Reliability investigations for SA communication architectures based on IEC 61850

Lars Andersson, Klaus-Peter Brand, *Senior Member, IEEE*,
Christoph Brunner, *Member, IEEE*, and Wolfgang Wimmer

***Abstract*—The new communication standard IEC 61850 is now introduced to substation automation replacing all wires by serial communication. Based on mainstream communication means like Ethernet it profits from a high flexibility regarding communication architectures. But any solution has to fulfill all reliability requirements resulting from the safety-critical mission of substation automation for a reliable power supply in transmission and distribution grids. To achieve this goal typical types of SA communication architectures are investigated starting from the relevant properties of IEC 61850, using proper reliability definitions and common failure modes. The relevant reliability figures are calculated. Different levels of redundancy, their limits for reliability and impact on the distributed functions are considered. The results clearly indicate what types of architectures have to be applied for the requested reliability of substation automation functions. This includes also function allocation and proposals for amending the standard.**

***Index Terms* – Reliability, substations, substation automation, communication, communication architectures, protection, control, IEC, standard, IEC 61850, distributed functions.**

I. Introduction

Substation automation (SA) is commonly used in controlling, protecting and monitoring of substations [1]. Up to now, the communication for SA has used private serial communication systems complemented by conventional parallel copper wiring, especially from the process to the switchgear. With the advent of IEC 61850 [2], there is a comprehensive global standard for all communication needs in the substation being introduced now.

Since the reliability of substation automation has a strong impact on the reliability of the power supply from the power transmission and distribution grid, the reliability of the used SA communication architectures is of great interest. This question valid for any communication system is now raised for the new communication standard, since its use of mainstream communication means like Ethernet provides a high flexibility not known from the private or dedicated communication systems used up to now. First considerations about essential features published by the authors in [3] and [4] are extended in this paper to a comprehensive, overall view on SA architectures based on IEC 61850.

The authors are with ABB Switzerland Ltd., Zurich and Baden:
lars.andersson@ch.abb.com, klaus-peter.brand@ch.abb.com,
christoph.brunner@ch.abb.com, wolfgang.wimmer@ch.abb.com

II. Relevant features of IEC 61850

The standard IEC 61850 allows the "free allocation of functions to devices" and, therefore, supports any kind of function integration, function distribution, and SA architecture. The supported communication methods ("services") offer some choice to meet the performance requirements. The mainstream communication means like MMS, TCP/IP and Ethernet selected by the standard are not only open for advances in communication technology but for a lot of communication architectures. Both the use of fiber optics and switches overcomes a lot of limitation of the Ethernet like collisions and allowed length extensions. The object oriented data model and the abstract definition of communication services hides the physical SA architecture for the user. Nevertheless, this architecture is essential for the system reliability.

The standard gives no rules for the SA communication structure. This paper will provide practical guidelines based on reliability calculations and regarding all relevant features of IEC 61850.

III. Introduction to reliability

Reliability according to IEC 60870-4 [5] is defined as a measure of equipment or a system to perform its intended function under specified conditions for a specified period of time. The substation shall continue to be operable, according to the "graceful degradation" principle, if any SA system component fails. There should be no single point of failure that would cause the substation to be inoperable.

Reliability needs proper operating intelligent electronic devices (IED). This means that also the MTBF has to be reasonable high. Redundancy may be one way to increase the system reliability but has to be applied very carefully as discussed below.

To calculate reliability, availability and safety figures, the Markov state model as introduced in [3] and shown in Figure 1 is applied. An important property especially for the safety is beneath the failure rate (L) and the repair rate (M) the error discovery rate (E).

We may assume that the system has three states:

- Normal working condition: everything is healthy and working
- Failure happened, however is not yet detected. Here the system might potentially be unavailable and unsafe for requests

- Failure detected: now measures can be taken to make the system safe again, however with possibly degraded availability, if the system has no redundant components

From this discussion it can be seen, that fast error recovery leads to short unsafe state, i.e. it enhances the safety. It can further be seen, that error detection time must also be considered as time of unavailability, i.e. it has to be added to the MTTR when calculating availability (or seen as part of MTTR, if simple availability calculation model is used). And the error detection time lasts naturally until the related measure has been taken – i.e. either go to a safe state, or repair the system respective activate the redundant part. To be able to quantify theses effects, we use the following Markov state model:

1) The Markov state model

P_1 is the normal operating state of the system. It gets dangerous (unsafe) on an error, which happens with rate L and leads to state P_2. It is safe again, if the IED has detected the error and taken a safe state (i.e. switch off, or block all outputs), which happens with rate E and leads to state P_3. The repair with a rate M leads back to normal operating state.

