UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

ELECTRICAL ENGINEERING

Markku Taikina-aho

REDUNDANT IEC 61850 COMMUNICATION PROTOCOLS IN SUBSTATION AUTOMATION

Master's thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 31st of October, 2011.

Supervisor	Kimmo Kauhaniemi
Evaluator	Erkki Antila
Instructor	Håkan Hultholm

ACKNOWLEDGEMENTS

This Master's thesis was made for ABB Substation Automation Systems located in Vaasa, Finland. It focuses on redundant communication aspects of the standard IEC 61850.

First and foremost, I would like to thank my instructor Håkan Hultholm from ABB for his support and guidance throughout my thesis. I also want to thank my supervisor Kimmo Kauhaniemi from the University of Vaasa for his good advice and Harri Paulasaari from ABB for giving me a very interesting topic for this thesis. I am also grateful to my colleagues in the project department for a great working environment.

Last but not least, I would like to thank my family and especially Pia for their support throughout my studies, and my fellow students for memorable years of study.

Vaasa 31.10.2011

Markku Taikina-aho

TABLE OF CONTENTS **page**

ABBREVIATIONS AND SYMBOLS

$	Separation mark used in MMS protocol
A	Availability
T_L	Fault detection time (RSTP)
T_{PA}	Proposal-Agreement time (RSTP)
$T_{recovery}$	Recovery time of RSTP network in ring topology

ABB	Asea Brown Boveri
ACSI	Abstract Communication Service Interface
ARP	Address Resolution Protocol
BIED	Breaker IED
BPDU	Bridge Protocol Data Unit
BRP	Beacon Redundancy Protocol
CoS	Class of Service
CRP	Cross-network Redundancy Protocol
DANH	Doubly Attached Node implementing HSR
DANP	Doubly Attached Node implementing PRP
DRP	Distributed Redundancy Protocol
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
FCS	Frame Check Sequence
GOOSE	Generic Object Oriented Substation Event
GSE	Generic Substation Event
GSSE	Generic Substation Status Event
GUI	Graphical User Interface
HMI	Human Machine Interface
HSB	Hot Stand-By
HSR	High-availability Seamless Redundancy
I/O	Input/Output
ICMP	Internet Control Message Protocol

IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IRIG-B	Inter-Range Instrumentation Group time code B
ISO	International Organization for Standardization
ITT600	Integrated Testing Toolbox 600 (Analyzer software by ABB)
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LD	Logical Device
LLDP	Link Layer Discovery Protocol
LN	Logical Node
LRE	Link Redundancy Entity
MAC	Media Access Control
MMRP	Multiple MAC Registration Protocol
MMS	Manufacturing Message Specification
MRP	Media Redundancy Protocol
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MU	Merging Unit
NCC	Network Control Center
NIC	Network Interface Card
NTP	Network Time Protocol
OPC	OLE (Object Linking and Embedding) for Process Control
OSI	Open Systems Interconnection
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
QoS	Quality of Service
RCT	Redundancy Control Trailer
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SAN	Singly Attached Node

SCADA	Supervisory Control and Data Acquisition
SCIL	Supervisory Control Implementation Language
SCL	Substation Configuration description Language
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
SV	Sampled Values
TCP/IP	Transmission Control Protocol/Internet Protocol
VDAN	Virtual Doubly Attached Node
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Markku Taikina-aho
Diplomityön nimi: Redundanttiset IEC 61850 tietoliikenneprotokollat sähköasema-automaatiossa
Valvojan nimi: Professori Kimmo Kauhaniemi
Tarkastajan nimi: Professori Erkki Antila
Ohjaajan nimi: Diplomi-insinööri Håkan Hultholm
Tutkinto: Diplomi-insinööri
Koulutusohjelma: Sähkö- ja energiatekniikan koulutusohjelma
Suunta: Sähkötekniikka
Opintojen aloitusvuosi: 2005
Diplomityön valmistumisvuosi: 2011 **Sivumäärä:** 133

TIIVISTELMÄ:

IEC 61850 -standardi on otettu avosylin vastaan sähkövoimajärjestelmäautomaatiossa. Standardin ensimmäinen, vuonna 2005 julkaistu painos ei kuitenkaan kiinnittänyt huomiota sähköaseman tietoliikenneverkon redundanttisiin kommunikaatioratkaisuihin. Myöhemmin julkaistut standardilaajennukset korjasivat tämän epäkohdan ja viittaavat kahteen korkean käytettävyyden redundanssiprotokollaan, jotka löytyvät standardista IEC 62439-3: Parallel Redundancy Protocol (PRP) ja High-availability Seamless Redundancy (HSR). Nämä kaksi protokollaa omaavat saumattoman (0 s.) tietoverkon korjausajan ja täyttävät vaativimmatkin sähköaseman tietoliikenneverkolle asetetut edellytykset.

Tässä diplomityössä on tutkittu näitä kahta redundanssiprotokollaa, niiden käyttöä ja mahdollisuuksia sähköasema-automaatiossa. Työssä on ensin esitelty IEC 61850 ominaisuuksia lyhyesti ja sen jälkeen kerrottu sähköaseman tietoliikenneverkosta, verkkotopologioista sekä tällä hetkellä käytössä olevista redundanssiprotokollista. Tämän jälkeen on tarkasteltu tarkemmin protokollia PRP ja HSR. Työn teoreettista osaa on täydennetty testausosiolla, jossa PRP:n toimintaa on tutkittu ABB:n suojareleillä. Testausosiossa on esitetty yleisiä näkökohtia ja selvitetty mahdollisia ongelmia, jotka on hyvä ottaa huomioon rakennettaessa kyseistä järjestelmää sekä tutkittu, onko ABB:n PRP-implementaatio standardin IEC 62439-3 mukainen.

Tämän diplomityön tavoitteena oli kerätä informaatiota ja kokemusta standardin IEC 62439-3 korkean käytettävyyden redundanssiprotokollista, sillä niitä tullaan vähitellen käyttämään kohdeyrityksen projekteissa. Testaus osoitti, että tämänhetkinen PRP versio on valmis käytettäväksi ABB:n PRP:tä tukevien suojareleiden kanssa. On kuitenkin huomattava, että PRP:stä on esitelty uusi versio, joka tulee vähitellen korvaamaan nykyisen version. Se tuo kuitenkin yhteensopivuuden HSR verkkoihin. HSR:ää ei löydy vielä markkinoilta, mutta sen odotetaan tulevan käyttöön lähitulevaisuudessa.

AVAINSANAT: Sähköasema-automaatio, IEC 61850, IEC 62439, tietoliikenne, redundanttisuus

UNIVERSITY OF VAASA
Faculty of technology
Author: Markku Taikina-aho
Topic of the Thesis: Redundant IEC 61850 communication protocols in substation automation
Supervisor: Professor Kimmo Kauhaniemi
Evaluator: Professor Erkki Antila
Instructor: M.Sc. Håkan Hultholm
Degree: Master of Science in Technology
Degree Programme: Degree Programme in Electrical and Energy Engineering
Major of Subject: Electrical Engineering
Year of Entering the University: 2005
Year of Completing the Thesis: 2011 **Pages:** 133

ABSTRACT:

The standard IEC 61850 has been adopted with open arms by the power system automation market. The first version of the standard published in 2005 did not however pay any attention to redundant communication aspects of the substation automation network. The recent extensions to the standard however corrected this defect and bring redundancy into view, adopting two high availability redundancy protocols from the existing standard IEC 62439-3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). These two protocols provide seamless (0 s.) network recovery times and fulfill even the most demanding requirements for substation automation network.

In this thesis, these two redundancy protocols, their usage and possibilities in substation automation are investigated. At first, the IEC 61850 features, substation communication network topologies, and also the redundancy protocols and methods used today are presented. After this, the protocols PRP and HSR are discussed more deeply. The theoretical part is followed by a test of a system with PRP and ABB devices to give general notes and clarify possible problems when building such a system, and to investigate if the ABB PRP implementation is accordant with the standard IEC 62439-3.

The objective of this thesis was to bring information and early experience about the two high-availability redundancy protocols, as they will be gradually introduced in the projects of the target company. The test confirmed that the current PRP version is ready to be used with the few ABB substation automation products that support it at the moment. However, a new version of PRP has been introduced and it will gradually replace the present version, bringing compatibility with HSR networks. HSR is not yet found on the market, but is expected to come to use in the very near future.

KEYWORDS: Substation automation, IEC 61850, IEC 62439, communication, redundancy

1 INTRODUCTION

Functional substation automation is the backbone for a reliable and efficient power system infrastructure. It is needed for controlling, protecting and monitoring a substation. Substations are one of the most important components of the power grid, providing interconnection between power generation and end consumers through transmission and distribution networks.

The rapid development of intelligent electronic devices (IED) and communication technology, growth of data amount, and interoperability between devices of different manufacturers have all brought stricter requirements for the communication inside a substation. The standard 'IEC 61850 – Communication networks and systems in substations' standardizes the communication inside a substation while taking these requirements into account. It defines communication in electrical substation automation systems as well as between them. The implementation of the standard IEC 61850 has been rapid; it is becoming the preferred communication protocol in substation automation solutions.

The reliability of the communication plays a great role in making the substation automation system operate properly. To make the system operation reliable and to increase availability, a redundancy method has to be used. Redundancy means spare or duplicate functionality, which allows the system to continue to operate without any loss of performance and availability during failure. The present solutions use Ethernet switches that reconfigure the network during failure, relying mostly on Rapid Spanning Tree Protocol (RSTP). However, the standard 'IEC 62439 – Industrial communication networks – High availability automation networks' presents two redundancy protocols that handle the redundancy in the end nodes with two different networks, achieving seamless recovery time. These protocols are called Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). These two protocols are now included in the IEC 61850 standard and are potential redundancy solutions to be used in substation automation systems that require high availability.

1.1 Scope of study

The objective of this Master's thesis is to investigate redundant IEC 61850 communication aspects, especially the highly available network protocols PRP and HSR included in the IEC 62439 standard. The use of these two protocols in substation automation with IEC 61850 is clarified and some comparisons to existing redundancy methods are done. In addition, most common substation communication network topologies are presented, along with today's basic redundancy protocols. A test network with PRP is made and the communication is analyzed with network analyzer software. The material is mainly based on scientific articles and the standards IEC 61850 and IEC 62439. The redundancy is handled only on communication protocol and media level.

This thesis is made for ABB's Substation Automation Systems -product group, which supplies automation systems for substations as well as for other industry and utility processes. The typical project of this product group consists of designing, building and commissioning an automation system which includes supervisory control and data acquisition (SCADA) software to monitor and control the process.

1.2 Structure of the thesis

This thesis consists of 7 chapters altogether. After the introduction presented in this chapter, the second chapter gives some basic information about the standard IEC 61850 and its communication features used in power distribution systems. The third chapter focuses generally on substation communication network and reliability aspects, also presenting the most common network topologies used in substations. The fourth chapter clarifies redundancy protocols and methods that the present substation applications use. In the fifth chapter, the redundancy protocols adopted by IEC 61850 (Parallel Redundancy Protocol and High-availability Seamless Redundancy) are presented and discussed, currently standardized in the standard IEC 62439 part 3. The test application of PRP is demonstrated in Chapter 6 along with measurements and results. Finally, the conclusions of this thesis are drawn in the Chapter 7.

2 IEC 61850 STANDARD

The standard 'IEC 61850 – Communication networks and systems in substations' is a global standard compiled by IEC (International Electrotechnical Commission). The first edition of the standard consists of ten sections altogether, the last of which was published in 2005. Some of the sections are divided into smaller parts. The parts of the of the standard are presented in Table 1 below.

Table 1. Parts of the standard IEC 61850. (IEC 61850-1 2003: 5).

Part	Title
1	Introduction and overview
2	Glossary
3	General requirements
4	System and project management
5	Communication requirements for functions and device models
6	Configuration description language for communication in electrical substations related to IEDs
(7)	Basic communication structure for substation and feeder equipment
7.1	Principles and models
7.2	Abstract communication service interface (ACSI)
7.3	Common data classes
7.4	Compatible logical node classes and data classes
(8)	Specific communication service mapping (SCSM)
8.1	Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
(9)	Specific communication service mapping (SCSM)
9.1	Sampled values over serial unidirectional multidrop point to point link
9.2	Sampled values over ISO/IEC 8802-3
10	Conformance testing

Part 1 gives the reader the introduction and overview of the IEC 61850 and part 2 includes only the glossary of terms. Part 3 gives the requirements for quality (reliability, maintainability etc.), specifies environmental conditions and references to other standards and specifications. Part 4 gives information about engineering requirements, system lifecycle aspects and quality assurance needed in system and project

management. Part 5 specifies the performance requirements for all different functions performed in substation automation system as well as for device models. It also gives a basic approach for logical nodes. Part 6 introduces the XML-based (Extensible Markup Language) Substation Configuration description Language (SCL) and IED configuration exchange between IEDs and engineering tools.

Part 7 is an important part including an overview of communication principles and models, describing relationships between other parts of whole IEC 61850 as well as interoperability obtaining. It also gives information about ACSI (Abstract Communication Service Interface) and its services, describes common data classes and related attributes and gives definitions of data classes and logical node classes. Parts 8 and 9 define mappings of services used for communication inside a substation and for transmission of sampled analogue values, while part 10 defines the testing for conformance. The standard has been extended and updated after its publication. The extensions of the standard are discussed in Chapter 2.3. (IEC 61850-1 2003: 23–25; IEC 61850-5 2003: 8–9; IEC 61850-7-1 2003: 9; Sidhu & Gangadharan 2005).

2.1 Objectives of the standard

The scope of the standard in brief is to support the communication of all functions performed in a substation. There are three main objectives for the standard which were taken into account by the standardization group and that were described as the most crucial requirements of the market (ABB 2010: 8; De Mesmaeker, Rietmann, Brand & Reinhardt 2005):

- **Interoperability**, which means the ability for IEDs to exchange information and use it for their own functions in real time, without need of protocol converters. Interoperability is required for IEDs from different manufacturers as well as for different versions of the same manufacturer. Interoperability has to support functions (protection, control, automation, monitoring, self supervision etc.) that are executed by IED software.

- **Free architecture**, which means support for centralized (e.g. Remote Terminal Unit, RTU) and decentralized system architectures. Because the standard is global, it has to support different operation philosophies around the world.
- **Long-term stability**, which means that the standard is future-proof, not getting obsolete in the future as technologies develop. This is required from substation devices as well as from technologies that are used in a typical substation.

The use of IEC 61850 is advantageous compared to legacy protocols due to objectives mentioned above, but also bringing cost benefits in the area of system design, commissioning and operation.

2.2 Communication features of the standard

The most important communication features of the standard IEC 61850 are described in this chapter. The basic communication technology in IEC 61850 is Ethernet with a speed of 100 Mbit/s at the IEDs. (ABB Oy 2010a: 11)

What makes IEC 61850 unique from the legacy protocols is the fact that IEC 61850 provides a model how data should be organized in a uniform way in every power system device. Older protocols have only defined how the data is transmitted on the wire, thus leaving the engineers to manually configure objects and map them to index numbers, register numbers or other power system variables. IEC 61850 reduces this configuration effort dramatically.

The other major approach that IEC 61850 takes is the separation of the domain related model for both data and communication services from the protocols. It can be said that data items and services are “abstracted” and are independent of the underlying protocols. The data objects and services are mapped to a protocol that meets the data and service requirements according to the standard. Because the development in the communication technology is quicker than the requirements in the field of substation automation, this separation enables the standard to be future-proof. Figure 1 shows the principle of this separation. (ABB 2010: 8–9; Mackiewicz 2006).

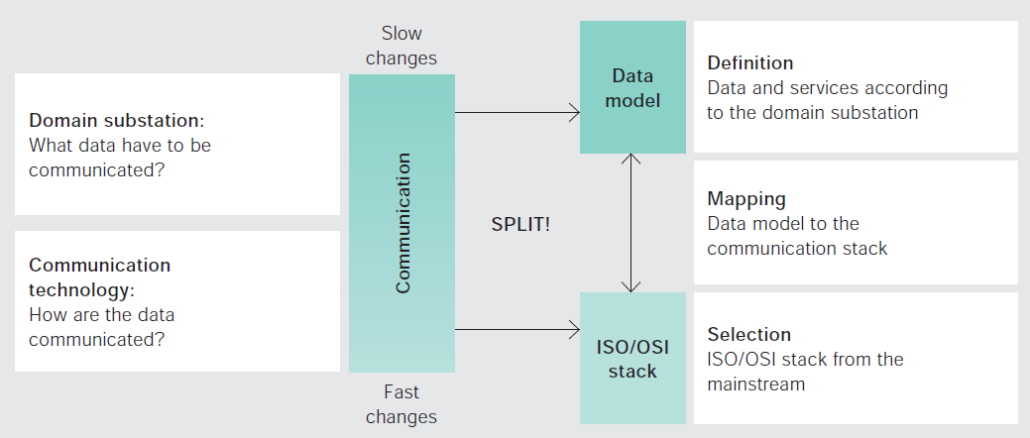


Figure 1. The separation between data model and communication stack. (ABB Oy 2010a: 9).

The standard is based on virtualization, which provides a view of real device and its aspects that are used for information exchange with other devices. The logical nodes in a logical device represent the functions of real devices, thus providing an image of the analogue world to the substation automation system. (IEC 61850-7-1 2003: 15).

2.2.1 Data model

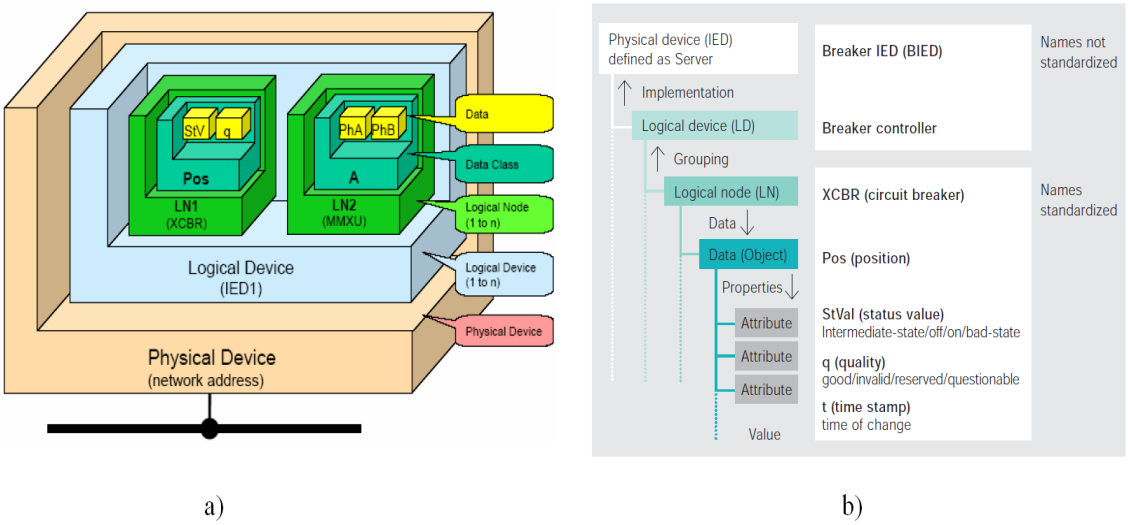
The data model begins with the physical device, which is the device that is connected to the network with a network address (e.g. IED). Each physical device includes one or more logical devices, which are used to classify similar functions into different entities in the physical device. The physical device itself acts as a gateway for logical devices in it. Each logical device contains logical nodes (LN). (Mackiewicz 2006).

For example, an ABB 615 Relion® series IED consists of three logical devices: CTRL (Control logical device), DR (Disturbance recorder logical device) and LD0 (Protection logical device), which includes also physical functionalities like inputs and outputs and the alarm LEDs (ABB Oy 2010b: 15).

The approach of the standard is to break down all application functions into the smallest pieces that are used to exchange information and that can be implemented separately in dedicated IEDs. These entities are called logical nodes, which are virtual representations

of the real power system functions (for example, logical node XCBR represents circuit breaker). Nevertheless, the functions in the substation are not standardized, only the logical nodes and interaction between them is standardized as the main goal is interoperability. In addition, a logical node, based to its functionality, contains a list of data (e.g. position) which can be mandatory, optional or conditional. The data objects contain data attributes (e.g. status value, time stamp). (ABB Oy 2010a: 9; IEC 61850-5 2003: 9, 25; IEC 61850-7-1 2003: 15; Mackiewicz 2006).

Figure 2 represents the data model in the form of container (a) and hierarchical tree (b). Briefly, logical devices are a composition of logical nodes while logical nodes and the data are the main concepts that describe real system and their functions. (IEC 61850-7-1 2003: 46–47).



a) b)

Figure 2. Data model of IEC 61850. (Gupta 2008; ABB Oy 2010a: 10).

The data model is a virtualized model providing an abstract view of the device and its objects. This model is then mapped to a protocol stack based on MMS (Manufacturing Message Specification), TCP/IP and Ethernet in the part 61850-8-1. The mapping process transforms the model information into a MMS variable object, providing an effortless way to refer to the individual data. MMS is a protocol originally designed for manufacturing but it was chosen into IEC 61850 because it is the only public protocol (ISO standard) that supports the complex naming and service models of IEC 61850.

Every object has its place in the information tree (see Figure 2). Figure 3 shows the anatomy of the object name. The first part of the object name is the logical device name, which can be named freely (Relay1). The second part defines the logical node where the object is. In the figure, the object belongs to switchgear (X) and is circuit breaker one (CBR1). Logical nodes can be added with reference number to indentify nodes, for example XCBR1 from XCBR2. Also a prefix can be added. The separation mark '$' is needed for mapping over MMS-protocol. The logical node is followed by functional constraint, which groups the data into categories by their information type. After that comes the data part. In the figure, Loc defines the operation mode of the circuit breaker (local or remote) and stVal contains the status value. (ABB Oy 2010a: 10; Mackiewicz 2006; IEC 61850-7-1 2003: 44, 79).

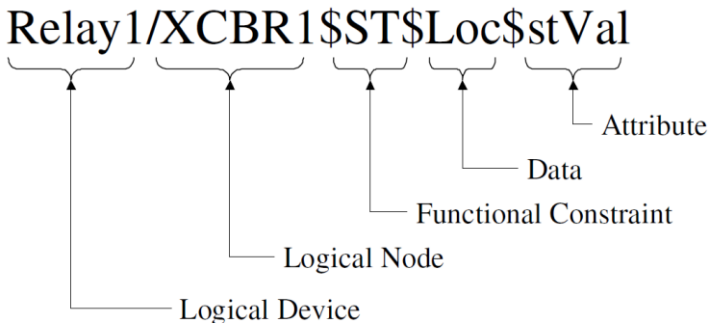


Figure 3. Object name of IEC 61850-8-1. (Mackiewicz 2006).

Every logical node is a grouping of data and associated services with name and relation to a power system function. The names of LNs begin with a letter that represents the group in which the LN belongs. There are logical nodes for switchgear that all begin with the letter "X" for example. Altogether, there are about 90 LNs defined, which cover the most common functionalities of substation and feeder equipment. The protection and protection related functions have been one main focus with 38 logical nodes. Table 2 shows the logical node groups and the number of nodes in them. (IEC 61850-7-1 2003: 16; Mackiewicz 2006).

Table 2. Logical node groups. (IEC 61850-7-1 2003: 16; Mackiewicz 2006).

Group Indicator	Logical node groups	Number
A	Automatic control	4
C	Supervisory control	5
G	Generic references	3
I	Interfacing and archiving	4
L	System logical nodes	3
M	Metering and measurement	8
P	Protection functions	28
R	Protection related functions	10
S	Sensors and monitoring	4
T	Instrument transformer	2
X	Switchgear	2
Y	Power transformer	4
Z	Further power system equipment	15
	Total number of logical nodes	**92**

Logical devices, logical nodes and data objects are all virtual terms, representing the real data used for communication. A device communicates only with the logical nodes or its data objects of another device. The real data represented by logical node is not directly accessible, which has the advantage that information modeling and communication does not depend on operating systems, storage systems or programming languages. (IEC 61850-7-1 2003: 9, 15, 57).

2.2.2 Communication schemes and data model mapping

IEC 61850 has adopted mainstream technology for the communication, which is based on the ISO/OSI-model (International Organization for Standardization/Open Systems Interconnection). The model presents the communication functions in seven layers that are: Application (layer 7), Presentation (layer 6), Session (layer 5), Transport (layer 4), Network (layer 3), Data-link (layer 2) and Physical layer (layer 1). Furthermore, the OSI model can be divided to two profiles: Application profile (layers 5–7) and transport profile (layers 1–4). The communication protocols that IEC 61850 uses are MMS (Manufacturing Message Specification) mapped on layers 5–7, TCP/IP (Transmission Control Protocol/Internet Protocol) mapped on layers 3–4 and Ethernet that is mapped on layers 1–2. Figure 4 shows the OSI reference model. (ABB Oy 2010a:11; IEC 61850-8-1 2004: 21–22).

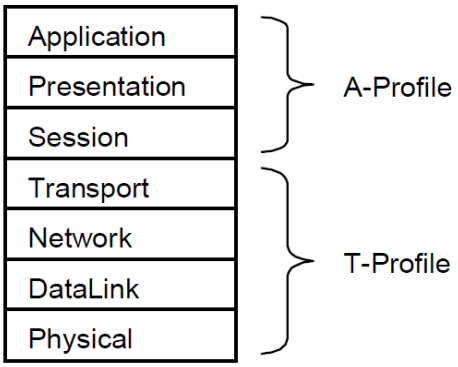


Figure 4. ISO-OSI reference model with profiles. (IEC 61850-8-1 2004: 21).

IEC 61850 offers three kinds of communication schemes and services. These are:

- Client-Server communication
- GOOSE messages
- Sampled Values

In Client-Server communication, the client request data from the server that offers it. The client may also receive report indications from the server (IEC 61850-7-1 2003: 55). In substation automation system, this kind communication is used for transferring quite large amounts of information (can run to kilobits or megabits) and the communication happens vertically, e.g. between station level and bay level devices. This data is not time critical; it can be for example information exchange like fault record or event record etc. It uses the full OSI-model (MMS over TCP) with reliable data transfer.

GOOSE (Generic Object Oriented Substation Event) messages are used for fast horizontal communication between IEDs. These messages are time-critical, including data like trip or interlocking commands, for achieving sufficient protection and control schemes. GOOSE messages are transmitted over Local Area Network (LAN) as a multicast, and the initiation for data transmission is executed only on occurrence of the event.

Sampled Values are also time-critical data. They are messages for instrumentation and measurement like sampled values of current or voltage signals from IEDs or non-conventional instrument transformers. Sampled values are continuous stream of data, the size of which is defined by sampling resolution. These messages can be sent either as unicast (to one receiver) or as multicast (several receivers). (ABB Oy 2010a: 35, 54; De Mesmaeker et al. 2005; Goraj 2010a: 30; IEC 61850-7-1 2003: 41).

Because of the approach that IEC 61580 takes, separating the data model and services from underlying protocols (i.e. using abstract models), the standard uses the concept of ACSI (Abstract Communication Service Interface). IEC 61850 defines a set of abstract services to be used between applications, allowing compatible information exchange between substation devices. ACSI provides a communication interface for these communication services, which define mechanisms for reading and writing object values and for other operations like device control. However, the abstract model needs to be operated over real protocols that are practical to implement and can operate in the power industry computing environments. IEC 61850-1 2003: 7, 18–19; IEC 61850-7-1 2003: 49, Mackiewicz 2006).

Figure 5 shows the mapping of data model and services in IEC 61850. The object model and its services are mapped to the application layer for MMS. GOOSE messages and sampled values are time-critical and thus mapped straight to the Ethernet link layer.

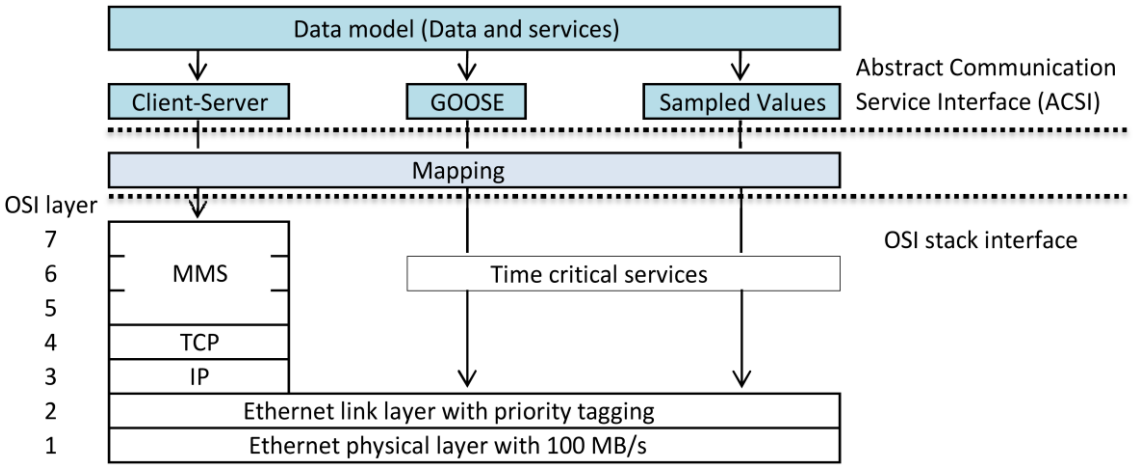


Figure 5. Mapping of data model and services. (ABB Oy 2010a: 11; Brand 2004).

The mappings are defined in IEC 61850-8-1 (Client-Server and GOOSE communication) and in IEC 61850-9-1 and IEC 61850-9-2 (Sampled Values). (ABB Oy 2010a: 11; IEC 61850-7-1 2003: 65; Mackiewicz 2006).

2.2.3 GOOSE and Sampled Values

IEC 61850 presents two real-time communication methods that can be used successfully in protection engineering: Generic Substation Event (GSE) and Sampled Values (SV) messaging. GSE messages are divided into two types: Generic Substation Status Event (GSSE) and to Generic Object Oriented Substation Status Event (GOOSE). The main difference between GSSE and GOOSE is the fact that GSSE is an older message type, which only supports data in form of binary-only. GOOSE is more flexible, supporting both analog and binary data. All new substation automation systems use GOOSE only instead of GSSE for horizontal communication. GSSE and GOOSE can both exist in a system, but are not compatible with each other.

GOOSE, as mentioned before, is described as rapid horizontal communication between IEDs. GOOSE messages are mapped straight to Ethernet layer (layer 2), thus providing fast transmission of time-critical data. The messages are transmitted over LAN as a multicast, so the same substation event message is delivered simultaneously to multiple IEDs. The IEDs that are configured to receive the message can subscribe it.

However, due to nature of the multicast and the design of the Ethernet, the messages are connectionless. This means that we cannot know which IEDs will receive the message, the message delivery is not ensured, and the acknowledgement of the successful receiving of the message is not sent by the IED. Because of this, IEC 61850 specifies a retransmission scheme, which increases the probability of successful reception in all subscribing IEDs. Furthermore, GOOSE uses periodic heartbeat messages to enable detection of link or device failure.

Figure 6 shows the example of GOOSE message transmission scheme. In the figure, T0 is the time between the heartbeat messages. As an event happens, a burst of messages is

transmitted, with gradually increasing time (T1–T3). Eventually, the time is settled back to T0. (Hou & Dolezilek 2008; Goraj 2010a: 30–32).

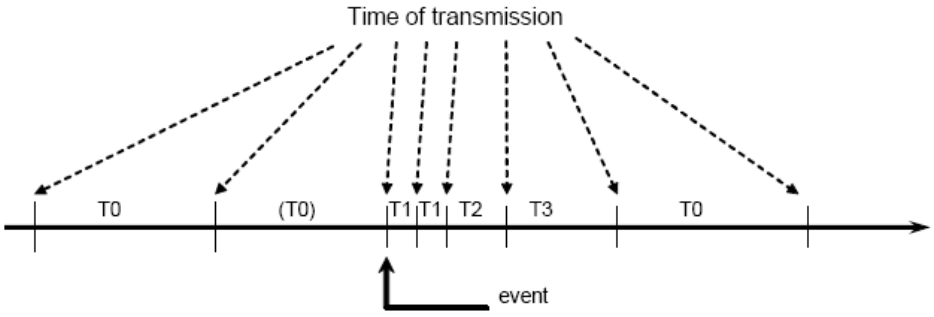


Figure 6. GOOSE retransmission scheme during an event. (Hou & Dolezilek 2008).

An interesting detail is that the signal exchange between bay level devices is not actually a new feature brought by IEC 61850. The legacy LON protocol already had a support for bay level devices to communicate with each other, for example interlocking and blocking signals between protection relays. (ABB Oy 2006: 3).

The digital information exchange between IEDs and next generation voltage and current sensors is becoming possible. IEC 61850 defines Sampled Values (SV) for this purpose. Sampled Values are also mapped to the Ethernet layer (layer 2) being time-critical data. SV messages are used for transferring digitalized measurement values of current and voltage from switchyard to IEDs inside substation. The data collection (from current and voltage sensors) and digitization is made by a Merging Unit (MU), which sample the signals at an appropriate, synchronized rate. Like GOOSE messages, SV messages are also transmitted via LAN as multicast to any number of subscribing IEDs in the Ethernet network.

There is an implementation agreement at the moment called IEC 61850-9-2LE (Light Edition), defining the base sample rates of the MUs. A sample rate of 80 samples per power system cycle (1/50 Hz) is used for basic protection and monitoring, while higher rate of 256 samples per cycle is used for high-frequency applications (e.g. power quality or high-resolution oscillography). Depending on the sample rate and the number of

MUs, a switch with speed of 100 Mbit/s or 1 Gbit/s is needed for process level communication. The process bus is discussed in Chapter 2.2.5.

The sampled value streams that Merging Units generate must be synchronized in time with accuracy of a few microseconds. This is because IEDs use sampled values for protection, and they need to be in chronological order. Time synchronization in IEC 61850 is discussed more detailed in the next section. (Goraj 2010a: 34–35; Hou & Dolezilek 2008; Mackiewicz 2006).

2.2.4 Time synchronization

In order to properly analyze the events and other data (e.g. post-fault data) in the substation automation system, events need an accurate time stamp (i.e. they need to be synchronized). Time synchronization is used for synchronizing all devices within the system. The time source is usually external (satellite or radio clock). IEC 61850 presents five different requirement levels of time accuracy for time synchronization, ranging from 1 millisecond to 1 microsecond against real time. It also presents the protocol SNTP (Simple Network Time Protocol) for time synchronization accomplished via LAN communication. (ABB Oy 2010a: 10; IEC 61850-5 2003: 48–49, 81; IEC 61850-8-1 2004: 89).

SNTP is, as its name states, a simpler modification of NTP (Network Time Protocol). These two protocols differ in the areas of error checking and time correction. In addition, the SNTP uses only one time server at a time, while NTP uses multiple ones. They both provide synchronization over LAN. With SNTP, the system is capable to reach time accuracy of 1 millisecond. However, this is not precise enough for Sampled Values (of voltages and currents) needed for protection, which require an accuracy of 1 microsecond. Therefore, more precise time synchronization methods must be used. There are two protocols that are capable of bringing higher accuracies: IRIG-B and PTP (Precision Time Protocol). (ABB Oy 2010a: 10; Spectracom 2004).

IRIG-B (Inter-Range Instrumentation Group time code B) can reach an accuracy of one microsecond. It is simple to implement and is supported widely in devices. However, it

has a drawback; it needs a separate cabling from data network for all devices that require time sync. IRIG-B is widely used in today's applications that require microsecond accuracies.

The IEEE (Institute of Electrical and Electronics Engineers) standard IEEE 1588 presents the Precision Time Protocol (PTP), which reaches accuracies of sub microseconds. PTP is very much like SNTP synchronizing time over LAN, but in addition it allows hardware assisted time stamping. A time stamp is added to the packet coming in the device and a correction is done when packet leaves the device. This allows high precision of time synchronization. On the other hand, devices need hardware implementation to support PTP.

PTP was originally specified in the standard IEEE 1588-2002, followed by IEEE 1588 version 2 in 2008 (PTPv2). PTP is advantageous to use in substations, because it eliminates the separate cabling of IRIG-B, achieves required accuracies in both event timing and critical applications like Sampled Values and eases the deployment of precision time networks in modern Ethernet-based substations. PTP is expected to be adopted by IEC 61850. (Moore 2009; Goraj 2010b: 3–4, 13, 29).

Currently, switch manufacturers (RuggedCom, Moxa etc.) have some switches that support PTPv2, and GPS manufacturers (e.g. Meinberg) support it already. ABB IEDs will support it in the future, beginning from the transmission relays (Relion® 670 series). There is no need to have accuracy of one microsecond in small substation today; it is needed when Sampled Values come into use. (ABB DA Online Support 2011).

2.2.5 Substation automation system interfaces and levels

The functions of a substation automation system refer to the tasks that are performed in a substation, e.g. control, monitor and protection of the substation and its feeders. Furthermore, there are functions needed for maintaining the system. In IEC 61850, the functions are assigned into three different levels: station level, bay/unit level and process level. Figure 7 shows these levels as well as logical interfaces (1–10) between them. The logical interfaces are explained in Table 3.

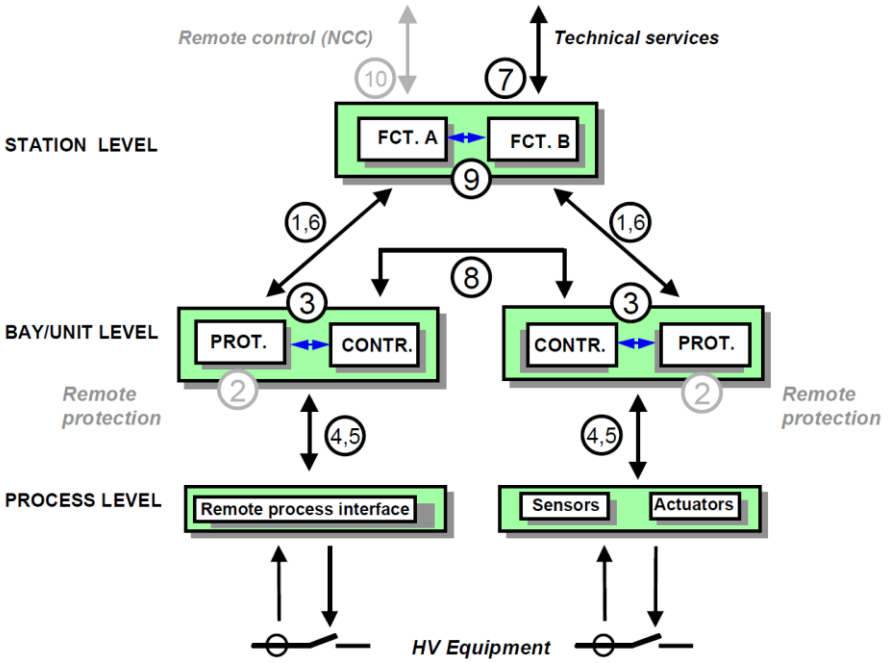


Figure 7. Substation automation system levels and interfaces. (IEC 61850-5 2003: 15).

