21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

B5-110

CIGRE 2006

Requirements of interoperable distributed functions and architectures in IEC 61850-based SA Systems

Klaus-Peter Brand, Peter Rietmann*, Tetsuji Maeda, Wolfgang Wimmer

ABB Switzerland Ltd. Power Technology Systems, Baden

Switzerland

SUMMARY

Interoperability according to the standard IEC 61850 means the capability of two or more intelligent electronic devices (IEDs) to exchange information and to use it in the performance of their functions for correct co-operation. Neither the actual definition, i.e. algorithms, nor the actual allocation of functions fall inside the scope of the standard. The utilities and vendors of SA systems have to take into account that even with the standardized data model and services as well as the comprehensive description by the substation configuration description language, the IEC 61850 standard allows certain degrees of freedom which especially surface in complex distributed functions. The application of distributed functions to complex switchyard topologies with dynamic power flows, i.e. changes of incoming and / or outgoing feeders, is very challenging, since IEC 61850 does not provide a clear model for this kind of applications and their functional demands. For these, it is not always possible to find an interoperable distributed solution that is valid for all vendor-specific implementations. It is therefore strongly recommended that the definition of data interfaces shall, in future editions of the standard, handle more complex topologies. These extended definitions shall cover e.g. protection zones for breaker failure protection, electrically connected parts for reverse blocking schemes as well as interlocking. Another gap in IEC 61850 are the missing definitions for redundant connection of an IED to one or two communication networks. The fact that an increasing number of utilities is requesting fully redundant communication, and not only a single ring, shows the need for higher levels of availability. With the current version of the standard, however, the implementation of a fully redundant communication results in a non-interoperable solution.

KEYWORDS

IEC 61850, Distributed functions, Interlocking, Reverse blocking, Breaker failure protection

*peter.rietmann@ch.abb.com

1 INTRODUCTION

IEC 61850 supports interoperability of IEDs in different system architectures. The choice of the system architecture out of all the options is mainly determined by cost considerations, reliability and performance requirements. Yet any choice should by no means jeopardize the standard's goal of achieving interoperability. IEC 61850 does not define any redundancy concepts, even though reliability requirements would call for it. Thus the most critical architectures in terms of interoperability are redundant ones.

Distributed applications often need time-critical communication and are very sensitive regarding interoperability, both in non-redundant and redundant communication architectures. An investigation into redundant architectures has been done e.g. in [1]. This paper mainly focuses on interoperability in distributed concepts, and not on the verification of any protection or control philosophy.

2 DISTRIBUTED FUNCTIONS

Table 1 shows a list of typical distributed functions in substation automation (SA) systems, their allocation and the impact on interoperability, e.g. when mixing devices from different vendors.

For the interoperability, three possible classifications are made:

- Non Critical – can be implemented with low risks
- Critical (vendor-specific) – can be implemented, locks into a vendor-specific concept
- Critical (gaps) – gaps in the standard

2.1.1.1.1.1 Distributed functions	**Allocation of function**			**Interoperability**		
	Station Level	**In one bay**	**More than one bay**	**Non critical**	**Critical (vendor-specific solutions)**	**Critical (gaps in the standard)**
Reverse blocking			**X**	**X**		**C**
Auto-reclosure		**X**		**X**		
Interlocking			**X**	**X**		
Double-command blocking			**X**		**X**	
Voltage selection			**X**		**X**	**C**
Breaker failure protection			**X**		**X**	**C**
Station level authority	**X**				**X**	**C**
Distributed synchrocheck			**X**		**X**	**C**

X = simple switc yard topology or functional demands

2.1.1.1.1.1.1.1 C = Complex switchyard topology or functional demands

Table 1 - Interoperability of distributed functions

To illustrate the borders of interoperability, this paper focuses on the more detailed analysis of the applications Reverse blocking, Interlocking and Breaker failure protection.

