NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

SP-8 Report

Reliability for IEC 61850

November 20, 2013

Contributing Members:
Alex Echeverria (Chairman – New York Power Authority), Simon Chano (Former Chairman – TransÉnergie), John Babu (Northeast Utilities), Bob Beresh (Hydro One), Dave Bertagnolli (ISO New England), Abiye Fisseha (Central Maine Power), John Freeman (Central Maine Power), David Lambert (TransÉnergie), Brian Langlais (Central Maine Power), Hai (Quoc) Le (NPCC), Frank Ronci (New York Power Authority), George Wegh (Northeast Utilities), Mohammad Zubair (Hydro One)

Table of Contents

Note: Terms in bold typeface are defined in the *NPCC Glossary of Terms.*

1. INTRODUCTION

Since 2011, the Task Force on System Protection has reviewed a number of protection systems designed using the IEC 61850 technology. This technology embodies a new approach to substation automation and **protection** design using modern computer and network technology. IEC 61850 utilizes Generic Object Orientated System-wide Events (GOOSE) messages over a dedicated LAN to replace the conventional hard wired logic necessary for intra-**relay** communication. Appendix B provides an overview of the **Protection System** Using IEC 61850.

A subgroup of the Task Force on System Protection has also been looking into concerns with the implementation of the 61850 **protection** based technology including the impact it may have on the current NPCC **protection** design requirements as stated in Directory #4 (D4) and Directory #7 (D7). Appendix C proposed a comparison of the relative probability of failure of traditional substation **protection** design and new **protection** design using IED 61850 technology, which integrates the substation **protection** and control functions for all **elements** at a **Buk Power System (BPS)** substation

At the September 2012 meeting, TFSP agreed that a formal Ad Hoc Working Group (SP-8) should be formed to be comprised of interested TFSP members or their representatives. The SP-8 was tasked to recommend any additional requirements in D4 and D7 for the evaluation of the **protection system** design using 61850 Technology. SP-8 may also provide guidance to be included in the Appendix of D4 and D7. For this report, maintenance and testing criteria as it pertains to Directory #3 (D3) requirements is not included. However, section 5 (Design Consideration to Facilitate Maintenance) has been added in this report for guidance.

2. IEC 61850 APPLICATION ARCHITECTURE IN PROTECTION IMPLEMENTATIONS

a. Physical Analog Inputs for Protection Applications (Duplication Issues, Separation, Etc.)

i. Merging unit design consideration shall address the inherent reduction in **protection system** reliability and availability that the use of merging units presents. The failure of a merging unit shall not lead to the loss of more than one **protection group** per **element**. To address the inherent reduction in reliability, more than one merging unit shall be provided for each **protection group** at all times.

ii. Continuous streaming of sampled values may consume a large amount of LAN bandwidth. The network architecture shall account for bandwidth-intensive applications and **protection system** response, as required by planning standards, shall not be impacted by increased traffic during any scenario.

iii. Process bus network reconfigurations shall not result in momentary or permanent unavailability of both **protection** schemes for any **BPS element**.

iv. Analog/Digital conversion, processing and communication speeds shall maintain a level of accuracy that at a minimum meets current utility **protection** performance criteria.

b. Physical Digital Inputs for **Protection** Applications

i. The failure of a merging unit or IED that transmits digital inputs for **protection group** applications shall not lead to the momentary or permanent loss of more than one **protection group** for the same **element**.

ii. Inputs necessary for correct **protection system** operation shall be conditioned for a communication loss or power failure such that upon restoration of communication or power the intended input state is received.

c. Intra-station **Protection** Communications

Redundant communications within a **protection group** can significantly increase **protection** availability and reliability.

Sampled values and GOOSE messages shall have the highest priority among all traffic in the network and network interfaces of end-devices.

i. Sampled Values

1. Loss of one **protection group's** sampled value data stream shall not momentarily or permanently compromise the redundant **protection group's** sampled value data stream, unless studies demonstrate that the total clearing time including momentary interruption is acceptable.

2. If a failover scheme is used, the loss of sampled value data shall not result in any undesired protection operations.

3. Network traffic shall not affect protection performance.

4. **Protection** performance shall be evaluated under stressed network and failover conditions to ensure that protection coordination and performance is within the acceptable design limits.

ii. GOOSE Messages

1. Network configurations that impact the delivery or latency of GOOSE messages in one **protection group** shall not momentarily or permanently affect the delivery or latency of GOOSE messages in the redundant **protection group** for the same element, unless studies demonstrate that the total clearing time including momentary interruption is acceptable**.**

2. The reception and processing of a GOOSE message is time critical, specifically during events and relaying operations. The use of GOOSE messages for **protection** shall be configured (dataset priority, how messages are published, VLANS, network configuration, etc.) such that the maximum clearing times as specified by Planning Studies are met.

iii. Time Synchronization

1. If process bus is not employed, time synchronization shall meet the minimum accuracy requirement in Directory 4, 5.20.3 and Directory 7.

2. If the process bus is employed, a single device failure shall not lead to the momentary or permanent loss of time synchronization for more than one **protection group** for the same **element**.

d. Physical Digital Outputs for **Protection** Applications

i. The failure of a merging unit or IED that transmits digital outputs for **protection group** applications shall not lead to the momentary or permanent loss of more than one **protection group** for the same **element**.

ii. Outputs necessary for correct **protection system** operation shall be conditioned for a communication loss or power failure such that upon restoration of communication or power the intended output state is restored.

iii. Contact outputs used for tripping interrupting devices shall be properly rated to make, break and carry the DC current for the tripping circuits that they are applied to.

