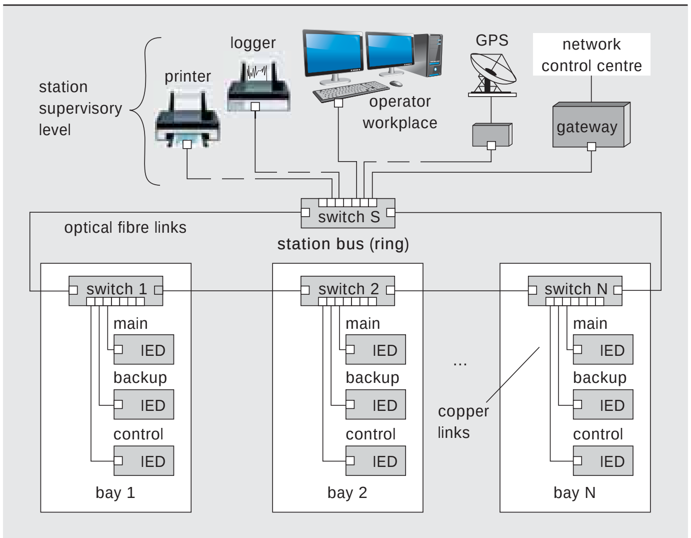
Seamless redundancy

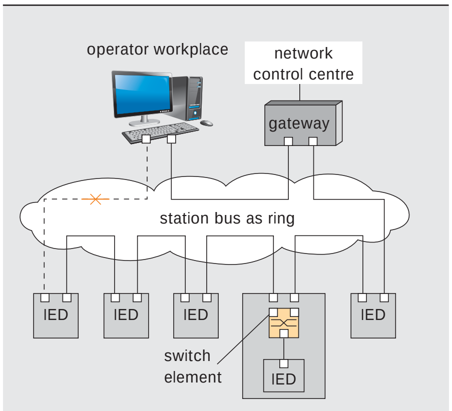
Bumpless Ethernet redundancy for substations with IEC 61850

HUBERT KIRRMANN – The IEC 61850 standard has become the backbone of substation automation, allowing for the first time interoperation between protection, measurement and control devices from different manufacturers on the same Ethernet local area network, station or process bus. This network is duplicated in substations that require a very high availability. Interoperability requires that all devices use the same redundancy concept. IEC 61850 now specifies a network redundancy that fulfills the requirements of substation automation, for the station bus as well as for the process bus. It is based on two complementary protocols defined in the IEC 62439-3 standard: parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR) protocol. Both are able to overcome the failure of a link or switch with zero switchover time, while allowing clock synchronization according to IEEE 1588 to operate reliably. Developed by ABB in collaboration with other companies, both PRP and HSR will be part of the second edition of the IEC 61850 standard.

1 A non-redundant station bus



2 A ring with switching end nodes



The IEC 61850 standard replaces the numerous busses and links in use today by a hierarchy of well specified switched Ethernet networks, namely the station bus between the bays and the process bus within a bay. To achieve interoperability, IEC 61850 Edition 2 specifies in greater detail the underlying protocols of these busses. Two indispensable network features for a real-time system are given particular attention: time synchronization and network redundancy. Time synchronization is solved by the simple network time protocol (SNTP) [1], with stricter requirements taken care of by the IEEE standard 1588 [2]. Redundancy was a major hurdle, since the lack of a commonly accepted redundancy protocol prompted manufacturers to market incompatible proprietary solutions.

IEC 61850 edition 2 now includes two redundancy protocols, which are defined in the IEC standard 62439-3 [3] and applicable to substations of any size and topology for the station bus as well as for the process bus: parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR). In both protocols, each node has two identical Ethernet ports for one network connection. They rely on the duplication of all transmitted information and provide zero-switchover time if links or switches fail, thus fulfilling all the difficult real-time requirements of substation automation.

PRP (IEC 62439-3 Clause 4) specifies that each device is connected in parallel to two local area networks of similar topology. HSR (IEC 62439-3 Clause 5) applies the PRP principle to rings and to rings of rings to achieve cost-effective redundancy. To this effect, each device incorporates a switch element that forwards frames from port to port.

