Paper accepted for presentation at 2003 IEEE Bologna Power Tech Conference, June 23th-26th, Bologna, Italy

Safety related, distributed functions in substations and the standard IEC 61850

Klaus-Peter Brand, *Senior Member, IEEE*, Martin Ostertag, and Wolfgang Wimmer

Abstract--**In a substation, a lot of distributed, safety related functions have to be performed. IEC 61850 is intended to replace all wires by serial communication. To achieve this goal IEC 61850 has to fulfill hard real-time criteria. Starting from the definition of these criteria the communication methods of IEC 61850 are investigated. The result shows the feasibility of these methods for interlocking and illustrates their usage. Some application rules are given.**

Index Terms **– Communication, control systems, distributed functions, IEC, IEC 61850, interlocking, protection, safety, standards, substation automation, substations.**

I. Introduction

Up to now, communication in substations was made either by the conventional parallel copper wiring or by a private serial communication system mostly realized by an RTU type interface to remote network control and by an operators work place (HMI) at station level. The focus was on vertical communications. Horizontal communication especially needed for distributed, safety related functions like interlocking, protection or automatics having all hard real-time requirements was left to wires. The advent of the new standard IEC61850 [1] for all type of communication in substations raises the question if these hard real-time requirements may be provided by mainstream communication technology also [2], [3].

II. Distributed, safety related substation functions

The vertical communication is provided in most cases either as polled master-slave link or, like in IEC 61850, as client server link. No function distribution is needed and system response times in the order of 1 second are required. No hard real-time requirements have to be met since human beings are involved e.g. to operate breakers or to acknowledge alarms. Regarding disturbance recording a high amount of data may be involved.

Horizontal communication takes place normally between intelligent electronic devices (IEDs), without master device and without human interference. Most common such functions in substations are interlocking or breaker failure protection. Also protection schemes and automatics are working in this way. Many IEDs may be included in big substations, i.e. the functions may be highly distributed. A few signals are exchanged only but most of them are safety related and need response times between 1 ms and 100 ms. If we include analogue samples coming from data acquisition units in the process to protection and measuring devices, at least timing accuracy down to some few μs may be requested.

III. Fail safe vs. reliability

Reliability means that the function operates if needed. A further requirement for many substation automation and protection functions is that at least a single failure shall have no impact on the reliability. Safe means that the function never operates if not needed, especially in case of failures in its environment like in the allocated IED. A function is fail-safe, if even in case of a failure it can reach a safe state, e.g. by shutting itself down. Normally, fail-safe and high availability are contradicting requirements since e.g. reducing unwanted operations by shutting down in any case will reduce the availability also. To understand the impact of measures and analyze its behavior a Markov state model may be applied [4].

IV. Quantitative analysis

A. 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

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

0-7803-7967-5/03/$17.00 ©2003 IEEE

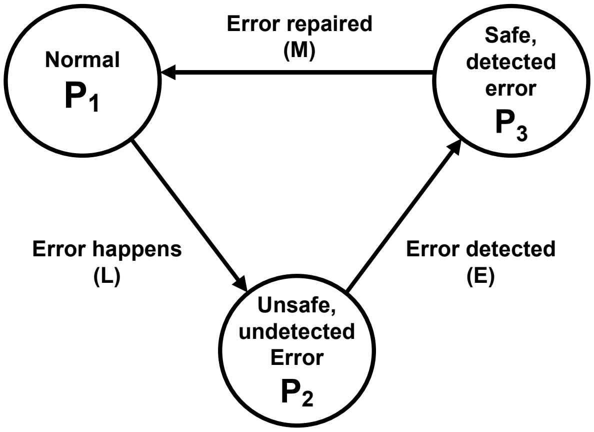

Fig. 1. Safety Markov model with three basic states for error analysis

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:

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

B. *The application to interlocking*

Interlocking safety is beneath a correct algorithm determined by the hardware on which it runs. In case of a distributed system, additionally faults in the communication system have to be considered. To model this, the logical node data model and names from IEC61850 are used. In the following the Markov model explained above is used for communication related failure situations in the (distributed) interlocking function. It is assumed that the switch control function CSWI and the interlocking function for this switch CILO are located on the same IED, however switch positions from other switches, e.g. in other bays, needed for interlocking, are sent e.g. from an appropriate CSWI switch control function via the communication system.