3. NETWORK COMMUNICATION ARCHITECTURE

a. Physical Topology

i. Protection LANs for redundant **protection groups** shall be powered by different battery systems as specified in Directory 4 and Directory 7.

ii. The network topology shall be designed in a way that will ensure that a single broken path does not momentarily or permanently disable both **protection groups**, unless studies demonstrate that the total clearing time including momentary interruption is acceptable.

iii. Network devices with redundant power supplies shall be powered from the same DC battery system.

iv. Nonredundant devices that need to interface with both “A” and “B” **protection groups** shall not introduce a momentary or permanent common mode failure.

b. Network Device Configurations

i. Protection LANs shall take into account the following attributes in the design and configuration:

1. Redundancy: The use of network redundancy protocol and network configuration should be considered to improve LAN availability.

2. Prioritization: **Protection** related data shall take priority over other types of data that may be transported over the protection LANs. **Protection** LANs shall be designed such that the **protection** response shall not be adversely impacted during stressed network conditions. (Due to the possibilities for non-protection network traffic such as DME record retrieval, security video streaming, phasor measurements, etc. the requirement for **protection** message response time shall meet the critical clearing time requirements in all network loading conditions. Network designs shall keep the **protection** performance as the highest priority traffic.)

3. Speed: The protection LAN propagation times during stressed network conditions shall be included in the calculation of clearing times of protected equipment. Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical

effects include queuing delay, packet loss or the blocking of new connections.

4. Failure modes: The failure of a single network device shall not momentarily or permanently disable both **protection groups**, unless studies demonstrate that the total clearing time including momentary interruption is acceptable[1].

4. MONITORING (ELEMENT FAILURE)

Relay hardware, communication paths, communication hardware and merging units shall be continuously monitored for software failure, hardware failure and/or communication failure and annunciated in order to allow prompt attention by the appropriate operating authorities.

5. DESIGN CONSIDERATION TO FACILITATE MAINTENANCE

a. The network architecture shall provide a dedicated and secure method for personnel to connect to the LAN for testing, troubleshooting and operational purposes.

b. A method shall be provided to isolate the operation of **protective relaying**, while maintaining a network communication path to give personnel the ability to view a proper **relay** response while under test.

c. Pre-commissioning testing specific to the entity's design shall be performed to ensure interoperability of IEC 61850 devices. The fact that an IED has a conformance certificate will not guarantee it will inter-operate with other conformance certified IEDs in the same substations.

d. Firmware upgrades, automation software updates shall be tested and documented in a controlled, off-line environment prior to being placed into service to determine if there are any adverse impacts which could prevent proper **protection system** operation. Reference IEEE C37.231-2012.

e. Network monitoring tools shall be used to facilitate troubleshooting/corrective maintenance to reduce outage times, and assist in event and disturbance analysis.

f. All GOOSE messages should contain information to uniquely identify its publishing device. GOOSE message identifiers should provide descriptive nomenclature to aid maintenance and troubleshooting activities.

[1] Under the presently available network protocols (RSTP, ERSTP, etc.), a network based **protection system** utilizing a shared LAN for both **protection groups** can be exposed to significant disruptions during the self-healing process known as re-convergence. During this period no GOOSE traffic is passed by the network switches and results in a momentary loss of protection. If both **protection groups** share the same network, re-convergence following a switch failure can result in the loss of both **protection groups** for a single network element failure.

g. Documentation of the system configuration shall be developed to aid testing, troubleshooting, and maintenance. Examples of this include logic diagrams, signal lists, GOOSE mapping tables, and basis documents.

6. ENVIRONMENT (PROPOSED REVISION TO D4 SECTION 5.12)

a. Each separate **protection group** and **teleprotection** protecting the same system **element** shall be on different non-adjacent vertical mounting assemblies or enclosures, except as noted in 6.f.

b. **Protection group** LAN devices for redundant **protection groups** shall be on different non-adjacent vertical mounting assemblies or enclosures, except as noted in 6.f.

c. Wiring or Fiber Optics for separate **protection groups** and **teleprotections** protecting the same system **element** shall not be in the same cable.

d. Cabling for separate **protection groups** and **teleprotections** protecting the same system **element** shall be physically separated. This can be accomplished by being in different raceways, trays, trenches, etc.

e. In the event a common raceway is used, cabling for separate **protection groups** protecting the same system **element** shall be separated by a fire barrier.

f. Electronic devices physically located outdoor in the substation yard which serve as **components** of **protection groups**, protecting the same **element,** shall be physically separated. This can be accomplished by separate enclosures, or by a fire barrier.

g. An electronic device which serves as a **component** of a **protection group**, and is physically located near primary equipment and outside of the control house, may be subject to more severe environmental conditions than if it was located inside of a building. These environmental conditions may include extreme temperatures, corrosive atmosphere, and electromagnetic interference (EMI). Electronic device selection and secondary enclosure design ("cabinets") shall ensure that environmental conditions do not reduce **protection group** reliability and availability and that the electronic devices contained therein are not subject to environmental conditions above the accepted limits specified by the IEEE or IEC. As a minimum, any outdoor enclosure shall have a NEMA 4X rating for non-EMI related environmental conditions.

For further reference, see IEEE C37.90-2005, IEEE C37.90.1-2012, IEEE C37.90.2-2004, IEEE C37.90.3-2001, IEEE 1613-2003/1613a2008 (Class 2), IEC 61850-3 ed2.0 and NEMA 250-2003.

