CIGRE SESSION 48

B5-214

Paris 2020

Optimising LAN Architecture For Improved Reliability And Resilience

R HUGHES[1]
Rod Hughes Consulting Pty Ltd
Australia

SUMMARY

Protection Systems are designed under the ethos of "not if, but when". This applies to the inevitability of a power system fault that must be cleared; through to the failure of some part of the protection system itself must not prevent that clearance. This effectively drives reliability considerations that the protection system and circuit breaker must trip when grid faults occur.

In that respect, the Australian National Electricity Rules (NER)[2] section S5.1.9 (c) states that not only the Network Service Provider "*must provide sufficient primary protection systems and back-up protection systems*", but also that (d) "*the primary protection system must have sufficient redundancy*" i.e. there is redundancy within the primary protection plus back up protection. This must remain true even "*with a single protection element (including any communications facility upon which the protection system depends) out of service*".

Apart from ensuring the circuit breaker will trip when required despite an element of the protection system has failed/out-of-service, the protection system must also not operate when it shouldn't, i.e. it must also be "stable" and not cause inadvertent outages. Wire-based systems have proven to be inherently reliable, but device failure, mechanical failure of the primary plant (CB status contacts), design errors, vermin attacks or so-called "finger-errors" during maintenance can raise questions about stability that we tend to "just live with"!

SCADA inherently relies on communication systems between the control centre and the substation. In the late 1980's, SCADA communication extended to the protection relays themselves as the relays began to provide RS232 or RS485 ports, and now ports for connection to a Local Area Network (LAN). In 2004, under the Standard for Power System Data Communications (SPSDC)[3], the Australian Energy Market Operator stipulated that SCADA must

[1] Email: rgh@rodhughesconsulting.com
[2] Australian Energy Market Commission web site: https://tinyurl.com/yjcs57x6
[3] Australian Energy Market Operator web site: https://tinyurl.com/wb2hndc

also provide "*sufficient redundancy*" from the point of interface between the "real world" to the "digital world". SPSDC effectively requires redundant sources of analogue measurements, redundant sources of CB status signals, and redundant controllable open/close outputs to the circuit breakers.

Also in 2004, IEC 61850 expanded our thinking "in the blink of an eye". It wasn't only the SCADA system that relied on communication paths, but critical "sub cycle" timing protection operation signals now also depend on the LAN. CB Status, protection operation, CB Fail initiation, Autoreclose triggers, CB trips, CB open/close commands, CT/VT values, CB Fail all now would appear on a LAN based infrastructure, possibly even via LAN connections in the yard to "intelligent switchgear" and "intelligent primary plant".

Under a LAN based environment, loss of messages containing critical real time information that the protection needs can result in protection functions not having the right information for correct operation, i.e. the potential for failure to operate when needed, as well as operating when it shouldn't. Automation functions, SCADA, condition monitoring, metering and any other digitally enabled functions can be at least impaired if not blocked by a LAN failure.

It is not surprising then that in implementing a LAN-based protection environment we should demand at least the same, or preferably improved, degree of reliability (operate when required) and stability (not operate when not required) as we have "enjoyed" with wire-based systems.

For many years, the typical generic LAN architecture with some degree of resilience to LAN failure was Rapid Spanning Tree Protocol (RSTP). However even "small" RSTP networks could take more than 100 milliseconds to "heal" and re-establish communications between devices. Even just 100 milliseconds is "several lifetimes" as far as protection operation and fault clearance is concerned. So whilst the system is somewhat resilient, major power system outages could result as a consequence of messages "disappearing".

IEC 62439-3 introduced Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) as so-called "bumpless" LAN protocols and architectures – basically the communication between the devices is ALWAYS working even with one segment out of service. This is effectively "continuous instantaneous resiliency" for a single failure of the LAN.

This paper explores the opportunity of LAN-based technologies to not only meet redundancy and reliability considerations, but also improve stability with even higher resiliency systems.

