Making Complex Protection and Control Systems Easy to Maintain

Rich Hunt
GE Grid Solutions
Apex, NC USA
richard.hunt@ge.com

***Abstract*—Process bus, the concept of distributed I/O for protection and control, has long been promoted as more cost-effective than traditional systems. I/O devices can potentially be manufactured as part of primary equipment, effectively eliminating the need for custom copper wiring design, installation, and terminations. A large part of the business case is that the cost of the additional devices (I/O devices and communications devices) will be more than offset by time and labor savings. However, this is only the capital cost of process bus. There is also an operating and maintenance cost to consider: will the increased number of devices that make up a process bus protection and control system lead to increased costs due to device reliability.**

Simple reliability analysis shows that process bus has the same level of availability as conventional protection systems. However, the overall reliability, in terms of mean time between failures (MTBF) will be greatly reduced, due to the large number of devices that comprise the system.

Based on this simple reliability analysis, a key requirement for process bus must be to limit process down time. The best way to do this is to use simple to replace devices and components. The goal is exactly that of the commercial aviation industry, where uptime and availability is critical: modular components, with simple physical interfaces, and limited configuration requirements drive process down time towards 0 through simple swap out of failed components. Process bus systems, properly designed, permit this reduced process downtime, offsetting the smaller MTBF of the system through simple component replacements.

I. Introduction

Process bus is simply distributed I/O for protection and control systems. I/O devices, the interface between analog measurements and digital communications, are located at primary equipment in the switchyard. These I/O devices publish data via an Ethernet communications network to protective relays. I/O devices are devices such as merging units that sample analog measurements; remote I/O modules that use contact I/O for status and control of primary equipment; and process interface units (PIUs) that both sample analog measurements and include contact I/O. Protective relays no longer require field wiring to acquire measurements: they simply connect to the communications network to subscribe to the appropriate data.

There has been much discussion in the utility industry about process bus since the publication of the IEC 61850 Standard. The concepts in the 61850 Standard describe a practical method to transmit the required data between I/O devices in protective relays. The majority of the discussion has been around the business case for process bus. This business case is essentially that process bus greatly reduces the amount of labor required for installing protection systems by greatly reducing the effort in managing copper wiring. Process bus obviously requires more IEDs than conventional relaying because of the addition of I/O and communication devices. Therefore, the logic is the cost savings due of reduced labor requirements offsets the increased capital cost of process bus devices.[1][1] This is the upfront capital cost of process bus. In practice, project costs for conventional relay installation and process bus installations are liable to be similar. Process bus has the advantage of requiring less skilled resources, and is a strong reason for adoption.

The rest of the discussion around process bus has been on more technical aspects. This includes practical considerations for installing process bus,[2] considerations for testing process bus protection systems[3], and testing advantages to process bus protection systems.[4] One topic that has only been lightly discussed is that of reliability. The focus has been to show that process bus systems will be as available as conventional protection and control systems.[5]

However, there are two other aspects concerning process bus that require discussion. These are the long term system reliability, and the long term costs to maintain or replace a process bus system and devices. It is apparent that these two aspects are interrelated: a system with more devices or components will have more failures, which will impact long term costs. However, the solution to the long term cost of device failure is also a positive part of the business case.

To clearly describe the reliability concerns, with more devices comprising the protection and control system, there will be more device failures, which will impact both system reliability, and system operations. While a process bus based system will be as available as a conventional system, it cannot

be as reliable over time. It is important to understand the reliability of process bus systems over time to help define the true cost benefits of process bus. A reliability discussion will quickly focus on the time, cost, and risk to replacing failed devices. This focus will drive thinking on operations requirements, product design, and the cost of repairing failed devices. So an important discussion is once again the cost-benefit discussion. Does the speed of installation, and the resulting cost savings due to the speed of installation, more than offset the cost of reduced reliability? Devices that are difficult and costly to replace will completely offset any savings accrued during the installation phase.

The process bus system design drives the business case. With relays, merging units, and other I/O devices that are simple to replace, the long term costs are better than with traditional protection and control systems. Once a process bus system is installed, maintaining this system should be simple. Component failures are alarmed and replaced through like-for-like swaps, without requiring system reconfiguration or recommissioning. The cost of a replacement therefore becomes essentially the cost of the material or device required for replacement. This is the true business case for process bus: reducing process downtime, costs, and effort while replacing or upgrading protection and control systems.

II. Process Bus Architectures for Reliability Analysis

The first step to understanding how the reliability of process bus impacts operating costs is to perform some basic reliability analysis on typical protection and control systems. Every system is different, so it is useful to start with a simple case study to gain basic understanding. The simplest case is to look at is a single zone of protection in a substation.

The basic zone of protection in a transmission substation is a breaker-and-a-half line terminal using distance protection. This is a good test case for reliability analysis. Distance protection adds a little complexity to the analysis (through the number of signals required) that will help fully illustrate the concepts. The conventional protection system, which is the control case, is that of Fig. 1. Two microprocessor-based relays, hard wired to primary equipment, operating in parallel for reliability. The protective relays need to control both circuit breakers, measure currents from both circuit breakers, and measure the line voltage. Process bus changes the system by adding I/O devices. These I/O devices must provide control points for the circuit breakers, measure the currents from the breakers, and measure the line voltage. There are many permutations of process bus I/O devices. This analysis will use process interface units (PIUs) to keep the number of devices to a minimum. Every measurement point will use redundant PIUs, as in Fig. 2.