7. OTHER CONSIDERATIONS

a. The configuration of IEC 61850 protection system should remain as simple as possible to minimize the risks associated with test and maintenance.

b. While isolated testing of a device is acceptable for some commissioning tests, end-to-end secondary injection testing should be conducted to ensure that all interfacing protections perform as designed under dynamic/fault conditions.

c. Integrated Network Switches: It is not recommended that an entity design a network that utilizes switches that are integrated in **protective relays**, since this will mean that a single contingency outage could result in both a **protection** device failure and the

protection LAN failure. (Some commercially available **protective relays** can be equipped to serve as a network switch as well as a **protective relay**. It is recommended that the function of switches and protective device be kept as a separate device so that maintenance, failure, or removal of the **protective relay** does not disrupt or disable the rest of the **protection group**.)

d. Diversity of manufacturers should be considered for network switches.

e. The following example provides one possible network design where two redundant **protection groups** are isolated separate networks in order to eliminate a single point of failure. This IEC 61850 network based **protection system** relies on the network to pass information critical to the operation of the **protection system** and thus the network becomes part of the **protection system**. The main concern when designing the network architecture was a single point of failure which could permanently or momentarily disable both **protection groups** from operating.

   Rapid spanning tree protocol is used in a loop network which monitors the health of the network by checking the continuity of the loop, while blocking the network traffic at one point in the loop, called the blocking port, to prevent re-circulation of a network message, leading to a broadcast storm. The main switch, called the root bridge controls continuity check and controls the blocking port(s) which can be turned on should a failure of any other point in the network occur, re-establishing the network. When the root bridge (switch) detects a break in the network, it senses the paths remaining, turns on blocking ports and re-establishes the network based on a calculated lowest cost path to each switch. During this period of time, known as re-convergence, the network switches do not pass normal traffic until the network is “re-built”. The worst case outage scenario is a failure of the Root Bridge, and this type of network can only have one Root Bridge. The result is during a network **component** failure, the network will self-heal using rapid spanning tree protocol (or other similar protocols), but when both **protection groups** are on the same network, neither will be capable of exchanging information via GOOSE messages.

   The resulting design was two independent networks, each using rapid spanning tree protocol, removed the possibility of a single failure on either network affecting the other **protection group**. This system required a main and backup data concentrator and substation HMI for the operator interface. The redundant HMIs need to poll data from **relays** in both **protection groups**, which required main and backup routers be installed to connect the two networks. The routers allow the HMI and data concentrator to monitor MMS messages from **relays** on either network, but the self-healing protocols, and resulting momentary outages are blocked by the routers from spreading between the two networks.

   The design of the system was to have the Bay Control **relay** in either **protection group** capable of performing the normal breaker/disconnect control functions, with only one active at a time. The Interlocking between the two Bay Controllers, for blocking close commands in the active system was no longer possible via GOOSE messages, so hard wired contacts were used to block the close permissive from a lockout in system A to the active Bay Controller in system B. See Figure 1 below.

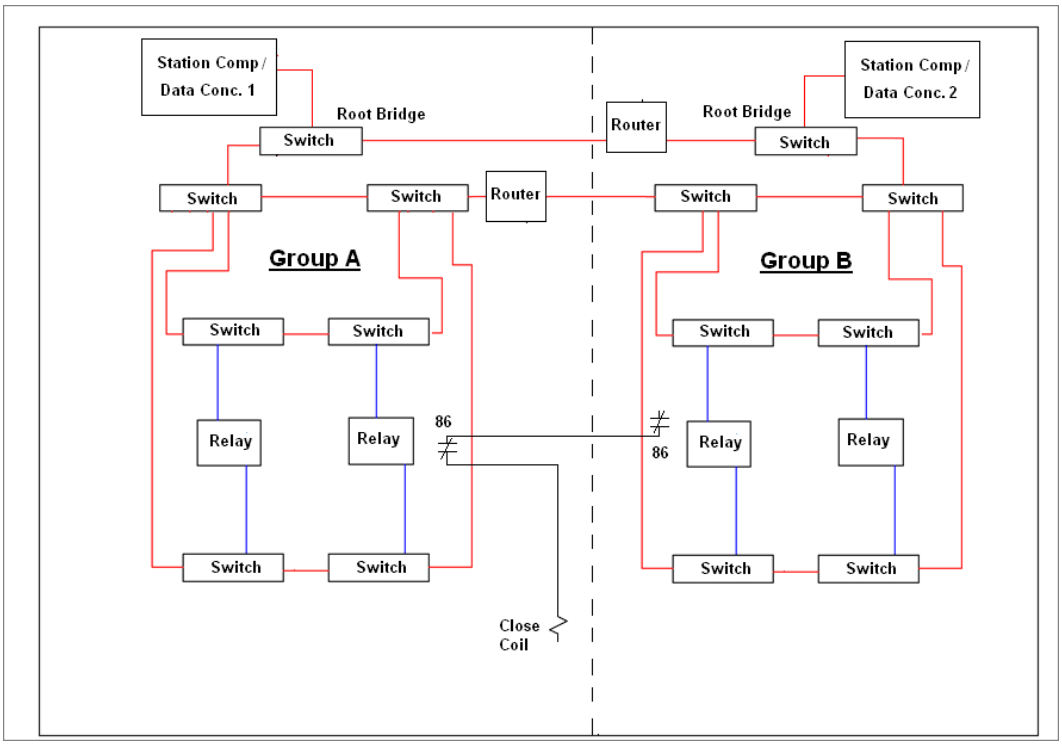

Figure 1

f. In any IEC 61850 implementation, only devices that have been tested and certified by a UCA accredited facility as conforming with IEC 61850-5 ed2.0, Section 6.6 - Conformance test requirements, shall be used.

g. Status inputs associated with primary equipment auxiliary contacts that are not regularly exercised and maintained (MOD aux contacts) may require additional security to verify the status input is valid. See Figure 2 below.