P_2 is the unsafe state, and P_2 is therefore the probability to be in an unsafe state. So the safety probability S is:

$$S = 1 - P_2 = P_1 + P_3$$

If we assume independent (and therefore exponentially distributed) probabilities for the rates, a static situation for all P_i, and a model start at P_1, we can express the unsafety probability P_2 as

$$P_2 = \frac{1}{1 + \frac{E}{L} + \frac{E}{M}}$$

and the resulting safety probability S as

$$S = \frac{1}{1 + \frac{1}{\frac{E}{L} + \frac{E}{M}}}.$$

By the way, the availability is the probability to be able to do what the system is intended to do, which is the normal state, and therefore has probability A:

$$A = P_1 = \frac{1}{1 + \frac{L}{E} + \frac{L}{M}}$$

2) Application to redundant system with reconfiguration time

An automation system relying on a communication system might be considered unsafe when some application IEDs are no longer reachable due to some failure in the network, until the network has detected the failure and reconfigured to connect all IEDs again. This means that L is the failure rate within the network.

For a non-redundant system E is the error detection rate, and M the repair rate.

For a redundant system from the safety point of view, however, E is the error detection and automatic recovery rate, and M is always 1, because the recovery has 'repaired' the system, as seen from functionality and safety point of view. For a real influence of repair rate on the redundant system availability another model like the availability diagram or fault tree method [6] will be taken.

To get a practical example (taken from [3]), let us take a redundant communication system with 10 switches, each a MTTF of 50 years, e.g. a ring. This means that L is 10 / 50 = 0.2 / y. Let us further assume an average error detection and recovery time of 100 ms, meaning E = 1000 /100 = 10 /s. As M is assumed to be 1, we can simplify above formula to

$$S = \frac{1}{1 + \frac{L}{E(L+1)}}$$

Then we get as safety 99.9999962%, i.e. practically no unsafety, compared to an accepted protection safety better than 99.999(see also the integrity level definitions in [7] – highest safety integrity level for low demand systems)

If we have a recovery time of 1s, this results in S= 0.999999619, i.e. practically no difference.

If we have a recovery time of 1 s, and a switch MTTF of 5 years, this would result in a safety of 99.9996%, which then approaches the protection safety and should not be accepted, because it is only a part of the overall protection safety including the IED HW also.

An MTTF of 20 years for 10 switches in the communication system results in S = 99.9999%, which could be the limit to be tolerated – it is a factor of 10 better than the requirement for overall protection safety, however only a part of it.

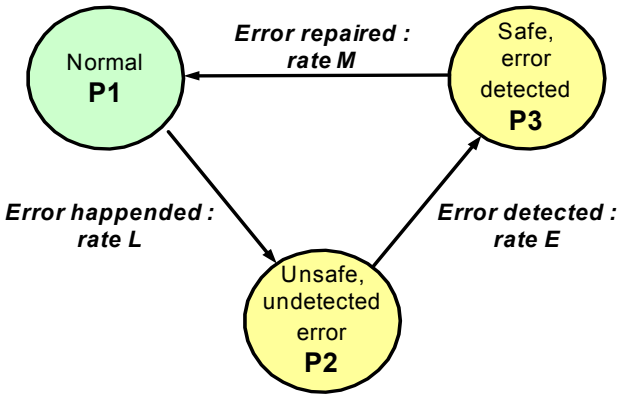

Figure 1 - Safety Markov state model (P1 normal operating state; P2 unsafe state with error but before detection; P3 safe sate after error detection) introduced in [3] and used in this paper also

IV. Failure Modes and Scenarios

A. Definition and assumption

A failure means that some component in the SA system is not working as intended and having an impact on the requested

functionality of the SA system. The basic assumption is that the failure modes are independent from each other.

B. Internal device and link failures

Same as most entities, also electronics components used by IEDs are ageing with a continuous degradation or an immediate malfunction. The result may be the loss of power supply, loss of processing electronics, or loss of communication ports like failing diodes for fiber optic links.
The user experiences the resulting losses in applications e.g. loosing the access to the complete SA for controlling and monitoring via HMI or NCC gateway, the access to one single bay or to one IED only. Other results may be the loss of local (e.g. IED failure) or distributed (e.g. communication port failure) protection or automation functions.
Most losses are permanent, i.e. requiring human intervention. Other losses may be transient or coped by a proper design and an embedded recovery strategy, i.e. the system may be recovering from this failures.