KEYWORDS

Reliability, Redundancy, Resilience, Stability, LAN, Architecture, RSTP, HSR, PRP, IEC 61850.

1. Reliability: MTBF vs Availability

Naturally in any system we prefer to use devices that have less likelihood of failure. Typically such likelihood is described in the vendors Mean Time Between Failure (MTBF) statistics. This can be a useful indicator, but as with all indicators they should be understood as to what they represent.

MTBF is a MEAN, an average. Obvious, but that implies there are extremes in the actual values that have been established in order to calculate the Mean value. Some failures may have been near instantaneous, whilst others could be many times the Mean value. Equally the Mean implies at least some failures have occurred so we can never assume failures won't happen.

The second aspect is about the number of samples the mean is based upon, which is based on how those samples have been collected, and over what period of time. Some vendors use statistical methods based on the theoretical MTBF of the components used in their products – which has other cascading statistical issues. Other vendors may use statistics of number of devices returned to the factory for repair – one electromechanical device vendor some years ago calculated that their MTBF for the particular device was in excess of 300 years, however that did not take into account all the field repairs carried out by the users or repairs carried out by the national distributors avoiding the delays in return to the factory.

Consequently, simply comparing two vendors MTBF alone is not a definitive indicator of better or worse overall reliability. It is part of the assessment, but not the entire assessment.

An extension of MTBF statistics is the broader concept of Availability. This is arguably the more important issue than just MTBF alone in regards to correct operation of real-time automation systems. Availability is a derivative from simple MTBF that incorporates the Mean Time To Restore (MTTR), including all site works, re-commissioning and return into service.

$$\text{Availability \%} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})} \times 100$$

MTTR depends on several influencing factors, most of which are not vendor or device dependant, but are more based on the system integrator's implementation and the response time of operations staff with such factors comprising:

- IED self-alarming and external monitoring requires the system integrator to provide a means for communicating the alarm to the operations staff etc.
- The response time for appropriate operations technicians to get to site (may be several hours in remote locations) etc.
- The ability and time to repair or replace faulty equipment/systems e.g. spares holding, ability to replace without disrupting other systems etc.
- The ability to re-commission test the system and return to service with subsequent records update etc.
- Cyber secure remote access, remote testing and remote reconfiguration capabilities to reassign functional assignment to hot-standby devices[4].

Clearly, if a real-time critical function has a long MTTR the overall Availability may be significantly impaired, regardless of good MTBF.

[4] "5-minute" System Restoration Using Remote Access and IEC 61850 : R. Hughes CIGRE SC B3 Contribution 2012, https://ideology.atlassian.net/wiki/x/HYBq reference RH19P, RH19D

In reverse, if the objective is to achieve 99.999% (so-called "five nines") Availability with the general target of power system protection to achieve <8 hours MTTR[5], this would require the overall system to have an MTBF of 91.3 years!

One of the ways to increase overall Availability of the protection system to clear power system faults is of course the well know duplicated protection systems known as "X and Y" or "Main 1 and Main 2". This can be referred to as an "any one out of two" duplication, and may be considered as an "OR" logic function.
Availability of such duplicated, i.e. parallel systems is calculated as follows:

e.g. System 1 has Availability $A_{S1} = 98.0\%$
System 2 has Availability $A_{S2} = 97.0\%$
Overall Availability = $1- \{(1- A_{S1}) \times (1- A_{S2})\} = 99.94\%$
i.e. parallel "OR" systems have a higher Availability than either of the individual systems increases the chances of a power system fault being cleared in the event of a coincident secondary system failure.

On the other hand, the inherent nature of an "OR" based duplication for reliability is that due to potential failure in either system causing an unwanted operation, there is an increase in the overall likelihood of a certain type of failure in either system could cause an unwanted/unnecessary blackout.