Because process bus relies on communications, there are many variations in architecture possible. This analysis examines 5 different process bus architectures. All the architectures use redundancy to provide availability of the system. The architectures use both simple point-to-point and networked architectures, both as independent redundant systems and as fully interconnected and interoperable systems.

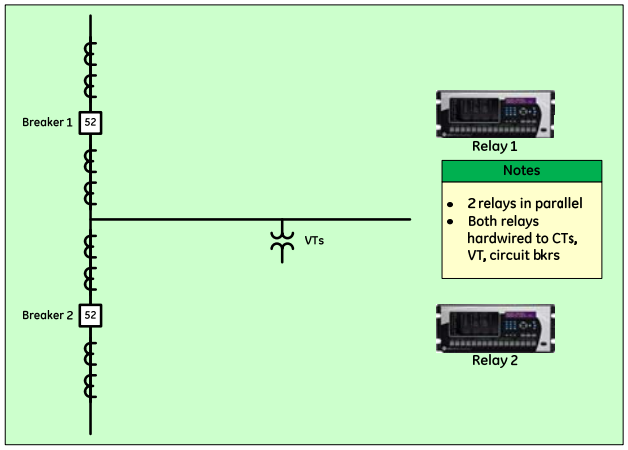

Fig. 1. Conventional relay system

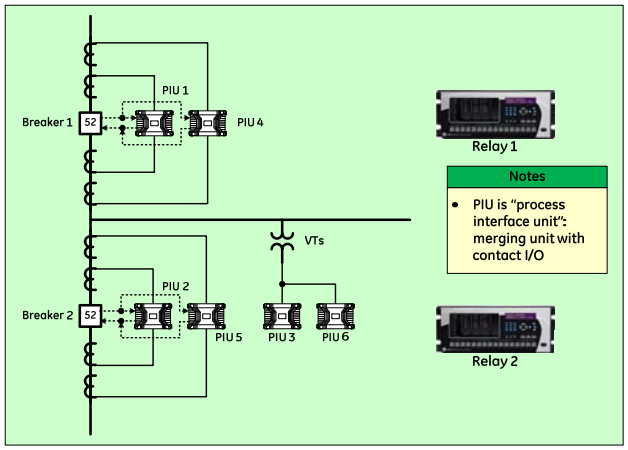

Fig. 2. Process bus devices

For definition purposes, "point-to-point" means a direct communications connection between the relays and PIUs. "Network" means the relay and the PIUs are connected to a switched Ethernet network and all data travels over this network between the devices.

A. *Option 1: Independent point-to-point process bus*

This configuration models two different process bus systems from two different suppliers, where devices may or may not be interoperable. This is essentially a conventional protection system with process bus for I/O. System A is a point-to-point process system between Relay 1 and three of the PIUs. System B is a second, independent process bus system between Relay 2 and the other three PIUs.

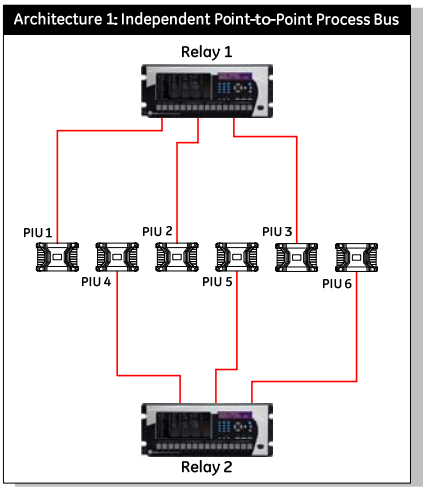

Fig. 3. Option 1 - independent point-to-point process bus

B. *Option 2: Interoperable point-to-point process bus*

This configuration models interoperable PIUs and relays from separate suppliers, using the simplicity of point-to-point connections. This option also models a fully redundant and interoperable system from a single supplier. In this configuration, the PIUs connect to both of the relays. The relays can use data from any parallel set of PIUs (such and PIU 1 and PIU 4). If one PIU is not available, the relay simply uses data from the other PIU in the pair. In this manner, both protection system still operate even on the failure of a PIU.

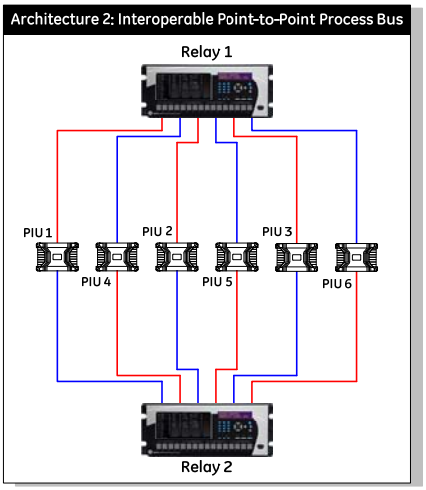

Fig. 4. Option 2 - interoperable point-to-point process bus

C. *Option 3: Independent point-to-point / switched network process bus*

This configuration models a protection system using process bus from different suppliers supporting different communications architectures. System A is point-to-point, with Relay 1 connected to three of the PIUs. System B is switched network with Relay 2 and the other three PIUs connected through an Ethernet network. Time synchronization will use IEEE 1588-compliant signals from a satellite clock published through the network. The PIUs and relays on the two systems do not interoperate or communicate with each other.