C. External causes

Components of the system and, especially, communication links may be cut or destroyed by an external impact like the unwanted action of a service man. Assuming a statistically behavior of such events also, this failure mode can be assessed same as any internal failure but the measures against may be totally different.

V. REDUNDANCY

A. Basics of SA communication architectures

Substation automation consists commonly of three levels i.e. the station level with the station level operators place (HMI) and the NCC gateway (GW), the bay level with its units (BU) for protection and control, and the process level near the switchyard considered in the investigations also. All these levels are connected by the communication system. The basic assumption is that this network according to IEC 61850 is based on a switched (S) Ethernet, because only then functions distributed to more than one IED with some real time requirements additional to station level connection (vertical communication) for operation and supervision can be used.

B. Basic communication architectures

The communication network may be non-redundant, e.g. comprising of one central switch being connected to all IEDs by one link (star type, Figure 2 without dashed part). Some inherent communication redundancy is provided e.g. by a ring of switches ("ring redundancy") connected to IEDs with a single link (Figure 3 without dashed links). The communication system may also consist of *two* independent non-redundant or ring subsystems where each IED has a separate port to each network, providing a higher level of redundancy (
Figure 2 and Figure 3 with dashed parts). Further, big systems with many switches may need due to technical restrictions and performance requirements a structure of several redundant networks, which are redundantly connected. This last type will not be considered here.

The overall SA system redundancy depends not only on the redundancy of the communication system but also on the IEDs, especially on the number of parallel communication ports determining the number of possible links to the switches. Not more than two parallel ports per IED are considered in the following investigation (see Figure 2, Figure 3, Figure 4). Duplication of the communication networks (Figure 2 and Figure 4 with dashed links if applicable) makes only sense for IEDs with two ports or duplicated IEDs.

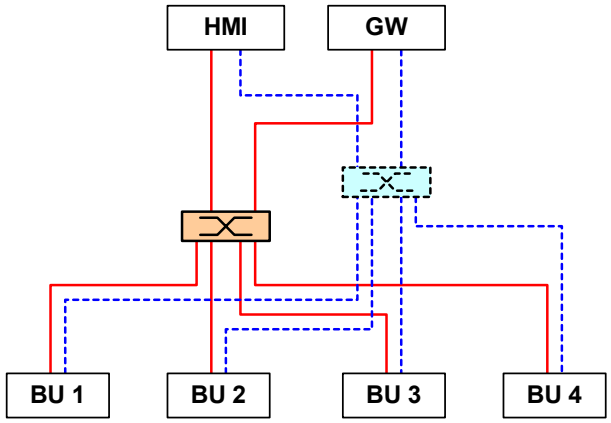

Figure 2 - Example for non-redundant communication system (dashed a second communication system in parallel is shown)

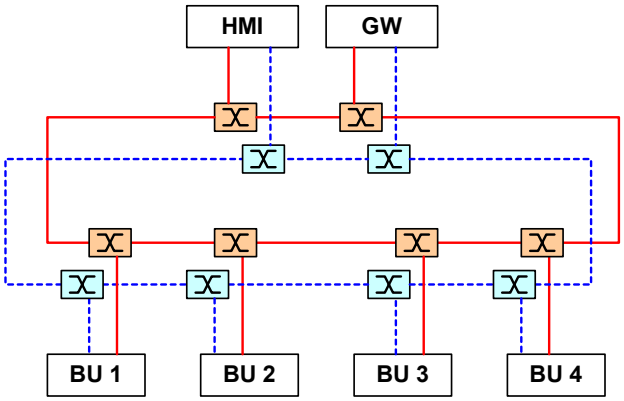

Figure 3 - Example for a doubled, parallel redundant communication system (second ring dashed)

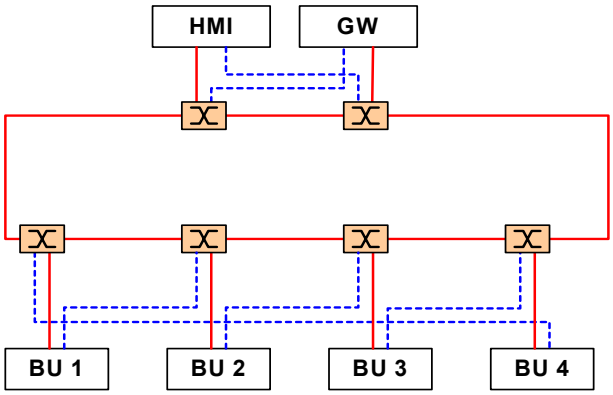

Figure 4 - Example for communication system with ring redundancy (dashed a solution with two-port IEDs is indicated where the second port is crossed reducing the number of switches)

C. Evaluation criteria and evaluation

For an evaluation of the different architectures we need to make some assumptions about the failure rates of the components. Although this may differ for components from the market – e.g. the failure rate difference between office-type switches and industrial-type switches can be a factor of 10 – it gives some guidance on the evaluation of different communication system redundancy structures.