2. Redundancy and Resilience

Traditional "redundancy" has been implemented as two independent duplicated wire-based systems. Fundamentally, independent duplication anticipated either system may not operate at all due to protection devices non-detecting the fault, loss of power supply, a CT left short circuited, a VT fuse blown, a trip link left open, or a failure of a single part of the "communication system upon which the protection depends".

However with one system in this failed state, that system may be impaired to some degree, but a physical failure itself or the consequence of the failure may equally lead to a mal-operation of functions causing an unwanted CB trip, i.e. the system may not necessarily be stable because it is not operating as normal.

Duplicated wire-based systems were not inherently/automatically resilient in that the failed system needed human intervention to fix the failure and return it to normal operation, which may take some time as discussed as the MTTR in the previous section.

However the NER doesn't actually say "duplication" as the requirement. The NER actually says the primary protection system "*must have sufficient redundancy*" ! Communications paths can be implemented with redundancy, but in a manner also providing resilience that to all specific purposes, the system remains operating "normally" even with one path out of service. If the system is operating normally, then stability has not been compromised. As digital systems tend to have far more functions, complexity and dependence on the LAN, automatic Resilience (self-healing) is an equal objective and priority as Redundancy.

[5] Australian market rules allows a transmission line to be operating without duplicate protection in service, i.e. with only one protection system operating for up to 8 hours.

3. Failure Mode and Effects Analysis - FMEA

CIGRE Technical Brochure (TB) 687 (2017)[6] references IEC 60300-2 (2004-04)[7]. The Working Group survey identified that 39% of respondents admitted their Reliability, Availability, Maintainability and Performance (RAMP) requirements were not defined!

This TB goes on to discuss in Chapter 11 the range of views about IEC 61850 and its impact on RAMP. This seems to suggest that many utilities are yet to embrace the opportunity of IEC 61850 based systems to dramatically improve RAMP by carefully and comprehensively considered function implementation and network optimisation.

FMEA is a forward looking analysis of what might go wrong and the impact on the rest of the system. Of course just understanding the impact then obligates a further stage of mitigation of those failure modes that have unacceptable impact on the rest of the system. In essence, the results of FMEA mitigation have been in existence for decades with the principle of duplication.

Ironically, traditional duplicated "conventional" wire-based systems have almost obviated the engineering process step of specific and comprehensive FMEA. This is itself a risk that engineers may not have the skills for conducting FMEA and mitigation engineering. This risk is compounded by new technologies which have a whole new realm of failure modes, and even further compounded by even more advanced functions relying on many more sources of information communicated via the LAN.

Hence in any digital system, there is an obligation to consider the failure modes, but more importantly the optimisation of the system in terms of providing even more reliability and more resilience to reduce the possibility and duration that the systems are not operating normally.

The critical engineering step is that FMEA mitigation has to consider what redundancy "looks like" for LAN-based systems in two aspects:

- Reliability: operate when required (clear real grid faults)
- Stability: not operate when not required (no inadvertent blackouts)

4. LAN Protocols

4.1 Spanning Tree Protocols (STP)

STP has been used for "decades" as a means of providing inherent resiliency of the LAN network. This protocol is implemented in each of the LAN switches on the ports connecting switch-to-switch in order to form a ring. The IEDs themselves are single port IEDs referred to as a Single Attached Node (SAN). The network switches communicate with each other to disable/enable sections of the ring to prevent continuous message circulation or re-converge to heal a broken ring. Re-convergence in the popular Rapid Spanning Tree Protocol (RSTP) may take say ~five milliseconds per switch. Hence in a ring of 20 switches, it may take ~100 milliseconds for communication to be restored to all IEDs.

IEC 61850-8-1 MMS (e.g. SCADA, condition monitoring, metering ….) allows messages to be configured to use Buffered Reports so that any important messages will be re-sent after re-convergence.