2.2 BASIC PRACTICAL REQUIREMENTS

The basic requirements of different users are independent of the technology and are the driver for how to solve, implement and optimize required functions for monitoring, control and protection. Besides the actual functionality, the requirements described in this chapter shall ensure optimal maintenance, high security and lowest possible life-cycle cost when considering distributed functionality.

Interoperability

Interoperability is one of the main targets of IEC 61850. This is an important issue when investing into a future-proof technology. Interoperability has to be considered concerning functionality but also concerning the equipment supporting e.g. the communication infrastructure.

Availability

Depending on the functionality as such, different levels of availability may be applicable. For mission-critical functions, e.g. protection-related ones, high availability should be applied. This can be achieved by using highly reliable products and by introducing redundancy where necessary.

Single point of failure
Critical functions shall not only rely on a single component, especially if the involved component has a relatively low mean-time-to-failure. In this case a backup component shall take over the function of the faulty part within a time that does not jeopardize the execution of the function involved.

Performance / Safety
The performance requirements may differ with the kind of distributed function. The architecture supporting the distributed function shall ensure minimal transmission time also under avalanche conditions and shall not adversely impact mission-critical functions.

Maintenance
It is essential that maintenance work on one or several bays does not affect the rest of the system at all. E.g. it shall be possible to take the bay control or protection devices of one bay out of service without interrupting or disturbing the communication between the other IEDs.

System extension
Extension of a installed system at a later stage shall have only minimal or even no impact at all on its service. Online system extension shall be supported.

Refurbishment
Throughout stepwise refurbishment of old conventional systems with new SA systems, station-wide functionality shall not be lost. The parallel operation of the old conventional part and the bays already equipped with new modern technology shall be possible. Remote access from a higher-level control centre shall not be affected and telecontrol of old as well as refurbished bays be possible at any time.

Local operation
In high voltage substations, high availability of bay control has to be achieved with a completely distributed approach and a graceful degradation of control functions. In a worst-case scenario, bay control shall be possible locally at bay level and be independent of other bay IEDs. Nevertheless, reasonable security checks shall be provided.

Testing & Commissioning
For factory testing only the typical bays are set-up and connected to the system in most cases. This perfectly serves to verify functionality that is either bay-related or involves communication between bay and station level. As soon as distributed functionality involving all bays is introduced, information from all these bays is needed. This can be achieved in two ways. All bays can be set-up and connected to process simulators, or only the typical bays whilst missing bays are simulated by a tool. The second method is mostly preferred when considering cost and time efficiency.

System design
Applying serial communication for distributed functions may not make sense in each and every case for several reasons. Important considerations are the locations of all devices involved in performing the distributed function and the amount of information to be exchanged. E.g. bay-related distributed functions performed by devices in the same cubicle may exchange the required information via hardwired connections. Bay-wise maintenance, retrofit and local operation lead to an architecture where distributed functions are performed by as few IEDs as possible.

All above requirements and criteria are discussed in the analysis of various examples for distributed applications in the following chapters.

2.3 COMMUNICATION ARCHITECTURES

The influence of different communication system architectures on the safety and availability of distributed SA functions, especially on reverse blocking and interlocking, has already been investigated in [1]. The most interesting resultant architectures in the context of this paper are illustrated in Figure 1, referring to the scenarios S1 and S3 in [1]. Considering the basic communication architectures with Ethernet switches having a reasonably high availability, the ring (as shown by S1 in Figure 1) is a suitable and economical solution. The reconfiguration time upon communication network failures is a critical issue in terms of safety and should not exceed 100 ms.

If higher availability and especially short reconfiguration times are needed, duplicated communication networks are recommended (S3 in Figure 1 shows two star networks, but rings could also be used). These need special handling at protocol level to run them in parallel, however. Due to its zero reconfiguration time, this solution provides higher safety both for interlocking and protection-related functions. Due to the non-standardized protocol additions needed, its interoperability can however not be guaranteed.