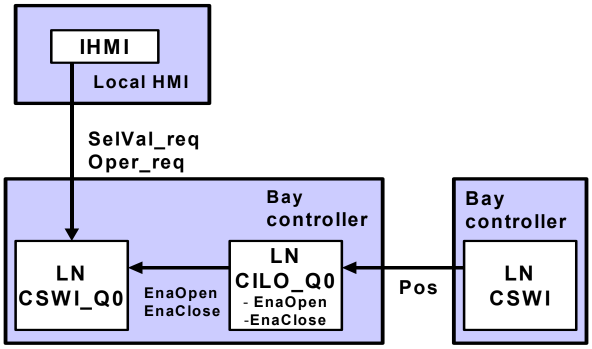

Fig. 2. Decentralized interlocking

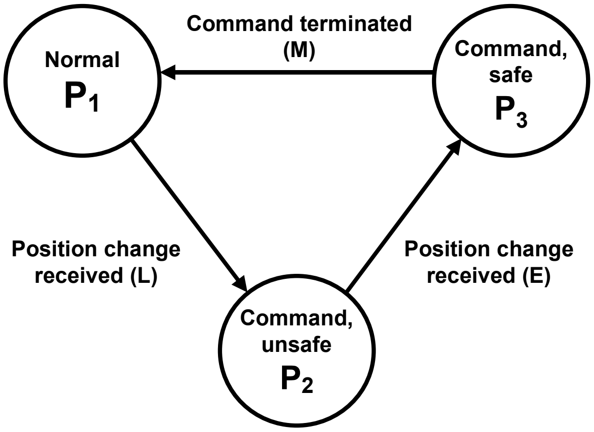

Fig. 3. Safety Markov model for Command with Interlocking

P_1 is the normal state when a command is performed (i.e. from sending a select request from the HMI until receiving the command termination or equivalent switch state change from the CSWI control function). The situation is endangered by a position change at another bay / IED, which happens with rate L and leads to state P_2, because then the CILOs interlocking algorithm uses outdated data. This rate is dependent on the number of switching operations to be performed. It is safe again, if the command executing IED has received this position change and can consider it for interlocking calculation or command block, which happens with rate E and leads to state P_3, safe command execution. This rate relates to the delay from change detection at one IED until communicated to the other IED. The command terminates with a rate M depending mostly on switch run time, leading back to normal state. The same formulas for state probability apply as for Fig. 1.

V. Real Time Features of IEC 61850

A. *The scope of IEC 61850*

The scope of IEC 61850 is the complete communication in substations. The goal of IEC 61850 is *Interoperability*, i.e. the ability of IEDs from one or several manufacturers to exchange information and use the information for their own functions. Additionally, the standard shall support the *free configuration*, i.e. all philosophies in allocation of functions to devices and control levels. It must work equally well for centralized (RTU like) or decentralized (SCS like) systems. To safeguard investments, the standard shall be future proof, i.e. provide *long-term stability*. It must be able to follow the progress in communication technology as well as evolving system requirements. IEC 61850 should replace the complete wiring in the substation.

B. *The approach of IEC 61850*

The first step is to decompose from the communication point of view all functions into smallest objects (Logical Nodes), which communicate with each other and contain all data to be exchanged according to standardized services. The second step is to split the domain specific application model (data, services) from the communication stack by a clear abstract communication service interface (ACSI). The communication stack is selected from the mainstream communication technology, i.e. it comprises MMS, TCP/IP, and Ethernet. The adaptation of the abstract model to the real communication stack is defined in a standardized specific communication service mapping (SCSM).