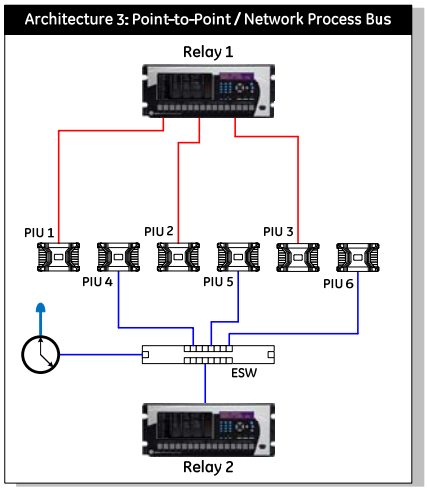

Fig. 5. Option 3 - Independent point-to-point / switched network process bus

D. *Option 4: Independent switched network process bus*

This configuration models a system where it is desired to keep System A and System B protection completely independent, including the communications between relays and PIUs. System A is Relay 1 connected through one network to three of the PIUs. System B protection is Relay 2 connected through a different network to three of the PIUs. Each network has a clock for time synchronization. The relays and PIUs do not interoperate or communicate with each other.

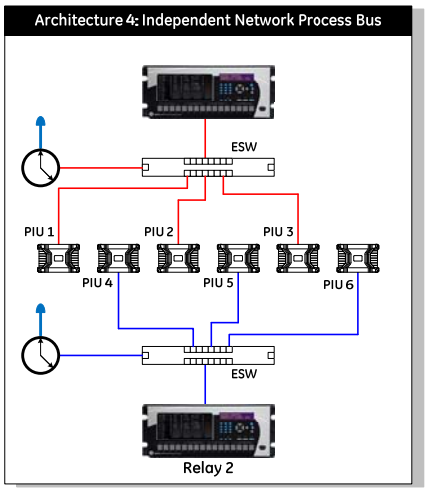

Fig. 6. Option 4 - Independent switched network process bus

E. *Option 5: Interoperable switched network process bus*

This configuration models a fully interoperable switched network process bus. The devices in this configuration can be devices from different suppliers that are interoperable, or can be devices provided by a single supplier. Both relays communicate to all PIUs, and can use PIU data redundantly. The two networks can use any network configuration, from star-connected networks to ring networks using RSTP or PRP. Time synchronization is through redundant IEEE 1588-compliant satellite clocks.

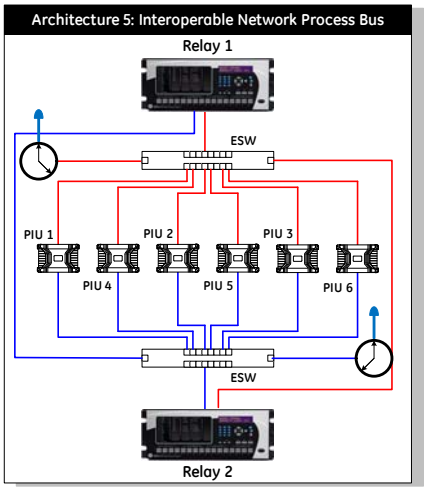

Fig. 7. Option 5: Interoperable switched network process bus

III. Reliability Analysis

The reliability analysis looks at the performance of each of these architectures in detail. The general goal is to show the availability and the system MTBF to provide performance comparisons. The analysis also takes a look at the overall system reliability at 1 year of service, 10 years of service, 20 years of service, and 30 years of service. Also determined is the opposite of reliability: the probability a system, not just an individual device, will fail over the same time intervals. The details for these calculations will be contained in the appendices to this paper.

Simple reliability analysis uses the failure rate (□) of individual components to determine system reliability. The failure rate of devices in practice is a complex topic, and the failure rate of systems is even more complex. To keep variables to a minimum, the analysis here uses some basic assumptions. The first assumption is that the failure rate □ of devices is constant over time, and this failure rate is known. The other assumptions are to simplify device and system models. The models focus how process bus impacts reliability. Therefore, common system components and their failures, such as instrument transformers and DC power, are common to all types of protection, and are ignored. However, possible failures due to the use of process bus are included. These failures are included in the models as a small failure rate due to unforeseen operating circumstances of process bus: lost data, or incompatibility in some way between PIUs and relays. The models assume that redundant devices are provided by different suppliers, but the reliability of these redundant devices is identical. This simplifies calculations, and eliminates the need to consider common mode failure as a reliability concern. Overall network reliability for the switched network architectures is ignored. This is a reasonable assumption to make. The relays and the PIUs are star-connected through an Ethernet switch to the network. Any link or port failure is a failure of communications, and is generically modeled as a switch failure. System reliability models are in Appendix B, and device reliability models and data are in Appendix C.

