# REDUNDANCY FOR POWER UTILITY COMMUNICATION NETWORKS

***Fred Steinhauser***

*Power Utility Communication, OMICRON electronics, Klaus, Austria*
*fred.steinhauser@omicronenergy.com*

**Keywords**: Redundancy, PRP, HSR, IEC 61850, Digital Substation

## Abstract

Redundancy has always been a topic for the protection, automation, and control (PAC) of electrical power systems. Where deemed required, there were duplicated systems deployed. The duplicated protection systems typically got their information from different CT/VT cores and issued their commands to dedicated trip coils of the circuit breakers. The systems were named "Main" and "Backup" or "Main 1" and "Main 2" or so. This caused considerable efforts. If certain installations were regarded as not so important, compromises were made by saving parts of the duplications or by applying no duplication at all.

The experiences from these PAC systems and the classification of the importance of the assets and the related amount of duplication could also be a guidance for the selection of an appropriate degree of communication network redundancy. Possibly, the expenses for a highly redundant communication network architecture are not adequate for an installation that would not have had any duplicated systems when implemented in conventional technology. On the other hand, fully redundant communication networks appear only logical in substations where fully duplicated PAC systems had been deployed in the past.

## 1. Introduction

With the proliferation of IEC 61850, the topic of redundancy has (again) gained much interest regarding the resilience of the substation communication networks, which are also called Station Bus and Process Bus in this context.

In particular, the lack of recognized communication network redundancy concepts has hindered the proliferation of Sampled Values in the beginning. In addition to a self-healing property that compensates for a broken piece of communication network equipment over time, also "bumpless redundancy" is required in such applications, which means that no data packets will be lost even in the case of one communication network component failing.

In the meanwhile, IEC 61850 has accounted for this by adopting two concepts for redundant communication networking from IEC 62439: HSR (High Availability Seamless Redundancy) and PRP (Parallel Redundancy Protocol). Both options provide the mentioned bumpless redundancy. They are based on different concepts and both have their pros and cons. The selection of the one or other option for the substation communication network is an important task of the system design. The technical report IEC 61850-90-4 (Network engineering guidelines) supports the system designers in this process.

So, while the problem is technically solved and suited options are available, the selection of the best suited communication architecture still remains a challenge. It starts at the clear formulation of the requirements that may preferably be derived from the importance of the assets managed by the PAC system. Experience and common sense are then needed to come up with an adequate and economical solution.

## 2. Redundancy of Protection, Automation, and Control Systems

Depending on the importance of systems, which is mainly determined by voltage level and supplied customers / assets, there is an established practice of applying at least redundant protection systems.

### *2.1 Duplicated Protection Systems*

The protection of important assets in the power system is commonly built with redundancy. Typically, this is done by duplicating parts of the system, mostly the protection relays itself. This is not only done to cope with the complete failure of a relay, but also to compensate for functional problems under unexpected conditions.

The naming for two relays varies from utility to utility, they may be called "Main" and "Backup", "Main 1" and "Main 2" or "X" and "Y" and so on. In the following, the main/backup notation shall be used, with the abbreviations "M" and "B" used in the figures.

The logic to connect the decision of the two protection relays is as simple as it can be: it is an OR connection. If any of the two protection relays trips, the circuit breaker is tripped.

The OR connection is implemented by duplicated trip coils at the circuit breaker, which itself is not duplicated. A breaker failure will not be cleared by a "backup breaker" installed in series next to the "main breaker". The breaker failure protection scheme must invoke breakers located at adjacent locations. The simplistic trip logic allows the implementation of this redundant scheme with relatively small efforts.

