full digital system loaded with its final configuration on site, parallel to the conventional system in operation.

The SAS specification shall ensure the possibility to use some methods for migration.

Primary equipment oriented methods:

- Transfer busbar if available in the substation
- Mobile circuit breaker

- Bay Transfer method (RTE practice) if no transfer busbar is available in the substation this method is used for line bays migration and shall be used in the SAS according to the description below:

  The line is remotely supervised and protected by the full busbar coupler secondary equipment.
  - The full secondary equipment associated to the line circuit breaker (line CTs and VTs protections and automatic functions) are shunted.
  - All functions necessary to protect a line are included in the busbar coupler bay and are activated if needed with the proper configuration.

In the digital system the re configuration of the coupler bay protection and control functions shall not be too cumbersome.

Secondary equipment oriented methods:
- Back up data base and configuration
- Test mode
- Configuration flexibility at substation and bay level
- Special remote control interface to ensure data coherency with the remote control center and to avoid multiple reconfigurations of the remote MMI.
- Downloading client data, remote control data, process data, site diagrams, established and exchanged in an unambiguous and coherent format. Use of XML files shall be recommended in the specification. The aim is to ensure configuration coherency and integrity and to prevent double manual operation on data.

5.1.3.3 Review of different erection strategies

Based on feedback from utilities and manufacturer proposals, several erection approaches are listed and compared below:

Full parallel erection

One major prerequisite to adopt this approach is having sufficient free room in bay kiosks to put the new digital equipment parallel to the conventional one : in this approach, the full digital substation control system with its definitive configuration can be tested on site before commissioning.
To counter free room limitations, it shall be possible to emulate the missing digital bays so that the substation level system devices are loaded with the final configuration although not all digital bays are connected to the system.

Bay level migration

This approach requires digital to analog interface to connect the new digital bay to the conventional station level control system as long as all digital bays are not installed and in operation. One major problem in this approach is the cost of the migration interfaces.

Remote control migration

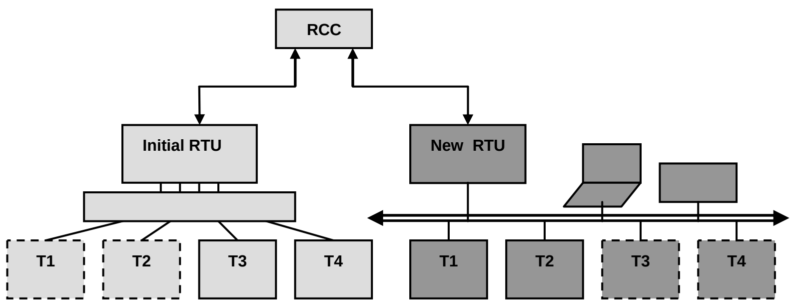

Figure 5.1-2 Remote control migration

5.1.4. Acceptance, quality and type tests

5.1.4.1 General Overview

Acceptance tests are intended to verify to the customer and Supplier that the SAS is in conformance with functional, technological, performance specification and free from failures and thus operates as intended.
The Acceptance Test is meant as a security for both the Purchasing Company and Selling Company. The tests are also confirming that both parties are in agreement with the functions and facilities, which are included.
The tests are approved and signed by a representative of the customer. The signing of the tests does not absolve the seller of responsibility during the guarantee period.

	Type tests	FAT	SAT
Technological conformity tests	x		
Performance tests	x	x	x
Functional conformity tests		x	x
Commissioning tests			x

Figure 5.1-3 Acceptance test matrix

General guidelines on acceptance tests

- Testing requirements should be established by the customer
- They should be coherent with technical specifications

Where applicable the technical requirement of the technical specifications should be identified and correspondence with a dedicated test shall be made.

It is recommended to involve the customer in the testing process as much as possible although it represents additional investment (tools, human resources). It helps developing competencies and confidence at an early stage on the SAS, it helps sparing training costs.

5.1.4.2 Type Tests

Newly designed products shall be proven by a type test to ensure the usability in practice in case there are no references available. The type test shall be performed using samples from the manufacturing process. The type test is the verification of the product against the technical data (figure 5.1-4) which are specified, such as:

- mechanical withstand ability
- electromagnetic compatibility
- climatic influences
- functional correctness and completeness

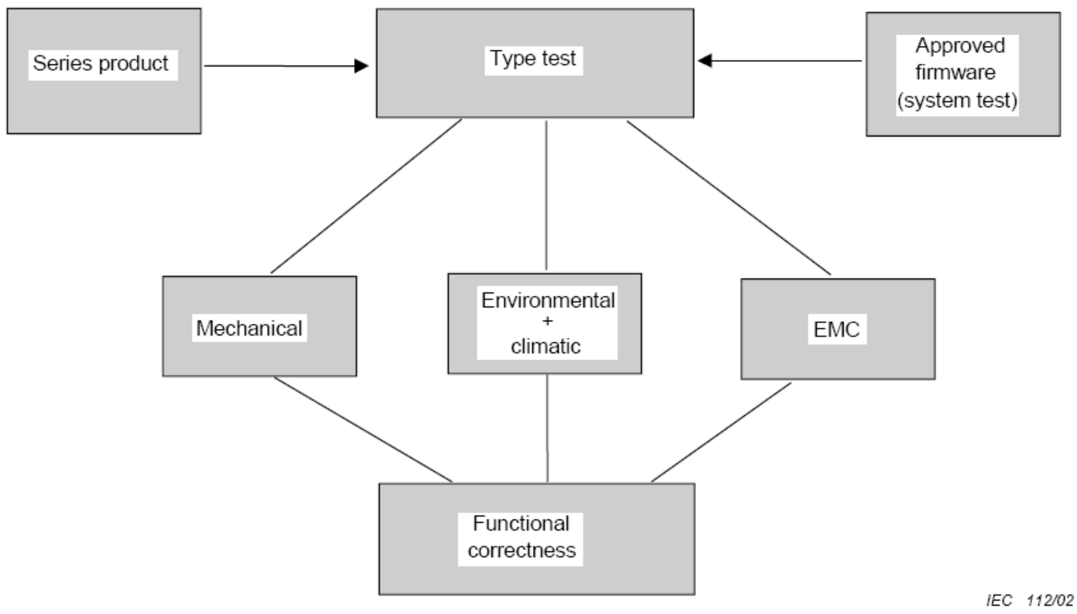

Figure 5.1-4 Type test content

Source of picture: IEC61850

The type test can be carried out by the use of system tested software. Before regular production delivery can be started the product has to pass the type test.

Type Tests verify the correct behavior of the IEDs of the SAS under the test conditions corresponding to the technical data. This test marks the final stage of the hardware development and is the precondition for the start of full production.

Depending on the customers need they can be generated by independent certification labs, by the manufacturer or by the utilities themselves. They include Technological Conformity tests verifying hardware quality, insulation, climatic, EMC against specification, reliability assessment against specification, quality and depth of self-supervision against specification.

Supplier shall provide a certificate together with the offering documents and on request provide a detailed report to the customer.

5.1.4.3 Factory Acceptance Test (FAT)

Factory Acceptance Test includes Customer agreed performance and functional tests of the specifically manufactured SAS, and of its components : devices with their main functions complete end to end test of all bays.

FAT are performed in the manufacturer's factory using process simulation test equipment and the parameter set for the planned application.

FAT are very important as they contribute to avoid and spare costly and time consuming system upgrades caused by late detection of software defects as well as additional testing on energized substations.

They are much more efficient than on-site testing to check critical and complex functions, because each function shall be solicited and thoroughly investigated. On the contrary, on site testing is partial because lots of functions are very rarely solicited (such as three phase autoreclosure or loss of synchronism)

FAT is typically applied to single systems and in case of e.g. frame contracts only once typically for the first substation.