Lost IEC 61850-8-1 GOOSE messages during the re-convergence may be a problem to power system operation if the re-convergence coincides with a critical protection operation. The provision of duplicate X and Y systems should mean that the unaffected system would still

[6] Experience concerning availability and reliability of digital substation automation systems (DSAS)"

[7] Guidance for dependability management

operate in required time but we must also consider the real possibility that only the one system with the failed LAN has detected the primary system fault.

The loss of IEC 61850-8-1 GOOSE to a particular IED for even as little as 100 milliseconds could have serious consequences such as :

- Delay in CB trip beyond critical clearance times
- Delay in CB Fail initiation

both leading to potential system instability, more significant fault damage and outage duration. It may even be that complete sequence(s) of <<protection operation causing CB opening resulting in protection reset>> may be missed. Missing the occurrence of these sequences could lead to failure to initiate Autoreclose and disturbance recordings leaving the Sequence Of Events and operator only seeing the CB has opened for no apparent reason.

Of course one or more of the IEC 61850-9-2 / IEC 61869-9 CT/VT Sampled Value streams could also be lost and hence the protection function itself not be able to operate correctly in the first place. This must be taken into account by the vendor as well as the systems integrator to ensure that the protection will not mal-operate during this time and specific validation testing may need to be carried out by the systems integrator.

Whilst STP solutions are well proven, there are therefore significant FMEA considerations (reliability and stability) for optimisation of STP rings in a more digitally based substation automation system in regards to:

- Duration of re-convergence,
- Types of messages, and
- Impact on system performance of missing/delayed messages.

It would be fair to say that the protection based requirements, even with duplicate X and Y systems, are tending to indicate STP systems are not an ideal solution due to their “bumpy” impact on system operations due to the re-convergence times.

4.2 High-availability Seamless Redundancy (HSR) Protocol

This protocol is defined in IEC 62439-3 and is commonly referred to as a “bumpless LAN”, i.e. a failure of the LAN is barely noticeable, if at all. HSR is further described in IEC 61850-90-4. Unlike STP switch-based protocols, HSR is implemented by the IED vendor in the IED itself and is therefore a new procurement criteria for the IEDs. The HSR IEDs are therefore two port device Dual Attached Nodes (DAN) with messages being sent simultaneously in both directions around the ring IED-to-IED.

In essence a failure of the LAN network has extremely minor impact on functional performance due to the IEDs receiving the same message from two diverse paths and operating on the basis of the first of the duplicate messages received. The fast repetition cycle of GOOSE following an event is arguably moot in bumpless networks and so the fast repetition rate can be optimised to reduce bandwidth requirements if considered necessary.

As with any ring topology, the effective bandwidth of the HSR ring is limited to the lowest bandwidth IED in the ring. Some of the devices (IEDs/RedBox/QuadBox) may also limit the total number of devices in the ring due to their limited processing power for the potential number of messages they have to manage in their internal memory – each IED has to remember the messages it initiated in each direction to identify when each message has returned via the other port so as not to forward it again. Some devices are known to have a limit as low as 25 devices in the ring. Rings may be joined by duplicate interconnections using two back-to-back 3-port so called “redundancy boxes” (RedBox) or 4-port QuadBox as described in the above referenced Standards.

Note that both Multicast Filtering and Virtual LAN (VLAN) mechanisms for managing the flow of messages within the LAN in the ring are not applicable for HSR – all of the IEDs have to receive and forward all messages, i.e. they must all support the maximum bandwidth requirement. However multiple interconnected rings may be configured with Multicast Filtering and/or VLANs to control which messages are transferred from ring-to-ring to optimise bandwidth requirements of the IEDs in each ring.

Maintenance and testing of a LAN-based system inherently requires new tools and processes. Isolation mechanisms for bumpless LANs are more complex as you cannot simply disconnect a fibre to isolate a device as this would now mean the rest of the system (perhaps all of both X and Y systems if on the same ring) would then be operating with a single common mode of potential failure.

