REPORT ON UCAIug 2011 INTEROPERABILITY TEST

IEC 61850 INTEROPERABILITY

FINAL REPORT, JUNE 2011
VERSION 1.0

SEPTEMBER 14, 2011

PROJECT MANAGER
H. FALK, SISCO

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

SISCO, INC

NOTE

For further information about UCA International, contact:

Kay Clinard
UCAIug
10604 Candler Falls Court
Raleigh, NC 27614
Ph: +1-919-847-2241
Fx: +1-919-869-2700
e-mail: kay@ucaiug.org

Citations

This report was prepared by

SISCO, Inc.
6605 19 ½ Mile Rd.
Sterling Heights, MI 48314

Principal Investigator

H. Falk

The test plans and procedures were prepared and edited by:

Herbert Falk (SISCO)
Maciej Goraj (RuggedCom)
Dean Ouellette (RTDS)
Cédric Harispuru (SIEMENS)

This report describes research sponsored by:

UCA International User's Group
American Electric Power
Electric Power Research Institute

A Special Thanks to EDF for hosting the IOP Tests in Paris, France

Description

The UCA International User Group has sponsored/supported the development of IEC 61850 and its testing. The User Group has a very active testing committee regarding the conformance and testing of IEC 61850. Additionally, the User Group is the certifying organization of conformance test results generated by UCA User Group certified test labs.

This interoperability test represents the first sponsorship of a formal set of interoperability tests by UCA International. Prior to this event, interoperability was proven at expositions (e.g. CIGRE or others) or with limited participation (e.g. FGH, Germany) due to a set of vendors deciding to perform the tests.

The difference with these tests, as opposed to others, was:

- The process was open to any vendor.
- There were formal test procedures developed and documented.
- There were third party observers that observed and graded the execution of the test procedures.

The purpose of the tests was to demonstrate interoperability in the exchange of:

- Substation Configuration Language Files
- Generic Object Oriented Substation Events
- Sampled Values
- Client/Server information

Additionally, Ethernet switches and routers were tested for interoperability regarding implementations of the Rapid Spanning Tree Protocol (RSTP).

Results and Findings

To start the test, participants submitted IEC 61850-6 Substation Configuration Language (SCL) files. Several validation tools (Siemens, Kalkitech, and other proprietary tools) were used to validate the correct formation of these models according to the standard. Each participant then attempted to import and utilizes the information in the files for a particular suite of tests (e.g. GOOSE, SV, or Client Server).

The exception to this process was the Network Infrastructure testing. This set of tests started with network topological drawings/connectivity and then proceeded with the procedural testing.

Challenges and Objectives

This report is of interest to any utility professional that is preparing to implement products from multiple vendors that need to exchange or use information from different applications. The data contained in this report provides an overview of the functionality that can be purchased from the various vendors. It also explains the issues surrounding the use and implementation of the standards and the level to which these standards have been implemented by the vendors.

The implementation and general exchange issues discussed in the report will provide data to assist the utility professional in budgeting and scheduling an integration projects using these standards.

As the standards progress, this type of activity becomes increasingly important to provide all players with an in-depth understanding of the standards and the areas that need to be extended to ensure these standards can be implemented/clarified in a cost effective manner.

Our primary challenge in the future is to extend the tests beyond the original participants, increase the degree of coverage, and to educate the industry on the results.

Keywords

SUBSTATION CONFIGURATION LANGUAGE
SUBSTATION
SAMPLED VALUES
RSTP
SNTP
IEC 61850
SCL
GOOSE
RAPID SPANNING TREE ALGORITHM

Abstract

On March 28 – April 1, 2011 in Clamart, France, software and hardware vendors serving the electric utility industry met to test the capability of their products to exchange data and correctly interpret power system data based on the IEC 61850 set of standards. This test represents the first formal interoperability test since the publication of the Edition 1 of IEC 61850 (approximately five years). Prior to this set of tests, IEC 61850 testing has concentrated on conformance testing.

This set of tests focused on interoperability in the following areas: 1) exchanging of configuration information through the use of the Substation Configuration Language (IEC 61850-6); 2) compliance and interoperability testing of the communication services specified by IEC 61850-7-2, IEC 61850-8-1, and IEC 61850-9-2LE; 3) the exchange of a power system functions and data as specified by IEC 61850-7-4; and, the basic Ethernet network infrastructure and resiliency for recovery. This report documents the results of this testing.

There were seventeen (17) vendors participating in these tests and ten (10) witnesses from seven(7) different companies. Personnel from RTDS, RuggedCom, Siemens, and SISCO had the primary responsibility of developing the various test cases.

Preface

The reliability of power grids is an increasingly visible topic in the news today. This is due in large part to the need to operate closer to available transmission capacities than at any time in the history of the electric utility industry. Ever-increasing demand in the face of reduced power plant construction is a major factor.

One way to improve the reliability issue is to improve the availability and timeliness of the real-time power system used to protect and control transmission and distribution systems. This permits operation closer to maximum capacity while avoiding unplanned outages. One key to improve the flow of information is to have common standardized semantics and communication services. The global power system market looks to IEC 61850 to provide this capability.

Several initiatives are underway to increase the scope of applicability of IEC 61850 to beyond intra-substation communication. These initiatives include the use of IEC 61850 for inter-substation as well as substation to control center information exchange. In order to achieve the promise of IEC 61850 for these three use cases, interoperability of various implementations becomes a primary concern.

Although the UCA User's Group has an active Testing Subcommittee, traditionally this committee has focused on conformance testing and not interoperability. Although conformance forms a basis to achieve wider interoperability, it does not represent a multi-vendor graded interoperability "plug-fest".

This report presents the results of the 2011 interoperability test using IEC 61850 to demonstrate multi-vendor information and configuration exchange. The goal of this report is to raise awareness of the importance and status of this effort and to encourage adoption by additional product suppliers and utilities.

Kay Clinard
President, UCAIug
July 2011

Acknowledgments

UCA wishes to thank the many people who worked hard to make the 2011 interoperability test a success. Not all people who contributed can be named here. However, UCA would like to give special recognition to the following witnesses and participants of the interoperability test:

Company		Witnesses
EDF		Thierry COSTE Aurélie DEHOUCK-NEVEU
Enernex		Bruce Muschlitz
KEMA		Bas Mulder Richard Schimmel
RED ELECTRICA DE ESPAÑA, S.A.U.		Carlos Rodríguez del Castillo
Mikronika		Alexander Charkin
KETOP		Zhang Ran He Chum
Endesa S.A.		Jaume Badia Llesuy

Company	LOGOS	Participant Names
Alstom		Andrew Darby Dylan Stewart
ARC Informatique		Jacques Sarot Jean-Sébastien Bourgois Benoît Lepeuple
EFACEC Engenharia e Sistemas, S.A		Rogério Dias Paulo Cláudio Silva
General Electric (GE)		Rafael Pomposo Alberto Huidobro Enrique Gondra Jose Carlos Billalabeitia
Hirschmann Automation & Control		Frank Gudat Johannes Schilling Laurant Witkowski Andreas Dreher
KETOP		Zhang Ran He Chum
OSIsoft		Yves Gauthier
Prosoft-Systems		Ivanov Yuri Borodin Oleg Alexey Lesnov Alexander Pozyuban
RTDS		Dean Ouellette Marc Desjardine Eric Xu

Company	LOGOS	Participant Names
RuggedCom		Maciej Goraj Sajjid Salyani Reinhard Besemer Muhammad Rahman Martin Grinberg
Schneider-Electric		Michael Haecker Mohammed Rafi Didier Giarratano
Schweitzer Engineering Laboratories		Tim Tibbals David Dolezilek Fernando Calero Rich Tolleson Sean Poole
Siemens		Cédric Harispuru Gerhard Wieserner Rudolf Feix Daniel Mai Heiko Englert Clemens Hoga
SISCO		Herbert Falk Margaret Goodrich
Toshiba		Shigeki KATAYAMA Fumio KAWANO Gordon Main
Triangle Microworks		Phil Young George Schimmel
ZIV		David Gil Egoitz Otaola Ferran Castro Jesus Rodriguez Joan Sans Josep Salat

Contents

Table of Figures

Table of Tables

1 Introduction

This document reports the results of the IEC 61850 2011 interoperability tests, which took place on March 28- April 1, in Clamart, France. According to the Gridwise Architecture Council, interoperability testing proves "...the capability of systems, products and units to provide and receive services and information between each other, and to use the services and information exchanged to operate effectively together in predictable ways without significant user intervention..."[1] The standards for this test included various parts of the IEC 61850 standards.

This set of interoperability tests focused on data exchange tests that addressed the following specific interoperability objectives regarding:

- Network infrastructure - the ability of IEC 61850-3 compliant Ethernet switches to interoperate in a multiple vendor environment. Additionally, the ability/performance of those switches to recover from a loss of link or root bridge failure using rapid spanning tree protocol. These test were executed using multiple switch/network topologies and are referred to as "**network infrastructure**" tests.
- Configuration Exchange – The ability of IEC 61850 IED tooling, or System Engineering tooling, to exchange configuration information through the use of IEC 61850-6. There are two (2) suites of tests: "**IED Configuration**" and "**System Configuration Exchange**".
- Exchange of real-time information through the use of IEC 61850-8-1 Generic Object Oriented Substation Event (GOOSE) protocol. This suite of tests is referred to as "GOOSE" testing.
- Exchange of real-time information through the use of IEC 61850-9-2 Sampled Values using the UCA IEC 61850-9-2LE profile. This suite of tests is referred to as "**Sampled Value**" testing.
- Exchange of real-time information through the use of IEC 61850-8-1 Client/Server services.. This suite of tests is referred to as "**Client/Server**" testing.
- Ability to synchronize clocks using the SNTP protocol as specified in IEC 61850-8-1. This testing is referred to as "**SNTP**" testing.

Additionally, these tests were executed in accordance with the IEC 61850 Edition 1 specifications with the appropriate technical issues (e.g. as required by conformance testing) being implemented.

This interoperability test may be the part of a series of IEC 61850 interoperability tests. Goals of future tests are described in Section 4.

---

1 As defined in the GWAC Interoperability Checklist 1.0, http://www.gridwiseac.org/pdfs/gwac_decisionmakerchecklist.pdf

1.1 Scope of the IEC 61850 2011 Interoperability Test

1.1.1 General Test Objectives

The general objectives of the interoperability tests and demonstrations are:

1. Demonstrate interoperability between different products based on the edition 1 IEC 61850 version.
2. Verify compliance with the IEC 61850 for those IEC 61850 files, objects, and services involved in the information exchanges supported by the tests
3. Demonstrate the exchange of configuration information using IEC 61850-6 Substation Configuration Language XML files.
4. Validate interoperability of Rapid Spanning Tree Protocol in a multi-vendor Ethernet switch environment.

Secondary objectives included the following:

5. Validate the correctness and completeness of IEC draft standards, resulting in higher quality standards by removing discrepancies and clarifying ambiguities.
6. Detect ambiguities and issues regarding current deployments.

1.1.2 Expectations

Based upon the number of participants, number of test cases, and test duration, not all participants will be able to test all permutations/combinations of tests/participants. The total number of possible test cases that could be executed, based upon vendor pairings, exceeds 2600 total test cases.

1.1.3 References

1) IEC 61850-6 ED1.0 - Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs

2) IEC61850-7-2 ED1.0 - Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)

3) IEC 61850-7-3 ED1.0 - Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes

4) IEC 61850-7-4 ED1.0 - Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes

5) IEC 61850-8-1 ED1.0 - Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

6) IEC 61850-9-2 ED1.0 - Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3

7) UCA 61850-9-2LE R2-1- Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3

8) IEEE 802.1D-2004 – MAC Bridges

2 SCL System Testing

During the SCL exchange testing, certain categories of issues/problems were encountered:

- SCL VALIDATION

Not all SCL validators validate the data types of initialized values. Additionally, some scl validation was performed through the use of XSD validation only. This means that many IEC 61850-6 mandated validation checks could not be performed.

It also became clear that there was not a single validation tool, brought to the IOP, that could fully validate SCL.

- Guidance for Data Attribute Instance was lacking is several cases.

  In particular, the values to use for Boolean and NULL initial values are not clear in IEC 61850-6.
- The revised XSD file for IEC 61850-6 ED.1 including technical issue changes was never generally released. The released ED.1 XSD schema is version 1.4. The schema, including technical issues, is version 2.0. Since 2.0 was never released, there were some implementations still exporting 1.4 validated SCL that could not be validated using the 2.0 schema.

However, many of the encountered problems were found to be resolved with Edition 2 of IEC 61850-6. Therefore, it is recommended that the edition 2 version of SCL be rapidly adopted in order to achieve wider interoperability.

2.1 Pre-IOP Issues Encountered

During the preparation for the interoperability test, SCL files were exchanged between many of the test participants. The exchanges allowed the detection of interchange and standard issues prior to the actual on-site test. Each of the encountered issues was resolved prior to the actual tests in Paris.

This section details these issues and the resolutions.

2.1.1 Incorrect Data Types for Values

2.1.1.1 Initialized Values

Several of the exchanged files had initialized values that were not of the DataType of the encompassing Data Attribute Instance (DAI). As an example:

```
<DAI name="orIdent" valKind="RO">
<Val>Dummy String</Val>
</DAI>
```

According to IEC 61850 orIdent is an OCTETString and shall be encoded per base64Bindary Coding according to 6.8 or RFC 2045. As an OCTETString, the digits are limited to values 0-9 and A-F. Therefore, the initial value of “Dummy String” does not represent a valid OCTETString value.

Several other similar situations were encountered with floating point values. The offending value was “'f1.000000e-001'“ (e.g. the ‘f’ should not be present).

The problems were aggrevated by the fact that not all of the SCL validators validate the data types of initial values.

2.1.1.1.1 Initalization of Boolean Values

Boolean values are initialized to be values representing True or False. However, IEC 61850-6 is mute on the actual value that should be used. This means that values consisting of: T, F, Yes, No, Y, N, On, Off, and other permutations could all be argued to be valid. Additionally, permutations could include mixtures of capitalization.

Although IEC 61850-6 is mute on the initial value, the World Wide Web Consortium (W3C) is not. W3C defines:

2.1.1.2 boolean

[Definition:] **boolean** has the ·value space· required to support the mathematical concept of binary-valued logic: {true, false}.

2.1.1.2.1 Lexical representation

An instance of a datatype that is defined as ·boolean· can have the following legal literals {true, false, 1, 0}.

2.1.1.2.2 Canonical representation

- The canonical representation for **boolean** is the set of literals {true, false}.
- Therefore, allowed representation should be: true, false, 1, and 0.
- Obviously, with lack of guidance from IEC 61850-6, validators returned mixed results.

2.1.1.2.3 Multiple Initial Values

The following SCL extract was encountered in an exchanged SCL file:

```
<DOI name="StrVal">
   <SDI name="setMag">
      <DAI name="f" valKind="Set">
               <Val> 1</ Val >
               <Val> 2</ Val >
               <Val> 3</ Val >
               <Val> 4</ Val >
       </DAI>
   </SDI>
</DOI>
```

In this extract, it is unclear as to the intent of the SCL. A “f” attribute may only be initialized with a single value, yet the extract shows an attempt to initialize the value with four (4) different values.

Some of the SCL validators actually validated this extract. This is more due to the fact that the XSD in IEC 61850-6 allows multiple initial values, as would make sense for settings groups, but does not explicitly differentiate the constraints as part of the XSD.

Some of the SCL validators went beyond XSD validation and declared an error when this was encountered.

Thus, there is a clear difference in SCL validation versus XSD validation.

2.1.1.3 Settings Group Initial Values

In the following example, it is clear that the SCL file is attempting to initialize the value of setMag for SettingGroup (sGroup) 1 through 4.

```
<DOI name="StrVal">
   <SDI name="setMag">
      <DAI name="f" valKind="Set">
               <Val sGroup="1"/>
               <Val sGroup="2"/>
               <Val sGroup="3"/>
               <Val sGroup="4"/>
```



```
        </DAI>
    </SDI>
</DOI>
```

However, setMag is an analog value and the declaration of the group setting should be interpreted as NULL (e.g. no vlaue). It is unclear, in IEC 61850, if this type of initialization is allowed for values other than string values. The editor of IEC 61850-6 responded to the issue:

"StrVal is a setting. Thus it might have different values in different setting groups. The SCL snippet below could define the values for the setting groups 1 to 4, if the Val element would additionally contain a value. In this form, without a value, it is superfluous (may be even wrong, as an 'empty string' value is probably not allowed for StrVal.setmag, which is an Analogvalue)."

For the purposes of the interoperability tests, the syntax was disallowed except for String value initialization. It was also identified that IEC 61850-6 will need to be updated to provide similar guidance.

2.1.2 Communication Addressing

Similar to initialization of values, the "P-xxx" communication addressing constructs have similar issues.

In an SCL file, it is typical to find:

```
<Address>
    <P type="IP">172.16.2.2</P>
    <P type="IP-SUBNET">255.255.0.0</P>
    <P type="OSI-AP-Title">1,3,9999,23</P>
    <P type="OSI-AE-Qualifier">23</P>
    <P type="OSI-PSEL">00000001</P>
    <P type="OSI-SSEL">0001</P>
    <P type="OSI-TSEL">0001</P>
    <P type="IP-GATEWAY">0.0.0.0</P>
</Address>
```

According to IEC 61850-6, the XSD of a “P” is:

```
<xs:complexType name="tP">
	<xs:simpleContent>
		<xs:extension base="tPAddr">
			<xs:attribute name="type" type="tPTypeEnum" use="required"/>
		</xs:extension>
	</xs:simpleContent>
</xs:complexType>
```

Therefore, XSD validation would allow any value as long as the type value is from the following enumerated list:

```
<xs:simpleType name="tPredefinedPTypeEnum">
	<xs:restriction base="xs:Name">
		<xs:enumeration value="IP"/>
		<xs:enumeration value="IP-SUBNET"/>
		<xs:enumeration value="IP-GATEWAY"/>
		<xs:enumeration value="OSI-NSAP"/>
		<xs:enumeration value="OSI-TSEL"/>
		<xs:enumeration value="OSI-SSEL"/>
		<xs:enumeration value="OSI-PSEL"/>
		<xs:enumeration value="OSI-AP-Title"/>
		<xs:enumeration value="OSI-AP-Invoke"/>
		<xs:enumeration value="OSI-AE-Qualifier"/>
		<xs:enumeration value="OSI-AE-Invoke"/>
		<xs:enumeration value="MAC-Address"/>
		<xs:enumeration value="APPID"/>
		<xs:enumeration value="VLAN-PRIORITY"/>
		<xs:enumeration value="VLAN-ID"/>
	</xs:restriction>
</xs:simpleType>
```

However, for each of the enumerated values, IEC 61850-6 also specifies explicit type constraints. The types, most often found to have invalid values in the actual SCL files, were: MAC-Address, VLAN-ID, and any of the Selector types.

The typical issue with MAC addresses were that SCL files used “:“ to separate the octet values instead of the use of “-” which is prescribed in the XSD:

```
<xs:complexType name="tP_MAC-Address">
	<xs:simpleContent>
		<xs:restriction base="tP">
			<xs:minLength value="17"/>
			<xs:maxLength value="17"/>
```

```
                        <xs:pattern value="[\d,A-F]{2}\-[\d,A-F]{2}\-[\d,A-F]{2}\-[\d,A-F]{2}\-
[\d,A-F]{2}\-[\d,A-
                                    F]{2}"/>
                        <xs:attribute name="type" type="tPTypeEnum" use="required"
fixed="MAC-Address"/>
                </xs:restriction>
            </xs:simpleContent>
        </xs:complexType>
```

The typical issue with VLAN-IDs was the use of less than three digit values and the interpretation that the value is a decimal value. In the XSD provided by IEC 61850-6, it is clear that three hexadecimal digits are required:

```
        <xs:complexType name="tP_VLAN-ID">
            <xs:simpleContent>
                <xs:restriction base="tP">
                        <xs:minLength value="3"/>
                        <xs:maxLength value="3"/>
                        <xs:pattern value="[\d,A-F]+"/>
                        <xs:attribute name="type" type="tPTypeEnum" use="required"
fixed="VLAN-ID"/>
                </xs:restriction>
            </xs:simpleContent>
        </xs:complexType>
```

Many of the SCL files had spaces (e.g. whitespace) between the digit values. This is not allowed per the XSD:

```
        <xs:complexType name="tP_OSI-PSEL">
            <xs:simpleContent>
                <xs:restriction base="tP">
                        <xs:maxLength value="16"/>
                        <xs:pattern value="[\d,A-F]+"/>
                        <xs:attribute name="type" type="tPTypeEnum" use="required"
fixed="OSI-PSEL"/>
                </xs:restriction>
            </xs:simpleContent>
        </xs:complexType>
```

Validators, that used XSD validation only, validated the files with these types of errors. Others, that went beyond XSD validation indicated errors.

Clearly, the XSD validation is not sufficient unless the actual data type is provided within the SCL file. As an example:

<P type="OSI-PSEL" xsi:type="tp_OSI_PSEL">00 00 00 01</P>

If the xsi:type were included in the SCL file, XSD validation would have flagged the error. However, the use of xsi:type is not required in SCL files. Therefore, SCL validation requires more than just XSD validation.

2.2 Issues encountered during on-site tests

Although SCL files were exchanged in advance, some problems were encountered during the actual on-site execution. The following sections help summarize the actual problems/issues.

2.2.1 CID Exchange

In general, the CID SCL exchange was performed as part of the testing of Client/Server, GOOSE, and Sampled Value testing. There are individual test results for each pair/participant included in those testing sections. The encountered interoperability issues follow.

2.2.1.1 Inability to support a DataType

There were several examples of this type of problem.

2.2.1.1.1 Support of Integer 128

The first encountered was the lack of an implementation to support the INT128 SCL datatype. The issue was not in the SCL file exchange itself, rather in the ability to map/support such a value in the implementations memory/application. The resolution to the issue was to map the INT128 to an internal Integer value (e.g. the largest possible range). However, by doing such a mapping, the allowed range of values would be decreased.

It is clear that not all implementations must support Integer 128, and therefore neither implementation was incorrect. However, there was no mechanism to determine this problem in advance since the PICs/PIXIT do not specify which datatypes are supportable. Therefore, it is recommended that the PICS/PIXIT be expanded to include the specification of what IEC 61850 DataTypes, as specified by IEC 61850-7-2, are supportable.

Additionally, IEC 61850-6 ED.2 states:

"INT128 exists only for backwards compatibility reasons, and shall no longer be used."

Thus INT128 should be demoted to INT64, if encountered.

2.2.1.1.2 Double Point Status

In several instances, IEC 61850-7-3 Double Point Status (DPS) were published in GOOSE messages. However, several of the logic processors required programming to actually support DPS mappings as their native status type was Single Point Status (SPS). Therefore, users need to understand that some programming may be required in order to achieve application interoperability based upon SCL file exchange.

2.2.1.2 Communication Service Section Support

In several cases, the CID files were devoid of the CommunicationServices section. This created issues when importing these files into some System Configuration systems and other SCL systems.

Upon investigation, the IEC 61850-6 XSD does allow for the section to be empty. However, upon further investigation, the section should be present for all IEC 61850 publishers (e.g. GOOSE and SV) and servers. It should not need to be present for subscribers or clients.

2.2.1.3 LNPrefix Default Value

ED.1 of IEC 61850-6 does not concretely define the default value that should be assumed if the LNPrefix is not present. The lack of a concrete definition caused some manual reconfiguration to occur in order to allow information exchange between a couple of vendors.

ED.2 of IEC 61850-6 explicitly defines the default value to be “” (e.g. no prefix). Therefore, ED.2 has resolved the issue and the use of “” for a default should be assumed by implementations.

2.2.1.4 Length of Logical Device Names

In IEC 61850-6 ED.1, Logical Device names had a maximum length of 32 characters. However, in ED.2, the length has been extended to support 64 characters. The extension to 64 characters was done on the basis of IEC 61850 Technical Issue 130. Therefore, implementations should be able to support the full 64 character length.

IEC 61850-6 ED.2 specifies a 64 character maximum length.

2.2.1.5 DataObject vs. Data Attribute Names

During one of the exchanges, there were two different interpretations of Data Object Name (DOName) and Data Object Name (DAName). IEC 61850-6 ED.1 is not clear in regards to the segmentation of hierarchical naming. This made it difficult, in some test cases, to determine if a FCDA (DAName) or DO (DOName) was being tested/exchanged.

The particular discussion involved was xxx.cval.mag a DOName or DAName.

IEC 61850-6 ED.2 clarifies and concretely defines the differentiation. ED.2 defines a DOName can only contain the name hierarchy up to the first encountered FCDA. Therefore, the example of xxx.cval.mag would be categorized as a DAName.

2.2.1.6 Configuration Revision (Confrev) Maintenance

During the SCL exchanges, some SCL changes were made and the exporters did not update the SCL Confrev. In order to accurately detect if changes have occurred, the value of Confrev needs to be incremented when any change is made to the contents of an SCL file that has already been exchanged. Additionally, it is recommended that:

- IEC 61850 Clients verify that the SCL configuration matches with the configuration of the IED before information exchange.

- The testing of Confrev be a test case for future interoperability/conformance tests.

2.2.1.7 Initialization of Control Model (ctlModel)

During the IOP testing, it became clear that the ctlModel attribute is mandatory for certain Data Objects (DOs) such as Mod (Mode). However, not all servers allow the control of Mod. Therefore, there was a discussion regarding how to conform with the mandatory requirement of ctlModel of being present, but having a server that does not allow control on a particular DO.

The decision, for interoperability, is that the ctlModel value should be “StatusOnly” to reflect that the DO is not controllable.

It also became clear that the actual value of ctlModel needs to be validated by clients since local action can change the value and such a change could cause a client’s control action to fail at an inopportune time.

2.2.2 SCD Exchange

There were three vendors that attempted to import CID files to create SCD files. Two of the vendors attempt to exchange SCD files. These were the two vendors that provided System Engineering Tools to be tested during the IOP. Other vendors provided IEDs and IED configuration tooling.

2.2.2.1 Creation of SCD Files from CID

The following table shows the results companies that imported CID files to create an SCD file. The table shows which files the vendors were able to be import. Some of the files, imported, required some of the CID issues (e.g. detailed in the previous section) to be corrected prior to successful import.

It is noteworthy that the SCD testing was low on the priority list to complete and therefore, more time was focused on CID exchange to support IED testing. Thus, no vendor was able to import all available CID file to create a master SCD file.

Table 2-1: System Engineering Tool Results for CID Imports

	Company	ARC Informatique	Efacec Automation	Siemens	Siemens
	System Engineering Tool	PCVUE	Automation Studio	DIGSI	SICAM PAS
CID SCL Providing Company					
Alstom	P545		P		
Efacec Automation	BCU500				
GE	F650				
GE	SR350			P	P
Prosoft-Systems	MC ECA				
RTDS	GTNET				
Schneider-Electric	P139				
Schweitzer Engineering Laboratories	421	P	P		
Siemens	SIPROTECT-4-7SJ64		P		
SISCO	UAP				
Toshiba	GRZ 100				
Traingle Microworks	HAMMER				
ZIV	TPU-1				
ZIV	7IDV				

Note: Due to the number of available witnesses, and the test procedures not allowing vendors to witness other vendor's test, several tests were executed but not witnessed and therefore those results are not shown in the table.

2.2.2.2 SCD File Exchange

Due to time constraints, only two vendors attempted to perform an SCD file exchange. The two companies were: EFACEC and Siemens.

EFACEC attempted to import an SCD file exported by Siemens. A problem occurred during the import. There were problems encountered with the import. However, time did not allow the diagnosis or resolution of the problem.

Siemens attempted to import an SCD file exported by EFACEC. A problem occurred. The problem was diagnosed to be an unsupported XML Namespace issue. Due to lack of time, the problem was not able to be corrected.

The XML Namespace issue is interesting and needs to be the subject of future standards discussions and testing.

3 Client/Server Testing

A formal set of test procedures were prepared and used to conduct and score the tests (see Annex C). These procedures were made available ahead of time and all participants were encouraged to execute as many of these tests as possible prior to coming to Clamart, France.

However, corporate IT security policies typically did not allow the advanced testing to occur. The sole exception was the exchange of SCL CID files.

During the Client/Server testing, certain categories of issues/problems were encountered:

- CID/SCL issue

  The specifics of these issues can be found in chapter 2.

- There was a discussion regarding the Floating Point Not-a-Number (NAN)

  During a information exchange, a server returned a floating point value of -0 (known as Not-a-Number). The client did not initially accept the value. NAN is a valid 61850 and IEEE floating point number thus 61850 clients need to be able to accept/process such a value. The actual processing is considered a local issue.

- The filename specification/directory information to retrieve COMTRADE files (and files in general) is ambiguous leading to problems in file transfer.

  Upon investigation, ISO/IEC 9506 is clear that a MMS file directory response returns filenames that include a fully qualified "path". MMS requires that the fully qualified path name be used to transfer a file.

  Therefore, IEC 61850-8-1 ED.2 was updated to reflect the requirements of ISO/IEC 9506. Therefore, FileDirectory responses shall return a filename that includes a fully qualified path. In order to transfer a file, the filename (e.g. fully qualified name) shall be required.

- There was a discussion about how a client should handle/process a timestamp whose timestamp accuracy is unspecified (allowed in IEC 61850).

  The conclusion was that the processing is a local issue and dependent upon the local application's use of the timestamp information.

3.1 Participants and Their Products

All participants in this test were supposed to have the opportunity to spend four full days at the test site in Clamart, France. However, due to Ethernet and IP networking configuration issues, actual testing time was limited to three (3) days.

Participants brought their own hardware/software to use in the test. The SCL files used for testing were loaded onto a file server that was used for exchange.

Participants were allowed to correct deficiencies or errors found during testing and then, as time permitted, retest. All official testing took place on-site in Clamart, France.

Each participant was required to use an actual product(s) so that testing would demonstrate interoperability of real products. The participants and their products are listed in Table 3-1 that follows.

Table 3-1 Participants and Their Products

VENDOR	PRODUCT NAME	
	CLIENT	SERVER
ALSTOM		MICOM P545RELAY
ARC INFORMATIQUE	CIMWAY/PCVUE	
EFACEC AUTOMATION	AUTOMATION STUDIO V2 UC500 STATION SERVER	BCU 500 BAY CONTROLLER V2
GENERAL ELECTRIC		1.) F650 RELAY 2.) SR3 RELAY
OSISOFT	61850 INTERFACE	
PROSOFT SYSTEMS	MC ECA	
SCHNEIDER ELECTRIC - ENERGY		P139 RELAY
SIEMENS	SICAM PAS	SIPROTEC 4-7SJ64 RELAY
SISCO	AXS4-61850	
SCHWEITZER ENGINEERING LABORATORIES		421 RELAY
TOSHIBA		GRZ100 RELAY
TRIANGLE MICROWORKS	HAMMER	
ZIV	TPU-1 CPT	7IDV RELAY

A description of each product used in the tests is contained in Appendix A.

There were forty-nine (49) possible combinations for testing the twenty-nine (29) possible test cases. This combination created approximately 1400 tests that could have been executed. Based upon the number of possible tests to be executed, not all tests were executed in all possible combinations.

3.2 Interoperability Test Results

Note: The actual test cases definitions are found in Appendix C.

3.2.1 Test Results for SCL File exchange and Configuration

3.2.1.1 Servers providing SCL files

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P						P			
Efacec Automation	Automation Studio										
Efacec Automation	UC500						P	P	Not Recorded		P
OSIsoft	61850 Interface								P		
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					P		P			
ZIV	TPU-1										
ZIV	CPT				P					P	

3.2.1.2 Clients importing SCL files

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P						P			
Efacec Automation	Automation Studio							P	Not Recorded		
Efacec Automation	UC500						P	P			P
OSIsoft	61850 Interface			P					P		
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					P		P			
ZIV	TPU-1										
ZIV	CPT				P					P	

3.2.2 Test Results for Reading Functionally Constrained Data

In IEC 61850-8-1, the reading of Functionally Constrained Data (FCD) has the end result of reading a data structure. The following section details all of the test results for this testing.

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio										
Efacec Automation	UC500										
OSIsoft	61850 Interface										
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					P		P			
ZIV	TPU-1										
ZIV	CPT				F –N1						

N1 - Not implemented or configured in the client.

3.2.3 Test Results for Reading Functionally Constrained Data Attributes

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio							P			
Efacec Automation	UC500						P	P	P		P
OSIsoft	61850 Interface			P					P		
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					P		P			
ZIV	TPU-1										
ZIV	CPT				P					P	

3.2.4 Test Results for Control

3.2.4.1 Direct Control

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio							P			
Efacec Automation	UC500						P	P	P		P
OSIsoft	61850 Interface										
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER							P			
ZIV	TPU-1										
ZIV	CPT				P					P	

3.2.4.2 Select Before Operate

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue										
Efacec Automation	Automation Studio										
Efacec Automation	UC500										
OSIsoft	61850 Interface										
Siemens	SICAM PAS										
SISCO	AXS4-61850	P									
Traingle Microworks	HAMMER										
ZIV	TPU-1										
ZIV	CPT										

3.2.4.3 Select Before Operate with Enhanced Security

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
Arc Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio							P			
Efacec Automation	UC500						P	P	P		
OSIsoft	61850 Interface										
Siemens	SICAM PAS										
SISCO	AXS4-61850										
Traingle Microworks	HAMMER										
ZIV	TPU-1										
ZIV	CPT										

3.2.5 Test Results for Buffered Reporting

3.2.5.1 Enabling

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio										
Efacec Automation	UC500						P	P	P		P
OSIsoft	61850 Interface			P							
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Triangle Microworks	HAMMER					P		P			
ZIV	TPU-1										
ZIV	CPT				P						

3.2.5.2 Resynchronization

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU500	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio										
Efacec Automation	UC500						P	P	P		P
OSIsoft	61850 Interface			P							
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					N1		P			
ZIV	TPU-1										
ZIV	CPT				P						

N1 - When a client enables one of the BRCBs the reports are sent to all connected clients. There is no way to keep track of who received what, so it will just send the first available report in the buffer to all – writing the entryId is not possible

3.2.5.3 Purging

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio										
Efacec Automation	UC500										P
OSIsoft	61850 Interface								P		
Siemens	SICAM PAS										
SISCO	AXS4-61850	P					P				
Traingle Microworks	HAMMER					N1		P			
ZIV	TPU-1										
ZIV	CPT				N2						

N1 - When a client enables one of the BRCBs the reports are sent to all connected clients.
N2 – Not supported by Client.