C. Real-time messages

Basically, the selected stack looks not very well suited to real-time requirements. IEC 61850 defines two messages for use with hard real-time conditions. One type is for information changing sporadically on events like blocking, release, tripping, and position indications, i.e. mostly Boolean data, used in peer-to-peer or horizontal communication for automatics, interlocking and protection. This message type is called generic substation event GSE. The other type is the sampled analogue value (SAV), used to permanently send streams of analog sample values. To reach proper performance avoiding unnecessary overhead, both message types are mapped directly to the link layer of Ethernet, i.e. the level 2 of the ISO/OSI model. The synchronized sampled analogue values are distributed as unconfirmed data stream, and single temporary losses of samples are handled by the application. The use of Ethernet switches may avoid also nearly all collisions (see below). The event driven messages of type GSE with single or few data values transfer safety related information, but because of the short response times needed there is also no time for confirmation and repetition on outstanding confirmation in real time. Therefore, these messages are sent immediately at time of an event (change of any data in the message) and are then repeated with an increasing time interval from T_{min} to T_{max}. The repetition with T_{max} continues forever, until the next event happens and the repetition rate starts again with T_{min} (see Fig. 4).

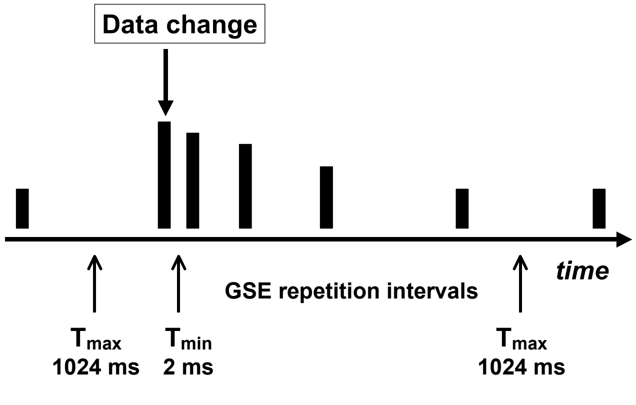

Fig. 4. The time behavior of GSE messages

This mechanism allows a very short repetition time T_{min} in case that the first message(s) after a change are lost, but lowers the bus load to T_{max} as a background traffic in case that no event happens. This T_{max} determines then, for safety related functions, the supervision time for detecting at a client that the source of data does no longer exist or does not match the needed response time, and invalidates the previously received data values. 61850 does not specify how you get from one time to the next. In the following we assume that we double the time between consecutive sendings until the maximum is reached.

The GSE implementation mechanism further lowers the busload by using Ethernet multicast, so that e.g. for interlocking the same data (switch positions) are sent with one telegram only to all clients needing them.

VI. Application of analysis on IEC 61850

A. Design criteria

There are several criteria that can be used to evaluate the feasibility of a certain solution. For the purpose of this paper, the following criteria are considered:

- For distributed functions, the same availability and safety as for protection devices is required.
- Detection of device failure and handling of a communication failure are independent.
- Failures in the electrical high voltage network and in the communication network are not correlated
- Failures of IEDs and failures in the electrical high voltage network are not correlated

Based on these assumptions, the methods described in clause IV are applied to the following distributed functions:

- Function with requested fail-safe behavior (the function uses communication to achieve a certain reaction on another IED), like interlocking.
- Function with requested reliable behavior (the function needs certain information from other IEDs in order to make a correct decision) like reverse blocking of protection.

B. Application to Interlocking

We now apply the interlocking Markov model from Fig. 3 with some typical numbers. According to

Fig. 2 the interlocking logic at an IED performing a command needs the switch states from another bay available at another IED. We assume that the switch state information from all switches needed for interlocking is distributed by a GSE message with a Tmin of 10 ms and a Tmax of 1 s. Then according to our model above, the system is unsafe at an ongoing command during the time a switch position change happens until the command executing IED has seen this change.

If we assume that no more than two consecutive GSE messages are lost (see above), the maximum communication delay (E in Fig. 3) might be calculated as follows:

- Delay by GSE transmission between repetitions (T_{min}) = 10 ms at first time, 20 ms at second time.
- Delay within the protocol stack 5 ms at each IED = 10 ms (Implementations show that even shorter times are achievable)
- Delay for change detection at source < 5 ms (if not coming via process bus)

- Delay on the communication system; this depends on the message length and the communication system. If we assume a switch loop for a redundant system with 100 Mbit/s speed, and maximum message length of 1.5 kB, this is in the order of 3 ms for highest priority messages.

These figures result in a communication delay of a first message around 18 ms, followed by a second and third message 10 ms respective 20 ms later. At maximum the first two messages can be lost, resulting in an overall maximum transmission delay from application to application of 48 ms.