Interfaces 2 and 10 are outside the scope of the first edition of IEC 61850 and thus marked with grey color in Figure 7.

However, an extension to the standard (IEC 61850-90-1) defines the use of IEC 61850 between substations, and another extension (IEC 61850-90-2) is under preparation to define IEC 61850 communication between substations and remote control centers (IEC 61850-90-2 2010: 7).

Table 3. The interfaces of substation automation system. (IEC 61850-5 2003: 15).

Interface	Meaning
1	Protection-data exchange between bay and station level
2	Protection-data exchange between bay level and remote protection
3	Data exchange within bay level
4	CT and VT instantaneous data exchange (especially samples) between process and bay level
5	Control-data exchange between process and bay level
6	Control-data exchange between bay and station level
7	Data exchange between substation (level) and a remote engineer's workplace
8	Direct data exchange between the bays especially for fast functions such as interlocking
9	Data exchange within station level
10	Control-data exchange between substation (devices) and a remote control center

Process level functions include every function that is interfacing the process itself. They communicate via interfaces 4 and 5 to the bay level. The devices in the process level typically consist of remote process interfaces like intelligent sensors and actuators or I/Os (Input/Output).

Bay level functions mainly use the data of one bay and act on the primary equipment of the bay. The communication within bay level is done via interface 3 while communication to the process level uses interfaces 4 and 5. Control, protection and monitoring units are categorized as bay level devices.

Station level functions can be divided into two classes: process related station level functions and interface related station level functions. The former ones use the data of more than one bay or whole substation and act on the primary equipment of more than one bay or whole substation, communicating via interface 8. The latter ones are functions that enable the interface of the substation automation system to the local station operator HMI (Human Machine Interface) and to remote control center among others. The communication is done via interfaces 1 and 6 with the bay level, via interface 7 and via interface 10 (remote control interface to outside world). The devices in the station level include station computer, operator's workplace as well as interfaces to remote communication.

The interfaces can be used to define two important bus systems or LANs: station bus and process bus. Station bus connects station level with bay level as well as different bay IEDs with each other and is thus combined with interfaces 1, 6, 3, 8 and 9. Process bus connects bay level with process level and its different IEDs with each other, combined with interfaces 4 and 5. Depending on the application, it can also use interface 8. (IEC 61850-5 2003: 14–16).

The station bus connects all bays with station level, carrying information e.g. measurement, interlocking and operation. It has several benefits like GOOSE messages that use Ethernet network, thus reducing the traditional copper wiring.

The process bus is needed for sending sampled values from electronic instrument transformers to protection and control relays, and it also allows connection of intelligent switchgear (circuit breakers, disconnectors etc.). From the past to today, applications have used process interface hardwired to control and protection devices. These wires are used to communicate with the process: to get position indications from switchgear and analogue signals from current and voltage transformers. However, the process bus takes a step further, providing a digital link to switchgear and instrument transformers and thus reducing the copper wiring within the switchyard. Briefly, it replaces the copper wires with communication bus. Figure 8 shows a common example of substation automation system architecture using station and process bus and the three levels. In the picture, the rightmost process interface is hardwired to control and protection devices as made traditionally, while other process interfaces use IEC 61850 Process bus. (McGhee & Goraj & Moore 2010; Andersson & Brand 2000; Brunner 2010).

Because the process bus is used to transfer continuous sampled values from the primary process, it has a significant requirement on the bandwidth. The process bus will use fiber optic cables. (ABB Oy 2010a: 35).

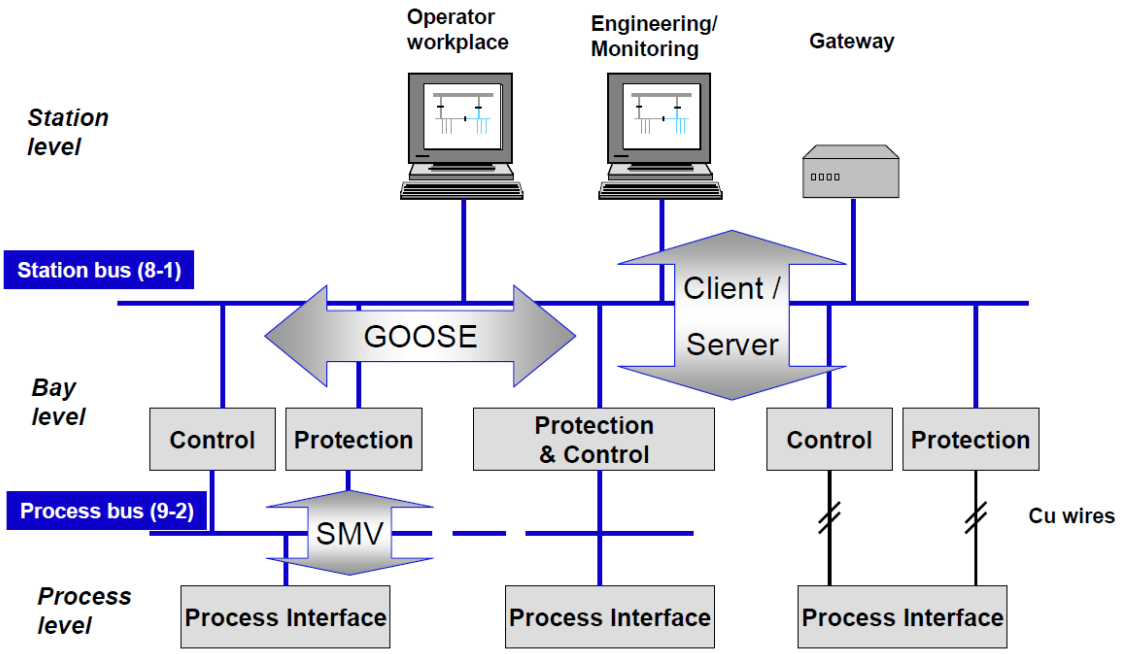


Figure 8. An example of substation system architecture. (Schnakofsky 2011: 16).

The merging unit (MU) is a key element in the process bus, converting the voltages and currents of instrument transformers to an IEC 61850 messages and makes them available on the process bus. Switchgear can be connected to the process bus e.g. with distributed remote I/O units that use IEC 61850 communication. This interface is often called as breaker IED or BIED. The process bus thus carries current and voltage samples along with switch positions, commands, protection trips etc. between primary and secondary equipment. A trip signal can be transmitted from the protection relay to the circuit breaker e.g. using GOOSE messages. Figure 9 shows an example of the usage MU and BIED in the process level with Ethernet switch, thus forming and IEC 61850-9-2 based process bus. (ABB Oy 2010a: 48–49; Brunner 2010).

The exchange of information between process equipment and substation automation has high requirements for the real time behavior, especially in the area regarding protection: sampled values from instrument transformers to the protection relay and trip signal from the relay to the circuit breaker. This requires high-precise time synchronization. (Brunner 2010).

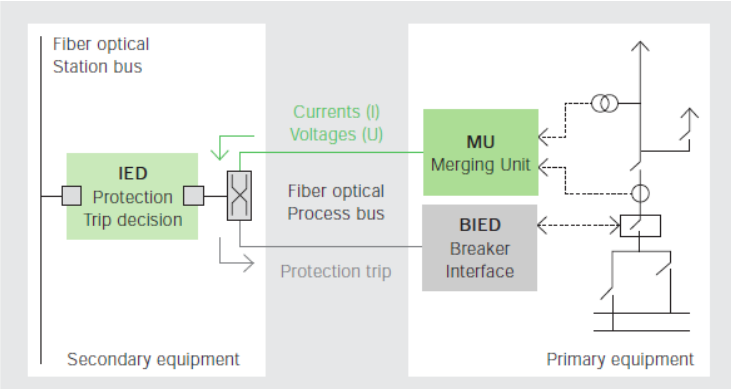


Figure 9. The usage of MU and BIED on the process bus, connected by an Ethernet switch. (ABB Oy 2010a: 50).

There are still very few real substations with digital IEC 61850 process bus. Manufacturers have already offered MUs as pilot products, but BIEDs are still rare. The high-precise time synchronization (1 µs) has been also a major challenge to this date. As a matter of fact, the IEC 61850 edition 1 did not specify the time synchronization for the microsecond requiring sampled values on the process bus. Therefore, user organization

UCA International defined an implementation agreement called IEC 61850-9-2LE, defining the formerly mentioned MU sample rates and time synchronization by pulse per second (1PPS), which requires a separate synchronization network. IEEE 1588 is expected to replace 1PPS, providing high accurate time synchronization over Ethernet and removing the separate synchronization network. (ABB Oy 2010a: 48–49; Brunner 2010; Goraj 2010a: 35; McGhee et al. 2010).

Although the term 'process bus' refers to a separate communication network, it is possible to combine the communication traffic of station level and process level to one physical network carrying both of them. (Brunner 2010).

At the moment, some of the ABB Relion® 670 series IEDs already support IEC 61850-9-2LE process bus communication. It also allows mixing conventional wiring and fiber-optic communication based on IEC 61850-9-2LE, which allows moving from conventional wiring to IEC 61850 digital process bus one step at time. (ABB Oy 2011a: 5).

2.3 IEC 61850 extensions

The development of IEC 61850 is still continuing. Originally IEC 61850 was merely designed for substation automation systems, but it has been extended to other application areas as well. These include wind power systems, hydro power systems and distributed energy resources. Moreover, the standard has also extended to apply communication between substations as well as between substations and network control centers. The extension of the application range can be seen from the new title of the standard: "IEC 61850 – Communication Networks and Systems for Power Utility Automation". The usage of IEC 61850 in the area of distributed generation shows the significance of the standard for smart grids.

In addition, most of the fourteen parts of the original IEC 61850 standard are also updated at the moment. They are revised, extended and then published as new editions. The part IEC 61850-6 edition 2.0 was published in the end of 2009 as the first part that

carries the entry of a new edition. Second editions of the parts try to solve remaining challenges from their first editions. In addition to correction of errors and small details, they contain new add-ons. These add-ons include clarification of unclear parts, data model and SCL extensions for communication between substations, data model extensions for new application functions, SCL extensions and implementation of SCL conformance and among others. They also add new common data classes, provide longer names for logical nodes (128 char.) and add new parts to the standard. Furthermore, the second editions of the parts IEC 61850-8-1 and IEC 61850-9-2 (station and process bus) bring also support for redundant IED interfaces, which are clarified in the Chapter 5. For clarity, it is recommended to specify the part and its edition when we talk about IEC 61850 in detail.

The IEC 61850 extensions will be backwards compatible to the first edition of the standard. It is thus guaranteed that investments in products and solutions are secured and the customer or supplier will benefit from present and future advantages of IEC 61850. The development of IEC 61850 will not decelerate in the future; there are task forces that have already begun working with parts that will carry the entry of edition 3. (ABB Oy 2010a: 48–51; IEC 61850-6 2009; Siemens 2010, Schwarz 2010).

3 COMMUNICATION NETWORK AND RELIABILITY IN SUBSTATIONS

The real-time protection, control and monitoring functions of the substation automation systems require fast, highly reliable and deterministic communication networks. A deterministic network has predictable, calculable and consistent response time and the data transfers between end points within a guaranteed time. Moreover, the substation environment has to be observed: the devices must operate properly under substation conditions. This chapter focuses on communication network within a substation environment. In addition, some reliability aspects are taken into account. Because the architecture of the substation communication network is not standardized, the most common topologies are investigated in the Chapter 3.3. (Ali & Thomas 2010; IEB Media 2011).

3.1 Ethernet and switches

Ethernet is a mainstream technology, supporting CAT5/CAT6 cabling with both RJ45 (copper) connector and fiber optics as well. When Ethernet is used in an industrial environment like a substation, the term ‘Industrial Ethernet’ is used. Industrial Ethernet used in substations does not differ from common Ethernet in the standard level, but it requires additional features from the equipment in the area of reliability, redundancy, tolerance for substation environment conditions, suitability of power supplies and services that provide short response times.

The choice whether to use fiber or copper in substation network can be difficult for the designer. Fiber optics has some technical advantages over copper like immunity to electrical interference and ability to be used over long distances as well as for bandwidth hungry applications like video streaming, but is more expensive than copper. The designer has to take into account cost versus reliability and criticality factors of the system to be protected. It can also be practical to make a compromise to use: copper to connect IEDs and switches within a bay and fiber to connect switches between bays. On stricter demands, it can be required that only fiber is used in the substation, excluding

station devices like station computers or gateways that are allowed to use copper. (Hoga 2007; Moore & Goraj 2010). Using copper between IEDs and switches causes galvanic connection between IEDs and could theoretically cause a fault (e.g. surge) to spread over copper LAN to other IEDs and devices.

Most substations do use combinations of fiber and copper cabling. While fiber is a preferred option (noise immunity) as transfer medium in a substation, copper cables can be used inside control room cabinets for short interconnections. However, a study made by EPRI (Electric Power Research Institute) in 1997 tested shielded and unshielded twisted pair copper cables for the electromagnetic noise immunity. The study conclusion states that these copper cables are not suitable as LAN media in substation due to fast electrical transients, which have a harmful effect on the copper cable causing significant frame loss (e.g. 66% at 2 kV) which is unacceptable for real-time control. The study recommends that fiber optic media is used to connect all protection IEDs in a substation. Also the standard 'IEEE 1615 - Recommended Practice for Network Communication in Electric Power Substations' (2007: 36–40) says that for uninterrupted communication during electrical transients, all communication links longer than two meters should be fiber. Furthermore, copper is not recommended to use outside of the substation control house. A conclusion for this topic could say that all connections that are exposed to electromagnetic interference should be fiber optics. (Madren 2004; Pozzuoli 2003: 24–25).

Due to the nature of Ethernet, all IEDs using IEC 61850 have to be connected to an Ethernet switch. Because Ethernet is a packet based technology where IEDs can start transmitting data at any time, switches are needed to send the packets to desired direction and prevent collisions of these packets. The incoming packets are stored in memory and placed in a queue for the sending port, and the packet is transmitted as it reaches the front. This is called the 'store and forward' process.

A modern managed Ethernet switch (management processor inside) has many additional features to manage and optimize the network. These may include the following among others:

- Class of Service/Quality of Service (CoS/QoS) (IEEE 802.1p) to tag traffic with different prioritization levels. High real-time traffic has always the highest priority.
- Virtual Local Area Network (VLAN) (IEEE 802.1Q) to allow grouping of IEDs into different VLANs to segregate and secure traffic to different levels of the network.
- Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) to configure fault tolerant ring network, which configures itself during failure. RSTP is discussed in Chapter 4.1.
- Simple Network Management Protocol (SNMP) to manage and monitor devices in the network.
- Internet Group Management Protocol (IGMP) and Multiple MAC Registration Protocol (MMRP) to support and manage multicasting.
- Link Aggregation to increase bandwidth and redundancy between devices. Link Aggregation is discussed in Chapter 4.2.
- Port mirroring, user interface and cyber security functions.
  (Ali & Thomas 2010; Moore & Goraj 2010; Pozzuoli & Moore 2006)

3.2 Reliability requirements

IEC 61850-3 defines requirements for substation communication. It states that the substation must remain operable in case of failure of a communication component. Furthermore, the failure should not result in multiple component failures or cause undetected loss of functions. It is therefore reasonable to maintain adequate local supervision and control. It depends on the application if some special arrangements are needed in the substation automation system.

In case of redundant communication elements, a failure that could disable both redundant elements must not exist (they should be powered from independent power sources). Redundancy is not mandatory for the communication system, though. It depends on the importance of the substation and the consequences of an outage.

However, the communication network failure does not stop the protection at the IED level, but GOOSE messages will fail since the network is not available (Kirrmann et al. 2008).

There must not be any single point of failure that will result in a non-operable substation. In addition, a failure resulting in undesired control action of the system (e.g. tripping, circuit breaker closing) shall not occur. The failures of a substation automation system must not disable local metering and local control functions in the substation. These requirements are crucial especially for the process bus, and can be one reason why it has not yet become common in substation automation. However, these requirements can be fulfilled with the seamless redundancy protocols handled in Chapter 5.

IEC 61850-3 refers to standard IEC 60870-4 for further and more detailed reliability and performance requirements as well as availability requirements. (IEC 61850-3 2002: 13).

From the substation environment's point of view, the key issues that can affect network performance in substation can be divided to EMI (Electromagnetic interference) phenomena and environmental conditions. Environmental conditions include climatic, mechanical and other non-electrical influences. There are requirements for temperature, humidity, barometric pressure, mechanical and seismic and pollution and corrosion influences among others. IEC 61850-3 refers to standards IEC 60870-2-2 and 60694 for detailed information for requirements. Network equipment is needed to be 'substation hardened' to withstand these conditions. (IEC 61850-3 2002: 17–19; Pozzuoli & Moore 2006).

Also the IEEE standard 1613 gives requirements for environment and EMI immunity for equipment inside substation (Pozzuoli & Moore 2006). Devices certified for both IEC 61850-3 and IEEE 1613 are guaranteed for reliable and solid performance inside harsh substation environment.

3.2.1 Reliability and availability fundamentals

Reliability is defined as the probability of a system performing its function over a certain time period. It is important to notice that reliability differs from availability. Availability defines the ability of a system to provide service whereas reliability measures the system ability to function without interruptions. In brief, reliability provides information of how often component fails while availability includes the downtime that failures provide. However, a system with poor reliability can have high availability if the restoration time is rapid enough (see equation 1). (Vargas 2000: 4, 9)

There are three terms which are used in availability calculations: MTBF (Mean Time Between Failures), MTTF (Mean Time To Failure) and MTTR (Mean Time To Repair). MTBF presents the number of hours between failures. MTTF is a similar term to MTBF, describing how many hours it takes from a device to fail after it was put into service. MTTR describes the amount of time between network failure and restoration to proper condition, including detection, diagnosis and repair time itself.

The terms MTBF and MTTF are often confused. Usually MTBF includes both MTTF and MTTR, representing the time between maintenance calls. However, if availability is high (MTTR << MTTF), MTTF is roughly equal to MTBF and it makes no practical difference which one to use.

The availability of the network can be calculated as the ratio of uptime to the total time as the equation

$$A_N = \frac{MTTF_N}{MTTF_N + MTTR_N} \quad (1)$$

shows. Here, $MTTF_N$ is the Mean Time To Failure of the network and $MTTR_N$ is Mean Time To Repair network. (Oggerino 2010: 11–12; IEC 62439-1 2010: 35–36).

To calculate the availability or the MTTF of the whole system, the following equations in the Figure 10 are applied.

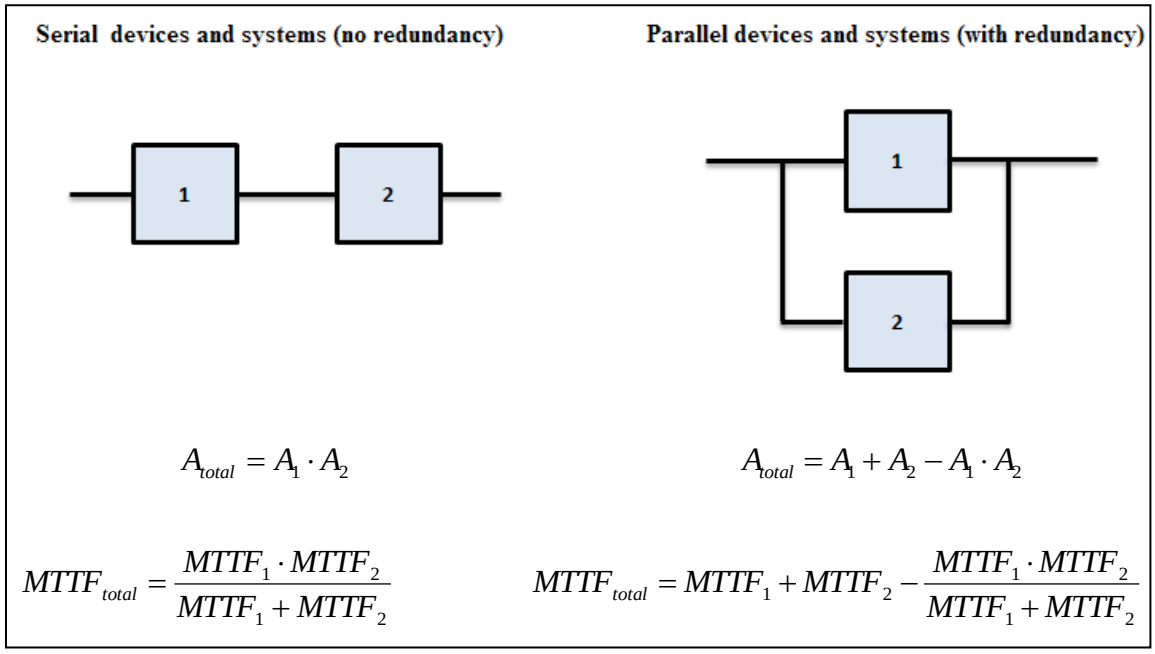


Figure 10. Availability and MTTF of different systems. (Kanabar & Sidhu 2009).

The availability is often described with number of nines. For example, an availability percentage of 99.999 means downtime of 5.26 minutes in a year, while adding one nine (99.9999 %) equals yearly downtime of 30 seconds. An estimate is often made, presenting that after availability percentage of 99, every additional nine costs twice as much thus doubling the cost of the network. However, it does make the network ten times more available. (Oggerino 2010: 10; Vargas 2000: 7).

Network supervision is a crucial element for gaining availability. It shortens the MTTR value dramatically, because the fault can be detected immediately. In addition, the self supervision function implemented in IEDs monitors the state of IED hardware and operation of IED system functions, thus reporting the operator of malfunction of the IED. The health status of the network(s) and the connected devices (switches, IEDs etc.) must be monitored to get the full benefit of redundancy, otherwise it will help little (ABB Oy 2009a: 4, 6; IEC 62439-3 2010: 18).

Especially, the condition monitoring of the redundant networks is very important. When the failure occurs and redundancy acts, the network recovers but is no longer redundant. Redundancy must be restored and only condition monitoring will tell if the redundancy

has acted. Also, a fault may not cause malfunction right away, and this cannot be seen in unmonitored network. SNMP and possible IEC 61850 objects are good means for monitoring and supervising the health of the network(s) and devices.

3.2.2 Failures and failure rate

Another measure of reliability of the component is the failure rate, which is the inverse of MTBF. It describes the number of failures in a certain time (usually per hour). The failure rate of a component usually changes during its lifetime but it can be assumed to be constant due to small variance. However, the detailed failure rate of components follow the diagram known as the ‘bathtub curve’ as shown in Figure 11, describing the relative failure rate over time.

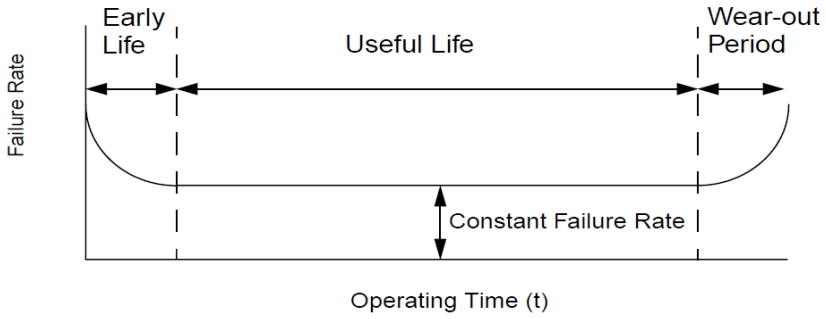


Figure 11. Failure rate over operating time a.k.a. the ‘bathtub curve’ (Vargas 2000: 6).

The ‘bathtub curve’ divides the lifetime of a population of electronic components into three regions: early life, useful life and wear-out period. The failure rate in the early life region is higher due to infant mortality phenomenon, where manufacturing errors as well as other defects take place. After that, the failure rate remains constant and only random failures happen. In the wear-out period, failure rate raises because the lifetime of components is coming to an end, i.e. are starting to wear out. (Vargas 2000: 5–6).

The ‘bathtub curve’ does not describe the failure rate of a single item, but an entire population of items over time. It is used as visual model to demonstrate the three periods of the product failures; not to determine the exact and expected behavior of one product family. (Wilkins 2002).

The failures of substation automation components can be classified to internal device and link failures and to external causes. The former ones include device failures, resulting in loss of power supply, processing electronics or communication ports. Usually the user experiences application losses, like losing access to the whole substation automation system via HMI or NCC (Network Control Center), losing the access to one single bay or to an individual IED. Most of these losses are constant and need repairing, but some can be temporary and the system can recover from these failures, for example by means of redundancy.

The latter ones include failures that are caused by external influences. Components of the system as well as communication links can be destroyed for example of careless action of a service man. (Andersson, Brand, Brunner & Wimmer 2005).

As mentioned, a single point of failure is very undesirable because it results in failure of the whole system. It can appear because of design error or because of an external cause that disables also redundant elements, for example extreme temperature. (IEC 62439-1 2010: 15).

3.3 Communication network topologies

There are many applicable network topologies that may be used in substation automation with IEC 61850, each of which provides different levels of performance, redundancy, availability and cost. The basic topologies are cascading, star and ring topologies, which are presented in the following sections, along with topology of ring of IEDs.

3.3.1 Cascading (linear, bus) topology

In cascading topology, every one of the switches is connected straight to the previous or next switch via one port. This architecture is simple and cost effective. The worst case delay (latency) that system can tolerate defines how many switches can be cascaded altogether. Delay will increase as the message gets transmitted from switch to another,

in addition to internal processing time. This has to be taken into account if the application is very time-sensitive. Figure 12 shows the principle of the cascading architecture.

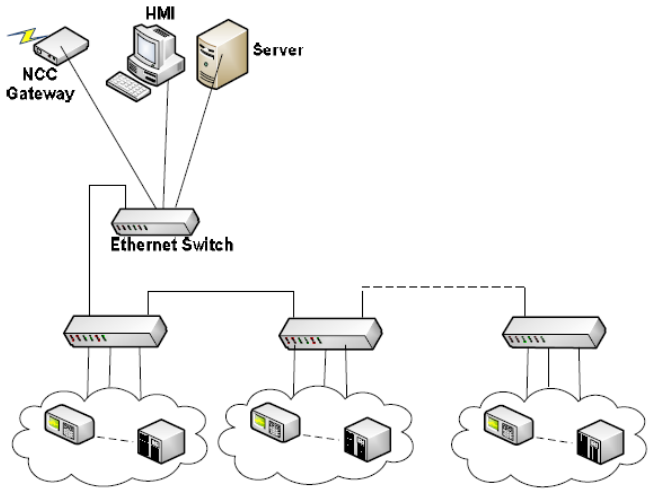


Figure 12. Cascaded topology. (Kanabar & Sidhu 2009).

Moreover, this topology has a disadvantage of not offering any redundancy. A fault in the cascading chain will disable all connections to devices downstream of the failed connection, which gives a reason to avoid this topology. (Pozzuoli & Moore 2006).

3.3.2 Star topology

The most basic topology in switched networks is star topology. Here, every switch is connected to one central switch (backbone switch). This architecture offers the lowest amount of latency, since a message goes from switch to another only through the central switch. Other advantages offered by star topology are simplicity, easy configuration and scalability. However, redundancy is not available in this topology either. Moreover, the major drawback of this architecture is the fact that the central switch becomes a single point of failure. Figure 13 shows the star topology. (Pozzuoli & Moore 2006; Moore & Goraj 2010).

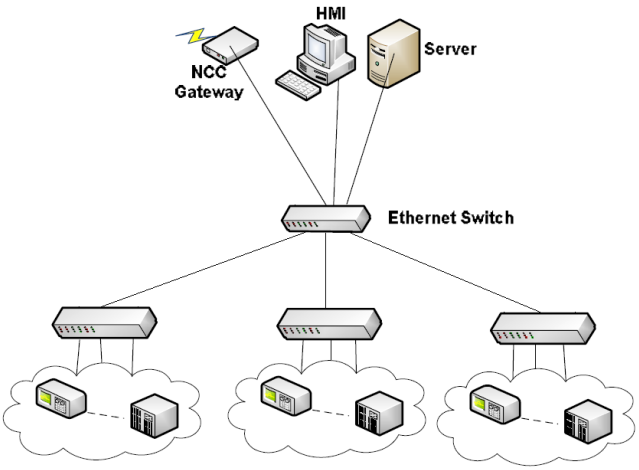


Figure 13. Star topology. (Moore & Goraj 2010). Picture edited.

3.3.3 Ring topology

The Ethernet ring topology with automatic reconfiguration during failure is the most common architecture for substation automation systems according to IEC 61850 (ABB Oy 2010a: 11). This architecture is similar to cascading topology; only one additional link is connected to close the loop between the last and first switch. Traditionally Ethernet switches have not supported loops because the messages would keep circulating in the loop, eventually eating up all the bandwidth. Nowadays switches are managed and include a redundancy protocol that provides the elimination of the loops and prevent infinite data transmission in the network. The most widely used redundancy protocol is RSTP (Rapid Spanning Tree Protocol), which also provides reconfiguration of network during failure. RSTP is discussed more detailed in Chapter 4.2.

The ring topology brings some level redundancy which is seen as immunity to physical break in the network. The amount of switches that can be connected to the ring is defined by the redundancy protocol. RSTP limits the ring to 40 hops, which is a link from switch to another. It is important to notice that the more switches there is in the ring, the longer it takes to reconfigure the switches during failure. In ring topology, RSTP can provide reconfiguration time of 5 milliseconds per one hop, so the total reconfiguration time in the ring of 40 hops can be about 200 ms. Figure 14 presents the principle of ring topology.

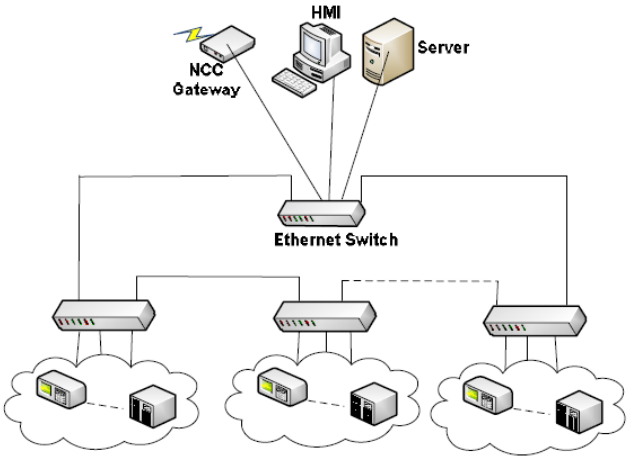


Figure 14. Ring topology. (Kanabar & Sidhu 2009).

The ring topology does not improve any network latency while it is similar to cascading topology. However, managed Ethernet switches utilize CoS (Class of Service) to reduce latency especially in frame queuing by setting different priorization levels for frames. (Pozzuoli & Moore 2006; Moore & Goraj 2010; Kanabar & Sidhu 2009).

If IEDs are dual homed, the ring topology can be doubled, thus forming a redundant dual ring topology. This is presented in Chapter 3.3.6.

3.3.4 Ring of IEDs topology

The ring of IEDs is a very recent topology that is used in IEC 61850 based substations. Here, the IEDs have an embedded switch module, which may implement typical features of managed switches, for example RSTP for redundancy and SNMP for port supervision. The main advantage of the topology is the cost reduction by elimination of a number of communication links and standalone switches. (Moore & Goraj 2010).

Some of the ABB IEDs also support this topology. The ABB Relion® 615 series IEDs offer a communication module of two Ethernet ports. This enables a self-healing Ethernet ring topology when used with managed switch with RSTP support. The switch handles the ring consistency by routing the data and correcting the data flow during communication failure, while the IEDs act as unmanaged switches forwarding the data traffic. This solution supports connection of up to 30 IEDs of 615 series in the ring. If

the application has more than 30 relays, it is highly recommended to form several rings of IEDs, with no more than thirty IEDs per ring. Figure 15 shows the topology of ring of IEDs. (ABB Oy 2010c: 20).

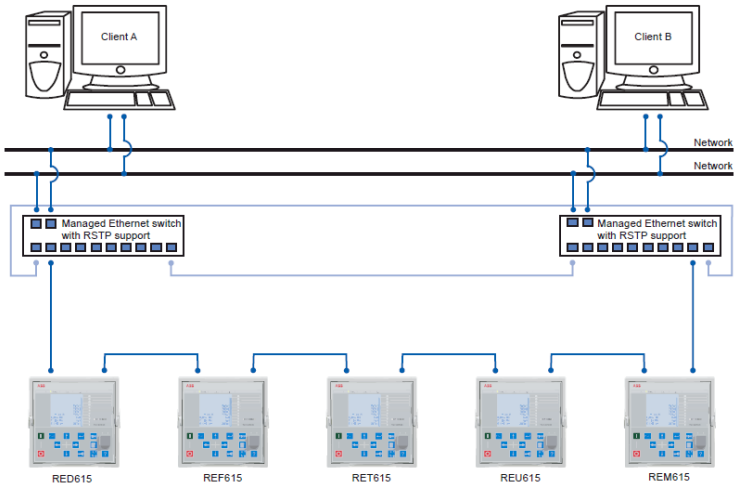


Figure 15. Ring of IEDs with ABB Relion® 615 series IEDs. (ABB Oy 2010c: 21).

However, at the moment this self-healing Ethernet ring with 615 series IEDs has some issues to take under consideration. There is no detailed documentation for this solution, no configurable parameters and no supervision for IED port status. However, the general supervision of the IED ring can be done by supervising the corresponding ports of the Ethernet switches via SNMP. Furthermore, the performance of recovery time in case of a connection failure is quite poor; it is in the range of few seconds. (ABB Oy 2011b: 31, 78).

3.3.5 Other topologies

There are also many other topologies that can be used in substation automation. There are hybrid topologies like star-ring topology or meshed topologies, and topologies where IEDs use dual homing (IED is attached to network with two links). With dual homing, redundant star and ring topologies can be constructed, connecting the network interfaces of IEDs to two rings or two stars, where the other network can act as backup. All these topologies offer even more reliability and availability by tolerating numerous faults, but increase costs. Figure 16 presents some of these topologies. These topologies

are not investigated further in this thesis. (Kanabar & Sidhu 2009; Moore & Goraj 2010; Pozzuoli & Moore 2006).

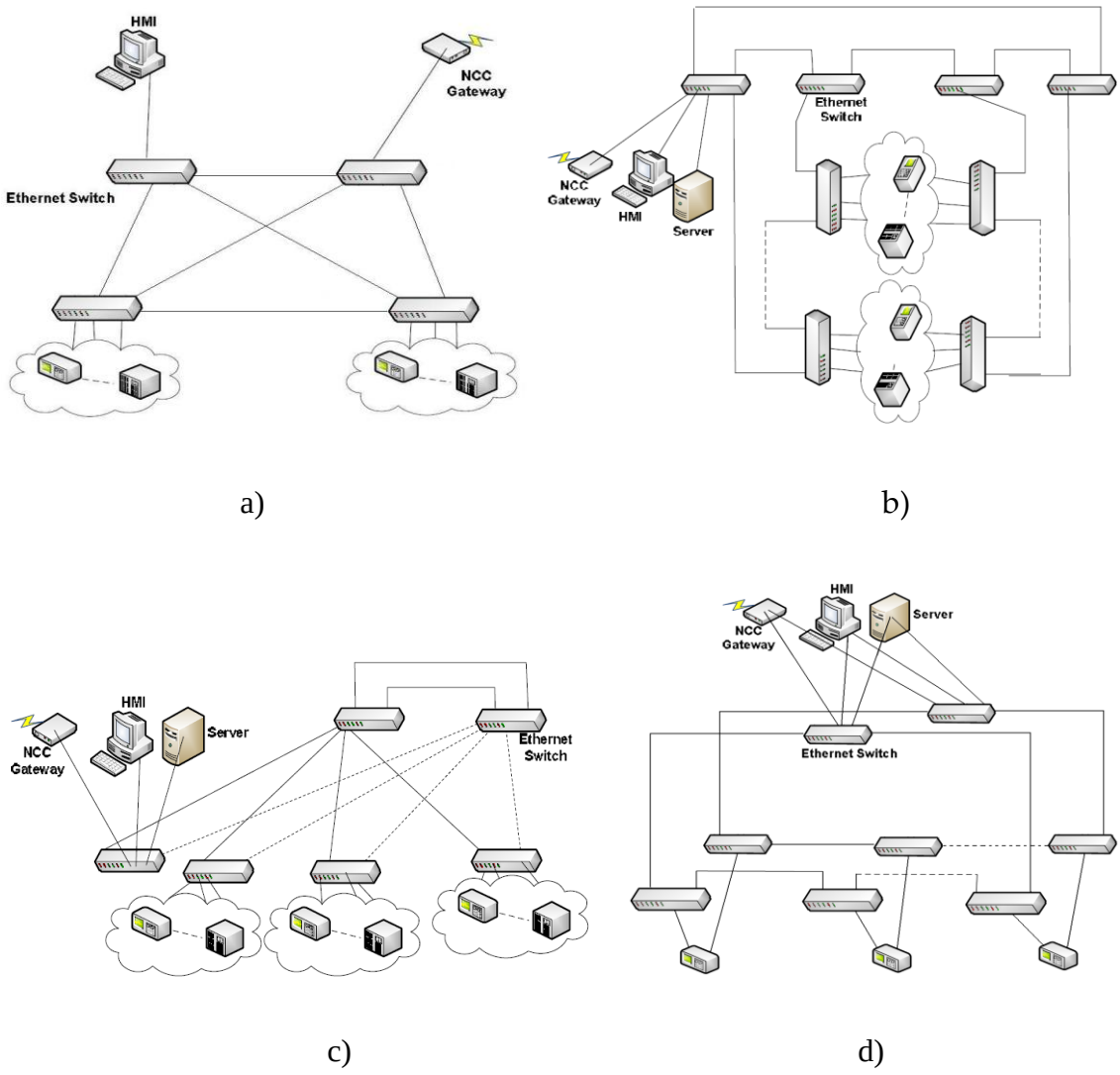


Figure 16. a) Meshed topology, b) redundant ring topology, c) star-ring topology, d) redundant dual ring topology. Picture edited. (Hoga 2010; Kanabar & Sidhu 2009; Moore & Goraj 2010).