3.2.5.4 Test Results for UnBuffered Reporting

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
	Product	P545	BCU	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
Company											
ARC Informatique	CimWay/ PcVue	P									
Efacec Automation	Automation Studio										
Efacec Automation	UC500							P			
OSIsoft	61850 Interface			P							
Siemens	SICAM PAS										
SISCO	AXS4-61850	P	P				P				
Traingle Microworks	HAMMER					P					
ZIV	TPU-1										
ZIV	CPT				P					P	

3.2.5.5 Test Results for COMTRADE File Transfer

	Company	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	Toshiba	ZIV
Company	Product	P545	BCU	F650	SR350	MCECA	P139	421	SIPROTECT-4-7SJ64	GRZ 100	7IDV
ARC Informatique	CimWay/ PcVue										
Efacec Automation	Automation Studio										
Efacec Automation	UC500								P		N1
OSIsoft	61850 Interface										
Siemens	SICAM PAS										
SISCO	AXS4-61850	P					P				
Traingle Microworks	HAMMER										
ZIV	TPU-1										
ZIV	CPT										

N1 – Could not accomplish the test due to IEC 61850-8-1 FileDirectory/FileOpen interpretation issue.

Note: File directory of /COMTRADE/* was used to retrieve file listing. Some vendors returned names that were not fully qualified. Client automatically concatenated to create the fully qualified filename for Open. This replicated similar results that other vendors had during the FGH testing. The cause of returning non-fully qualified names was determined to be an ambiguity in IEC 61850-8-1 ED.1 which is to be corrected in ED.2.

4 GOOSE Testing

A formal set of test procedures were prepared and used to conduct and score the tests (see Annex D). These procedures were made available ahead of time and all participants were encouraged to execute as many of these tests as possible prior to coming to Clamart, France.

However, corporate IT security policies typically did not allow the advanced testing to occur. The sole exception was the exchange of SCL CID files.

During the GOOSE testing, certain categories of issues/problems were encountered:

- CID/SCL issue - The specifics of these issues can be found in chapter 2.
- Additionally, it many IEDs had limited number of GOOSE subscriptions and SCL had no mechanism to allow this type of information to be exchanged.
- There was a discussion about the default use of VLAN ID 0.
- It was decided that the use of VLAN ID=0 in GOOSE or SMV traffic need to be further clarified in IEC 61850. In default configuration most of Ethernet switches will be retagging VLAN ID 0 by a valid VLAN ID value configured in PVID and will be removing the whole VLAN tag as in most default configurations all egress ports are configured as untagged. Therefore , it is recommended that operational systems shall have default configuration changed in order to make use of VLAN and priority information. However the default value of VLAN ID 0 in IEDs and default configuration of Ethernet switches can be used for a quick out-of-the-box system integration
- Due to VLAN ID 0 default, and MAC HASH filtering in IEDs, a GOOSE subscriber received SV traffic which caused instability of communication processing.
- The underlying issue, besides VLAN 0, is the fact that IEDs typically use MAC HASH mechanisms for hardware multicast address filtering (e.g. subscription). Depending upon the HASH algorithm, there is a 1:64 or 1:128 probability that two different destination multicast MAC Addresses will generate the same HASH value. In such a instance, both sets of traffic will be delivered to the IED unless the switch enforces VLAN and/or MAC filtering.
- Ethernet switches, unlike many IEDs, utilize perfect matching for MAC Addresses as opposed to HASH codes. Therefore, port traffic restriction is possible within the switch based upon destination multicast address in addition to VLANs.
- Based upon IOP participant discussion, it is recommended that MAC Filtering be utilized in addition to VLANs.
- Functionally Constrained Data (FCD) and Functionally Constrained Data Attribute (FCDA) support for GOOSE DataSet members was varied.
- It is clear in the test result matrixes, that many publishers only have the ability to publish FCDA DataSet members. Additionally, many subscribers also have a similar restriction. Although this behavior is non-conformant to IEC 61850 (e.g. IEC 61850

requires support for both), it is the state of the implementations tested. Therefore, to achieve GOOSE interoperability, FCDA DataSet members will need to be used.
- Additionally, it is recommended that the PIXIT templates be updated to allow improved documentation.

4.1 Participants and Their Products

All participants in this test were supposed to have the opportunity to spend four full days at the test site in Clamart, France. However, due to Ethernet and IP networking configuration issues, actual testing time was limited to three (3) days.

Participants brought their own hardware/software to use in the test. The SCL files used for testing were loaded onto a file server that was used for exchange.

Participants were allowed to correct deficiencies or errors found during testing and then, as time permitted, retest. All official testing took place on-site in Clamart, France.

Each participant was required to use an actual product(s) so that testing would demonstrate interoperability of real products. The participants and their products are listed in Table 4-1 below.

TABLE 4-1
PARTICIPANTS AND THEIR GOOSE RELATED PRODUCTS

Vendor	Product Name	
	Publisher	Subscriber
Alstom	MiCOM P545Relay	MiCOM P545Relay
Efacec Automation	BCU 500 Bay Controller v2	BCU 500 Bay Controller v2
General Electric	1.) F650 Relay 2.) SR3 Relay	1.) F650 Relay 2.) SR3 Relay
Prosoft Systems	MC ECA	MC ECA
RTDS	GTNET-GSE	GTNET-GSE
Schneider electric - Energy	P139 Relay	P139 Relay
Siemens	SIPROTEC 4-7SJ64 Relay	SIPROTEC 4-7SJ64 Relay
SISCO	Unified Analytic Platform (UAP)	UAP
Schweitzer Engineering Laboratories	421 Relay	421 Relay
Toshiba	GRZ100 Relay	GRZ100 Relay
Triangle Microworks	Hammer	Hammer
ZIV	TPU-1 7IDV Relay	TPU-1 7IDV Relay

4.2 SCL Exchange

	Company (subscriber)	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	RTDS	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	SISCO	Triangle	Toshiba	ZIV	ZIV
Company (Publisher)	Product	P545	BCU500	F650	SR350	MC ECA	GTNET	P139	421	SIPROTECT-4-7SJ64	UAP	ANVIL	GRZ 100	TPU-1	7IDV
Alstom	P545				P – N3						P				
Efacec Automation	BCU500				P		P	P	P		P				P
GE	F650					F – N2	P						P		
GE	SR350	P – N4	P			F – N2	P	P – N3		P			P		P
Prosoft-Systems	MC ECA			P	P		P	P			P		P		
RTDS	GTNET		P	P	P	F – N2		P					P		P
Schneider-electric	P139		P		P	F – N2	P		P		P	P	P		
Schweitzer Engineering Laboratories	421		P					P							
Siemens	SIPROTECT-4-7SJ64 PAS				P										
SISCO	UAP	P	P			F – N2		P					F – N2		
Toshiba	GRZ 100			P	P	F – N2	P	P			P				P
Traingle Microworks	HAMMER							P							
ZIV	TPU-1														P
ZIV	7IDV		P		P		P						P	F – N2	

N1 – Not observable since the P545 was unable to map a DPC item internally.
N2 – Prosoft required manual configuration from contents of SCL File.
N3 – Importer could not initially import file due to an ambiguity in ED1.0 SCL (IEC 61850-6) regarding the default value of LN prefixes if the prefix is not present. This has been resolved in ED2.0.
N4 – Warning generated due to Integer64 datatype.

4.3 FCD Based DataSet

	Company (subscriber)	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	RTDS	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	SISCO	Triangle	Toshiba	ZIV	ZIV
Company (Publisher)	Product	P545	BCU500	F650	SR350	MC ECA	GTNET	P139	421	SIPROTEC T-4-7SJ64	UAP	HAMMER	GRZ 100	TPU-1	7IDV
Alstom	P545					P					P				
Efacec Automation	BCU500														
GE	F650														
GE	SR350					P		P							
Prosoft-Systems	MC ECA	P					P	P			P		P		P
RTDS	GTNET														
Schneider-electric	P139				F – N2	P	P		P		P	P			
Schweitzer Engineering Laboratories	421		P					P							
Siemens	SIPROTECT-4-7SJ64 PAS														
SISCO	UAP	? – N1				P		P							
Toshiba	GRZ 100														
Traingle Microworks	ANVIL														
ZIV	TPU-1														
ZIV	7IDV					P	P						P		

N1 – Not observable since the P545 was unable to map a DPC item internally.
N2 – GE is unable to subscribe for FCD based datasets.

4.4 FCDA Based DataSet

	Company (subscriber)	Alstom	Efacec Automation	GE	GE	Prosoft- Systems	RTDS	Schneider- electric	Schweitzer Engineering Laboratories	Siemens	SISCO	Triangle	Toshiba	ZIV	ZIV
Company (Publisher)	Product	P545	BCU500	F650	SR35 0	MC ECA	GTNET	P139	421	SIPROTECT -4-7SJ64	UAP	HAMMER	GRZ 100	TPU-1	7IDV
Alstom	P545				P	P					P				
Efacec Automation	BCU500				P	P	P	P	P		P				P
GE	F650						P						P		
GE	SR350	P	P			P	P	P		P			P		P
Prosoft- Systems	MC ECA	P		P	P		P	P			P		P		
RTDS	GTNET		P	P	P	P		P					P		P
Schneider- electric	P139		P		P	P	P		P		P	P	P		
Schweitzer Engineering Laboratories	421		P					P							
Siemens	SIPROTECT -4-7SJ64 PAS				P										
SISCO	UAP	P	P			P		P					P		
Toshiba	GRZ 100			P	P	P	P	P			P				P
Traingle Microworks	ANVIL							P							
ZIV	TPU-1														P
ZIV	7IDV		P		P		P						P	P	

4.5 Test Bit

	COMPANY (SUBSCRIBER)	ALSTOM	EFACEC AUTOMATION	GE	GE	PROSOFT-SYSTEMS	RTDS	SCHNEIDER-ELECTRIC	SCHWEITZER [SEL]	SIEMENS	SISCO	TRIANGLE HAMMER	TOSHIBA	ZIV	ZIV
COMPANY (PUBLISHER)	PRODUCT	P545	BCU500	F650	SR350	MC ECA	GTNET	P139	421	SIPROTECT-4-7SJ64	UAP		GRZ 100	TPU-1	7IDV
ALSTOM	P545					NOT TESTABLE					P				
EFACEC AUTOMATION	BCU500														
GE	F650														
GE	SR350							NOT SUPPORTED							
PROSOFT-SYSTEMS	MC ECA	NOT TESTABLE													
RTDS	GTNET		P					I – N1							
SCHNEIDER-ELECTRIC	P139		P		NOT SUPPORTED		P – N1		P		P	I – N3			
SCHWEITZER ENGINEERING LABORATORIES	421		P					P							
SIEMENS	SIPROTECT-4-7SJ64 PAS	P-N4													
SISCO	UAP	P	P					P							
TOSHIBA	GRZ 100														
TRAINGLE MICROWORKS	ANVIL														
ZIV	TPU-1														P
ZIV	7IDV													P	

N1 – When Test Bit is reset, and the Sequence Number is not changed, the values are not processed.

N2 - When Test Bit is in the GOOSE Header, the values are ignored. If the Test Bit is set as part of the quality, the values are displayed.

N3 – If GOOSE Test Bit is set without a State Number change, the change of the bit is not observed.

N4 – Test bit was appropriately generated by publisher, but not processed by the subscriber.

4.6 Time Allowed to Live Detection

	COMPANY (SUBSCRIBER)	ALSTOM	EFACEC AUTOMATION	GE	GE	PROSOFT-SYSTEMS	RTDS	SCHNEIDER-ELECTRIC	SCHWEITZER ENGINEERING LABORATORIES	SIEMENS	SISCO	TRIANGLE	TOSHIBA	ZIV	ZIV
COMPANY (PUBLISHER)	PRODUCT	P545	BCU500	F650	SR350	MC ECA	GTNET	P139	421	SIPROTECT-4-7SJ64	UAP	HAMMER	GRZ 100	TPU-1	7IDV
ALSTOM	P545				P	P					P				
EFACEC AUTOMATION	BCU500				P		P	P	P		P				P
GE	F650					P	P						P		
GE	SR350	P	P			P	P	P					P		P
PROSOFT-SYSTEMS	MC ECA	P		P	P		P	P			P		P		P
RTDS	GTNET		P	P	P	P							P		P
SCHNEIDER-ELECTRIC	P139		P		P	P						P	P		
SCHWEITZER ENGINEERING LABORATORIES	421														
SIEMENS	SIPROTECT-4-7SJ64 PAS		P		P					P					
SISCO	UAP	P	P			P							P		
TOSHIBA	GRZ 100			P	P	P	P	P			P				P
TRAINGLE MICROWORKS	ANVIL							P							
ZIV	TPU-1														P
ZIV	7IDV		P		P	P	P						P	P	

Note: Some TAL periods appeared to be longer than would typically be excepted based upon the observed retransmission curve.

4.7 Control Block Enable/Disable

	Company (subscriber)	Alstom	Efacec Automation	GE	GE	Prosoft-Systems	RTDS	Schneider-electric	Schweitzer Engineering Laboratories	Siemens	SISCO	Triangle	Toshiba	ZIV	ZIV
Company (Publisher)	Product	P545	BCU500	F650	SR350	MC ECA	GTNET	P139	421	SIPROTECT-4-7SJ64	UAP	HAMMER	GRZ 100	TPU-1	7IDV
Alstom	P545										Not Testable				
Efacec Automation	BCU500				P		P		P		P				P
GE	F650					P	P						P		
GE	SR350		P			P	P	P		P			P		P
Prosoft-Systems	MC ECA	P		P	P		P				P		P		P
RTDS	GTNET		P	P	P	P							P		P
Schneider-electric	P139				P								P		
Schweitzer Engineering Laboratories	421														
Siemens	SIPROTECT-4-7SJ64 PAS			P											
SISCO	UAP	P – N1	P			P							P		
Toshiba	GRZ 100			P	P	P	P				P				P
Traingle Microworks	ANVIL														
ZIV	TPU-1														P
ZIV	7IDV		P		P	P	P						P	P	

N1 – demonstrated using local enable/disable since no control block is exposed.

5 SAMpled Value Testing

A formal set of test procedures were prepared and used to conduct and score the tests (see chapter12). These procedures were made available ahead of time and all participants were encouraged to execute as many of these tests as possible prior to coming to Clamart, France.

However, Sampled Values does not lend itself to be tested over the Internet and therefore, no testing was performed prior to arrival. All tested SV publishers and subscribers were found to be interoperable except for a minor SCL issue. One issue encountered was that some implementations were at revision 3 of 9-2LE and others were at version 2 of 9-2LE. Therefore, the 9-2LE version 3 implementations were reconfigured (no code change) to be compatible with version 2 implementations. The underlying issue to the initial interoperability problem was that 9-2LE version 3 has not been made publically available. This is being addressed.

There were three (3) companies which provided publishers and subscribers for testing. The participants, and the tested products, can be found in Table 5-1.

Table 5-1 Participants for Sampled Value Testing

	Product Name	
Vendor	Subscriber	Publisher
Alstom	MiCOM P545Relay	COSI-NXMU
RTDS		GTNET-SV1
Schweitzer Engineering Laboratories	SEL-421SV-MU	

The following sections detail the results of the executions of the test cases.

5.1 SCL Exchange

The following results indicate the ability of a publisher to provide a SCL file that is consumed by the subscriber.

Table 5-2: SV Test Results for SCL Exchange

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	N1	N1

N1- Failed to exchange properly due to lack of a mandatory Data Object being missing in the file.

5.2 9-2LE DataStream

The following sections detail the test results for the interoperability of 9-2LE version 2 data streams. The following table shows that no problems were encountered in the publication/subscription of the data streams.

Table 5-3: SV Test Results for 9-2LE DataStream Exchange

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	P	P

The following sections detail specific investigations into the interoperability of the packet exchanges.

5.2.1 Publication of Sample Count

The ability to convey information for 50 and 60 hertz systems was performed. The test results are in the following tables.

Table 5-4 - SV Test Results for 50Hz

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	P	P

Table 5-5: SV Test Results for 60Hz

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	P	P

5.3 Test of smpSynch

The reactions of the subscribers to the two different values of smpSynch are shown in the following table.

Table 5-6: SV Test Results for smpSynch

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P - N1	P
RTDS	GTNET	P – N1	P

N1 – The P545 continued to process the SV stream even with smpSynch being False.

5.4 Test of Detailed Quality

The following test results show that there are no issues regarding the exchange of detailed quality information in the 9-2LE data streams.

Table 5-7: SV Test Results for smpSynch

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	P	P

5.5 Test of Harmonic Content

The following test results show that there are no issues regarding the exchange of harmonic information in the 9-2LE data streams.

Table 5-8: SV Test Results for Harmonic Content Exchange

	Company (Subscriber)	Alstom	Schweitzer Engineering Laboratories
Company (publisher)	Product	P545	421
Asltom	COSI-NXMU	P	P
RTDS	GTNET	P	P

6 SNTP Testing

IEC 61850-8-1 ED.1 specifies Simple Network Time Protocol (SNTP – RFC 2030) as a possible mechanism for time synchronization. It was decided, upon arrival in Clarmart, to test SNTP interoperability. Since the decision to develop and perform the test was not originally planned, not all vendors had the opportunity to test.

The results in Table 6-1 show that no interoperability issues were encountered.

6.1 Test Case

The test case for SNTP was intentionally kept simple and focused on interoperability and not the precision of the time synchronization.

Test Case: The implementation under test (IUT) will significantly skew its local clock so that the time can be observed. The IUT will then use SNTP to resynchronize with a designated SNTP server. The observer should observe that the local time has been re-synchronized.

6.2 Test Results

The SNTP server was provided by RuggedCom. All IUTs were tested solely against the single SNTP server. The results are shown in Table 6-1.

Table 6-1: SNTP Interoperability Test Results

			SNTP Server
			RuggedCom
Client Company	Product	Operating System	
Alstom Grid	P545		P
Efacec Automation	UC500		P
GE	SR350		P
GE	F650		P
Prosoft- Systems	MCECA		P
Schneider- electric	MICOM P139		P
Siemens	7SJ		P
SISCO	UAP	Windows 2003	P
SISCO	AXS4-61850	Windows 7	P
Toshiba	GRZ100		P
ZIV	7IDV		P

7 Network Infrastructure Testing

The purpose of testing networking devices is to show interoperability between vendors of networking devices compliant to IEC 61850-3. The scope of the interoperability testing is a set of features of layer 2 Ethernet switches that are relevant to IEC 61850 based communication networks typical for electrical substations. This interoperability testing is going to be performed under real life conditions with background traffic generated by a number of IEDs, Merging Units and substation SCADA applications and includes the following main features to be tested:

RSTP

- Multicast filtering

VLAN

- Other advanced features such as IGMP, GMRP, NAT, cyber security, etc., are out of scope of this test.
- This test is limited to IEC 61850 Edition 1, therefore emerging technologies such as redundancy with PRP, HSR or Time Synchronization with IEEE 1588 are out of scope of the test.

The following switch vendors provided Ethernet Switches/equipment that were used to form the basis of the network infrastructure used for the other tests.

Table 7-1 Switch Vendors for Basic Infrastructure

Vendor	Product(s)
Hirschmann	RSR30 MACH 1000
RuggedCom	RS900G RSG2100
Schweitzer Engineering Laboratories	
Siemens	SCALANCE XR324

The following vendors participated in the RSTP testing.

Table 7-2 Switch Vendors for Basic Infrastructure

Vendor	Product(s)
Hirschmann	RSR30 MACH 1000
RuggedCom	RS900G RSG2100
Siemens	SCALANCE XR324

- During the staging of the infrastructure, one vendor's switch was found to have hardware/software interoperability issues. Therefore, that switch was removed from the infrastructure and all other infrastructure tests.

When GOOSE and SV application are configured with VLAN ID=0 then mixing in the same network switches that remove VLAN tag (normal IEEE 802.1Q behaviour) and switches configured to forward this tag ("VLAN Transparent" or "VLAN unaware" modes) will result in forwarding of all frames but the VLAN tag will be removed and priority information will be lost. This is still interoperable as no frames are lost, however it can lead to unexpected behaviour at the application level (priority information removed from GOOSE and SV frames).

Therefore, the use of VLAN ID=0 is not recommended for use in operational substations.

- In regards to RSTP testing, there were the following interesting results:
- The disabling of port auto-negotiation had a major detrimental impact on RSTP recovery times.

  Therefore, it is recommended that auto-negotiation be enabled in order to minimize the RSTP recovery time.

- Highly meshed network topologies should not be utilized in substations if higher speed RSTP recovery is needed to support GOOSE or SV.