The results of this analysis are summarized in Table 1. The general results of this reliability analysis should not be surprising. Process bus requires more devices to work, and therefore has a negative impact on reliability. In this model, a relay needs data from 3 PIUs (or 3 PIU pairs) to operate, so the critical path for the protection system is the relay and 3 PIUs in series. Once a network is introduced, the relay, 3 PIUs, an Ethernet switch, and a clock are all on the critical path.

However, the protection system is highly available using any process bus architecture. The MTBF of the total system is reduced by using process bus. And reduced more so once a switched network is introduced. This is the intuitive result, as switched network process bus has more devices in the critical reliability path than point-to-point process bus, and both have more devices than conventional protection systems. All of the options are highly reliable, at least 99% reliable, for the first year. "Probability of failure" in the table is the inverse of reliability. If a system is 99% reliable, then there's a 1% chance the system will fail. This failure is a failure of the system, not of an individual device. This is a good metric to consider while thinking about the impact of process bus on system operations.

Table 1: Reliability Analysis

	General		At 1 year		At 10 years		At 20 years		At 30 years	
	Availability	MTBF	Reliability	Prob of Failure	Reliability	Prob of Failure	Reliability	Prob of Failure	Reliability	Prob of Failure
Conv.	1.00000	300	0.99998	0.0%	0.99762	0.2%	0.99094	0.9%	0.98060	1.9%
Option 1	1.00000	47	0.99903	0.1%	0.92659	7.3%	0.78053	21.9%	0.62486	37.5%
Option 2	1.00000	47	0.99974	0.0%	0.97646	2.4%	0.91522	8.5%	0.82995	17.0%
Option 3	1.00000	33	0.99586	0.4%	0.79411	20.6%	0.55853	44.1%	0.39599	60.4%
Option 4	1.00000	11	0.98232	1.8%	0.42253	57.7%	0.11196	88.8%	0.02749	97.3%
Option 5	1.00000	11	0.99183	0.8%	0.60797	39.2%	0.24339	75.7%	0.08357	91.6%

The general assumption in the industry is that a fleet of microprocessor based devices has approximately a 20 year lifespan. Therefore, the reliability of a process bus zone of protection at 20 years is of special interest. From the data, there are two general conclusions to draw. The first is that interoperable systems have better overall reliability than independent systems. The second, and more obvious, conclusion is that there is a high likelihood that a switched network process bus system will fail by 20 years. This likelihood of failure is due to two reasons: more devices in the critical path, and the very poor reliability of communications devices compared to other IEDs used in the substation. The lifespan of Ethernet switches is determined by the short lifespan of fiber-optic transceivers, combined with the heat produced by these transceivers, and the management of this heat through the device. The lifespan of satellite clocks is determined by, in great part, the antenna. The active components required in the antenna head to acquire satellite signals have major exposure to undesirable environmental conditions. See Table C-1 for the data used for device reliability.

Table 2: Reliability Analysis with ideal devices

	General		At 1 year		At 10 years		At 20 years		At 30 years	
	Availability	MTBF	Reliability	Prob of Failure	Reliability	Prob of Failure	Reliability	Prob of Failure	Reliability	Prob of Failure
Conv.	1.00000	300	0.99998	0.0%	0.99762	0.2%	0.99094	0.9%	0.98060	1.9%
Option 1	1.00000	69	0.99954	0.0%	0.96226	3.8%	0.87695	12.3%	0.77256	22.7%
Option 2	1.00000	69	0.99988	0.0%	0.98899	1.1%	0.95873	4.1%	0.91349	8.7%
Option 3	1.00000	59	0.99932	0.1%	0.94624	5.4%	0.83270	16.7%	0.70352	29.6%
Option 4	1.00000	46	0.99898	0.1%	0.92341	7.7%	0.77256	22.7%	0.61352	38.6%
Option 5	1.00000	46	0.99983	0.0%	0.98353	1.6%	0.93874	6.1%	0.87308	12.7%

The reliability analysis as documented in Table 1 is based on assumed reliability data for the devices. Much of this is documented reliability data based on actual devices. However, it is interesting to look at the reliability process bus with ideal devices. Ideal devices all have the same MTBF value as the best-performing device, with a small adjustment for hidden failures that may occur during process bus. This means the reliability analysis of Table 2 is based on architecture only, and not on actual devices. The performance of process bus systems is much better with ideal devices. Though the same general conclusions hold: point-to-point architectures are more reliable than switched network architectures, and interoperable architectures are more reliable than independent redundant architectures.

IV. PRACTICAL CONSIDERATIONS FOR RELIABILITY

Looking at the results of Table 1 seems to indicate that process bus is so unreliable that it is not appropriate for use in substations. Since Table 1 is based, in part, on actual devices, the results of Table 2 seem to indicate the goal should be to improve the reliability of devices before using process bus. In either case, reliability is just one input to the decision to adopt process bus. What these results do indicate is the need to consider reliability when adopting process bus. The protection system must be as available as desired, and the time, resources, and cost necessary to maintain the protection system must be controlled.

Simple reliability analysis, as performed here, doesn't accurately consider the impact of device repair or replacement. The assumption is a constant failure rate over time for all devices, this failure rate is constant in the same for a new device inserted as a replacement in existing system, and the same level of system failure still exists. In practice, the failure rate of devices changes over time as they age, so replacing devices will functionally (though not mathematically in the analysis) improve reliability. System maintenance and device replacement will therefore change the actual reliability in practice.