The bay level IEDs shall be configured according the application needed for the project.

The result of the FAT should be documented and signed by both the manufacturer and the customer.

A good compromise is for the customer to have access to testing of critical essential functions. It shall focus on precise functional testing against specifications, performance testing against specification

The main goal of the FAT functional test is to verify the functions against the specifications.

FAT procedure	Tests /
Inspection of equipments	Equipment is connected and without visible failure
System documentation	All documents are updated and available in conformance with system components under test
Function testing	Tests on all functions
station level functions	display screen equipment, HMI
	substation overview with all fields and information necessary for normal operation status of all apparatus and measurements
	type bays (line transformer, bus coupler…) detailed view with all fields and information necessary for normal operation status of all apparatus and measurements
	operation functions o station remote modes o bay operations
	synchronizing equipment
	alarm list
	event list layout
Bay functions	connect simulators to all bays and send controls from HMI and remote control center,
	analogue simulations
	Test of "third party" equipment integrated in the bay such as Registered protections?
	End to end test to verify that when a bay input signal changes, the correct information is obtained at the station HMI, at the remote control center

Table 5-1 FAT tests overview

5.1.4.4 Site Acceptance Test (SAT)

The acceptance test of the SAS on site (SAT) shall be carried out on the completely installed equipment in individual steps. Site Acceptance Test (SAT) includes the verification of each data and control point, also the correct functionality, inside the SAS and between the SAS and its operating environment, on the complete installed equipment using the final parameter set. The Site Acceptance Test is the pre-condition for the SAS being accepted and put into service. The tests include:

- Verification of good delivery : the received products comply with the tested ones
- Verification of the devices health
- Verification of good software implementation in all devices (manufacturer
- verification procedure)
- Verification of all input and outputs
- Verification of applications conformity
- Verification of supervision system
- Verification of setting conformity
- Verification of scheme response

Refer also to the following CIGRE report: WG 34-10 2000.

5.1.4.5 Trial Operation

After the approved Site Acceptance Test it is useful to have a disturbance free Trial Operation time. Using the SA-system in normal operating conditions most of the small “hidden failures” of the SA-system and engineering can be brought out. Typically the length of the Trial Operation time is about two months.

This disturbance free test period is interrupted if an operational problem arises. After the problem is fixed the test will restart from the beginning.

By an operational problem is meant a fault or problem in the system or its communications that endangers the reliable process monitoring and control of the substation.

Fixing a non-critical problem is allowed to do so that the disturbance free test period is interrupted and continued after fixing. The fixing time is added to the end of the test period.

Takeover of the system occurs when the customer has approved the factory inspection, commissioning test and the disturbance free test and the system and documents included in the purchase have been delivered to the customer. A protocol concerning acceptance is usually written and the supplier and the customer will sign it.

5.1.4.6 Quality system

Quality assurance and project plan are useful to check the status of system equipment and configuration during all phases of tests. Inspections shall therefore be carried out during tests; based on hold and witness points indicated in the test plan, this inspection will provide information and confidence on the quality of the tests and reduce the risk of failure during FAT or SAT with all related costs and problems

The supplier of the substation control system should have a documented quality assurance system. The customer must have the right to evaluate the manufacturer's quality assurance documents, and the customer must be able to evaluate quality control of the purchased system at the factory during manufacturing.

The applicable ISO standards for the quality assurance are:

- ISO 9001: Quality management systems -- Requirements
- ISO 9004: Quality management systems -- Guidelines for performance improvements

The applicable ISO standards for the environmental assurance are:

- ISO 14001: Environmental management systems -- Specification with guidance for use
- ISO 14004: Environmental management systems -- General guidelines on principles, systems and support techniques

5.1.5. Documentation

5.1.5.1 Schedule for submittal of documents

Documentation can be divided into four different categories:

Offer documents:	documentation delivered with the offer
Base design documents:	documentation delivered some months after the order
Detailed design documents:	documentation and manuals delivered before commissioning
Final documentation set:	final documentation, usually not more than one month after the acceptance of the delivery

5.1.5.2 Offer documents

The offer should contain all technical data of the offered system and also clarification of the operating principles and construction of the system. Additionally the offer could include:

- how many years is the supplier committed to support the system maintenance, spare parts and system knowledge assistance
- the aging and wearing parts of the equipment and needs of maintenance
- expansion capacity, possibilities to add new functions
- training program for operations and maintenance personnel
- assortment of essential spare parts in operation and maintenance
- deviations of the offer compared to the requirements stated in the technical specification
- references of previous, similar deliveries, including type and version information
- alternatives in remote workplace implementations, a proposal for the implementation.

5.1.5.3 Base design documents

Quite soon after the order and at the beginning of the detailed engineering phase the supplier should deliver for approval at least the following documents:

- specification of the control system programs and equipment
- preliminary signal lists.

5.1.5.4 Detailed design documents

After detailed engineering phase the supplier should deliver for approval the following documents:

- final circuit diagrams and wiring tables
- diagrams of internal circuits of all the devices included in the system and component lists
- manuals and installation instructions, often at least partly translated into native language
- logic schemes of the station control system and its bay level interface units.
- signal lists for commissioning

Before the commissioning of the system the supplier has to deliver directions for the use and maintenance of the system and its individual equipment translated into the native language. The directions should include system administration procedures in the native language for the operator personnel, e.g. start-ups and logins on the station level and remote connections as well as handling the most common problem situations.

Also wiring diagrams and circuit diagrams as-built are needed. After the approved Factory test the Factory Test report should be delivered by the supplier.

5.1.5.5 Final documentation set

Usually not later than one month after the takeover and acceptance the supplier should deliver the final documents. The form of final documentation set follows the specification or the mutual agreement. For example the supplier can have responsibility to deliver several series of paper copies and one set as data files in electronic form. The final documents included in the delivery are as-built drawings and lists drawn according to the applicable standards. Example of documents is listed below:

- circuit diagrams
- wiring tables
- component lists
- lay-out drawings of the equipment
- cable list

- final signal lists
- final logic schemes of station control system and bay units
- commissioning test report
- The backup copies of the software, parameterizing and setting programs shall be furnished in electronic form

The supplier should include the buyer's drawing number and an empty field for the handler's sign in the title block of the final drawings.

The supplier shall submit the complete technical documentation, including instruction manuals, diagrams, drawings and software for all equipment being proposed, whether it consists of items manufactured by the supplier himself, or purchased from others.

Regardless of their nature, the documents shall be accepted in the native language or in the English language.

A schedule for submittal of the documentation shall be part of the Proposal.

The Technical Documentation to be submitted, especially schematics, wiring drawings and single-line diagrams, bills of equipment and other documents, shall be part of the engineering design and shall be produced using the IEC or ANSI symbols. Observing the customer standards, this shall be made available to the eventual supplier of the System, including typical drawings for assistance.

The consistency with the supplied hardware and software components, in terms of version and revision, shall be strictly complied with. Modifications and updates of the documents shall be informed by the supplier by means of a Document Update Sheet with all indications required (number of the manual, chapter, section, page, the modifications performed, etc.);

In case graphics computing is used for generation of drawings, the CD/diskettes shall be delivered with all drawings produced with the standard design software, which normally does not eliminate the above requirement regarding the quantity of copies of documents to be submitted. The customer's instructions for production of documents in digital media, if any, shall be observed.

All drawings are and shall remain the exclusive property of the customer, who shall be allowed to dispose of them at its discretion. However, it is hereby understood that the supplier shall not be responsible for eventual errors or losses that may arise from their utilization.