7.1 Basic Network Topologies

7.1.1 Single Ring

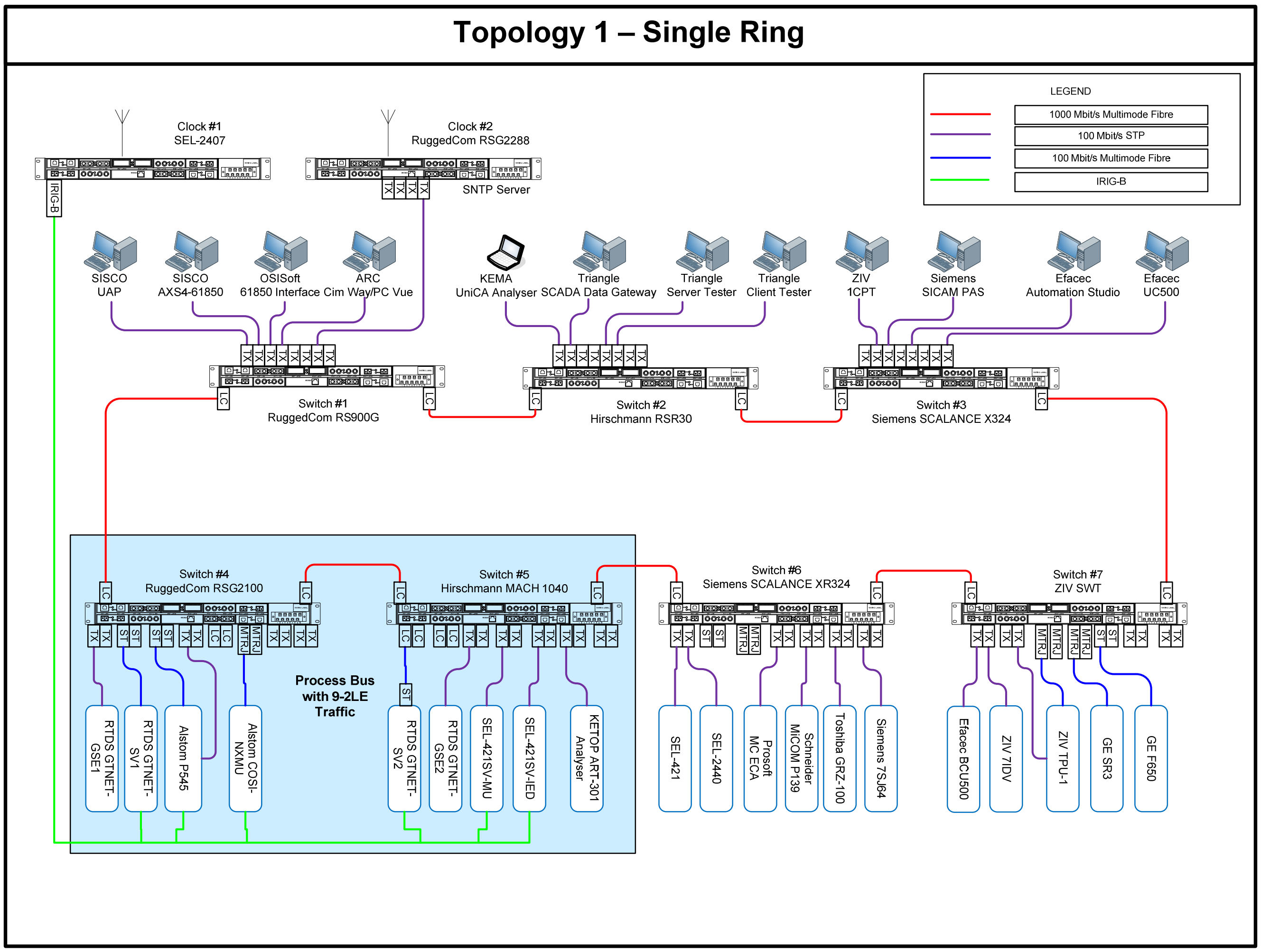


Figure 7-1: Topology 1 - Single Ring

7.1.2 Main ring with two sub-rings

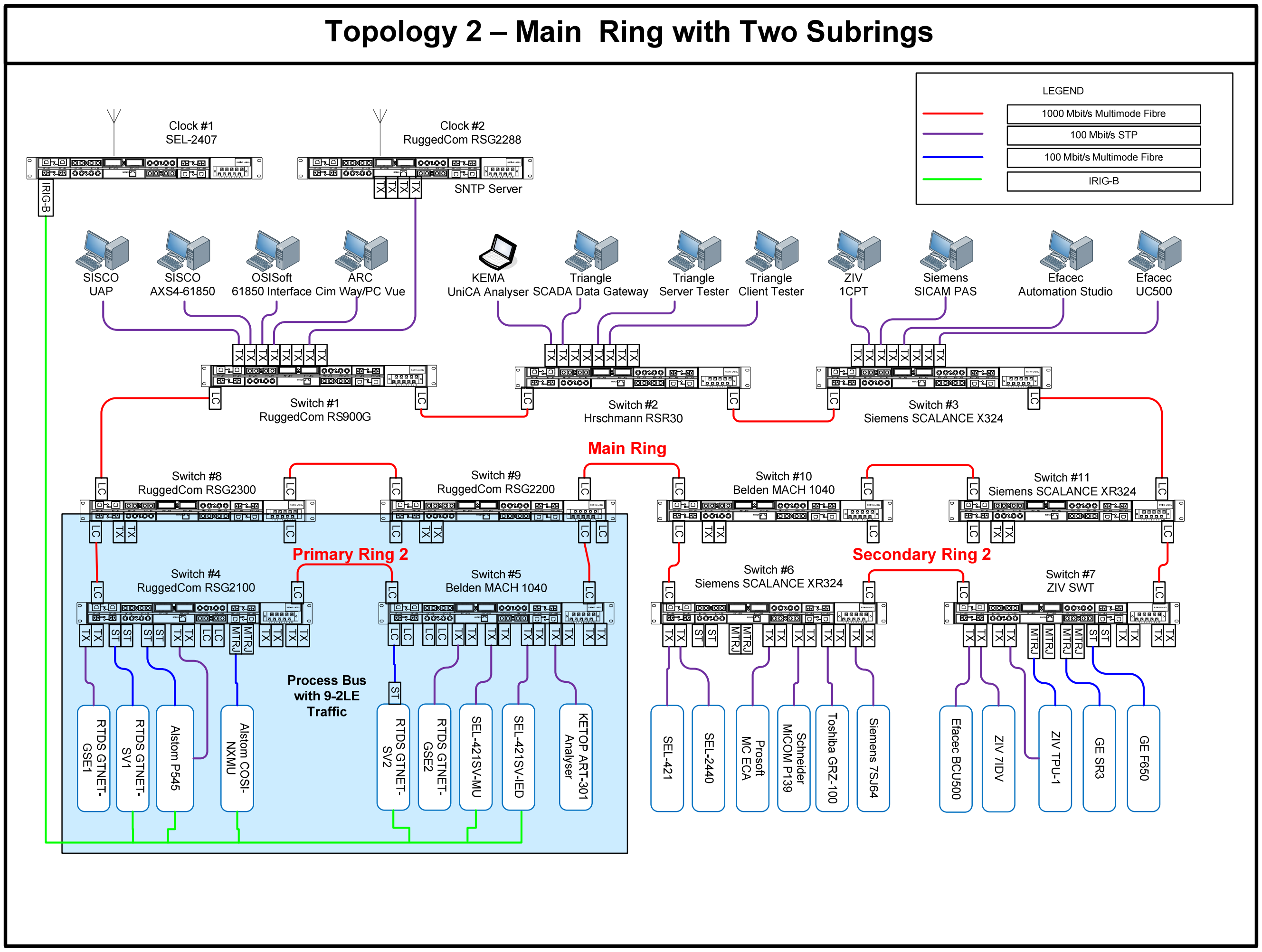


Figure 7-2: Topology 2 – Main ring with two sub-rings

7.1.3 Main ring with mesh

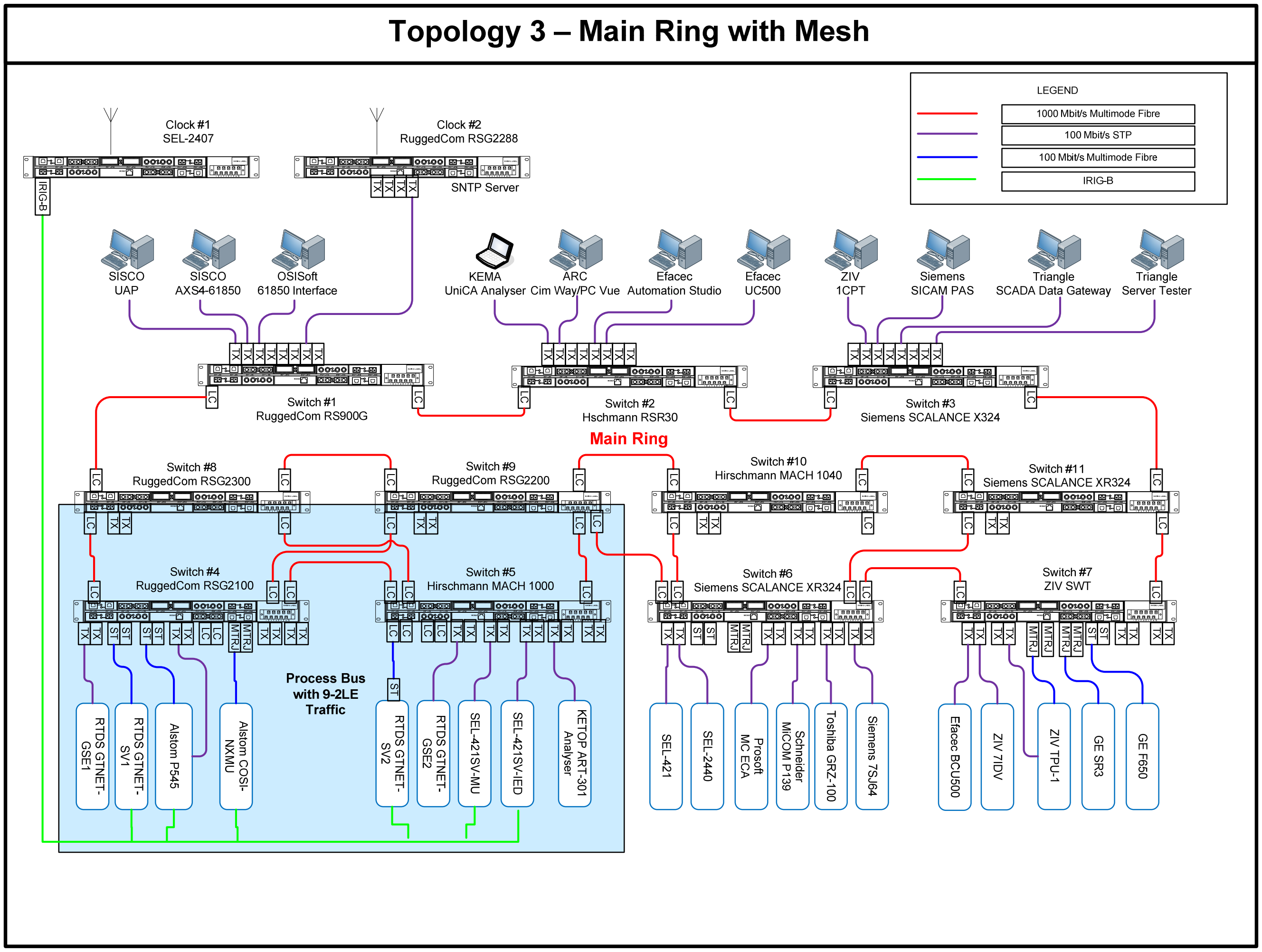


Figure 7-3: Topology 3 – Main ring with Mesh

7.1.4 Ring of IEDs with integrated switch

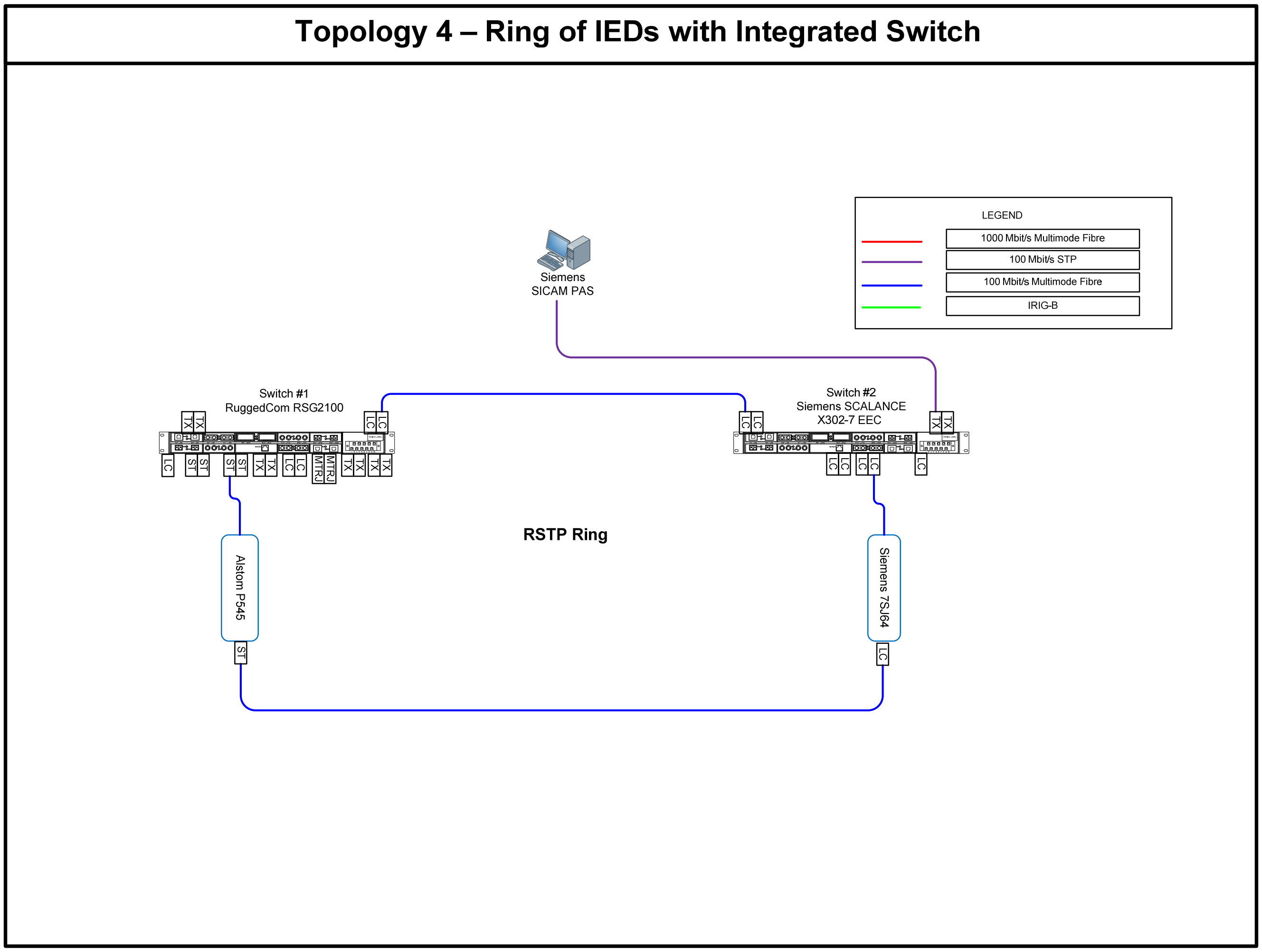


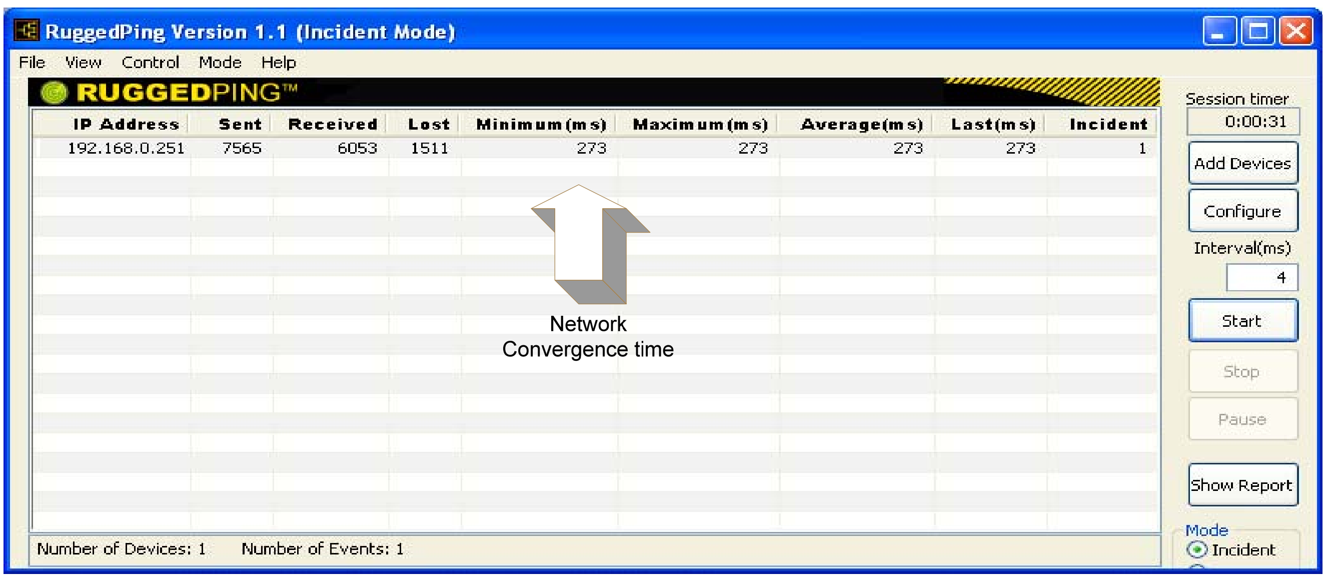
Figure 7-4: Topology 4 – Ring of IEDs

7.2 RSTP Interoperability & performance testing

All Ethernet switches are compliant to IEC 61850-3 and implements standard IEEE 802.1D-2004 RSTP protocol enabled and other proprietary or non-standard enhancements to RSTP are disabled.

The recovery time is measured by two monitoring PCs running specialized ping application:

- Consists on having two monitoring PCs, source PC and destination PC
- The source PC is running a free tool called RuggedPing.
- RuggedPing is a high accuracy graphical ping tool capable of processing incoming ping responses with a granularity of 1ms.
- The source PC is configured to Ping the destination PC with 4ms interval
- The accuracy of the RuggedPing tool is +/- 4ms
- The link failure situations are simulated by manual disconnections of gigabit fiber cables from Ethernet switches.
- The measured time values regarding Failover and Recovery times are strongly depending on, how fast the disconnection at the switch ports can be done manually (how fast the LC plug of the optical fibre ring can be removed at the switch port in order to simulate disconnection failures).
- Significant deviations in failover times are observed due to manual disconnections of fiber links
- More accurate testing would require other method than manual link disconnections



Screenshot of RuggedPing testing tool

7.3 RSTP Testing in Single Ring Topology

7.3.1 RSTP Convergence Time upon Link Failure

Purpose of the test:

- Test the network reconfiguration behaviour in case of single link failure
- Test the network reconfiguration behaviour in case of link reconnection

Test actions:

- Disconnect link between the root bridge and the neighboring bridge on the right
- Disconnect link between the root bridge and the neighboring bridge on the left
- Repeat the each test three times to see variations
- Then change the position of the root bridge to test all switches in the topology configured as root bridge

Note: Failure of links directly connected to the root bridge are expected to result in the worst network recovery time.

7.3.1.1 Root bridge at Switch#1 – RuggedCom RS900G

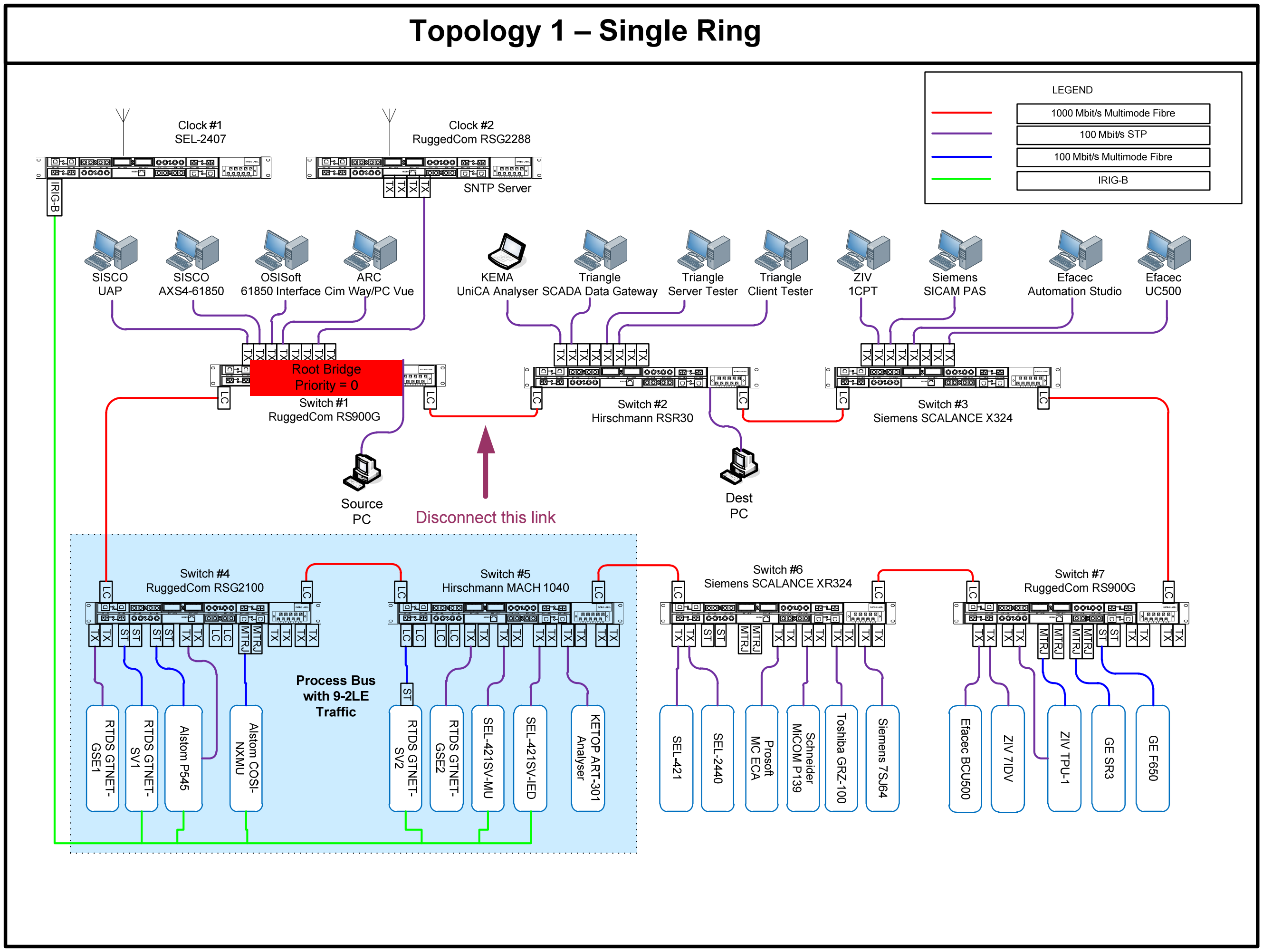


Figure 7-5: RSTP Convergence Testing procedure

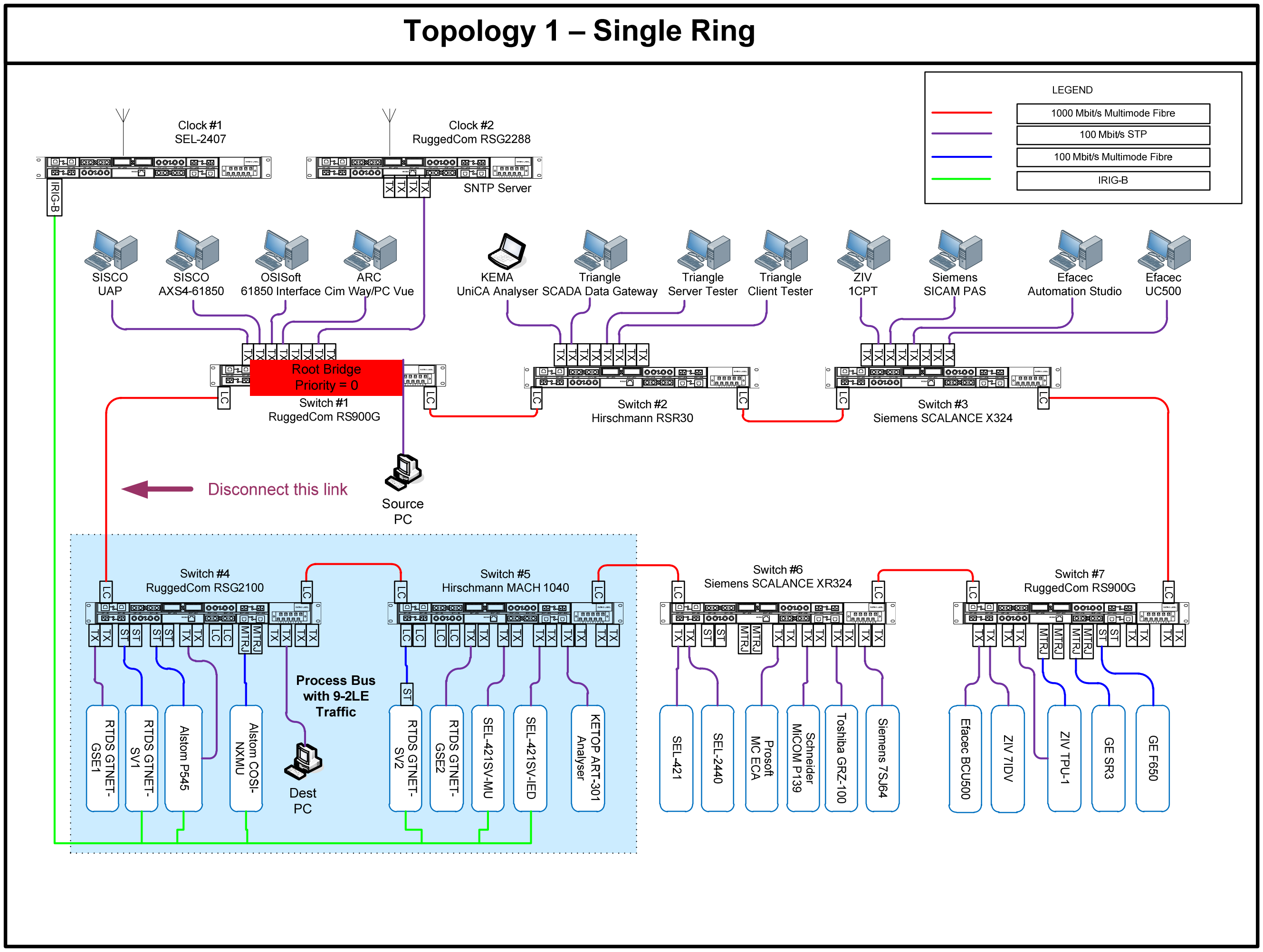


Figure 7-6: RSTP Convergence Single Ring

7.3.1.2 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	Root	0	Source PC	
SW2	-	32768	Dest PC	
SW3	-	32768		
SW4	-	32768	Dest PC	
SW5	-	32768		
SW6	-	32768		
SW7	-	32768		

7.3.1.3 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW1 and SW2	36ms 10pkt lost	40ms 11pkt lost	36 ms 10pkt lost	Background Process bus traffic - Alstom and Schweitzer
2	Reconnect link between SW1 and SW2	4ms 2pkt lost	4ms 2pkt lost	4 ms 2pkt lost	
3	Disconnect link between SW1 and SW2	37ms			Background GOOSE traffic added, SISCO simulator connected to SW1 (root bridge). 4 different GOOSE messages, all of them triggering events every 1ms. 14000 packets per second determined via Wireshark; 12 Mb/s generation by process bus 3xMUs
4	Reconnect link between SW1 and SW2	5ms			
5	Disconnect link between SW1 and SW2	40ms	36ms	36ms	No GOOSE, no SV traffic. As expected RSTP performance is the same as in the situation with high GOOSE and SV background traffic. One of the fundamental RSTP design requirements is prioritization of RSTP BPDU messages over regular user traffic. It means that even high rate application traffic like GOOSE or Sampled Values do not affect RSTP protocol.
6	Reconnect link between SW1 and SW2	4ms	8ms	4ms	
7	Change Dest PC to SW4 Disconnect link between SW1 and SW4	27ms 8pkt lost	33ms 9pkt lost	36ms 10pkt lost	
8	Reconnect link between SW1 and SW4	9 ms 3pkt lost	12ms 4pkt lost	12ms 4pkt lost	

Witnesses: Bruce Muschlitz (Enernex), Thierry Coste (EDF), Aurélie DEHOUCK-NEVEU (EDF)

7.3.1.4 Root bridge at Switch#2 – Hirschmann RSR30

7.3.1.4.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW2	Root	0	Source PC	
SW3	-	32768	Dest PC	
SW4	-	32768		
SW5	-	32768		
SW6	-	32768		
SW7	-	32768		
SW1	-	32768	Dest PC	

7.3.1.4.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW2 and SW3	32ms 9pkt lost	33ms 9pkt lost	28ms 8pkt lost	
2	Reconnect link between SW2 and SW3	12ms 4pkt lost	12ms 4pkt lost	12ms 4pkt lost	
3	Change Dest PC to SW1. Disconnect link between SW2 and SW1	33ms 9pkt lost	32ms 9pkt lost	31ms 9pkt lost	
4	Reconnect link between SW2 and SW1	4ms 2pkt lost	4ms 2pkt lost	4ms 2pkt lost	
5	Change Dest PC to SW7 Disconnect link between SW3 and SW7	64ms 17pkt lost	52ms 14pkt lost	56ms 15pkt lost	
6	Reconnect link between SW3 and SW7	8ms 3pkt lost	8ms 3pkt lost	8ms 3pkt lost	

7.3.1.5 Root bridge at Switch#3 – Siemens SCALANCE XR324

7.3.1.5.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW3	Root	0	Source PC	
SW4	-	32768		
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Dest PC	
SW1	-	32768		
SW2	-	32768	Dest PC	

7.3.1.5.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW3 and SW7	89ms 23pkt lost	65ms 17pkt lost	100ms 26pkt lost	The fiber link failure detection time is the cause of the longer failover time in this case. It depends on how the link was disconnected.
2	Reconnect link between SW3 and SW7	8ms 3pkt lost	8ms 3pkt lost	8ms 3pkt lost	
3	Change Dest PC to SW2. Disconnect link between SW3 and SW2	104ms 27pkt lost	48ms 13pkt lost	52ms 14pkt lost	
4	Reconnect link between SW3 and SW2	8ms 3pkt lost	4ms 2pkt lost	4ms 2pkt lost	

7.3.1.6 Root bridge at Switch#4 – RuggedCom RSG2100

7.3.1.6.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW4	Root	0	Source PC	
SW5	-	32768	Dest PC	
SW6	-	32768		
SW7	-	32768		
SW1	-	32768	Dest PC	
SW2	-	32768		
SW3	-	32768		

7.3.1.6.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW4 and SW5	56ms 15pkt lost	69ms 18pkt lost	61ms 16pkt lost	
2	Reconnect link between SW4 and SW5	9ms 3pkt lost	8ms 3pkt lost	16ms 5pkt lost	
3	Disconnect link between SW4 and SW5	120ms 31pkt lost	104ms 27pkt lost	76ms 20pkt lost	Disconnecting only 1 fiber. Auto negotiation is set to ON on all links. Disconnection of just 1 link at TX port of the root (at SW#4).
4	Reconnect link between SW4 and SW5	9ms 3pkt lost	8ms 3pkt lost	4ms 2pkt lost	
5	Disconnect link between SW4 and SW5	21ms 6pkt lost	28ms 8pkt lost	28ms 8pkt lost	Disconnecting only 1 fiber. Auto negotiation is set to ON on all links. Disconnection of just 1 link at RX port of the root (at SW#4). Explanation: failure of just a single link is faster than failure of both links at the same time (compare results with test 3) because it may happen that the partner switch may detect link failure faster and initiate the link down of the other partner.
6	Reconnect link between SW4 and SW5	4ms 2pkt lost	13ms 4pkt lost	6ms 3pkt lost	

		Failover/Recovery Time [ms] and Ping packets lost			Comments
7	Disconnect link between SW4 and SW5	100ms 26pkt lost	116ms 30pkt lost	76ms 20pkt lost	Disconnecting only 1 fiber. Auto negotiation is set to OFF on link between SW#4 and SW#5. The purpose is to measure the effect of auto negotiation OFF on the failover time. Disconnection of just 1 link at TX port of the root (at SW#4).
8	Reconnect link between SW4 and SW5	12ms 4pkt lost	9ms 3pkt lost	13ms 4pkt lost	
9	Disconnect link between SW4 and SW5	5313ms 1329pkt lost	5508ms 3304pkt lost	5580ms 1396pkt lost	Disconnecting only 1 fiber. Auto negotiation is set to OFF on link between SW#4 and SW#5. The purpose is to measure the effect of auto negotiation OFF on the failover time. Disconnection of just 1 link at RX port of the root (at SW#4). Expected very long recovery time because at SW#5 the link is still up, so SW#5 thinks he still sees the root, it is the root itself that is not receiving RSTP Hello messages from SW#5 and it initiates the topology change (hello timer is 3 missed RSTP Hello messages, Hello timer is 2 seconds in this test).
10	Reconnect link between SW4 and SW5	8ms 3pkt lost	5ms 2pkt lost	4ms 2pkt lost	
11	Change Dest PC to SW1. Disconnect link between SW4 and SW1	24ms 7pkt lost	24ms 7pkt lost	25ms 7pkt lost	
12	Reconnect link between SW4 and SW1	9ms 3pkt lost	12ms 4pkt lost	16ms 5pkt lost	

7.3.1.7 Root bridge at Switch#5 – Hirschmann MACH 1000

7.3.1.7.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW5	Root	0	Source PC	
SW6	-	32768	Dest PC	
SW7	-	32768		
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768	Dest PC	

7.3.1.7.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW5 and SW6	44ms 12pkt lost	36ms 10pkt lost	36ms 10pkt lost	
2	Reconnect link between SW5 and SW6	13ms 4pkt lost	13ms 4pkt lost	13ms 4pkt lost	
3	Change Dest PC to SW4. Disconnect link between SW5 and SW4	84ms 22pkt lost	84ms 22pkt lost	84ms 22pkt lost	
4	Reconnect link between SW5 and SW4	8ms 3pkt lost	13ms 4pkt lost	8ms 3pkt lost	

7.3.1.8 Root bridge at Switch#6 – Siemens SCALANCE XR324

7.3.1.8.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW6	Root	0	Source PC	
SW7	-	32768	Dest PC	
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768		
SW5	-	32768	Dest PC	

7.3.1.8.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Change Dest PC to SW7. Disconnect link between SW6 and SW7	24ms 7pkt lost	24ms 7pkt lost	24ms 7pkt lost	
2	Reconnect link between SW6 and SW7	8ms 3pkt lost	8ms 3pkt lost	8ms 3pkt lost	
3	Change Dest PC to SW5. Disconnect link between SW6 and SW5	36ms 10pkt lost	40ms 11pkt lost	48ms 13pkt lost	
4	Reconnect link between SW6 and SW5	8ms 3pkt lost	12ms 4pkt lost	8ms 3pkt lost	

7.3.1.9 Root bridge at Switch#7 – RuggedCom RS900G

7.3.1.9.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW7	Root	0	Source PC	
SW1	-	32768	Dest PC	
SW2	-	32768		
SW3	-	32768		
SW4	-	32768		
SW5	-	32768		
SW6	-	32768	Dest PC	

7.3.1.9.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW7 and SW3	40ms 11pkt lost	36ms 10pkt lost	40ms 11pkt lost	
2	Reconnect link between SW7 and SW3	20ms 6pkt lost	21ms 6pkt lost	20ms 6pkt lost	
3	Change Dest PC to SW6. Disconnect link between SW7 and SW6	44ms 12pkt lost	48ms 17pkt lost	65ms 4pkt lost	
4	Reconnect link between SW7 and SW6	23ms 7pkt lost	28ms 8pkt lost	28ms 8pkt lost	

7.3.1.10 Summary of test results

- Initially four switch vendors were going to participate in this test: Hirschmann, Siemens, RuggedCom, ZIV
- All four vendors have demonstrated RSTP interoperability according to IEEE 802.1D-2004 standard
- It has been detected that ZIV switch does not support auto-negotiation feature on fiber Gigabit links
- For this reason ZIV switch did not participate in RSTP performance testing and was replaced by a RuggedCom switch
- The following measured times were observed in all cases for Root Bridge configured at Hirschmann, Siemens, RuggedCom switches:
- Failover time: between 30ms and 104ms
- Recovery time: between 4ms and 16ms
- The deviations in measurements were caused by the fact the link failures were simulated by manual disconnection of fiber links which introduces inaccuracy (depending how fast the LC connector is removed from the switch).
- One test included background traffic with GOOSE messages triggered every 1ms and additional 12Mbit/s of traffic generated by three merging units. As expected no RSTP performance degradation was observed. This is explained by one of the fundamental RSTP design requirements of prioritizing RSTP BPDU messages over regular user traffic. It means that even high rate application traffic like GOOSE or Sampled Values do not affect RSTP performance.

- One test (Root Bridge at switch #4) included additional test cases with auto-negotiation feature disabled.
- It has been observed that disabled auto-negotiation dramatically increases the failover time.
- Failover times of up to 6 seconds were observed upon link failure with auto-negotiation disabled.
- The worst case is when only one of the two fibers fails (RX or TX). When only one fiber of the Ethernet port fails, the link is still up on the switch directly connected to the root. Then in case the disconnected path is the RX on the root, the neighbouring switch thinks it still sees the root. The root should realize its RX port has failed and should stop sending BPDUs immediately out of this port. When the root stops sending BPDUs then the neighbouring switch stops receiving them and it initiates the topology change after three missed "RSTP Hello" messages. In this test "RSTP Hello timer" was set to 2 seconds, which explains the failover time of 6 seconds. Nevertheless the result could be even worse because the RSTP standard does not explicitly require the root bridge to stop sending BPDUs after link failure detection. In fact if only one of the two fibers of a connection fails, then depending on the priority settings this may lead to an "oscillating behaviour" and RSTP protocol may not be able to establish a stable connection, this behaviour is conformant with RSTP standard
- Recommendation is that auto negotiation shall always be enabled on Gigabit fiber links.

7.3.2 RSTP Convergence Time upon Root Bridge Failure

Purpose of the test:

- Test the network reconfiguration behaviour in case of root bridge failure
- Test the network reconfiguration behaviour when root bridge recovers and reconnects to the topology

Test actions:

- Power off the root bridge and measure the failover time
- Power on the root bridge and measure the recovery time
- Repeat the test three times to see variations

Note: The measuring PCs are located at switches that are neighbours of the root bridge, this represents the worst case scenario**.**

Procedure:

- Configure Switch#2 as the Root Bridge in the network by setting the Bridge Priority = 0, and Switch#1 to be the Backup Root Bridge with Bridge Priority = 4096

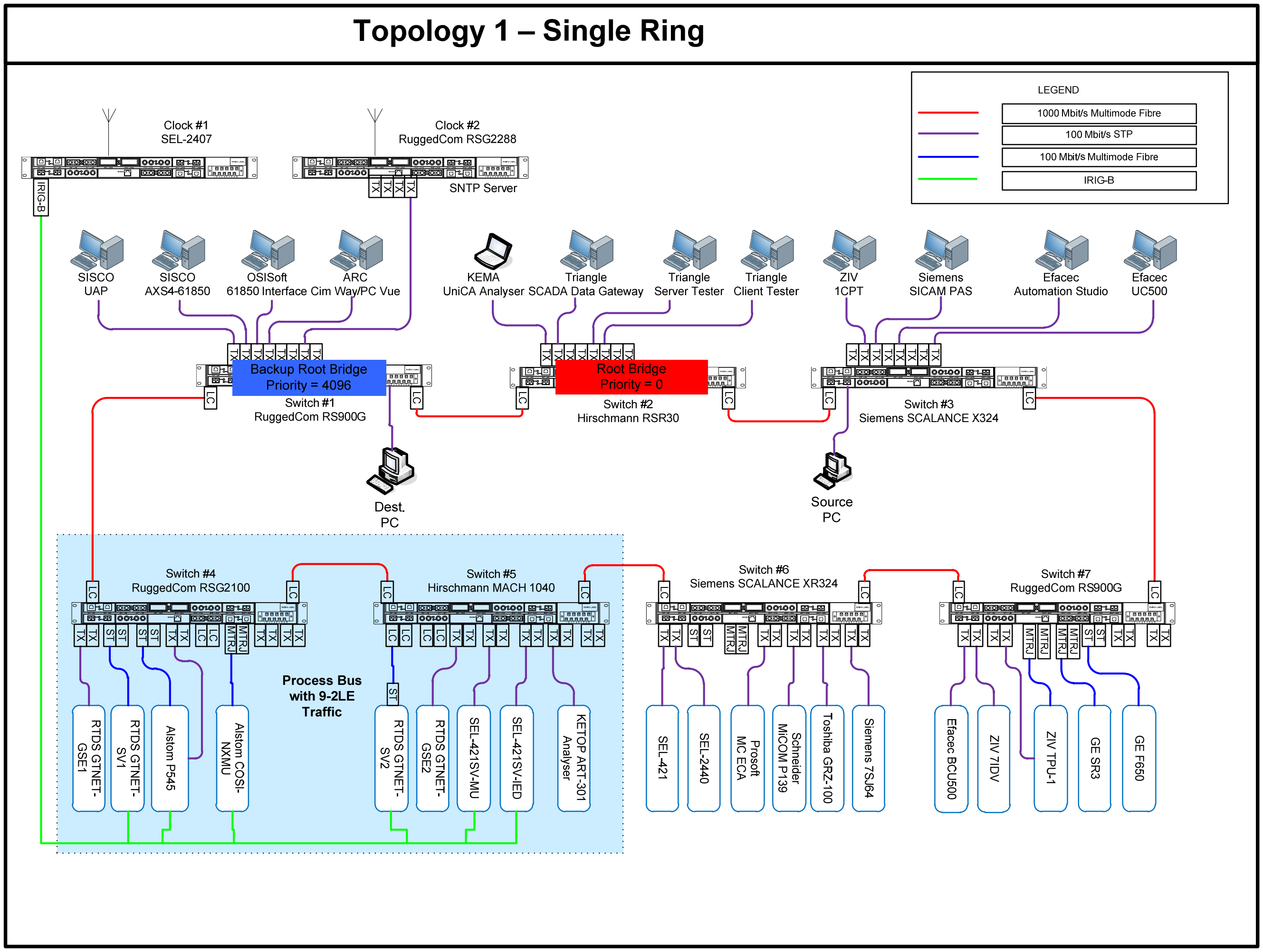


Figure 7-7: RSTP Convergence Single Ring with Root Bridge Failure

- Start communication between IEDs
- Connect one PC to Switch#3 and another PC to Switch#1 in the network
- Change the priority of the Root Bridge (Switch#5) to 32768
- Use RuggedPing to Ping the Destination PC connected to Switch#1 with 4 ms interval
- Power Off the Root Bridge (Switch#2) during the traffic flow and record the failover time from RuggedPing
- Verify the communication between IEDs
- Stop and Start RuggedPing and Power on the Root Bridge
- Record the network recovery time from RuggedPing
- Verify the communication between IEDs

7.3.2.1 Root bridge at Switch#2 (Hirschmann) backup root bridge at Switch#1 (RuggedCom)

7.3.2.1.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	Backup Root	4096	Dest PC	
SW2	Root	0		
SW3	-	32768	Source PC	
SW4	-	32768		
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Dest PC	

7.3.2.1.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Power off the root bridge	132ms 34pkt lost	104ms 27pkt lost	89ms 23pkt lost	Dest PC on SW1
2	Power on the root bridge	17ms 5pkt lost	12ms 4pkt lost	20ms 6pkt lost	Dest PC on SW1
3	Power off the root bridge	84ms 22pkt lost	84ms 22pkt lost	61ms 16pkt lost	Dest PC on SW7
4	Power on the root bridge	12ms 4pkt lost	17ms 5pkt lost	16ms 5pkt lost	Dest PC on SW7

Witnesses: Bruce Muschlitz (Enernex), Jaume Badia (Endesa)

7.3.2.2 Summary of test results

Switches from three vendors participated in this test: Hirschmann, Siemens, RuggedCom

The following measured times were observed:

- Failover time: between 61ms and 132ms
- Recovery time: between 12ms and 20ms

The deviations in measurements were caused by the fact the RSTP has non-deterministic behaviour upon root bridge failure situations.

The failover and recovery times are slightly longer than in case of link failure. However the difference is not significant because the tested topology was relatively small. In larger topologies Root bridge failures would experience much higher failover times.

7.4 RSTP Testing in Ring with Two Sub-rings Topology

This topology is typical in high voltage substations with the main ring connecting station level devices such as gateways, substation computers running local SCADA or IEC 61850 clients applications. The two sub-rings are divided per voltage level.