As mentioned, each topology has its advantages and disadvantages in the areas of redundancy, performance and cost. They are achievable through managed Ethernet switches that offer many features needed in substation automation, ring topology being the most common architecture used in the substation automation today. (Pozzuoli & Moore 2006).

4 PRESENT REDUNDANCY PROTOCOLS IN SUBSTATION AUTOMATION

This chapter discusses present redundancy protocols and methods used in substation automation in brief. The de facto redundancy protocol used today is Rapid Spanning Tree Protocol (RSTP), which is an evolution of the older Spanning Tree Protocol (STP). There are also some proprietary protocols based on RSTP that manufacturers have developed. These protocols are investigated in the following sections along with Link Aggregation Control Protocol, which enables the configuration of multiple links between Ethernet switches to one single link.

4.1 Rapid Spanning Tree Protocol (RSTP)

The history of Spanning Tree Protocol begins in 1990 when it was published in the standard IEEE 802.1D-1990, designed for solving the problem of traffic loops. The main idea in the STP is to disable some links, forcing them in to a hot standby mode and thus making the network to form a topology of a tree. This tree connects every switch but eliminates the loops. STP has been proven to be a reliable redundancy protocol but originally it was not designed for quick operation. After a link failure, STP needs at least 30 seconds to restore the network, which is far too slow for real-time automation networks. In 2001, an extension to the standard (802.1w) was published, introducing RSTP, which provides a recovery time of a few seconds while adding some new improvements. Furthermore, the original standard has been published as a new edition (802.1D-2004), outdating the STP and reducing the recovery time of RSTP down to a few milliseconds. (Pustylnik, Zafirovic-Vukotic & Moore 2008).

RSTP is layer 2 redundancy protocol, which provides network redundancy while preventing loops in the network. Spanning tree is formed when there are multiple paths or connections to different switches. It configures some of the links into blocked-state and in the case a network segment becomes unreachable, RSTP reconfigures the network and activates the blocked link or links. This all happens automatically, but the result depends also on defined parameters. (Midence & Iadonisi 2009).

There is also an extension to RSTP, called Multiple Spanning Tree Protocol (MSTP), which allows multiple spanning trees in to the same bridged network by mapping one or more VLANs on to the network. (RuggedCom 2011: 99–100).

4.1.1 RSTP operation

The RSTP operation is based on role and state configuration of bridges and their ports. The RSTP bridge can be assigned with two roles; root or designated. A network has one root bridge, which can be seen as a logical center of the network. All other bridges are designated bridges. The ports of the bridges are assigned with state (describes the port state in relation to address learning and frame forwarding) and role (describes if the port is facing the center or the edges of the network and if it can be used).

The port states are discarding, learning and forwarding. When the port is put to service, it will be in the discarding state, where it only looks for RSTP traffic in order to define its role in the network. When it is specified that the port will play an active part in the network, its state changes to learning. In learning state, the port learns addresses but does not transfer frames. The time it spends in this state is quite short. After this, the bridge changes ports state to forwarding, where it will also participate in frame transferring in addition to address learning. It can also change back to discarding, if it occurs that port is not supposed to be active in the network. (RuggedCom 2011: 95–96)

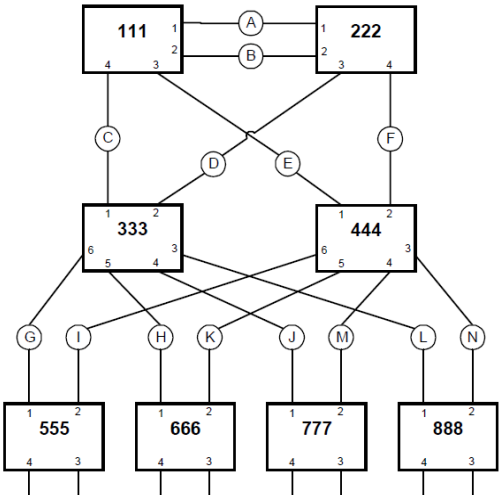
There are five roles that port can be assigned to: root, designated, alternate, backup and disabled port. Every bridge except the root bridge has a single root port, which is the best (quickest) way to send traffic to the root bridge. A port will be assigned as designated if it is the best port to serve a LAN segment it is connected to. The alternate port is an alternate way to root port and will take its role if the root port fails. The backup port mainly acts as a backup for designated port and can exist if there are at least two links from a bridge to another. The port role can be also disabled if the port is not operational or is excluded from the active topology by management. (Ruggedcom 2011: 96–97; IEEE 802.1D 2004: 139, 145).

Furthermore, a port can also be assigned as edge port in the case where it is directly attached to an end node (cannot form bridging loops, port state always in forwarding state). There will be no unnecessary topology change messages as the port will serve only end nodes. (Ruggedcom 2011; 97).

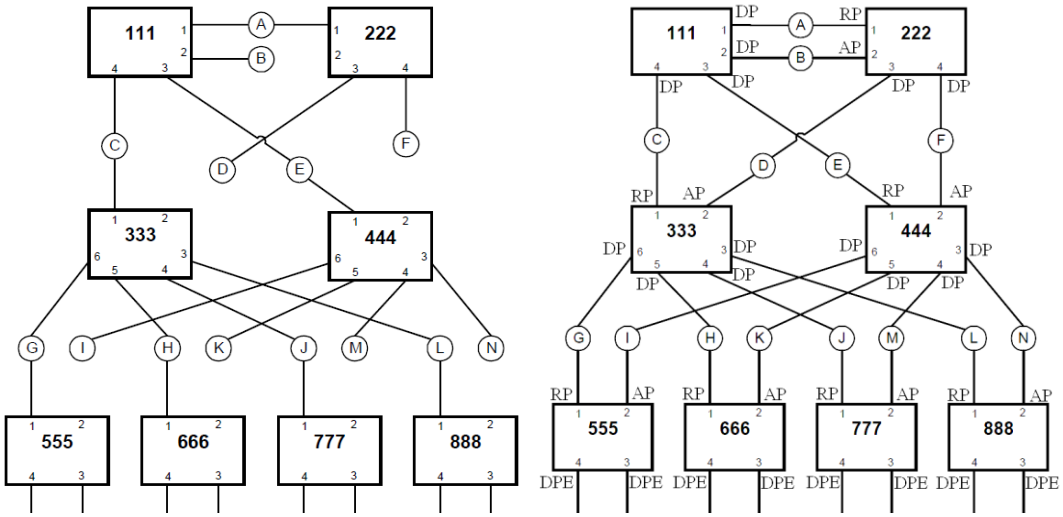
The topology computation starts with defining the root bridge, which has the best bridge identifier. The bridge identifier consists of bridge MAC (Media Access Control) address and manageable numerical priority component (the lower priority, the better identifier). Every designated bridge has a root path cost value (for the root bridge this is zero). The cost is calculated as the sum of the individual port costs of the links between designated bridge and root bridge. The port with the lowest path cost to root bridge will become the root port (root bridge will not have root port). If the two ports have the same root path cost, the port with best port identifier is chosen as root port. This path cost value is the main metric when defining root and designated ports. Any operational bridge port that is not a root port or designated port is an alternate port, or a backup port in the case there are two or more connections from a bridge to another. Furthermore, every bridge on the network sends configuration messages called BPDUs (Bridge Protocol Data Unit). They include information about bridge and port roles, root path costs and data from the current topology among others. (IEEE 802.1D 2004: 138–139; Ruggedcom 2011: 97)

There is mechanism called proposal-agreement that takes place between RSTP bridges. It provides RSTP bridge to actively confirm that a port can change its state to forwarding, without the use of any network timers (like in STP). This brings faster configuration times. (Pustylnik et al. 2008).

The alternate and backup ports do not participate in the network, so the active topology is based on root and designated ports. Each ports role can change if a failure occurs. Figure 17 shows the principle of the RSTP topology calculation. In the figure, case a) shows the physical topology and the case b) shows the RSTP active topology, where the tree is formed and loops are eliminated. Case c) shows the roles of the ports, where the roles of ports are presented as follows: Root port (RP), designated port (DP), alternative port (AP) and designated port with edge port configuration (DPE).



a)



b) c)

Figure 17. Physical topology (a), active topology (b) and port roles of bridges (c). Picture edited. (IEEE 802.1D 2004: 140–141).

4.1.2 RSTP performance considerations

As mentioned, RSTP provides recovery from switch failures and link failures between switches. What comes to the network recovery time, it depends on the topology and RSTP implementation. For meshed topologies, RSTP may provide a deterministic

recovery time in the case of failure, apart from root bridge failure where recovery time is difficult to predict. Actually, the RSTP standard does not define recovery times for meshed topologies. Ring topology instead provides deterministic and calculable RSTP recovery time in all failure scenarios. (IEC 62439 2010: 44).

The (worst case) recovery time of ring topology network using RSTP can be calculated using the following formula:

$$T_{recovery} = T_L + (N \cdot T_{PA}), \quad (2)$$

where T_L is fault detection time, N is the number of switches in the ring and T_{PA} is the time that it takes to perform RSTP proposal-agreement mechanism. Many vendors report fault detection times in the 5 ms range as well as the proposal-agreement times.

Using the formula above, a ring of 10 switches has a recovery time of about 55 ms. RSTP can provide recovery time 5 ms per hop or less; even a performance of 2 ms per hop can be reached with today's high speed switches. However, in the case of root bridge failure (although rare), the recovery time doubles because it takes longer to determine and configure a new root bridge. Some vendors have implemented proprietary root failure improvements to reduce the root failure recovery times. Using the formula again with root bridge failure, the worst case recovery time of the ring of 10 switches would be 110 ms. (DesRuisseaux 2009).

The T_L and T_{PA} values used in formula 2 can however vary depending on the vendor, product or port type, so the network designer should carefully study the RSTP properties of the switches when choosing devices to network. For example, RuggedCom provides the following values for RSTP performance (Pustylnik et al. 2008):

- T_{PA} = 5 ms
- T_L = 4–6 ms for 100Base-TX and 100Base-FX links
  = 20 ms for 1000Base-X links
  = 700 ms for 1000Base-T links

As seen, different link types take different time for fault detection. The usage of gigabit Ethernet over fiber (1000Base-X) and copper (1000Base-T) multiplies the fault detection time of RSTP compared to 100 Mb Ethernet, especially with copper. Gigabit copper should thus be totally avoided in substation automation networks when using RSTP (see also Table 5). Furthermore, it has to be ensured that the switches support the latest RSTP standard IEEE 802.1D-2004 to gain the above mentioned recovery times.

We can see that RSTP recovery time is not enough for the applications that demand seamless recovery time (0 ms), for example IEC 61850 sampled values on the process bus. This is why redundancy methods with zero recovery time are needed, and are only provided by Parallel Redundancy Protocol or High-availability Seamless Redundancy. (DesRuisseaux 2009, ABB Oy 2010a: 59).

Furthermore, the network using RSTP can include not more than 40 switches. Proprietary extension RuggedCom eRSTP™ however allows a network of 160 switches. (Pustylnik et al 2008).

4.2 Link Aggregation Control Protocol (LACP)

The Link Aggregation Control Protocol originally defined in IEEE 802.3ad can also be seen as a redundancy method. It combines multiple physical network links into a single logical link, which increases both capacity and availability of the communications channel between devices. In addition, Link Aggregation (also known as port trunking or port bundling) provides load balancing, so that the processing and communication is divided between several links.

Link aggregation prevents the interconnected devices from the failure of any single link between them. The failure of a link reduces the available bandwidth, but the connection remains between the remaining links and data flow is not interrupted. However, in the case of physical connectivity change, Link Aggregation must reconfigure the configuration. Normally this is done in 1 second or less. Link aggregation can be used with point-to-point links e.g. between two switches or between a switch and end station

(server, router) as seen in Figure 18. Aggregations among more than two systems (multipoint) are not supported. (RuggedCom 2011: 89; SysKonnect 2002: 5, 11–12).

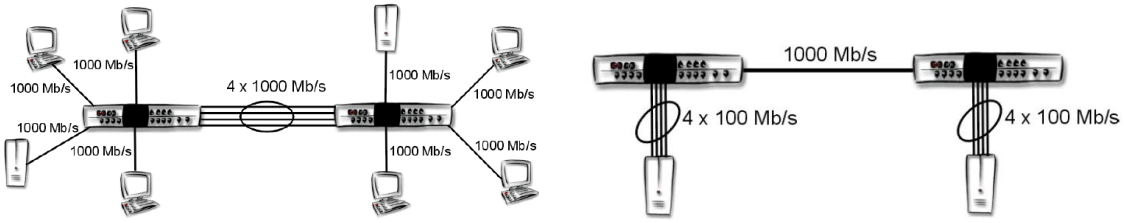


Figure 18. Link aggregation examples. The former one presents connection between switches and the latter one between servers and switches. The aggregation connection is ringed. (SysKonnect 2002: 7–8).

The Link Aggregation requires all physical links to run at same speed, otherwise the performance will drop. The LACP configuration must also be done on both sides of the aggregated link. Especially, between switches the configuration must match or otherwise a loop can be formed. Layer 2 features like Spanning Tree treat a port trunk as single link. However, it shall be noted that RSTP is a superior way to handle redundancy between two switches connected with more than one physical link. Especially, if increased bandwidth is not required and RSTP is enabled, Link aggregation should not be used, since it may cause longer fail-over time. (RuggedCom 2011: 90–91). Because of this, the most useful way to use Link Aggregation at the moment may be to gain redundancy between switches and end stations like servers, while RSTP handles the redundancy in the network.

There are also proprietary protocols and methods that are enhancements over LACP or work as a proprietary option, especially in the server network cards. They are often referred as NIC (Network Interface Card) teaming. For example, Intel provides teaming software called Advanced Network Services (ANS) while Broadcom offers Broadcom Advanced Server Program (BASP). These softwares offer teaming modes that can include also Link Aggregation as defined in IEEE 802.3ad, but also proprietary modes, which may not even need support from the switch. These are however not handled further in this thesis. (Bhutani & Mahmood 2003).

4.3 Dual homing redundancy

Dual homing (also dual link redundancy) can be seen as a redundancy method between end nodes (IEDs) and Ethernet switches. In dual homing, an IED has two separate network interfaces. One is active and carries the traffic, while the other one acts as a backup link. In case of a failure, the traffic is switched over to the backup link. The switchover takes time, but can be quite fast. Usually the dual homing is completed via a proprietary extension. Figure 19 shows the principle of dual homing of IEDs. During link failure, the backup link takes over the traffic.

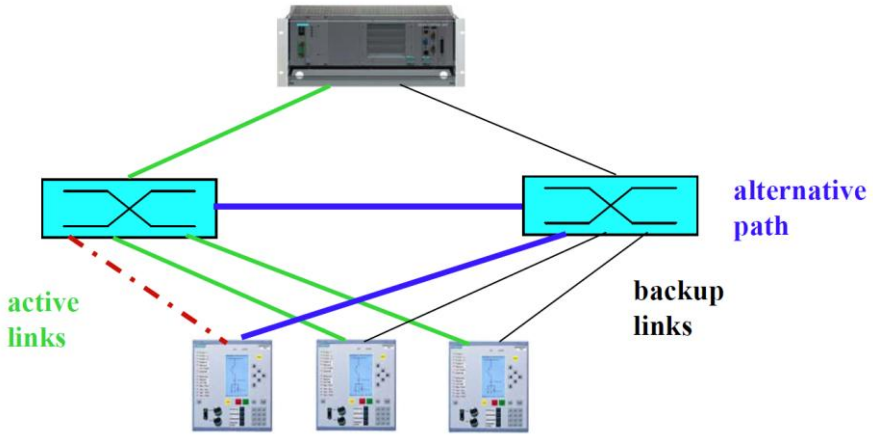


Figure 19. Dual homing example. (Hoga 2010a).

A popular method is to mix ring redundancy and dual homing. The Ethernet switches use RSTP as the redundancy while dual homing brings redundancy between IEDs and switches. If the two links of IEDs are connected to different Ethernet switches, a switch failure can be tolerated. (Hoga 2010).

The mode of the two ports can also be changeable. For example, Siemens Ethernet IED module EN100 can be set to use either dual link redundancy or to use switch mode with RSTP, depending on the wanted configuration and topology. There is also a possibility to use a proprietary ring redundancy protocol with Siemens IEDs. (Siemens 2009).

The proprietary NIC teaming softwares presented in the previous section can also be used to gather dual homing in servers and workstation computers.

4.4 Proprietary protocols

Many different Ethernet switch manufacturers provide proprietary ring-based redundancy protocols and extensions today. These are however vendor-specific methods and are not interoperable with each other. Table 4 shows a comparison of these protocols along with the standardized RSTP.

It must be noticed that the Rapid Spanning Tree Protocol defined in IEEE 802.1D-2004 has equal or even better performance compared to vendor-specific protocols. It has also benefits like support for any network topology and interoperability. The vendors developed their own protocols since there was no standard protocol for industrial Ethernet redundancy providing sufficient network recovery performance. These protocols can be seen as proprietary enhancements to the older RSTP defined in IEEE 802.1w-2001. In addition, some the public information regarding RSTP performance is still partly outdated, misleading to the older version of RSTP. (Pustylnik et al. 2008).

Table 4. The features of RSTP and proprietary redundancy protocols. (Pustylnik et al. 2008).

Protocol	Vendor	Can be used in multi-vendor environment	Max Bridge Diameter	Topology	Single ring link failover time (for different number of switches)		
					10	15	20
STP	IEEE Standard	Yes	40	Any	>30s		
RSTP (802.1w)	IEEE Standard	Yes	40	Any	Several seconds		
HiPER Ring [4],[5]	Hirschmann	No	Virtually unlimited	Ring	200-500ms, independent of number of switches		
Turbo Ring [4],[6]	Moxa	No	Virtually unlimited	Ring	<200ms	<250ms	<300ms
S-Ring [8]	GarrettCom	No	data not available	Ring	<250ms		
RS-Ring [8]	GarrettCom	No	data not available	Ring	<100ms		
RapidRing™ [7]	Contemporary Controls	No	50	Ring	<300ms		
RSTP (802.1D-2004)	IEEE Standard	Yes	40	Any	<50ms	<75ms	<100ms
eRSTP™	RuggedCom enhancements to IEEE Standard	Yes	160	Any	<50ms	<75ms	<100ms

However, lately these protocols have also evolved. For example, Moxa has released new version of Turbo Ring (V2), which provides 20 ms recovery time. The proprietary redundancy protocols are not handled further in this thesis.

5 IEC 62439 – HIGH AVAILABILITY AUTOMATION NETWORKS

The first edition of IEC 61850 did not discuss substation communication network redundancy methods or even Ethernet network topologies. As a result, manufacturers started to develop their own redundancy methods, thus threatening one of the main goals of the IEC 61850; interoperability. To prevent this progress, the standard IEC 62439 was brought out. The first edition was published in 2010, specifying and standardizing several redundancy methods for industrial Ethernet that were originally developed by different manufacturers. IEC 61850 now adopts two redundancy protocols standardized in IEC 62439-3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) that will be discussed in this chapter.

When choosing redundancy method, time requirements for station and process buses play a great role. Table 5 shows the time requirements compiled by IEC Technical Committee 57 Working Group 10. As seen, the process bus with sampled values and station bus used for busbar protection require seamless redundancy. Also the GOOSE messages require rapid recovery time. The zero-time recovery (seamless recovery) can only be fulfilled with PRP and HSR. Seamless recovery is especially crucial with process bus, because if even one sample is missing, the protection relay experiences measuring blackout. (Hoga 2010a; Kirrmann, Rietmann & Kunsman 2008).

Table 5. Recovery time requirements defined by IEC TC57 WG10. (Kirrmann et al. 2008).

Communicating partners	Bus	Recovery time
SCADA to IED, client-server	station bus	400 ms
IED to IED, interlocking	station bus	4 ms
IED to IED, reverse blocking	station bus	4 ms
Busbar protection	station bus	0 ms
Sampled Values	process bus	0 ms

Although RSTP cannot provide as rapid recovery times as stated in Table 5, it can be fairly used in station bus operating as single ring and limited number of IEDs. The station bus should preferably not carry time-critical messages. (Kirrmann et al. 2008).

The Parallel Redundancy Protocol (originally developed by ABB) brings a totally different view for redundancy compared to present redundancy protocols (that are handled by Ethernet switches in the network). In PRP, every device has two Ethernet ports that are attached to two independent networks. The message is sent simultaneously through both networks to the destination, which uses the first one and discards the later-coming one. If failure occurs in one network, the data gets through from the other network with zero recovery time. HSR can be seen as a special case of PRP, bringing its principle into a single ring topology, where the two networks are treated as two directions in the ring and the need of Ethernet switches is eliminated. (Dreher 2011; Kirrmann 2011: 34). PRP and HSR are discussed in Chapters 5.2 and 5.3.

IEC 62439 standardizes also other redundancy protocols (Kirrmann 2011: 33–34):

- **Media Redundancy Protocol (MRP).** MRP is based on Hirschmann-Siemens Hiper-ring protocol and can be used only in single ring architecture. It is a competitor for RSTP in ring topology.
- **Cross-network Redundancy Protocol (CRP).** Originated from Fieldbus Foundation, the CRP uses (like PRP) doubly attached nodes and two LANs, but here they are interconnected. Only one port is active during normal operation.
- **Beacon Redundancy Protocol (BRP).** BRP (originally developed by Rockwell) owns similar characteristics to CRP. It sends a beacon at short intervals to detect failures in the network. Only one port is active during normal operation.
- **Distributed Redundancy Protocol (DRP).** DRP is originally developed by SupCon Group (China) and competes with MRP in ring topology.

These protocols have worst case recovery times between few milliseconds and 1 second. The comparison and performance of all IEC 62439 redundancy protocols can be seen in Appendix 1. This thesis does not handle these protocols further.

An upcoming extension ‘IEC 61850-90-4: Network engineering guidelines’ will include an overview of all relevant substation communication network topics (Hoga 2010a). Also, as the IEC 62439 is published, there is no need to use proprietary redundancy protocols any more in IEC 61850 based substation automation.

5.1 Redundancy classification

Redundancy method/protocol can be classified depending on its type. IEC 62439 presents redundancy as two classes, where every present and new IEC 62439 redundancy protocol can be divided (IEC 62439-1 2010: 22; ABB Oy 2010a: 59–60):

- **Redundancy managed within the network (dynamic redundancy).** The network offers redundant switches and links but the end nodes are attached to the switches through non-redundant links. In normal situation, redundancy is not active and the activation costs some time. Redundancy within a network is handled by protocols that reconfigure the LAN if a switch or link failure occurs. An analogy to the real world for this type of redundancy would be a car, which needs a spare tire after tire breakdown and changing it needs time. A typical example of this kind of redundancy protocol is RSTP defined in IEEE 802.1D.
- **Redundancy managed in the end nodes (static redundancy).** End nodes with dual communication links (doubly attached node) are connected to two different networks and each node decides the network to use, or to use them simultaneously. The support for different topologies is good; the redundant networks can even have different architectures. The parallel operation of separate networks provides seamless recovery, which makes this kind of redundancy well applicable for time-critical applications. This class of redundancy costs about twice as much compared to the previous mentioned type, but the availability is high: the only non-redundant parts of the network are the end nodes themselves. An analogy to the real world for this type of redundancy would be a car with double tires; if one breaks, the car can still continue driving with one tire without interruption.

Both PRP and HSR use the latter redundancy class; redundancy managed in the end nodes (static redundancy). Both the protocols provide that no frame loss happens during failure. However, devices (e.g. IEDs) need support for these protocols. Figure 20 presents the principles of these two redundancy classes. The classes can be also combined in some situations. (IEC 62439-1 2010: 23).

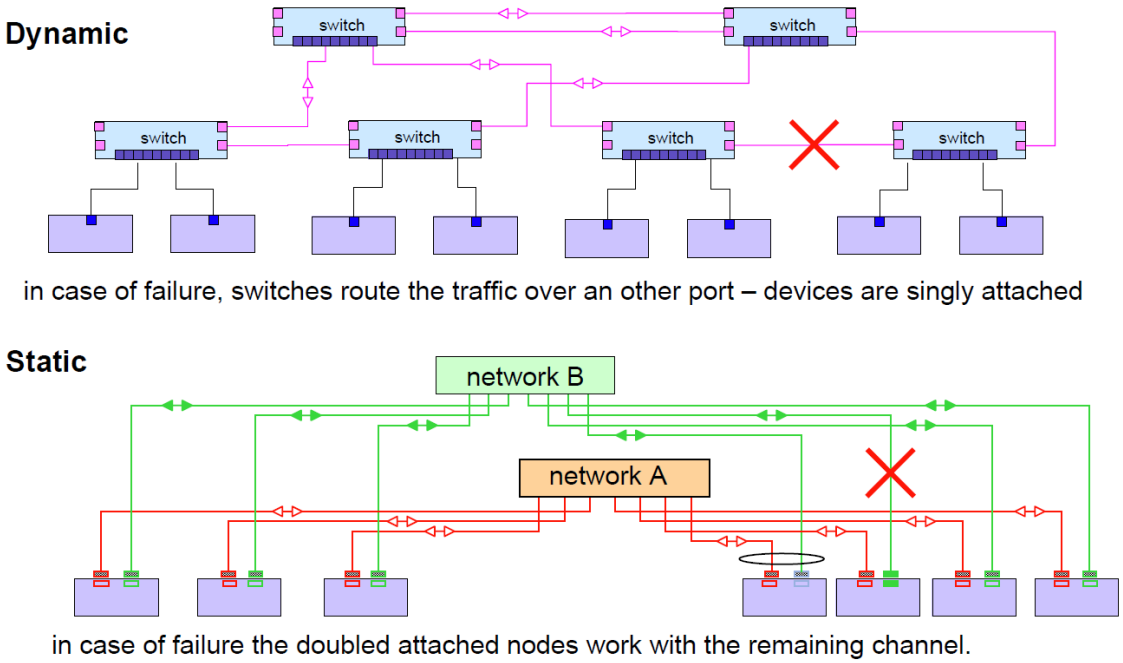


Figure 20. Redundancy classes categorized in IEC 62439. (Kirrmann 2006: 21).

5.2 Parallel Redundancy Protocol (PRP)

Parallel Redundancy Protocol is implemented into devices (e.g. IEDs). Every device that is using PRP is called **doubly attached node implementing PRP (DANP)**. A DANP has two communication ports and is attached to two separate networks, which are operated in parallel. (IEC 62439-3 2010: 9).

5.2.1 Operation principle

The operation of PRP is based on frame duplication. The sending DANP sends the same frame simultaneously to both LANs, and the receiving DANP receives the frame from both LANs within a certain time. The frame that arrives first is consumed and the duplicate is discarded. An example of PRP network is shown in Figure 21.

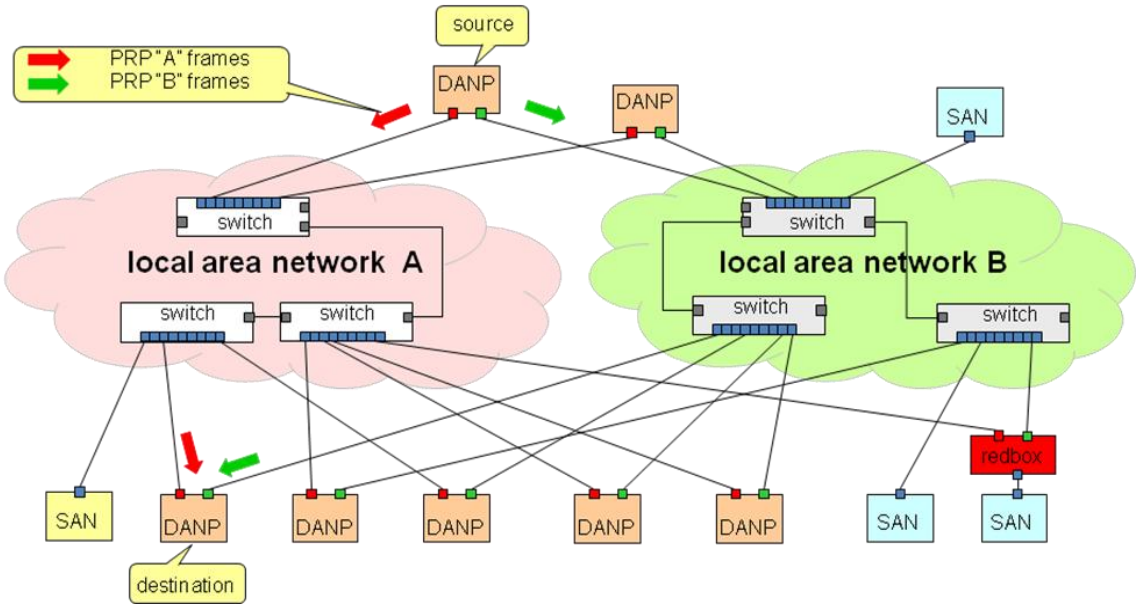


Figure 21. Example of PRP redundant network with doubly attached nodes (DANP) and singly attached nodes (SAN). Picture edited. (Kirrmann 2011: 5, 10).

As seen, the network is doubled in PRP redundancy. Any failure, even the total blackout of the other network, can be tolerated with zero recovery time since the message has two paths to the destination. The two LANs are considered identical, but can differ in performance and topology. Also the transmission delays can be different. There is a strict rule for the correct operation of PRP: the two LANs have no connection between them and must never be connected. (Hoga 2010a; Kirrmann, Hansson & Müri 2007).

In addition to doubly attached nodes, singly attached nodes (SAN) like one-port IEDs can be connected to PRP network via two ways:

- **Connection to one LAN only.** A SAN can communicate **only** with other SANs **on the same** LAN. A SAN is able to communicate with all DANPs in the network.
- **Connection through a RedBox.** RedBox (Redundancy Box) is a device that is attached to both networks and acts like a DANP. SANs connected through RedBox can communicate to both LANs and to every SAN. The SAN behind RedBox appears as Virtual DAN (VDAN) to other DANPs. RedBox is discussed further in Chapter 5.4.1.

A SAN connected to PRP network does not need to support PRP in any way. SANs are devices with one communication port, such as maintenance laptops, printers, etc. Ethernet Switches in the PRP networks do not need PRP implementation (as they need in the case of RSTP) either, because the PRP redundancy is handled by the IED itself; not by the network (see Figure 19). Ethernet switches are considered as SANs because they are connected to one LAN only. (IEC 62439-3 2010: 12; Hoga 2010a).

PRP cannot cover end node failures itself, since it is only designed to cover Ethernet switch failures and link failures, but it allows connection of duplicated nodes to the network, e.g. primary and backup protection relays. (Kirrmann et al. 2007).

5.2.2 Node structure

A PRP node (DANP) has two Ethernet network ports operated in parallel. The two ports have the **same MAC address** and present the **same IP address**. PRP is thus operated on layer 2 (like RSTP) and allows the usual operation of network management protocols as well as supports the time-critical GOOSE and SV traffic (Kirrmann et al. 2008). The use of one MAC and one IP address simplify engineering and especially, allow the operation of Address Resolution Protocol (ARP) to work as in the case of a one-port node (SAN). ARP is needed for clarifying the correspondence between MAC and IP addresses. (IEC 62439-3 2010: 12).

The main reason why the two LANs of PRP network must not be connected is indeed the same MAC and IP addresses of the two ports. Connecting the LANs will lead to ambiguous addressing and will trouble the network as a result. (Hoga 2010a).

The most important component of a PRP node is a layer that handles the two ports and makes the PRP operation possible. This additional layer is called Link Redundancy Entity (LRE) and is inserted to the communication stack (OSI model) of a PRP node. The LRE has two tasks: handling of duplicates and redundancy management. Furthermore, it hides the two network interfaces from upper layers, presenting the same interface towards upper layers as a single network interface. This means that applications and software do not need to be aware of PRP at all.

The LRE is the heart of the PRP operation, duplicating frames when sending the frame and discarding the duplicate when receiving the frames. Figure 22 shows the PRP node structure and the operation of LRE. Note: The LRE is called **DuoDriver** in ABB devices using PRP.

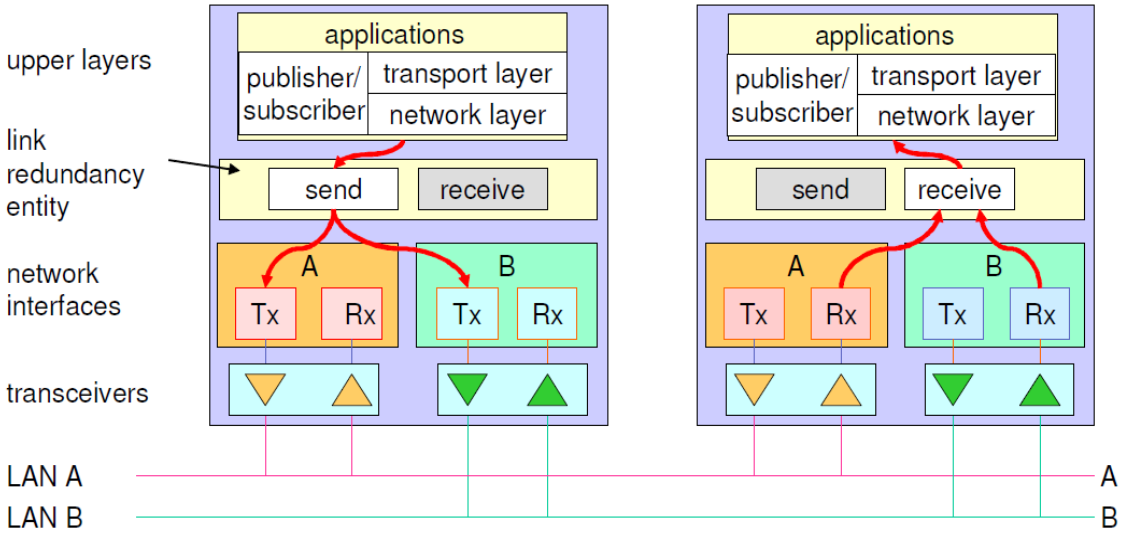


Figure 22. PRP node structure and operation of LRE. (Kirrmann et al. 2007).

When sending a frame, the LRE of the sending node duplicates the frame and sends it through both ports at the same time. These two frames travel through both LANs and arrive to the receiving node with different delays. The LRE of the receiving node forwards the first received frame to the upper layers and discards the duplicate frame that comes later. If a network interface or a network path experiences a failure, data keeps flowing over the other network. (IEC 62439-3 2010: 11–12; Kirrmann et al. 2007). Only a failure that makes both LANs inoperable will bring the redundancy down and makes the network unworkable.

The LRE manages the redundancy by inserting a special Redundancy Control Trailer (RCT) to the Ethernet frames it sends to identify duplicates. Furthermore, it periodically sends PRP supervision frames and evaluates them from other DANPs in the network. (IEC 62439-3 2010: 12). RCT and network supervision are discussed further in Chapters 5.2.4 and 5.2.5.

5.2.3 Duplicate handling

There are two methods which the LRE can use to handle duplicates in PRP nodes (IEC 62439-3 2010: 14):

- **Duplicate accept**, where the sending LRE uses the original frames (without Redundancy Control Trailer) and the receiving LRE forwards both arriving frames to upper layers.
- **Duplicate discard**, where the sending LRE inserts a Redundancy Control Trailer to both frames and receiving LRE forwards the first frame to upper layers and filters out the duplicate. This method is preferred and default.

In the duplicate accept method, the LRE does not try to discard the duplicate at all. The receiving node's LRE forwards both frames to upper layers and assumes that the applications as well as network protocols can withstand duplicates. This has however a drawback; increasing the processor load. The processor is interrupted twice as often as well as the communication stack is executed twice on frame reception. Furthermore, this method does not provide effortless redundancy supervision, because the correct reception of both frames is not monitored. TCP is designed to reject possible duplicates, so in practice it will discard the duplicate MMS frame in IEC 61850. The duplicate accept method can be used in application that cannot cope with the duplicate discard method´s extended frame structure, or for testing usage. Otherwise, the duplicate discard method should be used.

In the duplicate discard method, the LRE does its best to discard the duplicate frame (it is however not necessary to discard every single duplicate). This method is advantageous compared to duplicate accept method, since it reduces the processor load and improves error detection coverage and network supervision. The Redundancy Control Trailer is inserted to both frames, and the duplicate discarding in the receiving node is based on the data inside RCT. Identifying duplicates without a special frame header could be implemented as well (e.g. storing and comparing frames), but these solutions are quite hungry for processor time and memory. (IEC 62439-3 2010: 14; Kirrmann et al. 2007; Weibel 2008: 5).

5.2.4 Duplicate identification with Redundancy Control Trailer

The PRP duplicate identification is based on the contents of the Redundancy Control Trailer field, which is appended to duplicated frames by the sending node's LRE. The receiving node's LRE thus detects the duplicate frame about this information and discards the frame.

The Redundancy Control Trailer consists of the following parameters (IEC 62439-3 2010: 15):

- 16-bit sequence number (SequenceNr)
- 4-bit LAN identifier (Lan)
- 12-bit frame size (LSDU_size)

The first part of the RCT is the sequence number. This number is the same in the duplicated frames and is the most important parameter in detecting the duplicate. The sequence number is increased every time when LRE sends a frame to certain destination. This way the receiving LRE can recognize the duplicate, as the both frames carry the same sequence number. Because the size of the sequence number is fixed (16 bits), it will wrap to 0 after number of 65535 (Kirrmann 2011: 19).

The second part of the RCT is LAN identifier field. It shows the LAN from which the frame was sent on; LAN A (value 1010) or LAN B (value 1011). This field is used for checking that LANs are correctly installed and connected. This LAN identifier field is the only difference between the duplicated frame pair.

The third part of RCT is the size field. It tells the size of the LSDU (Link Service Data Unit), which is the payload of the frame that carries the real data itself. This field allows the receiving LRE easily identify frames that come from DANPs over frames that are sent by non-redundant ones (SANs). If the receiver detects that this field corresponds to the LSDU size and the LAN identifier matches to the LAN it is attached to, the frame is a candidate for discarding. It is preferable for the receiver is to scan the frames starting from the end. (IEC 62439-3 2010: 15; Kirrmann et al. 2007).

Figure 23 presents the structure of the Ethernet frame including the PRP Redundancy Control Trailer.

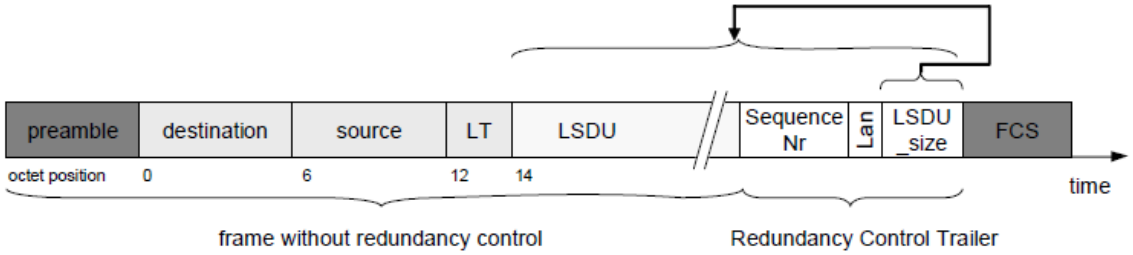


Figure 23. Ethernet frame structure with PRP RCT. (IEC 62439-3 2010: 15).