For our calculation we assume that a bay level IED like a protection or control bay unit (BU) has a mean time to failure (MTTF) around 100 y. For switches the MTTF depends on the number of ports. We assume for sizes up to 8 ports a MTTF of about 50 y, and for more ports e.g. as needed in star configurations around 40 y MTTF. Observe that these figures are at the high end of available industrial switches for the time being.

From this numbers we can immediately say that a star network like in Figure 2 without the dashed part will have a far lower availability than current SA systems, because the central switch's MTTF is less than half of those of a bay level IED and even much less than a star coupler working on physical level only, and also is a single point of failure for the whole communication network. This might be sufficient for switchyard operation, if the bays provide a backup control panel, but not for distributed functions like interlocking. Therefore this version will not be considered further.

The following basic communication architectures on station bus level are investigated:

S1: ring redundancy, IED connected with one port (Figure 3 without dashed part)

S2: ring redundancy, IED connected with two ports to two different switches (Figure 3 with dashed part)

S3: two star communication networks, each IED connected with one port two each (Figure 2 with dashed part)

S4: two ring communication networks (Figure 3 with dashed part)

S5: like S2, however each second switch connected so that two rings exist (Figure 5)

In addition, process bus architectures are investigated by themselves and in connection with the station bus architecture (S6/Figure 6, S7/Figure 7, and S8/Figure 8).

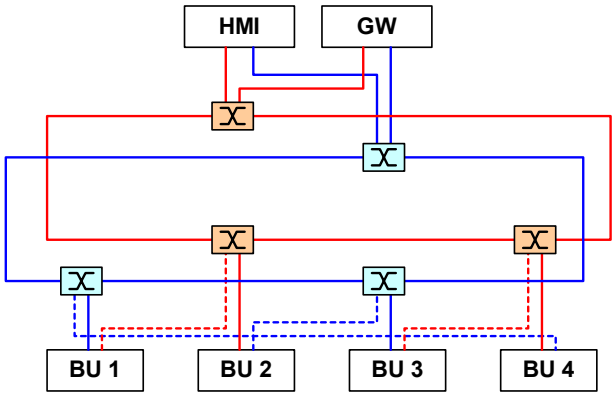

Figure 5 - Example for a doubled redundant communication system (two rings with ring-redundancy in parallel) with reduced number of switches

Observe that for a doubled network the recovery time on a failure is zero (0 ms), while for a ring network some reconfiguration time is necessary. Standard spanning tree algorithms need times in the order of 100 ms for ring recovery. Some proprietary implementations claim recovery times in the order of 1 – 10 ms. For the following investigations, the recovery time for the standard spanning tree algorithm is used.

If we assume 8 bays with one switch per bay normally, and two switches at station level, then we get for comparison the following reliability figures (system mean time to failure MTTF and mean time between repairs MTBR) and recovery times for the availability of two arbitrary bay level IEDs (BU) communicating which each other. Observe that the system MTTF (first column) as calculated here is without repair. The time with repair is calculated for a mean time to repair of 24 h.

Comm. archi-tecture	MTTF (y)	MTTF with repair (y)	MTBR (y)	Reco-very time (ms)	Relative architect-ture cost
S1	12.9	16.6	4.5	100	100
S2	17.6	49.9	4.5	100	105
S3	27.3	49.9	11.5	0	80
S4	34.5	49.9	2.4	0	200
S5	35.7	49.9	4.5	0	110

Table 1 - Reliability figures for basic SA communication architectures; MTTF with repair for 24 h mean time to repair.

The costs above are relative costs to S1 (S1=100%) just for switches, and just rough estimations. Real costs especially between ring and star depend naturally on available number of ports for the switches as well as the actual pricing. The additional cabling costs, and therefore also the cost difference between star and ring depend on the kind of cables and the geographic distribution (cable length). Just from cable costs S4 and S5 are comparable, and around twice that of S1 and S2. The MTTF with repair is practically identical for all systems, where the IED is connected with two ports, arising mainly from the two (non redundant) communicating IEDs. We see that between star (S3) as one extreme and double ring (S4) as the other extreme there are intermediate forms like S5, which have MTBR and cost somewhere in between. The optimum solution depends very heavily on the geography of the station and, therefore, the resulting communication equipment costs (switches, cables, plugs, etc.).