7.4.1 Topology

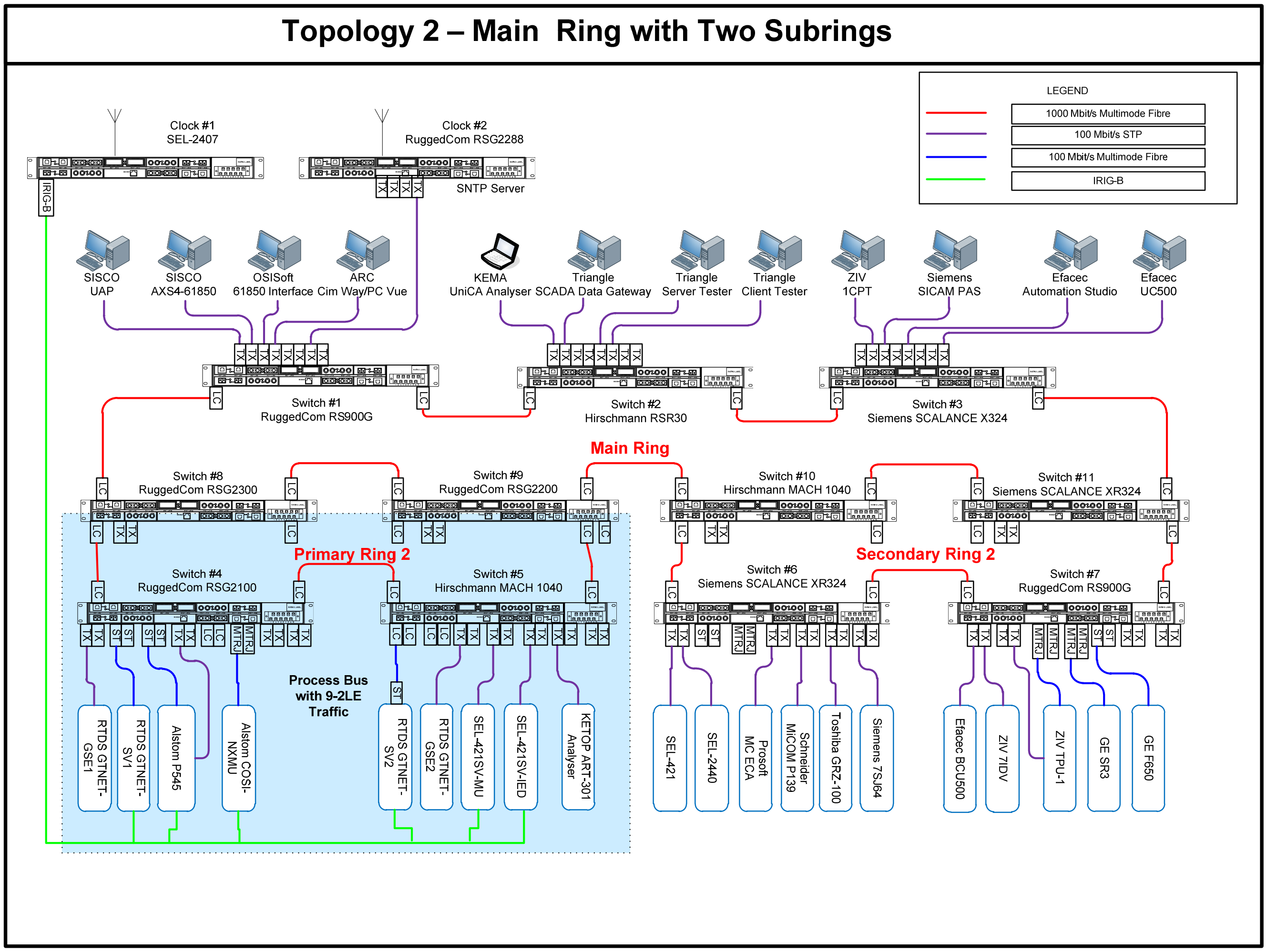


Figure 7-8: RSTP Convergence Topology 2 - Main Ring with Two Sub-rings

7.4.2 RSTP Convergence Time upon Link Failure

Purpose of the test:

- Test the network reconfiguration behaviour in case of single link failure
- Test the network reconfiguration behaviour in case of link reconnection

Test actions:

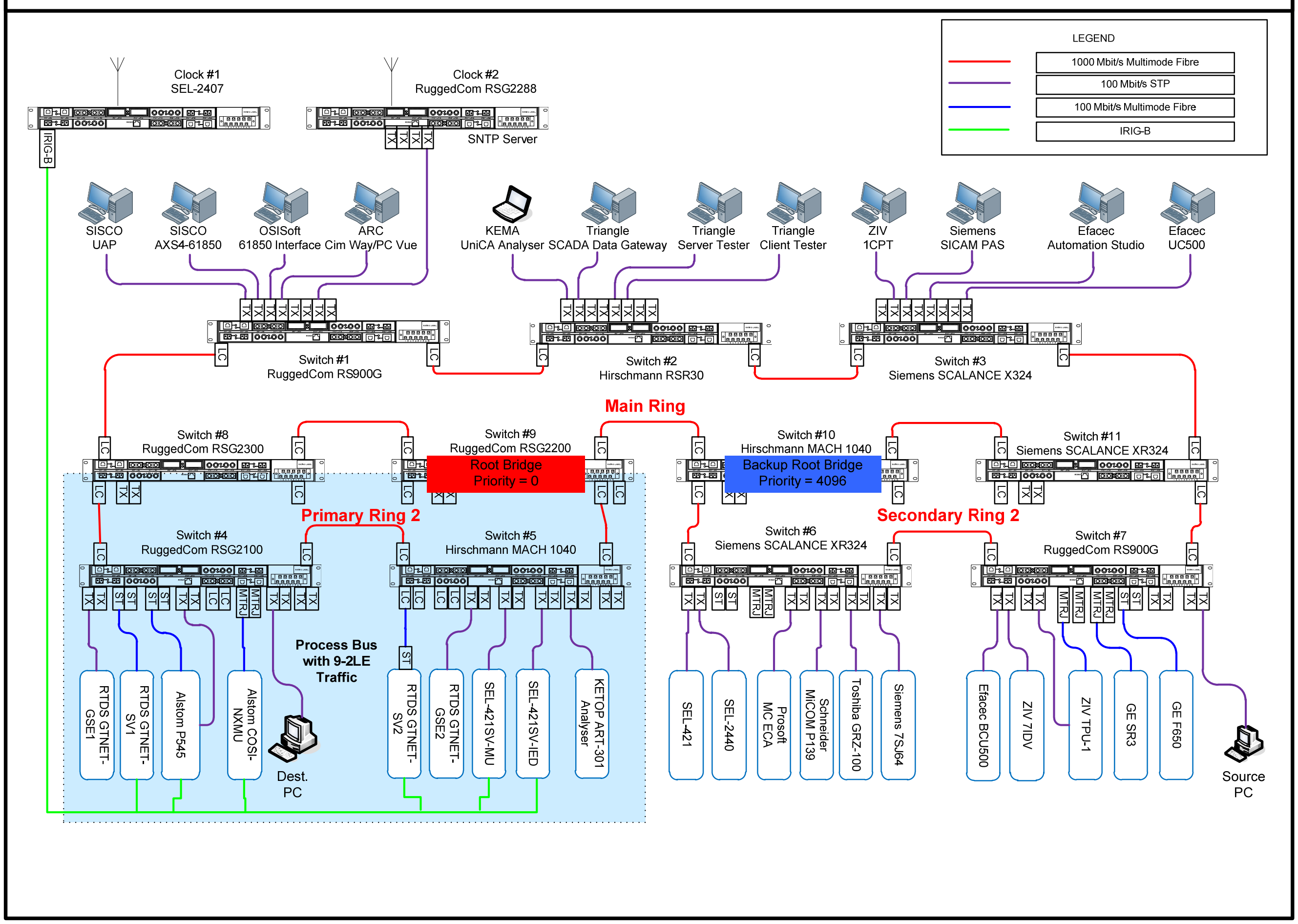
- Disconnect selected link
- Repeat the each test three times to see variations
- Then change the position of the root bridge to test different locations of the root bridge and backup root bridge

7.4.2.1 Root bridge at Switch#9 (RuggedCom) backup root bridge at Switch#10 (Hirschmann)

Procedure:

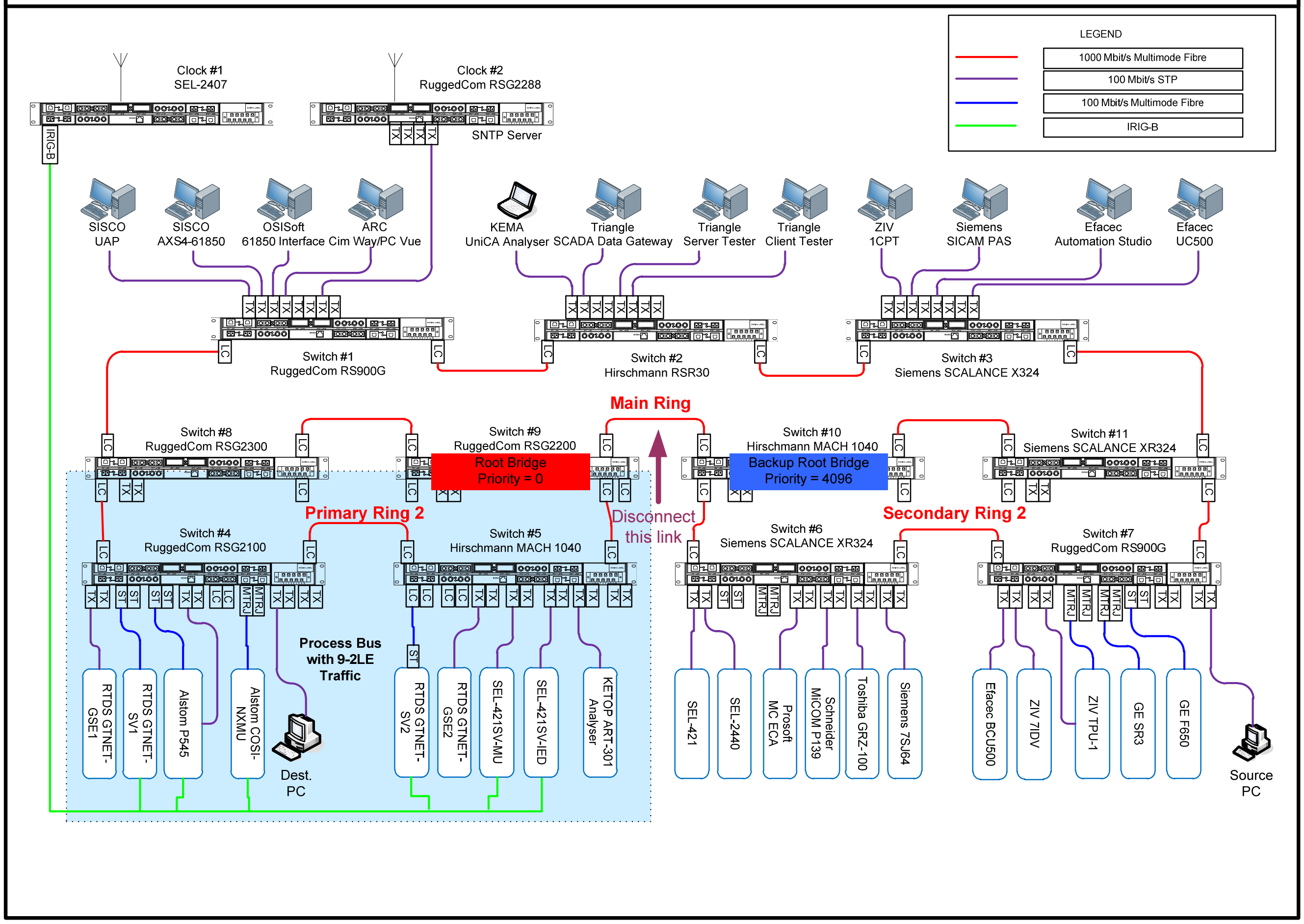
- From the previous test change the RSTP Bridge Priority of the Root Bridge and the Backup Root Bridge to be the default (Priority = 32768)
- Configure Switch#9 as the Root Bridge in the network by setting the Bridge Priority = 0 and Switch#10 as the backup Root Bridge with Priority = 4096

Topology 2 – Main Ring with Two Subrings



- Start communication between IEDs
- Connect one PC to Switch#4 and another PC to Switch#7 in the network
- Use RuggedPing in the Source PC connected to Switch#7
- Use RuggedPing to Ping the Destination PC connected to Switch#4 with 4 ms interval
- Disconnect the cable between Switch#9 and Switch#10 during the traffic flow

Topology 2 – Main Ring with Two Subrings



- Verify the communication between IEDs
- Stop RuggedPing and record the network failover time
- Restart RuggedPing and reconnect the cable between Switch#9 and Switch#10 and measure the network recovery time.
- Verify the communication between IEDs

7.4.2.1.1 Test Configuration:

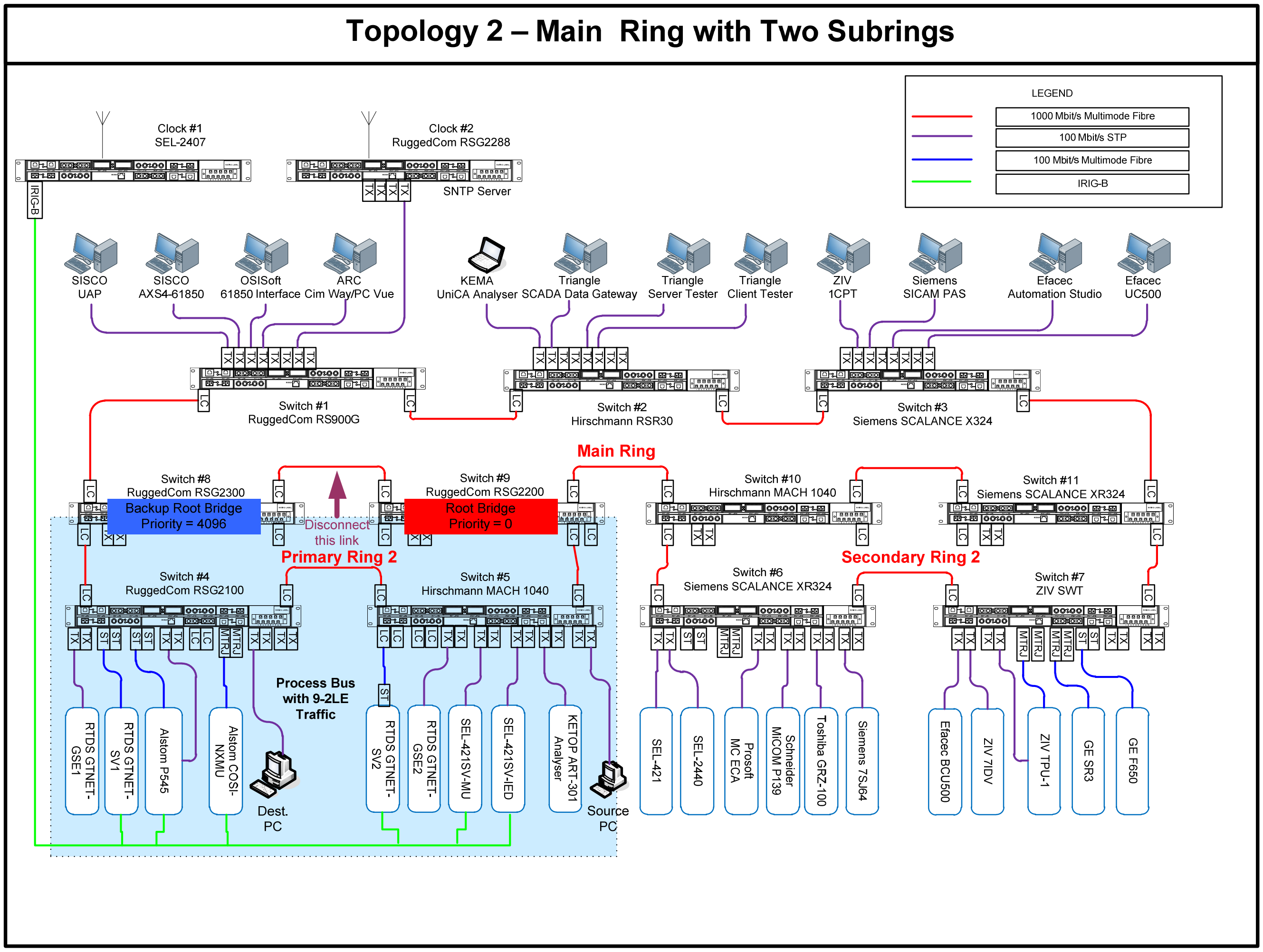
Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768	Dest PC	
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Source PC	
SW8	-	32768		
SW9	Root	0		
SW10	Backup Root	4096		
SW11	-	32768		

7.4.2.1.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW9 and SW10	56ms 15pkt lost	69ms 18pkt lost	64ms 17pkt lost	
2	Reconnect link between SW9 and SW10	12ms 4pkt lost	13ms 4pkt lost	12ms 4pkt lost	

Witness: Carlos Rodriguez (Red Eléctrica)

7.4.2.2 Root bridge at Switch#9 (RuggedCom) backup root bridge at Switch#8 (RuggedCom)



- Change the Position of the Backup Root Bridge and the Source PC as shown on the above figure
- Start communication between IEDs
- Start RuggedPing and disconnect the cable between Switch#8 and Switch#9 and measure the network failover time.
- Verify the communication between IEDs

7.4.2.2.1 Test Configuration:

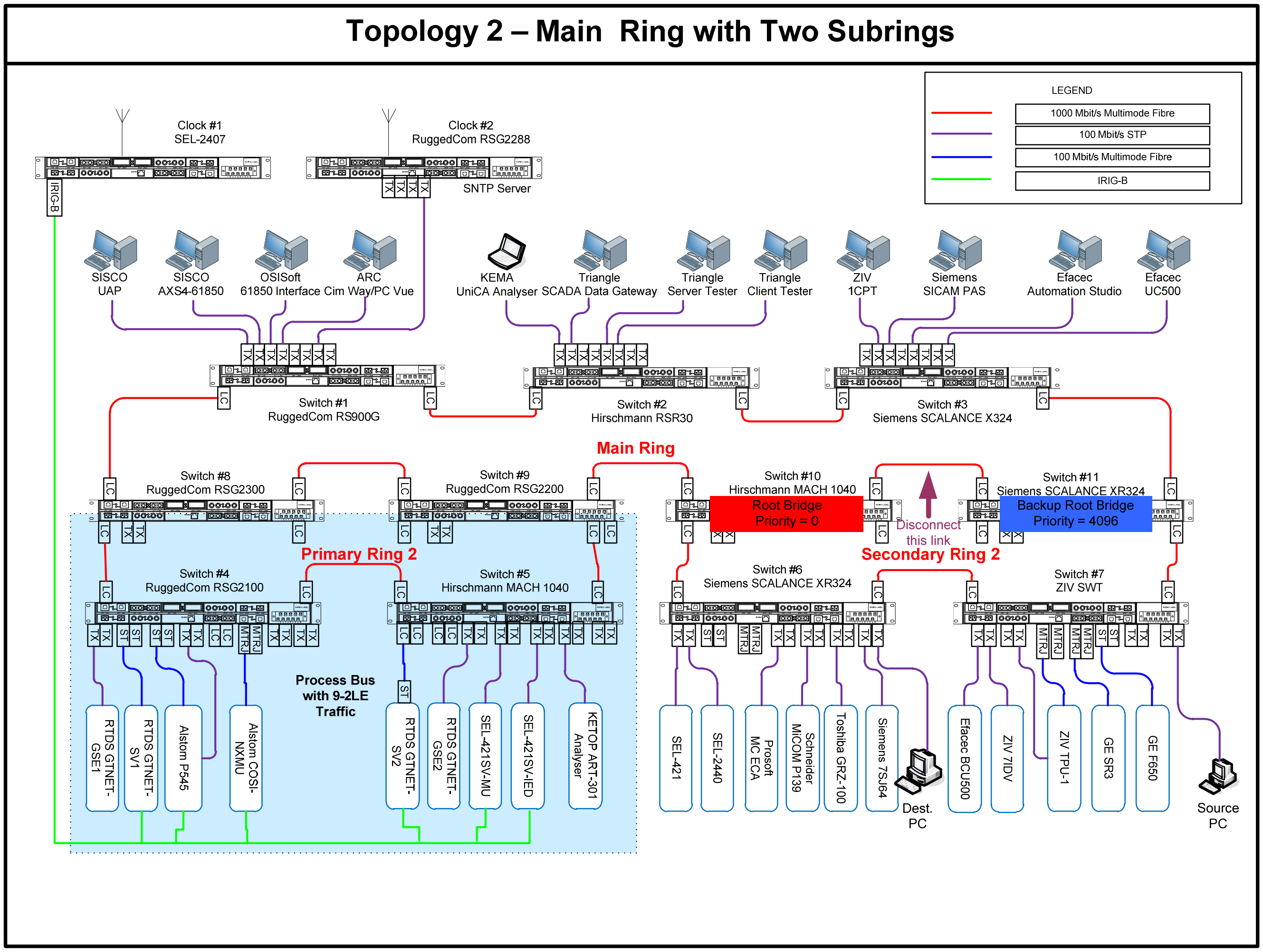
Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768	Dest PC	
SW5	-	32768	Source PC	
SW6	-	32768		
SW7	-	32768		
SW8	Backup Root	4096		
SW9	Root	0		
SW10	-	32768		
SW11	-	32768		

7.4.2.2.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW8 and SW9	49ms 13pkt lost	48ms 13pkt lost	49ms 13pkt lost	
2	Reconnect link between SW8 and SW9	33ms 9pkt lost	33ms 9pkt lost	33ms 9pkt lost	Reconnection of link between SW8 and SW9 means that the link between SW4 and SW5 will be blocked and the network has to reconfigured

Witnesses: Carlos Rodriguez (Red Eléctrica), Thierry Coste (EDF)

7.4.2.3 Root bridge at Switch#10 (Hirschmann) backup root bridge at Switch#11 (Siemens)



- Change the Position of the Backup Root Bridge and the Source PC as shown on the above figure
- Start communication between IEDs
- Start RuggedPing and disconnect the cable between Switch#10 and Switch#11 and measure the network failover time.
- Verify the communication between IEDs

7.4.2.3.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768		
SW5	-	32768		
SW6	-	32768		
SW7	-	32768		
SW8	-	32768		
SW9	-	32768		
SW10	Root	0		
SW11	Backup Root	4096		

7.4.2.3.2 Test Results:

		Failover/Recovery Time [ms] and Ping packets lost			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Disconnect link between SW10 and SW11	0ms	0ms	0ms	In this test the link between SW7 and SW11 is blocked by RSTP and the communication between source PC (SW7) and dest PC (SW6) is not going through SW10 and SW11 therefore breaking the connection between SW10 and SW11 does not cause communication failure between source PC and dest PC. Observed expected results 0 failover time. In fact there is a topology reconfiguration as the link between SW7 and SW11 has to be enabled, so RSTP packets are being exchanged between switches.
2	Reconnect link between SW10 and SW11	0ms	0ms	0ms	

Witness: Carlos Rodriguez (Red Eléctrica)

7.4.2.4 Summary of test results

Switches from three vendors participated in this test: Hirschmann, Siemens, RuggedCom

The following measured times were:

- Failover time: between 49ms and 69ms
- Recovery time: between 12ms and 33ms

7.4.3 RSTP Convergence Time upon Root Bridge Failure

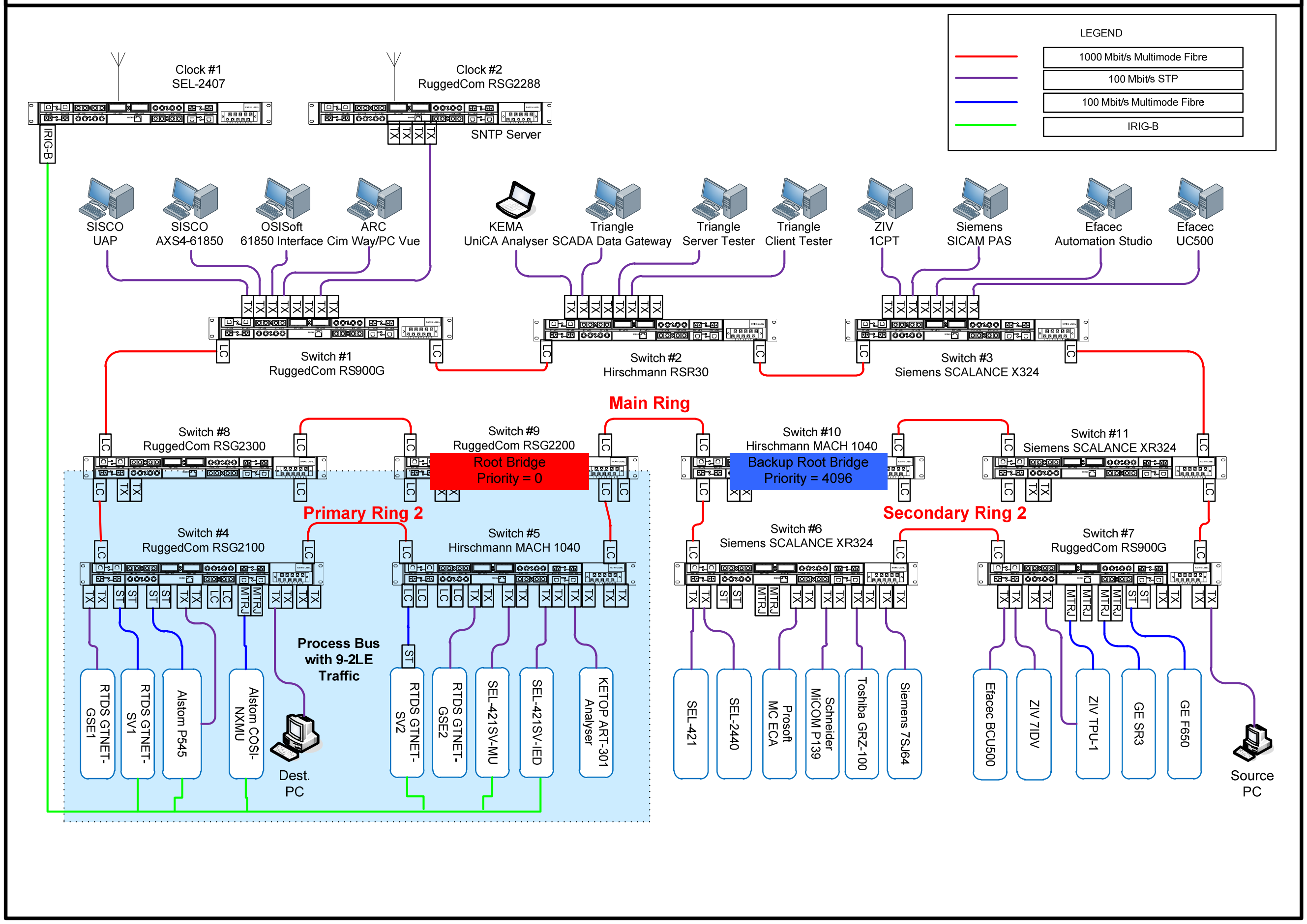
Purpose of the test:

- Test the network reconfiguration behavior in case of root bridge failure
- Test the network reconfiguration behavior when root bridge recovers and reconnects to the topology

Test actions:

- Power off the root bridge and measure the failover time
- Power on the root bridge and measure the recovery time
- Repeat the test three times to see variations

Topology 2 – Main Ring with Two Subrings



7.4.3.1 Procedure:

- Configure Root bridge as switch #9, Backup Root bridge as switch #10, Source PC at switch #7 and Destination PCs at switch #4.
- Start communication between IEDs
- Use RuggedPing to Ping the Destination PC connected to Switch#4 with 4 ms interval
- Power Off the Root Bridge (Switch#9) during the traffic flow and record the failover time from RuggedPing.
- Verify the communication between IEDs
- Stop and Start RuggedPing and Power on the Root Bridge
- Record the network recovery time from RuggedPing
- Verify the communication between IEDs

7.4.3.2 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768	Dest PC	
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Source PC	
SW8	-	32768		
SW9	Root	0		
SW10	Backup Root	4096		
SW11	-	32768		

7.4.3.3 Test Results:

		Failover/Recovery Time [ms]			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Power off the root bridge	6133ms	5605ms	5225ms	“incidents” are observed in RuggedPing tool, it means that after root bridge failure there were topology reconfigurations with several interruptions. After network reconfiguration the switches have certain time to clean the forwarding table, multiple switches declare themselves the root bridge, etc. The process to create the new topology is non-deterministic and can take significant amount of time in case of root bridge failure.
2	Power on the root bridge	52ms	48ms	48ms	Reconnection of the root bridge is much simpler situation. Once the root bridge is connected to the topology it declares itself the root, the rest of switches agree on it and the new topology is created.

Witnesses: Carlos Rodriguez (Red Eléctrica), Thierry Coste (EDF)

7.4.3.4 Summary of test results

Switches from three vendors participated in this test: Hirschmann, Siemens, RuggedCom

The following measured times were:

- Failover time: between 5225ms and 6133ms
- Recovery time: between 48ms and 52ms
- RSTP has non-deterministic behaviour in case of Root bridge failure. Very large failover times, in the range of 5-6 seconds, are observed.

7.5 RSTP Testing in Main Ring with Mesh Topology

7.5.1 Topology

Topology 2 is used as a base and additional links are added between the switches in the network as shown on figure below.

7.5.2 RSTP Convergence Time upon Root Bridge Failure

Root bridge failure in meshed topology is characterized by a non-deterministic failover and recovery time. In some situations in highly meshed networks the failover or recovery time can be in the range of several hundreds of milliseconds or even several seconds.

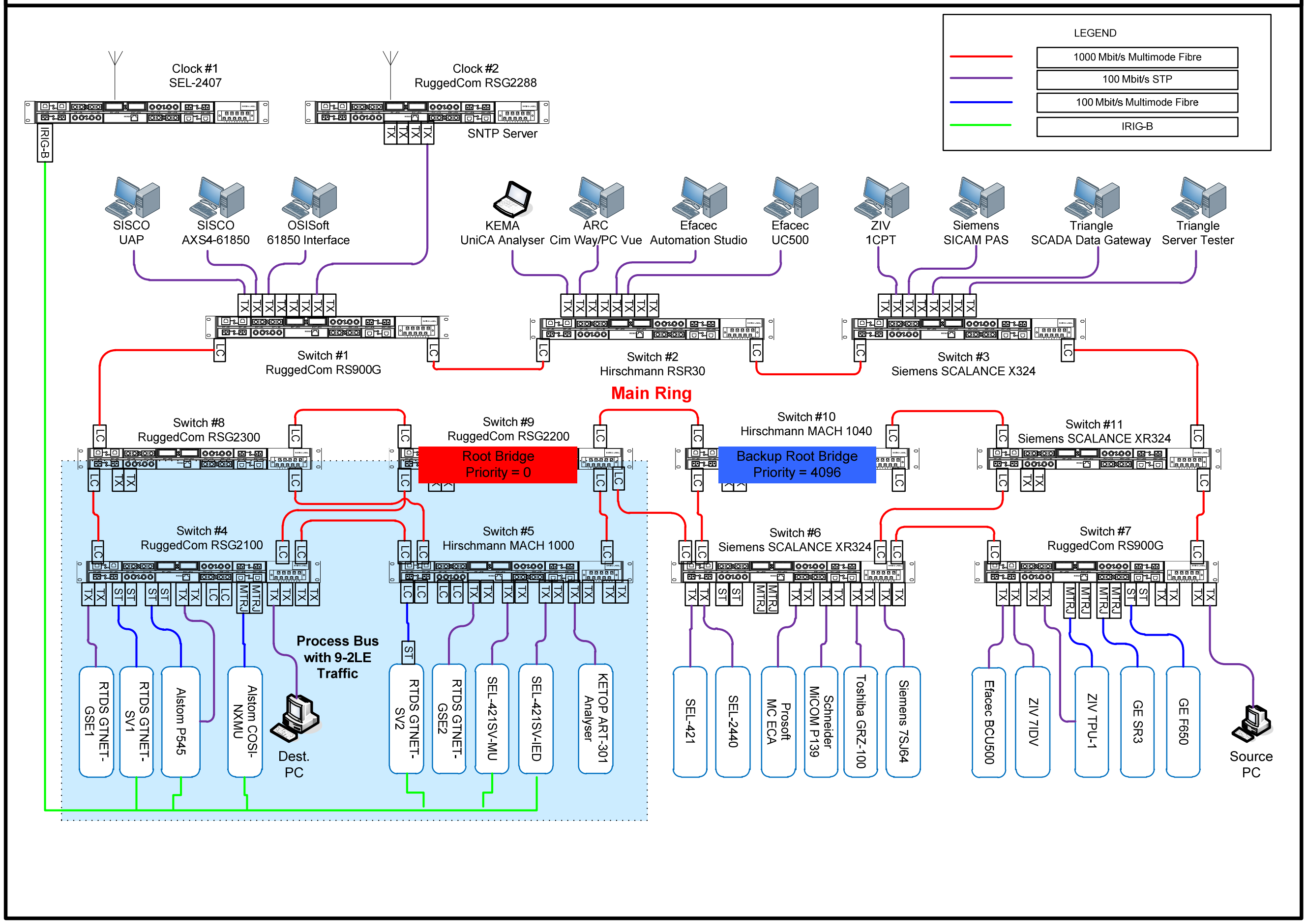
Purpose of the test:

- Test the network reconfiguration behaviour in case of root bridge failure in the meshed topology
- Test the network reconfiguration behaviour when root bridge recovers and reconnects to the topology

Test actions:

- Power off the root bridge and measure the failover time
- Power on the root bridge and measure the recovery time
- Repeat the test three times to see variations

Topology 3 – Main Ring with Mesh



7.5.2.1 Procedure:

- Configure Root bridge as switch #9, Backup Root bridge as switch #10, Source PC at switch #7 and Destination PCs at switch #4.
- Start communication between IEDs
- Use RuggedPing to Ping the Destination PC connected to Switch#4 with 4 ms interval
- Power Off the Root Bridge (Switch#9) during the traffic flow and record the failover time from RuggedPing.
- Verify the communication between IEDs
- Stop and Start RuggedPing and Power on the Root Bridge
- Record the network recovery time from RuggedPing
- Verify the communication between IEDs
- Repeat the above test several times annotating the recovery time.