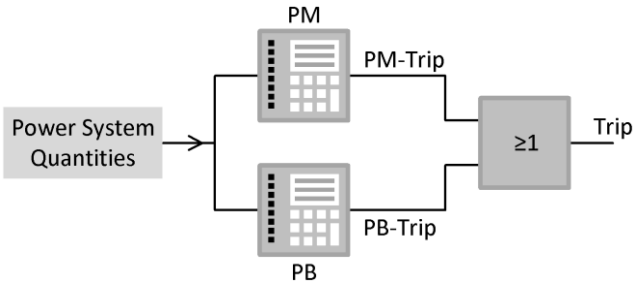


Figure 1 Duplicated protection relays with OR-ed trip

The assumed maloperation of a relay is that it does not react on a power system fault. This may not only come from a complete failure that entirely deactivates the relay, but also because of a weakness of the protection algorithm, that may not recognize certain power system faults. To avoid that both, the main and the backup relay have the same blind spot, these relays are not identical models. Mostly, the backup relay even comes from a different manufacturer than the main relay. Where this mix of brands is not desired, the backup relay must then work with a different operation principle. For instance, the LR91 from BBC [1] or the RALDA from ASEA (directional comparison relays) did complement the distance relays from these manufacturers to serve such schemes out of the portfolio of one manufacturer.

Another type of maloperation, the nuisance trips and related countermeasures, are out of the scope of this paper.

### *2.2 Duplicated Control Systems*

With the proliferation of combined protection and control devices, it is imaginable that the control functions will also exist in a duplicated form when the protection functions are duplicated. But making use of this duplication is by far not as straightforward as with protection.

The matter of selecting the correct control action if the two control devices do not agree is not as trivial as OR-ing two trip signals. The number of input and output signals is much higher and the connections to the assets are much more complex. Consequently, the control logic is also complex.

If there are two instances making contradicting statements, which one is correct? There is no independent proof to verify the one or the other. In high availability control system, a majority voting scheme (e.g. two out of three) is employed. It is obvious that more than two instances are needed to implement this. The NASA Space Shuttle had five computers on board and synchronizing their operation was a challenging task on its own.

What is possibly imaginable is having a backup control system in standby, which is only invoked if the active main control system has obviously failed. This could be deduced from a watchdog function, e.g. the periodic reception of integrity reports at the control centre.

If the main control device has failed, the control centre could switch over from the main control (CM) to the backup control (CB). At any moment, only one of the two control systems is active, which is not really a redundant scheme.

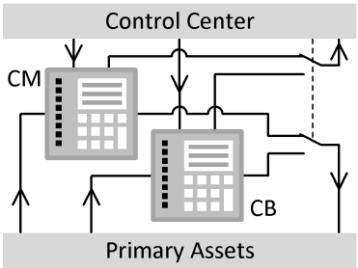


Figure 2 Main or backup control function explicitly invoked from the control centre.

As the wiring of the control device to the primary assets can be very extensive, the duplication of the control system also requires a duplication of this wiring, which is prohibitive with classical hard-wired technology. Such a switching scheme seems only doable with IEC 61850, where the wiring efforts are reduced to a few network connections and the switching action can be performed by activating/deactivating certain messages.

With the deployment of combined protection and control devices together with IEC 61850 communication, such systems would become feasible with reasonable efforts.

## 3. Communication Network Redundancy

With the introduction of power utility communication protocols as IEC 61850 that replace most of the classical hard-wiring with message exchange over a communication network, this power utility communication network became a mission critical part of the protection, automation and control system.

Failures in such communication networks must not lead to a disruption of services and this is ensured by network redundancy.

This became a topic when real-time messaging over communication network was introduced. GOOSE messages used for interlocking or even tripping must be reliably forwarded and delivered with minimal delay. Interruption of the message transmission for, let' say, the duration of about one cycle of the power system, may already impair the function of the protection and control system.

With the application of Sampled Values, this issue becomes even more severe. Protection algorithms will struggle to react properly on faults in the power system if the measurements from only a fraction of a cycle are missing.

The initial lack of proper redundancy options for the process bus was an impediment for the proliferation of Sampled Values, which has been resolved in the meanwhile.

IEC 61850 did not invent its own network redundancy mechanisms. Following the principle of building on established communication technologies (as with choosing Ethernet for local networks), options from the standard IEC 62439 were proposed for the use in power utility communication networks.

Of course, such redundancy mechanisms add efforts to the power utility communication system. This comes in terms of additional networking equipment and dedicated features implemented in all connected devices.

