Cigré SC 34 colloquim
October 12-13, 1999
Florence
Italy

The Single Failure Criterion in Integrated Protection and Local Control Systems

by

Bertil Lundqvist* Stig Holst

ABB Automation Products, Substation Automation Division
(Sweden)

Abstract
To really take advantage of the modern microprocessor technology, the third generation of microprocessor based protection and control equipment has been designed with a platform concept. The platform consists of a number of hardware modules for analogue inputs and A/D conversion, a main processing module, dc/dc supply module and a number of flexible input and output modules. Communication modules, for example a 56/64 kbit communication module for differential protection is also included in the platform. The platform incorporates an extensive library of protection and control software functions, monitoring functions and communication functions.

Thus**,** it is **technically possible to integrate the protection and control functions**, for example in a bay terminal for a power line. It is easy to see that the different control and protection functions are using the same information from the primary equipment and have many similarities, or that some functions are redundant. By co-ordinating these main functions and integrating them when possible, the functionality and performance of the control and protection system can be increased. The integration can both decrease the required wiring and space and increase the overall reliability and availability together with reduced investment and operation cost. Of paramount importance is then how the basic power system requirements on dependability, security, fault tolerance and availability can be achieved.

One main concern, which is discussed, is how reliability and availability can be maintained when many functions are integrated in one terminal, and which functions require redundancy from system reliability point of view. The impact on self-supervision on availability and requirements on redundancy is also discussed. **The single failure criterion** is used for the assessment of system dependability and security.

.

1. INTRODUCTION

The operation of a power system includes a large number of functions. The functions can be divided in station control- and network control functions, depending on where the functions are located. Example of the station control functions is:

- Protection of the high voltage equipment
- Control and interlocking of switching devices
- Condition monitoring and alarm
- Status indication and event recording
- Autoreclosing and automatic restoration of operation
- Synchrocheck, phasing and synchronising
- Fault location and disturbance recording
- Load shedding

The network control functions are mainly:
- Voltage control
- Frequency control
- Load and energy management

To perform these functions, the network control centre has to execute functions in the different power- and sub-stations in the network. This requires a SCADA (Supervisory Control and Data Acquisition) function in the different stations.

In a substation, all the above functions has traditionally been performed with a combination of stand- alone static and electromechanical devices, configured in a

number of separate systems. Control of switching devices, interlocking, alarm, event- and disturbance recording, protection, measuring are some of the subsystems, which all required individual wiring. Even with the introduction of the first and second generation of microprocessor based protection and control equipment and computerised Substation Control and SCADA systems, this design structure has been maintained.

It is easy to see that the **different control and protection functions are using the same information** from the primary equipment and have many similarities, or that some functions are redundant. By co-ordinating these main functions and integrating them when possible, the functionality and performance of the control and protection system will be increased.

The integration can both decrease the required wiring and space and increase the overall security and availability together with reduced investment and operation cost.

2. DEFINITION OF FUNCTIONS

The different protection and control functions in a substation have to be grouped for an analysis of the overall structure. This grouping of the different functions is not associated with a physical separation of the equipment. The function groups will be used to identify the factor that influences the structure.

The function groups are defined as strict groups of functions, including all components to perform the functions as CT, PT, wiring, dc-supply etc.

The function groups below will be used:

Fault clearing sub 1
Fault clearing sub 2

The "fault clearing" includes all the functions performed by the protection equipment.

The fault clearing has to be divided into two groups if redundant (duplicated) protection is required.

Emergency control functions
This group includes all the manually or automatically performed functions to prevent abnormal power system conditions to develop into a main system component fault. The group includes alarm, metering and other functions to detect abnormal conditions.

Non-emergency control functions
This group includes all functions for operation during non-system fault and safe status conditions. Both manual and automatic functions are included for voltage and frequency control, changing of operation mode as well as other functions related to the non-disturbed operation of the station.

In this group, manual and automatic functions for restoration of the operation after a disturbance are included.

Acquisition of information for analysis
This group contains functions for acquisition, storage, transmission and presentation of information to enable the analysis of the network and the equipment performance, both during normal operation and during system fault (post fault analysis).

Energy measurement is included in this group.

SCADA function
This group includes all local functions for the remote operation of the station. Both the data acquisition and remote control functions are included.