From the interlocking example [3] re-discussed in chapter III. we learn that for switches as considered in this paper, the 100 ms reconfiguration time of architectures S1 and S2 is sufficient to guarantee the needed interlocking safety. However, it is clear that lower switch MTTF might change this conclusion. Similar investigations like for interlocking in this paper should be done for other distributed functions used in substations also.

D. Process busses and functional redundancy

Possible process bus architectures are determined by the fact that protection is redundant (main 1, main 2) at least at the transmission level of the power system. Any solution has to

preserve this redundancy. Control is normally not implemented redundant. An architecture fulfilling this requirement is shown in Figure 6. Both bay protection units (BPU1, BPU2) own independently from each other a process communication system with a switch, a merging unit (MU1, MU2) as source of current and/or voltage according to IEC 61850, and a breaker IED (IED1, IED2) representing the breaker and being the sink of the trip. The non-redundant bay control unit (BCU) may be connected to both switches for operation via IED1 or IED2. The station bus connectivity may be single or doubled (dashed in Figure 6).

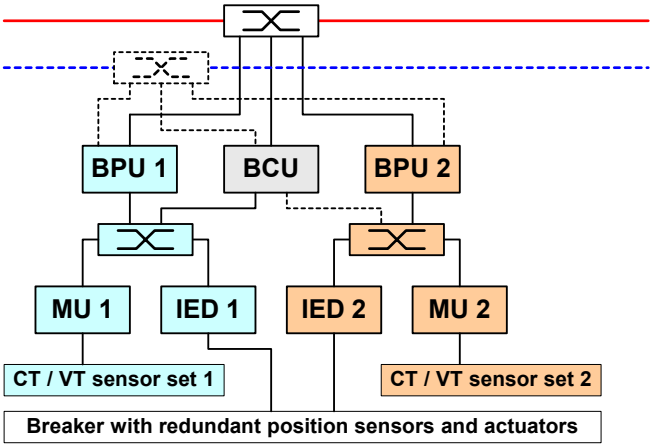

Figure 6 - Process bus communication for redundant protection

VI. Simplifying the Communication Architecture

According to Figure 6 with the dashed part the redundant station bus and redundant process bus together require 4 switches per bay. By combination of the process bus and the station bus switches, their total number is reduced to 2 per bay (Figure 7). The communication traffic on the process bus like the stream of current and voltage samples will not pollute the complete system since they may be confined locally to one switch using a virtual local network (VLAN) as standard means of the Ethernet technology.

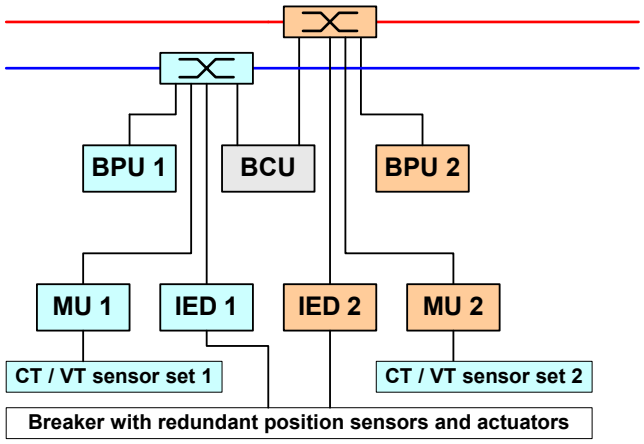

Figure 7 – Redundancy of protection, process bus and station bus

The architecture of Figure 7 may be simplified more without degrading the full redundancy by using a redundant controller also. To reduce the number of devices and, therefore, of potentially failing devices, the controllers may be combined with the protection units (Figure 8). This combination without redundancy is common on distribution level already. There is no argument against also on transmission level as long as two devices per bay remain and the control software is not degrading the protection performance. The first issue is fulfilled by definition of S8, the second issue by a proper implementation according to well-known and proven SW design principles. Each device needs only one non-redundant bus connection to the IEC 61850 bus. This is possible since IEC 61850 makes no difference between the station and process bus. The process bus interface has to support in addition to the station bus services as additional service the transmission of analogue sampled values. By this, the only difference between the communication architectures for transmission and distribution would be the redundancy in transmission substation automation systems.