In terms of reliability and process bus, there are two different areas to consider. The first is that of making the system more reliable, in other words improving MTTF/MTBF, either through careful system design or by selecting devices with lower failure rates. The other area is that of reducing process downtime (PDT) or mean time to repair (MTTR), making the system or devices simpler to repair or replace.

A. System design

Careful system design is using the simplest architecture possible to meet reliability requirements over a specified service time. In terms of protection and process bus, this means reliability over 20 years. The fewest number of devices is important: more devices on the critical path results in a lower MTBF for the system. In general, good system design will increase redundancy for high failure rate devices are subsystems.

Careful system design for process bus clearly shows that point-to-point interoperable process bus is the best solution in terms of reliability. This is because there only 4 redundant pairs of devices in the critical path (see Fig. B- 2 for the reliability model), and these devices are all high reliability devices. However, the industry is apparently favoring interoperable switched network process bus. The goal for this permutation of process bus should be to match the same performance of a point-to-point system. An MTBF of 50 years, and a reliability of 95% over a 20 year service time. Reviewing the performance data of Table C-1, and the reliability model of Fig. B- 5, the obvious place to improve is the Ethernet switches and the satellite clocks. One method to improve the reliability is to make these devices triple redundant. A single clock has an MTBF of 11 years, redundant clocks have an MTBF of 17 years, and triple redundant clocks have an MTBF of 20 years. This is not enough improvement in reliability. Note that is also not practical today to have triple (or more) redundant networks, and triple redundant clocks, as relays and PIUs don't support this capability.

B. Better devices

The switched network process bus solution has 6 devices on the critical path. To have a system MTBF of 50 years, this essentially requires at every device have an MTBF of 300 years. ($MTBF = 50 = \frac{MTBF\ per\ device}{6\ devices}$). If redundant pairs the devices are used, this requires an individual devices have an MTBF of 200 years ($300/1.5$). This kind of reliability is already true for protective relays. The data for PIUs suggest that these devices can be improved to this level with experience, and reasonable cost and effort. It is very difficult, however, to improve the reliability of Ethernet switches, satellite clocks, and antennas to this level. The limiting components of these devices such as the fiber-optic transceivers, the antennas, and other electronic parts, are already mature components. This means the reasonable expectation is that only small gains in reliability are possible for these devices.

C. Making repair better

All systems eventually experience failure. Process bus based systems have more devices, and are therefore more likely to have failures than conventional protection systems. At the point of system failure, the focus must transition to mean down time (MDT) or process down time (PDT). PDT is a measure of the entire time the system is down, including problem diagnosis, device repair or replacement, and system testing and commissioning. With the lower reliability of process bus, there must be a strong drive to reduce PDT to a minimum. Even without system failures, there will be more device failures with process bus. It is necessary to design the system such that replacing a filed device doesn't require any PDT.

Reducing PDT requires careful process design, careful system design, and careful device design. Consider the reliability model for the point-to-point interoperable process bus:

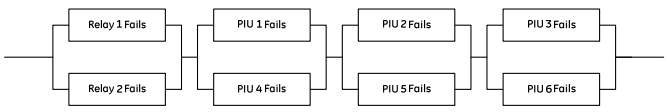

Fig. 8. Point-to-point interoperable process bus reliability model

The system is designed such that of any single device fails, such as PIU 1, protection still works. Protection still works if any other device fails, except PIU 4. The replacement of PIU 1, or any other failed device, is where careful process and device design is required.

The commercial aviation industry faces a similar challenge in terms of reliability and availability. A fly-by-wire control system is essentially the same as a process bus protection system: distributed devices send data and accept commands from a centralized control. The aviation industry has addressed the requirements of decreasing PDT by adopting a "design for replacement" strategy. Every individual device in the control system is a "black box" with a connectorized wiring and communications interface. On failure, the failed device is identified, removed, disconnected, and replaced in minutes. The devices are "black boxes", so device configuration is kept to a minimum (normally, none), and extensive system reconfiguration and testing is not required. The majority of PDT for an airline is getting the part to the plane, and documenting repair actions taken.

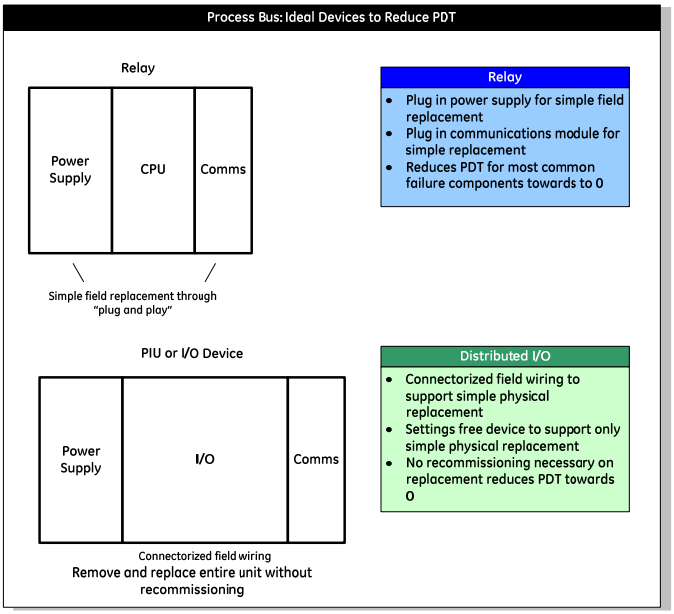

Fig. 9. PDT improvement for process bus devices

A similar philosophy needs to be adopted by the protection industry. Process bus is ideal for this modular, black box concept. Look again at the model of Fig. 8. If every individual device is designed such that the device, or low reliability parts of the device, can be replaced in a half hour or less, without requiring special tools, testing, or commissioning, then process bus goes a long way towards meeting the goal of reducing PDT to a minimum.