### *3.1 A disclaimer on the Spanning Tree Protocol*

Unfortunately, Ethernet networks managed by the Spanning Tree Protocol (STP), or more commonly its accelerated (rapid) version RSTP, are often discussed or even considered as a redundancy mechanism as well. To be clear: the "R" in RSTP has nothing to do with *ring* or *redundant*, it stands for *rapid*, and even this suggestion of fast action must be seen in relation to the relevant time scales in a substation communication network.

Promotors of RSTP emphasize on the ring structures that allow for re-routing traffic if some components in the ring fail. But it must be clearly noted that there is one thing that must not exist in an Ethernet network: a ring, technically called a *loop* in the context of STP. The genuine purpose of STP is to eliminate loops, configuring the network always to become a tree. It does so by evaluating "weights" for the switches and links and deactivating certain links and putting them in stand-by. To ensure that this tree spans as desired, some configuration in the switches is required, otherwise the tree configuration will be random, giving a message routing which is most likely not optimal. If an active switch or link fails, the STP mechanism will again kick in and reconfigure the tree by re-activating some of the stand-by links. This provides a kind of a self-healing mechanism, which is a by-product of STP, but not its primary purpose. The time required for the reconfiguration is not exactly defined and even with the "rapid" version it may take several hundred milliseconds. In an office network, it does not matter if a letter comes out of a printer one or two seconds later (or if the print job must be restarted), but in a substation environment such behaviour cannot be considered as redundant. Or in other words: in substations, STP should only be used where redundancy is *not* required.

Similar to the case with the duplicated control devices explained above, only one single path for the message exchange is active at any given time, with no path being available at all during reconfiguration of the network. This discriminates STP from genuine redundancy mechanisms, where two paths are always active during normal operation.

Thus, we will not consider RSTP as a serious redundancy option here.

### *3.2 "Bumpless" Redundancy*

The somewhat unpolished expression *bumpless* denotes a mechanism that ensures that no data packets are lost in a communication system, even if a network component fails. This is achieved by duplicating the messages, so that any receiver obtains the information via two different paths as long as all components are sane. If one path fails, the delivery of the information over the still working path is maintained.

The components in such a redundant system must be capable to cope with these duplicated messages. In particular, there must be a mechanism to detect and discard duplicates to either avoid endlessly circulating packets in networks or misinterpretation of the information in the receivers.

IEC 61850 has chosen the PRP and HSR redundancy protocols described in IEC 62439-3 [2] for the use in power utility communication networks. The application in this domain is explained in detail in the technical report IEC 61850-90-4 [3].

As a complementing measure, supervision of the communication components is required to become aware that a component has failed and that the communication system is then operating without further redundancy left. The failed component must then be replaced as quickly as possible to re-establish redundancy.

For the power systems protection engineer this may appear similar to an alert that a single-phase-to-ground fault has happened in an isolated or compensated power network. While the operation of the network is still possible in this state (at least for a while), action must be taken before a double ground fault occurs.

### *3.3 Parallel Redundancy Protocol*

The Parallel Redundancy Protocol (PRP) utilizes two networks (commonly called LAN A and LAN B) that deliver the messages in parallel between the senders and receivers. Also following the conventions used in most materials related to IEC 62439-3, LAN A is shaded with a reddish colour and LAN B in a greenish colour in the figures.

The devices participating in this redundant scheme are so called Doubly Attached Nodes (DANs) which have two ports dedicated for the connection to LAN A and LAN B.

A device sending the duplicated messages on the two LANs adds information at the end of the data packet (the Redundancy Control Trailer, RCT) which is used by the receivers to identify pairs of duplicated messages. As these trailers are just added at the end, the contents of the original packets up to their specified length remain unchanged and the RCTs are ignored by PRP unaware devices. On the other hand, The PRP devices will accept and respond properly also to packets without an RCT.

This provides the benefit that devices with normal (non-PRP) Ethernet communication which are not aware of PRP can also be connected as Singly Attached Nodes

(SANs) to one of the two LANs and participate in the communication.

This is very useful for connecting devices for which redundancy is not required, for instance devices of minor importance, PCs used for configuration and maintenance, or test equipment.