7.5.2.2 Test Configuration:

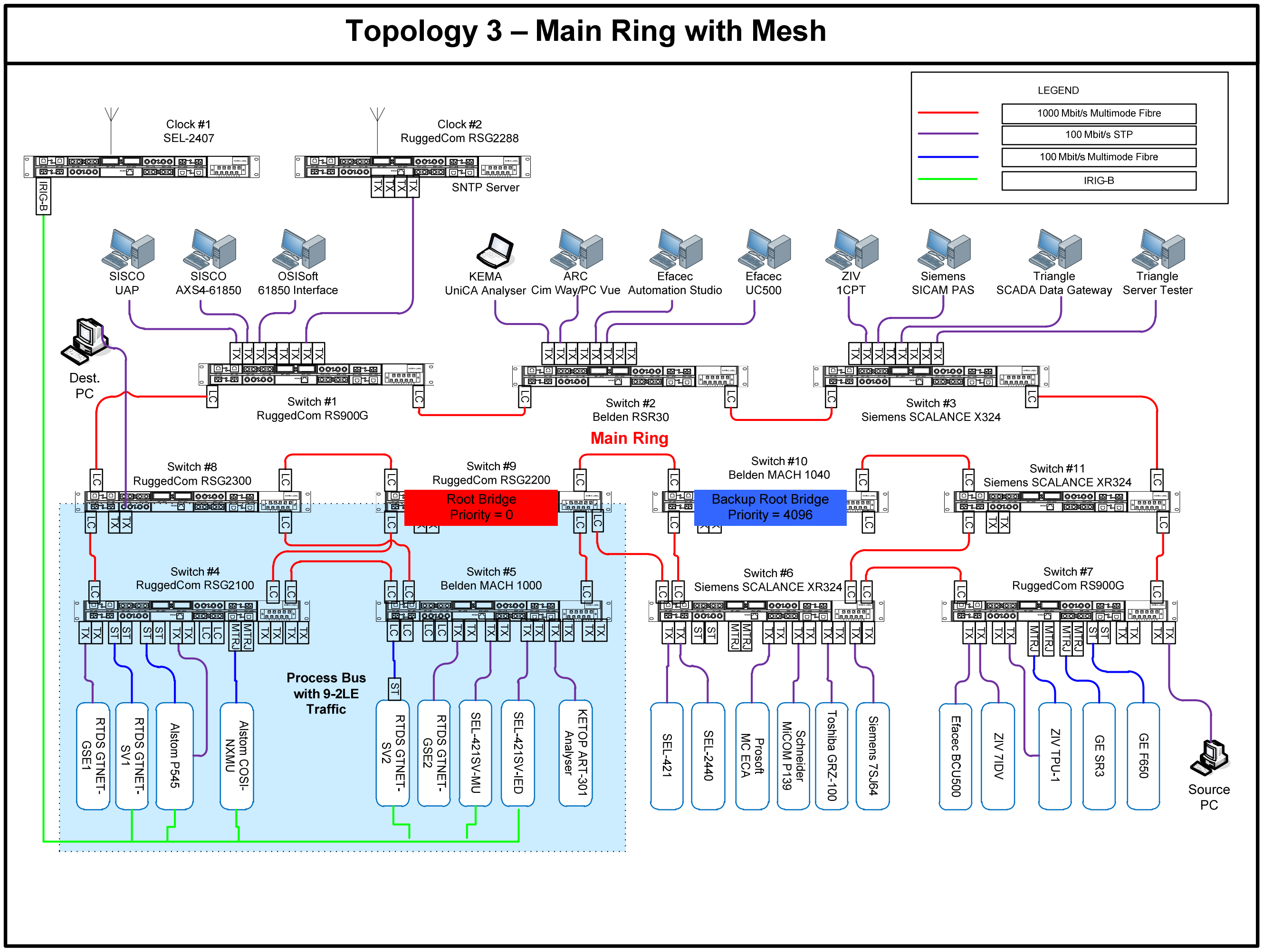
Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768	Dest PC	
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Source PC	
SW8	-	32768		
SW9	Root	0		
SW10	Backup Root	4096		
SW11	-	32768		

7.5.2.3 Test Results:

		Failover/Recovery Time [ms]			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Power off the root bridge	14585 ms	11628 ms	11136 ms	Statistics from internal log of SW1 were analyzed, it was stated that 23 topology change notifications were received by this switch before the final RSTP tree was built. Very long failover times in range of 15 seconds confirm that root bridge failure in meshed topology makes RSTP non-deterministic behaviour to recover the topology. Highly meshed topology shall be avoided in IEC 61850 systems.
2	Power on the root bridge	80ms	76ms	76ms	

Witnesses: Carlos Rodriguez (Red Eléctrica), Thierry Coste (EDF)

Changing the location of destination PC to switch #8. Repeat the above test several times annotating the recovery time.


Topology 3 – Main Ring with Mesh
LEGEND
1000 Mbit/s Multimode Fibre
100 Mbit/s STP
100 Mbit/s Multimode Fibre
IRIG-B
Clock #1
SEL-2407
Clock #2
RuggedCom RSG2288
SNTP Server
SISCO
UAP
SISCO
AXS4-61850
OSISoft
61850 Interface
KEMA
UniCA Analyser
ARC
Cim Way/PC Vue
Efacec
Automation Studio
Efacec
UC500
ZIV
1CPT
Siemens
SICAM PAS
Triangle
SCADA Data Gateway
Triangle
Server Tester
Dest.
PC
Switch #1
RuggedCom RS900G
Switch #2
Belden RSR30
Switch #3
Siemens SCALANCE X324
Main Ring
Switch #8
RuggedCom RSG2300
Switch #9
RuggedCom RSG2200
Root Bridge
Priority = 0
Switch #10
Belden MACH 1040
Backup Root Bridge
Priority = 4096
Switch #11
Siemens SCALANCE XR324
Switch #4
RuggedCom RSG2100
Switch #5
Belden MACH 1000
Switch #6
Siemens SCALANCE XR324
Switch #7
RuggedCom RS900G
Process Bus
with 9-2LE
Traffic
RTDS GTNET-GSE1
RTDS GTNET-SV1
Alstom P545
Alstom COSI-NXMU
RTDS GTNET-SV2
RTDS GTNET-GSE2
SEL-421SV-MU
SEL-421SV-IED
KETOP ART-301
Analyser
SEL-421
SEL-2440
Prosoft
MC ECA
Schneider
MICOM P139
Toshiba GRZ-100
Siemens 7SJ64
Efacec BCU500
ZIV 7IDV
ZIV TPU-1
GE SR3
GE F650
Source
PC

7.5.2.4 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	-	32768		
SW2	-	32768		
SW3	-	32768		
SW4	-	32768		
SW5	-	32768		
SW6	-	32768		
SW7	-	32768	Source PC	
SW8	-	32768	Dest PC	
SW9	Root	0		
SW10	Backup Root	4096		
SW11	-	32768		

7.5.2.5 Test Results:

		Failover/Recovery Time [ms]			Comments
Test ID	Action	Test 1	Test 2	Test 3	
1	Power off the root bridge	7280ms	10784 ms	13168 ms	
1	Power on the root bridge	112ms	104ms	904ms	

7.5.2.6 Summary of test results

Switches from three vendors participated in this test: Hirschmann, Siemens, RuggedCom

The following measured times were:

- Failover time: between 7280ms and 14585ms
- Recovery time: between 76ms and 904ms
- RSTP has non-deterministic behaviour in case of Root bridge failure, especially in highly meshed networks.
- Very long recovery times in the range of 15 seconds were observed
- Recovery times reached 900ms

Highly meshed topologies shall be avoided in IEC 61850 systems using RSTP.

7.6 RSTP Testing in Ring of IEDs Topology

7.6.1 RSTP Convergence Time upon Link Failure

Purpose of the test:

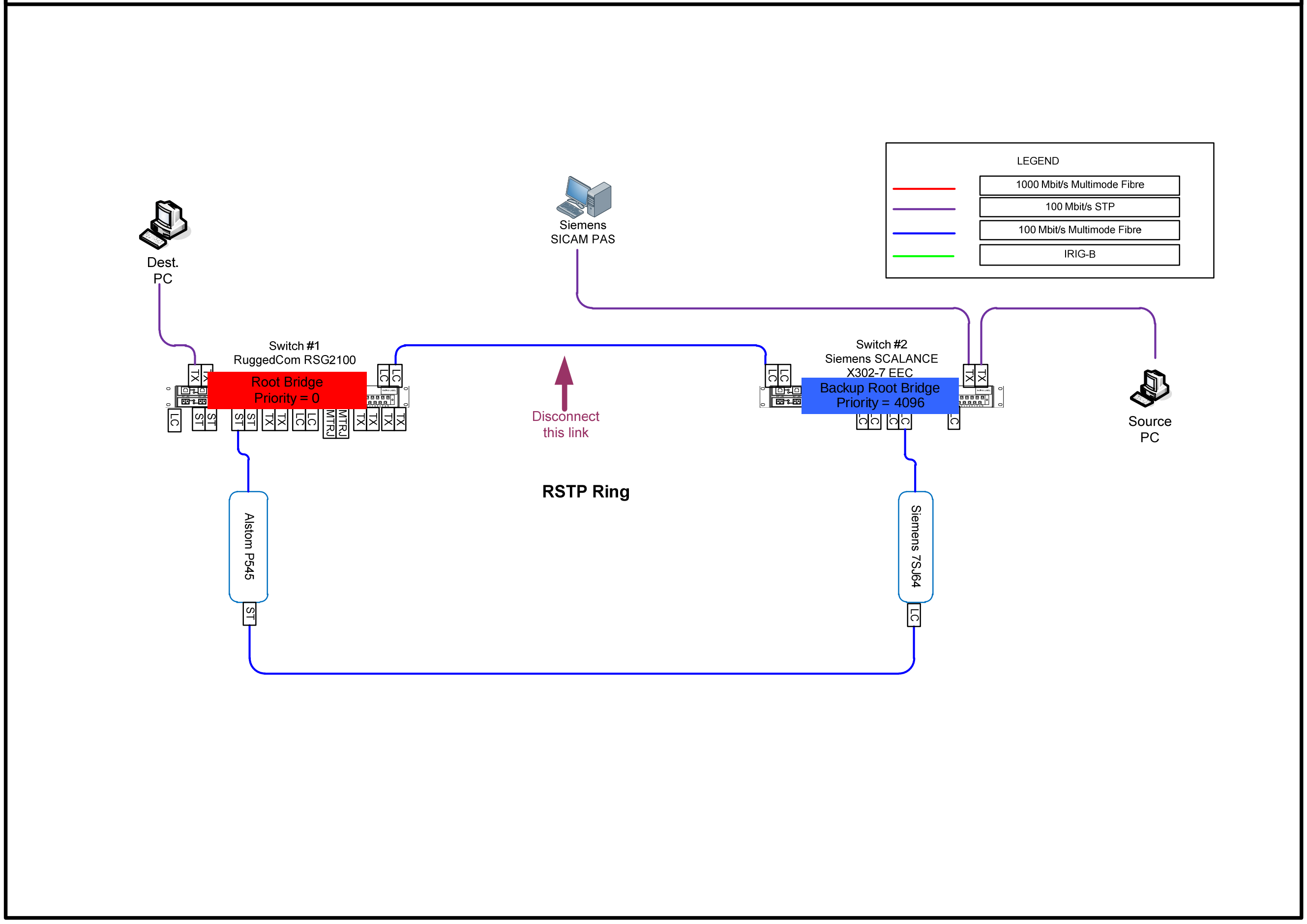
- Test the network reconfiguration behaviour in case of single link failure
- Test the network reconfiguration behaviour in case of link reconnection

Test actions:

- Disconnect selected link
- Repeat each test three times to see variations

7.6.2 Topology

Topology 4 – Ring of IEDs with Integrated Switch



7.6.2.1 Test Configuration:

Switch ID	Function	Priority	Ping	Comments
SW1	Root	0	Dest PC	
SW2	Backup Root	4096	Source PC	
SW3	-	32768		Siemens IED
SW4	-	32768		Alstom IED

7.6.2.2 Test Results:

		Failover/Recovery Time [ms]			Comments
Test ID	Action	Test 1	Test 2	Test 3	

7.6.2.3 Summary of test results

Standalone switches from two vendors participated in this test: Siemens, RuggedCom

IEDs with integrated switches participated in this test: Alstom Grid, Siemens

This test was aborted due to failure to converge in the Alstom P545. Time did not allow to determine the cause (hardware failure or implementation problem).

Alstom to investigate the cause with the IED when returned to Alstom factory.

7.7 VLAN and Multicast Filtering

The test cases described in this clause are performed using Topology 1 – Single Ring.

7.7.1 Interoperability of switches with default configuration and handling of VLAN ID=0

Purpose of the test:

- Test interoperability between switches in default configuration
- Test behavior and interoperability of switches upon frames with VLAN ID=0

7.7.1.1 Procedure:

- Connect all the switches with default configuration, only RSTP protocol shall be configured
- No VLANs are configured in the switches
- No multicast filters are configured in the switches
- For all RuggedCom switches set the “VLAN Aware = No”
- For all Hirschmann switches set “VLAN Zero Transparent Mode = disabled”
- Configure GOOSE application between two SEL IEDs with VLAN ID=0, priority=4
- Add background traffic from 4 merging units
- Start GOOSE publishing application
- Check with Wireshark in every switch in the network if all GOOSE frames are visible
- Check at the receiving SEL IED that GOOSE messages are received correctly

7.7.1.2 Summary of test results

- Switches from four vendors participated in this test: Hirschmann, Siemens, RuggedCom, ZIV
- Interoperability between all vendors has been demonstrated.
- All switches had shown to operate in accordance with IEC 61850-8-1 and IEEE 802.1Q.
- GOOSE messages with VLAN tag removed (untagged frames) have been observed in egress ports in all switches.
- GOOSE messages with VLAN tag removed (untagged frames) had been successfully received and processed at the subscribing SEL IED
- The total background traffic generated by 4 merging units had the average bandwidth of 19Mbit/s
- If traffic prioritization is going to be used then it is recommended to configure VLANs or use specialized non-standard modes such as “VLAN transparent” or “VLAN unaware”
- Behaviour of switches according to IEEE 802.1Q upon frames with VLAN ID = 0
- When VLAN ID = 0 is detected the switches are re-tagging the VLAN ID according to the PVID parameter
- In default configuration all ports are configured as untagged so even if the VLAN ID = 0 has been re-tagged to a different value, the whole VLAN tag will be removed at egress because ports are untagged
- GOOSE or SV frames are forwarded as untagged frames and are delivered to destination without the VLAN tag and without priority information
- With VLAN ID = 0 the user can make the GOOSE or SV work with minimum effort with out-of-the-box Ethernet switch configuration. This permits keeping the factory default settings of VLAN in IEDs and keeping the factory default settings of VLAN in Ethernet switches. However it will not be possible to use IEEE 802.1Q/p prioritization without specialized mechanisms such as “VLAN Transparent Mode” or “VLAN Unaware Mode” which that are out of scope of IEEE 802.1Q.

Hirschmann and RuggedCom apart from the standard IEEE 802.1Q mode additionally implement a special mode called “VLAN Transparent Mode” or “VLAN Unaware Mode” in which frames with VLAN ID=0 are forwarded with VLAN tag unchanged. In this mode compliance to IEEE 802.1Q is disabled however the switches are still compliant to IEEE 802.1D. This mode is used in customer specific environments where only priority of the VLAN tag is going to be used. When network segregation by VLAN ID is not required “VLAN transparent” or “VLAN unaware” enable the use of priorities with little configuration effort as only one setting per switch need to be set.

When GOOSE and SV application are configured with VLAN ID=0 then mixing in the same network switches that remove VLAN tag (normal IEEE 802.1Q behaviour) and switches configured to forward this tag (“VLAN Transparent” or “VLAN unaware” modes) will result in forwarding of all frames but the VLAN tag will be removed and priority information will be lost. This is still interoperable as no frames are lost, however it can lead to unexpected behaviour at the application level (priority information removed from GOOSE and SV frames).

Additional recommendation: IEDs shall permit reception of GOOSE and SV frames with and without VLAN tag as well as reception of GOOSE and SV frames with all possible VLAN ID values

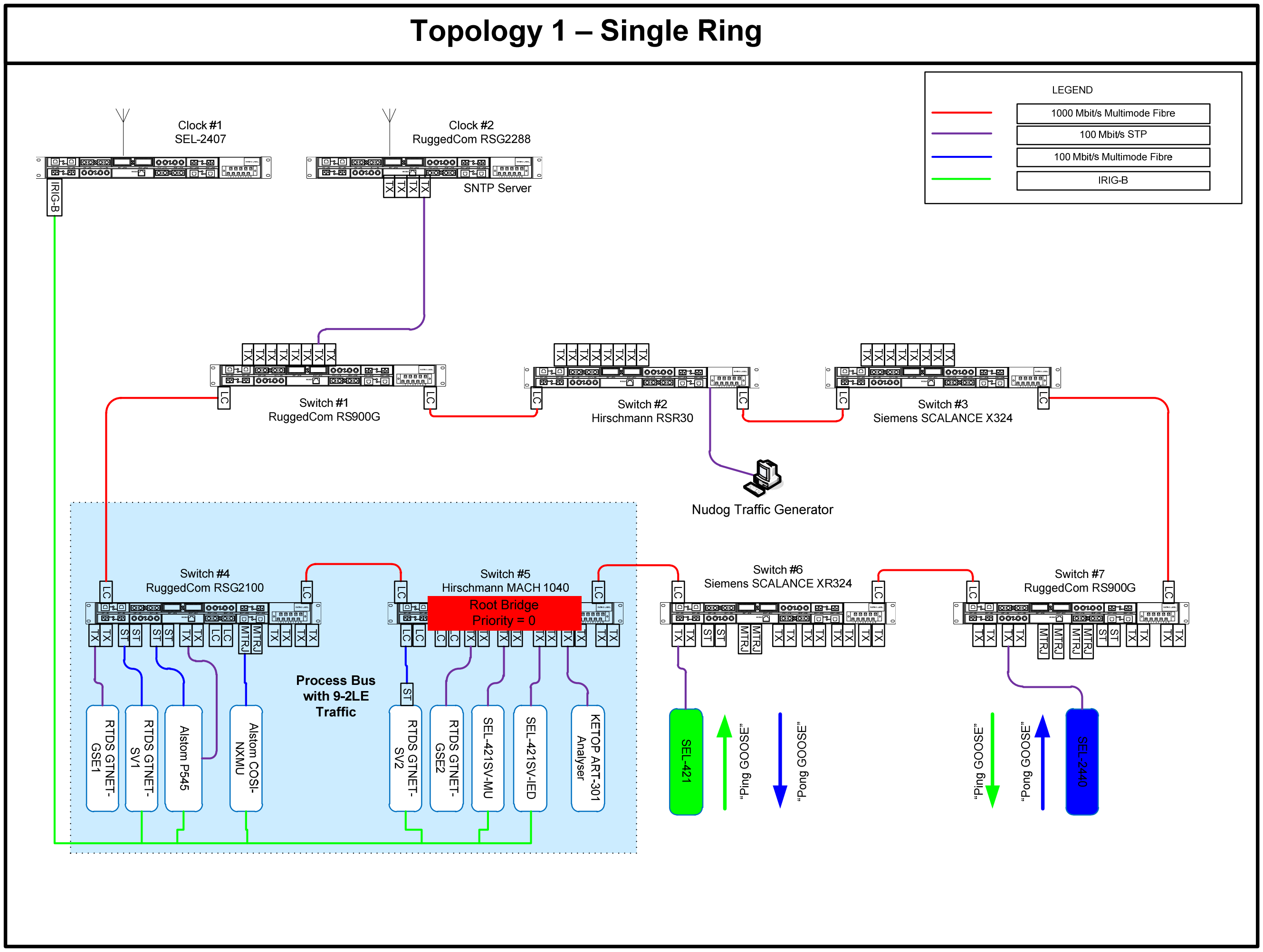
7.7.2 Performance of GOOSE with no filtering of multicast traffic

Purpose of the test:

- Show the influence of a layer 2 multicast traffic generated in the process bus on the devices in station bus.
- Performance of a GOOSE application between two IEDs in the station bus is going to be measured.

Procedure:

- Multicast layer 2 traffic generated by GOOSE and SV streams is not restricted and is propagated through the entire network.
- No VLANs are configured in the switches
- No multicast filters are configured in the switches
- The background traffic in this test case consists of:
- Four SV streams generated by merging units (at 80 samples/cycle at 60Hz)
- Six GOOSE applications sent by IEDs in the Process Bus. Devices from Alstom, RTDS and SEL
- Additional traffic only in tests 2,3,4: one very heavy GOOSE traffic (100Mbit/s) generated by a traffic injector device: Nudog Traffic Generator.
- Ping-pong GOOSE application is configured between two SEL IEDs
- SEL-421 is connected to SW#6 and SEL-2440 is connected to SW#7
- SEL-421 constantly sends “Ping GOOSE” every 4ms. Size of this GOOSE frame is 336 bytes. The content of the Data Set is the following:
- 16 x Bool
- 16 x quality
- 4 x Float
- 4 x quality
- SEL-2440 subscribes to “Ping GOOSE” from SEL-421 and uniquely responds to this GOOSE when it contains a data change. The response GOOSE is called “Pong GOOSE”.
- SEL-421 has one of the front panel pushbuttons configured to trigger a data change when pressed.
- SEL-421 subscribes to the response “Pong GOOSE” from SEL-2440 and calculates the round trip time.
- SEL-421 is configured to display the measured round-trip time on its front panel display.



Participant	Device	Destination Multicast MAC	VLAN ID	Priority	Comments
Alstom Grid	Alstom COSI-NXMU	01-0C-CD-04-00-03	0	4	
RTDS	RTDS GTNET-SV1	01-0C-CD-04-00-48	0	4	
RTDS	RTDS GTNET-SV2	01-0C-CD-04-00-49	0	4	
SEL	SEL-421SV-MU	01-0C-CD-04-00-79	0	4	

Table 1.SV traffic generated in the process bus

Participant	Device	Destination Multicast MAC	VLAN ID	Priority	Comments
Alstom Grid	MiCOM P545	01-0C-CD-01-00-01	0	4	
RTDS	RTDS GTNET-GSE1	01-0C-CD-01-00-46	0	4	
RTDS	RTDS GTNET-GSE1	01-0C-CD-01-01-46	0	4	
RTDS	RTDS GTNET-GSE2	01-0C-CD-01-00-4A	0	4	
SEL	SEL-421SV-IED	01-0C-CD-01-00-79	0	4	
SEL	SEL-421SV-IED	01-0C-CD-01-01-79	0	4	
-	Nudog Traffic Generator	01-0C-CD-04-00-99	0	4	Only in tests 2, 3 and 4. Layer 2 traffic, 100Mbit/s stream, GOOSE frames of 128 bytes size

Table 2. GOOSE traffic generated in the process bus

Test Results:

		Ping-pong GOOSE Round Trip Time [ms]			
Test ID	Action	Test 1	Test 2	Test 3	Comments
1	Trigger data change at SEL-421 measure round trip time of Ping-pong GOOSE at SEL-421	8ms	6ms	10ms	4 MUs, without additional Nudog traffic generator
2		33ms	10ms	8ms	4 MUs, with additional Nudog traffic generator streaming L2 multicast traffic at 100Mbit/s, GOOSE frames of 128 bytes size
3		27ms	20ms	18ms	
4		14ms	22ms	16ms	

7.7.2.1 Summary of test results

Switches from three vendors participated in this test: Hirschmann, Siemens, RuggedCom

It has been observed that even when four Sampled Values streams (total bandwidth of 19Mbit/s) are not filtered by Ethernet switches and propagated through the entire network the performance of GOOSE application was very good. Measured GOOSE round-trip times were in the range of 6-10ms.

The above results can be explained that SEL devices have highly optimized GOOSE implementation. It would be interesting exercise to repeat this test with IEDs from other vendors.

Deterioration of GOOSE performance was observed when additional 100Mbit/s of multicast layer 2 traffic was injected into the network from a traffic generator. Measured GOOSE round-trip times increased to 33ms.

Heavy multicast layer 2 traffic generated by GOOSE and Sampled Values applications shall be filtered in Ethernet switches in order to ensure desired performance of IED both in the process bus and in the station bus. Filtering can be done either using multicast filters in Ethernet switches or using VLANs.

7.7.3 Performance of GOOSE with filtering of multicast traffic using multicast destination MAC addresses

Purpose of the test:

- Demonstrate the improvement of network performance when heavy layer 2 multicast traffic (SV streams) is filtered.
- Test Results: The test has not been performed due to lack of time.

7.7.4 Performance of GOOSE with filtering of multicast traffic using VLANs

Purpose of the test:

- Demonstrate the use of VLANs as an alternative method to multicast MAC address filtering for logical isolation of process bus and station bus networks

Test Results: The test has not been performed due to lack of time.

8 Future Interoperability Tests

It is suggested that future interoperability test concentrate on:

- For SCL:
    - Concentration on SCD/SED file exchange based upon ED.1/ED.2 of IEC 61850-6.
    - Continued testing of CID file exchange.
    - Exchange of files that contain non-standard (e.g. vendor extended) XML Namespaces.
    - Testing based upon SCL Conformance Statements (SICS) of Edition 2.

- For Client/Server:
    - Further testing of more client/server pairs. This will mean there will be a need for more observers.
- Testing of the COMTRADE/file retrieval recommendations that were made that are now part of ED.2 of IEC 61850-8-1.

- For GOOSE:
    - Continue to refine test case definitions to yield more consistent results by observers.
    - Continue to concentrate of FCD exchange.

- For Sampled Values:
    - Attempt to have wider participation by vendors.

- Time Synchronization
    - At some time, when appropriate, test IEEE C37.238.

- Network Infrastructure
    - Continue to test for switch interoperability.
    - Add Routers to the testing scenarios.
    - Complete performance testing of GOOSE filtering using VLANs and/or destination multicast filtering in switches.
    - Test HSR/PRP for Ethernet redundancy when available.

9 SCL Test Cases

9.1 SCL testing for non-SCL Editors

9.1.1 CID Export or Creation

Test: CID Export/file provided of each IEC61850 server (from IED tool, IED itself, vendor) is provided. Validate the file.

Validation: **http://scl-validator.erlm.siemens.de/validator/upload.html** should be performed by the CID vendor in advance of the test.

Expected Result: The file is a conform file including GOOSE and Reports configuration and that the CID file is provided for the IOP.

9.1.1.1 Individual CID (or SCD) Import

Use Case: Using the exchange of SCL files for the purposes of configuration.

CID Imports of individual Vendors CID files, needed for other testing, Imports should be done on a pair wise vendor/implementation perspective as part of the SV, GOOSE, or Client/Server Testing.

Test: Import the CID.

Expected result: is that the individual SCL CID imports should import into the tooling without errors or warnings.

Note: this test does not require an SCD tool, but is used as the basis of configuring GOOSE subscribers, SV Subscribers, and 61850 Clients. As such, this is a Mandatory test.

9.2 SCD Editor Testing

In order to test the SCD Editor/Tooling, the following test cases can be performed. The over-arching use case for these tests is to make use of SCL file exchange for the basis of system engineering, modification, and exchange.

9.2.1 Individual CID Import

Test: CID Imports of individual Vendors CID files, needed for other testing, Imports should be done on a pair wise vendor/implementation perspective as part of the SV, GOOSE, or Client/Server Testing. The test shall import all CID files that are needed to create an SCD representing the system of the IOP.

Expected result: is that the individual SCL CID imports should import into the tooling without errors or warnings and all information from the CID is maintained. Witnesses should perform spot checks on the information from the original CID and the results in the SCD editor tool.

Note: This should result in merged information (e.g. from previously imported CID files) being present in the SCD file.

The witnesses should check that the SCL Editor information reflects an accurate representation:

- That the GOOSE information,
- Communication information,
- Report Control Block information, and
- Information pertaining to private tags are maintained.

9.2.2 CID Update

Use Case: An update of a CID is provided that adds or modifies information.

Pre-condition: The CID file to be updated, shall be provided by the SCL Editor vendor. Declaration of the base CID file upon which the update is based shall be documented. The CID file should provide at least one change in the following areas:

- 1 signal added and one deleted
- 1 GOOSE DataSet added and one deleted

Test: Import the updated CID file.

Expected result: The changes shall appear in the SCL editor tool.

Note: The modified CID file name must be recorded and the file must be available/archived so that it could be part of the test documentation. The name of the file should be xxxx_modified_yyyy_zzzz.cid. Where xxxx is the original name and yyyy is the vendor that created the modified file. Zzzz shall be the date of the modification.

9.2.3 SCD Export

Use case: In order to facilitate tool-to-tool exchange, an export is required.

Test: Export the SCD file with vendor tool. Then validate the file with an SCL validator.

Expected result: Export is possible and file validates.

CID attributes including private tags are kept

9.2.4 SCD Import

Use case: In order to facilitate tool-to-tool exchange, an import from a another vendor's tool is required.

Test: Import another vendor's validated SCD file. Then validate the file with an SCL validator.

Expected result: Export is possible and file validates. The imported information should be the same as provided in the file, however private information is not required to be maintained.

9.2.5 SCD Update

Use case: Another SCD/SCL editor has made a system modification either through import of an additional CID or manual edit.

Test: The exporting vendor shall export a modified SCD file that has been validated. The file shall at least have one additional IED added and a previous IED removed. The importing vendor shall import the file.

Expected Results: The changes are reflected in the importing tool.

Note: The updated SCD file shall be named xxxx_update_yyyy.scd. Where xxxx is the vendor that has produced the scd file, and yyyy shall be the date of the modification.

10 Client/Server Test Cases

The Client/Server tests total twenty-seven (27) possible test cases that could be executed for each combination of IEC 61850 Clients and Servers. For each combination, there is also a Substation Configuration Language (SCL) file exchanged used for Client configuration.

Step from Test Procedure	Test Description
CS-1	*SCL Exchange*
CS-1.1	Server provides either CID or SCD file for import.
CS-1.2	Client imports provided file and uses it for configuration, including communication addressing configuration.
CS-2	*Reading of Functionally Constrained Data*
CS-2.1	Client reads LN0.Beh
CS-2.2	Client reads a FCD of FC=MX that contains an Integer value
CS-2.3	Client reads a FCD of FC=MX that contains an Floating point value
CS-2.4	Client reads a FCD of FC=ST that contains a SPS
CS-2.5	Client reads a FCD of FC=ST that contains a DPS
CS-2.6	Client reads a FCD of FC=CO
CS-2.7	Client reads a FCD of FC=CF
CS-2.8	Client reads a FCD of FC=DC
CS-3	*Reading of Functionally Constrained Data Attributes*
CS-3.1	Client reads LN0.Beh
CS-3.2	Client reads a FCD of FC=MX that contains an Integer value
CS-3.3	Client reads a FCD of FC=MX that contains an Floating point value
CS-3.4	Client reads a FCD of FC=ST that contains a SPS
CS-3.5	Client reads a FCD of FC=ST that contains a DPS
CS-3.6	Client reads a FCD of FC=CO
CS-3.7	Client reads a FCD of FC=CF
CS-3.8	Client reads a FCD of FC=DC
CS-4	*Control Tests*
CS-4.1	Direct Control
CS-4.1.1	Direct Control with Remote enabled
CS-4.1.2	Direct Control with Remote disabled
CS-4.2	Select Before Operate (SBO)Control*
CS-4.2.1	SBO with Remote enabled
CS-4.2.2	SBO with Remote disabled
CS-4.3	Select Before Operate with enhanced Control (SBOwES)
CS-4.3.1	SBOwES with Remote enabled
CS-4.3.2	SBOwES with Remote disabled
CS-4.4	*Buffered Reporting*
CS-4.4.1	Initial enabling of buffered controlled block
CS-4.4.2	Resynchronization of reporting based upon loss of communication
CS-4.4.2	Purging of buffer
CS-4.5	*UnBuffered Reporting*
CS-4.5.1	Initial enabling of buffered controlled block
CS-4.6	*COMTRADE File Transfer*
* - SBO is not normally used within the industry, instead DirectOperate or SBO with Enhanced Security would be used.	

SCL FILE EXPORT/IMPORT

10.1.1 CID Export or Creation

Test: CID Export/file provided of each IEC61850 server (from IED tool, IED itself, vendor) is provided. Validate the file.

Validation: **http://scl-validator.erlm.siemens.de/validator/upload.html** should be performed by the CID vendor in advance of the test.

Expected Result: The file is a conform file including GOOSE and Reports configuration and that the CID file is provided for the IOP.

10.1.2 Individual CID (or SCD) Import

Use Case: Using the exchange of SCL files for the purposes of configuration.

CID Imports of individual Vendors CID files, needed for other testing, Imports should be done on a pair wise vendor/implementation perspective as part of the SV, GOOSE, or Client/Server Testing.

Test: Import the CID.

Expected result: is that the individual SCL CID imports should import into the tooling without errors or warnings.

Note: this test does not require an SCD tool, but is used as the basis of configuring GOOSE subscribers, SV Subscribers, and 61850 Clients. As such, this is a Mandatory test.

10.1.3 Read of Data

UseCase: Clients must be able to obtain information (e.g data) from servers. This is considered to be one of the several GetDataxxx services specified in IEC 61850-7-2. At the most basic level, the client/server combination must be capable of exchanging FCD and FCDA information.

The following test cases shall be used to verify that the combination of client and server can fulfill the use case.

10.1.4 Reading of an FCD

Some clients may not be capable of reading a FCD (e.g. they deal only with FCDAs), however servers must support the reading of FCDs. The following test cases are valid only for clients that claim to support FCD acquisition.

10.1.4.1 LN0

Test Case: There is one FCD that every Server must support and that is the Beh attribute of LN0. The client shall issue a read for the Beh attribute of at least one LN0.