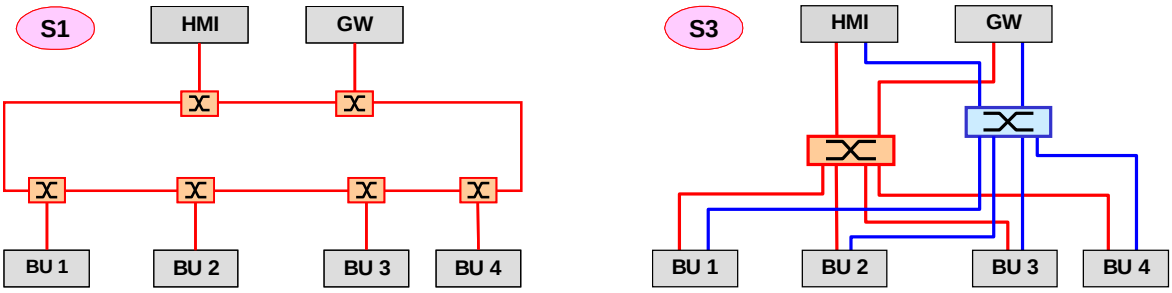

Figure 1 - Ring and duplicated network architectures

The reference cited above discusses also process bus-related architectures, whilst this paper considers communication between bays and to the station level only. Therefore, only the single ring and the duplicated communication systems with stars, rings or a mixture of both are meaningful alternatives. Besides the ring reconfiguration time, also the switch-dependent transmission delay of around 100 µs per switch as well as the message length and bit rate used have to be considered. If Main 1 and Main 2 protection systems are used, each of them should have its own communication system. The availability of this structure, i.e. handling of failed communication, is in a similar order as that of a duplicated communication system used jointly by the Main 1 and Main 2 protection systems, but remains fully interoperable. It might, however, lead to a higher probability of over-functioning. This has to be considered when designing protection systems.

3 DETAILED ANALYSIS: REVERSE BLOCKING

The problem to be solved with reverse blocking is that a downstream fault in a bay with outgoing power flow (outgoing feeder) protected by a protection P_2, could also be seen by protection P_1 at a bay with incoming power flow (incoming feeder) and result in the tripping of all consumers (see example in Figure 2). Therefore, the selectivity of the protection is lost and fault clearance restricts the power supply to more consumers than is actually necessary. A possible solution is to delay the trip on incoming lines, allowing the outgoing line to trip first. Unfortunately, this leads to longer fault clearance times, if the fault is not on an outgoing line. Using the reverse blocking scheme, the start signal of the outgoing feeder protection P_2 blocks any trip of the protection P_1 on incoming feeders. This needs data exchange from all outgoing to all incoming feeders. With IEC 61850, GOOSE messages are used to transmit the protection start signals of all outgoing feeder protections P_2 to all incoming feeder protections P_1, thus blocking them for as long as the start signal has the value TRUE.

In case the direction of the power flow through the substation remains unchanged, like shown in Figure 2, the outgoing and incoming feeders are known in advance, and the data exchange can be configured appropriately. Maintenance of an outgoing bay has no influence on the correct functioning of the scheme – its protection simply does not send any blocking signal, so that the protection of the incoming feeder works as backup in case of a fault.

The protection of newly added incoming bays only needs local configuration. If an outgoing bay is added, the new blocking signal has to be sent to the protections of all incoming bays. The new signal has to be included in the blocking logic like in conventional, hardwired reverse blocking schemes.

Start signals of protection functions are easily identified by means of the IEC 61850 data model. Therefore, interoperability poses no problem, as long as the protection IEDs are able to send (outgoing bays) respectively receive (incoming bays) GOOSE telegrams sufficiently fast (see IEC 61850-5

performance classes). To ensure sufficiently fast reverse blocking, the delay times caused by the switches need to be considered in large communication systems.