In normal operation, consider a section of the ring where there is a sequence of IEDs as X-1, Y-1, X-2, Y-2, X-3, Y-3 as shown in Figure 1-a, each supplied by respective PS-X and PS-Y auxiliary power supplies. Failure of any one section of the ring or any one IED is covered by the HSR mechanism so that all IEDs and messages remain in normal operation.

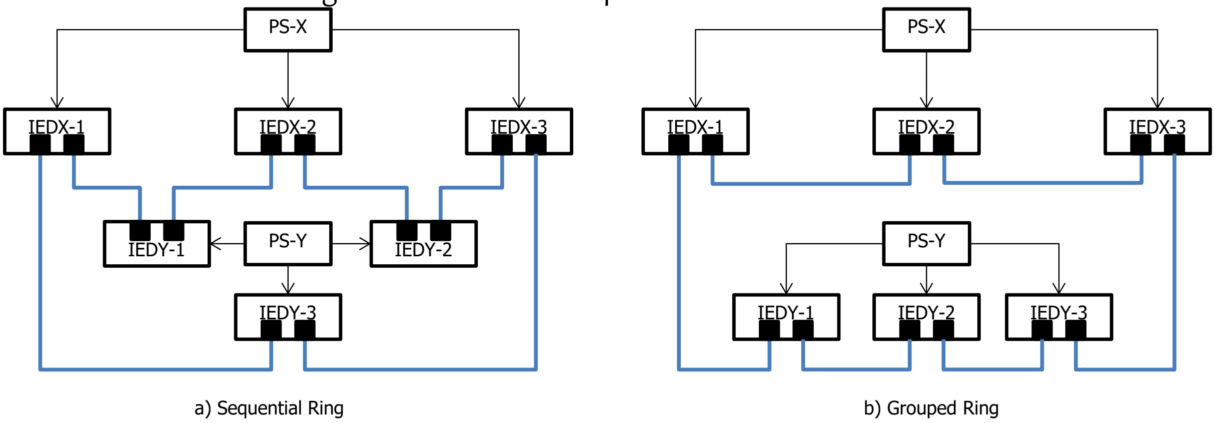

Figure 1 Alternative HSR arrangements

However considering the failure of the Y auxiliary power supply in Figure 1-a, then as well as the Y IEDs being inoperative, the X devices are now effectively fully isolated by the inoperative Y IEDs on either side and hence the X system is also inoperative. The Reliability supposedly created by Redundancy has been destroyed.

The solution to this is to either group all X IEDs in series around the ring and then all the Y IEDs around the other half of the ring as shown in Figure 1-b, or provision all IEDs as dual power supply devices connected to both the X and Y auxiliary supplies.

4.3 Parallel Redundancy Protocol (PRP)

PRP is another “bumpless LAN” protocol defined in IEC 62439-3 and described in IEC 61850-90-4. As with HSR, PRP is implemented by the vendor in the IED itself and as such is a procurement criteria.

Distinct from HSR, the two IED ports are connected to the switches in two independent LANs. In a similar manner as HSR, the IEDs are normally receiving the same message via both ports, operating on the basis of the first of the duplicate messages. As with HSR, the fast repetition cycle of GOOSE following an event is arguably moot in bumpless networks and so the repetition rate can be optimised to reduce bandwidth requirements if considered necessary.

PRP does allow an independent choice of the LAN configuration on either "side" – e.g. the IED connection to LAN A could be a standard single port connected to an RSTP switch ring, whilst the other side LAN B could be a dual port connection to a direct IED-to-IED HSR ring to achieve completely independent LAN principles avoiding common modes of failures. These choices can quickly become somewhat counterproductive in cost and complexity which the vendors may not universally support – ultimately the first choice must be for correct protection functionality, not a compromise just to satisfy an "exotic" LAN requirement. Optimisation of the LANs for each side requires both pragmatic objectives and practical solutions considered and specified prior to procurement and as part of tender evaluation.