Expected Results. The client value of the server's LN0.Beh.stval (FC=ST) shall match.

10.1.5 Reading of various FCs

In order to gain further interoperability testing, there are several other FCD reads that shall be performed. These are based upon the mutual agreement of which LNs/FCD values should be read.

10.1.5.1 Read of a MX FCD

The client shall read at least one mutually agreed upon FCD of the MX FC. However, it is recommended that multiple MX FCDs are chosen in order to validate data formats of Integer and Floating point values.

10.1.5.2 Integer Value Read

Test Case: The client will issue a read for a FCD of FC=MX that contains an Integer value.

Expected Results. The client value of the server's Integer value shall match.

10.1.5.3 Float32 Value Read

Test Case: The client will issue a read for a FCD of FC=MX that contains an Float32.

Expected Results. The client value of the server's FloatingPoint value shall match within possible rounding errors.

10.1.5.4 Read of a ST FCD

The client shall read at least one mutually agreed upon FCD of the ST FC. However, it is recommended that multiple ST FCDs are chosen in order to validate data formats of SPS and DPS values. Note that INS is already tested via the LN0 test.

10.1.5.5 SPS Value Read

Test Case: The client will issue a read for a FCD of FC=ST that contains an SPS value.

Expected Results. The client value of the server's stVal value shall match.

10.1.5.6 DPS Value Read

Test Case: The client will issue a read for a FCD of FC=ST that contains an DPS value.

Expected Results. The client value of the server's stVal value shall match.

10.1.5.7 Read of a CO FCD

Will be considered as part of the Direct Operate test case.

10.1.5.8 Read of a CF FCD

Test Case: The client will issue a read for a FCD of FC=CF value.

Expected Results. The client value should be able to be shown to be the same as the server's value.

10.1.5.9 Read of a DC FCD

Test Case: The client will issue a read for a FCD of FC=DC value.

Expected Results. The client value should be able to be shown to be the same as the server's value.

10.1.5.10 Reading of an FCDA

Some clients may not be capable of reading a FCDA (e.g. they deal only with FCDs), however servers must support the reading of FCDAs. The following test cases are valid only for clients that claim to support FCDA acquisition.

10.1.5.11 LN0

Test Case: There is one FCDA that every Server must support and that is the Beh attribute of LN0. The client shall issue a read for the Beh attribute of at least one LN0.

Expected Results. The client value of the server's LN0.Beh.stval (FC=ST) shall match.

10.1.5.12 Reading of various FCs

In order to gain further interoperability testing, there are several other FCDA reads that shall be performed. These are based upon the mutual agreement of which LNs/FCDA values should be read.

10.1.5.13 Read of a MX FCDA

The client shall read at least one mutually agreed upon FCDA of the MX FC. However, it is recommended that multiple MX FCDs are chosen in order to validate data formats of Integer and Floating point values.

10.1.5.13.1 Integer Value Read

Test Case: The client will issue a read for a FCDA of FC=MX that contains an Integer value.

Expected Results. The client value of the server's Integer value shall match.

10.1.5.13.2 Float32 Value Read

Test Case: The client will issue a read for a FCDA of FC=MX that contains an Float32.

Expected Results. The client value of the server's FloatingPoint value shall match within possible rounding errors.

10.1.5.14 Read of a ST FCDA

The client shall read at least one mutually agreed upon FCD of the ST FC. However, it is recommended that multiple ST FCDs are chosen in order to validate data formats of SPS and DPS values. Note that INS is already tested via the LN0 test.

10.1.5.14.1 SPS Value Read

Test Case: The client will issue a read for a FCDA of FC=ST that contains an SPS value.

Expected Results. The client value of the server's stVal value shall match.

10.1.5.14.2 DPS Value Read

Test Case: The client will issue a read for a FCDA of FC=ST that contains an DPS value.

Expected Results. The client value of the server's stVal value shall match.

10.1.5.15 Read of a CO FCDA

Will be considered as part of the Direct Operate test case.

10.1.5.16 Read of a CF FCDA

Test Case: The client will issue a read for a FCDA of FC=CF value.

Expected Results. The client value should be able to be shown to be the same as the server's value.

10.1.5.17 Read of a DC FCD

Test Case: The client will issue a read for a FCDA of FC=DC value.

Expected Results. The client value should be able to be shown to be the same as the server's value.

10.2 Control Test Cases

10.2.1 Direct Control

There is a need to be able to perform control between certain clients and servers. Direct Control is at a FCD level.

10.2.1.1 Remote Control Enabled

Pre-condition: The server is enabled for remote control and the direct control action indication on the server is reset. The FCD configuration is for Direct Operate.

Test Case: Client issues a direct control to the server that is enabled for remote control.

Expected Results: Server will indicate that a direct control action has taken place and the client shall indicate no error.

10.2.1.2 Remote Control Disabled

Pre-condition: The server is disabled for remote control and the direct control action indication on the server is reset. The FCD configuration is for Direct Operate.

Test Case: Client issues a direct control to the server that is enabled for remote control.

Expected Results: Server will indicate that no direct control action has taken place and the client shall indicate a control error.

10.2.2 Select Before Operate

There is a need to be able to perform control between certain clients and servers. SBO Control is at a FCD level.

10.2.2.1 Remote Control Enabled

Pre-condition: The server is enabled for remote control and the control action indication on the server is reset. The FCD configuration is for SBO.

Test Case: Client issues a SBO control service procedure to the server that is enabled for remote control.

Expected Results: Server will indicate that a direct control action has taken place and the client shall indicate no error.

10.2.2.2 Remote Control Disabled

Pre-condition: The server is enabled for remote control and the control action indication on the server is reset. The FCD configuration is for SBO.

Test Case: Client issues a SBO control service to the server that is enabled for remote control.

Expected Results: Server will indicate that no control action has taken place and the client shall indicate a control error. The Select shall fail.

10.2.3 Select Before Operate with Enhanced Security

There is a need to be able to perform control between certain clients and servers. SBO with Enhanced Security Control is at a FCD level.

10.2.3.1 Remote Control Enabled

Pre-condition: The server is enabled for remote control and the control action indication on the server is reset. The FCD configuration is for SBO with Enhanced Security (SBOE).

Test Case: Client issues a SBOE control service procedure to the server that is enabled for remote control.

Expected Results: Server will indicate that a direct control action has taken place and the client shall indicate no error.

10.2.3.2 Remote Control Disabled

Pre-condition: The server is enabled for remote control and the control action indication on the server is reset. The FCD configuration is for SBOE.

Test Case: Client issues a SBOE control service to the server that is enabled for remote control.

Expected Results: Server will indicate that no control action has taken place and the client shall indicate a control error. The Select shall fail.

10.3 Reporting

The use case for reporting is to basically reduce communication bandwidth, increase speed of event detection, and to allow a larger number of servers to be supported by a client. However, SCADA will be the primary use case.

10.3.1 Buffered Reporting

Pre-conditions: Client and server must mutually agree upon the trigger options that are to be supported. At a minimum, GI, dchng, and integrity are expected to be supported by the server. The mutually agreed upon attributes of the control block shall be recorded as part of the test matrix.

10.3.1.1 Initial Enabling of Control Block

Test Case: The client will write and enable a buffered report control block.

Expected Results: The client should begin receiving reports and shall give some indication that reports are being received.

10.3.1.2 Resynchronization of Reporting

Pre-condition: The Initial Enabling test case was executed and the connection between the client and server is brought down.

Test Case: The client will write and enable a buffered report control block with a resynchronization value.

Expected Results: The client should begin receiving reports and shall give some indication that reports are being received.

10.3.1.3 Purging of the Buffer

Pre-condition: The Initial Enabling test case was executed and the connection between the client and server is brought down.

Test Case: The client will purge the buffer write and enable a buffered report control block with a resynchronization value.

Expected Results: The client should begin receiving reports and shall give some indication that reports are being received. No old values should be received.

10.3.2 Un-buffered Reporting

Pre-conditions: Client and server must mutually agree upon the trigger options that are to be supported. At a minimum, GI, dchng, and integrity are expected to be supported by the server. The mutually agreed upon attributes of the control block shall be recorded as part of the test matrix.

10.3.2.1 Initial Enabling of Control Block

Test Case: The client will write and enable a unbuffered report control block.

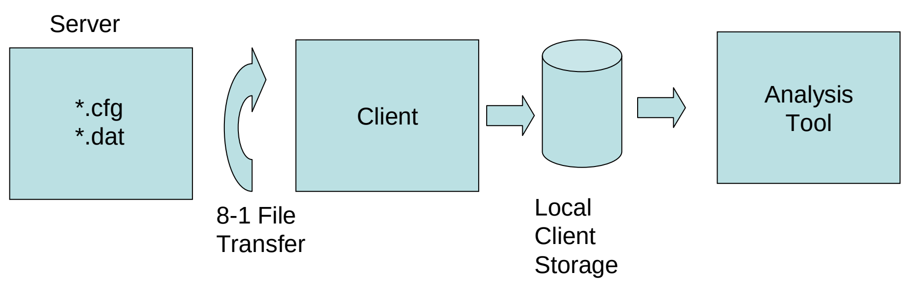
Expected Results: The client should begin receiving reports and shall give some indication that reports are being received.

10.4 File Transfer – Comtrade only

The use case for COMTRADE file transfer is that transient disturbances need to be analyzed and the transfer of COMTRADE files represents the basis for that analysis.

This means that the server needs to provide the appropriate COMTRADE files for transfer by the IEC 61850-8-1 File Transfer services.

The use case for the analysis is:



The server generates a set of COMTRADE files. The file set must include at least the COMTRADE *.cfg and *.dat files.

The Client uses 8-1 file transfer services to transfer the individual files, or a *.zip that contains all of the files, and stores the files locally.

A analysis tool is used to display the contents of the COMTRADE file set.

From IEC 61850-8-1 Edition 1:

IEEE C37.111(1999) (COMTRADE) files shall be contained within a file directory whose name is "COMTRADE". The file specifications shall be consistent with the naming conventions and suffixes specified in IEEE C37.111(1999).

The IEEE COMTRADE specification IEEE C37.111(1999) specifies the use of three different suffixes (e.g. hdr, cfg, and dat). In normal information/computational usage these suffixes may represent files other than COMTRADE.

If the directory contains a file with a suffix of "zip", that file shall convey the compressed contents of the COMTRADE hdr, cfg, and dat files of the files of the same name.

The COMTRADE directories shall be located in the appropriate directory path (e.g. within the LD directory or at the root level).

This would imply that COMTRADE files should be in an directory of the Logicial Device name and at the root level, in order to claim conformance. It is known, from past experience, that some implementations do not store the files in this location. Therefore, in order to achieve interoperability, the client must be able to be configured with the directory and file names to retrieve.

10.4.1 Transfer and comparison of COMTRADE Files

Pre-conditions: The server shall supply the directory name and file names to be transferred. Additionally, the server vendor shall provide a screen shot of one of the analog and digital channels representing the information in the COMTRADE file.

The client shall provide a COMTRADE analysis tool in which the COMTRADE information can be displayed. If the client vendor does not have such a tool, it is recommended that TOP (http://www.pqsoft.com/top/) be utilized for the purposes of comparison.

Test Case: The client will transfer the defined files and display the results in the COMTRADE analysis tool.

Expected results: The screen shots and the analysis tool results should match.

11 GOOSE Test Cases

Target: test the interoperability with correct reception and interpretation by the subscriber.

Publish test cases, with related subscriber tests when successful, will be described below for all IED combinations in Paris.

The use case is that IEDs/Applications need to be able to exchange information via GOOSE.

Precondition: Each Publishing IED shall provide a CID or SCD file that contains its configuration information. The IOP shall be considered a single system and as such the CID/SCD files shall conform to the uniqueness rules required by the 61850 suite of standards.

It is recommended that the device-name of each device be the same as IED.

- IED-Name of each Device:
  - It is recommended that the format of the IED name be:
  - Vendor + DeviceType+ IP number (e.g. 100)

It is recommended that the Ethernet GOOSE App-ID value shall be the same as last digits of MAC address

The CID configuration should provide a minimum of 2 GOOSE control blocks. One Dataset for a GOCB should contain FCDAs while the other contains DataSet members that are FCDs.

Should a publisher be capable the following types of DataSet members shall be defined for the FCDA DataSet:

- single point status: stVale and q
- double point status: stVal and q
- double point: stSeld and q
- a measurement value: mag.f and q

Should a publisher be capable the following types of DataSet members shall be defined for the FCD DataSet:

- A DataSet member that has a functional constraint of ST
- A DataSet member that has a functional constraint of MX

The VLAN used shall be determined by the Network Infrastructure definitions (currently defined as either 0x050 or 0x080).

User- friendly tests as much as possible for testers and witnesses

- → Few Etherreal traces and analysis
- →Extensive use of:
- HMI of IED (event list on display, single line editor with variables)

- HMI for substation: GOOSE signals to be sent to a report, received GOOSE to be sent to a report, both to be displayed in an event list
- LEDs of IED,
- SNMP information,
- IED integrated log files (List GOOSE published messages, List GOOSE subscribed connections with attributes, Protocol of GOOSE mismatch…)

→Use of GOOSE Inspector http://siemens.siprotec.de/download_neu/html_soft/soft_goose_m.htm

The Client/Server tests total twenty-seven (27) possible test cases that could be executed for each combination of IEC 61850 Clients and Servers. For each combination, there is also a Substation Configuration Language (SCL) file exchanged used for Client configuration.

Step from Test Procedure	Test Description
GO-1	Server provides either CID or SCD file for import.
GO-2	Exchange Functionally Constrained Data Attributes
GO-3	Exchange Functionally Constrained Data
GO-4	Ability to issue and interpret the GOOSE Test Bit
GO-5	Detection of Time Allowed to Live Expiration
GO-6	*GOOSE Control Blocks*
GO-6.1	Enabling of GOCB
GO-6.2	Disabling of GOCB

11.1 GOOSE Use cases and Test cases

11.1.1 Exchange a GOOSE with FCDAs

Test: A publisher shall publisher a DataSet whose members are FCDA. S should contain as many information types as possible from the below use cases.

Expected Results: Subscriber provides confirmation that the GOOSE was received and that the information was properly interpreted.

Notes: The mechanism to provide this verification for the witness observation is subscriber specific.

11.1.2 Exchange a GOOSE with FCDs

Test: A publisher shall publisher a DataSet whose members are FCDs. S should contain as many information types as possible from the below use cases.

Expected Results: Subscriber provides confirmation that the GOOSE was received and that the information was properly interpreted.

Notes: The mechanism to provide this verification for the witness observation is subscriber specific.

11.1.3 Test bit

Test: The publisher sends either the FCD or FCDA GOOSE with the test bit set.

Expected Result: The subscriber indicates that it has received and understood the GOOSE Test bit.

Notes: The mechanism to provide this verification for the witness observation is subscriber specific. Since the test are for ED.1, the behavior is a local issue.

11.1.4 Detection of TAL Expiration

Test: The transmission of the published GOOSE is interrupted.

Note: It is a local issue on how to accomplish this (e.g. pulling the publisher's cable or setting the Enable to false.).

Expected Result: The subscribing IED detects a TAL expiration and gives some local indication.

11.1.5 GOOSE Control Blocks

11.1.5.1 Enable of Transmission

Test: A client changes the enable of a GOOSE control block from FALSE to TRUE.

Note: It is a local issue on how to accomplish this (e.g. pulling the publisher's cable or setting the Enable to false.).

Expected Result: The subscribing IED detects the delivery of the GOOSE and gives some local indication.

11.1.5.2 Disable of Transmission

Test: A client changes the enable of a GOOSE control block from TRUE to FALSE.

Note: It is a local issue on how to accomplish this (e.g. pulling the publisher's cable or setting the Enable to false.).

Expected Result: The subscribing IED detects a TAL expiration and gives some local indication.

12 Sampled Value Test Cases

12.1 TEST Description

12.2 References

Step from Test Procedure	Test Description
SV-1	Configuration of Publisher
SV-2	Configuration of Subscriber
SV-3.1	Single Phase Fault
SV-3.2	Phase to Phase Fault
SV3.3	Three Phase Fault

Ref. A

'IMPLEMENTATION GUIDELINE FOR DIGITAL INTERFACE TO INSTRUMENT TRANSFORMERS USING IEC 61850-9-2', Revision 3 (R3-0).

12.3 Publishing of 9-2 Data

UseCase: The Publisher must be capable of configuring the data stream according to the 9-2LE implementation guideline [Ref. A].

The following test cases shall be used to verify that the Publisher is capable of producing a data stream according to the 9-2LE guideline.

12.3.1 Configuration of the PUBLISHER

The publisher should be able to configure the data stream properly according to the implementation guideline. However all subscribers may not use the identical parameters to filter for the 9-2 data.

12.3.1.1 CID File

Test Case: The Publisher should produce a valid CID file that matches the configuration/setup.

Expected Results. The CID file should pass schema validation.

12.3.1.2 Publisher’s Datastream

Test Case: The Publisher should produce a valid datastream that matches the configuration/setup.

Expected Results. The captured packets file should match the configuration/setup i.e. Ethernet source, Ethernet destination, VLAN tag, noASDU, svID, ConfRev, etc.

AppID shall always be 4000 hex.

12.3.1.2.1 SmpCnt

Test Case: The Publisher should produce a datastream with a smpCnt from 0-4799 @ 60Hz and 0-3999 @ 50Hz.

Expected Results. The captured packets file should contain correct smpCnts.

12.3.1.2.2 smpSynch

Test Case: The Publisher may be able to set the smpSynch flag.

Expected Results. The captured packets file should contain correct smpSynch if settable.

12.3.1.2.3 quality

Test Case: The Publisher may be able to set the detail quality bits.

Expected Results. The captured packets file should contain correct quality bits if settable.

12.3.1.2.4 Harmonic Content

Test Case: The Publisher should be able to produce an accurate waveform containing harmonic content.

Expected Results. The captured packets file should contain correct amount of fundamental and harmonic content.

12.3.2 Subscription of 9-2 Data

UseCase: Subscribers must be able to obtain information (e.g data) from Publishers according to the 9-2LE implementation guideline [Ref. A].

The following test cases shall be used to verify that the Subscriber is capable of reading a data stream according to the 9-2LE guideline.

12.3.2.1 Configuration of the SUBSCRIBER

The subscriber should be able to configure themselves to subscribe to the data stream being produced by the publisher.

12.3.2.1.1 CID File

Test Case: The Subscriber may be able to be configured according to the publisher's valid CID file.

Expected Results. The subscriber should use the CID file for configuration.

12.3.2.1.2 Subscription of Datastream

Test Case: The subscriber should listen to the published datastream.

Expected Results. The subscriber should process the datastream and be able to show data is being received properly. i.e. metering values, no data loss alarms, etc...

12.3.2.1.3 SmpCnt

Test Case: The subscriber should correctly interpret the smpCnt for 60Hz and 50Hz.

Expected Results. The subscriber shall correctly show nominal 50 Hz (from smpCnt 0-3999) and 60 Hz (from smpCnt 0-4799) metering.

12.3.2.1.4 smpSynch

Test Case: The Subscriber may be able to read the smpSynch flag.

Expected Results. The subscriber shall decode the smpSynch flag if supported.

12.3.2.1.5 quality

Test Case: The Subscriber may be able to read the detail quality bits.

Expected Results. The subscriber shall decode the quality bits if supported and process/indicate them.

12.3.2.1.6 Harmonic Content

Test Case: The Subscriber should be able to reproduce a waveform containing accurate harmonic content.

Expected Results. The captured IED record should contain the correct amount of fundamental and harmonic content compared with the publisher.

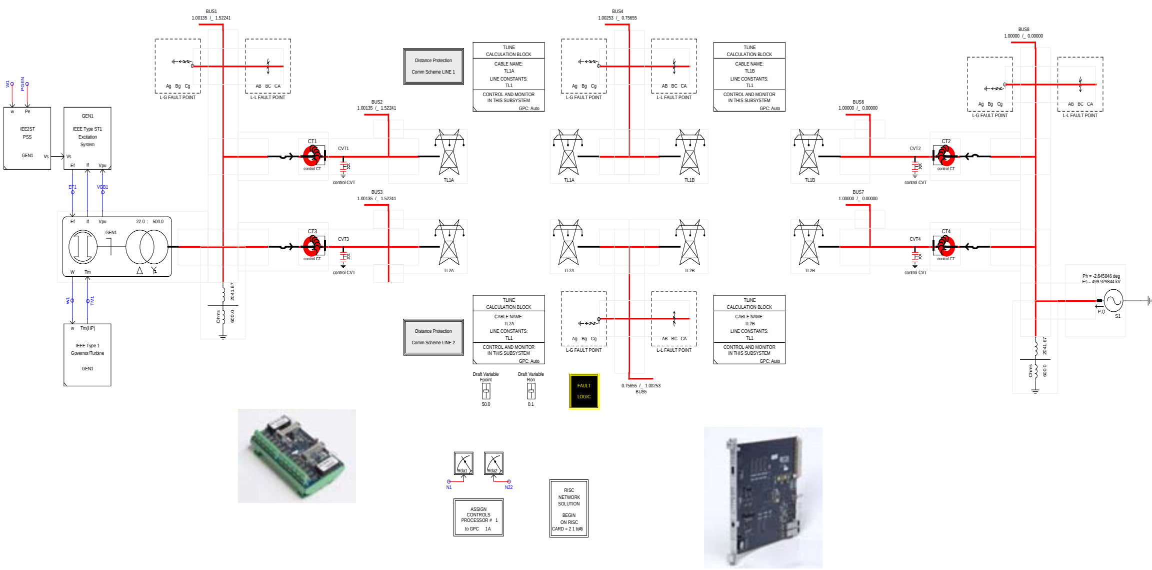
12.4 Application of 9-2 Data

UseCase: Subscribers obtaining 9-2 data must be able to properly use the data for the intended purpose i.e protection and control.

The following test cases shall be used to verify that the Subscriber is capable of using a 9-2LE data stream for their intended purpose.

12.4.1 Protection functions operation

The subscriber should be able to properly protect the intended part of the network that is affected by system faults i.e. real-time simulation or recorded waveforms.



12.4.1.1 Single phase fault

Test Case: Apply single phase fault at 10%, 50%, and 90% of the line length.

Expected Results. The IED should identify the proper fault type and clear the fault and reclose or block reclose.

12.4.1.2 Phase to phase fault

Test Case: Apply phase to phase fault at 10%, 50%, and 90% of the line length.

Expected Results. The IED should indentify the proper fault type and clear the fault and reclose or block reclose.

12.4.1.3 Three phase fault

Test Case: Apply three phase fault at 10%, 50%, and 90% of the line length.

Expected Results. The IED should indentify the proper fault type and clear the fault and reclose or block reclose.

12.4.2 Loss of datastream

Test Case: Analogue values lost (physically disconnected connection or publisher operating mode configured to Off) shall not cause IED to maloperate protection.

Expected Results: Protection does not maloperate.

13 Participant Product Descriptions

This appendix contains descriptions of the different products used for the interoperability tests. Product descriptions were provided by the individual participants.

13.1 Alstom

13.1.1 P545 IED

The P545 IED tested at the UCA IEC 61850 Interoperability Test belongs to the P543 - P546 range of high-speed current differential unit protection IEDs. The P54x is designed for all overhead line and cable applications, as it interfaces readily with the communications channel between line terminals. The interface options support direct fibre optic – including IEEE C37.94 - or multiplexed digital links.

Tripping uses a proven characteristic comparing differential current with through current. Phase differential elements of this type offer consistent detection of solid and resistive faults, with optimum faulted phase selection, tripping, and indication.

A full range of back-up protection is integrated. This enhances the dependability of the protection, as hot-standby elements can be brought into service whenever a signalling channel outage may occur. The P54x has high-speed subcycle distance elements, allowing use in differential applications, distance, or both in parallel. One relay type therefore becomes the standard in all HV-EHV-UHV line protection applications, duplicated where dual redundant main protection is demanded. Spares holdings are reduced, with one universal relay type used instead of two or more discrete models in the past.

Key features:

Current differential protection:

- Applicable to all lines and cables, long or short, strong and weak infeeds
- Phase selectivity without compromise on resistive fault sensitivity

Multi-terminal applications - each relay equipped for 2 or 3 ended schemes.

Adapted to suit many different substation and protected unit topologies:

- In-zone transformer-feeder applications (P543/P545)
- Compensates for line CT ratio mismatches and capacitive charging current
- Patented differential CT supervision technique allows independent alarms for each CT (including the remote CTs)
- Compensated overvoltage features to counter Ferranti effects on lightly loaded long transmission lines

Readily interfaces to end-end communications channels:

- Differential scheme, and distance teleprotection over MUX or fibre links

InterMiCOM ALSTOM option for end-end protection communication:

- Reliable and secure, saving the investment in external teleprotection equipment

Distance Protection:

- High speed operation in less than one cycle
- Optional Mho and Quadrilateral zones
- Load blinder prevents spurious trips cascading through the network in extreme conditions such as on the verge of a blackout

Power swing alarm and block, plus out of step trip:

- Unrivalled detection principle - automatic configuration, with no impedance starters or timer bands to set

Multi-shot autoreclosure with check synchronism

- Programmable scheme logic readily interfaces with multiple automation protocols, including DNP and IEC 61850
- The P543 - P546 range offers fast, highly selective protection for use in line and cable feeder applications, right up to the highest transmission voltages. All models include differential main protection, with distance protection as an ordering option.
- The model of P545 tested at the UCA IEC 61850 Interoperability Test featured a 9-2LE-compliant Sampled Values interface, in place of the conventional CT/VT inputs. The P545 subscribes to the Sampled Values datastream from a Merging Unit via its 9-2 Ethernet interface board, which re-samples the values and outputs the current and voltages as if they were from the conventional CT/VT module. The protection algorithms are unchanged - they are the same for the 9-2 Ethernet board and the CT/VT module(s).

13.1.2 Alstom COSI-NXCT-F3 and COSI-NXMU

The Alstom COSI product range (Compact Optical Sensor Intelligence) includes innovative digital instrument transformers for AC and DC applications. The COSI-NXCT and COSI-NXCT-F3 optical current sensors bring a new level of accuracy to sensing over the range between 1 A rms and 160 kA rms.

The reduced size and weight are attractive benefits compared to conventional oil-filled equipment, allowing placement in compact substations or in retrofit applications where space may be limited. The broad dynamic range makes these CTs particularly well suited for both high-precision metering and protection applications at the same time. The accurate measurement of DC and AC to the 100th harmonic and the measurement of phase angle is a must for new Smart Grid applications.

The COSI-NXCT-F3 optical current sensor is a flexible, portable optical current transformer sensor that is very easy to install. The COSI-NXCT-F3 consists of an electronics module, a fiberglass sensor box, and a flexible PVC conduit wrap-around sensing cable. The sensing cable is designed to be wrapped around high-voltage bushings, generator buses, and other conductors in ways not possible with conventional Current Transformers. The sensing cable is an all-dielectric cable, which connects to the electronics, giving the user the same high performance capability and output options as the high-voltage optical CT (COSI-NXCT). The COSI-NXCT-F3 is an ideal solution for installations in difficult spaces, on a temporary or permanent basis.

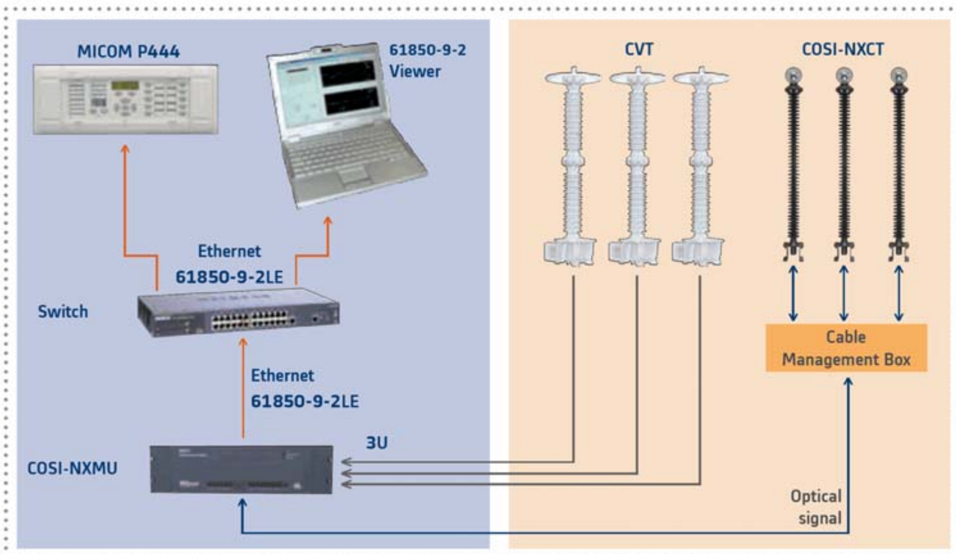
The COSI-NXCT-F3 has metering grade accuracy to 0.15%, and it can measure both AC and DC currents with this accuracy from 1 A to 160 kA, depending on the number of sensing cable loops used to measure the current.

Customer Benefits:

- Accuracy exceeds ANSI/IEEE Class 0.15S/IEC Class 0.2S for metering and IEC Class 5P/IEEE 10% for protection

- Wide dynamic range
- Bandwidth from DC to 100th harmonic
- No magnetic core saturation
- Excellent phase accuracy
- Flexible Form Factor
- Easy installation and configuration
- Intrinsically safe and environmental friendly: No oil, gas or SF6. No hazardous open secondaries. No violent failures

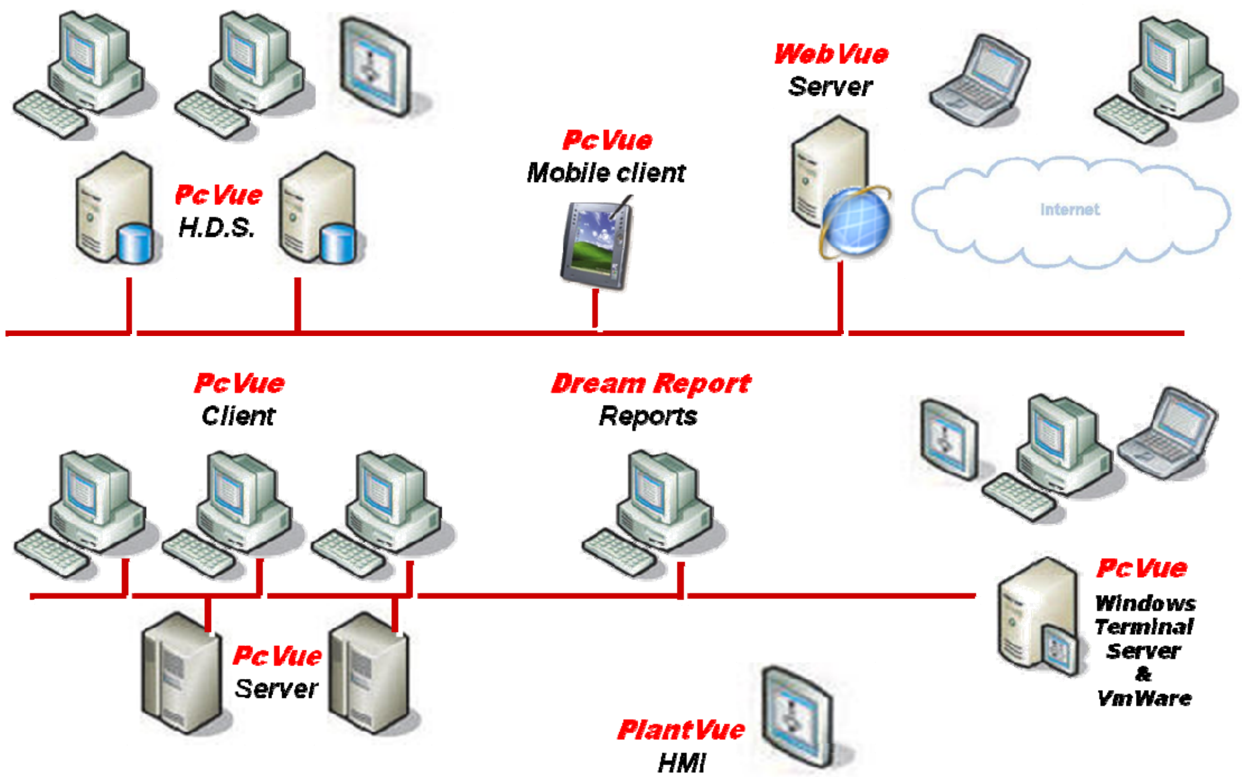
The COSI-NXMU is a hardware add-on to the COSI-NXCT-F3 electronics module that integrates a set of analog voltages together with the digital data from the COSI-NXCT-F3.



The COSI-NXMU provides:

- Global synchronization through a 1PPS input
- Merging and synchronization of primary optical CT and analog VT signals
- IEC 61850-9-2LE (Ethernet 100BaseFx) standardized interface
- 80 and 256 samples / cycle
- Redundant optical Ethernet outputs (choice of connector options)
- Configurable scaling via software

13.2 ARC Informatique



13.2.1 PcVue Solutions

Founded in 1981, **ARC Informatique** is a privately held company with its headquarters in Paris, France. The company manufactures and markets industrial software. Originally developed for the process industries the software now also caters for infrastructure, utilities and building management systems.

In 2008, ARC Informatique launched the **PcVue Solutions** offer of software, hardware and application support as a global service to the markets of Infrastructure, OEM HMI, building automation, power generation & distribution, airports, batch and continuous processes.

Certified ISO 9001 and ISO 14000, the company is establishing an international presence through direct sales offices in the USA, Europe and Asia and a network of partners and distributors. To date, over 41,000 licenses have been shipped worldwide.