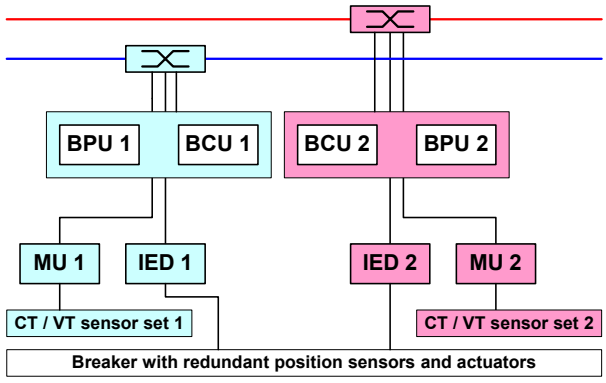

Figure 8 – Most simplified communication architecture with redundant combined protection and control, with redundant station bus and redundant process bus

For quantifying the reliability figures of the process bus, we take an MTTF of 150 y for the merging unit MU and 200 y for the breaker IEDs. Also the protection and bay controller can now be considered to have 150 y MTTF, because it does not need I/Os – all data comes via the process bus.

If we just consider the availability of a *bay protection* function, then this is the same for all configurations, because you always need an MU, a BPU, the breaker IED and one switch. With above component figures the overall MTTF results in 26 y. This is only around one fourth of the stand alone BPU reliability of 100 y. Therefore, redundancy is a must. The redundant system, two times independent protection with process bus, then has a system MTTF of 248000 y, if we assume 24 h mean time to repair.

Let's consider again the availability of communication of protection between two bays, where the bays are connected by one single switch (star configuration). The following table shows the results, where again the system MTTF is without repair, to be comparable to S1 – S5.

Comm. archi-tecture	MTTF (y)	MTTF with repair(y)	System MTBR (y)	Relative architect-ture cost
S6	14.6	19550	3.7	130
S7 – pro	34.2	60061	8.5	110

S7 – ctl	38.7	74.8	15.8	110
S8	34	60061	8.5	100

Table 2 - Reliability figures for SA communication architectures with process bus and at least redundant bay protection; MTTF with repair for 24 h mean time to repair (pro: protection; ctl: control)

The figures of S7 and S8 for protection functions, e.g. breaker failure, are identical. The controller reliability is not considered for the protection MTBR. Here S7 would be slightly worse, because of the additional controller HW. The cost difference stems from the controller HW. For control related functions, the MTTF with repair figure for S7 is worse, as the controller is not duplicated. For S8 the control figures are the same as for protection.

The problem of architecture according to Figure 8 with this architecture is, that at the end it consists of two duplicated systems with a common HMI. For protection as used now this is not a big issue, as this is the case already now. However for control or if distributed functions are used, some synchronization concept has to be found, at least at the HMI level.

Above calculations assume that e.g. a breaker failure trip is passed from one bay protection IED to the other bay protection IED. For S6 this is a must. In S7 and S8 however, the trip could go directly to the breaker IED of the second bay, thus enhancing the function reliability as well as the trip delay time.

Observe the big difference between the MTTF figures with and without repair. The consequence is that if you use process bus, you also need a supervision system, which immediately announces each failure, so that it can really be repaired within 24 h.

VII. Impact on Distributed Functions

A. Examples

Examples of distributed functions are *interlocking, fast autoreclosure* and *slow autoreclosure, load shedding*, *breaker failure*, *intertripping* or *reverse blocking* which are exchanging time critical signals between IEDs. The same holds for the *disturbance recorder* trigger and the *protection trip* over the communication network. *Protection functions* and (distributed) *synchrocheck* may require also the transmission of samples beyond the bay. All these distributed functions represent chains and will not operate if one of chain links fails. Examples are

- Interlocking: BIED-PS-(C-SS)-*n*C
- Breaker failure protection (BFP): MU-PS-P-PS-2(P-SS-BIED)
- Reverse blocking as subset of BFP
- Differential protection 2(MU-PS)-P

The abbreviations for the components are listed in Table 3. The local bay is where the BFP resides, the trip signal from the BFP, in case of non-operation of the local circuit breaker, must reach *n* adjacent bay for a successful execution of the function.

Abbreviation	Explanation
MU	Merging Unit
PS	Process bus switch, in case of a dedicated switch for the process bus
P	Protection IED
C	Control IED
PC	Combined Protection and Control IED
SS	Station bus switch, can also be used for the process bus
BIED	Breaker IED

Table 3 - Abbreviations used for distributed functions

B. Investigations

We now investigate two of the distributed functions with respect to the transmission distance for the critical signals between two functions, i.e. the breaker failure (BFP) and the command sequence with station interlocking. XX For each function we look at two cases i.e. the function may be located in a bay level device (C, P) or in a process level device (MU, BIED). We look at the different communication paths that the critical signals require for a successful execution of the function in some of the different architectures discussed above. The impact of *different architectures* is discussed here, *not* the impact of having *redundant networks* or functions. We look at four different examples. The architectures from the Figure 6, Figure 7 and Figure 8 above as well as a star network architecture that is a combination of the station bus star topology from Figure 2 (Lars: redundant with dashed part or non-redundant?) and the process bus star topology as in Figure 6.