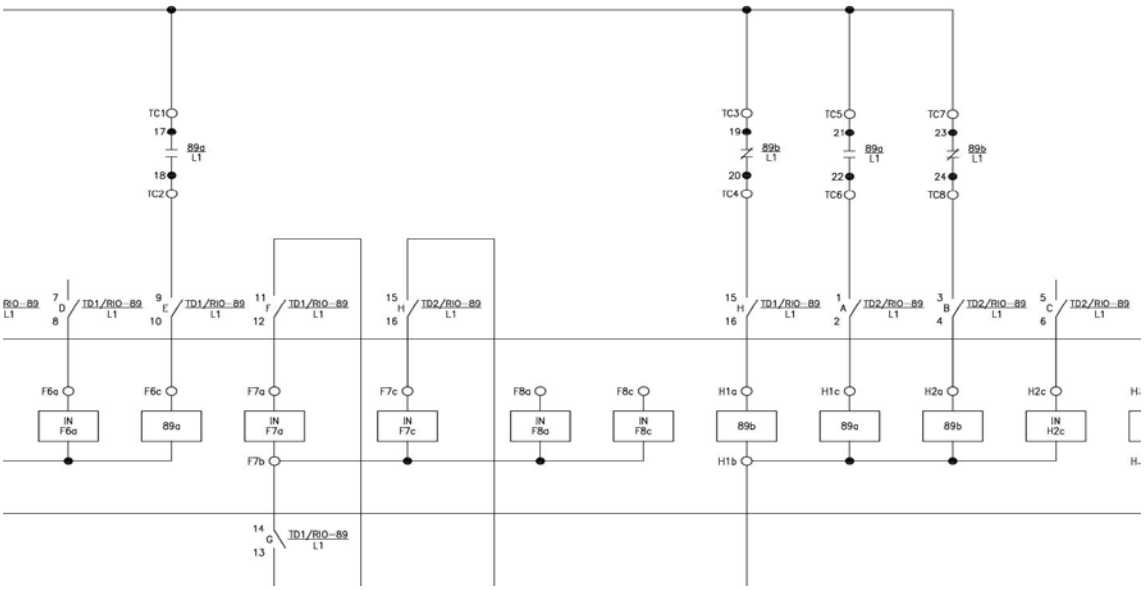

Figure 2

8. GLOSSARY OF TERMS

DME - Disturbance Monitoring Equipment
ERSTP - Enhanced Rapid Spanning Tree Protocol
IEC - International Electro-technical Commission
IED - Intelligent Electronic Device
Integrated Network Switch – A protective IED that also incorporates a network switch within the same enclosure.
GOOSE - Generic Object Oriented Substation Event
LAN - Local Area Network
Merging Unit – An intelligent electronic device (IED) that collects multichannel signals output by current transformers and voltage transformers synchronously, along with device status, control, then exchanges these signals with the protocol of IEC61850 to protective devices and measure-control devices.
RSTP - Rapid Spanning Tree Protocol

VLAN - Virtual Local Area Network

Appendix A

Task Force on System Protection

Scope of SP-8 Ad Hoc Working Group on IEC 61850 Protection System Technology

The SP-8 Ad Hoc Working Group will investigate and recommend any additional requirements in NPCC Directory #4 (D4) and Directory #7 (D7) for the evaluation of the **protection system** design using IEC 61850 technology. SP-8 may also provide guidance to be included in the Appendix of D4 and D7. A report will be developed and presented to TFSP at the September 2013 Meeting.

The areas the working group may take into account in this review include:

- Preservation of protection systems reliability and availability practices
- Appropriate use of local and remote protection functions
- Acceptable design practices using IEC 61850 and proprietary protocols
- Replacement, refurbishment, and retrofit migration strategies
- Self-supervision; identification of undetected failure modes
- Substation communication architecture and protocols
- Communication reliability aspects
- Modern communication equipment/tools interfaced with protection systems
- Merging units
- Remote access
- Cyber security impacts
- Configuration Tools
- Consultation with EPRI on challenges the industry faces in migrating to IEC 61850 technology

It is the intention of TFSP to separately treat the investigation and recommendation related to maintenance strategies for IEC 61850 based technology consistent with the requirements of NPCC Directory #3/NERC Standard PRC-005 at a later date.

Approved by RCC November 27, 2012

Appendix B

Protection System Using IEC 61850

1 GOOSE BASED SOLUTIONS

The implementation of GOOSE messages for **protection** is typically related to the exchange of signals with other substation devices. Some examples include, but are not limited to:

- Receiving a GOOSE message to detect a change of state of the breaker
- Sending a GOOSE message to initiate reclosing
- Sending a GOOSE message to initiate breaker failure **protection**
- Sending and receiving GOOSE messages for accelerated **protection** schemes
- Sending a GOOSE message to operate a breaker

One of the key requirements for the application of distributed protection functions using GOOSE messages is that the total scheme operating time is the same or faster than that of a hard wired conventional scheme.

2 IMPLEMENTATION OF PROTECTION SCHEMES USING IEC 61850 GOOSE

The implementation of protection schemes depends on the requirements of the application, the available communications channel and the substation communications protocol.

The introduction of IEC 61850 for substation communications and the significant increase in the availability of fiber optic cables between substations allows a new way of implementing protection schemes. Hard wiring between the **relay** outputs of **protection** devices and the inputs of other devices can be replaced with virtual connections using GOOSE messages transferred over network cables.

System hierarchy and process connection
Substation Automation (SA) systems have two logical hierarchical levels (Figure A1) which are found in most implementations as physical levels also:

a. The *process level* refers to the power system equipment in the substation represented by the process interface.
b. The *station level* refers to tasks for the complete substation and consists typically of the substation computer with central functions and HMI and of the gateway to the network control center. The station level also consists of **protection** and control IEDs (Intelligent Electronic Device) hosting the related functions.

Note that although the terms “process bus” and “station bus” are commonly used, these two communications networks do not necessarily need to be realized as independent networks.