With no need of authorization from the supplier, the customer has the right of using, copying, duplicating and releasing to others the drawings, instructions and any other information related to the equipment, to the extent that may be required for the work of third parties that may be performing any task related with the equipment or part thereof. Eventually, if the customer shall sell or lend the equipment or part thereof to others, the customer shall be entitled to deliver to such third party any or all of the corresponding documents, without any authorization from the supplier.

No statements, stamps or other references invalidating or restricting the rights of the customer shall be made or entered on the documents. The supplier shall eliminate or add a note waiving the restriction imposed by all such indications that may appear on drawings and on any other documents and provide evidence of such suppression or waiver with its signature.

The number of copies shall be specified in the specification.

5.1.5.6 Approval of documents

All equipment, for which approval of documents is required, shall initially have their documents submitted to the customer for analysis and approval after the first order. For the subsequent orders, there is no need of submittal of new documentation for approval, since the documents submitted previously and approved must be strictly complied with during the whole contract in question.

Any work performed before the documents are approved shall be at the cost and responsibility of the supplier. The customer is entitled to request any additional details and to demand, from the supplier, that any alterations be introduced in the design as may be required in order to comply with the provisions and with the objective of the customer's Technical Specification, at no additional cost to the customer.

The customer shall make comments regarding the submitted documents after their receipt. In case of re-submittal, a new time for review shall be set. Drawings that are revised or altered by the supplier after the approval shall be re-submitted for approval.

One (1) opaque copy of each drawing bearing the stamp "Approved Drawing", "Approved With Comments" or "Rejected" shall be returned by the customer to the supplier, while another copy shall be retained as the master copy, which shall prevail in the case of any doubt or discrepancy that may subsequently arise.

In the case of any document that is either REJECTED or APPROVED WITH COMMENTS, the same shall be returned to the supplier for the proper corrections and shall subsequently be submitted for new analysis during a period of time with the same duration and the supplier shall be responsible for any additional expenses arising from this fact.

The APPROVAL by the customer of any technical document related to the Systems represents a basic acceptance of the design and does not exempt the supplier from the responsibility of complying with the applicable specifications and standards, design failure, manufacture defects and material deficiencies.

When approved by the customer, the supplier's documents and drawings shall be included among the documents that are part of the contract. All expressions and notes contained in the drawings shall be deemed to be part of the Technical Specification and of the Contract. Documents failing to comply with any of the requirements of this clause shall be void and considered to be in conflict with the contractual requirements.

The time terms for submittal of the documents shall be strictly in accordance with the schedule required by the customer and / or submitted by the supplier.

5.1.5.7 **Software**

Three counterparts of the programs shall be submitted in the form of CDs or diskettes, properly identified. The specific programs of the Supply shall not be accompanied by the listing and the source code, provided that such shall be conflict with the rights previously assured by the Supplier.

5.2 Warranties, after sales services and training

5.2.1. Contractual aspects - Warranties – penalties

5.2.1.1 Contractual aspects

The Substation automation system specification shall include all general conditions applicable to any procurement, such as prices, terms of payment, time of delivery, delivery terms, guarantee and general terms of procurement.

Specific requirements may be needed regarding the division of responsibilities between different subcontractors and the definition for the guarantee period depending on the chosen maintenance model.

5.2.1.2 Responsibilities and cooperation of different parties

The scope and limits of the purchase should be specified in detail, especially when there are third parties, such as primary switchgear supplier, involved in a project. Responsibilities and cooperation of these parties particularly during the planning stage, the different testing phases, installation and commissioning should be clearly specified in a contract. Care has to be taken that, in the end, the customer will get a properly operating unit and full documentation. Things will go much more smoothly, if the division of tasks and responsibilities are agreed by all parties in a multilateral contract.

5.2.1.3 Guarantee period(s) and maintenance

There are many variants to guarantee the availability of the substation automation system and to do the modifications and extensions.

The traditional way is that the delivery includes a guarantee period of perhaps two years beginning from the takeover. In this case, the first step takeover will take place after all tests and the 2 months´ disturbance free test period has been approved by the customer, and all the documents included in the purchase have been delivered. A protocol concerning acceptance is written and the supplier and the buyer will sign it. During the guarantee period all the modifications will be made by the supplier. The inspection procedure for the final takeover shall be agreed by the supplier and the customer. Responsibility of the delivered system shall be transferred to the buyer after the accepted final takeover inspection. Usually, after this moment, maintenance service is purchased from the supplier, perhaps with agreed service level (24 hour response etc.).

If maintenance is done by the customer or his service partner (other than the SA-system supplier), all necessary testing tools and maintenance personal training must be included in the purchase. It could be advantageous, if the trained personal will receive a certificate by the supplier.

It is becoming more and more common not to buy just the automation system from the supplier, but also a performance guarantee which may be **a guarantee for availability and / or life cycle cost**. Guarantee values as criteria for the penalties (and bonuses) will be agreed in the ordering phase. It must also be defined how often the penalty situation is checked.

Another possibility is to make a separate **maintenance contract** with the supplier or a certified service company. These contracts may also include penalties for unavailability.

-

5.2.2. Training

Very often all equipment and systems require that training will be provided. One example is Brazil where a customer law is stating that “the supplier will be liable for any damage that occurs as a result of misinformation”.

Training can be divided into four specific modules for the staff of the customer from the areas of Design, Assembly and Installation, Operation and Maintenance.

5.2.2.1 General Aspects

The supplier is asked to provide a complete and efficient training, thoroughly covering all pertinent aspects of the equipment, devices and accessories comprising the proposed system, including specifically the design, installation, operation and maintenance philosophy, functioning of the equipment, circuits, settings, hardware, software, etc.

All costs arising from such training may be or may not the responsibility of the supplier. The training is done using equipment and manuals to be furnished and can be carried out at the customer’s facilities or at the supplier’s plant.

The client may demand that the training is given in the customer’s language, by competent and experienced professionals, with the utilization of teaching resources and training materials in quantities as are adequate for the learning and development of the participants.

In case the training is to be held outside customer’s facilities, all expenses incurred with room, board and transportation of the participants can be at the cost of the supplier.

Any training considered by the customer to be insufficient for fulfilling the proposed objectives shall be complemented or repeated, at no additional cost.

A Training Plan shall be submitted to the customer for approval, at least a few days in advance, containing as a minimum, for each course module:

- objective;
- contents of the program;
- list of pre-requisites (if applicable);
- evaluation standards (if applicable);
- location and date;
- no. of training hours (theoretical and practical);
- expected duration of each training;
- materials and resources used;
- curriculum vitae of the instructors.

In order to allow each participant time for organizing and preparing for the formal beginning of the training, the supplier shall submit to the customer the whole material that shall be employed in the training, at least a few days before the courses are started. The participants should receive individual copies of the pertinent documents of the course.

The execution of the training involves the distribution, to all pupils involved, of documents that shall be supplemented by information, diagrams, etc., that are supportive to the instruction.

5.2.2.2 Focus and Content of the Training

The supplier shall advise the customer, regarding each course, about the contents, documentation and proficiency of the instructor. The customer shall be responsible for approving such courses.

The training shall be objective and effective; for this purpose, it is recommended that it be directed solely to the equipment and software being supplied.

The domain of the resources furnished by the supplier shall be total, allowing for a proper, and more efficient and faster utilization of the resources. The familiarity of the team with the resources shall be the largest possible.

Once the training is over, the team shall be capable of operating, developing, maintaining and expanding the System supplied, with minimum support from the supplier.

The training shall completely cover the techniques and procedures for installation, development, operation, maintenance and expansion.

Any other courses deemed to be recommended for meeting the objectives of the training, but are not included in the costumer's Technical Specification may be presented and offered by the supplier.

If deficiencies are identified in any of the courses either during or after the courses are taught, the customer normally reserves the right of requesting complementary training in order to remedy such deficiencies, without incurring any additional costs to the customer.