Ethernet standard specifies a restriction for minimum frame size that can be sent. The frames that are too short to meet this minimum frame size (64 octets) need padding. The sender builds the padding itself and inserts the RCT after it (IEC 62439-3 2010: 16). Figure 24 shows the PRP frame with padding and RCT.

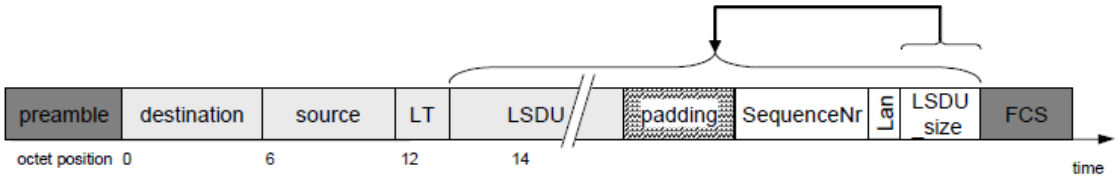


Figure 24. Ethernet frame with padding and PRP RCT. (IEC 62439-3 2010: 16).

The RCT is inserted to the end of the frame. This has the effect that RCT field remains transparent to the application, allowing SANs to understand PRP frames because singly attached nodes do not take into account the octets between the payload (LSDU) and the Frame Check Sequence (FCS); they treat it as padding. (Kirrmann 2011: 16; Kirrmann et al. 2007).

It has to be noted that receiving frame with RCT alone is not sufficient for identifying the source as PRP node (DANP). This is because certain protocols reply with the same frame they received. (IEC 62439-3 2010: 23).

5.2.5 Network management and supervision

The management of PRP network can be done as in the case of any normal LAN. The switches in the LANs are considered as singly attached nodes with one IP address, while the doubly attached end nodes have one MAC and IP address too. The device (e.g. workstation computer) managing the network should be DANP or a SAN attached through RedBox to easily access both networks.

To consider supervision of PRP network, Simple Network Management Protocol (SNMP) can be used. The state of redundancy can also be included in IEC 61850 objects in an IED. (Kirrmann et al. 2007, Kirrmann et al. 2008).

PRP nodes maintain a special 'node table', which they use for PRP communication and network management purposes. This table keeps a record of all other nodes that the node can see in the network. For every node it communicates with, the table records MAC address, node type (SAN or DANP), number of frames received, error counters (e.g. frames received over wrong LAN), last time the node was seen and the current sequence number that the node will use for frame sending, among others. It can be seen that the nodes in the PRP network have another slight "communication protocol" over the link layer as they use node tables for PRP communication. With the help of node tables, the nodes can monitor that the frames come in sequence and come correctly over both LANs as well as keep track of errors. If a node leaves the network, it will be erased from the node table after a time parameter NodeForgetTime, which is 60 seconds by default. When a node sends or receives a frame, the node table is read an updated. For example, if a certain destination (MAC address) of a frame is a SAN, this is seen in the node table, and the frame is sent only on the corresponding port with no RCT. The node table runs on background and needs no interaction from the user, but can be seen and exposed as for diagnostic purposes. (IEC 62439-3 2010: 18–19, 12, 27).

This 'node table' is however not mandatory. The PRP parameters (e.g. port status and error counters can be monitored via IEC 61850 objects, where they belong to a special dataset. A DANP without node table sends all frames appended with RCT over both ports. (IEC 62439-3 2010/Amd1: 21).

For supervision to work, each DANP's LRE periodically sends supervision messages and receives them from the other DANPs in the network. This allows checking the state of the networks and the connection of end nodes. The supervision frame confirms that the sender device is a DANP. It also tells the MAC addresses the device uses, and the PRP mode of the DANP (duplicate discard or duplicate accept). This information is updated to receiving node's node table.

The supervision frame is sent as multicast on every LifeCheckInterval, which is a changeable parameter with default value of 2000 ms. A special address is reserved for the multicast sending. Figure 25 shows the structure of the PRP supervision frame. (IEC 62439-3 2010: 12, 19, 25, 27). Because the supervision frame is not needed for any kind of network switchover, the 2 seconds sending interval is sufficient.

Offset	Length	0 7	8 15
0	6	PRP_DestinationAddress (multicast 01-15-4E-00-01-XX)	
6	6	PRP_SourceAddress (MAC address of the DAN)	
12	2	Type (0x8100 for VLAN)	
14	2	prio | cti	VLAN Identifier
16	2	Type (0x88FB for PRP)	
18	2	PRP_Ver	
20	2	PRP_TLV.Type = 20 or 21	PRP_TLV.Length = 12
22	6	PRP_SourceMacAddressA (MAC address A of the DAN)	
28	6	PRP_SourceMacAddressB (MAC address B of the DAN)	
34	2	PRP_TLV.Type = 30 or 31	PRP_TLV.Length = 6
36	6	PRP_SourceMacAddressA (MAC address A of the RedBox or VDAN)	
42	18	padding to 68 octets	
60	2	SequenceNr	
62	2	LAN = A or B	LSDU_Size = 46
64	4	FCS	

Figure 25. Structure of the PRP supervision frame (with VLAN tag). (Weibel 2008: 10).

Table 6 presents the meanings of the parameters.

Table 6. Parameters of the PRP supervision frame (Weibel 2008: 11).

Parameter		Description
PRP_DestinationAddress		reserved multicast address 01-15-4E-00-01-XX (XX is "00" by default, but if conflicts arise, XX can be configured to take any value between 0x00 and 0xFF)
PRP_SourceAddress		MAC address of the sending node
PRP_Ver		protocol version, set to "0" (zero) for this version of PRP
first PRP_TLV entry (Type, Length, Value)		
	PRP_TLV.Type	indicates the operation mode: Duplicate Discard (value 20) or Duplicate Accept (value 21)
	PRP_SourceMacAddressA PRP_SourceMacAddressB	MAC address used by each port (these addresses are identical, except if address substitution is used)
second PRP_TLV entry (Type, Length, Value), used by RedBoxes only		
	PRP_TLV.Type	indicates whether the supervision frame belongs to a RedBox (value 30) or a VDAN (value 31) Remark: The DAN itself does not send supervision frames, but the corresponding RedBox does it as a proxy on behalf of all VDANs connected to it.
	PRP_SourceMacAddressA	MAC address A used by the respective RedBox or a VDAN
SequenceNr		sequence number used for network supervision frames
LAN		LAN over which this supervision frame is sent
LSDU_Size		size of the LSDU (always 46, independent if tagging is used or not)

If a node does not receive PRP supervision frames form a source, but receives frames from that source over one LAN, the node identifies the source as SAN A or SAN B depending on the LAN it receives frames from. (IEC 62439-3 2010: 23, 27).

During the PRP test network build-up (see Chapter 6.2), it was noticed that the ABB IEDs used IEC 61850 objects to supervise redundancy (the state of ports). The LAN state and error counters can be supervised from the IED (REF542plus).

To form a sufficient supervision of networks, PRP nodes can use the IEC 61850 objects for supervision of ports, while SNMP can be used for supervision of Ethernet switches (also RedBoxes). Combining these two supervision methods will bring a good solution for network supervision. The IEC 62439-3 (2010: 28) states that SNMP can be also used for IED port supervision, which has the effect that one tool can supervise the whole network.

5.2.6 Rules for configuration

The standard IEC 62439-3 (2010: 19–20) presents some configuration guidelines that should be considered during installation and configuration:

- Network must consist of two fail-independent LANs with similar properties, such that one LAN is able to carry all traffic in the occurrence of redundancy.
- Labelling cables and Ethernet switches should be done to easily identify to which LAN a switch or cable belongs. One may use e.g. different colours.
- All DANPs in the network must have the same multicast address for PRP supervision frames as well as the same LifeCheckInterval parameter (time interval for sending supervision frame).
- Both adapters of every DANP shall have the same MAC address. The IP address of every device in the whole network (LAN A and LAN B) must be unique. Because the redundancy is transparent to upper layers, A DANP has always a same IP address whether seen by LAN A or LAN B.
- SANs that need to communicate with each other must be attached to one LAN, or to both LANs through RedBox.

A DANP can however support MAC address substitution, and in that case the MAC addresses can differ. If so, the MAC address of the DANP shall be the address of adapter A, while adapter B can use different MAC address. Address substitution is not specified further in the IEC 62439-3.

Also the connectors of the devices have a rule for labeling. When connectors are situated vertically, the upper one is identified as LAN A and the lower one as LAN B in the normal position. If the connectors are situated horizontally, the left connector is identified as LAN A and the right connector as LAN B (seen from the side where cables are plugged).

There are also additional recommendations in the reference ABB Oy (2011b: 76). For time synchronization, two independent GPS should be used, one for each LAN. Also

both networks should preferably use the same network architecture. As mentioned before, the two LANs must never be interconnected.

PRP is compatible with RSTP and with MRP (IEC 62439-2), so they can be further used inside LANs if seen necessary (Kirrmann et al. 2007). To assure fail-independent operation, the redundant LANs should not be powered from the same power source (Weibel 2008: 3).

5.2.7 PRP summary

The usage of Parallel Redundancy Protocol has many properties and characteristics that are demanded by IEC 61850. First of all, it achieves seamless recovery time, which makes it suitable for time-critical applications (especially IEC 61850 process bus). It tolerates any component failure that can happen in a network while remaining transparent to the application, which brings simplicity for engineering. The LANs can use any topology while allowing the use of singly attached end nodes (though in one LAN only). In addition to IEC 61850, it can be used also with other protocols of Industrial Ethernet.

PRP has however a disadvantage of increasing the costs because of the duplication of the network components. The end nodes also need a second Ethernet controller and a special layer to handle duplicate frames. Still, the Parallel Redundancy Protocol fulfills all requirements of IEC 61850 based substation automation and is thus worth the investment, especially for time-critical traffic's point of view. (Kirrmann et al 2007; Kirrmann et al. 2008).

Figure 26 below presents an example of the usage of PRP in the station bus substation network. The station bus is thus doubled. As seen in the figure, RedBoxes can be used to attach devices with only one port to both networks.

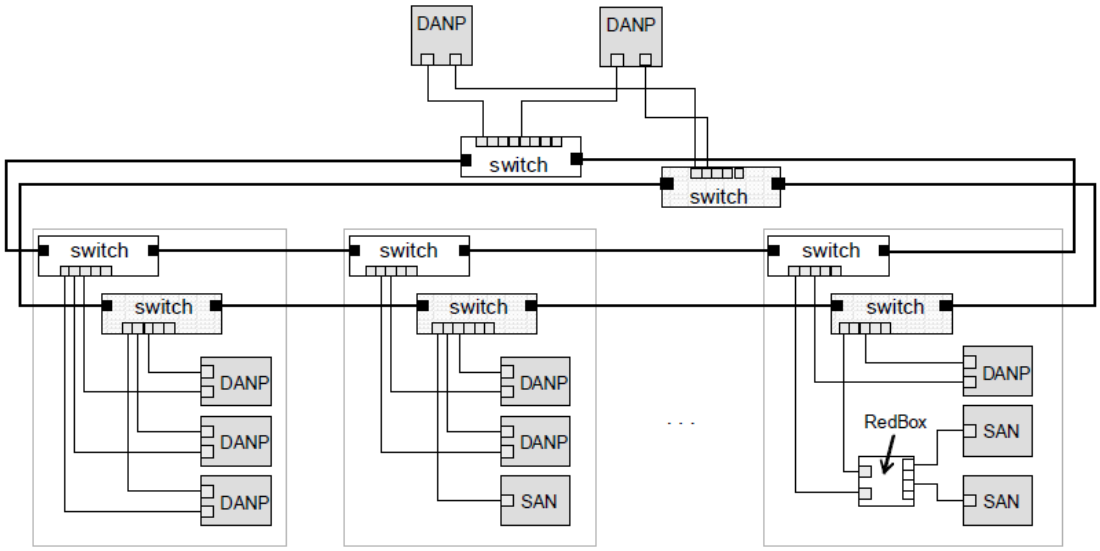


Figure 26. Duplicated station bus with PRP. (IEC 62439-3 2010: 11).

5.3 High-availability Seamless Redundancy (HSR)

The High-availability Seamless Redundancy handles redundancy in the end nodes as well. A HSR node has two ports operated in parallel, as in the case of PRP, but here the node is called **DANH (Doubly Attached Node implementing HSR)**. HSR can be seen as an implementation of PRP in a particular topology of ring and rings of rings. This is why most of the properties of PRP thus apply for HSR.

HSR allows reducing hardware costs because Ethernet switches are not needed in HSR network. Every node in the ring must however be a switching node, having two ports and a hardware integrated switch element, as the IEDs in the ring of IEDs topology (see Chapter 3.3.4). Here, the nodes implement HSR protocol. (ABB Oy 2010a: 60).

5.3.1 Operation principle

Like PRP, HSR uses frame duplication and sending them over different paths. The sending node sends two copies of the same frame through both its ports at the same time in to the ring. Here, the frames travel into opposite directions in the ring. Each node in

the ring forwards the frames except the node that sent that frame, and the node being an unique destination for the frame. Because of the sending node discards the frames it has already sent, the frames do not keep circulating in the ring. Figure 27 shows an example of HSR network.

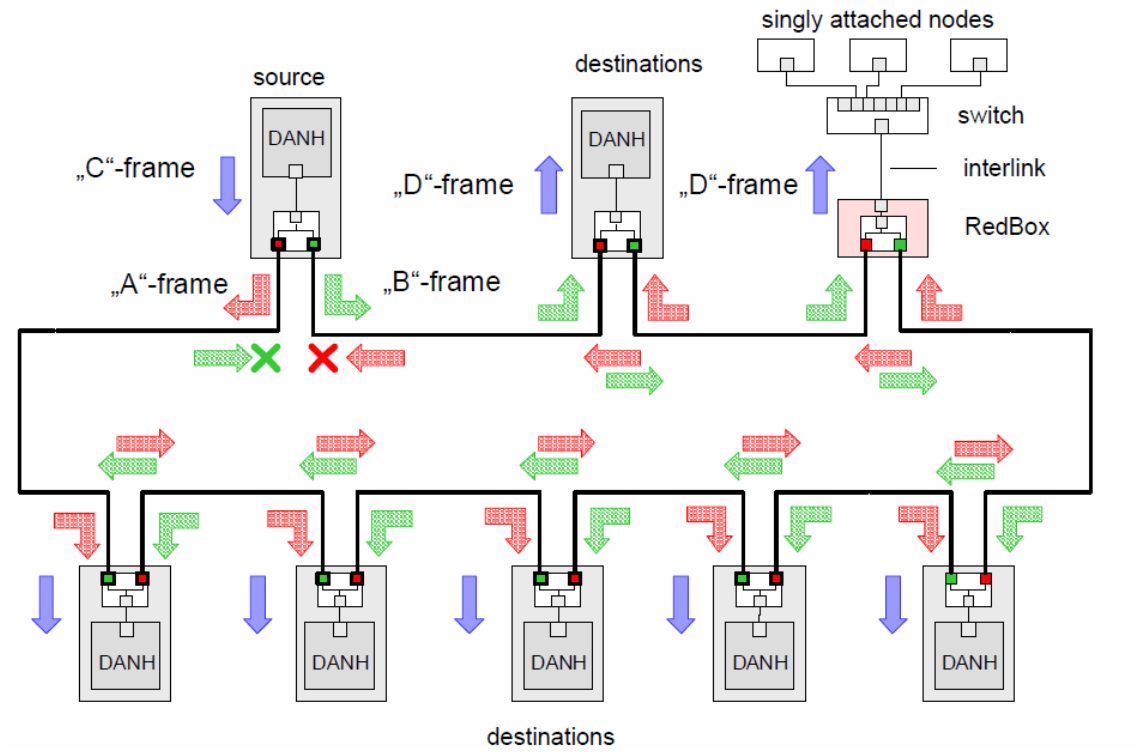


Figure 27. An example of HSR network in ring topology. A source multicasts the frame to every ring participant. (IEC 62439-3 2010: 32).

A destination node receives thus two identical frames, within a certain interval. The first frame is passed to upper layer and the later coming duplicate is discarded. This operation reminds very much that of PRP. To detect duplicates, the frames carry a HSR tag, which is discussed in Chapter 5.3.3.

Unlike in PRP, singly attached nodes cannot be connected straight to the ring, because they have only one port and do not deal with the HSR tag. Therefore, a RedBox is needed, acting as a proxy for the SANs behind it. When using HSR, Ethernet switches are not needed in the ring. A RedBox can also include a switch element for connecting SANs to network.

Because the frames are duplicated and sent to opposite directions, one frame gets through to the destination if a failure occurs and breaks the ring. However, because the source node duplicates the frames, the traffic of the ring is roughly doubled. This should be taken in to account if there are many traffic hungry HSR nodes in the network ring. (IEC 62439-3 2010: 31–32, 34; Kirrmann, Weber, Kleineberg & Weibel 2009).

5.3.2 Node structure

The node structure of a DANH is very similar to the one of DANP (PRP). A DANH has also two Ethernet ports with same MAC and IP addresses and form a single interface to the application, which is thus not aware of HSR. HSR is also layer 2 redundancy protocol and allows other link layer protocols like ARP to operate normally, simplifying engineering.

Figure 28 shows the HSR node structure and operation. The Link Redundancy Entity is also present in HSR node, handling both Ethernet ports and duplicates and presenting a single interface to upper layers, alike in PRP. Because the HSR nodes must also forward the frames, a switching logic is included to the LRE to enable this. (IEC 62439-3 2010: 33; Kirrmann et al. 2009).

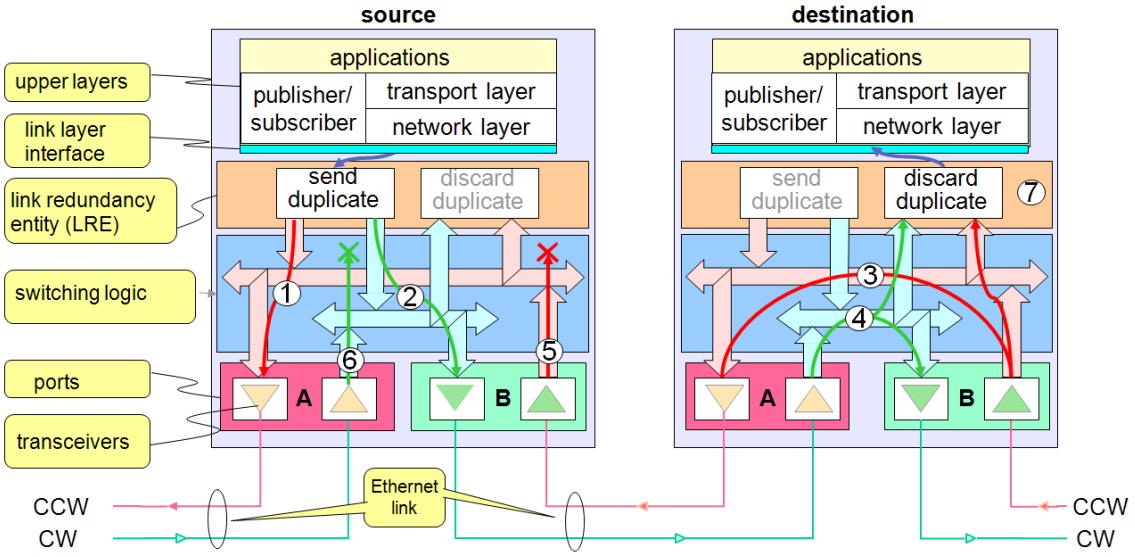


Figure 28. HSR node structure and operation. (Kirrmann 2010: 13).

In the figure, a source node multicasts a frame. The LRE duplicates the frame and sends it over both ports at the same time (1 and 2). The switching logic in the nodes forward the frames from one port to another (3 and 4), but not the own frames the node has sent (5 and 6). In the destination node, the LRE receives both frames (in fault-free operation), consumes the first one and discards the duplicate frame (7). The directions in the figure are clockwise (CW) and counterclockwise (CCW). (Kirrmann 2010: 13).

Alike in PRP, the LRE in the HSR node inserts a special identification called HSR tag to the frame it sends for duplicate identifying. It also sends HSR supervision frames and evaluates them from other HSR nodes in the network. (Kirrmann et al. 2009).

The LRE can forward a frame before receiving it entirely. This is called cut-through mode and it allows reducing the forwarding delay, especially with long frames.

5.3.3 Duplicate frame identification

For duplicate detection, the LRE uses a special six-octet HSR tag inserted to frames right before sending them. On the contrary to RCT in PRP frames, the HSR tag is inserted before the payload of the frame. This allows the cut-through operation introduced above, allowing quicker forwarding of a HSR frame.

The HSR tag consists of four parameters altogether (IEC 62439-3 2010: 48):

- 16-bit Ethertype field
- 4-bit path identifier
- 12-bit frame size (LSDU_size)
- 16-bit sequence number (SequenceNr)

The first part of the HSR tag is the Ethertype field, which identifies a HSR frame. The path field is used to identify different HSR frames (e.g. supervision frames from regular HSR frames). The LSDU size field is defined in the same way as in PRP, informing the size of the HSR tag and the payload of the frame. This field is however not used for

identifying a HSR frame (as it was in the case of PRP) because the Ethertype field does this task. It is however kept as a help for hardware implementation.

A node maintains a sequence number for each destination (MAC address). The sequence number is increased every time when the sending node sends a frame. The LRE detects the duplicate uniquely from source address and sequence number. (Kirrmann et al. 2009; Kirrmann 2010: 8).

Figure 29 below shows the structure of a HSR tagged frame.

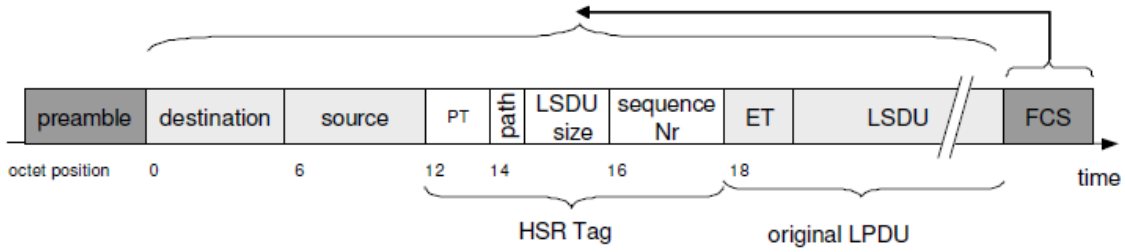


Figure 29. HSR tagged frame. (Kirrmann et al. 2009).

The HSR tag inserted before the payload (LSDU) has the effect that SANs cannot directly understand HSR frames, but it enables the node to forward such frame right after receiving the HSR tag. The forwarding can start after 5 µs at 100 Mbit/s. Thus in a HSR ring of 50 nodes, an end-to-end delay is averagely 125 µs. (Kirrmann et al. 2010).

5.3.4 Network supervision and management

To supervise the network, each DANH's LRE sends HSR supervision frames, similarly in PRP. The HSR supervision frame is sent over both ports on every LifeCheckInterval (2 seconds by default). This time does not need to be shorter, because it is not needed for any switchover, but to check redundancy. The HSR properties (e.g. port status) can be supervised as in PRP (SNMP, IEC 61850 objects).

All in all, HSR network supervision and management works as in the case of PRP. The network management computer can be attached through RedBox. (Kirrmann 2010: 37–38, 40).

5.3.5 Ring coupling

A HSR ring can be coupled to other HSR ring(s). For this, a device called QuadBox is needed. A QuadBox has quadruple ports with ability to forward frames as any other DANH. It passes the frames to the other ring unchanged, but is also able to filter those frames that are not intended to be forwarded to the other ring. For ring coupling, one QuadBox could be sufficient for correct operation of the rings in fault-free state, but two QuadBoxes are needed to defeat a single point of failure. Figure 30 presents an example of ring coupling. (IEC 62439-3 2010: 35).

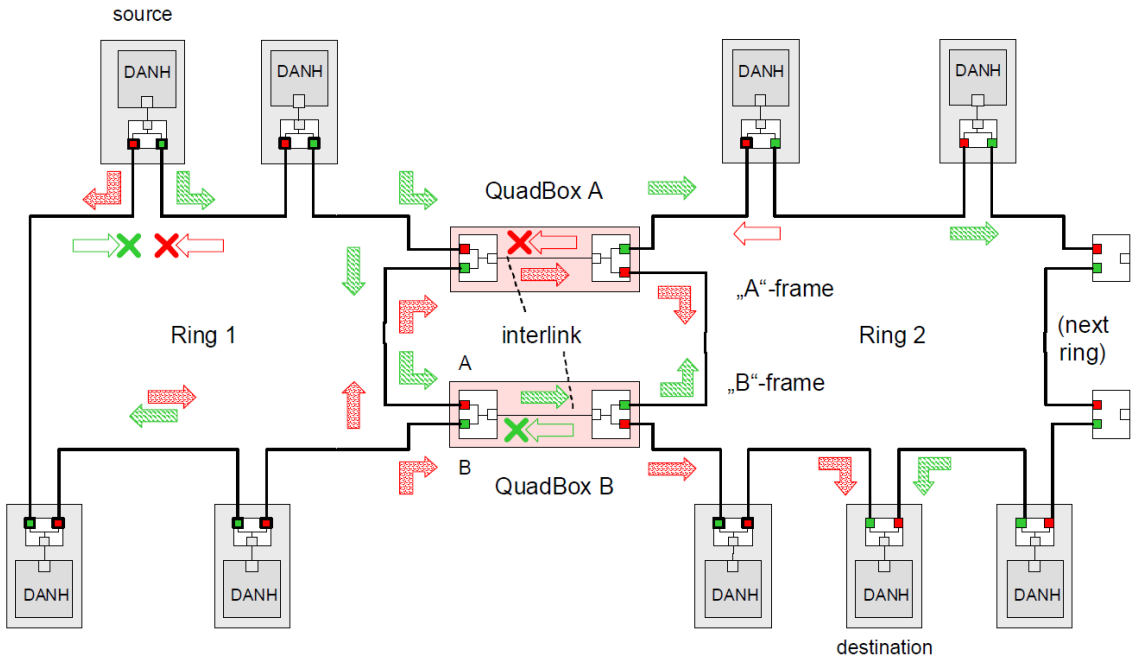


Figure 30. HRS ring coupling example. (IEC 62439-3 2010: 36).

The above figure shows a situation where a frame is sent to a destination that is present in the other ring. Because the ring has two QuadBoxes, the duplicate frames are duplicated as they are transferred to the second ring. However, this does not cause four frames circulating in the second ring, since the second QuadBox will not forward the frame from the other QuadBox, if it has already forwarded the one it received from the other ring. Also, it will not forward the frame coming from other ring if it has already forwarded the duplicate frame sent from the other QuadBox. This operation prevents duplication of the duplicates.

The QuadBox can be constructed of two RedBoxes. This has the effect that if one RedBox fails, the other ring remains fully redundant. (IEC 62439-3 2010: 35).

HSR rings can be formed hierarchically keeping the substation network in mind, e.g. station level devices have their own ring and every bay, substation building or voltage level have their own ring for IEDs. (IEC 62439-3 2010: 36–37; Kirrmann et al. 2009).

5.3.6 HSR summary

High-availability Seamless Redundancy is a protocol reusing many principles of the Parallel Redundancy Protocol. It also has many properties fulfilling the demanding requirements of IEC 61850, e.g. the seamless recovery time, making it suitable for time-critical processes. It also tolerates any single component failure and is transparent to the application, which brings simplicity for engineering. HSR can be used also with other protocols of Industrial Ethernet in addition to IEC 61850. The costs are reduced because of the embedded switches in IEDs; no Ethernet switches are needed in HSR ring. It is compatible with PRP and complements it.

However, HSR has also a disadvantage of reducing available bandwidth in a ring, especially for multicast messages. It also needs hardware implementation (switching logic for frame forwarding). Furthermore, devices with one port have to be attached through RedBox, because the HSR ring does not allow non-HSR traffic in principle. (Kirrmann 2010: 39, 43; Kirrmann et al. 2009).

Figure 31 shows an example of the usage of HSR in the station bus. The IEDs are formed in rings depending on the voltage level and the ring coupling is done using QuadBoxes.

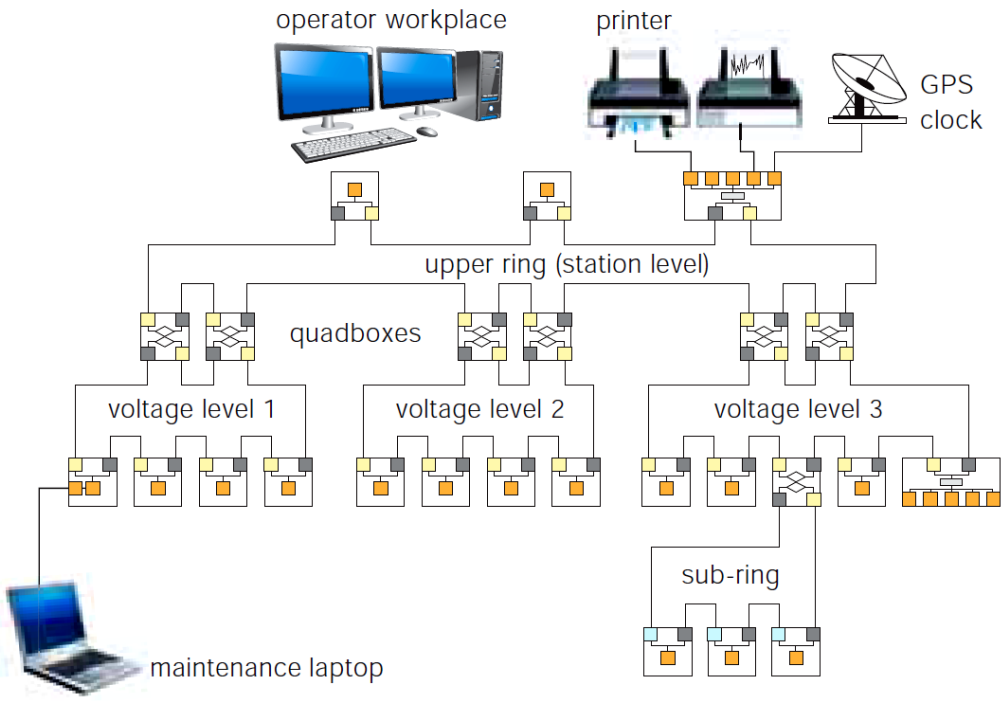


Figure 31. Station bus with HSR rings of rings. (ABB Oy 2010a: 61).

5.4 IEC 62439-3 Amendment 1

At the moment, there are pending modifications to the IEC 62439-3 standard. An amendment to the standard IEC 62439-3 is about to be published. Since the protocols specified in this part of the standard were adopted by IEC 61850, changes became necessary, such as clarifications of specifications (also slackening for them to allow various implementations), simplifying implementations and consideration for time synchronization with IEEE 1588. These changes are already being implemented in development projects, and the amendment specifies them to secure interoperability. (IEC 62439-3 2010/Amd1: 6).

The amendment also presents new version of PRP called PRP-1 while the present one is called PRP-0. The main advantage in PRP-1 is the fact that it allows better support for the PRP and HSR network coupling. However, the PRP-1 differs from the original PRP in the area of Redundancy Control Trailer. In addition to fields that were found in the

PRP-0, PRP-1 adds a 16 bit suffix after the LSDU size field, as seen in the Figure 32. The size of RCT is thus grown to 6 octets. The PRP-1 suffix is not calculated to the LSDU size field. (IEC 62439-3 2010/Amd1: 13–14).

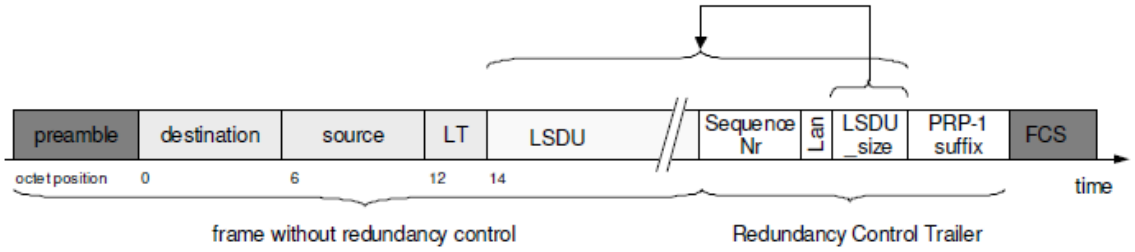


Figure 32. PRP-1 frame with RCT. (IEC 62439-3 2010/Amd1: 13).

The sequence number handling differs also from PRP-0. While PRP-0 increases the sequence number for each frame sent to a certain destination, PRP-1 increases the sequence number for each frame sent, not taken the destination into account. This allows connecting PRP and HSR networks with redundant connection points.

The PRP-1 suffix identifies the usage of PRP-1 frames, along with the frame size. A network is however assumed to be configured homogeneously to include nodes either as PRP-0 or as PRP-1. Supervision frames can be used to check correct configuration, since they carry the info of the PRP version. (IEC 62439-3 2010/Amd1: 14, 18).

Because of the pending amendment, most manufacturers have not yet released HSR products at all since they are waiting the latest IEC 62439-3 paper. The draft for the amendment can be expected to obtain the status of International Standard not earlier than in the end of 2011. For example, RuggedCom HSR products (RedBox) are planned to be released in the first or second quarter of 2012. This is also true for PRP RedBox. (Grendar 2011).

The first ABB IEDs with HSR implementation can be expected to be released on the market in 2012.

5.5 Common properties for seamless redundancy protocols

The standard IEC 62439-3 (2010: 13, 27, 51) presents that every doubly attached node (with switching logic) can be configured to use any of the following redundancy protocols: Reduced RSTP (no designated port role), RSTP, MRP, PRP or HSR. This allows devices e.g. IEDs to support new seamless redundancy protocols but also single LAN redundancy protocols. This provides that the same IED can be used for any level and topology for redundancy, and is thus very flexible to use and configure in different applications. The IEC 62439 presents a special MAC address substitution mode, where the two ports of a node can have different MAC addresses, which allows the connection of the ports to a single LAN.

For the upcoming ABB IEDs, the integrated switch module's mode of redundancy can be chosen between PRP and HSR. It provides a third port for debugging/maintenance, but this port can be also used to attach a SAN to redundant network. The IED can thus act as a simplified RedBox. (Suomi 2011).

The PRP can be implemented in software, but HSR should be preferably implemented in hardware because of the frame forwarding tasks (switching logic). What comes to the time synchronization, both the protocols already support the high precise time synchronization protocol IEEE 1588 PTP. (ABB Oy 2010a: 61; Kirrmann et al. 2009).

5.5.1 Redundancy box (RedBox)

Generally, the RedBox is needed for connecting singly attached nodes to redundant PRP and HSR networks. It has at least three ports; two of them connected to the redundant networks and one to an interlink (connection to the SAN). One or more SANs can be attached to RedBox, which acts as a proxy for them, making the transition from the single LAN to double LAN and vice versa. The SANs behind RedBox appear as Virtual Doubly Attached Nodes (VDAN), and the RedBoxes send supervision frames to the redundant networks on behalf of the SANs, appending also its own information to the frame (see Chapter 5.2.5). (IEC 62439-3 2010: 13).

A RedBox has a LRE as any other DANP or DANH. It has also an own IP address for management and possible local applications. The IEC 62439-3 (2010: 13; 44) divides the RedBoxes to PRP RedBox and to HSR RedBox, which has many operation modes. The standard does not tell if one physical RedBox can be configured to PRP or HSR mode, or if they must be totally different devices.

Figure 33 shows the structure of a HSR RedBox, where the LRE includes also the switching logic as any DANH. A RedBox can also include a switch, and in that case, the interlink is an inside connection as seen in the Figure 33 below.

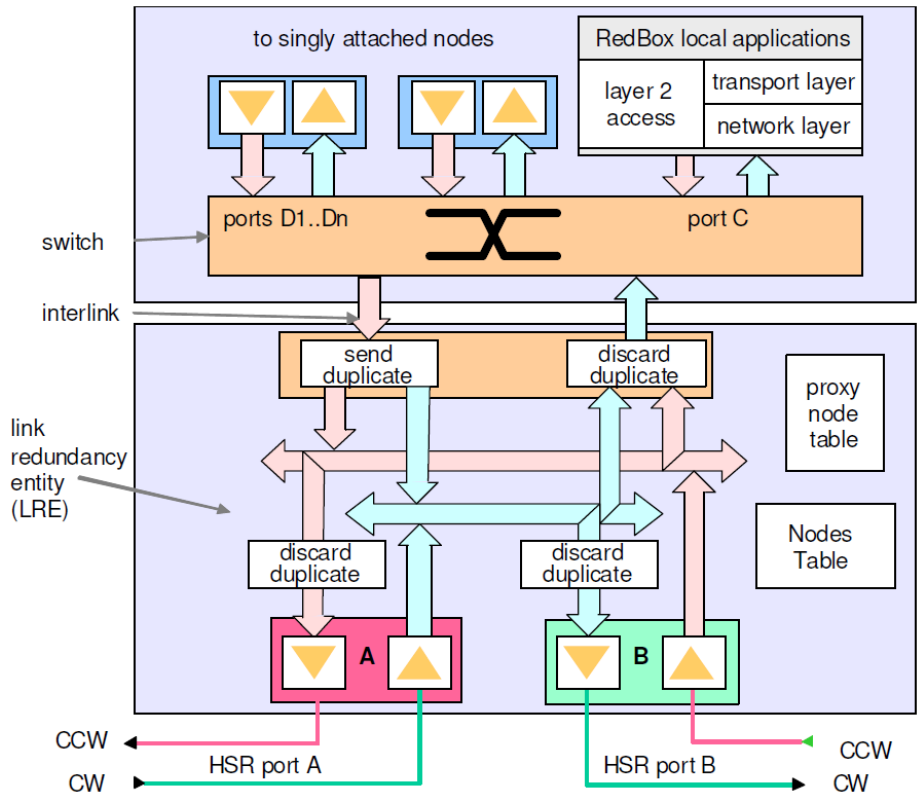


Figure 33. Structure of a RedBox (Redundancy box) for HSR network. (IEC 62439-3 2010: 40).