3. POWER SYSTEM REQUIREMENT

From the control and protection structure point of view the main requirement is:

Dependability
The dependability of a function is the probability that the function will be executed correctly when wanted.

Security
The security of a function is the probability that the function will **not** be performed when unwanted.

Degradation
Degradation is the percentage of individual functions in the whole system that will be inoperative by a **single** failure in the whole control and protection system.

4. FUNCTIONAL INTERACTION

The individual functions have requirement of independence towards other functions. From the system architecture point of view, three types of independence are of interest:

Redundant relation
The redundant relation is related to the dependability of the function. The functions in a redundant relation are **not** allowed to be lost simultaneously. The relation is, of course, bi-directional.

Normally the simultaneous loss of the function is related to a single failure anywhere in the hard- or software in the system. With selfsupervision and regular maintenance testing, the likelihood for more then one failure can be neglected and **a single failure criterion can be justified.** The specification of general design criteria for two or more faults will result in very complicated and expensive designs.

A redundant relation requires individual equipment performing the functions and excludes integration in a common hardware.

Security/dependability relation
The security/dependability relation is related to the loss of security in one function and a simultaneous loss of the dependability in an other function. This relation has one direction and is not bi-directional as the redundant relation.

The security/dependability relation allows the simultaneous loss of dependability in both functions and integration is possible if counter measure is taken to avoid an unwanted function when the other function is lost.

Degradation of functions
The degradation of functions described above is a form of functional interaction.

Requirement on degradation capability will limit the degree of integration that can be allowed.

5. SYSTEM ARCHITECTURE

The main high voltage equipment in a substation can be divided in bay related and common equipment. The bay equipment can be related to a line, transformer etc. Also the control and protection functions can to a high degree be related to the different bays. The different bays are interconnected via the high voltage busbar system. The interconnection of the individual bays requires common station level control and protection functions such as busbar protection, interlocking, control of switching devices with station overview etc.

Therefore, it is natural to divide the control and protection functions in bay and station level functions.

By performing the bay functions with individual hardware equipment, the degradation is limited in case of failure in the bay equipment to one bay. In case of extension of the station, one or more bays are added together with control and protection bay-units and the necessary complementary functions on the station level. The control and protection system can thus be extended with minimum interaction and extension of the existing station level part of the system. The extension will be of utmost importance due to that practically all stations have to be extended sooner or later. The maintenance can be better performed with less risk of interaction with other parts of the station when the equipment is bay related.

At lover voltages (< 100 kV) the equipment can be integrated for two or more bays due to the lower functionality at this voltages level, but this will not change the basic bay oriented architecture. In the future, with increased capability and experience of self supervised systems, this can also be the case for higher voltages.

The main function in the bay equipment will naturally be the protection function. This protection function can for lines, capacitor banks and reactors be performed with information acquisition from the bay only. Thus the fault clearing function will not degrade for any fault outside the bay.

The protection function for a transformer is normally dependent of information from more then one bay and in this case the protection function is mostly related to the bay with the highest voltage level.

In case of one-and-a-half or two breaker arrangements, the bay function preferably is subdivided in object (line etc.) functions and breaker related functions. This will not in principal change the "bay" orientation of the individual equipment.

The functions that not can be executed fully in the bay or require information from other bays is related to a station level. The functions on the station level are busbar protection, interlocking, control of breaker and isolator (operator control), SCADA etc. Some of these functions, for example interlocking, can partly be distributed to the bay-units.

The architecture will be based on distributed intelligence, with bay and station level, to enable minimum degradation in case of a fault in the control equipment and to prepare for future extensions of the station. The structure will also simplify the maintenance work. (Reduced consequences for mistakes).

The requirement on redundancy between duplicated protections will not allow the integration of all functions in a single bay-unit. The duplicated functions must be performed in fully separate hardware. (Separate fault clearing chains)

The function Emergency Control has a redundant relation toward the protection function, due to the fact that an abnormal power system condition can develop in a main system component failure. The emergency control function includes the detection of abnormal conditions, which mainly is a part of the alarm function. Therefore the alarm function has a redundant relation to the protection function.