Switches are inherently required for most LAN choices in PRP. This allows Multicast Filtering and/or VLANs to be used to control bandwidth around each of the LANs and to the individual IEDs.

5. Multicast Filtering and/or VLANs

Possibly one of the great debates: which to use! Both achieve similar results of controlling the bandwidth required on any port.

In general total GOOSE bandwidth is relatively small. Even with one millisecond initial repetition, the 40th repeat message would not be published till after 30 seconds have elapsed[8].

However bandwidth requirements on the backbone and on individual links to IEDs may be important where there are many IEC 61850-9-2 / IEC 61869-9 CT/VT Sampled Value streams – each stream representing ~8 Mb/s. As a multicast message, all devices would normally receive all the SV messages and therefore for some IEDs unnecessarily using up considerable IED port bandwidth, and hence delaying reception of critical GOOSE messages.

Some would base the choice on the fact that Multicast Filtering is purely a switch configuration without any impact on the IED configuration. It specifically restricts where multicast type messages (time synchronisation, SV and GOOSE) are distributed. As an example it would be somewhat pointless to send a GOOSE containing CB position and protection operations to a purely SV publishing Merging Unit, or a CB interface does not need to receive any SV streams. Simply configuring the switch ports for the IEDs to allow or restrict the types of multicast messages is an effective overall solution. Multicast Filtering can also be applied switch-to-switch in order to control the flow of traffic in certain parts of the backbone of the LAN. Even so, messages remain inherently serial (sequential one message after the other) so unnecessary traffic simply increases overall latency of critical messages. To some extent, this can be optimised using Message Priority settings to improve critical message latency.

Others would argue that VLANs provide more "control" over the messages themselves. VLAN's can apply to all types of messages including MMS (SCADA, condition monitoring, metering…), not just multicast messages. In any case, MMS inherently restricts messages flow via the most direct path source-to-destination as it is an Ethernet Layer 3 protocol[9].

[8] https://ideology.atlassian.net/wiki/x/bgFv <<Are 40 messages considered a "flood"?>>

[9] Layer 3 uses the IP address to identify where the destination IED exists in the LAN to restrict the message to flow only via the ports as a direct path to the destination. Other IEDs not involved are therefore "blind" to that message and reducing their bandwidth loading.

VLANs are used in conjunction with configuring the switch port as an Edge Port (only specific VLAN) or TRUNK Ports (multiple VLAN). The switch ports can recognise allowed incoming VLAN-ed messages. The outgoing ports may strip the VLAN ID and/or add it to the outgoing messages depending on how the switch port is configured for Forwarding as Tagged or Untagged. This can be somewhat confusing to technicians with the same message possibly appearing without a VLAN ID in some segments and appearing elsewhere with the VLAN ID. Indeed IEDs may reject messages received with wrong or missing VLAN ID[10]. VLAN-based systems have been known to grow to over 200 different VLANs and therefore need appropriate policies are required for both the IEDs and the LAN switches and must be respected in all phases of the life-cycle of the system.

6. High Resilience RSTP over PRP

As mentioned earlier, the opportunity presented by digital technologies is to improve the overall reliability and resilience over that which we have "enjoyed" with older technologies.
As we have seen here, RSTP offers a simple healing mechanism for a LAN, whilst PRP offers bumpless operation of the systems. Combining both of these solutions as RSTP being used for each side of the PRP LANs provides a highly resilient architecture where effectively the only system failure is a failure of the IED itself.

This solution is even more resilient than wire-based systems where the wires themselves are a significant risk factor for loss or reduction of functionality due to loose connections, broken wires and operator errors.

Figure 2 uses green to indicate X system related components and blue for the Y system components. Each side of the PRP (shown top and bottom) is configured as a dual Multiple Spanning Tree Protocol () ring (four RSTP rings in total). Each RSTP ring is managed by VLANs to carry either X or Y traffic plus some common traffic.