A RedBox maintains a nodes table as any other node. In addition, it keeps a proxy node table, which contains the entries behind it (MAC addresses of the SANs). (IEC 62439-3 2010: 48).

A HSR RedBox can be configured to three modes, which differ in the area of interlink traffic (IEC 62439-3 2010: 44):

- HSR-SAN, where the interlink carries untagged frames. This mode is used for connecting a SAN to HSR network.
- HSR-PRP, where interlink carries PRP tagged (A or B) frames. This mode is used for connecting different PRP and HSR networks. See Chapter 5.4.3.
- HSR-HSR, where interlink carries HSR tagged frames. This mode is used for HSR ring coupling, where the RedBox operates as a half of QuadBox. See Chapter 5.3.5.

5.5.2 Connecting PRP and HSR networks

Different HSR and PRP networks can be coupled together via two separate RedBoxes. The RedBoxes are configured to handle HSR traffic in the two ports, and PRP traffic on the interlink. The coupling can be done only with PRP-1 and HSR.

As a frame transits from network to other, the sequence number of RCT of the PRP-1 frame is reused for the HSR tag and vice versa. This supports the frame identification from a network to other and duplicate identification in the HSR ring as the two RedBoxes inject the same frame to the ring. Figure 34 presents an example of connecting HSR and PRP rings together. In the Figure, a PRP source sends a frame to destination node in the HSR ring. (IEC 62439-3 2010/Amd1: 37).

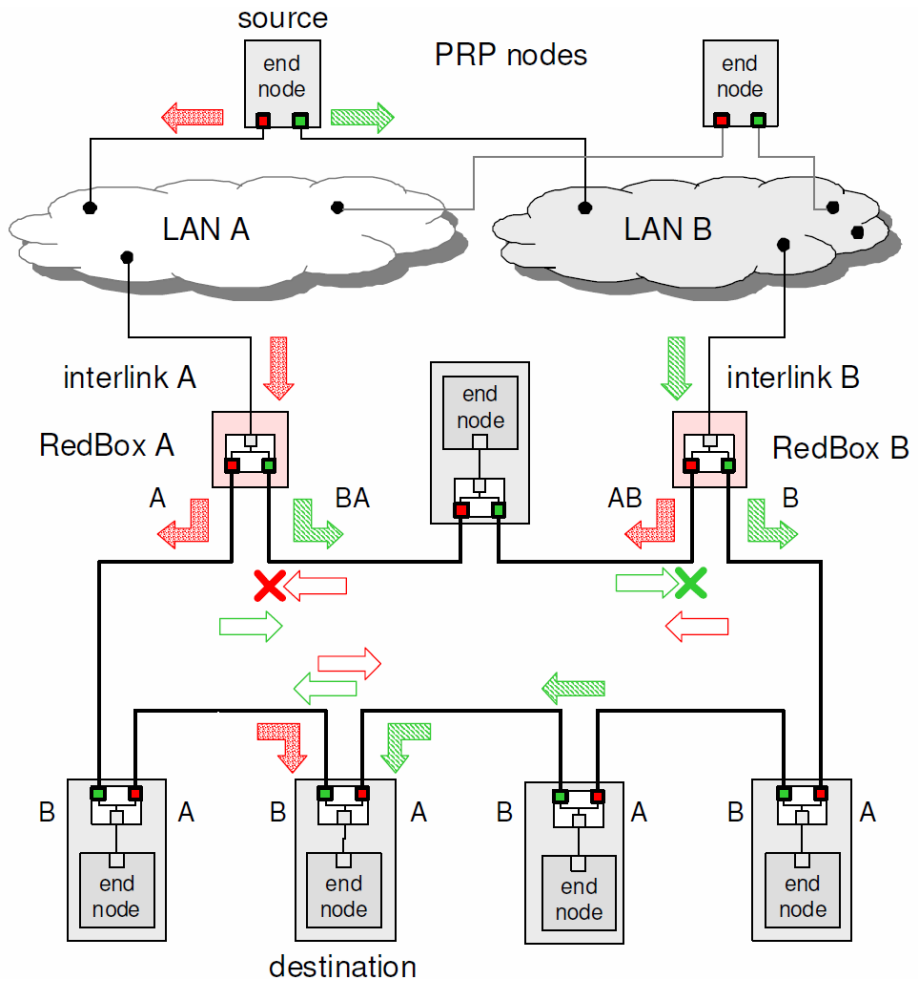


Figure 34. Connecting PRP and HSR networks. (IEC 62439-3 2010: 38).

The two RedBoxes are configured as RedBox A or RedBox B as the figure above shows to accept PRP frames on the interlink, and to tag the correct LAN identification if the sender is in the ring. The two RedBoxes would duplicate the frames as the frame is injected to the ring (frames BA and AB), but does not if the RedBox receives the frame before sending it itself. For example, if the RedBox A receives the AB frame before sending the A frame, it will not send it. On the contrary, if the RedBox B does not receive the frame A from Redbox A, it will generate the frame AB. Multicast frames are removed from the ring by the RedBox that forwarded them to the ring.

It can be seen that the RedBoxes convert the PRP frames to HSR frames and vice versa, keeping the frame duplicates still identified with the help of the reused sequence

number. Thus, the different HSR and PRP networks can be coupled together. (IEC 62439-3 2010: 38–39).

5.6 Comparison of the redundancy protocols PRP, HSR, RSTP and MRP

The seamless redundancy protocols standardized in IEC 62439-3 fulfill the high availability requirements of a modern IEC 61850 based substation. Along with RSTP, they can be used as redundancy protocol on their own or they all can be combined in a substation communication network. Table 7 below presents a comparison of these redundancy protocols and their performance. The Media Redundancy Protocol (a competitor of RSTP in ring topology) is also included to comparison for interest.

Table 7. Comparison of redundancy protocols for substation automation: PRP, HSR, MRP and RSTP. (IEC 61439-1: 23; DesRuisseaux 2009; Dreher 2011, Kirrmann 2010; Kirrmann 2011).

Property	RSTP	MRP	PRP	HSR
Standardization	IEEE 802.1D	IEC 62439-2	IEC 62439-3	IEC 62439-3
Frame loss during network failure	Yes	Yes	No	No
Redundancy handling	In the network	In the network	In the end nodes	In the end nodes
End node attachment	Single	Single	Double	Double
Network Topology	Ring, meshed	Ring	Any (2 separate LANs)	Ring, meshed
Recovery time	About 5 ms per switch in ring topology (depends on implementation)	500 ms, 200 ms, 30 ms or 10 ms worst case	Seamless (0 s.)	Seamless (0 s.)
Costs considerations	No additional costs, protocol is included in Ethernet switches	No additional costs, protocol is included in Ethernet switches	Double amount of Ethernet switches and other network equipment. Needs support from end nodes	Few additional links, but does not need Ethernet switches. Needs support from end nodes
Supports RSTP/MRP	RSTP	MRP	Yes	Yes
Connection of SANs	SANs only	SANs only	Only to other LAN or through RedBox	Only through RedBox
Maximum switch/node number	40	50	Not defined by the protocol	Not defined by the protocol, depends however on the ring traffic
License fee for implementation	Free of charge	Yes	Free of charge	Free of charge
Referenced by IEC 61850	Yes	No	Yes	Yes

As seen from the above table, the protocols are needed for different purposes. Only PRP and HSR can provide seamless recovery with no frame loss during failure, because they handle the redundancy in the doubly attached end nodes. They are a good choice for applications that cannot tolerate any network recovery delay. For a single ring topology, the present and most used redundancy protocol RSTP has a new competitor MRP,

which can provide better recovery times that are nearly independent of the amount of switches in the ring topology. Especially, the 10/30 ms recovery time is a good reason to choose MRP over RSTP. MRP standard is however owned by Hirschmann and Siemens (Hiper-ring) and has a license fee, which may cause that other Ethernet switch manufacturers do not want to implement it to their own products. (Dreher 2011; Grendar 2011). Furthermore, IEC 61850 mentions only PRP-1, HSR and RSTP for link layer redundancy of station and process bus.

It is worth mentioning that HSR and PRP can tolerate any network component (e.g. cable and Ethernet switch) failure because the message is sent over two different paths.

An appropriate question would be when to use a specific protocol and whether the gain in system availability is worth the costs invested in a high-availability redundancy protocol.

Hoga (2010a, 2010b) states that if a substation automation network carries only client-server communication (TCP/IP traffic with MMS), the RSTP and MRP are totally sufficient redundancy protocols to use. TCP/IP traffic is not considered time critical and it has a mechanism that will repeat the lost frames. When the GOOSE messages (interlocking, trip) are used, the system gets more critical. However, because of the retransmission mode of GOOSE, the time critical message does not necessarily get lost during network recovery. Furthermore, Hoga (2010a) calculated a probability for a situation where network is down during a time critical situation (e.g. GOOSE message). It states that if a network recovers once a year, the recovery time is 100 ms and the time critical event happens 50 times a year, the probability for such situation is 1:6.3 million per year, and is thus very minimal.

PRP and HSR provide an additional level to redundancy, which can be used at the same level as RSTP and MRP, but are especially required in the applications regarding to IEC 61850-9-2 Process bus (see Chapter 2.2.5). The seamless recovery is a requirement in the process bus because of the Sampled Values. Sampled Values is time-critical traffic like GOOSE messages, but does not have retransmission scheme; it is continuous stream of samples (see Chapter 2.2.3). During network reconfiguration, an IED

experiences a measuring blackout, which affects negatively to the protection. This is why seamless redundancy protocols are needed in the process bus. Also busbar protection requires seamless recover time (see Table 5 on page 53). (Hoga 2010b).

The network designer should determine which level of redundancy is needed for the substation network required by the application. The minimum level is RSTP, which is easily and effectively introduced in ring configuration. One must however verify the effect of different transmission speeds and port types on recovery time of RSTP network (see Chapter 4.1.2). PRP and HSR are to be used in the process bus applications, but are also reasonable to use in station bus if it carries much time critical traffic, or if an Ethernet switch failure must be tolerated. The comparison of IEC 62439 redundancy protocols is shown in Appendix 1 as a whole.

Figure 35 below shows an informative example how the IEC 61850 referenced redundancy protocols can be used and combined in a substation automation system. The station bus uses PRP combined with RSTP in both LANs. The bays use HSR or PRP depending on the case. As seen, the usage of the redundancy protocols can be very flexible.

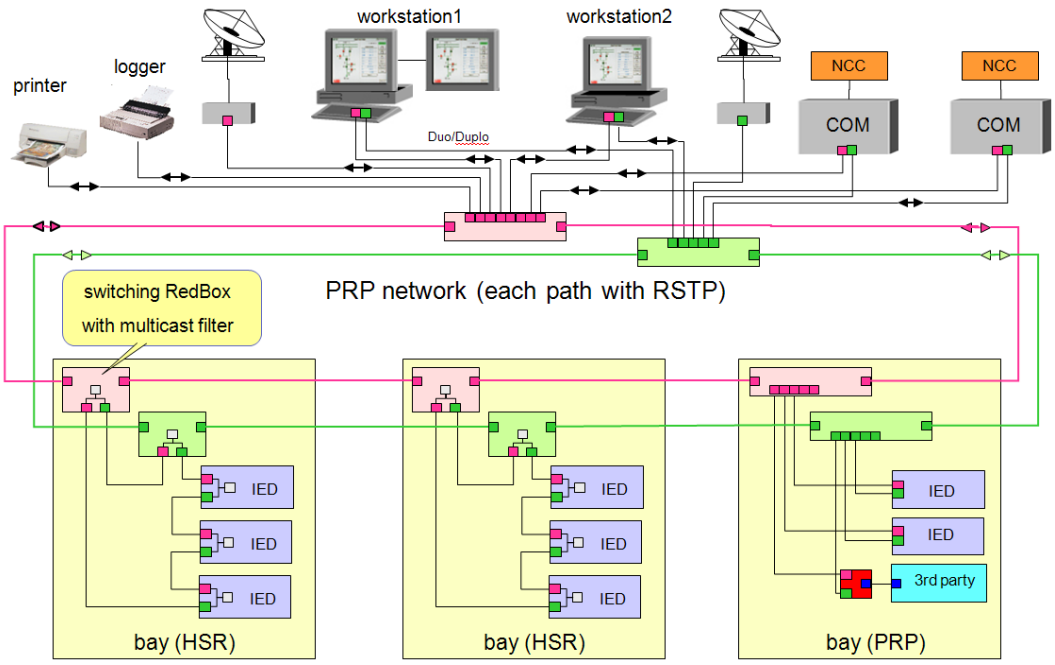


Figure 35. Mixing the IEC 61850 redundancy protocols. (Kirrmann 2010: 26).

6 TESTING PARALLEL REDUNDANCY PROTOCOL

At the moment, the current version of PRP is supported in the following ABB devices available on the market: Protection relay REF542plus, Station gateway COM600 as well as Relion® 670 series IEDs. Still, neither there are devices at the moment that support HSR on the market nor there are RedBoxes. These are however expected to be released in the very near future, as the amendment to the standard IEC 62439-3 gets official.

The two ports in COM600 can be used either in PRP mode or, in the case of only one network, with Intel teaming mode Switch Fault Tolerance, where the two ports are connected to two different switches to tolerate switch failure. The two ports of REF542plus, however, only allow PRP mode. The mechanism that handles the two-port redundancy and duplicates according to IEC 62439-3 is called DuoDriver in ABB devices. It plays the role of Link Redundancy Entity -layer (LRE) described in Chapter 5.2.2 and in addition to IEDs, it can be installed to any computer with suitable network interface card (NIC).

At the very beginning of writing this thesis, it was decided to test the Parallel Redundancy Protocol with ABB devices and MicroSCADA. The test was made to confirm

- if the operation is accordant with the IEC 62439 standard,
- if the commitments of the standard apply in real world and
- what must be taken into account when building and configuring a substation automation system with MicroSCADA and IEDs using Parallel Redundancy Protocol.

The test setup that was built and the test procedure of the PRP system along with a brief description of MicroSCADA are presented in the following parts of this chapter.

6.1 Test procedure preparation

The setup for testing PRP consisted of two separate MicroSCADA computers, two doubly attached REF 542plus protection relays and two singly attached Relion® 630 series protection relays (REF630 and REM630) along with two Ethernet switches and one analyzer computer. The two computers were configured to Hot Stand-By (HSB) mode to make the MicroSCADA redundant as well, which is a common solution in substation automation systems. Figure 36 below shows the lay-out of the test setup.

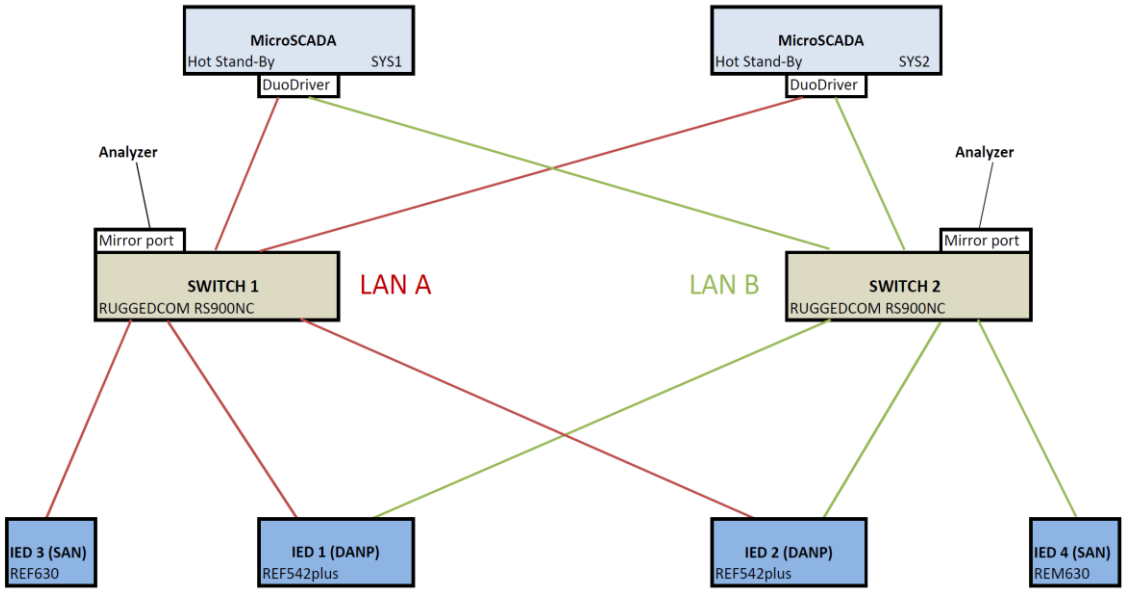


Figure 36. Lay-out of the setup for the PRP test. LAN A is shown with red and LAN B with green colour.

In a HSB system, the MicroSCADA applications are made redundant i.e. there is always a pair of applications connected in Hot Stand-By mode. One application is active (hot) receiving and processing the data from the process, also managing the process displays. While being hot, the application shadows all data (e.g. process, configuration) to the stand-by application situated in the other computer. This way the stand-by application is always in the same state as the hot application and ready to take over the process communication if the computer with the hot application fails. If so, the switchover happens rapidly and the state of stand-by application changes to hot, thus allowing the process to be supervised and controllable in the event of computer failure.

The MicroSCADA computers with HSB mode can be seen as a redundant end node in the network. (ABB Oy 2010d: 29–30).

6.1.1 MicroSCADA

MicroSCADA is a supervision software, which allows real-time monitoring and control of primary and secondary equipment of the transmission and distribution substations. It is designed mainly for substation automation and network control applications, but the application area covers also non-electrical applications like district heating, oil and gas distribution etc. At the writing moment of this thesis, the latest version of MicroSCADA is SYS 600 9.3 Feature Pack 1. The main components of a MicroSCADA system hardware are system servers, communication servers, workstations, peripheral equipment (printers, GPS clocks etc.), communication equipment (switches, routers, modems) together with IEDs, RTUs and other process devices (ABB Oy 2010d: 13).

MicroSCADA supports a variety of communication protocols including IEC 60870-5-101, -103 -104, DNP, Modbus, LON, SPA and IEC 61850 among others. To communicate with the process, a communication link is formed between the system server SYS 600 and process devices, e.g. IEDs and RTUs. Each protocol comes with its own individual characteristics as well as own physical media and interfaces, which has to be taken into account when using such protocol. A communication unit forms a software interface in SYS 600, which is protocol dependent. The most common communication units are PC-NET, which is used with most legacy protocols and IEC 61850 OPC Server/External OPC DA Client, which is used with IEC 61850. Usually SYS600, IEC 61850 OPC Server and OPC DA Client are all located in the same computer. The components of an IEC 61850 based system with MicroSCADA are shown in the Appendix 2.

The OPC (OLE for Process Control) is a de-facto standard which allows connecting various systems and devices to the automation system. It is increasingly used within the area of power industry. It defines the data exchange between servers and clients. SYS 600 allows full OPC connectivity and can act both as a server and a client. (ABB Oy 2010d: 18, 31).

The objects of the MicroSCADA system can be divided to **system objects**, which are used to configure and manage the components of the system, and to **application objects**, which define the application behavior.

Each and every station (e.g. IED), printer, system node (e.g. base system, PC-NET) and application has a system object, which has many attributes used for monitoring and configure the system. The most important system object types are System, Application, Link, Node, Station, Printer and Monitor. (ABB Oy 2010d: 16).

The applications in MicroSCADA have certain tasks. For example, an application can supervise power distribution or heat distribution. Different applications can also communicate with each other. Application objects related to application perform various tasks and are programmable. The most important application objects are presented in the table below with a brief description.

Table 8. MicroSCADA application objects. (ABB Oy 2010d: 17).

Application object	SCIL identification	Description
Process objects	P	Represent the connected process signals, store and supervise the real-time state of the process
Event handling objects	H	Specify the texts in relation to process objects as well as between state transistions (events)
Scales	X	Used for scaling the data sent by stations to real values of the measured entity
Data objects	D	Register and store data (calculated or sampled)
Command procedures	C	SCIL programs, executed automatically or manually
Time channels	T	Used for automatic time based control of data registerations and program executions
Event channels	A	Used for automatic event based data registerations and program executions

A great role in the MicroSCADA is played by programming language SCIL (Supervisory Control Implementation Language). All system and application objects are created and managed by SCIL. Also every supervision and control task is executed by SCIL programs, usually hidden from the user. It can also be used to generate new applications and dialogs to the user interface.

The MicroSCADA system has two databases, where most of the application objects are stored. The databases are **process database**, which contains process objects, event handling objects and scales and **report database**, which contains data objects, command procedures, time channels and event channels. (ABB Oy 2010d: 17).

6.1.2 Test equipment

What comes to the test material, the following table presents the hardware and software needed for the test setup in detail.

Table 9. Hardware (a) and software (b) used in the test procedure.

(a)

Hardware
2 x test computers
2 x Intel Pro 1000 MT Dual Port Network interface cards
2 x REF542plus protection relays
1 x REF630 protection relay
1 x REM630 protection relay
2 x RuggedCom RS900 Ethernet switches
1 x Sverker 650 Relay Test Unit
DC power sources
Analyzer computer
D-Link DUB-E100 USB-Ethernet NIC

(b)

Software
Windows XP Service Pack 2
ABB MicroSCADA Pro 9.3 Feature Pack 1 with Hotfix 2
DuoDriver (version 2.4.27077) (*)
IEC 61850 OPC Server (*)
External OPC DA Client (*)
Wireshark Network Analyzer (version 1.6.1)
ITT600 Network Analyzer (version 1.6.0.1)
Engineering tools for IEDs
(*) = Included in MicroSCADA installation

All the software listed in the table above (excluding engineering tools and ITT600) was installed in both test computers. The IEC 61850 OPC Server and External OPC DA Client are needed for IEC 61850 communication. The dual port Intel NICs are needed for DuoDriver (also quad port NICs can be used) because DuoDriver does not work with separate NICs. The Sverker 650 Relay Test Unit was used to generate a current measurement for the two REF542plus protection relays to create MMS traffic in both LANs. Finally, a separate analyzer computer was used to analyze traffic in the network(s) with both network analyzer programs and via switch port mirroring. Table 10 shows the IP addresses of the devices used in the network and node types according to Parallel Redundancy Protocol.

Table 10. IP addresses and node types of the devices in the test network.

Device	Address	Node type
MicroSCADA computer 1	192.168.2.1	DANP
MicroSCADA computer 2	192.168.2.2	DANP
Analyzer computer		
- NIC 1 (Ethernet NIC)	192.168.2.3	SAN
- NIC 2 (USB Ethernet adapter)	192.168.2.4	SAN
Ethernet Switch 1	192.168.2.11	SAN
Ethernet Switch 2	192.168.2.12	SAN
REF542plus Protection relay 1	192.168.2.21	DANP
REF542plus Protection relay 2	192.168.2.22	DANP
REF630 Protection relay	192.168.2.23	SAN
REM630 Protection relay	192.168.2.24	SAN

The two NICs of the analyzer computer were used independently to capture traffic from both network switches at the same time by using two instances of the analyzer program in certain tests. The analyzer computer's integrated Ethernet NIC was used together with D-Link USB Ethernet adapter for this purpose.

6.1.3 PRP properties of the MicroSCADA computer

The PRP functionality can be implemented to MicroSCADA computer with a compatible NIC by installing the DuoDriver software driver. This driver manages the two ports of the NIC and allows them operate according to the PRP specification, acting as the LRE layer (see Chapter 5.2.2). The installation package is included in MicroSCADA, and should be installed right after MicroSCADA installation.

The DuoDriver offers a separate management and configuration GUI (Graphical User Interface) for supervision and management of PRP after the installation, shown in Figure 37. It has frame counters for both adapters, including error rate, frames sent, frames received etc. and shows also status information of the ports as well as MAC addresses of the ports and PRP supervision multicast address. The information that the frame counters provide is needed if a network is incorrectly configured (especially the counter 'Duo frames received on wrong line') or if one will need deeper analysis of the traffic through the DuoDriver. These counters are useful for network debugging.

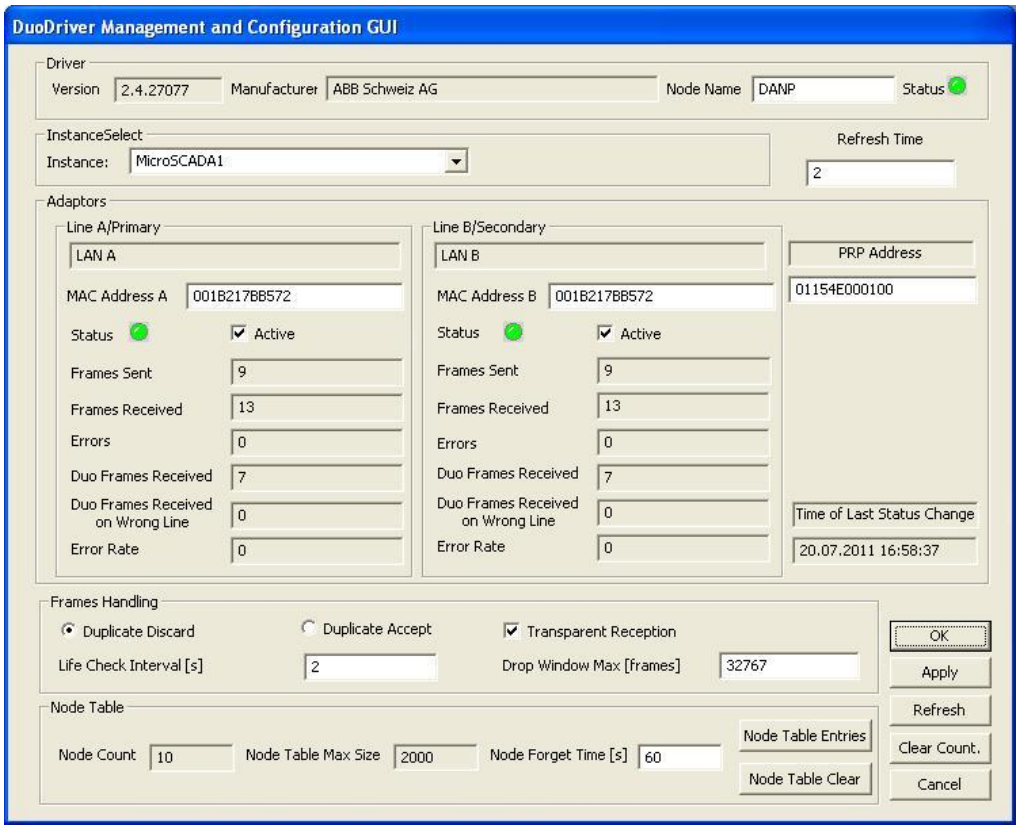


Figure 37. DuoDriver management interface.

For management, duplicate accept mode can also be chosen if necessary and the sending time interval of the supervision frame can be adjusted (Life Check Interval). The 'Drop Window Max' value is the maximum gap of sequence numbers related to duplicate discarding. Usually the default values are fairly usable for the configuration. The transparent reception enables PRP frame analyzing in the MicroSCADA computers, since it does not remove the RCT from the received frames when set on. The node tables of the current node can also be viewed from the GUI.

The DuoDriver information of the local computer is available through the OPC Server, which obtains the values from the DuoDriver and needs no special configuration. The status information is available via OPC attributes (Attributes\DuoDriver\'Instance name'\'LAN name'\Working) and can be mapped to MicroSCADA process objects through the OPC DA Client. Also the 'error rate' counter can be mapped if needed. The IEC 61850 OPC server updates the status information of the ports from the driver every

five seconds. Appendix 3 shows more details of DuoDriver status mapping and sending between HSB computers.

6.1.4 PRP properties of protection IED REF542plus

When planning to use PRP with REF542plus, it must be taken care of that the device is equipped with a dual port Ethernet board. In the REF542plus configuration tool, the topology of the ports must be set to Dual Channel in Ethernet Board parameters section to enable dual port operation.

The DuoDriver of REF542plus is not configurable and provides less information than the one installed to computer. The DuoDriver information of the device is found as IEC 61850 object under the logical node LPHD in the data object SrcSt (LD0.LPHD1.SrcSt in the test configuration), which is included in dataset StatIed. It provides two Boolean data attributes that describe the status of the DuoDriver (port status): stValA and stValB. It also manages error rate counters for both ports via attributes errRateA and errRateB, respectively. These attributes however provide enough information to supervise the DuoDriver state and to check if the network is configured correctly. The attributes and their values can be also viewed in the HMI of the IED itself. Other DuoDriver settings are default and not changeable, e.g. the duplicate discard mode is always used and the supervision frame sending interval is 2 seconds.

The IED DuoDriver status is available through OPC and can be mapped to MicroSCADA application with little effort. The data object ‘SrcSt’ must however be present in the IED configuration file.

6.1.5 Test network configuration notes

The installation of test setup began with installing the DuoDriver v. 2.4.27077 to both MicroSCADA computers after MicroSCADA setup. In the installation, the pairing of the network interface cards (NICs) was made. After the installation, it is good to make sure that the driver works properly. This can be easily made by continuously pinging a DANP while disconnecting one network at time. The driver and network behaves

correctly if the ping gets a continuous response. Ping itself is an ICMP (Internet Control Message Protocol) utility to test connection of a device on IP network. It sends an echo request to the target address and waits for reply, measuring also the time passed.

When the network is considered to be ready, it should be checked from the management GUI that the error counters do not keep increasing. If they do, it is a sign of an error in network configuration e.g. attachment of a port to a wrong LAN. Also the REF542plus maintain error counters. Nevertheless, if a device is attached wrongly to the network, it will not stop communicating; it will only increase the error counters. All devices should be correctly connected to the network for reliable supervision and network consistency. Because MicroSCADA can recognize the installed DuoDriver, it is worthwhile to install the DuoDriver before starting to build application.

MicroSCADA 9.3 Feature Pack 1 with Hotfix 2 was installed to both test computers. The test setup and application building is not documented further in this thesis, but engineering process with REF542plus and IEC 61850 can be found in the Appendix 2.

When using HSB setup with IEC 61850, both the computers have the OPC Server and OPC DA Client installed and running as shown in Figure 38. The IEDs can send their events to both HSB computers, although the supervising application is hot in only one of them. The latest data of the IEDs is thus available for both the OPC Servers.

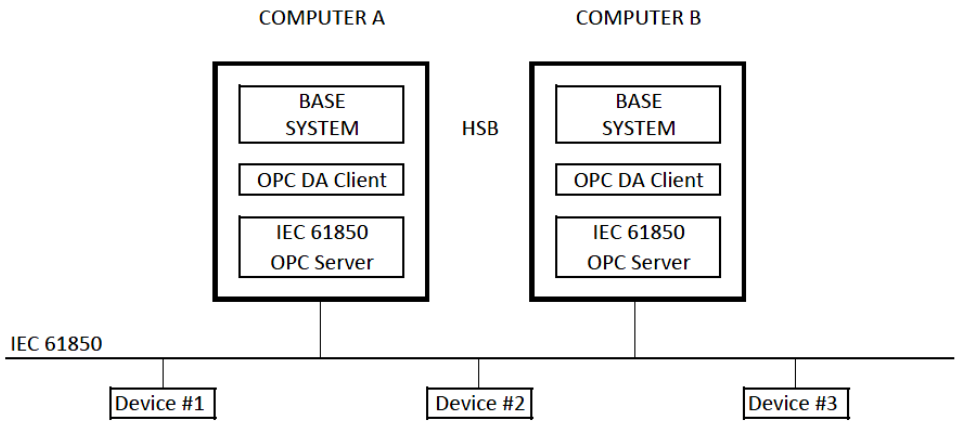


Figure 38. Principle of redundant (HSB) MicroSCADA system topology with IEC 61850. (ABB Oy 2010e: 47).

In the test setup, time synchronization was done so that SYS1 was configured as an SNTP time server and all other devices were set to sync to the time of the SYS1.

Also a fictitious single line diagram was built together with system self supervision picture, which is shown in Figure 39. It shows the shadowing phase of the HSB, DuoDriver supervision of both computers and both REF542plus protection relays. Furthermore, the connection to every IED is supervised.

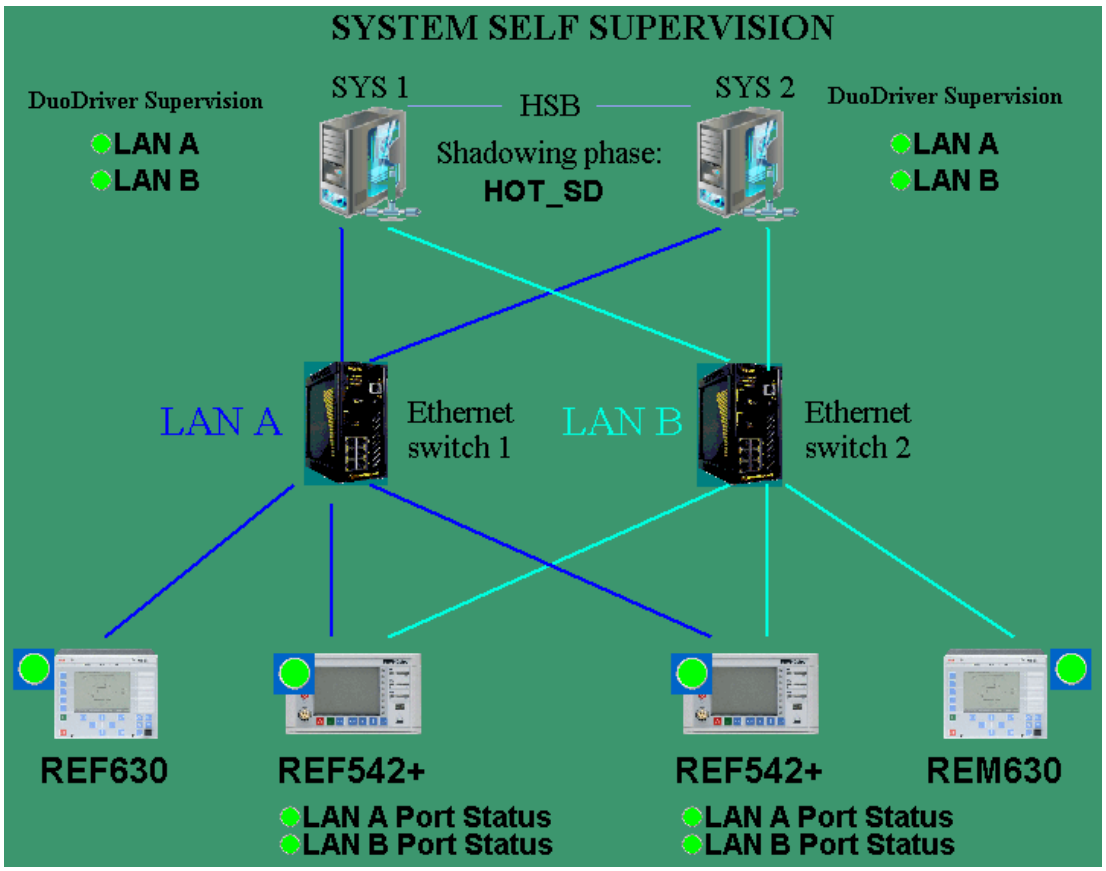


Figure 39. System self supervision display.

The guidelines for configuration of an IEC 61850 based MicroSCADA system using PRP can be found in the DuoDriver installation manual and from the case-specific MicroSCADA manuals as well as case-specific IED manuals. Also the standard IEC 62439-3 and related articles can help understanding the PRP fundamentals more deeply.

The overview of the whole test system setup is found in the Appendix 4.

6.2 Test measurements

Altogether nine tests were made during the testing phase. The sections below handle them one by one. Port mirroring in both Ethernet switches was used to gather the traffic for the analyzer software. The analyzer computer was connected to one port, and the egress (outgoing) traffic of all other ports was mirrored to this port (as seen in Figure 35 on page 85). Software that was used for network traffic capture and analysis included Wireshark (www.wireshark.com) and ITT600 (Integrated Testing Toolbox) by ABB.

6.2.1 Structure of the RCT and PRP Supervision Frame

The first test was meant to commonly clarify the structure of the Redundancy Control Trailer as well as the PRP Supervision Frame that are the basic elements of an IEC 62439-3 based PRP network, discussed in Chapter 5.2. In this test, the analyzer computer was attached to Ethernet Switch 1 (LAN A) and the network traffic was captured for a time of a few seconds. Firstly, a captured frame with RCT was analyzed. Figure 40 shows the structure of an MMS frame with RCT in Wireshark.

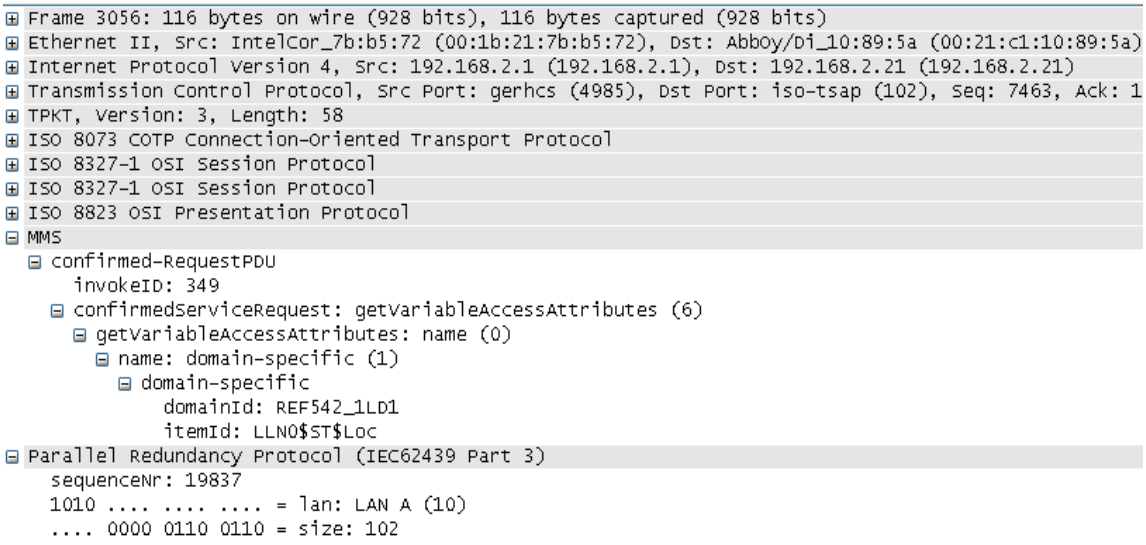


Figure 40. MMS frame with RCT in Wireshark.