IEC 61850 network topology

IEC 61850 encompasses two busses based on switched Ethernet technology [4]:

- The station bus [5] interconnects all bays and the station supervisory level; it mainly carries control information, such as measurements, interlocking and select-before-operate. Typically the manufacturing messaging specification (MMS) protocol is used to transfer data between station level and bay level intelligent electronic devices (IEDs) while generic object oriented substation events (GOOSE) looks after bay IED to bay IED data transfer.
- The process bus [6] interconnects the IEDs within a bay and mainly carries measurements, known as sampled values (SV), for protection. The SV are sampled at a nominal value of 4 kHz in 50 Hz grids (4.8 kHz in 60 Hz grids).

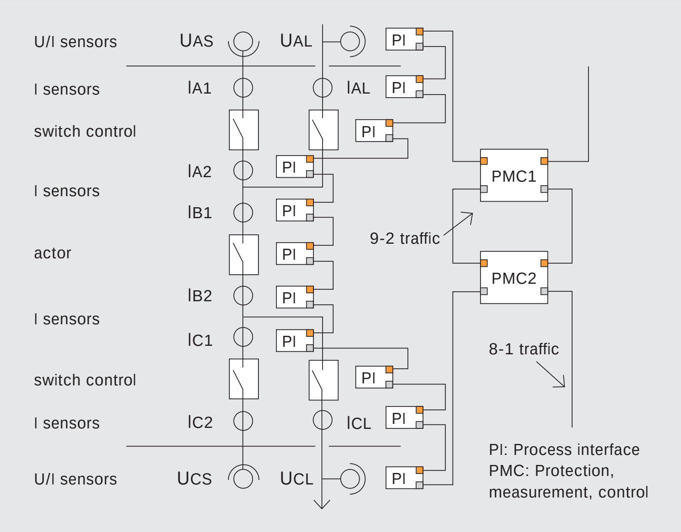
IEC 61850 does not prescribe a topology, tree, star or ring. Indeed, the same physical Ethernet network could carry both the station and the process bus traffic.

For the station bus, the network topology generally adopted in large substations is that each voltage level uses a ring of switches, which connect the main protection, backup protection and control IEDs → 1. In smaller medium-voltage substations, a cost-effective arrangement uses IEDs that include a switch element, which can be chained into a ring topology, making the network resilient to the loss of one link → 2.

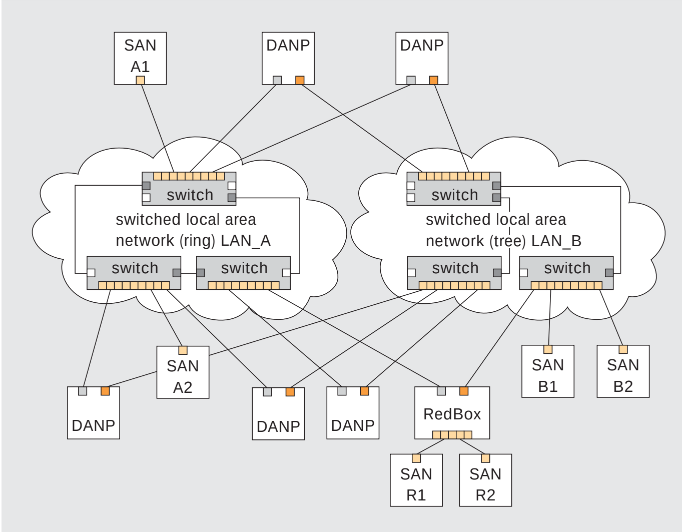
In large substations, the different voltage level rings are connected to the station level in a tree formation, allowing the station bus to exhibit a mixed ring and tree topology. Alternatively, a ring of rings formation can also be used.

At the process bus level, IEDs are typically simple measurement and control devices connected to the protection and control

3 A process bus topology



5 Redundancy in the nodes



4 Recovery times compiled by the IEC TC57 WG10

Communicating partners	Communicating partners	Recovery Time
SCADA to IED client-server	station bus	100 ms
IED to IED interlocking	station bus	4 ms
IED to IED reverse blocking	station bus	4 ms
bus bar protection	station bus	0 ms
sampled values	process bus	0 ms

units, which interface to the station bus ➔ 3. A ring topology at this level also offers a cost-effective wiring solution.

Timing requirements in substation networks

The timing requirements for the station and process buses are distinct; they dictate how redundancy is used.