The local bay is where the BFP resides in P or C, the trip signal from the BFP, in case of non-operation of the local circuit breaker. Must reach *n* adjacent bays for a successful execution on the function.

The device (P, PC, BIED) where the BFP resides is in bold. Left of this device is the path of the current measurement and right the paths of the trip signals. The number of adjacent bays is equal or greater two. The current measurements from the breaker bay must reach the BFP function; the trip signal from the BFP function must reach all circuit breakers in the adjacent bays. The paths of the critical data (current measurement and trip signal) are traced for two cases, i.e.in Table 4 when the BFP resides in the local Protection IED and in Table 5 when it resides in the local BIED.

Fig	Path	Expression
6	MU-PS-**P**-SS-(SS-P-PS-BIED)x	4+4x
7	MU-SS-**P**-SS-(SS-BIED)x	4+2x
8	MU-SS-**PC**-SS-(SS-BIED)x	4+2x
6+2	MU-PS-**P**-SS-(P-PS-BIED)x	4+3x

Table 4 - In these examples the BFP function resides in the protection IED, the current measurement is sent from the MU in the local bay.

Fig	Path	Expression
6	**BIED**-PS-P-SS-(SS-P-PS-BIED)x	4+4x
7	**BIED**-SS-(SS-BIED)x	2+2x

Fig	Path	Expression
8	**BIED**-SS-(SS-BIED)x	2+2x
6+2	**BIED**-PS-P-SS-(P-PS-BIED)x	4+3x

Table 5 – In these examples the BFP function resides in the BIED and the BIED has direct access to the current measurements

Lars: Schlussfolgerung für den BFP schon hier oder am Ende?
We investigate also the path for the critical signals for a command execution with station interlocking (see Table 6 and Table 7). The command function as well as the interlocking resides in the local control IED C. The command source is the station HMI, when the command is received in the control device a fresh update of all the relevant breaker positions is required for a proper operation of the interlocking. The breaker positions are sent on change or cyclically from all relevant bays. After a release from the interlocking the command is issued to the local BIED. ~~We here summarize the expression directly~~. Lars, ich habe die Tabellen 6 und 7 nicht verstanden. Bitte Bedeutung klarstellen!

Fig	Comm.	Breaker pos.	Execution	Expression
6	4	2+4x	3	9+4x
7	4	2+2x	3	9+2x
8	4	2+2x	3	9+2x
6+2	3	2+3x	3	9+3x

Table 6 - The command execution and interlocking resides in the local control IED.

Fig	Comm.	Breaker pos.	Execution	Expression
6	6	4+4x	0	10+4x
7	4	2+2x	0	6+2x
8	4	2+2x	0	6+2x
6+2	5	4+3x	0	9+3x

Table 7 - The command execution and interlocking resides in the local BIED

We can see some general results in the Tables above. Taking the minimal communication path length as the measure for availability of the function with respect to the communication architectures we see that the generally ring topologies are better than star topologies. The figures for these topologies can be directly taken from the Table 2 in chapter VI. Some special remarks have to be added here. The best results are for the ring topologies with a combined switch both for the station and process bus. In these topologies (Figure 7 and Figure 8) we can also see a modest improvement of the availability when the functions are allocated to the BIED instead of the bay level IED.
In the above examples t (Lars: what means t, why can we state this sentence?) is invariant to the availability if there are separate control and protection IEDs or if they are integrated in a combined control and protection IED. This is expected since there was no explicit data exchange between the control and protection IEDs.