PcVue is a full-featured product that represents the latest advances in SCADA software for multi-station monitoring and control. Its Smart Generators ease application configuration from third party sources including AutoCad®, CoDeSys, Siemens Step7®, FactoryLink® and ISaGRAF®. There are features, add-ins and tools to handle communications, networking, alarms and database management. Its WebVue thin-client solution operates in a web browser either on an intranet or via the Internet. Security and safety are ensured via standards based on Microsoft technologies, including Internet Information Server and Active Directory.

The new PcVue range has been designed using recommendations from integrators, OEMs and end-users, and based on ARC Informatique's considerable experience in the industrial automation sector. PcVue features modern ergonomics and tools based on object technology to minimize the time for application development, including the latest tools from Microsoft, user interface standards and the security features of Windows 7 and Windows Server 2008 R2.

PcVue provides a flexible solution for supervising industrial processes, utilities and infrastructure. It meets industrial standards of reliability and performance while maintaining the user-friendliness of an office application. It spans requirements from single-user standalone applications to complex client-server systems with redundancy.

CimWay is the data acquisition module in ARC Informatique portfolio. It supports communication with hundreds of device types via built-in protocols ranging from the multi-purpose Modbus and OPC-DA to the most specialized such as LonWorks, BACnet and IEC 61850.

For more information, visit www.pcvuesolutions.com

13.3 EFACEC Engenharia e Sistemas, S.A.

Automation Studio

Automation Studio is an “all-in-one” software that provides an easy to use engineering environment for the automation engineer or system integrator. It is also the single device tool for all Efacec automation products from controllers and relays to gateway and HMI products.

It has been designed for the engineer working on any type of projects from simple one-man projects to multiple distributed control system projects where cooperative teamwork is required.

All engineering activities from design, configuration and programming, through validation, testing and commissioning up to operation and maintenance are supported by the toolset, hence providing a single environment for all engineering roles during the entire system life-cycle.

It is based on modern engineering tool paradigms such as unified project system, single-click deployment, reconfigurable window layouts, copy/paste and drag/drop, wizards or diagram designers.

Automation Studio feature overview:

Integrated Engineering Environment

- Unified Project System
- Integrated Tools
- Intuitive Environment
- Simultaneous Editing
- Reconfigurable Window Layouts
- Common Supporting Windows
- Background tasks

Analysis Tools

- Sequence of events
- COMTRADE records and fault reports
- Statistical and trend data records

Configuration and Programming Tools

- SCADA Database Configuration
- IEC 61131-3 Editors and Compilers
- IED Configuration
- Device Templates and Automation Objects
- Wizards and Refactoring Tools
- Validation and Comparison
- Import and Export Tools
- Diagram Editing Tools
- Simulation Mode

Online Management

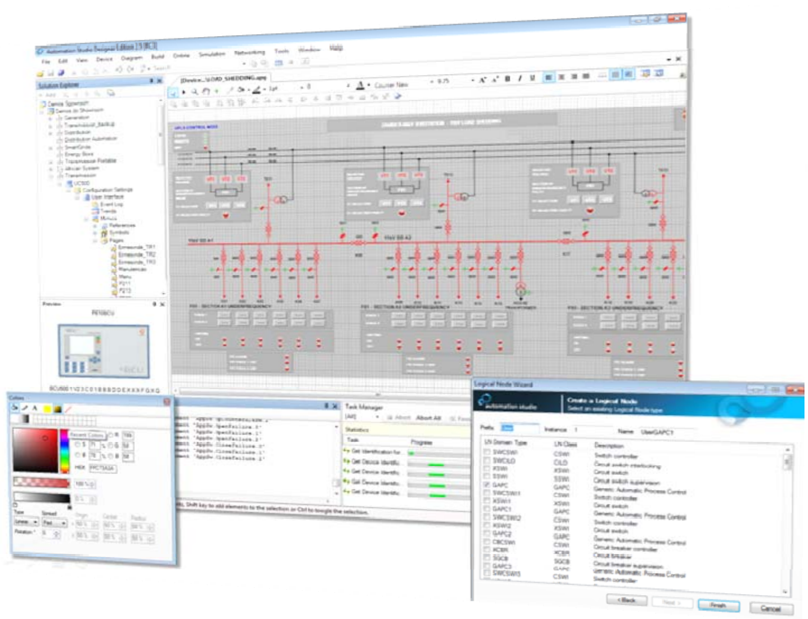
- Device Access for Deployment and Extraction
- Network Scanner and Commands
- System Control Panel
- Automatic Record Retrieval
- Online Monitoring Mode
- Access to IP Devices
- Operational Settings

IEC 61850

- Third-party IEC 61850 Devices
- SCL Import/Export, including SCD files
- Communication Engineering
- Create SCL from Online Device
- SCL Model Designer
- SCL Validator
- Device Browser

Automation Studio product editions:

- Automation Studio Explorer Edition
- Designed as a vendor-neutral commissioning and operational support tool, Explorer Edition includes features such as network scanning, IEC 61850 device browser and online monitoring together with SCL management. It also includes file viewers and editors for formats such as COMTRADE, event records or operational settings.
- Automation Studio Engineer Edition
- Mainly focused on device and HMI configuration and programming, Engineer Edition includes full library and system/device projects, mimics designer, IEC 61131-3 programming together with all Explorer Edition features.
- Automation Studio Designer Edition
- Targeted for team and system engineering, the Designer Edition adds comparison, refactoring, productivity wizards, compound mimic symbols, objects and templates, offline simulation, SCL model designer, system control panel, among other features.



13.3.1 BCU 500

BCU 500 is a flexible bay control unit for utility transmission and sub-transmission featuring protection-related functions.

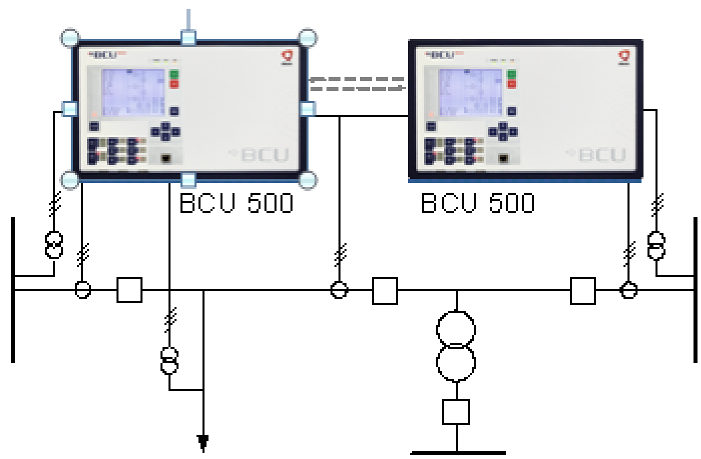
Main features:

- Multiple communications options
- This device can be used as a multiprotocol communication master and/or slave station
- Supports standard protocols like IEC 60870-5-101/104, DNP 3.0, IEC 60870-5-103, ModBus or IEC 61850.
- I/O
- Flexible and modular I/O configurations are available, allowing the BCU 500 to match the specific requirements of each application.
- Supports up to 304 I/O points from binary I/O to analog DC or AC inputs.
- Distributed automation according to IEC 61850
- Provides open system design and full compatibility with other compliant devices, engineering tools and systems
- The user may fully define logical nodes and logical device allocation, including user-defined logical node classes, providing unmatched logical configuration capabilities
- Includes both server and GOOSE messaging, enabling peer-to-peer distributed automation
- IEC 61131-3 PLC programming
- User-defined algorithms programmed in IEC 61131-3
- Supports prioritized cyclic and multi-event scheduling to meet diverse functional needs
- Built-in control and protection functions
- Firmware functions permit control and supervision of up 20 circuit breakers and switches with optional synchronism-check
- Control functions feature direct or select-before-operate controls, secure hardwire or distributed interlocking and multi-level authority sources
- A set of complementary built-in protection function is also available in BCU 500, such as current, voltage and frequency functions.
- User interface
- Local
- Bight high-contrast color LCD
- 16 Programmable alarms and 8 Programmable function keys
- Status LEDs to indicate POWER, RUN and LA\N
- Open/Close keys and Navigation Keypad
- Built-in webserver allows remote user interface without additional tools

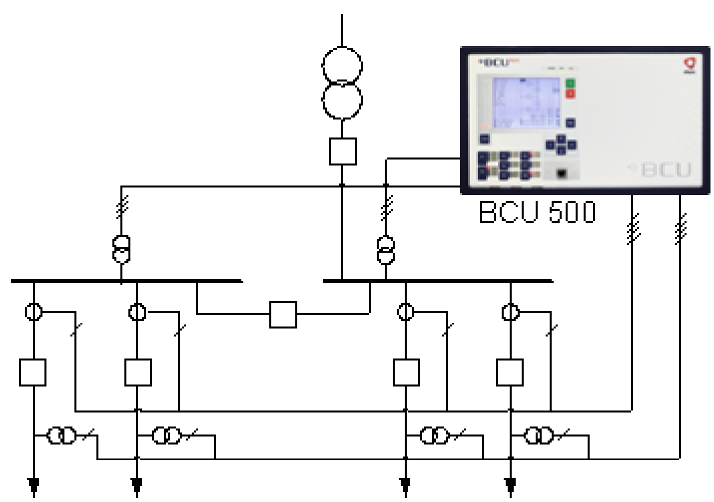
- Recording, measurement and metering
- Event recorder with millisecond or better precision
- Disturbance recorder
- Accurate measurement of magnitude, angle, power, energy, impedance and frequency for three-phase systems or other non-phase related current and voltage
- Integrated engineering
- Engineering is fully integrated in the Automation Studio toolset whether a device oriented or a distributed control system approach is required.
- While being highly adaptable products, configuration and maintenance efforts are reduced with features like templates, libraries, copy-paste or drag-and-drop.

Example application description:

- Double breaker or breaker-and-a-half topologies
- Complex user-defined automation schemes and distributed automation
- Synchronism-check included



- Multi-bay control in one single device
- Control functions, including load shedding and restoring



UC 500

The UC 500 server family provides an all-in-one flexible communication gateway, automation platform and HMI solution for utility and industrial applications.

The multiple hardware options and its modular and scalable software architecture support the full spectrum of applications from integrated cost effective station servers to high performing distributed applications, such as large substations or power plants.

Product range:

- **UC 500 Station Server**
- SCADA/HMI server, station controller or gateway/data concentrator.
- Software product for application to PC-based hardware platforms.
- **UC 500E Embedded Station Server**
- UC 500 station featuring industrial grade hardware platform with no rotating parts, suitable for harsh environments and targeting minimal maintenance.
- **UC 500H High-availability Station Server**
- UC 500 high-availability embedded hardware platform featuring hot swappable power supplies and redundant CPUs

Main features:

- **Single platform for station servers and HMI**
- **Multiple communication options**
  - o The available communication modules support over 50 different serial or IP communication protocols, including all well established communication standards
  - o Supporting up to 8 control/management center independent channels and up to 256 IED/RTU connection per unit
  - o Up to 16 different protocols may be active in each unit, hence allowing the integration of a diverse range of remote stations, SCADA software, RTUs, meters, protection relays, controllers or recorders of multiple manufactures
  - o Supports SNMP/ICMP monitoring, hence allowing full supervision of all active assets in the communication system.
- **IEC 61850 interface**
  - o For substation and power plant applications the UC 500 station servers fully support IEC 61850 and can be applied as a true IEC 61850 gateways
  - o Provides open system design and full compatibility with other compliant devices, engineering tools and systems
- Hosts SCADA/HMI server
  - o HMI solution provides a concise process view for operational purposes, management as well as for data analysis

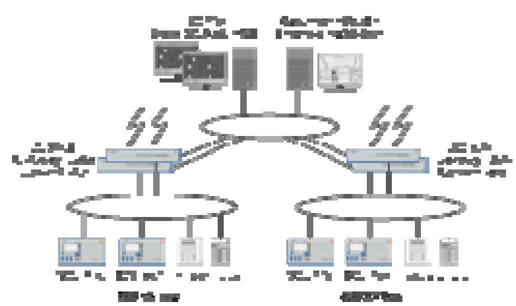
- o Mimics displays can be setup with full blown zoom-enabled 2D vector graphics
- o Gradients and transparencies and multiple animation options are available

- **Web-enabled interface**
- **IEC 61131-3 PLC programming**
  - o Optimized logic processor engine with large memory capacity for application of extensive user-defined algorithms programmed in IEC 61131-3
- **Multiple redundancy options**
  - o Both UC 500 and UC 500E can be deployed in standalone or in hot-standby configurations.
  - o Hot-standby configurations allow high availability with continuous data point and database synchronization from active to stand-by unit.
  - o Failure detection and failover management is handled by an external control panel that also performs serial port switching and manual redundancy control.
  - o The UC 500 also provides transparent redundant communication channel/port operation for selected protocols such as DNP or IEC protocols (in either serial or IP links)
- Security features built-in
  - o Supports encryption for selected protocols such as HTTPS
  - o Embedded OS option reduces security vulnerabilities
  - o Firewall and anti-virus options
- Data and control processing, alarms, events and historian
  - o Core data processing such as unit and linear conversions, measurement filtering, thresholds and alarms levels are available for each data point without requiring any additional IEC 61131-3 programming
  - o Processing of alarms and of alarm acceptance and notification is also included
  - o Direct or select-operate methods are available together with execution model mapping for multiple protocols as well as control blocking, final state checking and execution signaling in either SCADA, automation or gateway applications.
  - o A database centered history recording function which includes event data and periodic/statistical data logging is provided.
  - o Data records are provided with 1 ms resolution time stamping (source and local).

Example Applications:

UC 500

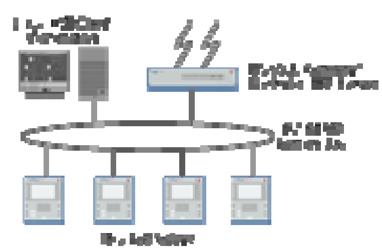
- Transmission substation local SCADA

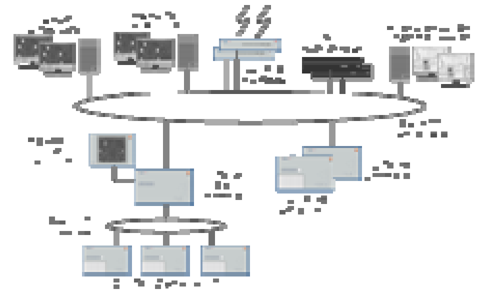


UC 500E

- Integrated distribution substation

  gateway and HMI server





UC 500H

- Hydro power plant DCS System group controller

13.4 GE

13.4.1 F650

KEY BENEFITS

- Unique built-in control features - Comprehensive protection plus programmable logic
- Flexible and cost effective control for complex systems - Use IEC compatible programmable logic to customize the functionality of your protection & control system to address unique, site specific applications
- Human machine interface (HMI) - Standard backlit LCD display with 4 x 20, optional 16 x 40 (240 x 128 pixels) graphical LCD, programmable buttons, and rotary knob for selecting setting menus, and submenus.
- Minimize replacement time - Modular with card draw-out construction
- Reduce troubleshooting time and maintenance costs - IRIG-B time synchronization, event reports, waveform capture, data logger
- Cost Effective Access information - Via multiple protocols, through standard RS232, & RS485, Ethernet Ports.
- Optimal integration flexibility via open standard protocols - Modbus RTU, DNP 3.0 Level 2, IEC60870-5-104, IEC61850, , IEC 870-5-103
- Minimize communication down time - Reliable redundant Ethernet Communication ports with 10/100BaseTX, 100BaseFX with ST connectors, and optional double 100BaseFX, with ST connectors
- Complete asset monitoring - Full metering including demand & energy
- Follow technology evolution - Flash memory for product field upgrade

APPLICATIONS

- F650: Management and primary protection of distribution feeders and bus couplers
- F650: Backup protection of busses, transformers and power lines
- G650: Packaged generator mains failure detection
- G650: Distributed generation management device
- G650: Reliable Distributed Generation interconnection protection system
- W650: Wind turbine protection, control and monitoring
- W650: Distributed generation grid interconnection device

FEATURES

- Protection and Control
  - Up to 32 Programmable digital inputs
  - Up to 16 digital outputs
  - Trip Circuit Supervision
  - Redundant power supply option
  - Configurable PLC logic according to IEC 61131-3
  - Fully configurable graphic display HMI interface
  - Alarms panel
- Monitoring and Metering
  - Energy metering
  - Demand metering
  - Trip circuit monitoring
  - Oscillography
  - Data logger
  - Sequence of event
  - Self diagnostic
- User Interface
  - Large graphic (16x40) or regular (4x20) character display
  - Easy to use control via Shuttle key
  - Front USB port or standard RS232
  - Rear wire 10/100BaseTX Ethernet for LAN connection.
  - Rear wire CAN bus port (OPEN CAN protocol - W650)
  - Optional fibre optic 100BaseFX Ethernet, single or redundant.
  - Optional rear RS485 port
  - 1 ready LED and 15 programmable LED indicators
  - EnerVista™ Integrator providing easy integration of data in the 650 relay into new or existing monitoring and control systems

- Overview
    - o The 650 family has been designed as a comprehensive protection, control, metering and monitoring package. The microprocessor based architecture is a complete solution for different applications that complies with the most relevant international standards.
    - o All the elements required for each application have been integrated into a single package for a cost-effective, reliable and simple utilization. The low number of components, thanks to the use of state of the art but mature technology, deliver a very highreliability.
    - o Hardware inputs and outputs have been designed in a modular way that allow easy migration from simple to more complex applications.
    - o The control functions include a full-scheme virtual PLC with an optional graphical display. The combination of both elements provide total control for a bay. This means real-time monitoring of breakers and selector switches, open and close commands supervised by the programmable interlockings and metering screens.
    - o The metering capability allows 0.5% accuracy for current and 1% from 10 V to 208 V for voltage in metering range.
    - o Monitoring functions include a 479 event recorder, and a programmable oscillography recorder.
    - o The 650's communications capability and option make the product very unique. These units include a maximum of three independent communication ports: COM1, COM2 and COM3, with many physical choices through the use of two removable plug and play boards.
    - o The brain of 650 units includes a powerful built-in virtual PLC. This PLC can be programmed according to the IEC 61131-3 language by functional block diagrams.
    - o 650 units come with 8 to 32 digital inputs and with 8 to 16 outputs depending on options. All digital inputs may be filtered with a separate debounce time to tailor customer requirements.
    - o On top of that, programmable threshold allows the use of different voltage levels (0 to 255 Vdc) in the same model. This is accomplished by programming the requested thresholds using advanced "quasi analog" inputs.
    - o EnerVistaTM software allows the user to program all the interlocking and switching sequences. This is done in an easy way through the graphic interface. No special knowledge of software application is needed.
    - o The same EnerVistaTM software provides a graphic interface for the HMI. The monitoring, metering and alarm panel screens can be created just by clicking and dragging the symbols. 650 units incorporate a complete library of symbols.
- Metering
    - o The F650 provides the following metering values.
    - o Current: Ia, Ib, Ic, In, Ig, Isg
    - o Phase-to-phase and phase-to-ground voltage values for bus and line: Van, Vbn, Vcn, Vab, Vbc, Vca, Vx.
    - o Active power (per phase and total): Wa, Wb, Wc, W.
    - o Reactive power (per phase and total): VARa, VARb, VARc, VAR.
    - o Power factor (per phase and total)
    - o Frequency
    - o These signals are available for local display, and accessible remotely using communications.
- Recording Functions
    - o The recording functions of the F650 include:

    - Event recorder capable of storing 479 time-tagged events (1 true millisecond accurate tagging).
    - Up to 20 separate oscillography records can be stored in memory. The capacity of each record will depend on the type of oscillo selected (1 Mbyte/Max. No. Osc).
    - These records are stored in non volatile memory. Therefore, there is no need for internal battery monitoring or maintenance.
- Trip circuit monitoring
    - 650 units offer as an option two complete supervision circuits for breaker trip and closing coils and circuits. These supervision inputs monitor both the battery voltage level and the continuity of the trip and/or closing circuits, applying current through those circuits and checking that it flows properly. In order to apply this feature it is necessary to choose I/O board 1 option 2.
- Communications
    - 650 units incorporate up to three ports that operate independently. Redundant ports are available for high reliability applications:
    - Available protocols for rear port 1 and 2 are ModBus RTU, IEC 103, and serial DNP 3.0.
    - The third port is located in a removable communications card. This plug and play card can be easily changed in the future as new standards arrive to the market, thus providing a migration path to the customer.
    - The protocol available for the third port is DNP 3.0 over TCP/IP, UDP/IP, ModBus TCP/IP and IEC 60870-5-104.
- Setup Program
    - Windows based EnerVistaTM software allows complete access to relay information as well as PLC type logic configuration.
- Keypad & Display
    - There are versions with text display (4x20 characters) as well as large graphic display (16x40 characters) with fluorescent backlit for a better visibility under all conditions.
- LED Indicators
    - Up to 15 programmable LEDs green, yellow and red, with tags tailored to the application allow quick and safe indicators understanding. Five additional large keys, all of them configurable, help automating frequently performed control functions (such as breaker open, close, recloser lockout).
- Easy Keys
    - The easy keys make the 650 equipment extremely easy to use, very much like the key controls in a domestic DVD.
- EnerVista™ Software
    - The 650 comes with EnerVistaTM, an industry-leading suite of software tools that simplifies every aspect of working with GE Multilin devices. EnerVistaTM software is extremely easy to use and provides advanced features that help you maximize your investment in GE Multilin products. EnerVistaTM 650 setup software allows complete access to relay information as well as PLC type logic configuration. PLC is programmed using standard IEC 1131-3.
- EnerVista**TM** Launchpad
    - EnerVistaTM Launchpad is a complete set of powerful device setup and configuration tools that is included with the 650.
    - Set up the 650 - and any other GE Multilin device - in minutes. Retrieve and view oscillography and event data at the click of a button.

  - Build an instant archive on any PC of the latest GE Multilin manuals, service advisories, application notes, specifications or firmware for your 650.
  - Automatic document and software version updates via the Internet and detailed e-mail notification of new releases.
- EnerVista**TM** Viewpoint
  - EnerVistaTM is a premium workflow-based toolset that provides engineers and technicians with everything they need to monitor, test and troubleshoot GE Multilin IEDs and manage settings files with ease. The 650 includes an evaluation version of EnerVistaTM Viewpoint.
  - Settings file change control and automatic error checking make creating, editing and storing settings a snap
  - Plug-and-Play monitoring automatically creates customized monitoring screens for your 650 - no programming required
  - Powerful testing tools help shorten your commissioning cycle
  - Quickly retrieve oscillography and event data when a fault occurs
  - See the EnerVistaTM Suite section for more information.

13.4.2 SR350

KEY BENEFITS

- Easy to use and intuitive overcurrent protection and control for feeder applications.
- Effortless draw-out construction eliminates requirement for test switches and reduces downtime
- Environmental monitoring system to alarm on destructive operating conditions and plan preventative maintenance
- Easy to use interface and set up in one simple step

- Accelerated Life Cycle Tested to ensure reliability of relay operation under abnormal conditions
- Advanced power system diagnostics to increase reliability through fault and disturbance recording capabilities
- Flexible communications with multiple ports & protocols to allow seamless integration into new and existing infrastructure
- Arc flash mitigation via zone inter-tripping, flex curves, and multiple settings group
- Powerful Security Audit Trail tool to increase security and minimize system risks by tracking setting changes
- Application flexibility with the use of programmable logic elements

APPLICATIONS

- Industrial feeders with enhanced breaker monitoring diagnostics, etc.
- Distribution utility down stream breaker protection
- Medium voltage Utility feeders with advanced control features Cold Load Pickup, auto reclose, multiple settings group, etc

FEATURES

- Protection and Control
    - Phase, neutral and ground TOC and IOC
    - Undervoltage, overvoltage, frequency
    - Neutral/ground directional
    - Negative sequence Overcurrent
    - ANSI, IAC, IEC, flex curves
    - Cable Thermal Model Protection
    - Breaker Failure
    - Cold Load Pick Up
    - Four-shot auto-reclose
    - 8 digital inputs, 7 contact outputs
    - Two setting groups
- Metering & Monitoring
    - Event Recorder: 256 events
    - Oscillography with 32 samples per cycle
    - IRIG-B clock synchronization
    - Relay health diagnostics
    - Security audit trail
- Metering - current, voltage, power, frequency
- User Interface
    - 4 line display for easy viewing of key data
    - 10 LED indicators for quick diagnostics
    - Front USB and rear RS485 serial communications
- Multiple Communication Protocols:
    - IEC 61850
    - IEC 61850 GOOSE,
    - MODBUS TCP/IP, MODBUS RTU,
    - DNP 3.0, IEC60870-5-104, IEC60870-5-103

- EnerVista™ Software
    - EnerVista Software- an industry-leading suite of software
    - tools that simplifies every aspect of working with GE Multilin devices.
    - Quick & easy configuration requiring minimal settings for most feeder applications.
- Overview
    - The 350 relay is a member of the SR 3 Series family of Multilin relays. This protective device is used to perform primary circuit protection on medium voltage feeders and down stream protection for distribution utilities.
    - The basic protection function of this relay includes multiple phase, ground, and neutral time and instantaneous overcurrent elements for coordination with upstream and downstream devices. Additionally, the device provides essential feeder breaker control features such as cold load pick up blocking, breaker failure, and auto reclose.
    - The robust 350 streamlines user work flow processes and simplifies engineering tasks such as configuration, wiring, testing, commissioning, and maintenance. This cost-effective relay also offers enhanced features such as diagnostics, preventative maintenance, arc flash mitigation and security.
- Easy to Use
    - Drawout Construction
    - The 350 offers a complete drawout feature eliminating the need for rewiring after testing has been concluded. The withdrawable feature also eliminates the need to open the switch gear door and disconnect communication cables, eg. Ethernet fiber, copper, RJ45, etc prior to removing the relay from the chasis
    - Effortless Retrofit
    - The small and compact 350 enables multiple relays to be mounted side by side on medium voltage panels. It also allows easy retrofit into existing S1 and S2 cutouts with adapter plates.
- Easy to Configure
    - Fast & Simple Configuration
    - The 350 requires minimal settings for configuring standard feeder protection applications. The entire feeder protection setup can be completed in one easy step.
    - Advanced Communications
    - Easy integration into new or existing infrastructure
    - With several Ethernet and serial port options, and a variety of protocols, the 350 provides advanced and flexible communication selections for new and existing energy management, SCADA, and DCS systems.
- Enhanced Diagnostics
    - Preventative Maintenance
    - The 350 allows users to track relay exposure to extreme environmental conditions by monitoring and alarming at high ambient temperatures. This data allows users to proactively schedule regular maintenance work and schedule upgrade activities. The diagnostics data enables the user to understand degradation of electronics due to extreme conditions.

- Cost Effective
    - Robust Design
    - The 350 is subjected to Accelerated Life Testing (ALT) to validate accurate relay function under specified normal conditions. The device is further tested for durability through Highly Accelerated Life Testing (HALT) where it undergoes extreme operating conditions. The robust 350 design ensures long term operation.
    - Reduced Life Cycle Cost
    - The 350 is designed to reduce total installation and life cycle cost for feeder protection. The draw out construction of the device reduces downtime during maintenance and decreases extra wiring needed for relay testing and commissioning.
    - Multiple Options
    - Several option for protection & communications are provided to match basic to high end application requirements.
    - Protection
    - The 350 feeder protection system offers protection, control and monitoring in one integrated, economical and compact package.
    - Timed Overcurrent (Phase, Ground, Neutral)
    - The 350 has three-phase TOC elements which enables coordination with upstream and downstream protection devices such as fuses, overload relays, etc to maximize fault selectivity and minimize interruptions and downtime.
    - Multiple time current curves are available including IAC, IEC, ANSI and IEEE curves. Additional user programmable flex curves can be used to customize and meet specific coordination requirements. The TOC has both linear and instantaneous reset timing function to coordinate with electro-mechanical relays
    - Instantaneous Overcurrent (Phase, Ground, Neutral)
    - The instantaneous element provides fast clearance of high magnitude faults to prevent damage to the power infrastructure and the equipment connected to it.
    - Neutral Overcurrent
    - The neutral signal is derived as the residual sum of the three phase CTs eliminating the need for an additional ground sensor.
    - Sensitive Ground Overcurrent
    - Sensitive ground protection feature detects ground faults on high impedance grounded systems in order to limit damage to conductors and equipment. Special low ratio CT's are used for this purpose to detect low magnitude ground faults.
    - Over/Under Voltage Protection
    - Overvoltage / Undervoltage protection features can cause a trip or generate an alarm when the voltage exceeds a specified voltage setting for a specified time.
    - Frequency Protection
    - The 350 offers overfrequency and underfrequency elements to improve network (grid) stability using voltage or frequency based load shedding techniques.
    - It also provides back up protection when protecting feeders and other frequency sensitive power equipment.
    - Arc Flash Mitigation
    - The 350 relay is equipped with multiple setting groups and two user definable inverse curves -FlexCurves A and B for fast and reliable arc-flash mitigation and breaker operation. In the event of an arc-flash, the relay can be set to communicate to any upstream or downstream devices via IEC 61850 GOOSE messaging.

    - Cable Thermal Model
    - The cable thermal modelelement protects feeder cables against overheating due to excessive load. It estimates the temperature rise of current carrying conductors based on the amount of current flow (I2R) and alarms when temperature rise exceeds a threshold value. This protection feature is essential to ensure the longevity of electrical feeders; particularly important to prevent premature cable failures, expensive repair costs and system down time.
    - Neutral/Ground Directional Overcurrent
    - The directional ground overcurrent isolates faulted feeders in ring bus or parallel feeder arrangements. It also allows detection of back feed of fault current from feeders with motors.
- Automation and Integration
    - Inputs & Outputs
    - The 350 features the following inputs and outputs for monitoring and control of typical feeder applications:
    - 8 contact Inputs with programmable thresholds
    - 2 Form A output relays for breaker trip and close with coil monitoring
    - 5 Form C output relays
    - IEC 61850 GOOSE
    - The 350 supports IEC 61850 Logical Nodes which allows for digital communications to DCS, SCADA and higher level control systems.
    - In addition, the 350 also supports IEC 61850 GOOSE communication, providing a means of sharing digital point state information between 350’s or other IEC61850 compliant IED’s.
    - Eliminates the need for hardwiring contact inputs to contact outputs via communication messaging.
    - Transmits information from one relay to the next in as fast as 8 ms.
    - Enables sequence coordination with upstream and downstream devices.
    - When Breaker Open operation malfunctions, GOOSE messaging sends a signal to the upstream breaker to trip and clear the fault.
    - Logic Elements
    - The 350 relay has sixteen Logic Elements available for the user to build simple logic using the state of any programmed contact, virtual, remote input or the output operand of a protection or control element.
    - The logic provides for assigning up to three triggering inputs in an “AND/OR” gate for the logic element operation and up to three blocking inputs in an “AND/OR” gate for defining the block signal. Pickup and dropout timers are available for delaying the logic element operation and reset respectively.
    - Virtual Inputs
    - Virtual inputs allow communication devices the ability to write digital commands to the 350 relay. These commands could be open/close the breaker, changing setting groups, or blocking protection elements.
    - Multiple Settings Group
    - Two separate settings groups are stored in nonvolatile memory, with only one group active at a given time. Switching between setting groups 1 and 2 can be done by means of a setting, a communication command or contact input activation.
    - The two settings groups allow users to store seasonal settings- such as for summer and winter or alternate profiles such as settings during maintenance operations.

- Security
  - Security Audit Trail
  - The Security Audit Trail feature provides complete traceability of relay setting changes at any given time and is NERC CIP compliant. The 350 maintains a history of the last 10 changes made to the 350 configuration, including modifications to settings and firmware upgrades. Security Setting Reports include the following information:
  - If Password was required to change settings
  - MAC address of user making setting changes
  - Listing of modified changes
  - Method of setting changes - Keypad, Front serial port, Ethernet, etc.
  - Password Control
  - With the implementation of the Password Security feature in the 350 relay, extra measures have been taken to ensure unauthorized changes are not made to the relay. When password security is enabled, changing of setpoints or issuing of commands will require passwords to be entered. Separate passwords are supported for remote and local operators, and separate access levels support changing of setpoints or sending commands.
- Advanced Communications
  - The 350 incorporates the latest communication technologies making it the easiest and the most flexible feeder protection relay for use and integration into new and existing infrastructures. The 350 relay provides the user with one front USB and one rear RS485 communication port. Also available with the 350 is a rear communication port with Ethernet Fiber and Copper. Through the use of these ports, continuous monitoring and control from a remote computer, SCADA system or PLC is possible.
  - The 350 supports popular industry standard protocols enabling easy, direct integration into electrical SCADA and HMI systems. The protocols supported by the 350 include:
  - IEC 61850
  - IEC 61850 GOOSE
  - DNP 3.0
  - Modbus RTU
  - Modbus TCP/IP
  - IEC 60870-5-103
  - IEC 60870-5-104
  - These protocols make it easy to connect to a Utility or Industrial automation system, eliminating the need for external protocol converter devices.

13.5 Hirschmann

13.5.1 MACH1000 19“ Modular Fast/Gigabit and Full Gigabit Ethernet Switch Family

The rugged Hirschmann layer-2/3 substation (IEC 61850) switches for managed Fast-ETHERNET applications deliver excellent performance and high port density in a compact form factor.

The Layer 3 software makes it possible to use all the switches Hirschmann™ MACH1040 family also as routers.