The time during which the substation tolerates an outage of the automation system is called the "grace" time, and the network recovery time must be lower than the grace time. As well as applying in cases of failure, the recovery time also applies to the reinsertion of repaired components.

When the station bus carries only command information, delays of some 100 ms are tolerated. However, a delay of only 4 ms is tolerated when interlocking, trip and reverse blocking signals are carried, although it is unlikely that a failure will take place exactly when an (infrequent) control sequence is issued. The process bus, which carries time-critical data from the measuring units, requires a deterministic mode of operation, with maximum delays in the order of 4 ms. The recovery times compiled by IEC technical committee 57 (TC57) working group 10 (WG10) are summarized in ➔ 4.

Redundancy will be regularly checked at intervals of less than one minute for the complete network. Only one device, station operator or gateway to the network communication center (NCC) is needed to monitor the network. Configuration errors are reported to the station operator or the NCC gateway.

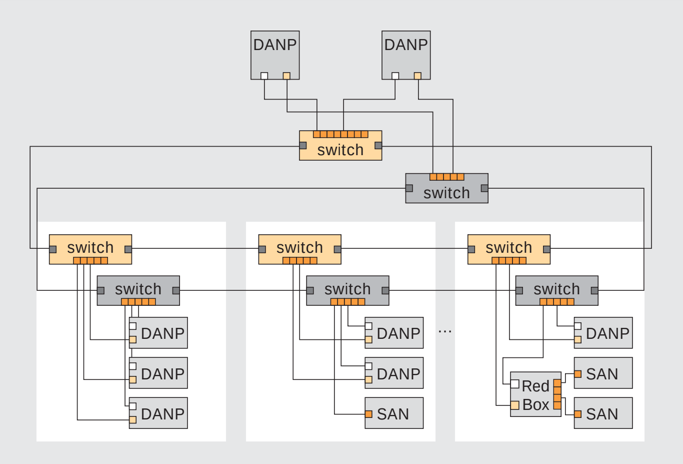
Highly available network topology

IEC 62439 [3] is applicable to all industrial Ethernet networks [7], since it considers only protocol-independent methods. It contemplates two basic methods to increase the availability of automation networks through redundancy:

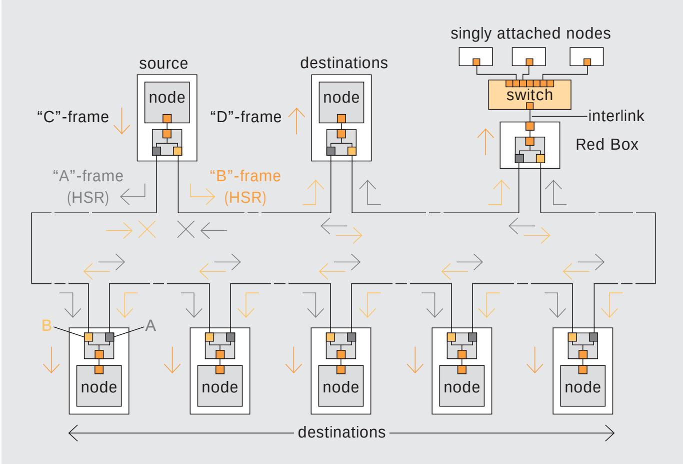
- Redundancy in the network. The network offers redundant links and switches, but nodes are individually attached to the switches through non-redundant links. The gain in availability is small since only part of the network is redundant. Redundancy is normally not active, and its insertion costs a recovery delay. A typical example of such a method is the rapid spanning tree protocol (RSTP IEEE 802.1D [8]). However, RSTP can only guarantee a recovery time of less than a second in a restricted topology. Nevertheless, RSTP is a good choice for the station bus in non-redundant systems, such as that shown in ➔ 1.

In a redundant network, the most important parameter is the recovery time needed to restore error-free operation after a failure. Both PRP and HSR offer zero recovery time.

6 A duplicated station bus with parallel redundancy protocol (PRP)



7 A high-availability seamless redundancy (HSR) protocol ring



- Redundancy in the nodes. A node is attached to two different redundant networks of arbitrary topology by two ports → 5. Each node independently chooses the network to use. This scheme supports any network topology; the redundant networks can even exhibit a different structure. The cost of implementing this redundancy method is about twice that of the redundancy method discussed in the previous bullet, but the gain in availability is large. The only non-redundant parts are the nodes themselves.