The general concept is illustrated graphically by Fig. 9. All devices, or the most likely to fail components of devices, can be quickly replaced by simply removing the failed device or component, and plugging in a replacement device or component. This requires devices support connectorized field wiring, replaceable/pluggable modules, and the elimination as much as possible of configuration are settings. The goal is to eliminate the need for a formal engineering project to replace a device by turning everything into simple component replacement.

The end result is that adopting process bus requires careful thought to maintain acceptable levels of reliability. The focus must be on the simplest architecture that meets reliable requirements, and must be on a design for replacement mindset using easily replaceable and interchangeable devices.

V. Device Design To Decrease Process Downtime

To decrease process downtime requires designing devices, and the system, to support this goal. In general, this means designing devices that can be replaced with minimal effort. This results in three main design goals for devices: a specifically defined function / algorithm for the device such that there is no configuration or only simple, transferable settings are required; defined data messaging between devices; and connectorized field wiring to simplify physical replacement.

This design for replacement can be defined for all three subsystems of a process bus protection and control system, including the distributed I/O devices, the communications network, and the protective relays.

The I/O devices for process bus are the easy to design to limit process downtime. Merging units, remote I/O modules, and process interface units are simply I/O devices that convert analog measurements into digital signals. These are simple devices, and it will be better to replace the entire device as opposed to device components. They have a specifically defined function from the start. The simplest plan is for these devices to be dumb I/O with at most address settings. Otherwise, they must have a reusable configuration or settings file. Removable terminal blocks or aviation style wiring connectors make physical replacement simple.

Another form of I/O device is non-conventional instrument transformers, such as fiber optic current transducers (FOCTs). Once again, these are simple I/O devices, with a defined function. FOCTs can be designed such that the light source, the lowest reliable component, can be easily replaced without removing the FOCT or having to recalibrate the FOCT.

The communications network can be more complex. The best solution is point-to-point communications between I/O devices and relays, as the communications network reduces down to fiber optic cables. If the process bus network is a LAN, then device replacement can be more complex. Ethernet switches have a defined function, and are simple to physically replace. However, transferring the configuration can be complicated. Replacing the switch like-for-like can make network configuration simple. Even better is to use "scheduled" networks through Time Sensitive Networking or Software Defined Networking, such that the configuration of individual switches is defined by the entire network.

It is difficult to have a completely predefined function or algorithm for protective relays, as the relays are actually the application. Fortunately, the CPU running the algorithms is the least likely to fail component. Power supplies and communications transceivers are the most likely to fail components. Relays should be designed such that power

supplies and communications transceivers are modules that can be easily field replaced without effort.

An additional plus for process bus systems, designed to minimize process downtime, is the ability to replace all the relays at once, using "plug in" control buildings. The entire protection and control system for a substation can be replaced at once, putting all the relays on the same generation of hardware, and on the same utility design standards.

VI. Summary

An important consideration when adopting process bus is that of reliability. A process bus system will be as available as a conventional protection and control system, but will not be as reliable over time. This is simply due to the increased number devices required to make up the system, which leads to more devices to fail. The reliability analysis performed in this paper shows a drastic reduction in the mean time between failures of the protection system using process bus, and shows a high likelihood of protection system failures. However, this does not mean that process bus should not be adopted.

When designing or adopting process bus for use, it is important to follow the basic rules for a reliable system: one should choose the simplest architecture possible to meet all the application requirements, with the fewest number of devices on the critical path. And one should attempt to use devices with the highest reliability possible. In the goal should be used devices that are simple, and simple to replace in the field, to reduce any process down time due to system failures to the minimum practical. It is clear from this analysis that point-to-point interoperable process bus is the architecture that best meets these requirements. It is the simplest architecture as for distance protection there only for devices on the critical path. And these are all high reliability devices, relays and PIUs. No low reliability Ethernet switches or satellite clocks are used. And the PIUs can be designed as simple to install, simple to remove, and simple to configure devices, making PDT a minimum.

Thinking in this manner redefines the business case for process bus. The upfront business case is that of reducing the amount of skilled resources required to design and install protection and control systems, while keeping project costs the same, if not slightly improving them. The real business case is that process bus makes device and system maintenance, replacement, and upgrade much simpler in terms of resources and effort, and much more cost effective.

Appendix A Basic Reliability Concepts

Basic reliability concepts are that of reliability (R), availability (A), failure rate (λ), mean time between failure (MTBF), mean time to failure (MTTF) and mean time to repair (MTTR). To define these terms:

MTBF is the mean time between failure, or the average time between failures for specific device. This can be calculated data, or is best determined from actual field data.