In a station equipped with redundant protections, the emergency control function can be integrated in one of the protection units (Multi- function terminal)

In non-redundant protection and control systems (single protection) it is very important that **the alarm function must not be lost** together with the protection function. This requires a back-up alarm system for some of the alarms, if the main alarm system is fully integrated with the protection. However, it can also be the case that this form of integration must be avoided for some alarms. The minimum functional level is that alarms for abnormal conditions that can develop into primary component failures are brought to the attention of an operator, when the protection function is lost

The security/dependability relation exists between all functions, that can change the operational status in the high voltage equipment and the protection functions. A

fault in the control equipment, that can result in an unwanted operation is not allowed to block the protection function (the unwanted operation can cause a high voltage fault). In case of fully redundant protection functions, this is not a restriction for the integration of functions, due to the fact that the two protection functions not are allowed to be lost simultaneously.

The security for functions that can change the operational status must be checked by functions like select-before-execute, and the capability of blocking this function from the selfsupervision of the protection functions to allow integration of all functions in a common bay-unit.

The functions for acquisition of information for post fault analysis have theoretically a security/dependability relation to the protection function. This relation will not exclude the integration of the disturbance recorder in the bay-protection. With bay oriented disturbance recorder, sufficient information will be available in the other bays to allow an analysis in case of a failure to operate of both the protection and disturbance recorder at a primary fault related to the bay. That type of combined faults is very unlikely and can not justify a disturbance recorder function separated from the protections.

To reduce the wiring in the station, naturally serial data communication has to be used between the different bay-units and the station level. To achieve maximum security for electrical interference on this information-bus opto fibre communication is preferred

The bus is mostly arranged as a multidrop bus with democratic access to the bus from all connected units or as a star connected physical separation down to bay level.

The bus interconnecting the bays with the station level is normally not duplicated due to that all "bay-protection" functions can be maintained also when the bus is lost. The loss of manual control of the breaker and isolators when the data bus is lost is normally compensated with an emergency control in the bay unit or a local mimic board. However, a local mimic board, which utilises the same serial communication data bus, gives almost no extra availability and if it is hardwired, it reduces the cost benefit of computerised control and protection systems.

In very important stations the station-bus can be duplicated to maintain the station level function, local operator control, with full overview of station status and the SCADA function.

The above limits for the integration for stations with or without duplicated protection functions are shoved in the Figures 1& 2.

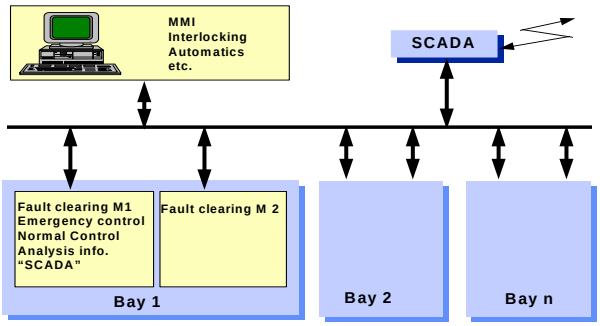

Figure 1 Maximum allowed bay integration with redundant protection (Local back up)

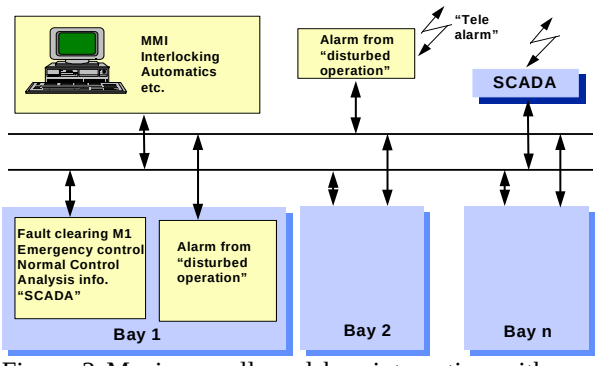

Figure 2 Maximum allowed bay integration with non-redundant protection (remote back up)

At the moment, the allowed degree of integration have not been used on voltage levels > 100 kV. Thus have for example, the bay control functions not been fully integrated with the protection. One of the reasons is that the control functions are to a relatively high degree customer specific and not standardised. The integration of the customer specific control functions in the protection equipment would reduce the cost for the system, but will require an acceptance of this concept, both from philosophical and organisational point of view.

However, not to jeopardise the fault clearing function and to allow a relevant testing, the redundant relations between the alarm and the protection function when non- duplicated protection is used is best achieved with different hardware systems.