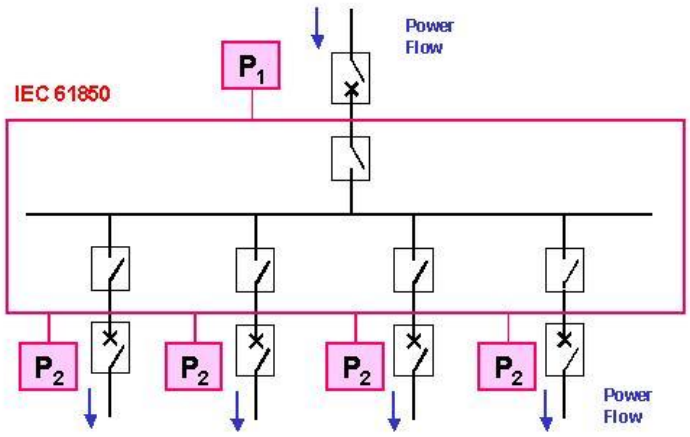

Figure 2 - Reverse Blocking Protection

A centralized approach, i.e. sending all start signals to a central IED, which then identifies the actual topology and distributes the blocking signals accordingly, adds further delay and introduces a single point of failure. Furthermore, when incoming bays are added, always two IEDs have to be changed, i.e. in the added bay and at the central place. If there are many incoming feeders and the additional delay can be tolerated, this approach might be advantageous from an engineering and maintenance point of view. However, in this case the central IED itself should be duplicated.

Criteria	**Decentral, ring**	**Decentral, separate Main 1 / Main 2**	**Central, ring**	**Central, separate Main 1 / Main 2**
Interoperable	Simple topology, static power flow	Simple topology, static power flow	yes	yes
Single point of failure	No	no	yes (or duplicate central IED)	no
Availability	+	+++	-	++
Performance (safety)	-	++	--	++
Influence of bay outage or extension	+ for simple topology / static flow - for a complex situation	+ for simple topology / static flow - for a complex situation	+	+

Table 2 - Reverse Blocking Summary

An easy way to duplication of the central IED exists if the protection system is divided into Main 1 and Main 2. In this case there could be a dedicated communication network and central point for Main 1 as well as for Main 2. If the duplication is made within the same communication system, then additional management functionality for its handling has to be provided. This could be relatively simple in case of blocking signals: both central IEDs work in parallel, and all incoming feeders use either of the blocking signals. If Main 1 and Main 2 operate completely separate, then the failure of a protection IED of an outgoing bay should lead to a longer upstream protection delay. Otherwise, this results in the non-selective tripping at the incoming feeder, even if the second system is fully operative and performs a selective trip with reverse blocking of the upstream protection. The protection failure

can be detected with standard IEC 61850 mechanisms applied to the received GOOSE telegram. To save HW and thus optimize repair effort, the central logic could reside in one of the existing protection IEDs of an incoming feeder. This does, however, not influence the slightly decreased availability and performance as compared to the decentralised approach.

The principle of reverse blocking could also be used for more complex switchyards and for dynamic power flow situations, if the direction of the power flow is measured and a topology analysis determines which incoming and outgoing feeders are connected. This comes close to a busbar protection based on fault direction. Since the needed topology data is not standardized in IEC 61850 currently, only a central solution can be interoperable. Table 2 gives a summary of the discussed solutions.

4 DETAILED ANAYSIS: INTERLOCKING

Interlocking assures that no command can be given to a power system switch (circuit breaker, isolator, earthing switch), which might endanger human beings or destroy power system components. The interlocking conditions for blocking or releasing a switch operation are based on the states of other switches and possibly some voltage measurements at the lines. Bay level interlocking depends on the positions of switches within the same bay as the commanded switch, and Station level interlocking on the position information from switches in other bays. For a bay-oriented control architecture, the bay level interlocking is often implemented within the bay control IED, or even realized with hardwiring. For station level interlocking the following possibilities exist:

1. The states of all switches are sent to all bay controllers, and each bay controller calculates both the bay level and the station level interlocking (decentralized solution).
2. All switch states are sent to a central IED, which calculates releases and blockings using bay and station level rules and sends them back to the bay controller (centralized solution).
3. The bay level interlocking is calculated by the bay controller based on the states of the switches in the allocated bay. Additionally, all switch positions needed for station level interlocking are sent to a central IED, which sends station level interlocking releases and blockings to the bay controller for consideration in addition to the bay interlocking (mixed solution).