The analyzed frame is a MMS frame, sent from SYS1 to protection relay REF542plus 1 (192.168.2.1 → 192.168.2.21). Because the sending and the receiving node are both

DANPs and use the duplicate discard mode, RCT is attached to the end of a frame. In the figure, this particular frame includes an MMS request for obtaining operation mode of the REF542plus 1. The RCT is appended after the payload (MMS in this case) of the frame including sequence number (19837), LAN identification (LAN A) and a size field (102). The RCT is thus accordant with the standard of PRP-0.

Also PRP supervision frames were captured, one of which is shown in Figure 41 below.

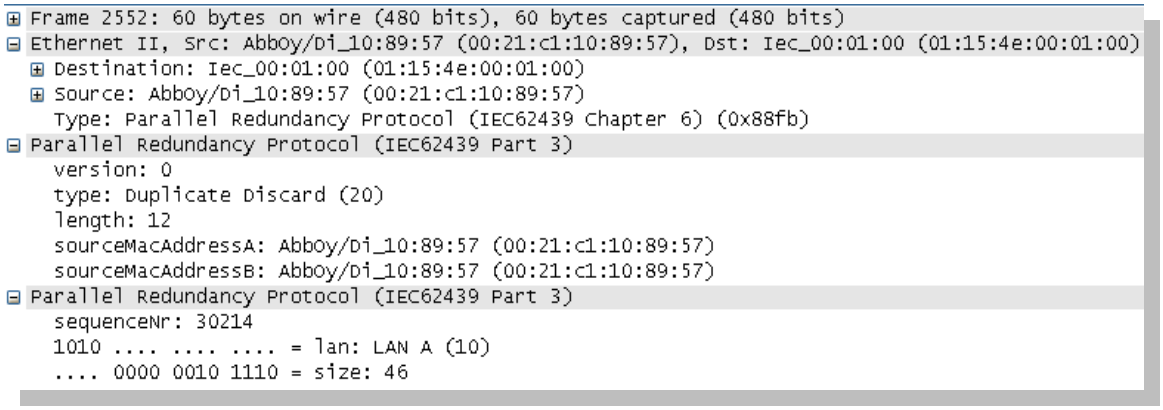


Figure 41. PRP Supervision frame in Wireshark.

The PRP Supervision frame is also accordant with PRP-0 (see Chapter 5.2.5). It is sent to the reserved multicast address (Iec_00:01:00 equals 01:15:4e:00:01:00) by REF542plus 2 (identified from MAC address). This frame is sent to all DANPs. The PRP supervision frame includes information about its sender, e.g. duplicate handling mode and MAC address. Also the RCT is appended in the end of the frame as in the case of normal frames.

6.2.2 Identical data flow in both networks

According to the standard, the traffic of DANPs both in LAN A and in LAN B should be identical. To confirm this, a capture of the traffic in both networks was made simultaneously, lasting a few seconds. The SANs (REF630 and REM630) were disconnected from the network during this test as only the traffic of DANPs was examined. Figure 42 and Figure 43 present a screenshot of the analyzer program ITT600 (Network analyzer from ABB), with the traffic of the two LANs captured.

No.	RecTime	SourceIP	DestinationIP	SourceMAC	DestinationMAC	DataSize	Application	Details	Transport
189	23.8.2011 11:00:48.999850	192.168.2.1	192.168.2.22	00:1B:21:7B:B5:72	00:21:C1:10:89:57	94	Unknown		UDP
190	23.8.2011 11:00:50.045585	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
191	23.8.2011 11:00:50.233268	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
192	23.8.2011 11:00:50.870242	0.0.0.0	0.0.0.0	00:1B:21:7B:B4:3C	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
193	23.8.2011 11:00:50.966576	0.0.0.0	0.0.0.0	00:21:C1:10:89:57	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
194	23.8.2011 11:00:51.286931	192.168.2.1	255.255.255.255	00:1B:21:7B:B5:72	FF:FF:FF:FF:FF:FF	86	Unknown		UDP
195	23.8.2011 11:00:51.286998	192.168.2.1	255.255.255.255	00:1B:21:7B:B5:72	FF:FF:FF:FF:FF:FF	86	Unknown		UDP
196	23.8.2011 11:00:51.837789	192.168.2.22	192.168.2.1	00:21:C1:10:89:57	00:1B:21:7B:B5:72	264	MMS	MMS report	TCP
197	23.8.2011 11:00:51.974447	192.168.2.1	192.168.2.22	00:1B:21:7B:B5:72	00:21:C1:10:89:57	60	MMS	TCP Keep alive	TCP
198	23.8.2011 11:00:52.045562	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
199	23.8.2011 11:00:52.233221	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
200	23.8.2011 11:00:52.870213	0.0.0.0	0.0.0.0	00:1B:21:7B:B4:3C	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
201	23.8.2011 11:00:52.966551	0.0.0.0	0.0.0.0	00:21:C1:10:89:57	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
202	23.8.2011 11:00:53.835837	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP
203	23.8.2011 11:00:53.836118	192.168.2.2	192.168.2.1	00:1B:21:7B:B4:3C	00:1B:21:7B:B5:72	60	Unknown		TCP
204	23.8.2011 11:00:54.045549	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
205	23.8.2011 11:00:54.233173	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
206	23.8.2011 11:00:54.287885	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP
207	23.8.2011 11:00:54.288174	192.168.2.2	192.168.2.1	00:1B:21:7B:B4:3C	00:1B:21:7B:B5:72	60	Unknown		TCP
208	23.8.2011 11:00:54.790792	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP

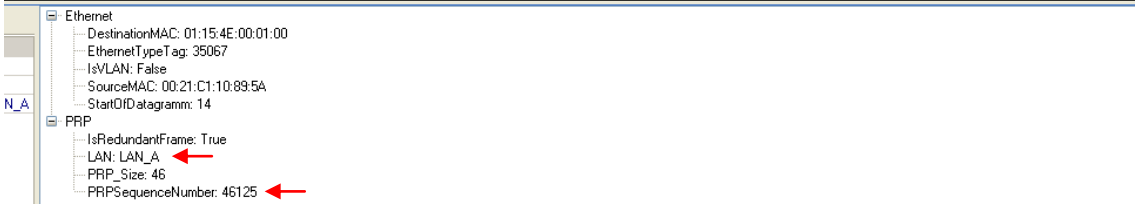


Figure 42. Captured traffic of LAN A in ITT600.

No.	RecTime	SourceIP	DestinationIP	SourceMAC	DestinationMAC	DataSize	Application	Details	Transport
189	23.8.2011 11:00:49.000071	192.168.2.1	192.168.2.22	00:1B:21:7B:B5:72	00:21:C1:10:89:57	94	Unknown		UDP
190	23.8.2011 11:00:50.045870	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
191	23.8.2011 11:00:50.233516	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
192	23.8.2011 11:00:50.870450	0.0.0.0	0.0.0.0	00:1B:21:7B:B4:3C	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
193	23.8.2011 11:00:50.966867	0.0.0.0	0.0.0.0	00:21:C1:10:89:57	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
194	23.8.2011 11:00:51.287226	192.168.2.1	255.255.255.255	00:1B:21:7B:B5:72	FF:FF:FF:FF:FF:FF	86	Unknown		UDP
195	23.8.2011 11:00:51.287506	192.168.2.1	255.255.255.255	00:1B:21:7B:B5:72	FF:FF:FF:FF:FF:FF	86	Unknown		UDP
196	23.8.2011 11:00:51.838105	192.168.2.22	192.168.2.1	00:21:C1:10:89:57	00:1B:21:7B:B5:72	264	MMS	MMS report	TCP
197	23.8.2011 11:00:51.974752	192.168.2.1	192.168.2.22	00:1B:21:7B:B5:72	00:21:C1:10:89:57	60	MMS	TCP Keep alive	TCP
198	23.8.2011 11:00:52.045882	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
199	23.8.2011 11:00:52.233531	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
200	23.8.2011 11:00:52.870496	0.0.0.0	0.0.0.0	00:1B:21:7B:B4:3C	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
201	23.8.2011 11:00:52.966880	0.0.0.0	0.0.0.0	00:21:C1:10:89:57	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
202	23.8.2011 11:00:53.836130	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP
203	23.8.2011 11:00:53.836363	192.168.2.2	192.168.2.1	00:1B:21:7B:B4:3C	00:1B:21:7B:B5:72	60	Unknown		TCP
204	23.8.2011 11:00:54.045900	0.0.0.0	0.0.0.0	00:21:C1:10:89:5A	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
205	23.8.2011 11:00:54.233423	0.0.0.0	0.0.0.0	00:1B:21:7B:B5:72	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
206	23.8.2011 11:00:54.288192	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP
207	23.8.2011 11:00:54.288395	192.168.2.2	192.168.2.1	00:1B:21:7B:B4:3C	00:1B:21:7B:B5:72	60	Unknown		TCP
208	23.8.2011 11:00:54.791101	192.168.2.1	192.168.2.2	00:1B:21:7B:B5:72	00:1B:21:7B:B4:3C	66	Unknown		TCP

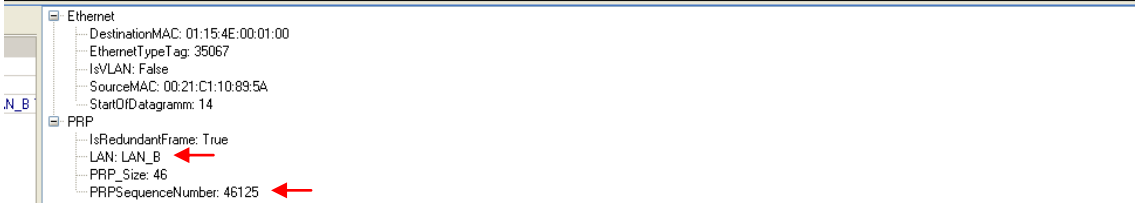


Figure 43. Captured traffic of LAN B in ITT600.

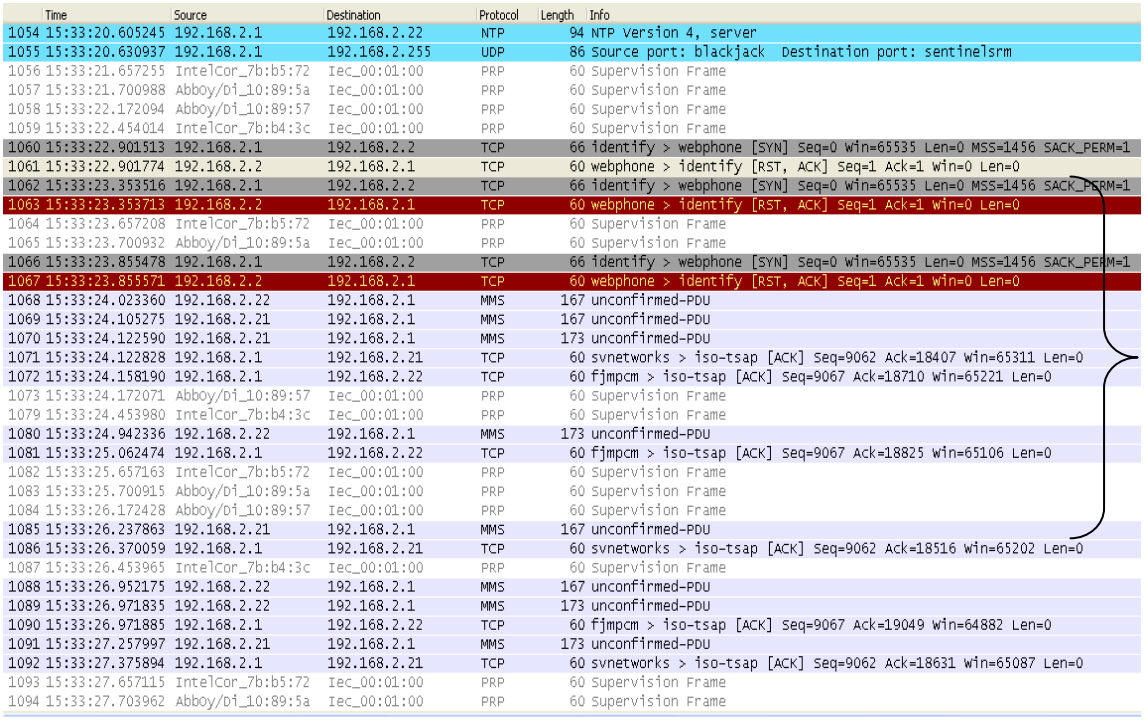
As seen from the figures above, the data flow between DANPs is identical in both LANs including PRP supervision frames. A duplicate PRP supervision frame in both LANs was analyzed, showing the LAN identification and the sequence number (marked with red arrows). The sequence number is the same for both frames, which is one sign that the frame is a duplicate. However, the traffic of both LANs can never be continuously absolutely identical because of the traffic of SANs (connected to one LAN only) and because the traffic generated by switches differs. The traffic of switches was filtered from the captures, as the subject for analysis was DANPs only. An Ethernet switch can create traffic e.g. Link Layer Discovery Protocol (LLDP) messages to advertise their identity and capabilities.

It was noticed during the test that ITT600 cannot retrieve the RCT appended in the frames sent by DANPs. It also lacks the PRP version number from the PRP supervision frame, but however shows the RCT in these frames. The attribute 'IsRedundantFrame' tell if the frame has RCT appended, showing thus the duplicate handling information.

6.2.3 Data flow during network failure

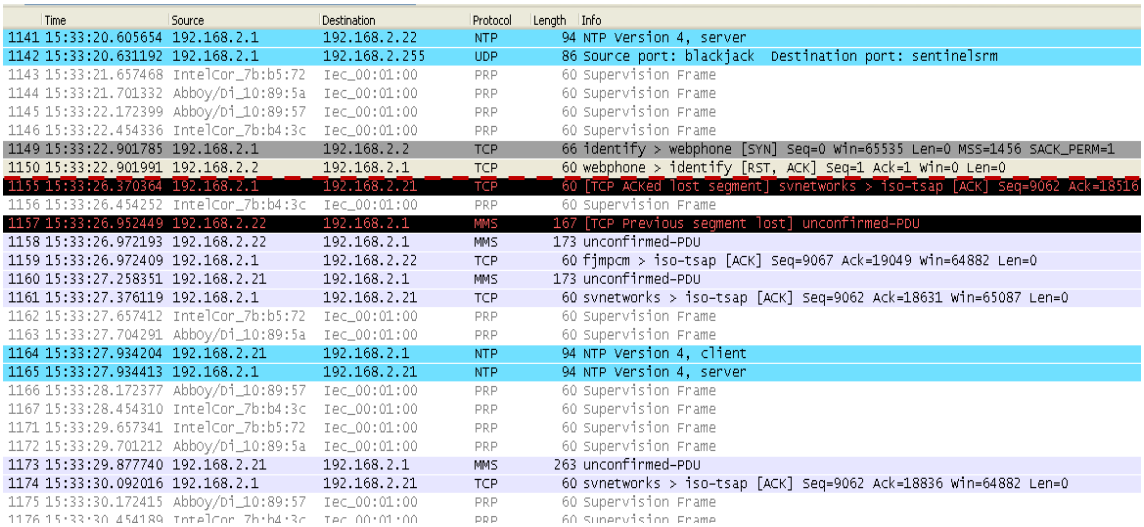
The data flow of DANPs during a network failure should be continuous according to PRP specifications (seamless recovery). In this test, the traffic of both networks was captured simultaneously while LAN B was simulated to fail for a few seconds. The simulation of a short failure was done by resetting all the ports of Ethernet Switch 2 at the same time from its operating system. Also during this test the SANs were disconnected from the network.

Figures 44 and 45 present the traffic in the LANs captured with Wireshark. In the test, a network failure of about three seconds was simulated in LAN B. As seen in the captured figures, the traffic of LAN A flows normally while LAN B has a communication breakout in the time of 15:33:23 (red dashed line in Figure 44). The right brace in Figure 44 shows the traffic in the LAN A, that is missed from LAN B during failure. When the LAN B recovers, a couple of frames have some lost TCP segments, which is common when the network starts operating again. After recovery, the data flow is identical again. The traffic generated by switches was filtered from the captures.



	Time	Source	Destination	Protocol	Length	Info
1054	15:33:20.605245	192.168.2.1	192.168.2.22	NTP	94	NTP Version 4, server
1055	15:33:20.630937	192.168.2.1	192.168.2.255	UDP	86	Source port: blackjack Destination port: sentinelsrm
1056	15:33:21.657255	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1057	15:33:21.700988	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1058	15:33:22.172094	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1059	15:33:22.454014	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1060	15:33:22.901513	192.168.2.1	192.168.2.2	TCP	66	identify > webphone [SYN] Seq=0 Win=65535 Len=0 MSS=1456 SACK_PERM=1
1061	15:33:22.901774	192.168.2.2	192.168.2.1	TCP	60	webphone > identify [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1062	15:33:23.353516	192.168.2.1	192.168.2.2	TCP	66	identify > webphone [SYN] Seq=0 Win=65535 Len=0 MSS=1456 SACK_PERM=1
1063	15:33:23.353713	192.168.2.2	192.168.2.1	TCP	60	webphone > identify [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1064	15:33:23.657208	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1065	15:33:23.700932	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1066	15:33:23.855478	192.168.2.1	192.168.2.2	TCP	66	identify > webphone [SYN] Seq=0 Win=65535 Len=0 MSS=1456 SACK_PERM=1
1067	15:33:23.855571	192.168.2.2	192.168.2.1	TCP	60	webphone > identify [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1068	15:33:24.023360	192.168.2.22	192.168.2.1	MMS	167	unconfirmed-PDU
1069	15:33:24.105275	192.168.2.21	192.168.2.1	MMS	167	unconfirmed-PDU
1070	15:33:24.122590	192.168.2.21	192.168.2.1	MMS	173	unconfirmed-PDU
1071	15:33:24.122828	192.168.2.1	192.168.2.21	TCP	60	svnetworks > iso-tsap [ACK] Seq=9062 Ack=18407 Win=65311 Len=0
1072	15:33:24.158190	192.168.2.1	192.168.2.22	TCP	60	fjmpcm > iso-tsap [ACK] Seq=9067 Ack=18710 Win=65221 Len=0
1073	15:33:24.172071	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1079	15:33:24.453980	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1080	15:33:24.942336	192.168.2.22	192.168.2.1	MMS	173	unconfirmed-PDU
1081	15:33:25.062474	192.168.2.1	192.168.2.22	TCP	60	fjmpcm > iso-tsap [ACK] Seq=9067 Ack=18825 Win=65106 Len=0
1082	15:33:25.657163	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1083	15:33:25.700915	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1084	15:33:26.172428	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1085	15:33:26.237863	192.168.2.21	192.168.2.1	MMS	167	unconfirmed-PDU
1086	15:33:26.370059	192.168.2.1	192.168.2.21	TCP	60	svnetworks > iso-tsap [ACK] Seq=9062 Ack=18516 Win=65202 Len=0
1087	15:33:26.453965	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1088	15:33:26.952175	192.168.2.22	192.168.2.1	MMS	167	unconfirmed-PDU
1089	15:33:26.971835	192.168.2.22	192.168.2.1	MMS	173	unconfirmed-PDU
1090	15:33:26.971885	192.168.2.1	192.168.2.22	TCP	60	fjmpcm > iso-tsap [ACK] Seq=9067 Ack=19049 Win=64882 Len=0
1091	15:33:27.257997	192.168.2.21	192.168.2.1	MMS	173	unconfirmed-PDU
1092	15:33:27.375894	192.168.2.1	192.168.2.21	TCP	60	svnetworks > iso-tsap [ACK] Seq=9062 Ack=18631 Win=65087 Len=0
1093	15:33:27.657115	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1094	15:33:27.703962	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame

Figure 44. Captured traffic on LAN A in Wireshark.



	Time	Source	Destination	Protocol	Length	Info
1141	15:33:20.605654	192.168.2.1	192.168.2.22	NTP	94	NTP Version 4, server
1142	15:33:20.631192	192.168.2.1	192.168.2.255	UDP	86	Source port: blackjack Destination port: sentinelsrm
1143	15:33:21.657468	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1144	15:33:21.701332	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1145	15:33:22.172399	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1146	15:33:22.454336	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1149	15:33:22.901785	192.168.2.1	192.168.2.2	TCP	66	identify > webphone [SYN] Seq=0 Win=65535 Len=0 MSS=1456 SACK_PERM=1
1150	15:33:22.901991	192.168.2.2	192.168.2.1	TCP	60	webphone > identify [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1155	15:33:26.370364	192.168.2.1	192.168.2.21	TCP	60	[TCP ACKed lost segment] svnetworks > iso-tsap [ACK] Seq=9062 Ack=18516
1156	15:33:26.454252	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1157	15:33:26.952449	192.168.2.22	192.168.2.1	MMS	167	[TCP Previous segment lost] unconfirmed-PDU
1158	15:33:26.972193	192.168.2.22	192.168.2.1	MMS	173	unconfirmed-PDU
1159	15:33:26.972409	192.168.2.1	192.168.2.22	TCP	60	fjmpcm > iso-tsap [ACK] Seq=9067 Ack=19049 Win=64882 Len=0
1160	15:33:27.258351	192.168.2.21	192.168.2.1	MMS	173	unconfirmed-PDU
1161	15:33:27.376119	192.168.2.1	192.168.2.21	TCP	60	svnetworks > iso-tsap [ACK] Seq=9062 Ack=18631 Win=65087 Len=0
1162	15:33:27.657412	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1163	15:33:27.704291	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1164	15:33:27.934204	192.168.2.21	192.168.2.1	NTP	94	NTP Version 4, client
1165	15:33:27.934413	192.168.2.1	192.168.2.21	NTP	94	NTP Version 4, server
1166	15:33:28.172377	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1167	15:33:28.454310	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame
1171	15:33:29.657341	IntelCor_7b:b5:72	Iec_00:01:00	PRP	60	Supervision Frame
1172	15:33:29.701212	Abboy/Bi_10:89:5a	Iec_00:01:00	PRP	60	Supervision Frame
1173	15:33:29.877740	192.168.2.21	192.168.2.1	MMS	263	unconfirmed-PDU
1174	15:33:30.092016	192.168.2.1	192.168.2.21	TCP	60	svnetworks > iso-tsap [ACK] Seq=9062 Ack=18836 Win=64882 Len=0
1175	15:33:30.172415	Abboy/Bi_10:89:57	Iec_00:01:00	PRP	60	Supervision Frame
1176	15:33:30.454189	IntelCor_7b:b4:3c	Iec_00:01:00	PRP	60	Supervision Frame

Figure 45. Captured traffic on LAN B in Wireshark. Communication blackout happens in time 15:33:23 and LAN recovers after three seconds.

Later, a test where the Ethernet switch 2 was completely powered down for a few minutes was performed. The system was up and running normally as LAN A was carrying the traffic normally during LAN B blackout.

6.2.4 Network connection recovery time after failure in a LAN

The purpose of this test was to measure how long it takes from the traffic to flow again in the LAN after recovery from the failure. This was investigated in two cases: In the case of Ethernet switch power failure, and in the case of LAN cable failure.

Firstly, the Ethernet switch power failure was investigated. In practice, the time from the start of the blackout to the point when traffic flows again was measured, thus presenting the start-up time of the Ethernet switch. This was performed to Ethernet switch 1 (LAN A) and for better accuracy, the power blackout simulation was done by resetting the switch from the operating system. Figure 46 below shows the traffic flow in the LAN A captured with ITT600 during reset.

No.	RecTime	SourceIP	DestinationIP	SourceMAC	DestinationMAC	DataSize	Application	Details	Transport
54	24.8.2011 11:40:23.796171	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	60	MMS	TCP Keep alive	TCP
55	24.8.2011 11:40:23.796533	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	60	MMS	TCP Keep alive	TCP
56	24.8.2011 11:40:23.840076	0.0.0.0	0.0.0.0	00:1B:21:7B:B4:	01:15:4E:00:01:00	60	PRP_Supervision	Supervision Message	Ethernet
57	24.8.2011 11:40:24.139273	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	90	ntp	NTP synchronisation:	UDP
58	24.8.2011 11:40:24.139394	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	90	ntp	NTP synchronisation:	UDP
59	24.8.2011 11:40:54.964111	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	62	MMS	TCP Keep alive or CO	TCP
60	24.8.2011 11:40:54.964324	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	60	MMS	TCP Keep alive or CO	TCP
61	24.8.2011 11:40:54.964551	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	60	MMS	TCP Keep alive	TCP
62	24.8.2011 11:40:54.964626	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	78	MMS	TCP Keep alive or CO	TCP
63	24.8.2011 11:40:54.965946	192.168.2.22	192.168.2.1	00:21:C1:10:89:5	00:1B:21:7B:B5:72	173	MMS	MMS report	TCP
64	24.8.2011 11:40:54.966111	192.168.2.1	192.168.2.22	00:1B:21:7B:B5:	00:21:C1:10:89:57	60	MMS	TCP Keep alive	TCP
65	24.8.2011 11:40:54.980438	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	78	MMS	TCP Keep alive or CO	TCP
66	24.8.2011 11:40:54.980630	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	246	MMS	MMS Initiate message	TCP
67	24.8.2011 11:40:54.991016	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	214	MMS	MMS Initiate message	TCP
68	24.8.2011 11:40:55.011036	192.168.2.1	192.168.2.23	00:1B:21:7B:B5:	00:02:A3:30:4F:81	91	MMS	MMS Confirmed reque	TCP
69	24.8.2011 11:40:55.020999	192.168.2.23	192.168.2.1	00:02:A3:30:4F:8	00:1B:21:7B:B5:72	217	MMS	MMS Confirmed respo	TCP

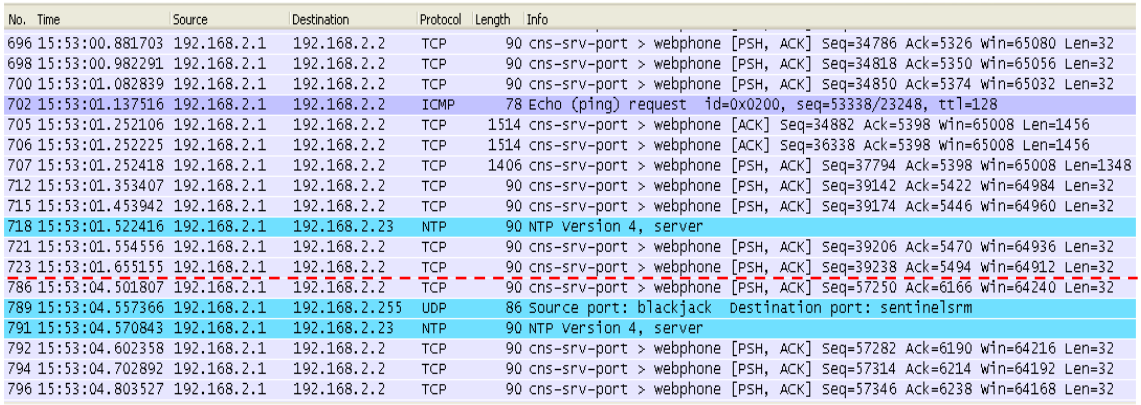
Figure 46. Capture of traffic in LAN A during switch failure in ITT600. Red dashed line shows the failure moment.

As seen in Figure above, the traffic continues to flow again in about 30 seconds. The precise time between the last frame before failure and the first frame after failure was 30.58 seconds. Later, the switch was powered down and up manually as quickly as possible, and the traffic continued after time of 30.82 seconds. It can thus be said that if a switch experiences power blackout, the traffic flow in the networks stops at least for 30 seconds, and more if the power is down longer. As mentioned before, there is a reason why the switches in the LANs should not share the same power source. The

booting time of switches can however vary depending on the manufacturer and switch type; the results of this test were done with RuggedCom RS900NC.

After the switch power failure, the LAN cable failure was investigated. Here, the time it takes to establish connection after connecting the cable to the Ethernet switch was measured. This was tested with hot MicroSCADA computer (SYS1), which was set to shadow the application state to the stand-by MicroSCADA computer (SYS2). This generates a lot of traffic between the HSB computers and makes it thus more accurate to measure the connection establish time of one specified port.

The time for connection establishment on LAN A port of the SYS1 was analyzed by resetting the corresponding port it was attached to in Ethernet switch 1 via the operating system. Figure 47 below shows the capture of traffic sent by SYS1 (192.168.2.1) during the port reset.



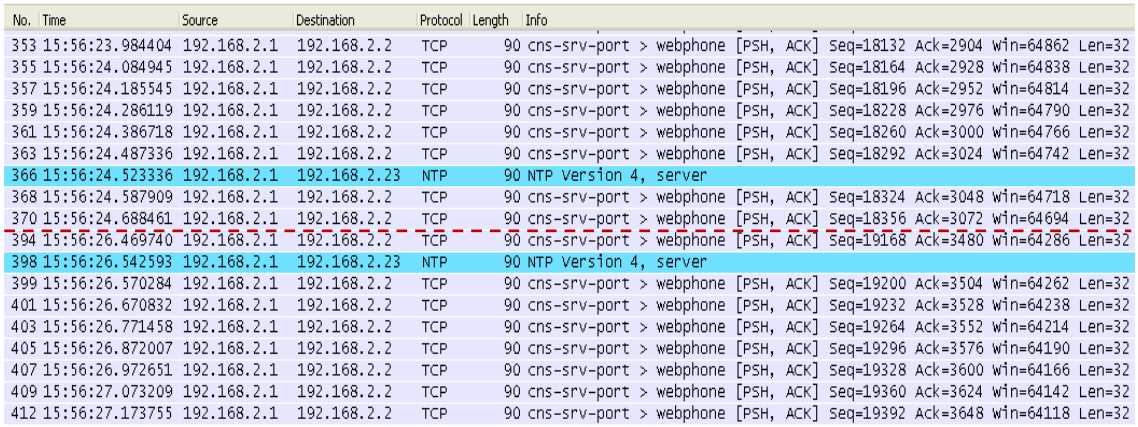
No.	Time	Source	Destination	Protocol	Length	Info
696	15:53:00.881703	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=34786 Ack=5326 Win=65080 Len=32
698	15:53:00.982291	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=34818 Ack=5350 Win=65056 Len=32
700	15:53:01.082839	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=34850 Ack=5374 Win=65032 Len=32
702	15:53:01.137516	192.168.2.1	192.168.2.2	ICMP	78	Echo (ping) request id=0x0200, seq=53338/23248, ttl=128
705	15:53:01.252106	192.168.2.1	192.168.2.2	TCP	1514	cns-srv-port > webphone [ACK] Seq=34882 Ack=5398 Win=65008 Len=1456
706	15:53:01.252225	192.168.2.1	192.168.2.2	TCP	1514	cns-srv-port > webphone [ACK] Seq=36338 Ack=5398 Win=65008 Len=1456
707	15:53:01.252418	192.168.2.1	192.168.2.2	TCP	1406	cns-srv-port > webphone [PSH, ACK] Seq=37794 Ack=5398 Win=65008 Len=1348
712	15:53:01.353407	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=39142 Ack=5422 Win=64984 Len=32
715	15:53:01.453942	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=39174 Ack=5446 Win=64960 Len=32
718	15:53:01.522416	192.168.2.1	192.168.2.23	NTP	90	NTP Version 4, server
721	15:53:01.554556	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=39206 Ack=5470 Win=64936 Len=32
723	15:53:01.655155	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=39238 Ack=5494 Win=64912 Len=32
786	15:53:04.501807	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=57250 Ack=6166 Win=64240 Len=32
789	15:53:04.557366	192.168.2.1	192.168.2.255	UDP	86	Source port: blackjack Destination port: sentinelsrm
791	15:53:04.570843	192.168.2.1	192.168.2.23	NTP	90	NTP Version 4, server
792	15:53:04.602358	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=57282 Ack=6190 Win=64216 Len=32
794	15:53:04.702892	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=57314 Ack=6214 Win=64192 Len=32
796	15:53:04.803527	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=57346 Ack=6238 Win=64168 Len=32

Figure 47. Captured traffic of SYS1 in LAN A in Wireshark. Red dashed line shows the moment when the port was reset.

After failure is recovered, connection is established in 2.8 seconds as seen from the above Figure. This may however include some time for resetting the port, and is thus not very reliable result.

Later, the test was repeated a couple of times by manually disconnecting and reconnecting the cable, as quickly as possible. Here, the measured time for connection

establish was approximately 1.8 seconds on every testing time, one of which is shown in Figure 48 below.



No.	Time	Source	Destination	Protocol	Length	Info
353	15:56:23.984404	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18132 Ack=2904 Win=64862 Len=32
355	15:56:24.084945	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18164 Ack=2928 Win=64838 Len=32
357	15:56:24.185545	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18196 Ack=2952 Win=64814 Len=32
359	15:56:24.286119	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18228 Ack=2976 Win=64790 Len=32
361	15:56:24.386718	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18260 Ack=3000 Win=64766 Len=32
363	15:56:24.487336	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18292 Ack=3024 Win=64742 Len=32
366	15:56:24.523336	192.168.2.1	192.168.2.23	NTP	90	NTP Version 4, server
368	15:56:24.587909	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18324 Ack=3048 Win=64718 Len=32
370	15:56:24.688461	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=18356 Ack=3072 Win=64694 Len=32
394	15:56:26.469740	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19168 Ack=3480 Win=64286 Len=32
398	15:56:26.542593	192.168.2.1	192.168.2.23	NTP	90	NTP Version 4, server
399	15:56:26.570284	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19200 Ack=3504 Win=64262 Len=32
401	15:56:26.670832	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19232 Ack=3528 Win=64238 Len=32
403	15:56:26.771458	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19264 Ack=3552 Win=64214 Len=32
405	15:56:26.872007	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19296 Ack=3576 Win=64190 Len=32
407	15:56:26.972651	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19328 Ack=3600 Win=64166 Len=32
409	15:56:27.073209	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19360 Ack=3624 Win=64142 Len=32
412	15:56:27.173755	192.168.2.1	192.168.2.2	TCP	90	cns-srv-port > webphone [PSH, ACK] Seq=19392 Ack=3648 Win=64118 Len=32

Figure 48. Captured traffic of SYS1 in LAN A in Wireshark. Red dashed line shows the moment when cable was disconnected for as short time as possible.

This result can still include some time related to disconnecting the port. A measurement was done afterwards to roughly estimate the connection opening time. Here, the cable was already unplugged, and a time was measured from the time the cable was plugged in. The result was that no noticeable delay was detected. A rough guess was made that the connection is formed almost immediately, not over the time of 200 ms. It can however be a lot more rapid. More accurate measuring devices are needed to measure the actual value for connection establishment.

A conclusion could say that if the connection experience short interruption, the connection is up again in less than two seconds after failure (the disconnecting increases the time). When cable is plugged in after failure, the connection is made a lot quicker. This test was only made with RJ45 (copper) and 100 Mbit port speed, and the result can differ with other port types and speeds.

To increase redundancy and tolerance against LAN cable breaks in one LAN of the PRP network, Rapid Spanning Tree Protocol can be used in ring or meshed type LANs.

6.2.5 Data flow between SANs

This test briefly investigated the data flow of SANs in the LANs. In this test, the analyzer computer was connected only to Ethernet switch 1 (LAN A) and to a port that operates normally (not mirroring). In this way the analyzer computer acts as a normal SAN connected to the LAN A. The connection to the SANs was tested by continuously pinging them from both MicroSCADA computer (SYS1) and analyzer computer.

In the test, the SYS1 was set to ping both SANs. It will see the devices in both networks. As a compare, the analyzer computer connected only in LAN A was also set to ping both SANs. During the pinging, SAN 4 (192.168.2.24) was transferred from LAN B to LAN A. Figure 49 shows the ping results of SYS1 (DANP) while Figure 50 shows the ping results of the analyzer computer (SAN). In this test, a third-party ping program was used, providing a timestamp to every packet sent. The sending interval was set to one second, and the clocks of the SYS1 and analyzer computer were synchronized with NTP.

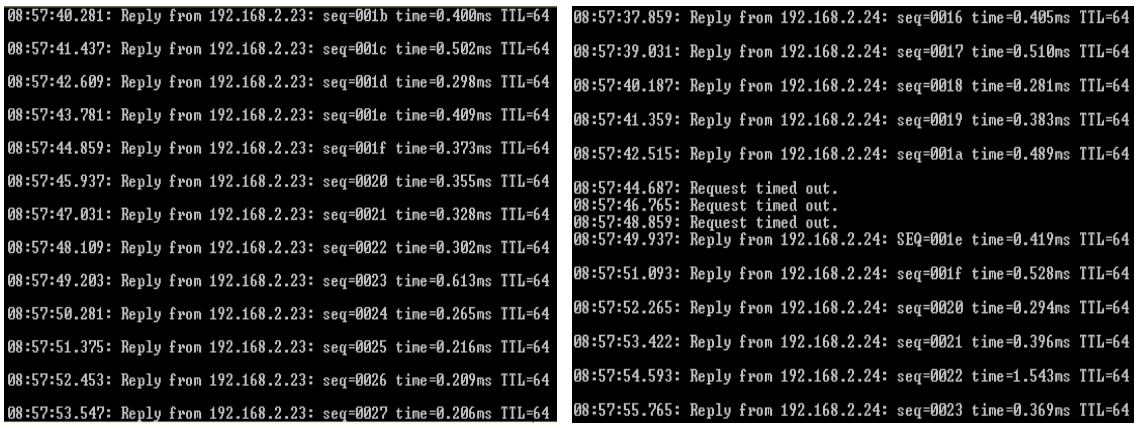


Figure 49. Snapshot of SYS1 command prompt pinging both SANs.

As seen in the figure, the DANP has access to SANs connected to either LAN. The SAN 4 was transferred from the LAN B to LAN A, and during that time the SAN cannot be reached as seen in the rightmost snapshot. When connected to LAN A, it will again be online.

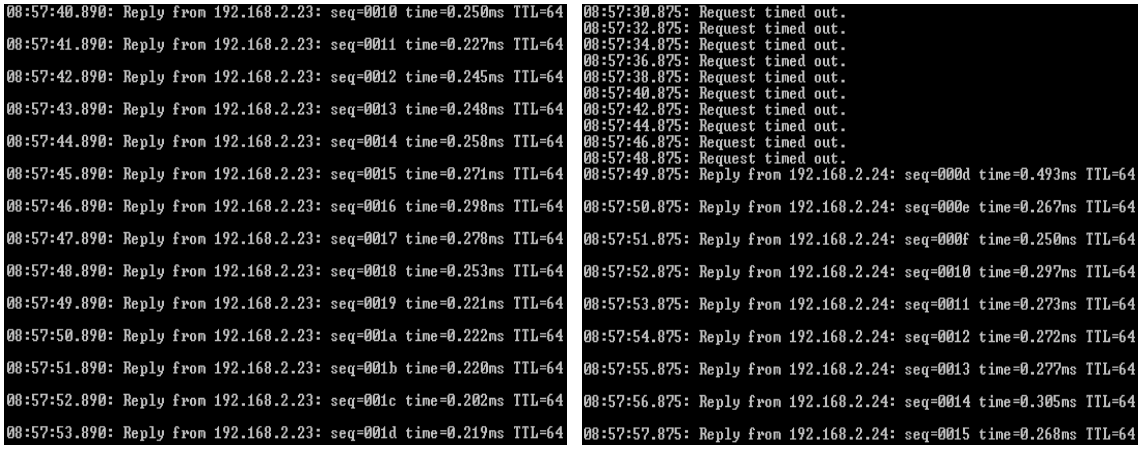


Figure 50. Snapshot of analyzer computer command prompt pinging both SANs. The computer was connected to LAN A.