5.2.2.3 Number of Participants

The participants shall be designated by the costumer to attend the courses based on categories that correspond to their work's functions.

The supplier shall be requested to quote all the hardware and software training, per category of course, and to establish a basic price per maximum number of participants. The estimate of the number of the customer participants for each category is between 10 and 15 people per module.

6 Considerations for IEC61850 based SA

According to the basic features, the functions have to be specified same as before, i.e. independent of the use of IEC 61850. It has to be decided if the selection of devices is left free for the supplier or limited by some pre-selection of devices homologized by the utility. Availability figures or failure scenarios have to be discussed to get the proper communication architecture. The environmental conditions have to be specified the same as before but some of these conditions may be decisive for the communication architecture and, especially, for the communication media selection, e.g. copper cable or glass fiber.

6.1 Substation related considerations

6.1.1. Single line diagram

The basis of any substation automation system is the single line diagram of the substation. The switchgear included

- determines the process related part of the data model, i.e. the use of the Logical Nodes of type X, T, Y , S, and G (process near logical nodes modeling switchgear data mainly – see chapter xx)
- predefines together with the philosophy of the utility the control and protection functions to be applied and, therefore, the use of all other Logical Nodes of the type P, R, C, and A (logical nodes for protection, control, and automation mainly – see chapter xx).
- allocates functions and devices to bays or busbars
- provides the high level part of the data identification structure by a plant designation system like IEC 61346 (see 6.5.3 Naming convention)

The single line diagram has to include all switching devices (incl. earthing switches), power transformers and instrument transformers. It has to indicate the type of bays (overhead line bay, cable bay, etc). It can be formally described by an SSD (System Specification Description) file using SCL as provided by part 6 of IEC 61850 (IEC 61850-6).

6.1.2. Process interface

As mentioned above IEC 61850 provides also a standardized serial communication between the bay level and the process level often called process bus (physical allocation). Client-server services (e.g. commands and reports) and GOOSE messages (e.g. position indications for interlocking or trips) according to IEC 61850-8-1 may be used if applicable same as on the station bus between bay and station level (physical allocation). IEC 61850 supports besides conventional equipment connected by parallel copper wires also the use of intelligent switchgear (electronics with serial interface integrated) connected by serial communication. In addition, the sampled data service (SV) may be used for samples of current and voltage according to IEC 61850-9-x both for non-conventional instrument transformers (NCIT) and conventional instrument transformers with process near A/D conversion.
The key point for the specification is how the process interface given by the switchgear looks.

6.2 Specification of functions and the related data model

6.2.1. Functions

Functions are not standardized by IEC 61850. Therefore, the functions have to be specified as in the past. This refers especially to the behavior of the functions like response times, protection characteristics, interlocking conditions, sequences, operator interfaces, etc. The well-known functions in substation automation systems are described e.g. in [2].

Note that compliancy with IEC 61850 does not imply compliancy with the functional requirements of the user.
At abstract level, the data model and the communication services requested for this data are independent from the behavior of the functions. At implementation level the most relevant function behavior is condensed in performance requirements, at least for distributed functions.

6.2.2. Data model

If the functions are fixed, the data model of IEC 61850 specifies automatically all mandatory data and, therefore the minimum signal list, which may be checked with help of the Logical Nodes involved.
In addition, the customer specification has to list what data declared as optional in IEC 61850 are requested for the substation automation system under consideration. If both the mandatory and optional data do not cover all needs determined by strategies for operation, protection and maintenance and requirements of the existing overall EMS/Scada system, the missing data have to be listed for extensions to be offered by the system provider if possible. The data model is given in part IEC 61850-7-4 and part IEC 61850-7-3.
If the data are specified as signal list only the mapping to the data objects of IEC 61850 has to be done by the system provider or integrator. Independent if the devices are pre-defined or selected in an optimization process some data may not be available. Other signals may not be needed in the solution offered. If the devices provide all requested functions at least the minimum of data needed for the functionality is provided. Very dedicated extensions may not be deliverable in any case at any time.
The grouping of Logical Nodes (LN) to Logical Devices (LD) is normally given by the product providers. The names of the LDs are not standardized in IEC 61850 and, therefore, also normally given or at least pre-defined by the product providers. To get an unique definition of all data and a clear reference to the switchgear at least a part of the LD name has to be configurable, e.g. for a functional or IED definition related to the single line of the substation according to some substation or plant designation system. IEC 61850 recommends using the designation system according to IEC 61346. Non-standardized designation systems may be in use by the utilities. Their dedicated requirements have to be stated (and later negotiated and agreed) in a naming convention.

6.2.3. Naming convention

The identification of data according to IEC 61850 is done with two fields, i.e. the LNName field (Logical Node Name) and the LDName field (Logical Device Name).
The LNName field contains Logical Nodes with Prefix and Postfix, Data and Attributes. Since Logical Nodes, Data and Attributes are defined in the standard IEC 61850 their naming has to be unchanged part of the naming convention. It may not be mentioned explicitly since it is implicitly given by the request for a system conformant with IEC 61850. Same holds for naming extensions, which have to be defined according to the strict extension rules including name spaces, Extensions should be reusable by the supplier also beyond the project under specification.
The LDName field contains data for the identification of the data in the substation. Therefore, most entries are needed for the plant (substation) designation system but some few may be predefined by the supplier. This field has to be changeable with data from the system engineering tool.

6.3 Communication related issues

6.3.1. Time synchronisation

The time synchronization requirements have to be specified if not yet done in the function specification above. Time synchronization requirements may be stated qualitatively in words, formally defined by the synchronization classes according to IEC 61850-5. Two basic levels of requirements for time synchronization are applicable:

- About 1 ms for the events reported
- About 1 ms for sample values and phasors

The classes regarding time synchronization are defined in IEC 61850-5 and should be used for uniformity reasons.
The system provider or integrator has to support these synchronization requirements by proper device selection and clock integration.

6.3.2. Services

Performance figures, availability figures or failure scenarios, and the synchronization requirements (dedicated service) determine services (defined in IEC 61850-7-2) not yet pre-defined by the data to be transmitted according to the data model.
Special for IEC 61850 are the dedicated services GOOSE and SV for time critical information. If there are choices or options in the standard, services may be specified also directly. Such an explicit specification may impose constraints against system optimization.

7 Weighting of requirements - evaluation and comparison of different substation automation systems

7.1 *The first stage - specification*

The first stage of evaluation and comparison of different substation automation system designs must be carried out when the utility is setting technical and functional requirements for the equipment, system and services, i.e. when the utility is writing down the specification. This stage of evaluation process is important for one to be able to set realistic and justified requirements and to point out to the bidders which features are considered to be the most important from the utility point of view.

7.1.1. Technical and functional requirements

As a preparatory work, the utility must carry out the following tasks:

- Functional specification to decide which are the necessary functions and their performance criteria.
- Set development goals for new features and functionality (e.g. improving data access).
- Risk and fault analysis for faults both in primary system and in secondary system. Even in a fault of the substation automation system the critical functions of the system must be available and functioning. This analysis helps to choose architecture and redundancy.
- Define interfaces to existing systems (SCADA, communication networks, etc.).
- Describe the type of project. Requirements and thus the evaluation process may differ considerably depending on the nature of the project:
    - renewal of the whole system,
    - a single new substation,
    - extension of a substation,
    - refurbishment, etc.