Criteria	**Decentral (1), ring**	**Decentral (1), dupl. network**	**Central (2), dupl. network**	**Mixed (3), dupl. network**
Interoperable	yes	yes	yes	yes
Single point of failure	no	no	yes (or duplicate center)	no (graceful degradation)
Availability	+	++	-	+
Performance (safety)	+ (- reconfiguration)	++	-	+ (- center)
Influence of bay outage or extension	+ for simple topology - for complex topology	+ for simple topology - for complex topology	++	++

Table 3 - Interlocking Summary

The decentralized solution (1) has the highest availability and best performance (communication-related safety). The loss of a bay level IED leads to unknown states at the receiving IEDs, which must safely be handled by the appropriate interlocking logic. This solution might also be practical from the engineering point of view, because all IEDs can get the same interlocking logic by just using the outputs for the switches that they have to handle. The effect of adding bays depends on the complexity of the substation configuration – mostly at least two bay IEDs are concerned, but often all bays in the substation. If the new bays are already planned in advance, then a switch state simulator for the open switches of the future bays can keep the change effort on existing bays small or maybe even zero.

With the centralized approach (2), the entire interlocking logic is in one central place, i.e. any evaluation is done only once centrally. However, this might affect all connected bays, and the central IED is a single point of failure. If it is duplicated, even more HW – and therefore potentially more repair work – is needed, as well as some additional logic to handle duplicated blocking inputs and failure of one source.

Solution 3 is a compromise between 1 and 2. As bay level interlocking is done in the bay units, and a failure of the central station level interlocking very often has not much more impact than the failure of just another bay, its negative effects may be acceptable. On the other side, it offers the advantage of changes with influence on several bays only being made only at one central place while keeping the bay level interlocking safe. If the station level interlocking resides e.g. in a buscoupler control IED, then even no additional HW is needed. The only problem is the increased response time to station level state changes leading to slightly less safety in case of spontaneous switch state changes in other bays e.g. through protection trips or – much less probable – by disturbances.

Note: the difference between ring and duplicated communication network for solutions 2 and 3 is not elaborated in Table 3 – it is identical to the differences in performance and availability for solution 1.

5 DETAILED ANALYSIS: BREAKER FAILURE PROTECTION

The distributed part of breaker failure protection comes from the need to trigger remote (neighbouring) circuit breakers (2) in case the local circuit breaker (breaker 1) has failed to operate (see Figure 3). IEC 61850 provides the Logical Node RBRF with data OpEx for this, to signal that some external circuit breaker has to trip. The modelling of breaker failure protection according to IEC 61850 is given in [1].

For simple switchyard configurations, the neighbouring breakers to be tripped are fixed or easily determined from the state of the busbar isolators, bus couplers and bus sections. If the logic is simple, the position of the related breakers together with the OpEx signals of each bay can be distributed with GOOSE messages, and all receivers decide on the basis of received OpEx and current switch positions, whether or not they shall trip. This distributed implementation has the same advantages and problems like that of distributed reverse blocking or station level interlocking. It especially needs a lot of adaptations if a new bay is added.