With regard to PRP, IEC 62439-3 Clause 4 specifies redundancy in devices in which the nodes use the two networks simultaneously. This offers zero recovery time, making PRP suited for all difficult real-time applications.

IEC 62439-3 Clause 5 defines another redundancy-in-the-nodes solution with HSR, in which a switch element is integrated in each device. The operating mode is the same as for PRP.

PRP operating principle

Each PRP node, called a doubly attached node with PRP (DANP) is attached to two independent local area networks (LANs) operated in parallel. The networks are completely separated to ensure failure independence and can have different topologies. Both networks operate in parallel, thus providing zero-time recovery and the continuous checking of redundancy to avoid lurking failures → 5.

Non-PRP Nodes, called singly attached nodes (SAN) are either attached to one network only (and can therefore communicate only with DANPs and SANs attached to the same network), or are attached through what is known as a red box, a device that behaves like a DANP → 6.

The nodes detect the duplicates with a sequence number inserted in the frames after the payload. This allows full transparency of PRP (DANP) and non-PRP (SANP) nodes. The complete PRP protocol can be executed in software. Node failures are not covered by PRP, but duplicated nodes may be connected via a PRP network.

HSR

HSR applies the PRP principle of parallel operation to a single ring, treating the two directions as two virtual LANs. This allows a significant reduction in hardware costs because no switches are used and only one link is added. However, all nodes of the ring must be switching nodes, ie, they have two ports and integrate a switch element, preferably implemented in hardware, as shown in → 7.

PRP offers easy integration of non-redundant devices, while HSR offers cost-effective ring topologies.

For each frame sent, a node sends two frames – one over each port. Both frames circulate in opposite directions over the ring and every node forwards the frames it receives from one port to the other. When the originating node receives a frame it sent itself, it discards it to avoid loops; therefore, no special ring protocol is needed.

To detect duplicates, the Ethernet frames include a sequence number incremented by the source for each sent frame. Contrary to PRP, the sequence number is not inserted after the payload, but in the header so the switch element can recognize the duplicates before they are received entirely. Therefore, cut-through operation with less than 5 µs per node is possible.

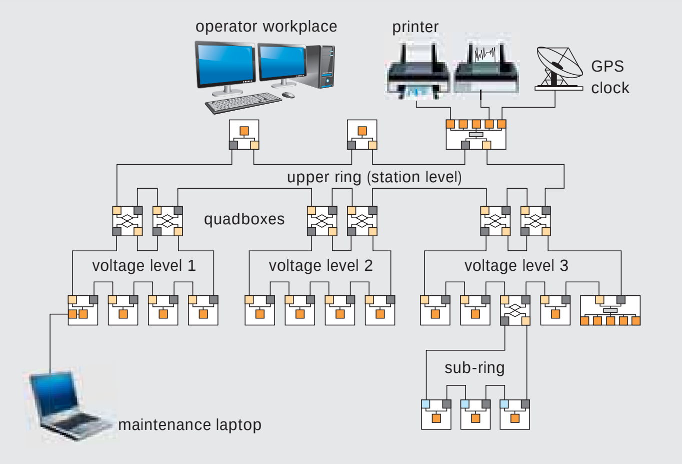
With respect to a single ring, the bus traffic is roughly doubled, but the average propagation time is reduced, allowing the ring to support a similar number of devices. Individually attached nodes, such as laptops and printers are attached through a "redundancy box" that acts as a ring element.

A pair of redundancy boxes can be used to attach a seamless ring to a duplicated PRP network. In this case, each red box sends the frames in one direction only. This overcomes the basic limitation of a ring, and enables the construction of a hierarchical or peer network → 8.