The requirements following from the above must be checked against the possibilities of current technologies and standards. For this reason, a review of available technologies is in place. This may include information gathering both from manufactures and from other utilities (references, experience from previous projects). After this review it is possible to set requirements on realistic basis:

7.1.2. Basic requirements for the system

These are obligatory requirements for functionality, extendibility, maintainability, interoperability, interfaces to user’s systems, reliability, performance, etc. (chapters 4.1 - 4.3 as reference)

7.1.3. Options

- because of lack of information (price, feasibility) a cost/benefit analysis may not be possible until tenders are available, and therefore the need of a certain function is resolved later
- it is also possible to request alternative solutions

At this stage it is also important to think out which of the features and performance requirements are decisive and which are negotiable. Also, if weighting factors are to be used, they should be set here.

7.1.4. Project management requirements

The utility must define resources and abilities of its own staff to decide the portion of in-house work and out-sourcing. As a result, responsibilities between the supplier / system integrator and the customer can be defined in the following fields and their sub-items:

- engineering
- erection
- testing
- operation
- maintenance
- co-operation with parties involved (switchgear supplier, …)

If the primary system supplier and the secondary system supplier are not the same, it is especially important to clarify who is the system integrator and thus responsible for the interface between the switchgear and the substation automation system.

Utility's documentation system (CAD) defines requirements for documentation.

Frame for the time schedule must be drawn.

Risks and financial resources must be analyzed to set commercial conditions, delivery terms, terms of payment, penalties, warranty conditions, etc.

7.2 The second stage - evaluation and comparison of tenders

The second stage of evaluation is needed when utilities are selecting between tendered systems. The selection will be made between those tendered systems which fulfill the requirements of the specification by taking into account the quality of the supplier (experience, references) and the price. In a more enhanced evaluation process the total life time economy is calculated, which includes added values, life cycle cost and risk analysis. In many cases it is difficult to quantify the performance of the equipment in monetary values, and thus some sort of scoring system with weighting factors may be more practical.

7.2.1. Basic steps

The first step is to check if tendered systems are fulfilling the requirements. In this phase it would be convenient if it is already beforehand (in stage one) clarified which are the obligatory requirements and which issues are negotiable.

The second basic issue is to evaluate project-specific items to see if it is possible to carry out the project according to the preliminary plan. This includes analysis of risks, critical time schedules, reliability of the supplier, project plan for engineering, FAT, erection, commissioning and SAT.

The third set of issues is economy related: price and commercial conditions including delivery terms, terms of payment, warranty conditions, etc. The differing commercial conditions must be valued to equalize the tenders.

7.2.2. Added values

Added values should be calculated at least for the optional functions and new features offered. This should be straight forward if there is a price for them in the tender. However, in many cases the value of a particular function is not easy to quantify. The numerical technology makes possible the implementation of several functions that were previously either too costly to consider or technically not feasible. These functions may not have a separate price if they are included in the basic system. The value of such a function has to be evaluated in some other way.

Two methods of calculating the added value may be used. The first is based on replacing the integrated software functions with stand-alone (conventional) equipment (e.g. oscillographic recorders) and the other on evaluating the data provided by these functions (e.g. how many interruptions can be prevented based on disturbance recorder data). In both cases both the investment and the yearly benefits and costs has to be calculated.

What makes the evaluation more difficult is the fact that, paradoxically, to achieve the overall benefits from the utility point of view, the cost of substation automation systems - and other related information technology based systems, SCADA etc. - may increase. Effective utilization of data also requires stronger employment of condition based maintenance and asset management concepts. The main conclusion here is that substation automation systems must not be evaluated as independent units but as a part of utility's other operations.

Examples of added values of improved and new functions

(1) Numerical technology allows complex protection functions to be implemented at a reasonable price. Today a non-switched or even a full scheme distance protection can be purchased at about the same price as a conventional switched distance protection relay a few years ago. Differential protection or current comparison protection for transmission lines with a serial communication link to the opposite substation is quite inexpensive compared to the past solutions, especially if a multiplexed link is used. With dedicated optical fibers the cost is higher, but anyhow this technology makes it possible to use comparison protection where it previously was not feasible.

The effect of better performance of protection is very difficult to quantify. The effect on interruptions or system stability is very much system dependent and even case dependent and thus universal precept cannot be given. Each case has to be calculated separately.

(2) One of the major improvements brought by modern numerical protective relays and substation automation systems is fault recording. Wave form recordings together with the substation event log offer great assistance in post fault analysis. Disturbance recording is now on a whole new level, especially in the medium voltage systems where oscillographic recorders have not been feasible for economical reasons.

Information technology facilities allow access to the information produced by the numerical equipment. With the aid of this additional and more detailed information it should be possible to find false settings, defects in protection schemes, etc. This makes it possible to take preventive actions before these defects cause malfunctions and unnecessary interruptions.

As a consequence of the above mentioned improved performance, a reduction in undelivered energy per year may be counted as a benefit for the system.

7.2.3. Life-cycle cost (LCC)

Life-cycle cost (LCC) includes the investment cost, added values, operating and maintenance costs. In this calculation the expected life-time is one important parameter. Fully numerical systems have been in operation less than 15 years, so the applied lifetimes are presumptions. It is generally accepted, though, that the life-time of a numerical system is much shorter than that of a conventional system. A peculiar trend is that while the expected lifetimes of secondary systems are decreasing from 30 years to 15-20 years, the lifetimes of primary components are increasing from 30 years to 40-50 years. The consequence is that primary and secondary systems are renewed at different paces. This sets high requirements for the interface between these two. Another consequence is that more often secondary systems have to be installed, commissioned and tested on operating and energized substations. This leads to an increasing amount of test related effort and costs.

7.2.3.1 Investment cost

The following cost components have to be taken into account:

- Secondary system hardware, software and wiring divided into portions of the substation automation supplier and the customer. The latter includes all hardware and wiring that is not included in the substation automation delivery by the supplier.
- Substation space cost, relating more specifically to the space requirement for the relay room.
- Erection cost of the system, divided into portions of the supplier and the customer.
- Customer's engineering cost.
- Supplier's engineering cost (may include also in the first sub-item).
- Software for engineering, testing, diagnostics and communication. A great portion of the software is included in the software of the first sub-item.
- Testing including pre-FAT, FAT, commissioning, and SAT, again divided into portions of the supplier and the customer.
    - Training of customer's staff.

In some cases also the investment cost of the communication links outside the substation may have to be included. If the communication network operations are outsourced and the links are rented, this cost is part of the annual costs.

7.2.3.2 Operating costs

Numerical systems allow gathering large amounts of data. This data needs to be transferred further via powerful communication links and then be processed, stored and analyzed by utility's staff. Improved transmission line protection also needs more communication links between substations. These are extra costs compared to the conventional systems. Especially the cost of the numerous communication links may have considerable effect on life cycle cost.

There are also several other components in the operational costs. Their impact, however, is relatively small in proportion.

Impact of substation automation system on the operating cost of the electrical network is included in added values, see 6.2.2.

7.2.3.3 Maintenance costs

The control and monitoring part of the substation automation should need very little maintenance. Maintenance cost consists mainly of corrective actions in cases of defects in software (version upgrades) or hardware (component replacement). Extensions etc. in the substation also may create needs to update the secondary system.

The utility should maintain the ability to perform these corrective and updating actions, either by its own staff, or by after sales services from the manufacturer.

In the first half of the 1990's these systems were still in the early development stage. For this reason, in history there have been many - from the user's point of view unnecessary - version upgrades caused by defects in the system software. After these version upgrades the systems may have shown unstable operation, which in turn has created a need for additional testing of these systems on energized substations. The most recent implementations, however, are in many ways more matured and it can be seen that the maintenance cost is gradually reaching the initially predicted level.

Inspection and regular check of safety related components and their inter-related functions (protection – circuit breaker) will be necessary from time to time according to the safety rules. In numerical systems the maintenance cost is reduced because self supervision makes it possible to lengthen the test interval. For instance, test interval of six years could be applied instead of three years applied to conventional protection systems.