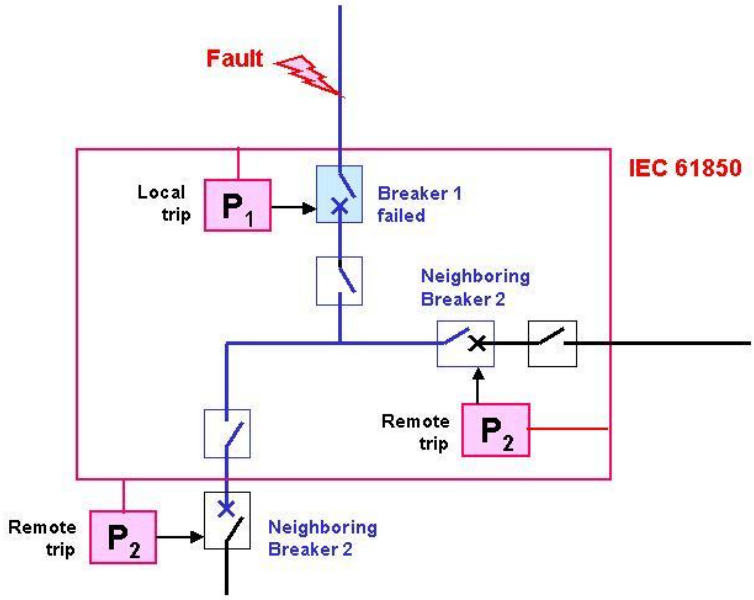

Figure 3 - Breaker Failure Protection

Here a centralized version of a decision algorithm for breaker failure protection with topology detection can be implemented. This is triggered by the received OpEx signals and sends an additional trip signal directly to the concerned bays. Such a solution can be built in an interoperable way, even

for very complex busbar configurations. Additional bays have to be introduced only at this central place. However, there is again a single point of failure. Solutions could be as described above for reverse blocking, i.e. duplication of the central unit either on the same communication system, or having separate central units in dedicated Main 1 and Main 2 communication systems. The strategy of putting the central logic into some existing IED e.g. for the bus coupler, could also be followed to overcome the problem of additional IEDs, which can fail.

6 CONCLUSION

The discussed examples show that the problematic in distributing functionality is very similar for breaker failure and interlocking. In general, the control has a local option as emergency backup, whereas protection must consider component failures. As several distributed functions usually belong to a complete substation automation solution, both distributed control and protection-related functions might use the same communication infrastructure. Requirements concerning availability and safety may be different for distribution and transmission substations, but also depend on other criteria. For a recommendation, the following considers a typical medium voltage (MV) substation for distribution and a typical high voltage (HV) substation for transmission.

MV substations have combined control and protection devices mounted in the switchgear compartments. According to IEC 61850, the recommended Goose message (signal) transmission times are 10 ms for critical functions and 100 ms for less critical ones. This can be fulfilled by a single ring configuration in combination with distributed implementations of all suited protection, protection-related and control functions such as interlocking. It will provide sufficient availability and safety with the added advantages of limited effort regarding the communication system and providing a maximum level of interoperability. For HV substations, the main characteristics are two separate IEDs for protection (Main 1, Main 2). To cope with the higher requirements concerning safety and the additional delays introduced by the process bus if used, IEC 61850 recommends much shorter transmission times for critical and non-critical functions. To ensure higher availability for the protection functions, two physically separated ring networks for Main 1 and Main 2 devices respective functions are recommended. To ensure that the higher safety can be achieved also for the control part, the control IEDs can be connected to both networks. It should be noted that the redundant connection of one IED is not an interoperable solution; several proprietary solutions exist on the market.

The application of distributed functions to complex switchyard topologies with dynamic power flows is very challenging, since the standard IEC 61850 does not provide a model for this kind of applications and their functional demands. Thus it is not possible to find an interoperable solution for such applications. It is strongly recommended that future editions of IEC 61850 standardize the data interfaces to handle more complex topologies and cover e.g. protection zones for breaker failure as well as electrically connected parts for reverse blocking and interlocking. Another gap in the standard are the missing provisions concerning the redundant connection of one IED to one or two communication networks. The fact that an increasing number of utilities requests fully redundant communication, and not only a single ring, shows the need for higher levels of availability. However, today's implementation of a fully redundant communication results in a non-interoperable solution.

BIBLIOGRAPHY

[1] Lars Andersson, Klaus-Peter Brand, Christoph Brunner, Wolfgang Wimmer
Reliability investigations for SA architectures based on IEC 61850,
IEEE PT05, Petersburg 2005, Paper 604

[2] Klaus-Peter Brand, Christoph Brunner, Ivan de Mesmaeker
How to use IEC 61850 in protection and automation
Electra 222, October 2005, 11-21