When connected to LAN A, the analyzer computer reaches the SAN 3 as normally. It cannot reach the SAN 4 connected to LAN B. After the SAN 4 is moved to LAN A, it will be reachable as presented in the rightmost snapshot. This is why every SAN that needs to communicate with other SANs must be connected to the same LAN, either A or B. Alternatively, the SAN can be connected to both LANs through RedBox, which is a preferable if the SAN is a crucial component of the network, e.g. single port IED.

6.2.6 Traffic analysis before and after DuoDriver

This test analyzed the traffic before and after the DuoDriver of SYS1. The analyzer computer was set to capture only the traffic allocated to SYS1 (192.168.2.1) in both LANs. At the same time, the analyzer program was set to capture incoming packets in SYS1. Thus, three capture sessions were open at the same time. The analyzer computer was connected back to the mirroring ports of Ethernet switches.

The captures are presented in Figure 51 (traffic in LAN A), Figure 52 (traffic in LAN B) and in Figure 53, which shows the traffic in SYS1. In the figures, one certain frame is also analyzed. For this test, Wireshark was used.

The transparent reception mode in DuoDriver management GUI enables analyzing the RCT in frames after DuoDriver, since this mode does not remove it upon reception.

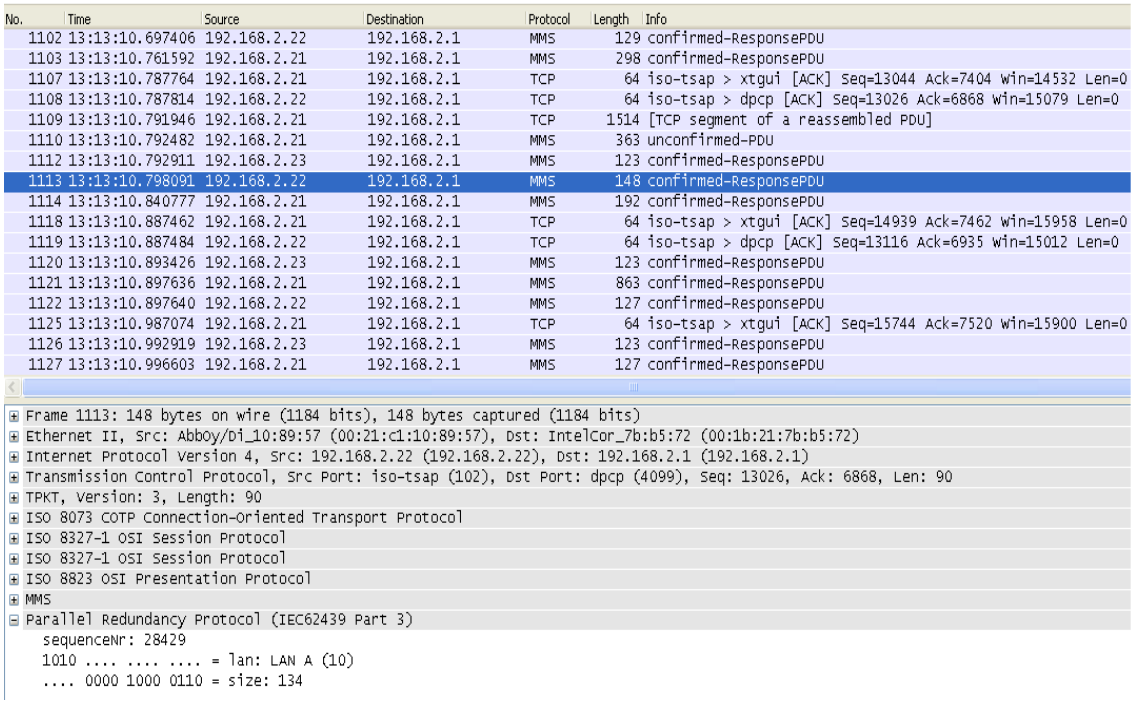


Figure 51. Captured traffic of LAN A in Wireshark.

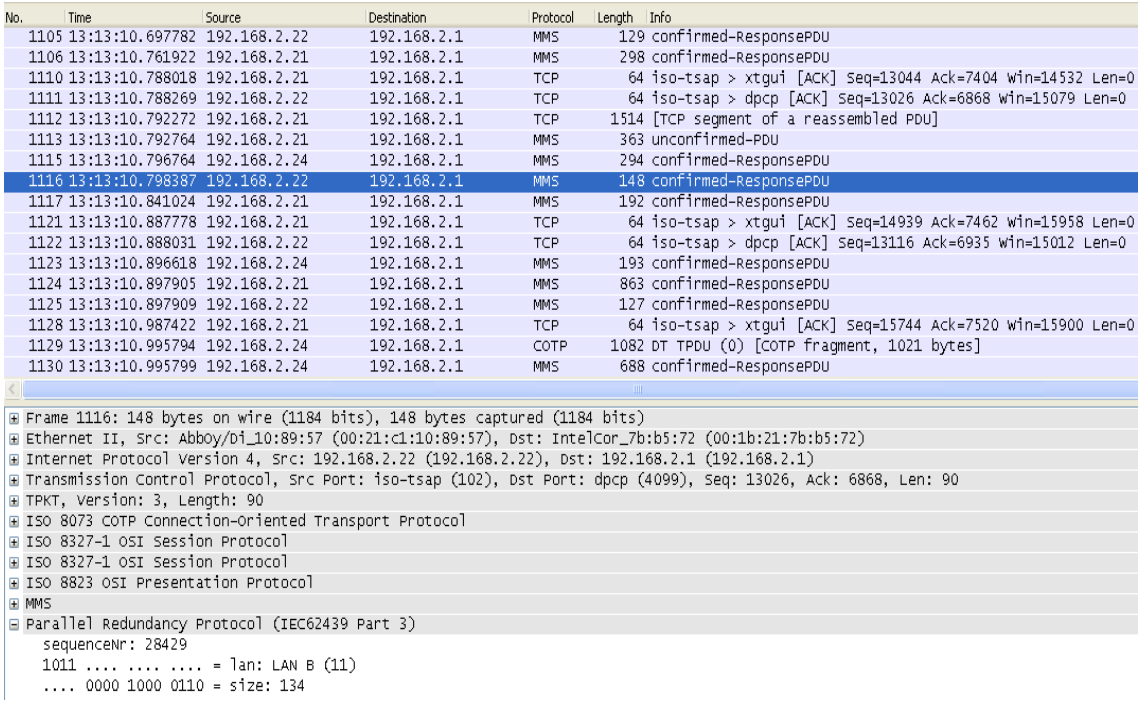


Figure 52. Captured traffic of LAN B in Wireshark.

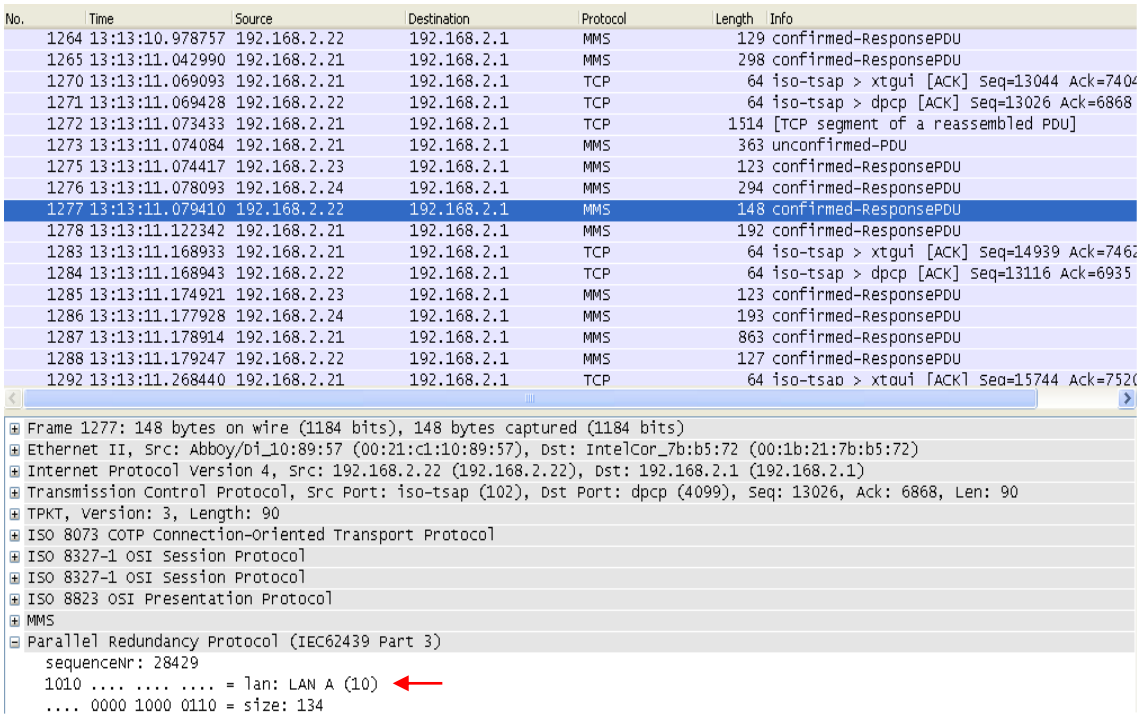


Figure 53. Captured traffic of SYS1 in Wireshark.

The above figures show the traffic before and after the DuoDriver of SYS1. It can be seen that the duplicates sent by other DANPs (192.168.2.21 and 192.168.2.22) are discarded, because only one frame gets through to the application. For example, the RCT of analyzed frame (sequence number 28429) in SYS1 tells that it is taken from LAN A, and the frame from LAN B is discarded (marked in Fig. 52 with red arrow). The duplicate discard algorithm of the DuoDriver accepts the frame that came first and discards the later coming duplicate. Frames sent by SANs are received normally, and they do not have RCT appended.

When looking at the capture times of the two LANs, a question arose; why do the frames captured from LAN B have a little bit bigger timestamp (however less than a millisecond) most of the time? The home page of Wireshark User's Guide gives information that Wireshark gets the timestamps from the system kernel via WinPcap library (special library for packet capturing) and when using USB network interfaces, the packets come a little later to the kernel. This can be the reason for LAN B capturing

the frames a little later, since a D-Link USB-Ethernet interface was used for LAN B captures. (Lamping, Sharpe & Warnicke 2011).

The analyzer computer time was synchronized to the time of SYS1 using Network Time Protocol. The time stamps of the SYS1 are however considerably bigger, which may reference to imperfection in the sync resolution or to behavior of the WinPcap library, which is affected by many characteristics, e.g. operating system and performance of the computer. Thus, the time stamps of the capture files are not millisecond-class comparable, when capturing network data of different computers. The order of the frames is however fully comparable, which serves this test well.

After investigating the ingress traffic of SYS1, the egress traffic was captured and examined. Again, three captures were made simultaneously; the sent traffic of SYS1 was captured together with captures of LAN A and LAN B. Figure 54 shows the sent traffic (source 192.168.2.1) in SYS1, while Figures 55 and 56 show the data flow in the LANs.

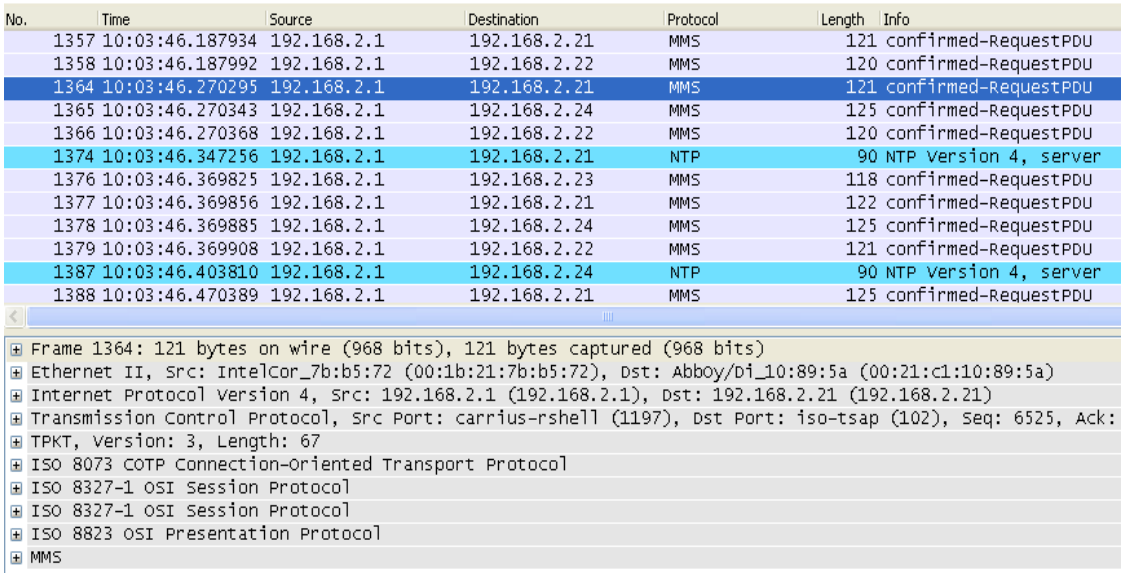


Figure 54. Traffic sent from SYS1 in Wireshark. The analyzed frame does not yet have RCT appended.

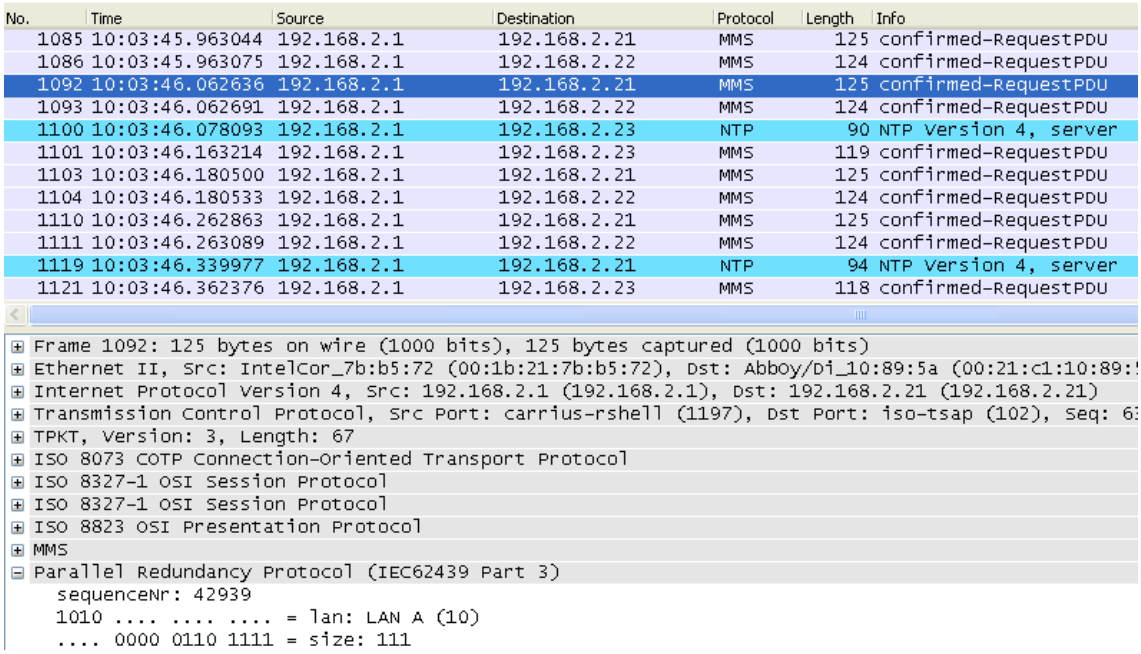


Figure 55. Captured traffic of LAN A in Wireshark.

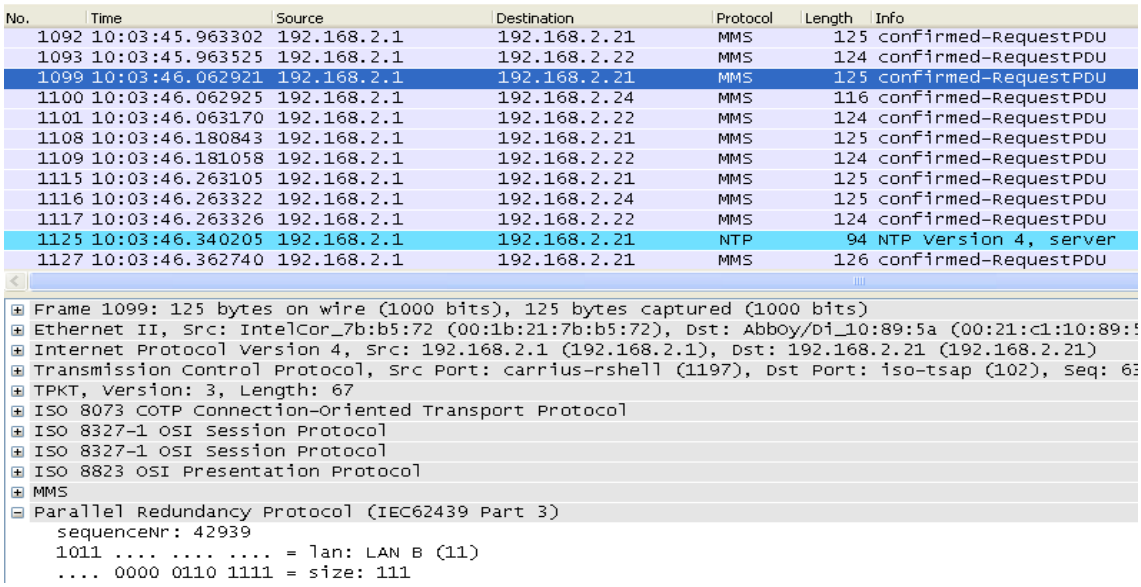


Figure 56. Captured traffic of LAN B in Wireshark.

In the above figures, a certain frame sent to REF542plus 1 was analyzed. It can be seen that after sending and going through DuoDriver, the frame is doubled and a RCT is appended after it. The RCT tells the sequence number (42939), LAN identification and size field. Also the length of the original frame is grown by 4 octets (32 bits) because of

the RCT. Also here, the time stamps of different computers are not precisely comparable; actually it seems that a frame was captured in the LAN before it was sent by the SYS1.

Figure 57 shows an analyzed NTP frame sent to SAN (192.168.2.23) in LAN A. Here, the RCT is not appended, because the destination is a SAN.

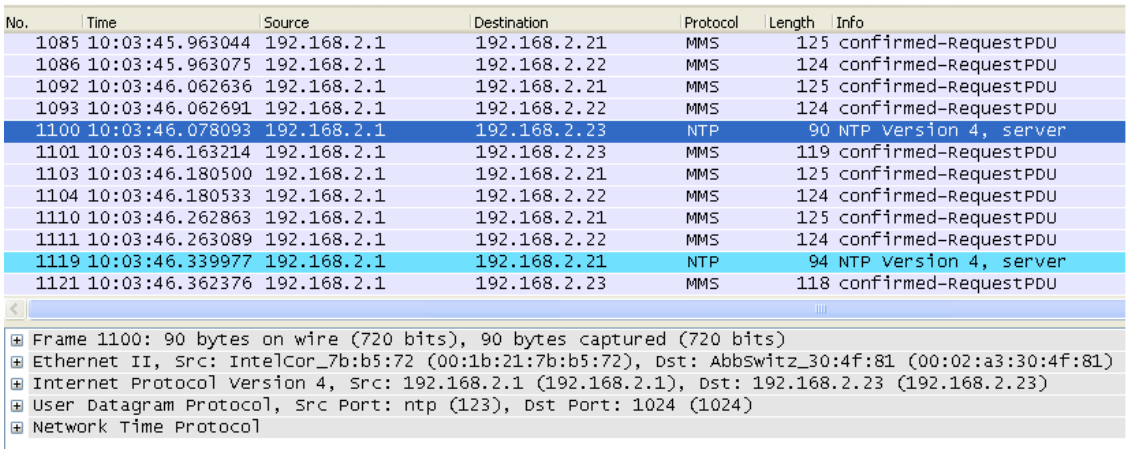


Figure 57. Analyzed frame sent to SAN in LAN A in Wireshark. No RCT appended.

This test confirmed that DuoDriver acts according to the standard, duplicating the frames on egress and discarding the duplicate frame on ingress based on the contents of the Redundancy Control Trailer. RCT is not appended if destination is a SAN.

6.2.7 Interconnecting the LANs

This test briefly investigates, what happens if the LANs are connected together. This should not be done in any case, but it was still tested what happens if it is done.

Right after connection, the error rate counters of the DANPs started to increase. The DuoDriver management GUI has a counter for ‘Duo Frame received on wrong line’ which increased every second. Shortly, all the connected devices in the network disconnected, one by one, resulting in an inoperable network. Sometimes a device came back online for a few moments, but lost connection again. Figures 58 and 59 below show the traffic in LAN A and LAN B during the connection of the LANs.

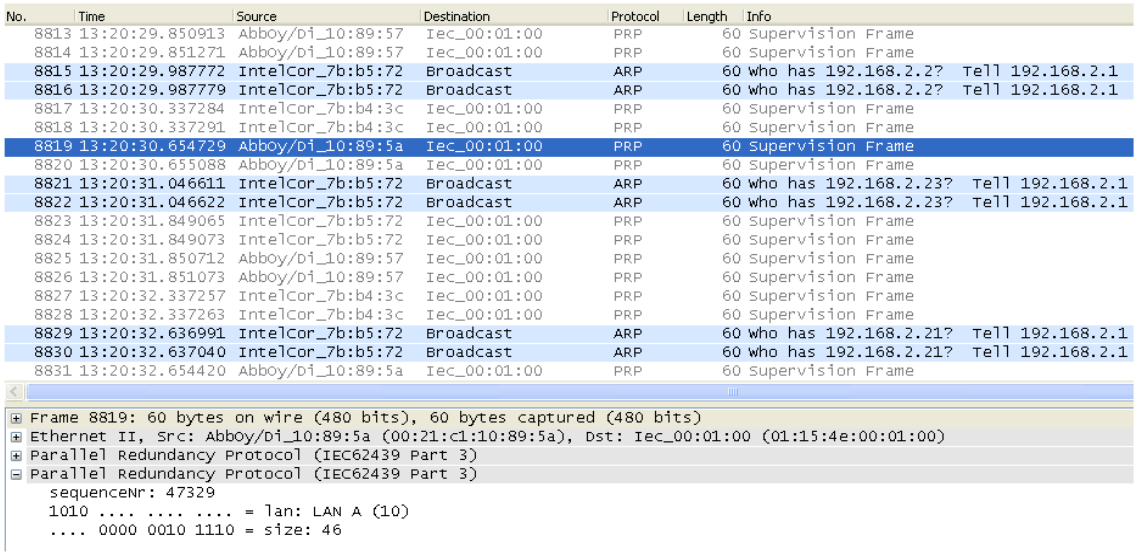


Figure 58. Captured traffic of LAN A in Wireshark.

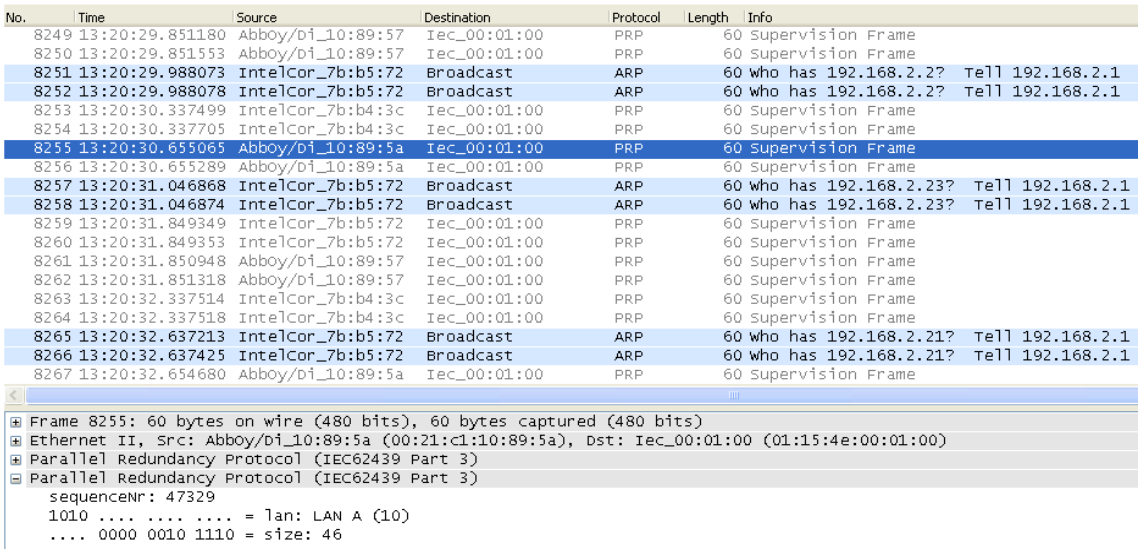


Figure 59. Captured traffic of LAN B in Wireshark.

The above Figures show that ARP is asking for IP addresses, but it seems that it does not know which one of the ports to map for the IP address since both ports with same MAC addresses are connected to the same network (MAC address conflict). Also the frames are sent twice i.e. both LANs carry the two duplicated frames with LAN identifications; the frame analyzed in the figures carries LAN A tag on both LANs. The connection between LANs thus leads to double addressing and troubles the network.

Figure 60 below shows a ping sent to every device in the network from SYS1 during LAN connection.

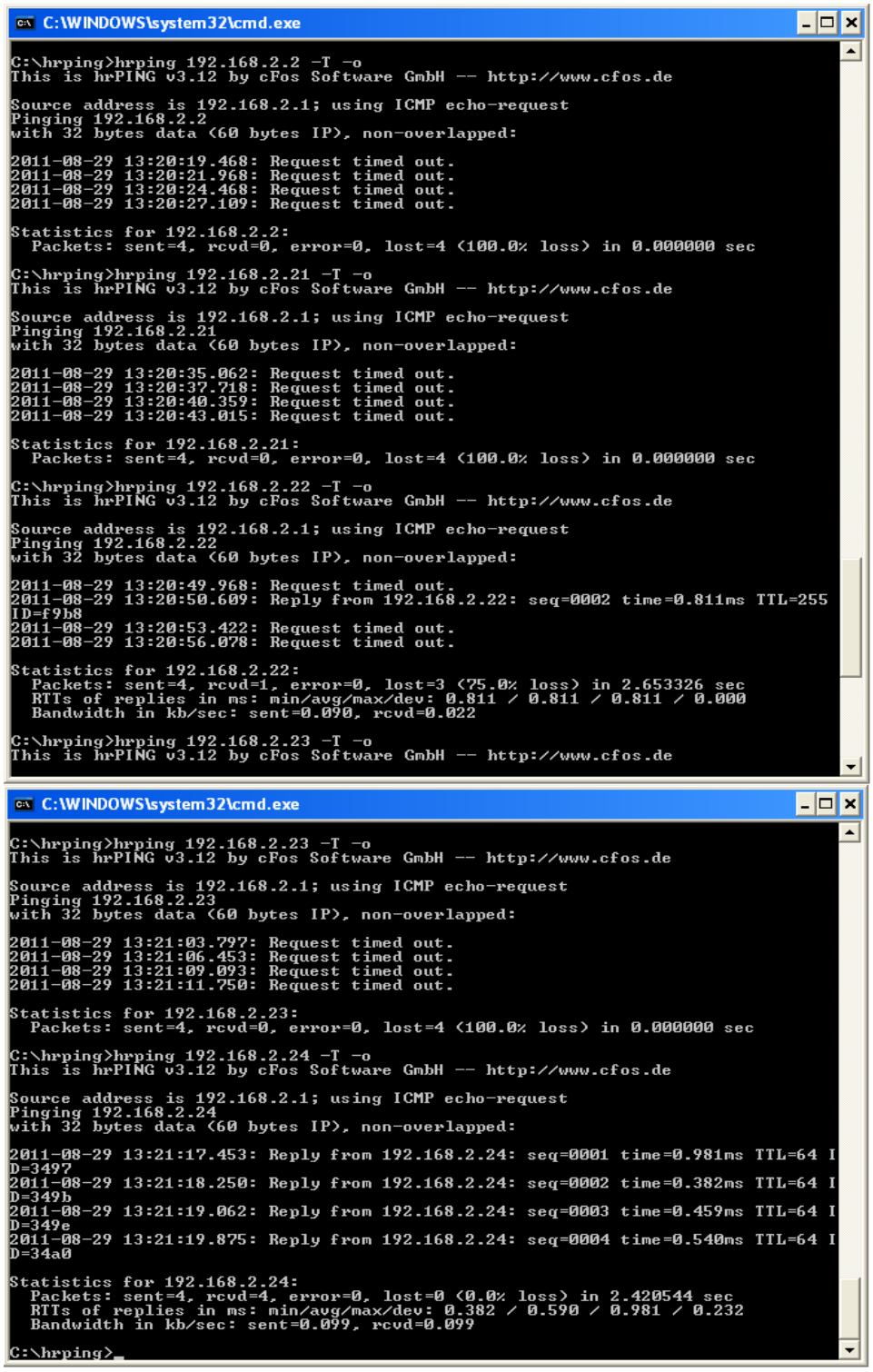


Figure 60. Pinging the devices during LAN A and LAN B connection.

This time, only SAN 4 gave reply for the ping, and DANP 2 responded only to one packet. This test clearly showed that connecting the two LANs of PRP network will lead to a nonworking network, and must thus never be done.

6.2.8 DuoDriver duplicate accept -mode

As mentioned before, the DuoDriver can operate in duplicate accept –mode with PRP (although not preferred). In this test, the DuoDrivers of MicroSCADA computers were set to operate in duplicate accept mode. Afterwards, the traffic sent to SYS2 was captured. The HSB shadowing was set on in the test.

Figures 61 and 62 show the capture of SYS2 with different frames analyzed. A filter showing only destination of 192.168.2.2 and multicasted PRP supervision frames was used. It can be seen that both of the coming frames are sent to upper levels. In fact, the TCP recognizes the duplicate as it is designed to do, coloured black in the figure (TCP duplicate ack, or TCP retransmission proposal). No frames have RCT appended. This is also true for PRP supervision frames sent by SYS1 (also operated in duplicate accept mode).

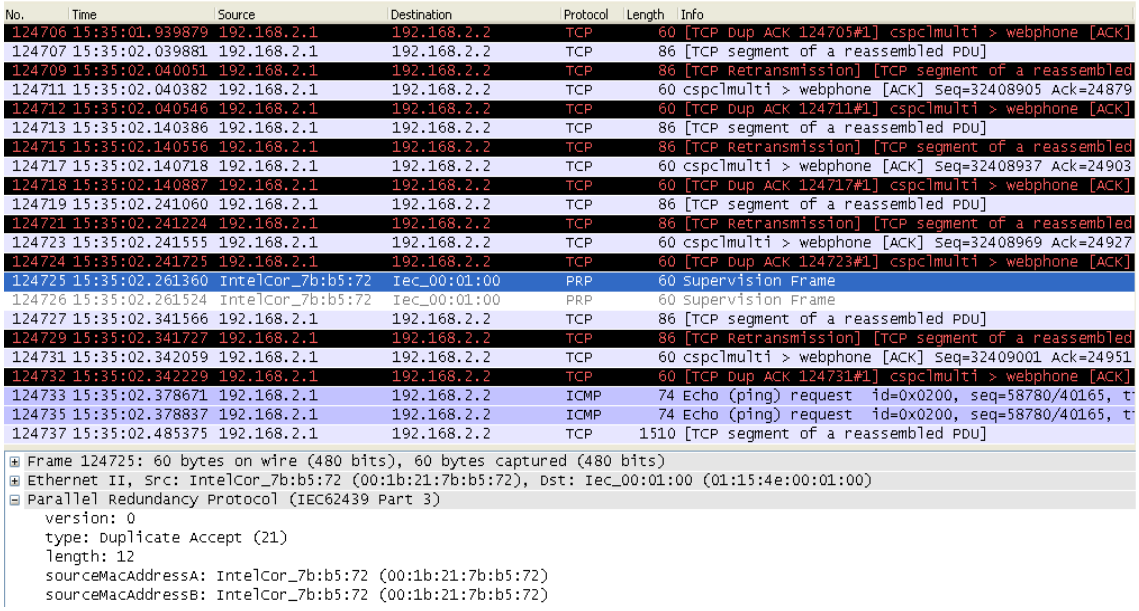


Figure 61. Captured traffic of SYS1 in Wireshark. PRP supervision frame analyzed. No RCT is appended.

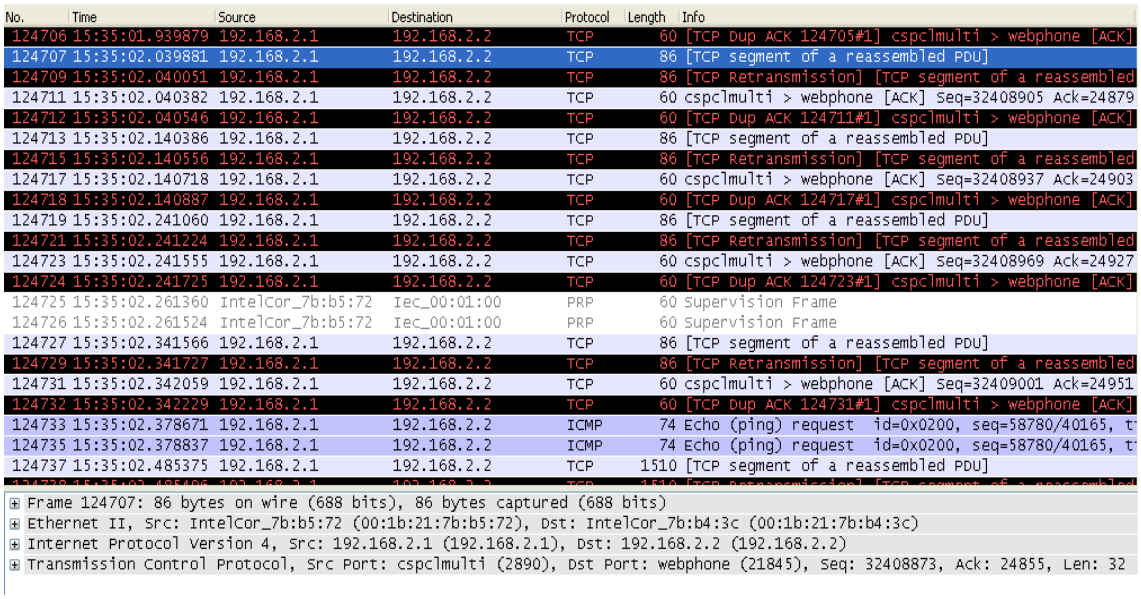


Figure 62. Captured traffic of SYS1 in Wireshark. TCP frame analyzed. No RCT is appended.

The duplicate accept -method does not discard the duplicate. However, because the duplicate is discarded in every case (in the case of TCP), this mode is not preferred. Furthermore, because the frames in this mode lack the presence of RCT, error counters are not updated if the configuration is done wrongly. All in all, the duplicate discard is advantageous to be performed already at the link level (DuoDriver level) since it is more efficient way. Therefore, duplicate discard-method should always be used if possible.

6.2.9 MMS traffic with Hot Stand-by

The last test briefly analyzes the HSB functionality in the IEC 61850 based system and if it is correctly configured in the test application. As described in Figure 38 on page 92, IEDs should send their MMS reports to both computers' OPC servers to make sure that no information is lost in the case of switchover, allowing application to continue from the same state it was on the computer that failed. The OPC DA clients on the computers have adjustable buffers that store the information every time. When the buffer size is longer than the switchover time, correct operation is achieved.

Figures 63 and 64 show the MMS traffic in LAN A captured with ITT600 and with two sequential frames analyzed. ITT600 can decode MMS information, if the correct SCL file is loaded, or a connection to IEDs is established. On the contrary, Wireshark cannot properly decode MMS information.

In the figures, the frames analyzed were sent from REF542plus 1 to both MicroSCADA computers (192.168.2.21 → 192.168.2.1 and 192.168.2.21 → 192.168.2.2). When analyzing the frames, it was noticed that they send the same measurement information to different computers.

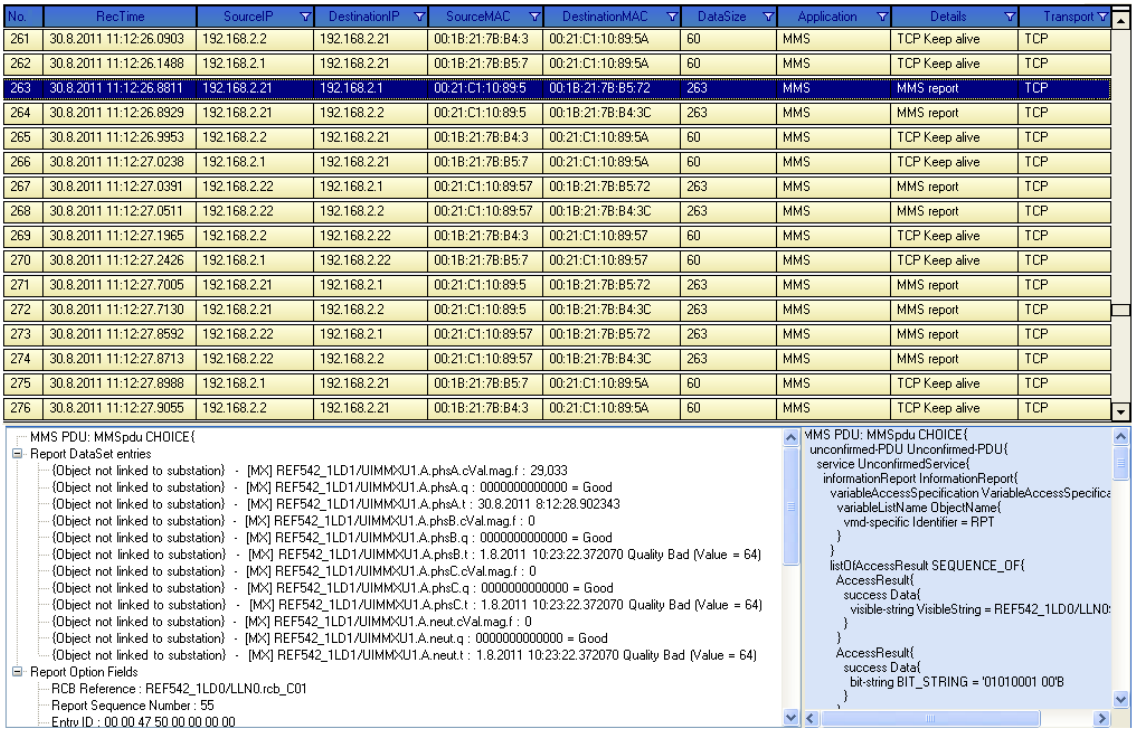


Figure 63. Traffic of LAN A with an MMS frame analyzed in ITT600.