Certain design and procurement policies support this optimised architecture:

- Switches have hot swappable dual power supplies.
- IEDs preferably having hot swappable dual power supplies
- Switch modules are hot swappable
- Switch modules do not have both X and Y connections to allow module replacement without disruption to the other system
- VLANs segregate general X and Y traffic over segregated fibre backbone
- Specific VLANs carry "common" traffic such as:
    - Cross-connected/common X:Y messages (CB Fail, Autoreclose, Disturbance Recording)
    - HMI/SCADA commands/reports
    - Clock synchronisation
    - "Isolation" configuration commands
    - Test messages

[10] E.g. one particular utility suffered much frustration over several weeks debugging communication between one IED using decimal "20" VLAN setting, the other using the same "20" but as Hexadecimal (32 decimal)

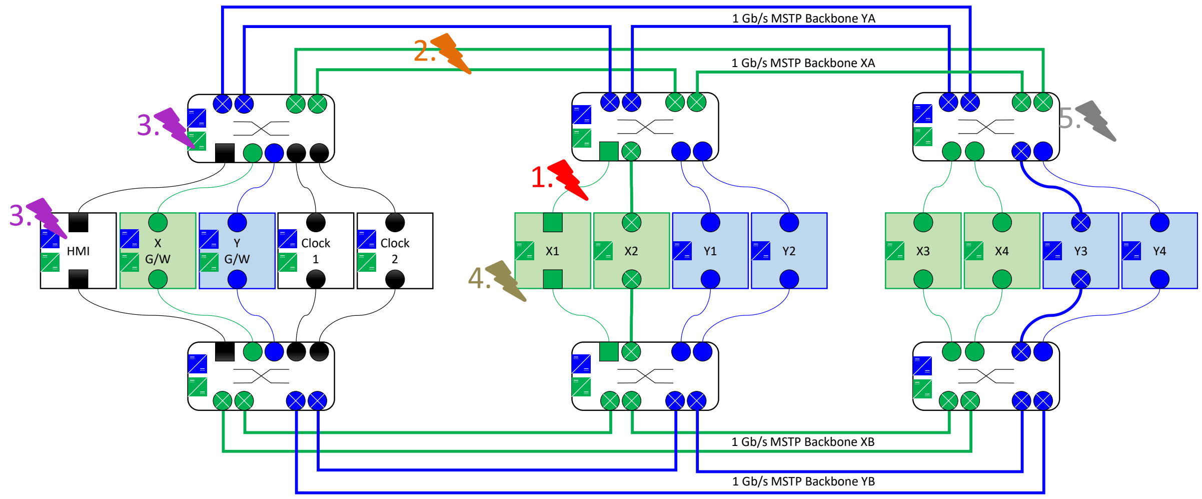

Figure 2 Highly Resilient RSTP over PRP LAN

FMEA of the five failure modes indicated in Figure 2as:

1. Failure of IED link to switch: covered by bumpless alternative PRP LAN connection
2. Failure of backbone link: covered by self-healing RSTP recovery (perhaps >100 ms re convergence) with duration of re convergence covered by bumpless alternative PRP link
3. Failure of one power supply: covered by dual power supplies
4. Failure of IEDs with single power supply: covered by duplicate X/Y IEDs
5. Failure of single complete switch: covered by alternative PRP LAN

This optimised RSTP-over-PRP architecture shows that even with both X and Y protections sharing the same LAN PRP infrastructure, apart from the IED itself failing, there is an N-2 redundancy of the LAN infrastructure. It would take a second failure for the X or Y system to be impaired. A single failure anywhere in the LAN still retains full X and Y operation, and is therefore far higher reliability and stability than we have ever "enjoyed" with wire based systems.

Some may have concerns that both X and Y messages are handled by common hardware. However the FMEA clearly shows there is "more than sufficient redundancy" to satisfy the requirements of the NER and maintain full operation even with "one element of the communication system out of service".