7.3 Weighting of requirements

Decision-making tools are needed, especially if the compared systems have somewhat equal investment costs.

Life cycle cost is in itself a good total performance measure of a substation automation system, if all cost components can be included. The problem is that the calculation of LCC is more or less an estimation with many uncertainties.

Sometimes it is more convenient to use qualitative measures, i.e. weight the different performance aspects of the systems. Weighting factors may be different from case to case. In a case of a critical substation (e.g. irreplaceable power plant connection) you do not want to risk the time schedule and planned outage time. In that case there is no room for experiments and R&D, but instead well-proven systems and equipment that have been on the market and in operation for some while are preferred even though newest developments could offer attractive features. For a less critical substation (e.g. distribution with an alternative feeding direction) you may experiment some new functions and features and take more technology risks.

If qualitative measuring is used, it is fair that the selection criteria and weighting factors are pre-defined.

Examples of comparison:

Example 1: Price

	Supplier 1	Supplier 2	Supplier 3
System price			

Table 7-1 Weighting of requirements – Price

Example 2: Investment cost

	Supplier 1	Supplier 2	Supplier 3
Investment cost			

Table 7-2 Weighting of requirements – Investment Cost

Example 3: Life cycle cost

	Supplier 1	Supplier 2	Supplier 3
Investment cost			
Operating cost			
Maintenance cost			
Added values			
Total cost			

Table 7-3 Weighting of requirements – Life cycle cost

Example 4: Qualitative comparison with point scoring and weighting factors

	Weight	Supplier 1	Supplier 2	Supplier 3
Investment cost				
Operating cost				
Maintenance cost				
Added values				
Life cycle cost				
Technical merits				
Risk assessment				
Project management				
Expandability				
Scalability				
Interchangeability				
SW&HW version management				
Interoperability & compatibility to user's systems				
Accordance with standards				
Engineering tools				
Diagnostic tools				
Testing tools				
Services				
Documentation				
Quality assurance				
Certificates & type tests				
References				
Experience				
Total scoring				

Table 7-4 Weighting of requirements – Qualitative Comparison

8 Conclusions and recommendations

When preparing a specification for SA, it is very important to have a proper structure that covers all requirements of a customer in terms of functionality, performance, availability and efficient project management. To be able to make a proper evaluation of the different offers, the requirements in the specification shall be easy to measure and to compare. Thus a simplified structure with clear, straightforward requirements will help to provide an optimal link between the customer’s needs and the evaluation procedure.

There are different possibilities to consider the new global standard IEC 61850 in the specification for SA. The most preferred way is to focus on the functionality and to define e.g. IEC 61850-8-1 for the station bus without defining further details on the protocol implementation itself. When including more details concerning IEC 61850 in specifications, it is important that the basic features and limitations of the standard are clearly understood. It also bears the risk that too many details might jeopardize the efficiency of the project execution due to their focusing on bits and bites rather than on functional and related system issues.

The weighting of the requirements and the evaluation of the different offers shall take into account all aspects that are relevant for a project. The base is given by the customer’s specification, but apart from that, also other factors need to be considered, like economics-related items and qualitative evaluation. It is also important for the evaluation that the substation automation system is considered as part of the utility’s operations. At the end, the highest overall ranking of all items assessed and weighted during the evaluation process shall be used for the comparison of all offers.

A Terminology

Bay (IEC 61850)
A substation consists of closely connected subparts with some common functionality. Examples are the switchgear between an incoming or outgoing line and the busbar, the bus coupler with its circuit breaker and related isolators and earthing switches, the transformer with its related switchgear between the two busbars representing the two voltage levels, the diameter in a 1 ½ breaker arrangement, etc. These subparts comprise very often a device to be protected like a transformer or a line end, and the control of its switchgear has some common restrictions like mutual interlocking or well-defined operation sequences. The identification of such sub-parts is important for maintenance purposes (what parts may be switched off at the same time with a minimum impact on the rest of the substation) or for extension plans (what has to be added if a new line shall be linked in). These subparts are called “bays” and managed by devices with the generic names “bay controller” and “bay protection”. They represent an additional control level below the overall station level that is called “bay level”.

Configuration (of a system or device) **(IEC 61850)**
A step in system design: selecting functional units, assigning their locations and defining their interconnections.

Configuration list (IEC 61850)
An overview of all compatible hardware and software versions of components and IEDs including the software versions of relevant supporting tools operating together in a SAS-product family. Additionally the configuration list contains the supported transmission protocols for communication with IEDs of other manufacturers.

Conformance test (IEC 61850)
Check of data flow on serial links in accordance with the standard conditions concerning access organization, formats and bit sequences, time synchronization, timing, signal form and level, reaction to errors. The conformance test can be carried out and certified for the standard or specially described parts of the standard. The conformance test should be carried out by a certified organization.

Device
A mechanism or piece of equipment designed to serve a purpose or perform a function. (IEEE Std 100-1996, IEEE Dictionary of Electrical and Electronic Terms); e.g., breaker, relay, or sub-station computer.

FAT (Factory acceptance test) (IEC 61850)
Customer agreed functional tests of the specifically manufactured SAS or its parts using the parameter set for the planned application. The FAT must be carried out in the factory of the manufacturer by the use of process simulating test equipment.

Function (IEC 61850)
Tasks, which are performed by the substation automation system. Generally, a function consists of logical nodes, which exchange data, with each other. Depending on the function definition functions itself exchange data with other functions. A function is called distributed when two or more logical nodes that are located in different physical devices perform it.

IED (Intelligent Electronic Device) (IEC 61850)
Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source. (e.g., electronic multifunction meters, digital relays, controllers) An entity capable of executing the behavior of one or more specified LNs in a particular context and delimited by its interfaces.

IED-parameter set (IEC 61850)
Set including all parameter values needed for the definition of the behavior of the IED and its adaptation to the substation conditions. Where the IED has to operate autonomously, the

IED-parameter-set can be generated without system parameters using an IED-specific parameterization tool. Where the IED is a part of the SAS the IED-parameter set includes system parameters, which must be coordinated by a general parameterization tool at the SAS-level.

Interchangeability (IEC 61850)
The ability to replace a device from the same vendor, or from different vendors, utilizing the same communication interface and as a minimum, with the same functionality, and with no impact on the rest of the system.

Interface (IEC 61850)
A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate.

Interoperability (IEC 61850)
The ability of two or more IEDs from the same vendor, or different vendors, to exchange information and use that information for correct co-operation.

Parameters (IEC 61850)
Variables, which define the behavior of partial functions of the SAS and its IEDs within a given range of values.

Remote Terminal Unit (IEC 61850)
Typically an outstation in a SCADA system. An RTU acts as an interface between the communication network and the substation equipment.

SAS-installation (IEC 61850)
The concrete instance of a substation automation system consisting of different interoperable IEDs of one or more manufacturers

SAS-parameter set (IEC 61850)
All parameter values needed for the definition of the behavior of the overall SAS and its adaptation to the substation conditions. The SAS-parameter set includes the IED-parameter sets of all participating IEDs.

Site acceptance test (IEC 61850)
Verification of each data and control point and the correct functionality inside the SAS and between the SAS and its operating environment at the whole installed plant by use of the final parameter set. The SAT is the precondition for the SAS being put into operation.

System (IEC 61850)
A set of interrelated elements considered in a defined context as a whole and separated from its environment. The logical system is a union of all communicating functions performing some overall task like “management of a substation”. The physical system is composed of all devices and the interconnecting physical communication network (commonly fiber optics). The boundary of a system is given by its logical or physical interfaces. Examples are industrial systems, management systems, information systems, etc. Within the scope of this standard, system refers to substation automation systems always if not mentioned otherwise.