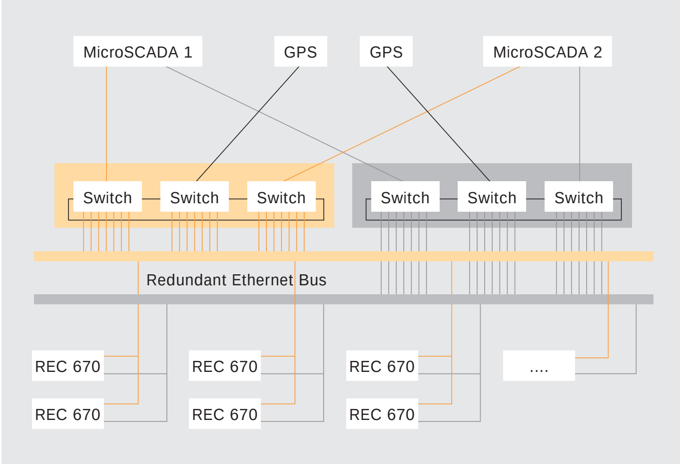
Precision clock synchronization

The PRP/HSR scheme presents a challenge for time synchronization as defined in IEEE 1588 because the delays over the two redundant networks are different. Here, some restriction to IEEE 1588 actually enabled the robustness and precision of the clock system to be increased.

8 HSR ring of rings



9 A system overview using PRP



10 PRP and HSR features

PRP and HSR provide ideal redundancy schemes for IEC 61850-based substations in that they:

- Fulfill all requirements of substation automation according to IEC 61850
- Can be used in a variety of topolgies, eg, rings, trees.
- Are transparent to the application
- Tolerate any single network component failure
- Achieve zero recovery time, making it suitable for the most time-critical processes
- Do not rely on higher layer protocols
- Are compatible with RSTP
- PRP allows nodes not equipped for redundancy to operate on the same network
- Use off-the shelf network components (tools, controllers, switches and links)
- Support precision time synchronization according to IEEE 1588
- Have been proven in the field in high-voltage substations

Field experience

The first substation automation (SA) system for a high-voltage substation with control devices operating under PRP is now ready for installation. The tests have proven that the technology is mature for substation automation devices and it performs as expected. One of the major requirements for this project was to have fully redundant communication down to the bay level IEDs to remove any single point of failure in the substation control. This called for full duplication, with redundant station computers (MicroSCADA 1 and MicroSCADA 2 in hot stand-by configuration for control and monitoring at the substation level as well as redundant gateway functionality for telecontrol. For bay level control, ABB's latest control device for high-voltage applications, the REC670, is used → 9.

The bay control units (REC670) are connected by two completely separated network rings. The entire system is synchronized using SNTP sent in parallel to both networks using two independent GPS receivers with integrated SNTP time servers. The communication system is supervised using SNMP and the failure of the redundant connection of any device is immediately reported to the system.

Ideal redundancy schemes

PRP and HSR make an important contribution in achieving interoperability – with respect to redundant communication – between protection, measurement and control devices from different manufacturers → 10. Their success relies on the ability of ABB to team up with competitors and suppliers to ensure device interoperability in the customer's interest.

Hubert Kirrmann
ABB Switzerland
Corporate Research
Baden, Switzerland
hubert.kirrmann@ch.abb.com

References

[1] Internet RFC 2030 simple network time protocol (SNTP) Version 4 (1996) from IPv4, IPv6 and OSI.
[2] The Institute of Electrical and Electronic Engineers. IEEE Std 1588: Standard for a precision clock synchronization protocol for networked measurement and control systems.
[3] International Electrotechnical Commission, Geneva IEC 62439 (2010). Highly available automation network suites.
[4] The Institute of Electrical and Electronic Engineers, (2005). CSMA/CD access method and physical layer specifications. IEEE Std 802.3.
[5] International Electrotechnical Commission, Geneva. IEC 61850-8: Communication networks and systems in substations. Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.
[6] International Electrotechnical Commission, Geneva. IEC 61850-9-2: Communication networks and systems in substations. Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3.
[7] International Electrotechnical Commission, Geneva (2006). IEC 61784-2, Additional profiles for ISO/IEC 8802.3 based communication networks in real-time applications.
[8] The Institute of Electrical and Electronic Engineers, (2004). ANSI/IEEE Std 801.2D, Media access control (MAC) Bridges.

Futher reading

- International Electrotechnical Commission, Geneva TC57 WG10 IEC 6185090-4. Network engineering guidelines (in preparation).
- Dzung, D., and Kirrmann, H. (2006). Selecting a standard redundancy method for highly available industrial networks. WFSC 2006 Torino.
- Meier, S. (2007, January 25). ZHW InES – PRP: Doppelt gemoppelt hält besser. Electrosuisse, ITG Fachtagung, Zurich-Kloten.