An example of an integrated station with duplicated integrated protection and control terminals are shown in figure 3

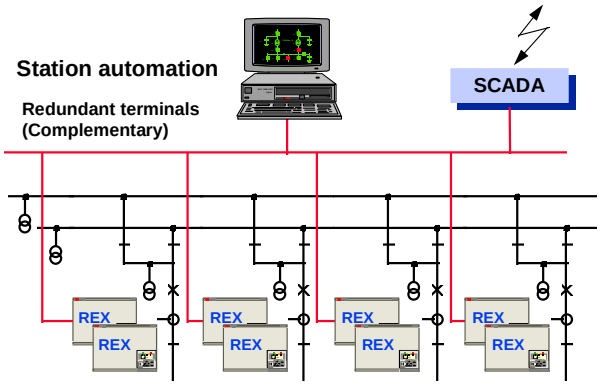

Figure 3 Integration in a 400 kV station

6. DESIGN TOOLS

The design tools has a major impact on the dependability and security of an integrated protection and control system.

An example of a design tool is graphical PC-tool, based on the international standard IEC 1131-3 (Windows)
The graphics are based on function block programming, originally designed for programmable logic controllers (PLC).
In this tool the designer get a very good overview of all internal connections between the function blocks.
The tool can be used to change an example configuration or to add new logics. The design is made with pretested function blocks for interlocking, autoreclosure etc.

The designer has also a set of logical elements, and-gates or-gates timers etc. available for design of additional logics Thus, a terminal can be tailor-made to a specific application including both protection and control functions, see figure 4.

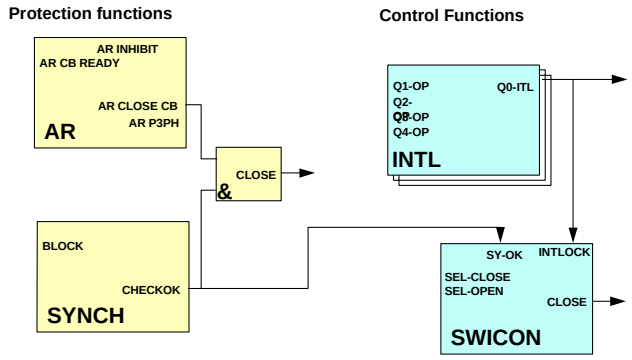

Fig. 4. Integration of protection and control

However, the testing and verification of a new configuration is extremely important. Thus an approach with a customer specific standard solution is preferable.

7. ADVANTAGES OF INTEGRATED CONTROL

The integrated control and protection system of today and for the future is a bay oriented system from the functional point of view, with distributed intelligence.

Some general statement can be considered first. Currently, the use of distributed “intelligence”, communicating via optical fibres and the use of PCs, as man-machine-interface is commonplace. Thus new developments are continuously taking place within this area, reducing the costs and increasing the performance. Further more the "new" generation of engineers are trained and familiar with this technology. The top down system used in the past is no longer appropriate, since decentralised system can more easily be adapted to future changes. It is also easy to upgrade or extend such a distributed system.

For a between a conventional substation and a substation using numerical technology (integrated functions in a distributed system), it is important to make this comparison between "mature" installations. A first trial installation of numerical technology will always be expensive.

The benefits for the "integrated" station can be summarised for short term:
- Lower engineering cost by using standardised hardware and software modules
- Lower installation cost with less cabling
- Lower commissioning cost with pre-tested modules and configuration
- Fewer cubicles requiring less space, auxiliary power and wiring.

The long-term benefits can be summarised:
- Lower operation cost with remote access to the bay level
- Increased availability with self-supervision of the whole system, giving lower interruption- and fault tracing cost
- Increased lifetime of equipment with scheduled maintenance from statistical data.

Finally several new functions and the possibility and necessity to utilise expert system in the future to reduce the operation cost will give added value to control and protection system, that can be extended with new functions within the basic structure of information handling.

8. FUTURE TRENDS

Traditional substations are built-up of separate high-voltage apparatus and protection and control components, This components require additional equipment like mirror relays , cables and other intermediate equipment to form a system solution

However, some new ideas have emerged, where the high voltage apparatus is combined in a new way, and optical current and voltage transducers are integrated in the high voltage apparatus.