System life cycle (IEC 61850)
Has two specific meanings:

1. The manufacturer’s system life cycle is the time period between the start of the production of a newly developed SAS-product family and the announcement of the product family discontinuation, including its compatible IEDs.
2. The purchaser’s system life cycle is the time period between the commissioning of the SAS-installation mainly based on a SAS-product family and the decommissioning of the latest SAS-installation from the same family.

System parameters
Data, which define the co-operation of IEDs in the SAS. They are especially important in the definitions for:

- configuration of the SAS
- communication between IEDs
- marshalling of data between IEDs
- processing and visualization of data from other IEDs e.g. at the station level.

System test
Check of correct behavior of the IEDs and of the overall SAS under various application conditions. The system test marks the final stage of the development of IEDs as part of a SAS-product family.

Test equipment
All tools and instruments which simulate and verify the input/outputs of the operating environment of the SAS such as switchgear, transformers, network control centers or connected telecommunication units on the one side, and the serial links between the IEDs of the SAS on the other.

Type test (IEC 61850)
Verification of correct behavior of the IEDs of the SAS by use of the system tested software under the environmental test conditions corresponding to the terminology given in IEC61850-2 should be used.

B Definition of acronyms

Term	Definition
ACSI	Abstract Communication Service Interface
AEP	American Electric Power
AMR	Automatic Meter Reading
AMRA	Automatic Meter Reading Association
API	Application Program Interface
ASDU	Application Service Data Unit
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
AVR	Automatic Voltage Regulator
BCPU	Bay Control and Protection Unit
BCU	Bay Control Unit
BPU	Bay Protection Unit
CAD	Computer Aided Design
CASM	Common Application Service Models
CB	Circuit Breaker
CBS	Cost Breakdown Structure
CC	Control Centre
CD	Compact Disk
	Committee Draft
CDV	Committee Draft for Vote
COSEM	Companion Specification for Energy Metering
CT	Current transformer
DBMS	Database Management System
DLMS	Device Language Message Specification
DMS	Distribution Management System
ECT	Electronic Current Transducer
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
E/F	Earth fault
EM	Electromagnetic
EMS	Energy Management System
EPA	Enhanced Performance Architecture
EPRI	Electric Power Research Institute
ET	Electrical Current Transducer
EVT	Electronic Voltage Transducer
FDIS	Final Draft International Standard

Term	Definition
FMS	Fieldbus Message Specification
FYCF	Five Year Cost Forecast
GIS	Gas insulated switchgear
GOMSFE	Generic Object Models for Substation & Feeder Equipment
GPS	Global Positioning System
GUI	Graphical User Interface
HMI	Human machine interface
HV	High Voltage
ICCP	Inter-Control Centre Communications Protocol
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineers
I/O	Input / Output
IRIG-B	Inter-Range Instrumentation Group (Format B)
IS	International Standard
ISDN	Integrated Service Data Network
ISO	International Standardization Organization
LAN	Local Area Network
LCC	Life Cycle Cost
LCCF	Life Cycle Cost Forecast
LV	Low Voltage
MMI	Man Machine Interface
MMS	Manufacturing Message Specification
ms	Milliseconds
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MU	Merging Unit
MV	Medium Voltage
NPV	Net Present Value
O/C	Overcurrent
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OSI	Open System Interconnect
PC	Personal Computer
PLC	Program Logic Controller
PSTN	Public Switched Telephone Network
R&D	Research and Development
RAID	Redundant Array of Independent Disks
RFQ	Request for Quote

Term	Definition
ROM	Read Only Memory
RRM	Report Reference Model
RTU	Remote Terminal Unit
SAS	Substation Automation System
SBO	Select –Before-Operate
SC	Secondary Converter or Study Committee
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Configuration Language
SCSM	Specific Communication Service Mapping
SOAP	Simple Object Access Protocol
TASE	Telecontrol Application Service Element
TC	Technical Committee
TCP/IP	Transmission Control Protocol/Internet Protocol
TR	Technical Report
TYCF	Ten Year Cost Forecast
UA	User Association
UCA	Utility Communication Architecture
ULTC	Under load tap changer
UML	Unified Modeling Language
VT	Voltage transformer
WAN	Wide Area Network
WBS	Work Breakdown Structure
WD	Working Draft
XML	Extensible Markup Language

C References

[1] CIGRE Paper 34-104 *Digital communications for power system protection: security, availability and speed*

[2] CIGRE Paper 34-110 *Present state and trend of application of communication including LAN to protection and substation control*

[3] IEC 61850 Standard

[4] CIGRE WG 13-09. *Monitoring and Diagnostic Techniques for Switching Equipment*

[5] CIGRE WG 34-07 *The automation of new and existing substations: why and how, Report*

[6] IEEE Transactions on Power Delivery, Vol 16, No1, January 2001 : *The impact of functional integration on the Reliability of Substation Protection and Control*

[7] International Electrotechnical Vocabulary VEI 191 International Electrotechnical Commission June 1988.

[8] Merlin GerinTechnical Report 134 : *"Approche industrielle de la sureté de fonctionnement"* H. Krotoff

[9] Canadian Electrical association Power system Planning: Fundamental reliability consideration in the design, manufacturing and application of multifunction digital relays reliability consideration in the design, manufacturing and application of multifunction digital relays

[10] ISBN 3-85758-951-5 Substation Automation Handbook

D Applicable Standards

- Environment / Type test standards
- Communication standards

	Essay	Main protection	Station level PC / Work station	Bay level controller	Station level controller	IEC 61000-6-5 (reference)
	Insulation and isolation tests					
	Continuity of the masses	=		=	=	
	Isolation resistance	=		=	=	
	Rigidity dielectrically to 50 Hz	=		=	=	
	Shock tension	=		=	=	
	Influence essays of the environment on equipment					
	Degree of protection of the casing	>				
	DC power supply influence – amplitude	=		>	>	
	DC power supply influence – amplitude domain limit	=		=	=	
	DC power supply influence – AC component			>	>	
	DC power supply influence – voltage collapse	=		<	<	
	DC power supply influence – short interruptions	=		=	=	
	DC power supply influence – interruption / gradual power on			=	=	
	DC power supply influence – fast load changes					
	AC power supply influence – amplitude domain nominal					
	AC power supply influence – frequency variation					
	AC power supply influence – third harmonic					
	AC power supply influence – voltage collapse					
	AC power supply influence – short interruptions					
	AC power supply influence – long interruptions					
	Ambient temperature influence and of its variations	=	=	>		
	EMC - Electrostatic disposals	<	=	=	=	=
	EMC - Electromagnetic radiated field HF	=	=	=	>	>
	EMC - Fast transient	=	=	=	=	=
	EMC - Lightning waves energetic	=		=	=	=
	EMC - Driven disruptions, induced by the fields HF	=		=	=	=
	EMC - Oscillatory absorbed waves	=	=	=	=	=
	EMC - Magnetic field to industrial frequency	>		=	=	=
	Storage cold (essays of robustness)	>	=	>	=	
	Storage in dry heat (essays of robustness)	=	=	=	=	
	Storage with heat cycle humid (essays of robustness)	=	=	<	<	
	Endurance to vibrations (essays of robustness)	=		=	=	
	Seismic	=				
	Influence essays of the equipment on the environment					
	Absorbed power in permanent system		=	=		
	Disruptions EMC radiated and driven by equipment	=		=	=	
	Start-up current (continuous current)	=	=	=	=	
	Currents form check			>	=	
	Characterization essays					