However if still a concern, a slightly less optimised architecture involves additional switches top and bottom which would allow total segregation of X and Y traffic on each side. The same total number of IED and switch ports are required, the same number of switch power supply modules are required, but potentially more panel space may be required to mount the additional switches.

Hence this combined RSTP/PRP arrangement maximizes the independent IED operation whilst ensuring bumpless communication even during Spanning Tree re-convergence.

7. Non-critical systems with Single Attached Nodes

In the overall Substation Automation System, there will be a significant variety of devices that do not specifically need the super-reliability/resilience in the redundancy of the protection SCADA systems. Condition Monitoring for example generally does not require redundancy provisions, nor does general on/off controls such as for yard lighting. The substation LAN architecture must be flexible enough to cater for both redundant and non-redundant requirements.

Equally there are certain devices in the network such as the local HMI and test equipment which are usually inherently SAN type devices. These devices usually involve some complexity. The HMI, as with SCADA, invariably needs to be connected to both the X and Y systems in some form to access status, values and events. Test equipment may be used with both or selectively X or Y, but also has to manage "isolation" and message paths in PRP/HSR networks.

In the case of HSR, all devices in the ring must support HSR directly meeting the same minimum bandwidth requirements. SAN IEDs that do not support HSR directly have to be connected via at least a 3-port RedBox, or via a standard multiport switch connected to a RedBox, or a RedBox with integrated multiple SAN ports.

RSTP and PRP however can support connection of SAN IEDs directly to their network. In the case of PRP, it is just a decision of which of the two PRP LAN's is to be used. However the availability of PRP LANs begs the question of why ignore the relatively low-incremental-cost opportunity to use a RedBox to reduce the likelihood of impaired or total loss of such non-redundant functionality due to a LAN failure.

8. Conclusion

The adoption of the so-called "Digital Substation" philosophy is by no means a unique prescription of the extent to which it will be implemented or how that is going to be implemented. The mid and longer term interests of the asset of having a "future-enabling" infrastructure" must not be taken lightly. There is an "inevitability" of adopting new technologies, and more importantly needing support for increased functionality.

Optimising does not imply a unique "one size fits all" solution. It does however require an assessment of what is needed and an equal assessment of the various options available. However there is an obligation to consider both aspects in terms of the life of the asset in order that future requirements are not "hog-tied" by myopic considerations of the past that did not create an "enabling" environment for future, perhaps as yet undefined, requirements.

Both HSR and PRP both provide effectively automatic redundancy and resilience of the communication path. This leads to the questions for ongoing debate for possibly many years such as: Is it acceptable to connect the X and Y protections to the same network? What are the implications for LAN fault detection (the system is never "not working"), maintenance "isolation" and testing? Has total independence from any common failure mode (network storming, incorrect IED/switch configuration ...) been achieved, or what additional measures need to be applied to achieve that?

However, it is clear that LAN-enabled protection systems must be carefully and comprehensively considered to optimise not just normal redundancy-based reliability for power system fault conditions, but also higher availability through higher resiliency systems to maintain stable operation at all times.

BIBLIOGRAPHY

As new applications for the Substation Automation System are created, there will be continued evolution of network requirements. The following references are to work that is not yet completed, but would be worthwhile following or obtaining when completed.

CIGRE Working Groups https://www.cigre.org/article/GB/cigre-active-working-groups

[1] CIGRE WG B5.56 Optimization of Protection Automation and Control Systems (WG formed 2015)

[2] CIGRE WG B5.60 Protection, Automation and Control Architectures with Functionality Independent of Hardware (WG formed 2017)

[3] CIGRE WG B5.63 Protection, Automation and Control System Asset Management (WG formed 2017)

[4] CIGRE WG B5.66 Cyber Security requirements for PACS and the Resilience of PAC Architectures (WG formed 2017)

IEC TC 57 WG10

[5] IEC 61850 90 20 Guideline for redundant IEDs with IEC 61850