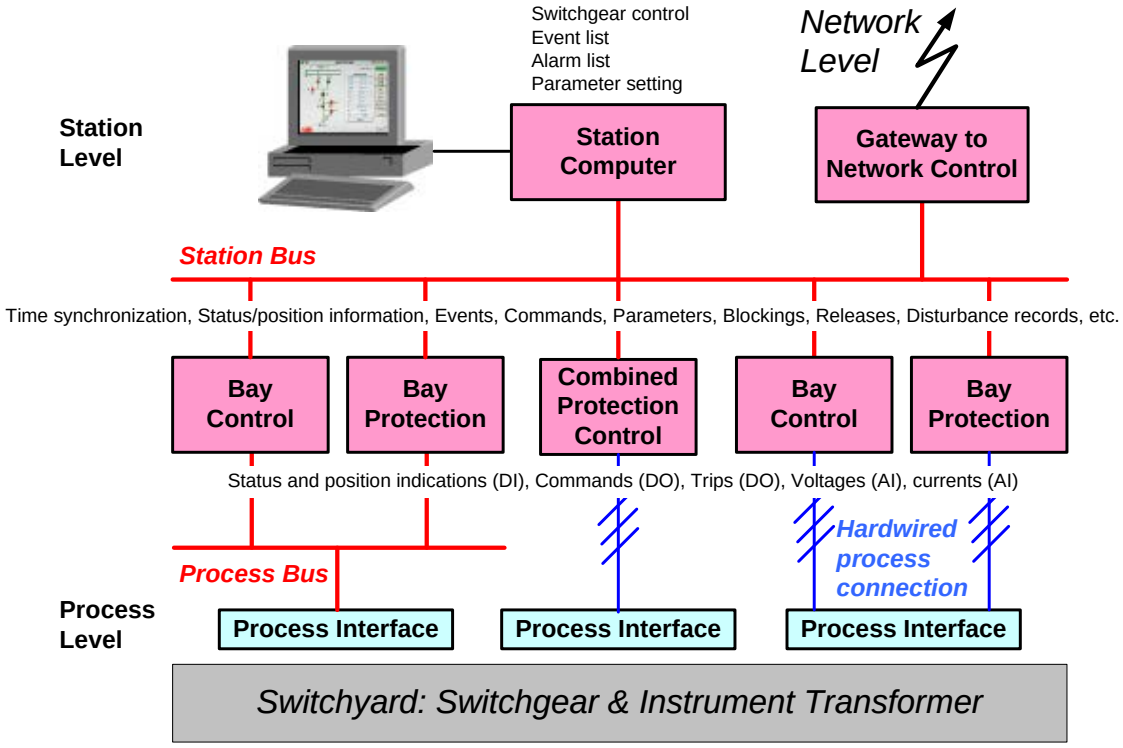

Figure A1 – System hierarchy and process connection for exchanged data

Functions and data exchange
Control functions are the acquisition of switch states (breakers, isolators and ground switches, etc.) and the provision of commands to the switches.

Process links
The conversion of hardwired signals to digital data can be realized at the process level. For example, the I/Os and the related converters from the station level IEDs may be moved to the process level and connected with the application functions processed in the station level IED (See Figure A2 on the right hand side). As a result, new process devices such as merging units (MU) are introduced.