λ is the failure rate over time of a device. For the analysis performed in these examples, λ is represented by $\lambda = \frac{1}{MTTF}$. Note that λ is normally defined as the number failures over a set period of time, such as 1,000,000 hours.

Reliability is the measure the system performance over time. The strict definition of reliability is given by the equation $R(t) = e^{-\lambda t}$. λ and t must be in the same units: hours, years.

MTTF, or mean time to failure, is the average time it takes a device to fail. For purposes of this analysis, MTBF at MTTF considered to be equivalent. The strict definition of MTTF is given by the equation.

$$MTTF = \int_0^\infty R(t)dt$$

MTTR, or mean time to repair, is how long it takes to repair a failed system.

Availability is a measure of the likelihood that a system or device is going to be operating. Availability is defined by the equation $A = \frac{MTBF}{MTBF + MTTR}$.

Reliability of series connected devices

The reliability of two devices connected in series is determined by multiplying the individual reliability of the two devices together. Consider this simple example:

Figure A- 1: Series reliability

So:

$$\begin{aligned} R_S &= R_1 \times R_2 \\ &= e^{-\lambda_1 t} \times e^{-\lambda_2 t} \\ &= e^{-(\lambda_1 + \lambda_2)t} \end{aligned}$$

And MTTF is:

$$\begin{aligned} MTTF &= \int_0^\infty R(t)dt \\ &= \int_0^\infty e^{-(\lambda_1 + \lambda_2)t}dt \\ &= \frac{1}{\lambda_1 + \lambda_2} \end{aligned}$$

Therefore, system calculations are:

$$R_S = R_1 \times R_2$$

$$MTTF_S = \frac{1}{\lambda_1 + \lambda_2}$$

$$\lambda_S = \frac{1}{MTTF_S} = \lambda_1 + \lambda_2$$

Reliability of parallel connected devices

The reliability of devices connected in parallel is determined by multiplying the unreliability of all the devices, and subtracting this from the ideal reliability of one. Consider the simple example:

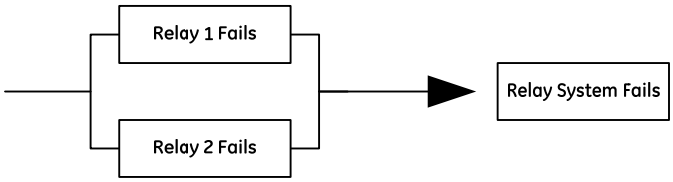

Figure A- 2: Parallel reliability

Then the reliability is then:

$$\begin{aligned} R_S &= 1-(1-R_1)\times(1-R_2) \\ &= 1-\left(1-e^{-\lambda_1 t}\right)\times\left(1-e^{-\lambda_2 t}\right) \\ &= e^{-\lambda_1 t}+e^{-\lambda_2 t}-e^{-(\lambda_1+\lambda_2)t} \end{aligned}$$

And MTTF is:

$$\begin{aligned} MTTF &= \int_0^\infty R(t)dt \\ &= \int_0^\infty e^{-\lambda_1 t}+e^{-\lambda_2 t}-e^{-(\lambda_1+\lambda_2)t}dt \\ &= \frac{1}{\lambda_1}+\frac{1}{\lambda_2}-\frac{1}{\lambda_1+\lambda_2} \end{aligned}$$

Therefore, system calculations are:

$$R_S = 1-(1-R_1)\times(1-R_2)$$

$$MTTF_S = \frac{1}{\lambda_1}+\frac{1}{\lambda_2}-\frac{1}{\lambda_1+\lambda_2}$$

$$\lambda_S = \frac{1}{MTTF_S}$$

RELIABILITY IN CONCEPT

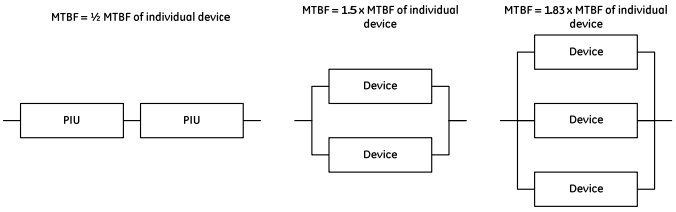

Figure A- 2: Devices and MTBF

APPENDIX B - ARCHITECTURE RELIABILITY MODELS

The following are reliability models for the 5 process bus architectures:

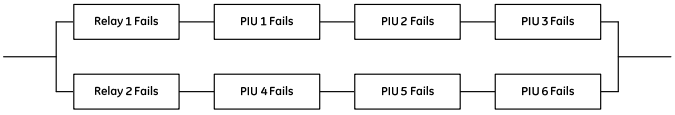

Figure B- 1: Option 1 reliability model

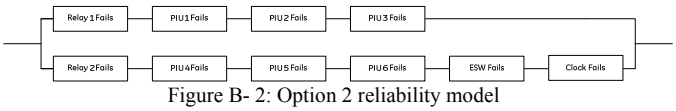

Figure B- 2: Option 2 reliability model

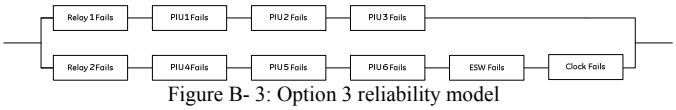

Figure B- 3: Option 3 reliability model

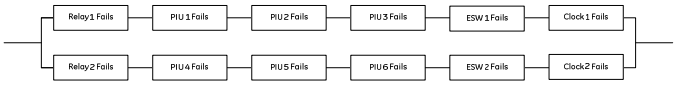

Figure B- 4: Option 4 reliability model

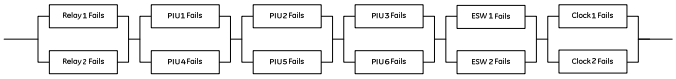

Figure B- 5: Option 5 reliability model

APPENDIX C - RELIABILITY DATA

Individual device data used to calculate reliability parameters:

Table C-1: Reliability data for model devices

	Device	MTBF (years)	MTTR (hrs)	U * 10^{-6}
Switch	Ethernet Switch	50	48	110
	Hidden Failure	2500	48	2
Clock	Clock	15.3	48	358
	Antenna	39.5	48	139
Process Bus Relay	Relay	200	48	27
	Hidden Failure	2500	120	5
CT PIU	PIU Failure	120	48	46
	Hidden Failure	2500	48	2
VT PIU	PIU Failure	120	48	46
	Hidden Failure	2500	48	2
Conventional Relay	Relay	200	120	68

Relay and Switch MTBF is based on anecdotal data. Clock MTBF data is taken from [7]. PIU data is based on actual device data. "Hidden Failure" in this context is intended as a "catch all" factor for unknown failures that may occur with process bus (device sampling issues, how relays handle lost packets, etc.). The MTTR data is only used for Availability calculations. 48 hours is simple device replacement (including diagnosis, travel time, etc.). 120 hours is a replacement that requires significant configuration and commissioning on replacement. This leads to the following reliability data for devices:

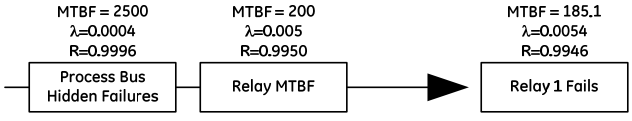

Figure C - 1: Process bus relay reliability

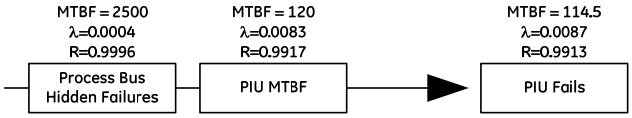

Figure C - 2: PIU reliability

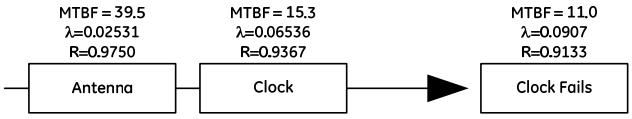

Figure C - 3: Clock reliability

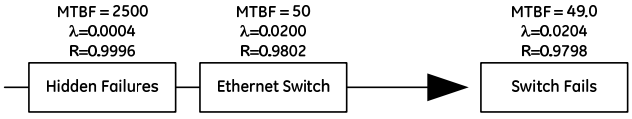

Figure C - 4: Ethernet switch reliability

BIOGRAPHY

Rich Hunt is a Market Development Leader with GE Grid Solutions, focusing on IEC 61850 solutions and strategies for protection and control systems. Rich has over 25 years' experience in the electric power industry with both utilities and solution providers. Rich earned the BSEE and MSEE from Virginia Tech, is a Senior Member of IEEE, a member of the Main Committee of the IEEE Power System Relaying Committee, the U.S. representative to the CIGRE B5 Technical Committee, and is a registered Professional Engineer.

REFERENCES

[1] R. Hunt, "Process Bus: a practical approach", *PAC World, Spring 2009*.

[2] T. Werner, A. Schnakofsky, "IEC 61850 process bus deployment considerations for digital substations", *PAC World Americas Conference, Raleigh, NC, September 2014*.

[3] R. Hunt, "Practical Considerations for Applying Process Bus", *SEAPAC 2011, CIGRE Australia Panel B5, Sydney, Australia, March 2011.*

[4] R. Hunt, D. McGinn, "Best Practices for Testing Process Bus Protection and Control Systems", *SEAPAC 2013, CIGRE Australia Panel B5, Brisbane, Australia, March 2013*

[5] R. Hunt, T. Ernst, "Using IEC 61850 Process Bus to Meet NERC PRC-005-2 Condition Based Maintenance Requirements", *PAC World Americas Conference, Raleigh, NC, September 2014.*

[6] C.A. Dutra, S.L. Zimath, L.B. de Oliveira, "Process Bus Reliability Analysis" , *PAC World Americas Conference, Raleigh, NC, September 2014.*

[7] D.M.E. Ingram, P. Schaub, D.A. Campbell, R.R. Taylor, "Quantitative Assessment of Fault Tolerant Precision Timing for Electricity Substations", *IEEE Transactions on Instrumentation and Measurement, 62(10), pp. 2694-2703, IEEE, New York, NY.*

[8] R. Hunt, "Relay Lifecycle Management Using Process Bus", *PAC World Americas Conference, Raleigh, NC, September 2014.*