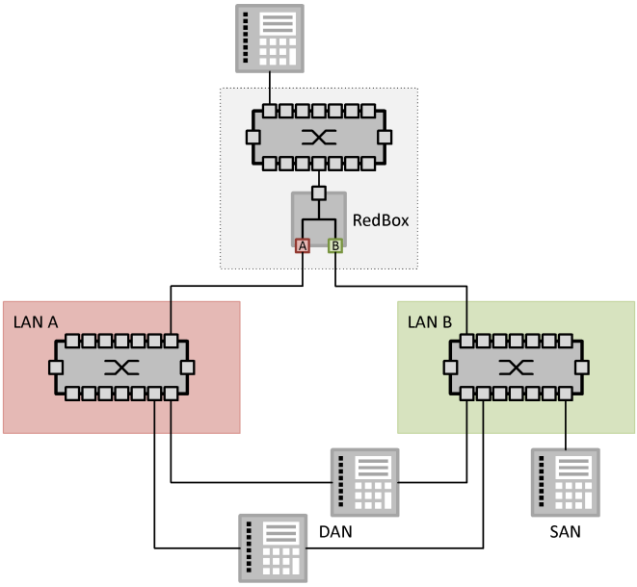


Figure 3 Basic concept of a PRP network

In Figure 3 above, a very basic PRP architecture with some connected components is shown. The two LANs A and B are depicted in their most simple form, which is a single Ethernet switch. But these networks can be as large as needed, using any layout deemed appropriate. The two networks do not even have to be of identical layout or run on identical link speeds. Due to the arbitrary size of the LANs, this architecture scales well and supports large numbers of IEDs. And there is one absolute no-go: there must be no direct connection between the two LANs, this would break the system immediately.

On top of the two LANs, there is a RedBox (Redundancy Box) drawn, which connects non-PRP devices (like the one on top of Figure 3) to the redundant communication system. Often, such RedBoxes are combined with an Ethernet switch to provide this function for multiple devices. The SAN connected to LAN B can communicate with the DANs and the IED in the top as well, but of course without any redundancy.

RSTP aficionados also propose to use RSTP for the PRP LANs. But it is questionable if the small benefit of the self-healing property of STP makes up for the required configuration and management efforts if the whole communication system is anyway covered by PRP.

PRP has established itself as the method of choice for station buses with a large number of IEDs, but it is also suited to be used for the process bus.

### *3.4 High-availability Seamless Redundancy*

Figure 4 below shows a basic High-availability Seamless Redundancy (HSR) network, which basically consists of a ring structure. There are no additional Ethernet switches in the HSR ring, but all devices in the ring must support the HSR protocol.

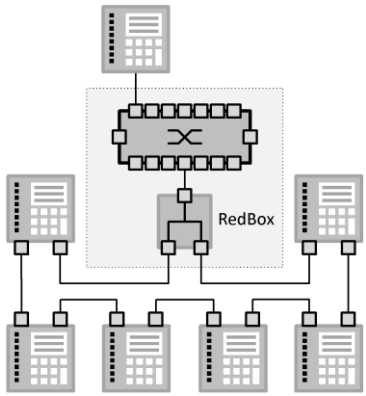


Figure 4 Basic concept of an HSR network

Such a system can be cost effective, since no additional switches are required to build the HSR ring itself. In turn, devices without HSR capabilities can be only connected through a RedBox, there is no option like for SANs in PRP networks.

Being simple and lean, HSR networks do not scale as well as PRP networks. The suggested upper limits vary from 16 to about 40 IEDs per HSR ring [4][5]. The actual limit depends on link speed and if a store-and-forward or cut-through mechanism for forwarding the packets is applied in the nodes. There are options for segmenting HSR networks and coupling HSR rings of more decent size to form larger HSR systems. But such network architectures tend to become more complex and due to the added coupling devices, the hardware cost benefits of HSR get diminished.

From the properties described above, HSR seems to be a suited choice for connecting a limited number of IEDs that shall be closely connected to each other, as in a process bus segment spanning only over a few feeders.