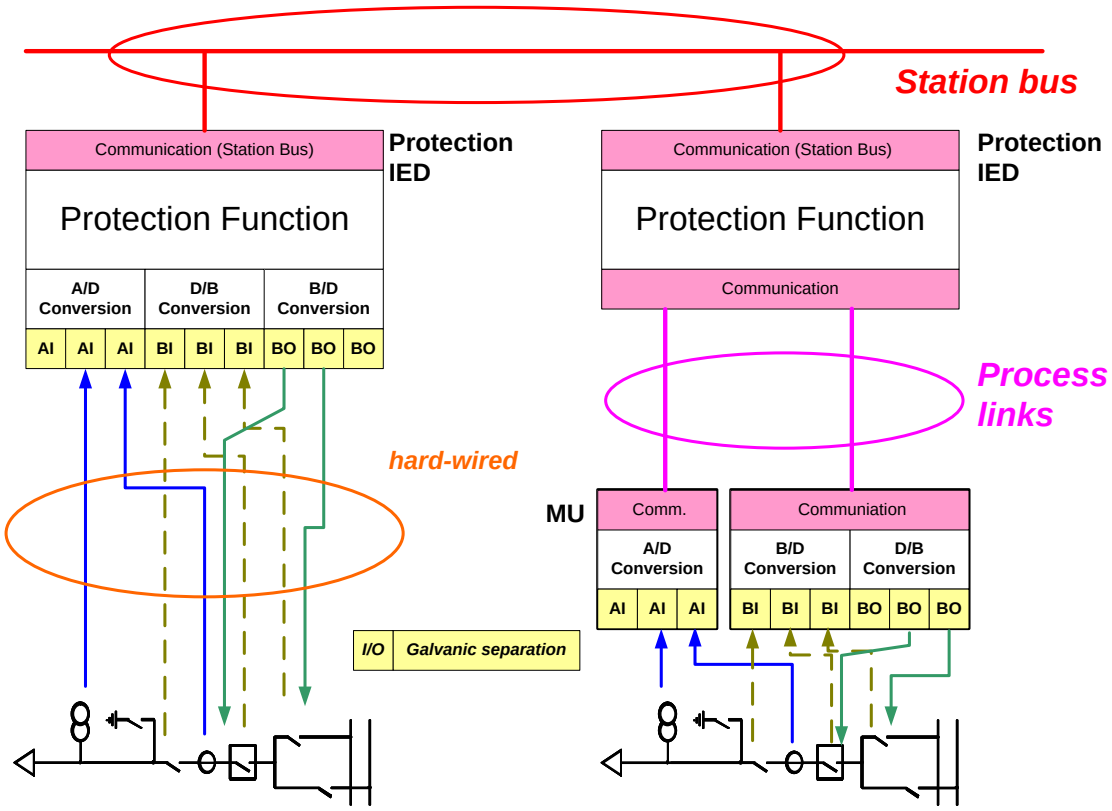

Figure A2 - From Hard Wire To Process Connections

3 Design of IEC 61850 Protocol

Design of IEC 61850 application is based on grouping data into Logical Nodes (LN) and referring to the related functions by name. The LNs are defined in IEC 61850-7-4 ed2.0. Figure A3 shows a basic example of a **protection** IED comprising of a distance protection with three zones (3 instances of LN PDIS); a time overcurrent protection (LN PTOC); the trip matrix (trip conditioning LN PTRC); data models of both of the instrument transformers (one instance both of LN TVTR and LN TCTR per phase); and of the circuit breaker (LN XCBR).

The left hand side of Figure A3 shows the IED hardwired without process bus.

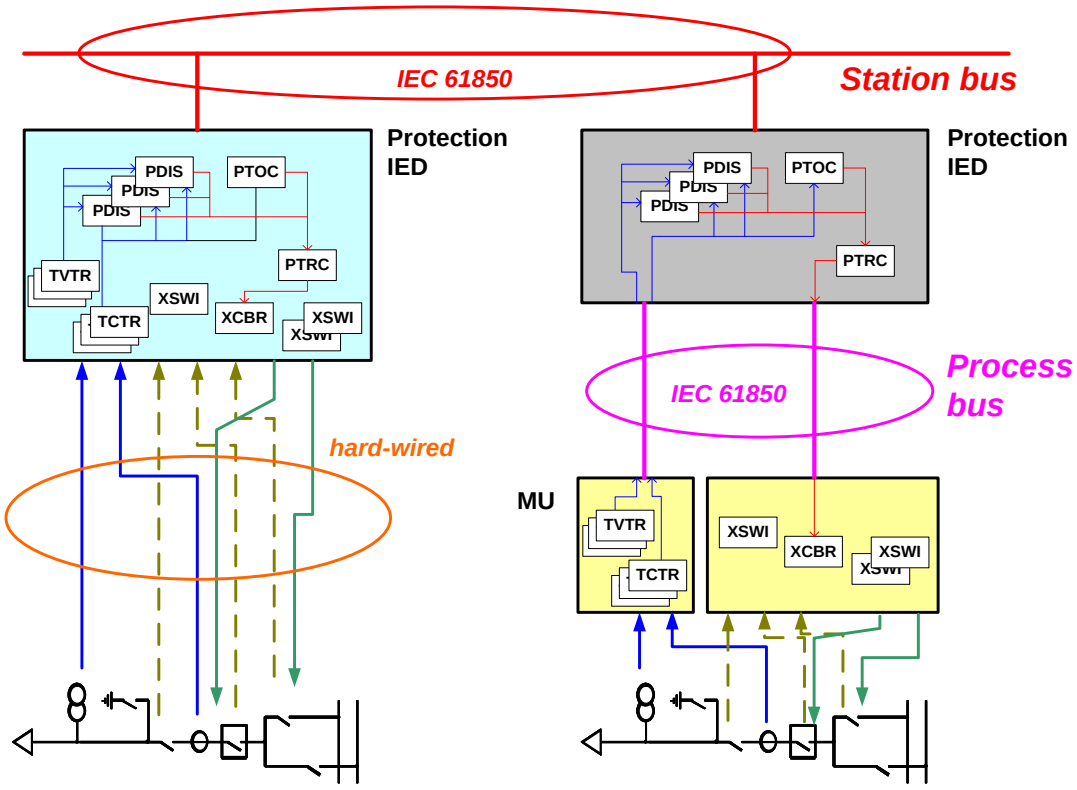

Figure A3 – Design of IEC 61850 Protocol

Figure A4 illustrates the basic principle of a Merging Unit.

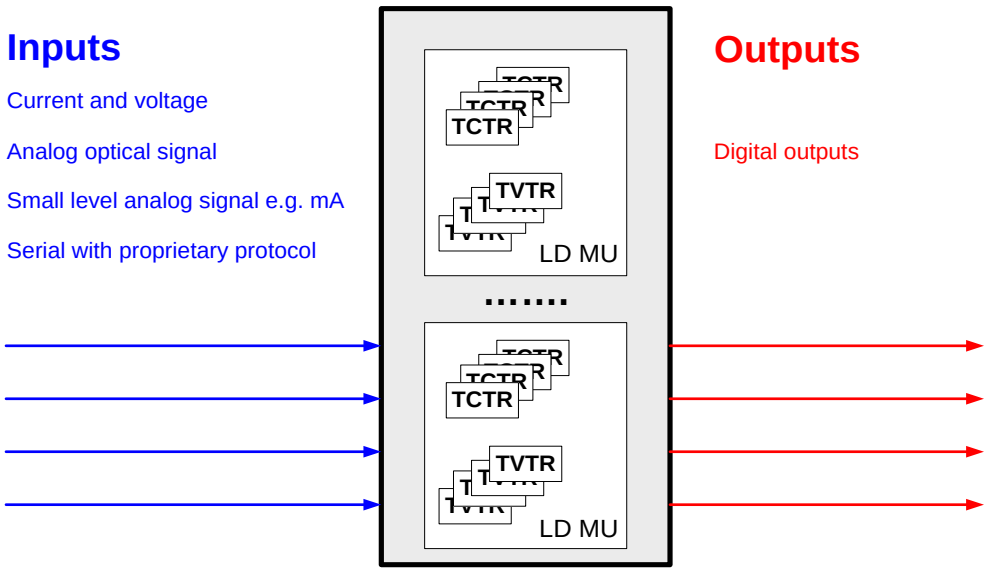

Figure A4 – Merging Unit

Ethernet and process bus architecture
The IEC 61850 standard for “Communication Networks and Systems in Substations” is a LAN based standard. Trips and other signals are passed between **relays** on a substation LAN instead of being hardwired. As these are critical signals for protection system operation, redundancy is applied on the LAN level. Each individual device is supplied with two LAN ports. However, according to the standard, only one of these is active at any point in time. A switch-over to the redundant port takes place only when a communications failure is detected for the main port.