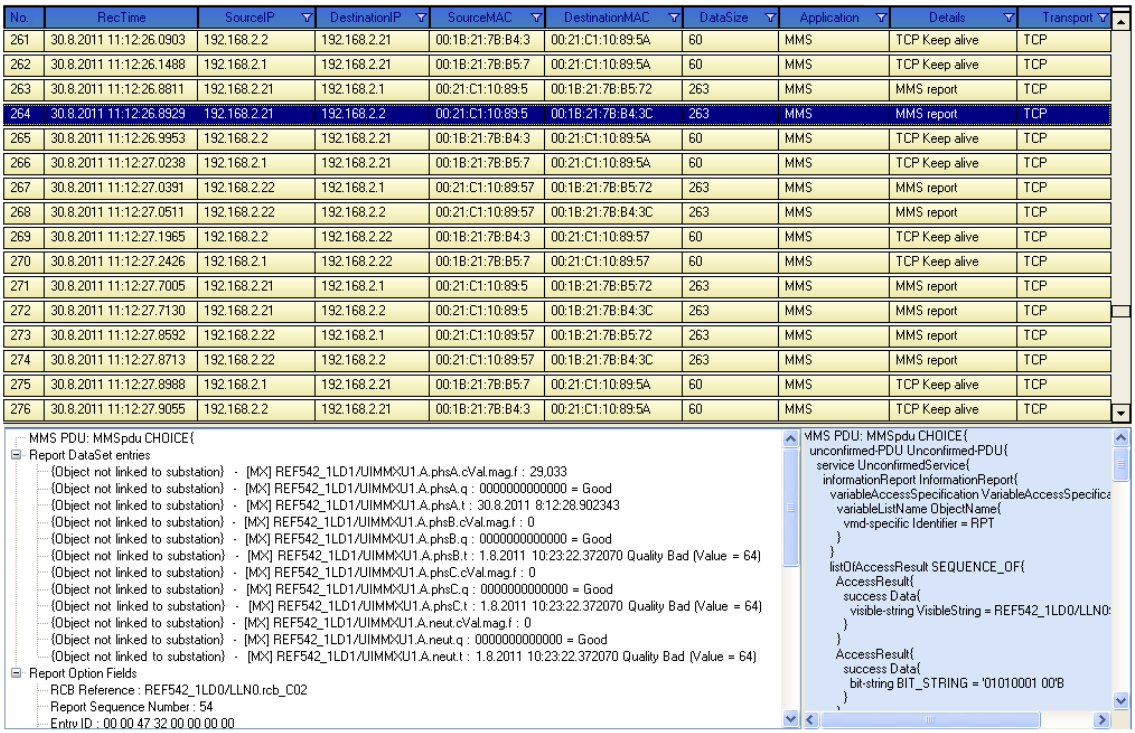


Figure 64. Traffic of LAN A with an MMS frame analyzed in ITT600.

As seen from the captures and analyzed frame, a measurement value is sent to both MicroSCADA computers, with at time interval of about 10 milliseconds, sometimes less. The measurement analyzed in the pictures presents the current value of phase A, 29.033 A (Logical Node *UI*MMXU*1*). This is the real value that IED sends and it is a good reference to check if there is a problem with measurement scaling in MicroSCADA. Other measurement values in the dataset are not sent because only A-phase is simulated with relay test unit. Every MMS report is sent to both computers, providing uninterrupted communication in the case of HSB switchover.

The HSB switchover was also tested, and it functioned rapidly. The switch-over time was noticed to be less than a second. Because of the fact that IEDs send the events to both HSB computers and the buffers in OPC DA clients store the changes, no event loss happens during switchover.

6.3 Conclusions of the test procedure

The performed test measurements confirmed that the PRP operation with the ABB IEDs and MicroSCADA is in accordance with the standard IEC 62439-3 2010. The first two tests showed that the structure of the Redundancy Control Trailer and PRP supervision frame were according to IEC 62439-3 2010 as well as the identical traffic in the networks between doubly attached nodes. The third and fourth test investigated the failure of the other LAN of PRP network while the fifth test confirmed the communication of singly attached nodes. The traffic analysis before and after DuoDriver performed in the sixth test confirmed the operation of DuoDriver accordant to the Link Redundancy Entity -layer (described in Chapter 5.2.2) duplicating the frames on egress and discarding the frames on ingress. The seventh test examined the case if the two LANs were connected, resulting in a non-operable network. The last two tests studied the PRP duplicate accept -mode of DuoDriver and a MMS traffic with IEC 61850 and HSB with a sample.

As a conclusion of the tests made, we can say that PRP is basically ready to be utilized in the projects of the ABB project group. However, the PRP-1 version with its modifications to the original standard is worth further investigation, especially to find out how it will affect to present devices and systems. In addition, at the time of writing this, no RedBoxes are available on the market, and the only protection IEDs that support PRP are REF542plus and Relion® 670 series IEDs.

The PRPs effect on extra work in engineering was quite small when building the test network. Because the PRP is operated at the link layer, devices have only one MAC and IP address and other network protocols (including GOOSE and Sampled Values) work as normally, which makes the engineering more effortless. The additional influence for the engineering work is the DuoDriver installation and configuration in MicroSCADA computers, and the configuration of supervision of the DuoDriver state to MicroSCADA supervision process display. In addition, since the network is doubled, the configuration work of the Ethernet switches also doubles. Carefulness is also needed in the network configuration with the following rules: not to connect the LANs in any

case, and to connect the ports of the devices to right LANs. Luckily, error counters in the DuoDriver (both in MicroSCADA computer and REF542plus) will show and detect these situations. Also RedBoxes can require some extra configuration work compared to normal network with singly attached IEDs.

It was also discovered that Wireshark used along with ABB ITT600 is good means for analyzing IEC 61580 based network traffic. ITT600 can decode the MMS messages for further examination, while Wireshark understands almost every known protocol, including PRP. While ITT600 is ABB internal only, Wireshark is available for everybody to use.

It is worth mentioning that the DuoDriver installed on the MicroSCADA computer for PRP test is not going to work with HSR protocol, because it needs the hardware-implemented switching logic between the ports. Thus, the MicroSCADA computer must be attached through RedBox. One solution with HSR is to connect the MicroSCADA computer to two RedBoxes and use NIC teaming for the computer ports.

7 CONCLUSIONS

The purpose of this thesis was to investigate the redundancy protocols used in IEC 61850 based substation automation systems. Especially, the new high-availability IEC 62439 redundancy protocols Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) were investigated, as they will gradually come to use in the substation automation projects of the target company. Furthermore, a test procedure was performed with PRP to investigate the operation and performance of the protocol and what must be taken into consideration when building a PRP system with ABB IEDs and MicroSCADA supervision software. In addition, some of the main features of the IEC 61850 standard and some reliability aspects were examined.

First, an overview of IEC 61850 standard was made. IEC 61850 has gained a lot of popularity after its publication and is becoming the main standard for substation automation. It standardizes the communication inside a substation with objectives for device interoperability, free system architectures and long-term stability of the standard. The extensions of the standard expand its area outside substation, enabling a way towards smart grids. They will also observe substation communication network redundancy aspects, which were examined in this thesis. IEC 61850 is an important international standard, which will bring improvements in the areas of cost and performance for the whole substation automation system.

After the IEC 61850 overview, the reliability aspects and topologies of a substation communication network were discussed. The operation of the substation communication network must fulfill the IEC 61850 requirements for communication reliability and availability. To enable this, the communication devices in the substation are hardened for the industrial environmental conditions and the communication network is improved with redundancy protocols and methods. It is crucial to supervise the redundancy and its state to gain the full benefit of it. What comes to network topologies, the most common one in substation automation at the moment is the ring topology, which offers an additional link for redundancy. It was also found out that fiber optics should be used as preferred communication media inside substations.

The present redundancy protocols and methods were clarified next. The Rapid Spanning Tree Protocol (RSTP) has been the most widely used protocol to bring redundancy to the communication network. It is implemented to Ethernet switches and effectively introduced in ring topology. With efficient implementation and 100 Mbit/s links, it provides recovery times of a class of 5 ms per each Ethernet switch in addition to fault detection time (also a class of 5 ms). The RSTP is often combined with dual homing (NIC teaming) to provide redundant links to end devices, especially with server computers.

The main focus for this thesis was the high-availability redundancy protocols standardized in IEC 62439 and adopted by IEC 61850: PRP and HSR. Both the protocols provide seamless (0 second) recovery time. The starting point for the usage of these protocols is the fact that the reliability of communication network becomes more important as the GOOSE messages and especially process bus applications (Sampled Values) are used, as their operation depends on the availability of the communication network. This is the main reason why there is a need for redundancy protocols with more rapid recovery time than RSTP can provide and which can fulfill even the most demanding requirements of IEC 61850.

Both the Parallel Redundancy Protocol and High-availability Seamless Redundancy bring a new viewpoint for the redundancy operation compared to RSTP and others. Their operation is based on frame duplication and sending over two different paths, which has the effect that the message will still get through to the destination if the other path gets faulty. While PRP uses two separate LANs as the paths for the message, HSR uses the two directions of the ring for redundant communication while not needing Ethernet switches at all. It can be said that PRP offers easy connection of non-redundant nodes whereas HSR allows cost-effective network solutions. What comes to the supervision of redundancy, IEC 61850 objects and Simple Network Management Protocol (SNMP) together provide a good solution. Also, a new device has been introduced to connect devices with one port to redundant networks: Redundancy Box (RedBox).

After the theoretical investigation of the high-availability redundancy protocols, a test procedure of PRP was performed with ABB IEDs and MicroSCADA. Altogether nine tests were made to investigate the PRP operation with the help of network analyzer software. The test showed that the operation and performance of PRP with ABB IEDs and MicroSCADA is accordant with the IEC 62439 standard and that the current version of PRP is ready to be utilized in substation automation. Also some early experience and information of building such setup was gained.

Further research could be needed to find out how the IEC 62439 Amendment 1 will affect to the present version of PRP. It is probable that the new version will gradually replace the older one, as it will also allow the connection between PRP and HSR networks. As the HSR is released on the market in the very near future, it is possible to investigate and apply it in practice and together with PRP in substation automation projects of the project department. The first projects will show more details that must be taken into account when using HSR as a redundancy protocol.

The IEC 61850 redundancy protocols investigated in this thesis are needed to fulfill different requirements for redundancy. While the basic level for redundancy is provided by RSTP, higher requirements are fulfilled by PRP and HSR that will provide seamless recovery. These two protocols do their justice in applications that need high availability of the communication network. These are GOOSE messages, and particularly process bus communication, which is still awaiting its proper breakthrough in IEC 61850 based substation automation systems.

REFERENCES

ABB Oy (2006). *Lon Bus Connection Devices: RER_, SPA-ZC_* [online]. Product guide [cited 8.6.2011]. Available from World Wide Web: <URL: http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/8b937c13a19ffd03c125717600257b5d/$file/lonbconndev_pg_750435%20enc.pdf>.

ABB Oy (2009a). *Self supervision techniques, 670 series – Principles and functions* [online]. 670 series document [cited 13.7.2011]. Available from World Wide Web: <URL: http://www05.abb.com/global/scot/scot313.nsf/veritydisplay/9830608e2e48f75fc12576f10031debf/$file/1mrk580172-xen_a_en_670_series_self_supervision.pdf>.

ABB Oy (2009b). P246 IEC 61850 in Substation Communication. Course material.

ABB Oy (2010a). *ABB review special report: IEC 61850* [online]. The corporate technical journal [cited 3.3.2011]. 64 p. Available from World Wide Web: <URL:http://www05.abb.com/global/scot/scot271.nsf/veritydisplay/ba5c0d1cacc015a7c12577840033f1a2/$file/abb_sr_iec_61850_72dpi.pdf>. ISSN 1013-3119.

ABB Oy (2010b). *Relion protection and control 615 series: IEC 61850 Engineering guide* [online]. Product manual [cited 23.5.2011]. Available from World Wide Web: <URL: http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/d8edc031e801 bbb1c1257721004717af/$file/re_615_iec61850_eng_756475_ene.pdf>.

ABB Oy (2010c). *Line differential protection and control RED 615* [online]. Product guide [cited 2.5.2011]. Available from World Wide Web: <URL: http://www05.abb.com/global/scot/scot229.nsf/veritydisplay/4ba07b7e191d8069c12577990023841a/$file/red615_pg_756500_ene.pdf>.

ABB Oy (2010d). MicroSCADA Pro SYS 600 9.3: System configuration. Configuration manual.

ABB Oy (2010e). MicroSCADA Pro SYS 600 9.3: IEC 61850 System design. Configuration manual.

ABB Oy (2011a). *Bay control REC670/650 – Relion® 670 and 650 series* [online]. Product brochure [cited 12.8.2011]. Available from World Wide Web: <URL: http://abblibrary.abb.com/global/scot/scot349.nsf/veritydisplay/be0ba0c332acf62bc1257830001fd6a5/$file/1MRK511226-SEN_E_en_Bay_control_REC670_650.pdf>.

ABB Oy (2011b). *SVC Release Notes R1-2011.* ABB Switzerland. Unpublished.

ABB DA Online Support (2011). E-mail conversation with application engineer Sven-Åke Sund, 14.6.2011.

Ali, Ikbal & Mini S. Thomas (2010). Reliable, fast and deterministic substation communication network architecture and its performance simulation. *IEEE Transactions on Power Delivery 25:4, October 2010.* 2364-2370.

Andersson, Lars & Klaus-Peter Brand (2000). The benefits of the coming standard IEC61850 for communication in substations. *Southern African Power System Protection Conference, Johannesburg, 8–9 November, 2000.* 6 p.

Andersson, Lars, Klaus-Peter Brand, Christoph Brunner & Wolfgang Wimmer (2005). Reliability investigations for SA communication architectures based on IEC 61850. *IEEE Power Tech, St. Petersburg, 2005.* 7 p.

Bhutani, Amit & Zafar Mahmood (2003). *Using NIC teaming to achieve high availability on Linux platforms* [online]. Dell Power Solutions [cited 21.6.2011]. Available from the World Wide Web: <URL: http://www.dell.com/content/topics/global.aspx/power/en/ps1q03_bhutani?c=us&l=en&cs=555>.

Brand, Klaus-Peter (2004). The standard IEC 61850 as prerequisite for intelligent applications in substations. *IEEE Power Engineering Society General Meeting, June 2004.* 5p.

Brunner, Christoph (2010). Will IEEE 1588 finally leverage the IEC 61850 process bus? *Managing the Change, 10th IET International Conference on Developments in Power System Protection, 2010.* 5 p.

De Mesmaeker, Ivan, Peter Rietmann, Klaus-Peter Brand & Petra Reinhardt (2005). Substation automation based on IEC 61850. *6th regional CIGRÉ conference, Cairo, November 21–23, 2005.* 10 p.

DesRuisseaux, Dan (2009). Use of RSTP to cost effectively address ring recovery applications in industrial Ethernet networks. *ODVA 2009 Conference & 13th Annual Meeting, February 25, 2009, Florida.* 8 p.

Dreher, Andreas (2011). Redundancy for industrial communication networks. *Industrial Ethernet Book, Issue 65.* 28–31. ISSN 1470-5745.

Goraj, Maciej (2010a). *Overview of IEC 61580* [online]. Presentation slides [cited 15.3.2011]. 40 p. Available from World Wide Web: <URL: http://www.lams.cl/libreria/IEC%2061850%20Overview.pdf>.

Goraj, Maciej (2010b). *Introduction to IEEE 1588 v2* [online]. Presentation slides [cited 22.3.2011]. 37 p. Available from World Wide Web: <URL: http://www.lams.cl/libreria/IEEE1588.pdf>.

Grendar, Trond (2011). E-mail conversation with RuggedCom Regional Sales Manager (Scandinavia). 23.9.2011.

Gupta, R.P. (2008). Substation automation using IEC 61850 standard. *15th National Power Systems Conferene, IIT Bombay, December 2008.* 462–466 p.

Hoga, Clemens (2007). New Ethernet technologies for substation automation. *IEEE Power Tech, Lausanne, 1–5 July, 2007.* 6 p.

Hoga, Clemens (2010a). Network solutions and their usability in substation applications. *PAC World Magazine, September 2010 Issue.*

Hoga, Clemens (2010b). *Network redundancy in substation applications* [online]. Siemens AG Germany [cited 9.9.2011]. Available from World Wide Web: <URL: http://romvchvlcomm.pbworks.com/f/Network+redundancy+in+substation+applications_Siemens_Hoga+.pdf>

Hou, Daqing & Dave Dolezilek (2008). *IEC 61850 – What it can and cannot offer to traditional protection schemes* [online]. Schweitzer Engineering Laboratories, Inc. [cited 16.3.2011]. 11 p. Available from World Wide Web: <URL: http://www2.selinc.com/techpprs/6335_IEC61850_DH-DD_20080912.pdf>

IEB Media (2011). Designing industrial Ethernet off-the-shelf [online]. Industrial Ethernet book [cited 14.4.2011]. Issue 57 / 36. Available from World Wide Web: <URL: http://www.iebmedia.com/index.php?id=6659&parentid=74&themeid=255&hpid=2&showdetail=true&bb=1&appsw=1&sstr=deterministic>.

IEC 61850-1 (2003). *Communication networks and systems in substations – Part 1: Introduction and overview.* 37 p.

IEC 61850-3 (2002). *Communication networks and systems in substations – Part 3: General requirements.* 33 p.

IEC 61850-5 (2003). *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models.* 131 p.

IEC 61850-6 (2009). *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs.* 2nd Edition. 215 p.

IEC 61850-7-1 (2003). *Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – principles and models.* 114 p.

IEC 61850-8-1 (2004). *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.*133 p.

IEC 61850-90-1 (2010). *Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations.* 79 p.

IEC 62439-1 (2010). *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods.* 52 p.

IEC 62439-3 (2010). *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).* 58 p.

IEC 62439-3 (2010) Amendment 1 [online]. *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).* 62 p. Inofficial [cited 9.8.2011]. Available from World Wide Web: <URL: http://lamspeople.epfl.ch/ kirrmann/Pubs/IEC_61439-3/WG15-12-04d_62439-3_AMD_HK_101109.pdf>.

IEEE 802.1D (2004). *IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges.* 269 p.

IEEE 1615 (2007). *IEEE Recommended Practice for Network Communication in Electric Power Substations.* IEEE Power Engineering Society. 91 p.

Kanabar, Mitalkumar G. & Tarlochan S. Sidhu (2009). Reliability and Availability Analysis of IEC 61850 Based Substation Communication Architectures. *IEEE Power & Energy Society General Meeting, July, 2009.* 8 p.

Kirrmann, Hubert (2006). *Standard Redundancy Methods for Highly Available Automation Networks – rationales behind the upcoming IEC 62439 standard* [online]. Presentation slides. Available from the World Wide Web: <URL: http://www.iestcfa.org/presentations/etfa06/EFTA06_Kirrmann.pdf>.

Kirrmann, Hubert (2010). *HSR – High Availability Seamless Redundancy: Fault-tolerance in Ethernet networks (IEC 62439-3)* [online]. Presentation slides [cited 6.9.2011]. Available from World Wide Web: <URL: http://lamspeople.epfl. ch/kirrmann/Pubs/IEC_61439-3/IEC_62439-3.5_HSR_Kirrmann.ppt>

Kirrmann, Hubert (2011). *Parallel Redundancy Protocol – an IEC standard for a seamless redundancy method applicable to hard real time Industrial Ethernet* [online]. Presentation slides [cited 8.8.2011]. Available from World Wide Web: <URL: http://lamspeople.epfl.ch/kirrmann/Pubs/IEC_61439-3/IEC_62439-3.4_ PRP _Kirrmann.ppt>.

Kirrmann, Hubert, Mats Hansson & Peter Müri (2007). IEC 62439 PRP: Bumpless recovery for highly available, hard real-time industrial networks. *IEEE Conference on Emerging Technologies and Factory Automation, 25–28 September, 2007.* 1936–1399 p.

Kirrmann, Hubert, Peter Rietmann & Steven Kunsman (2008). Standard network redundancy using IEC 62439. *PAC World Magazine, Autumn 2008 Issue.*

Kirrmann, Hubert, Karl Weber, Olivier Kleineberg & Hans Weibel (2009). HSR: Zero recovery time and low-cost redundancy for Industrial Ethernet. *IEEE Conference on Emerging technologies and Factory Automation, 22–25 September, 2009.* 4 p.

Lamping, Ulf, Richard Sharpe & Ed Warnicke (2011). *Wireshark User's Guide for Wireshark 1.7* [online]. Chapter 7.4 – Time stamps [cited 26.8. 2011]. Available from World Wide Web: <URL: http://www.wireshark.org/docs/wsug_html_ chunked/ChAdvTimestamps.html>.

Mackiewicz, R.E. (2006). Overview of IEC 61850 and benefits. *IEEE Power Engineering Society General Meeting, Montreal, 2006.* 8 p.

Madren, Frank (2004). *Ethernet in Power Utilities Substations – The changing Role of Fiber Media* [online]. A white paper for network engineers [cited 13.6.2011]. GarrettCom, Inc. Available from World Wide Web: <URL: http://www.garrettcom.com/techsupport/papers/utilities.pdf>

McGhee, Jim, Maciej Goraj & Roger Moore (2010). First practical experience with IEEE 1588 High Precision Time Synchronization in high voltage substation with IEC 61850 Process bus. *18th Conference of the Electric Power Supply Industry (CEPSI), Taipei, October 24–28, 2010.* 13 p.

Moore, Roger (2009). Time synchronization with IEEE 1588. *PAC World Magazine, Summer 2009 Issue.*

Moore, Roger & Maciej Goraj (2010). Ethernet for IEC 61850. *PAC World Magazine, September 2010 Issue.*

Oggerino, Chris (2001). *High Availability Network Fundamentals.* Indianapolis: Cisco Press. 237 p. ISBN 1-58713-017-3

Pozzuolio, Marzio (2003). *Ethernet in Substation Automation Applications – Issues and Requirements* [online]. Presentation slides [cited 13.6.2011]. RuggedCom Inc. Available from World Wide Web: <URL: ftp://www.pp5fmm.qsl.br/pub/mateus/wireless_novas/Ethernet%20in%20the%20Substation%20-%20Issues%20and%20Requirements%20v2.pdf>

Pozzuoli, M.P. & R. Moore (2006). Ethernet in the substation. *IEEE Power Engineering Society General Meeting, 2006.* 7 p.

Pustylnik, Michael, Mira Zafirovic-Vukotic & Roger Moore (2008). *Performance of the Rapid Spanning Tree Protocol in ring network topology* [online]. RuggedCom white paper [cited 20.5.2011]. Available from World Wide Web: <URL: http://www.ruggedcom.com/pdfs/white_papers/performance_of_rapid_spanning_tree_protocol_in_ring_network_topology.pdf>. 22 p.

RuggedCom (2011). *Rugged Operating System (ROS®) v. 3.9.1. User Guide* [online]. User manual for use with products RSG2100 and M2100 [cited 16.6.2011]. Available from World Wide Web: <URL: http://www.ruggedcom.com/pdfs/rswitch_soft_userguide/ros_user_guide_rsg2100_m2100.pdf>

Schnakofsky, Alejandro (2011). *Digitizing copper – What to consider for a successful integration* [online]. Presentation slides [cited 30.9.2011]. Available from World Wide Web: <URL: http://www05.abb.com/global/scot/scot299.nsf/veritydisplay/df10955eea73395785257848006cd255/$file/digitizing%20copper%20webinar%20rev2.pdf>.

Schwarz, Karlheinz (2010). *What is Edition 1 and Edition 2 of IEC 61850?* [online]. News on IEC 61850 and related standards [cited 11.10.2011]. Available from World Wide Web: <URL: http://blog.iec61850.com/2010/03/what-is-edition-1-and-edition-2-of-iec.html>.

Sidhu, T.S. & Pradeep K Gangadharan (2005). Control and Automation of Power System Substation using IEC 61850 Communication. *Proceedings of the 2005 IEEE Conference on Control Applications, Toronto, 28–31 August, 2005.* 1331–1336 p.

Siemens (2009). *Siprotec 4 - Ethernet Module EN100 for IEC 61850 with electrical/optical 100 MBit interface* [online]. Product manual [cited 27.9. 2011]. Available from World Wide Web: <URL: http://siemens.siprotec.de/download_neu/devices/1_General/Doku_Protokolle/Englisch/IEC_61850/COM_IEC61850_MODUL_A8_US.pdf>.

Siemens (2010). *Aspects on IEC 61850 Edition 2.0 & Current Activities* [online]. IEEE Power & Energy Society Transmission & Distribution Conference, Latin America, 2010. Conference slides [cited 23.3.2011]. Available from World Wide Web: <URL: http://www.ieee.org.br/tdlamerica2010/T_D_2010_Brasil_paineis_PDF/on%20 08_11/room%202/afternoom/IEC61850%20Edition2_OK_rev01.pdf>

Spectracom (2004). *What is the difference between NTP and SNTP?* [online]. Question response. Spectracom corporation [cited 18.3.2011]. Available from World Wide Web: <URL: http://www.spectracomcorp.com/portals/0/support/pdf/NTP_vs_SNTP.pdf>

Suomi, Frej (2011). Conversation with design engineer (R&D) Frej Suomi. 27.10.2011.

SysKonnect (2002). *Link Aggregation according to IEEE 802.3ad* [online]. SysKonnect White Paper [cited 21.6.2011]. Available from World Wide Web: <URL: http://legacyweb.triumf.ca/canarie/amsterdam-test/References/wp-lag-e.pdf>.

Vargas, Enrique (2000). *High Availability Fundamentals* [online]. California: Sun Microsystems [cited 12.4.2011]. 17 p. Available from World Wide Web: <URL: http://www.sun.com/ blueprints/1100/HAFund.pdf>.

Weibel, Hans (2008). *Tutorial on Parallel Redundancy Protocol (PRP)* [online]. Zurich University of Applied Sciences, Institute of Embedded Systems [cited 13.7.2011]. Available from World Wide Web: <URL: http://www.engineering.zhaw.ch/fileadmin/user_upload/engineering/_Institute_und_Zentren/INES/PRP/PRP_Tutorial.pdf>.

Wilkins, Dennis J. (2002). The Bathtub Curve and Product Failure Behavior: Part one – The Bathtub Curve, Infant Mortality and Burn-in. *Reliability HotWire eMagazine, Issue 21, November 2002.*

APPENDICES

APPENDIX 1. Comparison table of IEC 62439 redundancy protocols

The table below compares IEC 62439 redundancy protocols along with Spanning Tree Protocol, arranged by recovery time. (IEC 62439-1 2010: 23)

Table 11. Features of IEC 62439 redundancy protocols.

Protocol	Solution	Frame Loss	Redundancy protocol	End node attachment	Network Topology	Recovery time for the considered failures
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30 s typical not deterministic
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20 s typical not deterministic
RSTP	IEEE 802.1D	Yes	Within the network	Single	Single meshed, ring	Can be deterministic following the rules of Clause 8
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, cross-connected	1 s worst case for 512 end nodes
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches
MRP	IEC 62439-2	Yes	Within the network	Single	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 ms worst case for 500 end nodes
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0 s
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0 s

APPENDIX 2. IEC 61850 with MicroSCADA and REF542plus

The figures below show the components and tools related to engineering of the MicroSCADA system as well as REF542plus with IEC 61850 (ABB Oy 2010e: 12)

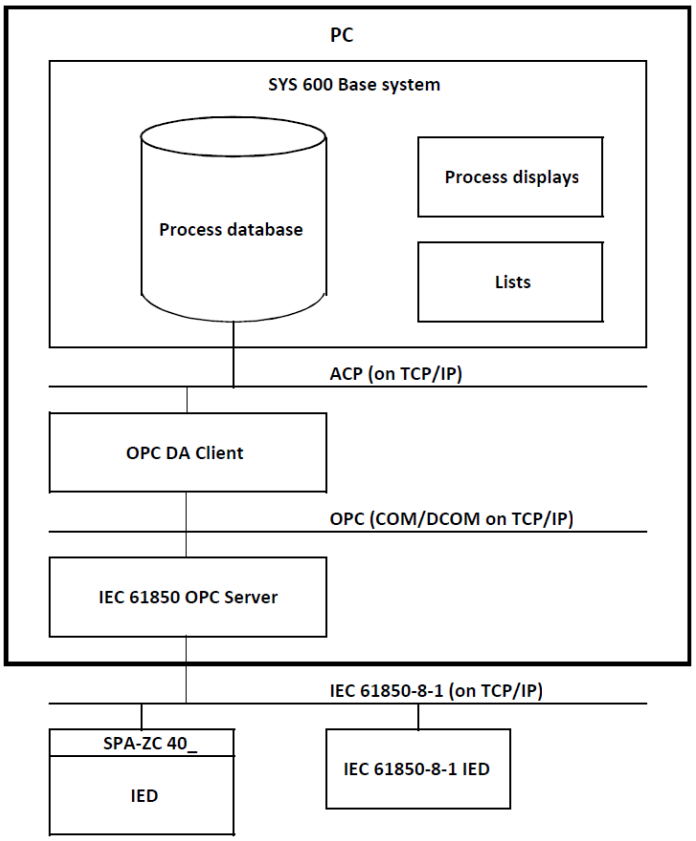


Figure 65. Data flow in MicroSCADA system with IEC 61850.

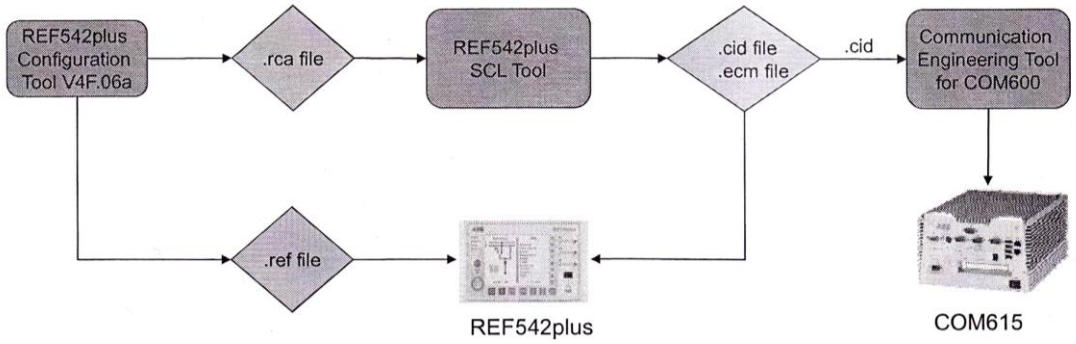


Figure 66. REF542plus engineering work flow with IEC 61850 and SCL. Here, the station computer COM615 is used. (ABB Oy 2009b).

APPENDIX 3. Stand-by DuoDriver status configuration

The DuoDriver status information (supervision of the LAN ports) is available after DuoDriver installation via OPC Server attributes. The stand-by MicroSCADA computer's DuoDriver information is practical to implement into the hot application for supervision. This appendix shows how the stand-by computer's network status information to the hot MicroSCADA application was implemented.

Firstly the DuoDriver and MicroSCADA were installed to the SYS1 computer, the application was made and the process objects for protective relays were imported to the database from CID file using SCL importer. When importing process objects, the 'Create Process Objects for DuoDriver Server Status' -box was checked in the importing options of the SCL importer. This checkbox creates two process objects to the process database: SYS_D0001I:P11 for LAN A status and SYS_D0001I:P12 for LAN B status. It is preferred to assign DuoDriver an own station. In the test setup, the relays were assigned to stations 1–4, and the DuoDriver status of SYS1 was assigned to station 5. These process objects were also linked to the supervision picture.

The DuoDriver status can also be installed using 'Install Standard Function' -tool in the Object Navigator, where DuoDriver Server Status is located under folder 'Supervision'. The OPC path for the DuoDriver status is *Attributes\DuoDriver\Instance\Line\Working*, where 'Instance' is the name given for the network in the DuoDriver installation (Also seen in the DuoDriver management GUI) and 'Line' is the LAN port name (seen e.g. from the Windows Network Connections, preferably renamed in the DuoDriver installation phase). For the correct operation of DuoDriver, the above mentioned two process objects must have the correct station number, OPC path and Block and Object Bit addresses. These also have to match in the OPC DA Client to get the information to the MicroSCADA and to the supervision display. After this configuration, the DuoDriver status information of SYS1 is configured and can be supervised.

In the test setup, SYS1 network instance name was set to *MicroSCADA1* and Line names to *LAN A* and *LAN B*. Respectively, the network instance name of SYS2 was set to *MicroSCADA2*.

After SYS1, the SYS2 was configured. The DuoDriver and MicroSCADA were installed, and the OPC Server and External OPC Client were configured. In the SYS2, the DuoDriver status was assigned to station 6 to identify it for the SYS2. Also two new process objects were created using 'Install Standard Function' -tool to the database: SYS_D0002I:P11 for LAN A status and SYS_D0002I:P12 for LAN B status for the SYS2. The main application in both HSB computers is identical.

Both computers send the DuoDriver status information to each other according to the Figure 67 below. A new instance of External OPC Client sends the DuoDriver status to other computer, where a new LAN Node is made to receive it. The External OPC DA Client can be linked to external MicroSCADA Base System using its IP address under the CPI Node Properties -window. STA 1–4 were assigned to IEDs, STA 5 to DuoDriver status of SYS1 and STA6 for DuoDriver status of SYS2.

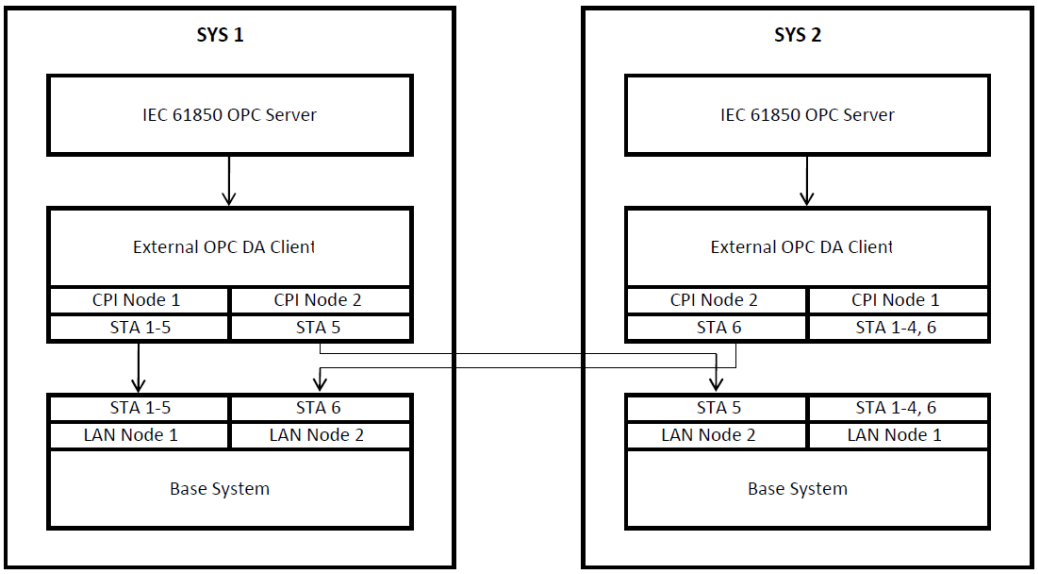


Figure 67. DuoDriver status sending between HSB MicroSCADA computers.

Regardless of the HSB state (which application is hot and which is cold) the DuoDriver status is sent correctly, as they send it to each other all the time. For now, this configuration does not correctly take into account the state when both LANs are disconnected (connection to the other computer External OPC DA Client is lost; the state is not updated). Therefore, it is practical to configure the status information so that

in the case of disconnection of both LANs, it is turned to purple (not sampled, no information available). The same was considered if the MicroSCADA system of the other computer is not running. This can be made e.g. using the Base System Attribute BNT (Base System Node Type) of the external HSB system.

The BNT attribute has the value ‘SYS’ if the connection to MicroSCADA Base System is established and state ‘UNKNOWN’ if it is not. Therefore, a special command procedure was made to set the process objects of the external DuoDriver’s status to ‘not sampled’ when the state of the external NOD:BNT attribute is ‘UNKNOWN’. This command procedure is executed every time a NOD-type system event happens as well as time intervals of one minute. The command procedure takes into account the current hot base system (attribute SYS:BNN). The SCIL code of the command procedure is presented below.

```
#local this_box, result, status_sys1, status_sys2

result= ops_call("ping -n 2 -w 10 192.168.2.1")
status_sys1= result.st
result= ops_call("ping -n 2 -w 10 192.168.2.2")
status_sys2= result.st

#if SYS:BNN=="SYS1" #then #block
   #if NOD10:BNT=="UNKNOWN" OR status_sys2==1 #then #block
      this_box=2
      #SET SYS_D000'this_box'I:1P11 = LIST(OS = 10, SU = 1)
      #SET SYS_D000'this_box'I:1P12 = LIST(OS = 10, SU = 1)
   #block_end
#block_end

#else_if SYS:BNN=="SYS2" #then #block
   #if NOD9:BNT=="UNKNOWN" OR status_sys1==1 #then #block
      this_box=1
      #SET SYS_D000'this_box'I:1P11 = LIST(OS = 10, SU = 1)
      #SET SYS_D000'this_box'I:1P12 = LIST(OS = 10, SU = 1)
   #block_end
#block_end
```

However, in the test application the NOD:BNT did not work correctly in the situation when the LANs were disconnected. For some reason, the value of the attribute does not update automatically. Therefore, ping command was added to the procedure to make it act correctly, as seen in the above code. Thus, if the NOD:BNT attribute of the external application is ‘UNKNOWN’ or a ping does not get response, the status of the external computer’s DuoDriver is set to ‘not sampled’.

The incorrect behavior of NOD:BNT attribute with DuoDriver is worth further investigation.

APPENDIX 4. System overview of PRP test setup