### *3.5 Combined PRP-HSR architectures*

As has been explained in the two preceding chapters, PRP and HSR have their specific strengths and weaknesses and it may be desirable to apply both of them for specific parts of a power utility communication network.

One example is to use PRP for the station bus and to combine it with an HSR ring for the process bus. The coupling between the two buses is performed with two RedBoxes. The two RedBoxes are required for the sake of redundancy and to cater for the case that one of the RedBoxes fails.

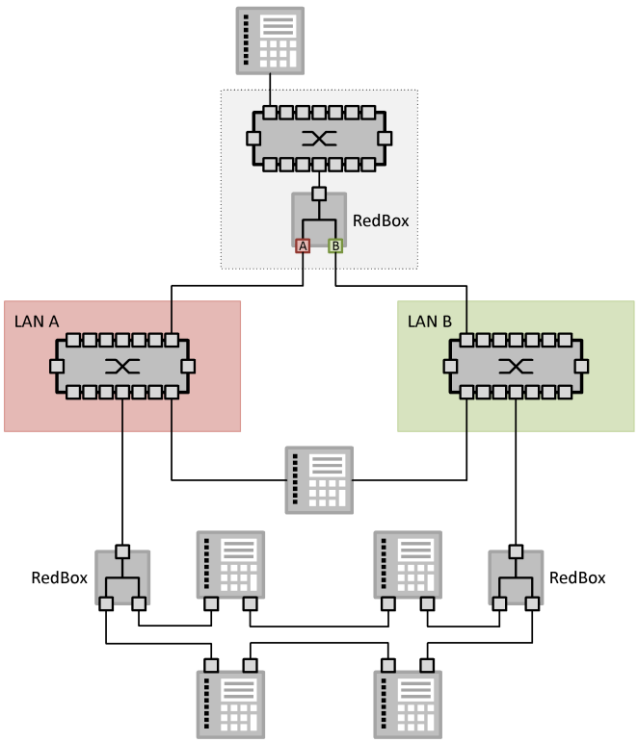


Figure 5 Coupled PRP and HSR networks

The two RedBoxes in Figure 5 coupling the PRP and the HSR network operate in a special coupling mode. As they are both duplicating messages which are already duplicated in the PRP network, there would be four copies of a message in the HSR ring. The two RedBoxes are aware of each other and discard excessive duplicates, so that only one duplicate of a message is traversing the HSR ring in each direction.

The three network layouts shown above are only very basic sketches outlining the principles. There are many options and in practice, the networks have many more IEDs, other devices, and network components connected. One common challenge for instance is the redundant connection of duplicated clocks and building a redundant time synchronization system.

## 4. Conclusion

Redundancy has always been applied in protection, automation, and control systems for important assets. The protection concepts with main and backup relays are well standardized in the industry.

With the proliferation of IEC 61850 and moving the information transfer from hard-wired signals to message exchange over the power utility communication network, this network became a mission critical part, so redundancy was required for the communication network as well. This applies in particular when using Sampled Values for delivering the measurements from the power system to the protection relays. Thus, redundant communication networks are a precondition for the Digital Substation.

The redundancy mechanisms PRP and HSR serve this requirement. The two concepts have their specific strengths and can be even combined. But there is no ideal network architecture that serves every need equally well. Thorough thought must be given to select a design that best fits a specific protection, automation, and control system.

## 5. References

[1] Engler, F., Lanz, O., Hänggli, M., Bacchini, G.: Transient Signals and their Processing in an Ultra High-Speed Directional Relay for EHV/UHV Transmission Line Protection. IEEE/PES 1984 Summer Meeting, Seattle.

[2] IEC 62439-9: Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). IEC TC 65/SC 65C, 2016.

[3] IEC TR 61850-90-4: Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines. IEC TC 57, 2020.

[4] Grasset, H.: Optimizing Protection and Control Schemes Based on GOOSE Messages. Schneider Electric White Paper 998-2095-01-19-15AR0, 2015.

[5] Hunt, R., Popescu, B.: Comparison of PRP and HSR Networks for Protection and Control Applications. Western Protective Relay Conference, Spokane, 2015.