The implementation of IEC 61850 standard benefits from fully redundant System A and System B **protection systems** and redundant communication buses for the majority of **protection** functions. Non-redundant protections are only considered for “distribution systems” (lower voltage levels) and possibly bus **protections**. For the latter cases, the speed requirements for switching over from a failed LAN to the redundant LAN are specified in the standard.

Bus architectures used for IEC 61850
IEC 61850 defines services over the Ethernet but no architecture. The serial links may be realized as a set of point-to-point connections or with switches as Ethernet LAN. Edition 1 specifies no redundant dual ports. Therefore, the Ethernet architecture was realized up to now mostly as a physical ring of switches which is reconfigured according to RSTP (Rapid Spanning Tree Protocol) in case of ring failures.

This reconfiguration is automatic but takes some time involving a few milliseconds per switch. This may be acceptable in case of limited ring sizes. Edition 2 offers in addition standardized dual port redundancy with zero time switch-over both by PRP (**P**arallel **R**edundancy **P**rotocol) and HSR (**H**igh-availability **S**eamless **R**edundancy Protocol). In both cases identical messages are sent out over both redundant ports and the receiver will get both if both communication channels are undisturbed. The message arriving first is processed but the second one will be discarded. There is no time delay also in case if one communication channel fails.

All these structures and recovery procedures may be used as building blocks for any Ethernet system, especially also for station and process Bus configurations according to IEC 61850.

.

Appendix C

Fault Tree Analysis Comparing Probability of Failure for Traditional Protection Design and New Protection Design Using IED 61850 Technology

The new approach to substation design using IED 61850 Technology integrates the substation protection and control functions for all **elements** at a BPS substation. This can be compared to the traditional design where, except for the station battery, each element is protected and controlled by a separate and redundant **protection system**.

The following is a Fault Tree Analysis comparing the probability of loss of protection for the entire Bulk Power System (BPS) station using traditional design vs. 61850 design architecture. Using a station comprised of three lines and a bus as an example, the assumptions used in this analysis are:

1. **Components** that make up the protection system could fail at any instant in time.
2. Both BPS stations are designed using electronic devices.
3. The probability of failure for an electronic device is assigned 0.1.
4. The probability of failure for wiring/cables is assigned 0.01
5. The probability of failure for station dc battery is assigned 0.01.
6. Wiring/cable associated with 61850 design architecture is negligible.

The results of Fault Tree Analysis in Figure A5 and Figure A6 showed that the protection design using 61850 Technology, in the worst case scenario, is significantly more vulnerable to loss of protection for the entire BPS station due to a **component** failure than the traditional design. However, there are other benefits derived from the 61850 design architecture that may override the apparent vulnerability of using 61850 technology. The use of networking allows for the monitoring of all active connections. This affords the owner the ability to immediately detect a failure and take action. Reliability is further improved by having redundancy in substation LANs with rapid spanning tree protocol (RSTP). The objective is to intelligently design the network to meet or exceed currently accepted reliability levels.