VIII. Conclusions

Considering the basic communication *architectures* discussed above, for switches with reasonable high availability the ring is an acceptable and economical, i.e. a suitable solution. The reconfiguration time is a critical issue for safety. If higher availability is needed, doubled communication networks are recommended. Having a zero reconfiguration time this solution provides higher safety also.
In HV substations, all bays are protected by redundant protection (main 1, main 2). Therefore, the related process bus has to be doubled by definition to keep away single point of failures. Sharing the process bus switches with station bus connectivity reduces the number of switches and communication ports. As already stated above, for higher availability and safety of the control function, the single controller can be connected to both communication networks. The requirement for double connections of the controller can be avoided by using combined protection and control IEDs in each of the two separate systems. By this we get also a redundant controller and a minimized number of hardware and, therefore, will get less system repairs and lower costs.
The ring provides full interoperability according to IEC 61850 and needs only switches with the same strategy for ring handling. Using devices with double connections needs for interoperability additions to the standard at least regarding supervision. Solutions with completely duplicated bay and process level needs dedicated application handling for control both in station level and process level interfaces. Regarding the impact on distributed functions, in most cases minimum path can be used which are covered by the reliability data calculated in section.

IX. References

[1] K.P.Brand, V.Lohmann, W.Wimmer *"Substation Automation Handbook"*, UAC 2003, ISBN 3-85759-951-5, 2003 (www.uac.ch)
[2] IEC 61850 *"Communication networks and systems in substations"*, 2002-2005 (www.iec.ch)
[3] K.P.Brand, M.Ostertag, W.Wimmer *"Safety related, distributed functions in substations and the standard IEC 61850"*, IEEE PowerTech 2003, Bologna, Paper IEEE_BPT03-232
[4] L.Andersson, C.Brunner, F.Engler *"Substation Automation based on IEC 61850 with new process-close Technologies"*, IEEE PowerTech 2003, Bologna, Paper IEEE_BPT03-306
[5] IEC 60870-4 *"Telecontrol equipment and systems; Part 4 – Performance requirements"*, 1990 (www.iec.ch)
[6] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.
[7] IEC 61508, Functional Safety of programmable electronic safety related systems
[8] Otto Preiss, Wolfgang Wimmer, Goals and Realisation of Integrated Substation Control Systems, DPSP&C 1994, Beijing

X. Biographies

Lars Andersson, M.S.C.S., was born in Helsingborg, Sweden, in 1960. He graduated from the Tycho Brahe Polytechnic School, Helsingborg, and studied at the Institute of Technology in Lund where he received Master of Science degrees in Computer Science in 1987. His employment experience included Swedish Royal Navy, the Institute of Technology Lund and ABB. His work with ABB has been focused on the application of communication in the substation domain and related architecture aspects. Andersson worked during 1994 and 1995 with the IEC 60870-5-103 as external expert to TC57 and been a member of the IEC TC57 since 1995, active in WG10 with the new

communication standard IEC61850. Andersson is presently working with architecture and communication by ABB Switzerland Ltd., Department for High Voltage Technology.

Klaus-Peter Brand (SM'89) was born in Neustadt/Aisch, Germany, in 1948. He studied Physics in Würzburg, Kiel, and Bonn (Germany). He got his Master (Dipl.Phys.) and his PhD (Dr.rer.nat.) from the University of Bonn. 1976, he joint the plasma physics group (SF_6) of BBC/ABB Research Center in Baden, Switzerland. From 1982, he was in different positions strongly involved developing substation automation systems and building up this business in ABB, Switzerland. He is working presently at the ABB University Switzerland as instructor and consultant. He is engaged in CIGRE B5 (former SC34). From 1995, he is being member of the AHWG and WG10 of IEC TC 57 worked from the beginning defining the standard IEC61850. He is acting now as editor and co-editor of different parts of this standard. Brand is also officer of the Swiss chapter of the IEEE PES.

Christoph Brunner (M'00), was born in Basel, Switzerland, in 1958. He M.Sc.E.E. graduated from the Swiss Federal Institute of Technology in 1983. He is member of IEEE-PES and IEEE-SA. Brunner started his career as a HW development engineer. Later he was project manager and development manager for telecontrol systems and RTUs used for utility automation. He now works as a project manager at ABB Switzerland Ltd in the business area Power Technology Products in Zurich / Switzerland where he is responsible for the communication architecture of the substation automation system. He is convenor of the WG 10 of the IEC TC57. This working group has the task to finalize and maintain IEC 61850.

Wolfgang Wimmer, was born in Bad Schwartau, Germany, in 1947. He studied Mathematics and Computer Science at the University of Hamburg (Germany), and also got there his Master (Dipl..Inf) and his PhD (Dr.rer.nat.). In 1979 he joined BBC/ABB in Baden, Switzerland. From 1983, he was in different positions strongly involved developing substation automation systems and building up this business in ABB, Switzerland. He is working presently at ABB Utility Automation, Switzerland, as principle systems engineer in the development of substation automation and monitoring systems. From 1996 he is a member of IEC TC57 WG10 working on the standard IEC61850. He is acting now as editor and co-editor of some parts of this standard.