In case that an IED stops sending, this can be detected latest after T_{max}, i.e. 1 s in our example calculation. This applies however only, if either the IED itself or the connecting communication system part fails.

The rate part to E depending on the normal delay then is

$$E = \frac{1000}{48} \approx 20\ s^{-1}.$$

In the case of an IED failure it is only 1 / 1 = 1 s^{-1}. For an IED with MTTF of 50 years or more this may be, however, neglected because it only happens if the IED fails and at the same time a switch at the failed IED is operating.

We now assume 10 switching operations per day (relatively high for HV, but low for MV). This leads to

$$L = \frac{10}{24 \cdot 60 \cdot 60} s^{-1}.$$

Last but not least we assume a switch running time of 20 ms, e.g. for a HV circuit breaker, leading to

$$M = \frac{1000}{20} = 50 s^{-1}.$$

For disconnectors this rate would be even lower leading to higher safety, therefore above value is good to use.

The result is a safety figure of S = 0.999994, which fulfills the highest safety integrity level (SIL 4) according to IEC 61508 [5] and is also in the order expected for protection.

It should be noted that by using additionally some algorithm prohibiting that two commands can be given at the same time reduces the value of L independent from the real rate of switching operations, decreasing the unsafety for interlocking further by some powers of 10^{-1}.

C. Application to protection

For communication between protection functions the IEC standard 60834 [6] demands a maximum communication system delay of 20 ms. As shown in [7], a GSE with T_{min} = 4 ms can fulfill this requirement, if both IEDs are directly connected. If however a more complex communication system architecture is used, then at least any additional delays e.g. by successive switches between the concerned source and destination IEDs must be below 2 ms.

The question of safety has to be addressed according to the function. If GSE is used for reverse blocking, then a blocking signal may be missed or come too late – the protection works even if not necessary, which is safe but may decrease power availability. This shows that protection safety is related to the availability of the communication network as described in [8]. If GSE is used for breaker failure, then a missing or late telegram with a change intended to trigger the breaker failure trip may lead to a missing trip, i.e. safety might be endangered.

VII. Influence of Ethernet implementation

A. Physical disturbances and fiber optics

The EMC environmental conditions in substation automation call for very robust physical communication media. IEC defined different integrity classes for data communication (see [9]). For commands and critical information transmission, a residual error rate of 10^{-14} is recommended. To achieve this, a sufficiently low bit error rate is required in addition to error detecting techniques as the CRC for Ethernet [10]. Also to keep loss of GSE messages due to temporary disturbances at the assumed level of maximum two consecutive ones, the bit error rate must be sufficiently low. For the substation requirement, this means that while it might be feasible to use copper transmission media within a cubicle, fiber optic connections are required for interconnection of cubicles or separately mounted IEDs.

B. Media access problems and switches

Traditional Ethernet as described in many textbooks uses CSMA/CD as media access method. All stations on the network sense collisions before and also while transmitting data. Based upon a back-off algorithm, one station will win bus arbitration and gain access to the network. The available bandwidth is shared between all devices connected to the LAN segment, and practically limits the usage of the available bandwidth to a maximum of 40%. However, using layer 2 switches in a modern LAN can significantly improve the overall usable bandwidth [11]. With Ethernet Switches, collisions can be completely avoided in the network. Each link between the Switch and the attached device can be operated in full duplex mode. Packets that would collide otherwise are queued in the switch (if they have to go to the same switch output port) and are sent one after the other instead of blocking the whole network. However it should be checked then that the overall queuing buffer capacity is sufficient not to loose messages in the worst-case situation.

C. Flow control, VLAN and Priorities

In addition to the real-time traffic considered up to now, also other types of communication traffic will occur in a real system. Examples for this are vertical communication like sending reports, or giving commands to IEDs. Also, disturbance data or configuration data traffic will use the same physical network. IEEE 802.1p and 802.1Q define mechanisms that can be used to shape the traffic on the network according to the needs of the application. 802.1p defines 8 different priorities that may be used on Ethernet level. The switches connecting the IEDs can use this information to handle packets with different priorities using different queues. Commercially available switches today mostly support two different priority classes. According to

IEC 61850 priorities have to be used for GSE and SMV services, to decouple the real time related traffic from the background traffic [12]. Another means to isolate especially the multicast traffic that is used for sampled values and the GSE communication are virtual LANs (VLANs) as defined in IEEE 802.1Q. Based on the VLAN tag included in a packet, or based on the port a packet arrives on, the Ethernet switch will not forward multicast traffic to all its outgoing ports but only to a subset of those ports, namely the ports that belong to the same virtual LAN.