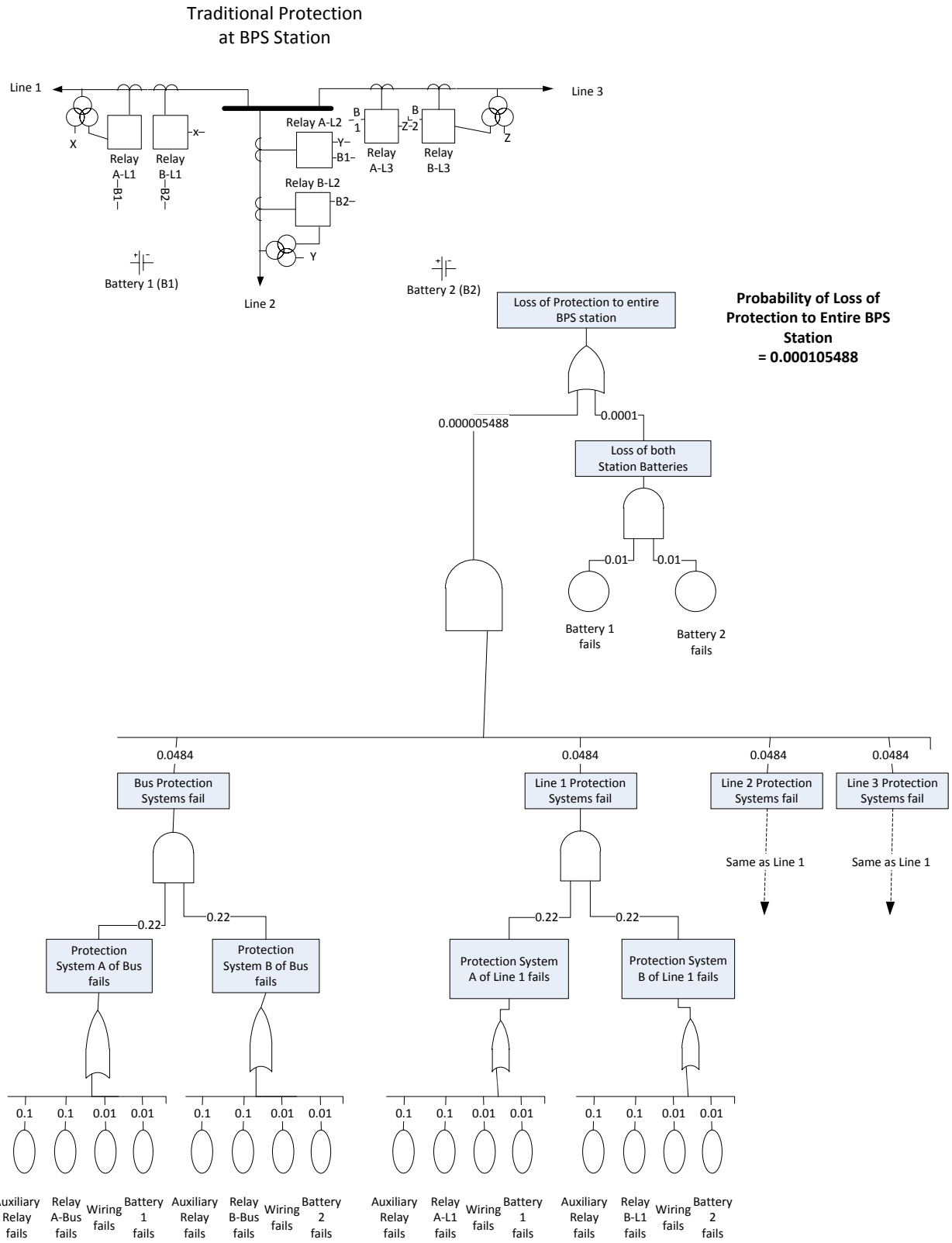

Figure A5 – Fault Tree Analysis for Traditional Protection Design at BPS Station

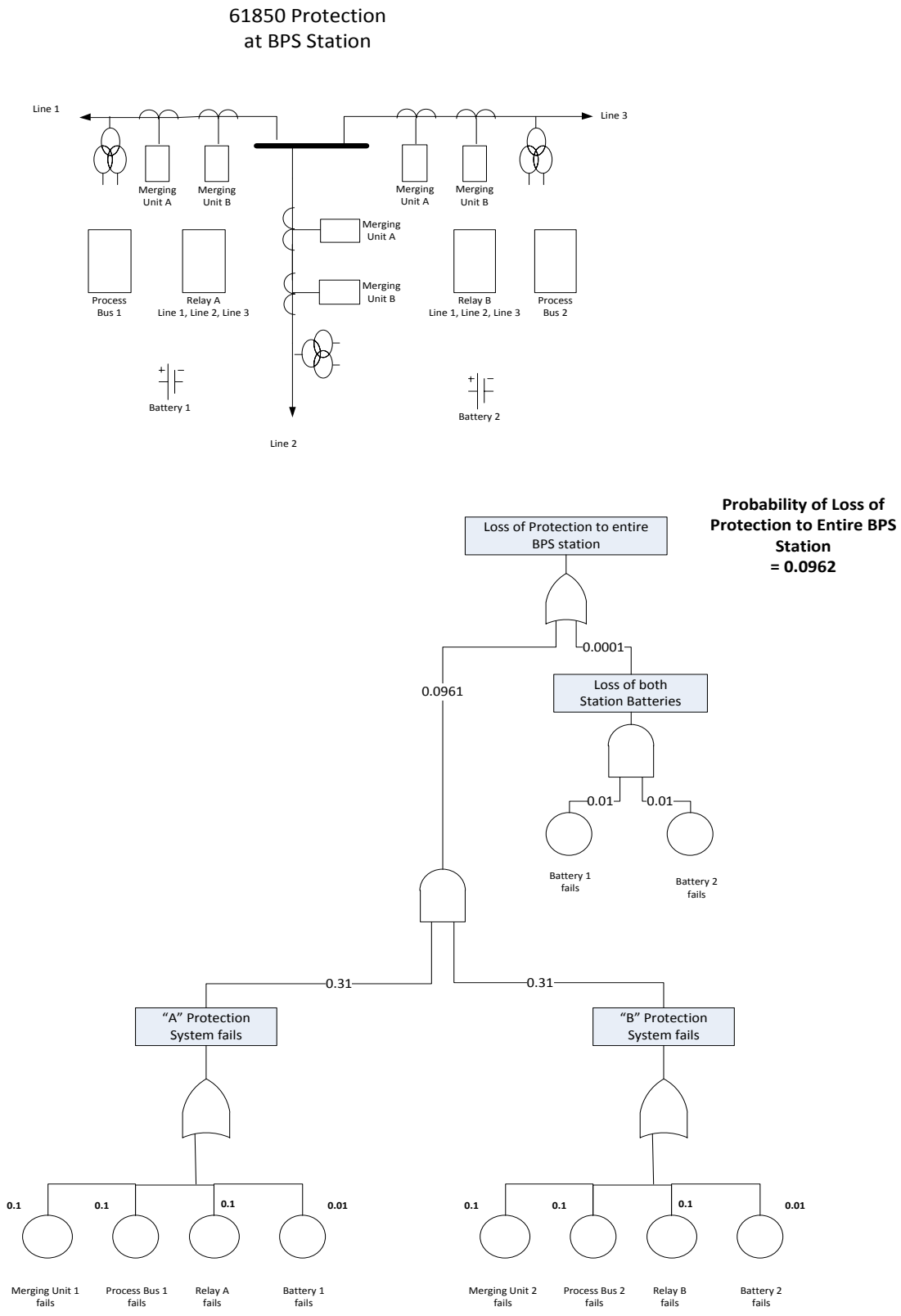

Figure A6 – Fault Tree Analysis for Protection Design Using IED 61850 Technology