	Essay	Main protection	Station level PC / Work station	Bay level controller	Station level controller	IEC 61000-6-5 (reference)
	Storage time of volatile data					
	Polarity inversion			=	=	
	Absorbed power of analogue inputs	=		=		
	Characteristic of the input / output	=		=		
	Continuous current rating of outputs			=		
	Continuous overload rating of analogue inputs	=		>		
	Frequency magnitude variation of the analogue inputs					
	Harmonic magnitude of the analogue inputs	>				
	Integrity					
	Non essays take into account in the Specification					
	DC power supply – tension to the frequency of the network					x
	EMC - Magnetic field impulsion			x	x	
	EMC - Oscillatory magnetic field drop shot			x		
	AC power supply - harmonic generated by the equipment					
	Check behavior to the current circuit					
	Absorbed power of installed auxiliary power supply					
	Absorbed power of installed analogue inputs					
	Behavior to vibrations	x		x	x	
	Behavior to mechanical shocks	x		x	x	
	Tremors	x		x	x	
	Free fall			x	x	
	Essay climate heat accelerated humid (60068-2-4) (does not exist anymore)					
	Essay climate heat continuous humid (60068-2-3 / 2-56) (does not exist anymore)					
	Essay climate composite humid heat and temp (60068-2-38)					
	Essay climate composite temperature (power switched off) (60068-2-14)					
	Extended functioning			x		
	Resistance to the heat and to the fire (60695-10-.. and 60695-2-….)					
	Mechanical resistance checks of the boundaries					
	Surtension (phase/neutral - phase/phase)					

Legend

> : *Requirement of the superior quoted document to the norm (comparison in relative for the case or the norm does not cover the requirement)*

< : *Requirement of the inferior quoted document to the norm*

= : *Identical requirement (nc: not conformant)*

x *Specified essay usually for the quoted equipment but not in the norm*

Not applicable

Not mentioned or not applicable

Table D-1 Applicable Standards – IED mapping

E Basic review on Dependability (Reliability definitions and parameters)

E.1 Reliability parameters

The following table clarifies the definition of main used reliability terms and parameters:

- **Availability:** Percentage of time for which the system functions correctly.
- **Dependability:** Generic term which combines the independent variables of reliability, availability, maintainability and safety.
- **Dependability study :** Based on the functional analysis, this is the analysis of the failures that can occur in a system
- **Maintainability:** The aptitude of a system to be repaired quickly.
- **Reliability:** The aptitude of a system to function correctly for as long as possible.
- **Safety:** The aptitude of a system to not put people in danger.

MTTR: Mean time to repair	Average time that is required to detect and repair a failure. It applies to all components in the system
MTTF: Mean time to fail	Average time until a system failure occurs according to the database standards - Practical: In best case the MTTF calculation is based on field return data - Theoretical**:** By new products the MTTF is calculated according the MIL-standard (MIL217 / UTE 60810) or - Ratio**:** The practical MTTF can be expected about 3 times higher than the theoretical
MTBF: Mean time between failure	Mean time from one failure to the next failure including detection and repair time. MTBF=MTTF+MTTR MTBF=MTTF when MTTR<<MTTF
MTTF for repair: Mean time to the next repair	This is based on the sum of all components ignoring redundancy. It corresponds to basic reliability (mean time between maintenance actions) according military standard.
MUT (Mean Up Time):	the average time of correct operation between two failures in a repairable system.
MDT (Mean Down Time):	Average time for which the system is not available. It includes the time to detect the fault, the time for the maintenance service team to get to the fault, the time to get the replacement parts for the equipment to be repaired and the time to repair.
Availability / no component repair	Is calculated from mission MTTF of the system and MTTR, i.e. it shows availability, if repair is done only after the mission (i.e. all redundant components) has failed. A = MTTF / (MTTF+MTTR)
Availability / repair	Is calculated from the availability of all components, i.e. assuming that each component is repaired directly after it failed within MTTR. This is the mission availability if repair actions of components are taken immediately. A(1,2) = MTTF(1,2) / (MTTF(1,2)+MTTR) A = A(1) * A(2) if 1 and 2 in series A = A(1) + A(2) - A(1)*A(2) if 1 and 2 in parallel

Table E-1 Reliability parameters definition

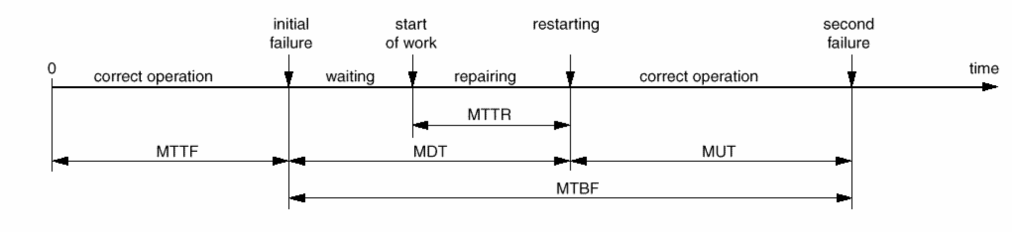

Figure E.1-1 Relation between different reliability parameters

The basis of all reliability calculations is in general:

- The MTBF figures of involved system items and / or sub items. it is recommended to assess reliability at the “lowest possible” level - corresponding to the smallest interchangeable item within the bonds of the first maintenance levels
- The MTTR figures of system components: the requirements depend on the internal utility maintenance outsourcing strategy: this data is relevant only if the manufacturer is in charge of the first level maintenance on the system. Availability requirements are useless if the utility is involved in the repair. In this case specification shall include qualitative recommendation such as: component easy to plug or unplug, accessibility test functions; tools to be able to identify solve the problem, quality of training. MTTR shall thus be optimized.

E.2 Reliability Databases

- UTE 60810 (new 2000 version)
- Military Handbook 217^{E} DoD (U.S.A.) October 1986. This database is still used but is outdated and is replaced by UTE 60810

E.3 Reliability standards

- IEC 300 (Dependability management),
- IEC 1069 (sûreté des systèmes programmables),
- IEC 61508 (Functional safety of electronical /electronic programmable electronic safety-related systems),
- IEC 1164 (Reliability growth)
- IEC 61124 (Reliability testing)
- IEC Standard 812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).

E.4 Methodology guidelines

The system dependability assessment is based on a dependability study made by the manufacturer. The methods to assess the dependability follow commonly a structured multi steps approach: functional, hardware / software, fault tolerance.

functional dependability

For the manufacturer the work consists in establishing Hardware and system / subsystems models with a description of functional allocations. Often used are

- Reliability oriented software tools
- Reliability databases
- logical methods such as reliability flowcharts, allowing assessment of reliability block by block, methods based on minimum assemblies with event tress, methods based on stochastic processes such as Markov grafs, FMECA : failure mode effect and criticality analysis

selection criteria	fault tree diagram	Markov graph	Pétri network
interaction of the operating mode in modelling	resolution impossible or false depending on the algorithms used	under certain conditions, resolution can be impossible or false depending on the algorithm used	suitable
numerical dispersion of data	resolution impossible or false depending on the algorithms used; no problem if simulation	under certain conditions, resolution can be impossible or false depending on the algorithm used	suitable
the timing of the failures is important	no	suitable	suitable
estimate involving rare events	simulation time which can be prohibitive, no problem in the case of analytical resolution	suitable	simulation time which can be prohibitive
estimate of:			
■ MUT	-	suitable	suitable
■ MTTF	suitable	suitable	suitable
■ D(t)	-	suitable	-
■ D(∞)	suitable (analytical calc.)	suitable	suitable
■ average D at t	suitable (simulation)	-	suitable
■ MTTR	-	suitable	suitable
■ λ_{eq}	-	suitable	suitable

fig. 21: criteria used to select the type of modelling used.

Figure E.4-1 Modeling selection criteria's for availability calculation

These tools allow

- to identify components that are critical for operation
- to orient and check design choices

This functional approach based on "unwanted events" objectives, is a convenient way to optimize the solution and to orient configuration choices (redundancy, functional allocations).