VIII. Conclusions

The discussed examples proof that IEC 61850 with its mapping to Ethernet can be used also for safety related, distributed functions in substations if the proper design measures are taken into account.

These measures include in particular

- the use of optical connections for all links that are exhibited to the harsh EMC conditions found in high voltage substations. This refers especially to connections between cubicles, and to IEDs mounted close to the primary equipment,
- the use of switched Ethernet to reduce collisions in the network [3]. The additional delays resulting from store-and-forward technology are compensated by high link speeds of 100 Mbps and a suitable communications architecture,
- the use of priority and VLAN features in the switched Ethernet in order to separate the real time related messages from the rest and restrict its flow to those network parts where it is needed, and
- a communications architecture that takes the required worst-case response times into account.

Throughout the discussions, it was assumed that in maximum two consecutive messages would be lost. The measures above help to ensure this. Under these assumptions, the optimal handling between minimum and maximum time for GOOSE messages is: keep minimum time for two repetitions, and then go to maximum time directly.

Although IEC61850 allows real time features, the number of messages for this purpose to run concurrently on the same network or VLAN is restricted by the bus capacity, the communication system architecture, and the amount of queuing space in the switches. Therefore a thorough analysis of the communication system architecture in relation to the worst-case communication load for real time data has to be performed.

IX. References

[1] IEC 61850 "*Communication networks and systems in substations"*, (publishing of standard parts in progress), 2002-2003

[2] J. T. Tengdin "*Synch Check with Distributed Voltages and GOOSE*", IEEE PES Summer Meeting, 1998

[3] T. Skeie, S. Johannessen, and Ch. Brunner; "*Ethernet in Substation Automation*", IEEE Control Systems Magazine, 22(3): 43-51, June 2002.

[4] EWICS TC7, *"Dependability of critical computer systems*", Elsevier Applied Science, London, 1988

[5] IEC 61508 *"Functional safety of electrical/electronic/programmable electronic safety-related systems*"

[6] IEC 60834 International Standard, *"Performance and Testing of Teleprotection Equipment of Power Systems*", International Electrotechnical Commission, 1988

[7] G. W. Scheer, D. A. Woodward "*Speed and Reliability of Ethernet Networks for Teleprotection and Control*"

[8] G. W. Scheer, D. J. Dolezilek *"Comparing the Reliability of Ethernet network Topologies in Substation control and monitoring networks"*

[9] IEC 60870-5-1 "*Telecontrol equipment and systems – Transmission protocols – Transmission frame format"*, 1990

[10] W. Stallings *"Local and Metropolitan Networks"* (6th ed.), Prentice Hall, 2000

[11] J. J. Roese *"Switched LAN's: Implementation, Operation, Maintenance",* McGraw Hill, 1998

[12] T. Skeie, S. Johannessen, and O. Holmeide, "*The Road to an End-to-End Deterministic Ethernet*", In Proceedings of 4th IEEE International Workshop on Factory Communication Systems (WFCS'02), September, 2002.

X. Biographies

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.

Martin Ostertag was born in Mannheim, Germany, in 1965. He graduated from the Electrical Engineering department at the University of Karlsruhe in 1991, where he also received his PhD (Dr.-Ing.) degree for a work on nonlinear optimization if Airbag Release Algorithms. He joined ABB Corporate Research in Baden-Dättwil / Switzerland in 1996, where he worked on distribution line communication systems. Presently, he is working at ABB Switzerland Ltd, Utility Automation Systems, where he is responsible for research and development for substation automation and protection.

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 Switzerland Ltd, Utility Automation Systems, as principle systems engineer in the development of substation automation and monitoring systems. From 1996 he is a member of IEC TC57 WG11 working on the standard IEC61850. He is acting now as editor and co-editor of different parts of this standard.