The high voltage apparatus has also built-in sensors and electronics for continuous supervision of the condition of the apparatus in question. The collection of data can be utilised for maintenance on demand, i.e. when some parameter or trend indicates that a fault may develop, for example the time-travel curve of the mechanism in a breaker, or the tap changer sound in a transformer.

The built- in electronic interfaces and the current and voltage transducers are connected to a fiberoptic process bus called Power Process Highway. Thus most of the copper cables in the station can be replaced. The only copper cable required is for the power supply to operating mechanism in breakers, cooling fans for transformers etc and the electronics. The trip signals are

sent on the Power Process Highway, with a maximum delay of 1 ms.
A coupling module for 500 kV is shown in figure 5

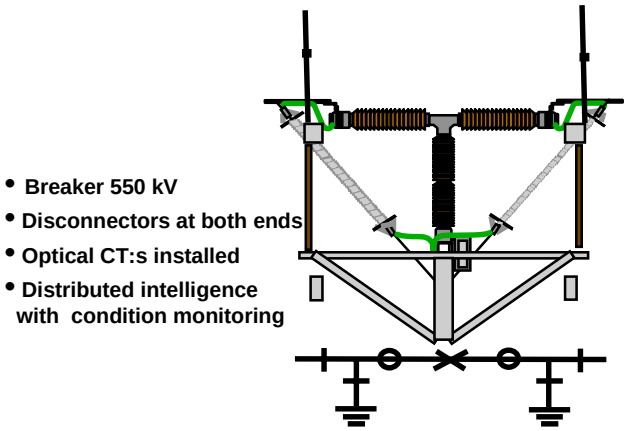

Figure 5. 550 kV coupling module

The principal design of the system is shown i figure 6.

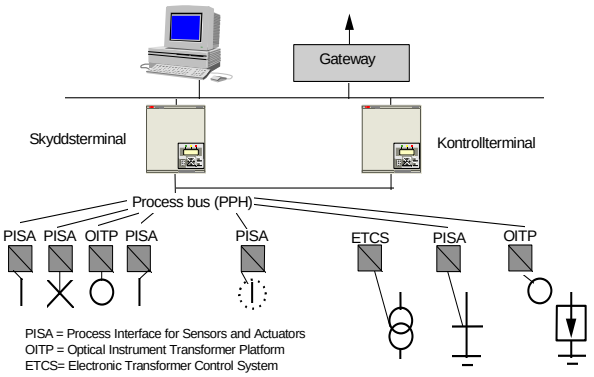

Figure 6 Principal system design

All information between the high voltage apparatus and the secondary system is carried out on the Power Process Highway

An analysis of a system according to the concept with a Power Process Highway with reference to the single failure criterion leads to the conclusion that the Power process Highway must be duplicated. However if the single failure criterion is applied with an unavailability approach, a single Power Process Highway can be adequate for most applications. The fact that the Power Process Highway is constantly self supervised can with a short time to repair give satisfactory availability for the system without duplication.

9. CONCLUSION

The functional interaction between the above mentioned function with respect to dependability and security, with the single failure criterion in mind, are important factors when assessing which function can be integrated or requires redundant equipment. Normally the simultaneous loss of the function is related to a single failure anywhere in the hard- or software in the system.

With selfsupervision and regular maintenance testing, the likelihood for more then one failure can be neglected and the **single failure criterion can be justified.** The specification of a general design criterion for two or more faults will result in a very complicated and expensive design.

10. REFERENCES

[1] L. Berglund S. Holst O. Werner-Erichsen, B. Lundqvist, “A co-ordinated digital protection and control system for transmission substations”, Cigrè 34-07, Bournemouth, UK, 1989.

[2]E. Ödmansson, C. Öhlen, “Integrated information systems; protection, substation control, network management - Available solutions on the market”, IEEE, Stockholm Powertech, Sweden, 1995.

[3] . Lundqvist, H. Kronander, A. J. Mackrell, “The integration of protection, monitoring, control and communication in modern electrical HV installations”, IEE, Conference publication No. 434, Nottingham, UK, 1997.

[4] . Degerfält, O. Kristofersson, M. Adolfsson, “The Intelligent Air Insulated Switchgear and Substations”, CEPSI, Malaysia, 1997

[5] . Jonsson, K Faber, B Lundqvist
The new paradigm in substation automation
CIGRE 34-105, Paris 1998