Designed for extremely high demands with regard to shock and vibration resistance as well as electromagnetic compatibility (MACH1000)

- Switch ports
  - 4 x GE (up to) / 24 x FE (up to) flexible media configuration in dual port steps
- Design
  - flexible order system
- Supported media
  - Multimode, single-mode, long-haul, GE-SFP FE-SFP, PoE, 10BASE FL
- Connectors
  - ST, SC, LC, RJ45, MTRJ, M12
- Ports
  - front or on rear
  - Temperature range 0° up to +60°C; -40° up to +85°C
- Conformal coating - optional
  - Software OpenRail layer2/3 professional
- Power supply
  - - low 24/36/48VDC (18-60)V
  - - high 125/250VDC (80-320)V and 110/230VAC (85-264)V
  - - optional clamp, or connector each voltage combination is possible (L, H, LH, HH, LL)
- Housing - metal
- Approvals
  - Substation IEC61850-3, IEEE1613
  - KEMA (MACH1000)
  - Safety cUL508

13.5.2 RSR 20/30 DIN Rail mount Fast/Gigabit Ethernet Switches Family

The, manageable switches of the RSR family are offered in a Fast (RSR 20) and a Gigabit Ethernet version (RSR 30) are designed for extremely high demands with regard to shock and vibration resistance as well as electromagnetic compatibility (EMC).

- Switch ports
  - 3 x GE (up to) / up to 8 x FE from pure 8 TX up to 10 Port fiber
- Design
  - metal housing
  - DIN rail or wall mountable
- Uplink ports - configurable
- Supported media - Multimode, single-mode, long-haul, GE-SFP, FE-SFP
- Connectors ST, SC, LC, RJ45, MTRJ
- Temperature range 0° up to +60°C /-40° up to +85°C
- Conformal coating optional
- Highest reliability high MTBF, extreme EMC, shock and vibration immunity
- Software OpenRail layer2 professional
- Wide range power supply
  - low 24/36/48 VDC (16,8-60)V
  - high 60/120/250 VDC (48-320)V and 110/230 VAC (90-265)V
  - each voltage combination is possible (H, LH, HH, LL)*
  - power supply redundancy
- Fast device - ACA21-USB support replacement
- Approvals
  - Substation IEC61850-3, IEEE1613
  - KEMA (MACH1000 = same technology like RSR)
  - Safety cUL508

13.6 KETOP Lab

Company Profile

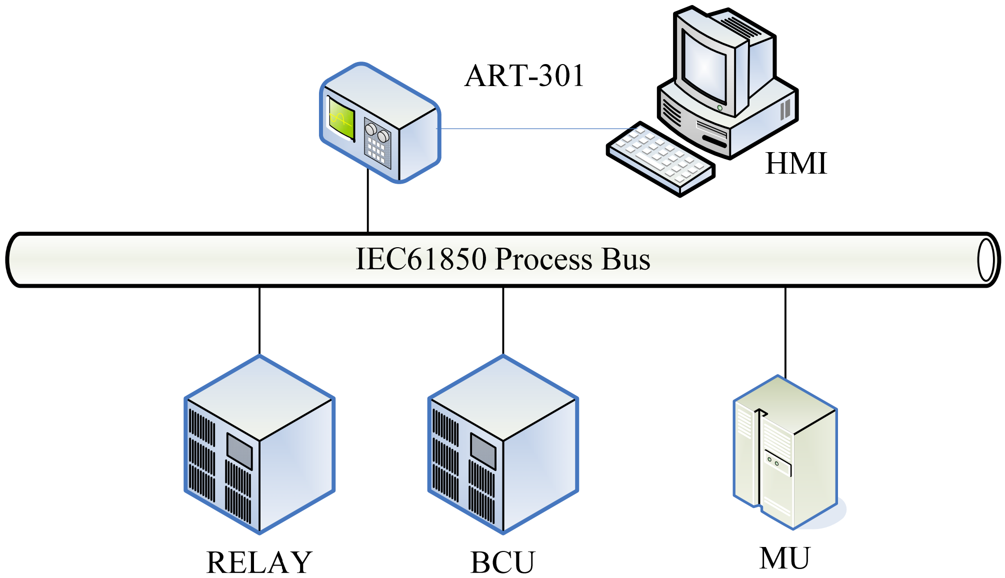
As a third party technical service organization, KETOP lab is located in Xuchang, Henan, China. It was also authorized as "National Testing Center for Relay Protection and Automation Equipment" by China State Bureau of Technical Supervision and CNCA (Certification and Accreditation Administration of P.R.China), undertaking the entrusted inspection test and quality supervision of power system relay protection and automation products.

Insisting on the international cooperation strategy, KETOP Lab signed collabration agreements with KEMA Netherlands in 2003, introducing the advanced protocol testing tools and technology firstly in China. In the same year, Protocol Research & Testing Center was established. Now we have the IEC60870-5（101/103/104 protocol）and IEC61850 test systems from KEMA, Modbus SIM and IEC60870-5-102 protocol professional test tools by independent R&D. On the basis of persistent research, we have set up testing platforms for WAMS(PMU), GPS Time Sych System、SAS/SCADA, Tele-Metering System, Fault Information System, Electric Load management System, Meters and Utility Software, and provided consulting and expertise training to many large utilities in China, e.g. Central China Grid and Southern Power Grid.

KETOP Protocol Research and Test Center has been actively taking part in the domestic and international standardization and expert groups, such as work groups of PMU test criteria, GPS standard, Modbus national standard, IEC61850 translation and draft groups of IEC/TC57, IEC/TC95, IEEE and CIGRE. Meanwhile, KETOP has developed many testing tools for the vendors and utilities, helping them to diagnose the products in R&D procedure and in operation.

13.6.1 ART-301 Product Description

ART-301 Smart Substation Process Level Analyzer can analyze the protocol information carried by IEC61850-9-2 and IEC61850-8-1 GOOSE telegram. Also it can report the encoding errors, protocol rule errors and application semantics errors.



Functional Overview:

- Sniffer the IEC61850 process level traffic in the Ethernet through switch
- Analyze the IEC61850-9-2 and GOOSE message in real time
- Store the message into TCP dump files
- Search the historical message data and show them by time scope

- Support Simultaneously 10 streams of 9-2LE traffic capturing
- Reminder of GOOSE data change
- Warning of encoding error of IEC61850 message
- Warning of stNum and sqNum error of GOOSE message
- Warning of SmpSynch, smpCnt, Quality's abnormal change in 9-2LE message
- 250 GB Flash Disk storage
- Windows XP Operating System

For more information, visit ***www.ketop.cn*** or

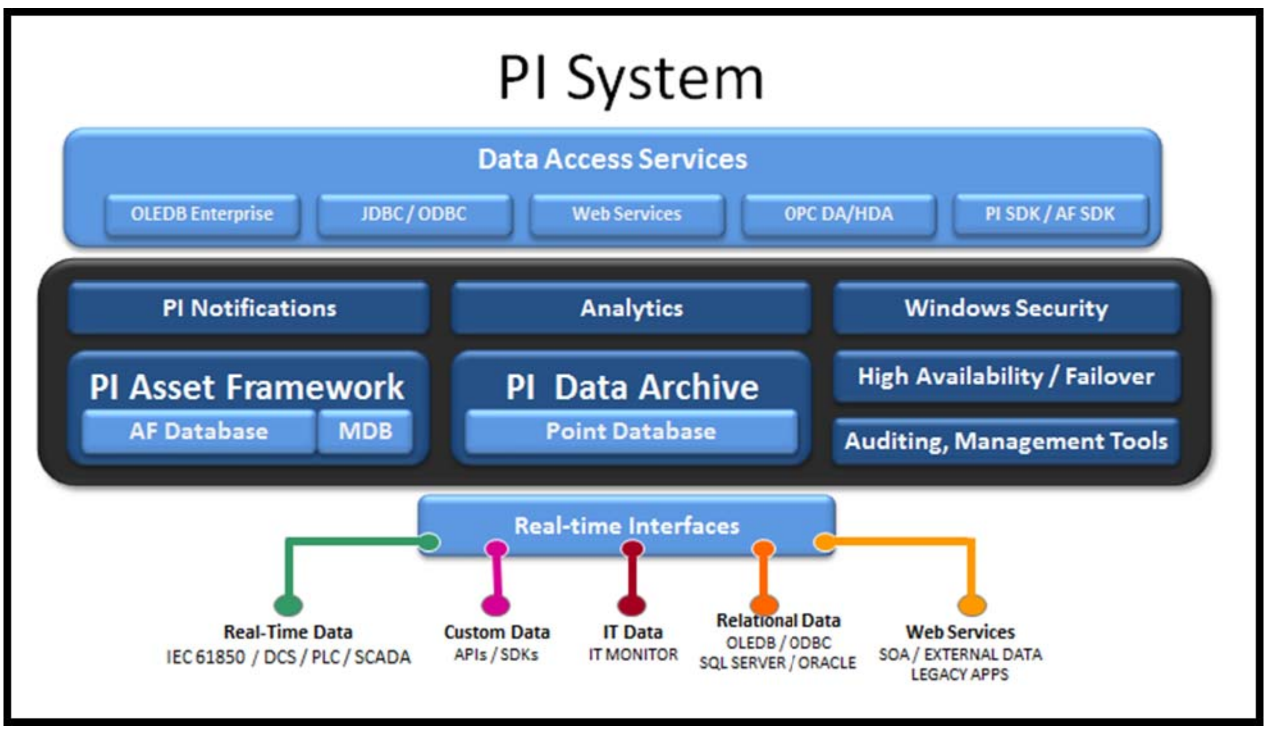
Call +86 374 3212841, Email: zhangran@ketop.cn

13.7 OSIsoft

13.7.1 PI System Overview and PI IEC 61850 Interface Overview

The PI Server is the real-time data collection, archiving, and distribution engine that powers the PI System. The PI Server brings all relevant data from disparate sources, such as enterprise systems, databases, and operational data sources into a single system, secures it so appropriate access is given to individuals based on their roles, and delivers it to users at all levels of the company in a uniform and consistent manner. The PI Server optimizes the data storage to use the least amount of disk space possible while still providing needed fidelity and allows retrieval of any data, no matter how old, quickly and accurately. As a result, users have a comprehensive, real-time view into operational, IT infrastructure, and business activities enabling them to make timely and profitable decisions.

The PI IEC 61850 Interface is a client application that can communicate to an IEC 61850 Server and send data to and from the PI System, via an embedded AXS4-61850 client from SISCO. The design of the interface allows running multiple instances of the interface simultaneously. Each instance of the interface is able to keep a connection to one IEC 61850 Server, which may be on the same or a different machine/node. More than one instance may be configured to connect to the same IEC 61850 Server. The interface may reside on a PI Interface node.



13.8 Prosoft Systems

13.8.1 MC ECA

13.8.1.1 Purpose

MC ECA (MKPA-2) is flex logic relay protection and emergency control automatic device for high and extra high voltage networks.

13.8.1.2 Main functions:

- MC ECA (MKPA-2) has been designed to control, protect and monitor optional elements of electrical network and realize next relay protection and automatic functions:
    - Out-of-step protection;
    - Frequency protection;
    - Over voltage protection;
    - Under voltage protection;
    - Extra high voltage reactor control automatic;
    - Overcurrent line protection and line power control automatic;
    - Line commutation control automatic;
    - Power transformer commutation control automatic;
    - Circuit-breaker failure protection;
    - Turn short circuit protection for transformer;
    - Voltage circuit control automatic;
    - Generator switch off automatic;
    - Short circuit power fall detection;
    - Any other protection or automatic function.

13.8.1.3 Features:

- Wide diapason ready project solutions;
- Several protection and automatic function on single device;
- Deep disturbance registration;
- Advanced self testing;
- Local and remote control (Device control panel and program for remote control);
- Advanced flex logic;
- Industrial design;
- SCADA support by OPC DA, IEC 608705-104, IEC 61850.

13.8.1.4 Technical Specifications

Input analog channels number	10
Analog channel sampling rate	2 kHz (40 sample/circle)
Input discrete channels number	6 ... 42
Output discrete channels number	6 ... 42
ADC capacity	16
Analog signal measuring accuracy	± 0.4 %
Maximum alternated current	1, 5, 10, 20 A
Maximum alternated voltage	100, 200, 500 V
Maximum constant current	±5, ±20, ±75, ±150 mA
Maximum constant voltage	±20, ±75, ±150 mV
Supply voltage	220 V (ac or dc)
Power consumption	< 70 W
Period of safety work (mean time between failures)	> 100000 hours
Device dimensions	482.6 x 422 x 132 mm
Weight	10 kg

13.8.1.5 Organization and principle of operation

MC ECA (MKPA-2) hardware is based on single processor x86-architecture in industrial execution. Each protection or emergency control automatic function realized as group of flex logic algorithms that placed in the device. Algorithms use the data that was calculated by analog and discrete acquired values. Any algorithm detecting power network emergency state cause MC ECA (MKPA-2) trip and start disturbance recorder. Remained after MC ECA (MKPA-2) trip record save with its time stamp in nonvolatile storage. Information about trip puts to MC ECA (MKPA-2) run-time journal. Alarm signal about MC ECA (MKPA-2) trip sends to remote control program SignW.

13.8.1.6 Software

MC ECA (MKPA-2) software consist of controller software that work on device, remote control program SignW that set on personal desktop and flax logic software development kid SoftConstructor.

SignW program permit do following operations: remote configuration of MC ECA (MKPA-2), saved disturbance analyze, view currently measured signals of MC ECA (MKPA-2).

SoftConstructor SDK is design for flex logic algorithms creation, editing and checkout. SoftConstructor based of FBD (Function Block Diagram) language and conform to IEC 61131-3.

It was overworked software modules that permit interconnection MC ECA (MKPA-2) and SCADA system by one of following protocols: OPC DA, IEC 60870-5-104, and IEC 61850. For time synchronization with SCADA system MC ECA (MKPA-2) use ICMP and NTP protocols.

13.9 RTDS

13.9.1 Testing with IEC 61850

The RTDS Simulator is a real time power system simulator widely used for closed-loop testing of physical protection and control equipment. For over 15 years now conventional protection equipment has been tested by driving power amplifiers (voltage and/or current) from the simulator’s analogue output channels and by reading back the status of contacts for trip, reclose and other miscellaneous elements. Since the simulator operates in true real time, the protection equipment and the response of the simulated network are just as they would be in the real system. For example if a fault simulated in the network results in a trip being issued by the protection, a breaker in the simulated network will be opened and the subsequent voltages and currents affected correspondingly. The closed-loop response of the real time simulator also allows multiple relays to be connected simultaneously so their interaction can be evaluated.

To address the testing of IEC 61850 compliant protection equipment, RTDS Technologies has developed the GTNET card. Depending on the active protocol, the GTNET card can provide IEC 61850 GOOSE or GSSE messaging or IEC 61850-9-2 sampled values for voltage and current.

13.9.2 GTNET – (Giga-Transceiver Network communication card)

The GTNET card occupies a single slot of an RTDS Simulator rack and draws power from the backplane. The card transmits and receives signals from a GPC processor through one of the GT ports on the rear of the processor card. Other GT-I/O cards can be connected in daisy chain to the GTNET and serviced through the same GPC GT port.

The Ethernet connection to the GTNET is provided by a 100Base-TX RJ45 port, or optionally by a 100Base-FX port with ST connectors located on the rear of the unit.

The GTNET is equipped a BNC coax that can accept or provide a 1PPS timing signal for IEC 61850-9-2 synchronization. It also has two ST optical connectors, one for receiving and one for transmitting a 1PPS signal optically.

13.9.3 GTNET – GSE for IEC 61850 GOOSE Messaging

The GSE firmware option for the GTNET allows a maximum of 64 binary input and 64 binary output signals to be exchanged between the RTDS Simulator and up to eight IEC 61850 compliant IED's. Both GSSE (UCA GOOSE) and GOOSE formatted messaging are supported, but cannot be provided simultaneously from one GTNET. The GTNET GOOSE configuration is done via an SCD file, configured with any SCL editor.

In addition to the binary messages, the GTNET-GSE IEC GOOSE can provide 8 analogue input and 8 analogue output signals. IEC GOOSE fields such as the Test mode, Needs Commissioning and individual Quality bitmaps can be dynamically changed and monitored during a simulation to allow many scenarios to be thoroughly tested and verified.

13.9.4 GTNET – SV for IEC 61850-9-2 Sampled Value Messaging

The SV firmware option provides IEC 61850-9-2 sampled value messaging for power system voltages and currents. In order to timestamp the sampled values, a one pulse per second (1PPS) signal can be input to the GTNET via a BNC or ST optical connections. Alternatively, the GTNET can provide a master 1PPS signal to the IED(s) being tested.

One GTNET card can provide sampled values for a maximum of eight signals (4 x V and 4 x I) simultaneously. The sampled values are sent out from the GTNET at a rate of 80 samples per 50 or 60 Hz cycle.

13.9.5 Interoperability

The GTNET-GSE and GTNET–SV options have been successfully tested with products from a number of different vendors. RTDS Technologies has also demonstrated closed-loop testing that included IEC 61850 GOOSE messaging and sampled value with multiple vendor products interoperating.

13.10 RuggedCom

13.10.1 RuggedSwitch® RSG2100

19 Port Modular Managed Ethernet Switch with Gigabit Uplinks

Product Description

The RuggedSwitch® RSG2100 is an industrially hardened, fully managed, modular, Ethernet switch specifically designed to operate reliably in electrically harsh and climatically demanding utility substation and industrial environments.

The RSG2100's superior rugged hardware design coupled with the embedded Rugged Operating System (ROS®) provides improved system reliability, advanced cyber security and networking features making it ideally suited for creating secure Ethernet networks for mission-critical, real-time, control applications.

The RSG2100's modular flexibility offers 10BaseFL /100BaseFX /1000BaseX fiber and 10/100/1000BaseTX copper port combinations. Optional front or rear mount connectors make the RSG2100 highly versatile for any application and can support multiple fiber connectors (ST, MTRJ, LC, SC) without loss of port density. The RSG2100 is packaged in a rugged galvanized steel enclosure with industrial grade DIN, panel, or 19" rack mount options.

Key Features and Benefits

- Maximize productivity with utility grade reliability
- Cyber attack prevention via advanced security
- Filed proven MTBF delivers low OPEX costs
- Common Features Description
- Meets / Exceeds IEC / IEEE / NEMA Industry Standards
- RuggedRated™ for reliability in harsh environments
- Flexibility with different fiber port options available
- Long haul fiber support

- Up to 19 Ports: 3 1000BaseX (Gigabit) + 16 10/100BaseX
- Power over Ethernet (PoE) version available
- EN50121-4 (Railway Applications)
- High immunity to EMI and heavy electrical surges
- -40ºC to +85ºC operating temperature
- Hazardous location certification: Class 1 Div 2
- Fully integrated power supply
- Universal high-voltage range: 88-300VDC or 85-264VAC
- Dual low-voltage DC inputs: 24VDC or 48VDC

13.10.2 RuggedSwitch® RSG2200

9 Port Managed Gigabit Ethernet Switch

Product Description

The RuggedSwitch® RSG2200 is an industrially hardened, fully managed, modular Gigabit Ethernet switch specifically designed to operate reliably in electrically harsh and climatically demanding utility substation and industrial environments.

The RSG2200's superior rugged hardware design coupled with the embedded Rugged Operating System (ROS®) provides improved system reliability, advanced cyber security and networking features making it ideal for creating mission-critical, Gigabit networks or aggregating switches into a Gigabit backbone.

The RSG2200's modular flexibility offers 1000BaseX fiber and 10/100/1000BaseTX copper port combinations. Support for front or rear mount connectors coupled with multiple fiber connector types (SFP, GBIC, LC, SC) without loss of port density makes the RSG2200 highly versatile and suitable for any application. The RSG2200 is packaged in a rugged galvanized steel enclosure with industrial grade DIN, panel, or 19" rack mount options.

Key Features and Benefits

- Maximize productivity with utility grade reliability
- Cyber attack prevention via advanced security
- Filed proven MTBF delivers low OPEX costs
- Common Features Description
- Meets / Exceeds IEC / IEEE / NEMA Industry Standards
- RuggedRated™ for reliability in harsh environments
- Flexibility with different fiber port options available
- Long haul fiber support
- Up to 9-Gigabit Ethernet ports - copper and/or fiber
- Up to 9 100FX Fiber Fast Ethernet ports
- 2 port modules for tremendous flexibility
- High immunity to EMI and heavy electrical surges
- -40ºC to +85ºC operating temperature
- Hazardous location certification: Class 1 Div 2
- Fully integrated power supply
- Universal high-voltage range: 88-300VDC or 85-264VAC
- Dual low-voltage DC inputs: 24VDC or 48VDC

13.10.3 RuggedSwitch® RSG2288

9 Port Gigabit Ethernet Switch with IEEE 1588v2 and IRIG-B Conversion

Product Description

The RuggedSwitch® RSG2288 is an industrially hardened, fully managed, modular Gigabit Ethernet switch specifically designed to operate reliably in electrically harsh and climatically demanding utility substation and industrial environments.

The RSG2288 features the IEEE 1588 v2 protocol with hardware time stamping allowing high precision time synchronization over the Ethernet network and conversion to IRIG-B for non-1588 devices. The RSG2288's superior rugged hardware design coupled with the embedded Rugged Operating System (ROS®) provides improved system reliability, and advanced cyber security and networking features making it ideal for creating mission-critical, Gigabit networks or aggregating switches into a Gigabit backbone.

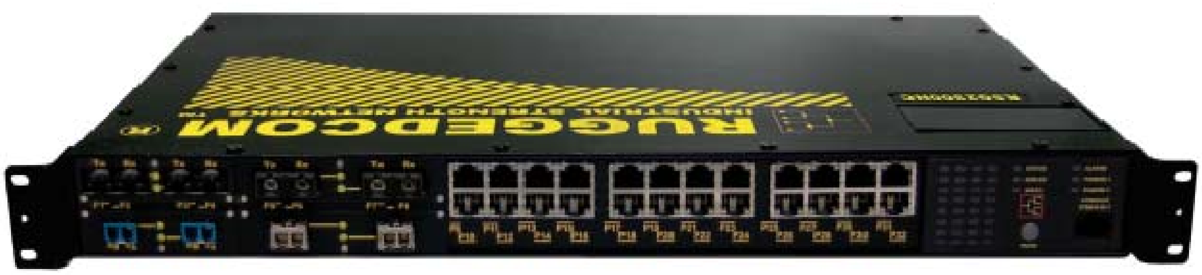
The RSG2288's modular flexibility offers 100FX or 1000BaseX fiber and 10/100/1000BaseTX copper port combinations. Support for front or rear mount connectors coupled with support for multiple fiber connector types (SFP, GBIC, LC, SC) without loss of port density makes the RSG2288 highly versatile and suitable for any application. The RSG2288 is packaged in a rugged galvanized steel enclosure with industrial grade DIN, panel, or 19" rackmount mounting options.

Key Features and Benefits

- Maximize productivity with utility grade reliability
- Cyber attack prevention via advanced security
- Filed proven MTBF delivers low OPEX costs
- Common Features Description
- Meets / Exceeds IEC / IEEE / NEMA Industry Standards
- RuggedRated™ for reliability in harsh environments
- Flexibility with different fiber port options available
- Long haul fiber support
- Up to 9 Ports: 1000BaseX (Gigabit) or up to 9 100FX (Fast Ethernet)
- IEEE 1588 v2 with hardware time stamping on all ports
- IEEE 1588 v2 to IRIG-B conversion
- Transparent clock operation for high precision on switched networks (better than 1µs accuracy, typically 100ns)
- High immunity to EMI and heavy electrical surges
- -40ºC to +85ºC operating temperature
- Hazardous location certification: Class 1 Div 2
- Fully integrated power supply
- Universal high-voltage range: 88-300VDC or 85-264VAC
- Dual low-voltage DC inputs: 24VDC or 48VDC

13.10.4 RuggedSwitch® RSG2300

32 Port Managed Ethernet Switch with Modular Gigabit Uplink Ports



Product Description

The RuggedSwitch® RSG2300 is an industrially hardened, fully managed, modular, Ethernet switch specifically designed to operate reliably in electrically harsh and climatically demanding utility substation and industrial environments.

The RSG2300's superior rugged hardware design coupled with the embedded Rugged Operating System (ROS®) provides improved system reliability, advanced cyber security and networking features making it ideally suited for creating secure Ethernet networks for mission-critical, real-time, control applications.

The RSG2300's modular flexibility offers 10BaseFL /100BaseFX /1000BaseX fiber and 10/100/1000BaseTX copper port combinations. Optional front or rear mount connectors make the RSG2300 highly versatile for any application and can support multiple fiber connectors (ST, MTRJ, LC, SC) without loss of port density. The RSG2300 is packaged in a rugged galvanized steel enclosure with industrial grade DIN, panel, or 19" rack-mount options.

Key Features and Benefits

- Maximize productivity with utility grade reliability
- Cyber attack prevention via advanced security
- Filed proven MTBF delivers low OPEX costs
- Common Features Description
- Meets / Exceeds IEC / IEEE / NEMA Industry Standards
- RuggedRatedTM for reliability in harsh environments
- Flexibility with different fiber port options available
- Long haul fiber support

- Up to 32 Ports: 24 10/100BaseTX and optional 4 1000BaseX (Gigabit) or 8 100BaseX
- Power over Ethernet (PoE) version available
- High immunity to EMI and heavy electrical surges
- -40ºC to +85ºC operating temperature
- Hazardous location certification: Class 1 Div 2
- Fully integrated power supply
- Universal high-voltage range: 88-300VDC or 85-264VAC
- Dual low-voltage DC inputs: 24VDC or 48VDC

13.10.5 RuggedSwitch® RS900G

10 Port Managed Ethernet Switch with Gigabit Uplinks

Product Description

The RuggedSwitch® RS900G is an industrially hardened, fully managed Ethernet switch providing dual fiber optical Gigabit Ethernet ports and eight Fast Ethernet copper ports.

Designed to operate reliably in harsh industrial environments the RS900G provides a high level of immunity to electromagnetic interference and heavy electrical surges typical of environments found in electric utility substations, factory floors or in curb side traffic control cabinets. An operating temperature range of -40°C to +85°C coupled with hazardous location certification, optional conformal coating and a galvanized steel enclosure allows the RS900G to be placed in almost any location.

The versatility and wide selection of fiber optics allows the RS900G to be used in a variety of applications. The RS900G provides two fiber optical Gigabit Ethernet ports for creating a fiber optical backbone with high noise immunity and long haul connectivity.

Key Features and Benefits

- Maximize productivity with utility grade reliability
- Cyber attack prevention via advanced security
- Filed proven MTBF delivers low OPEX costs
- Common Features Description
- Meets / Exceeds IEC / IEEE / NEMA Industry Standards
- RuggedRated™ for reliability in harsh environments
- Flexibility with different fiber port options available
- Long haul fiber support
- 10 Ports: 8 10/100BaseTX and +2 1000BaseX (Gigabit)
- EN50121-4 (Railway Applications)
- High immunity to EMI and heavy electrical surges
- -40ºC to +85ºC operating temperature
- Hazardous location certification: Class 1 Div 2
- Fully integrated power supply
- Universal high-voltage range: 88-300VDC or 85-264VAC
- Dual low-voltage DC inputs: 24VDC or 48VDC

13.11 Schneider Electric

13.11.1 Application and Scope

MiCOM P139 is a cost-effective one-box solution for integrated numerical time-overcurrent protection and control. The units protection functions provide selective short-circuit, ground fault and overload protection in medium and high voltage systems.

The systems can be operated as solidly, low-impedance, resonant grounded or isolated. The offered protection functions enable the user to cover a wide range of applications in the protection of cable and lines, transformers and motors.

Four parameter subsets allow easy adaptation to changing system operation conditions.

The maximum configuration of binary inputs and outputs provide the signaling of 10 switchgear units whereas 6 of them are controllable.

The MiCOM P139 is provided with over 250 predefined bay types and allows download of customized bay types.

Primary and secondary devices are monitored and controlled using binary inputs and power outputs that are independent of auxiliary voltages, by the direct connection option for current and voltage transformers and by the comprehensive interlocking capability.

This simplifies the handling of the protection and control technology for HV or MV bays from planning to bringing into service.

MiCOM P139 provides an extensive number of protection and control functions. By means of a straight-forward configuration procedure, the user can flexibly adapt the device to the scope of protection required in each particular application. Due to the powerful freely configurable logic of the device, special applications can be adapted.

Following global functions are available in the MiCOM P139:

- Parameter subset selection (4 subsets)
- Measured operating data to support the user during commissioning, testing and operation
- Operating data recording (time-tagged signal)
- Overload data acquisition
- Overload recording (time-tagged signal))
- Ground fault data acquisition
- Ground fault recording (time-tagged signal)
- Measured fault data
- Fault data acquisition
- Fault recording (time-tagged signal)

The MiCOM P139 is of modular design. The pluggable modules are housed in a robust aluminum case and electrically connected via an analogue and a digital bus printed circuit board.

The nominal currents or the nominal voltages respectively of the measuring inputs can be set with the help of parameters.

For comprehensive local operation, the device is equipped with a local control panel, which is also available as detachable HMI (option)

- Graphic LC-display
- 17 LED indicators
- PC interface

13.11.2 Information interface

Information exchange is done via the local control panel, the PC interface and 2 optional communication interfaces.

The first communication interface has settable protocols conforming to IEC 60870-5-103, IEC 60870-5-101, DNP 3.0, Modbus and Courier (COMM1) or provides alternatively protocol conforming to IEC 61850 (IEC), intended for integration Sample EPRI Technical Reportinto substation control systems.

The 2nd communication interface (COMM2) conforms to IEC 60870-5-103 and is intended for remote setting access only.

Additionally, the optional InterMiCOM interface (COMM 3) allows a direct transfer of any digital status information between two devices.

Clock synchronization can be achieved using one of the protocols or using the IRIG-B signal input.

13.11.3 Functional Overview

Functional overview				P139	
ANSI	**IEC 61850**	**Function group**	**Function**	**VT´s not fitted**	**VT´s fitted**
50 P/Q/N	DtpPhs-/DtpEft-/ DtpNgsPTCOx	DTOC	Definite-time o/c protection, four stages, phase-selective	●	●
51 P/Q/N	ItpPhs-/ItpEft-/ ItpNgsPTCOx	IDMT1/ IDMT2	Inverse-time o/c protection, single-stage, phase-selective	●	●
67	DtpPhs-/ DtpResRDIRx	SCDD	Short circuit direction detection		●
50/27	PSOF1	SOTF	Switch onto fault protection	●	●
85	PSCH1	PSIG	Protective signaling	●	●
79	RREC1	ARC	Auto-reclosure control (3-pole)	●	●
25	RSYN1	ASC	Automatic synchronism check		(●)
67W/YN	PSDE1	GFDSS	Ground fault direction determination (wattmetric)		●
	PTEF1	TGFD	Transient ground fault direction dtermination		(●)
37/48/49/ 49LR/50S/66	MotPMRI1/ MotPMSS1/ MotPTTR1/ ZMOT1	MP	Motorprotection	●	●
49	ThmPTTR1	THERM	Thermal overload protection	●	●
			Coolant temperature measuring (using MEASI)	(●)	(●)
46	UbpNgsPTOCx	I2>	Unbalance protection	●	●
27/59/47 P/Q/N	VtpPhs-/VtpNgs-/ VtpPss-/VtpRefPTyVx	U<>	Over/Undervoltage protection		●
81	FrqPTyFx	f<>	Over- / Underfrequenceprotection		●
32/37	PdpAct-/ PdpRealPDyPx	P<>	Directional power protection		●
50/62BF	RBRFx	CBF	Circuit breaker failure protection	●	●
	XCBR1	CBM	Circuit breaker monitoring	●	●
30/74	AlmGGIO1	MCMON	Measuring circuit monitoring	●	●
		LIMIT	Limit value monitoring	●	●
	PHAR1	MAIN	Inrushstabilizing	●	●
LGC	PloGGIOx	LOGIC	Programmable logic	●	●
	LLN0.SGCB	PSS	Parameter subset selection	●	●
	Mmuxxx		Measuring	●	●
			Analog inputs and outputs	(●)	(●)
26	RtdGGIO1	MEASI	RTD input	(●)	(●)
	IdcGGIO1		Measuring data input 20 mA, one settable input value	(●)	(●)
		MEASO	Measuring data output 20 mA, two settable output values	(●)	(●)
	PTRCx/ RDRE1	FT_RC	Fault recording	●	●
52	XCBRx, XSWIx, CSWIx	BM	Control and monitoring of up to 6 switchgear units	(●)	(●)
	CtlGGIO2	BEF_1	Single-pole commands	(●)	(●)
	CtlGGIO1	MEL_1	Single-pole signals	(●)	(●)
LGC		V_LOG	Interlocking logic	(●)	(●)
	CntGGIO1	ZW	Binary Counter	●	●
16S		KOMMx	2 Communication interfaces serial, RS 422/485 or FO	(●)	(●)
CLK		IRIGB	Time synchronisation IRIG-B	(●)	(●)
16E		IEC	Communication interface Ethenet	(●)	(●)
16E	GosGGIOx	GOOSE	IEC 61850	(●)	(●)

● = STANDARD; (●) = ORDER OPTION

13.12 Schweitzer Engineering Laboratories

13.12.1 SEL-2440 Discrete Programmable Automation Controller

13.12.1.1 Major Features and Benefits

13.12.1.1.1 Fast and Powerful I/O

- Utilize an exceptional and compact combination of inputs, outputs, and communications.
- Analyze system events with inputs and other events timed to the microsecond.
- Synchronize control with outputs that are synchronized to IRIG-B time.
- Perform actions quickly with a processing interval of 2 ms and an input to output interval of 7 ms.
- Program new features with logic, latches, timers, counters, edge-triggers, and math functions.
- Ensure safe operation by using an input with logic programmed for local/remote control.

13.12.1.1.2 Convenient Maintenance and Support

- LEDs provide status for every I/O point and communications port.
- Removable terminal blocks make installation and replacement quick and efficient.
- Positive retention connectors ensure that connections are not lost due to sagging cables.
- Front-panel management port makes device management convenient.

13.12.1.1.3 Flexible Communications and Integration

- Communicate with DNP3, Modbus®, and IEC 61850 protocols over Ethernet and serial connections. Direct and select-before-operate (SBO) outputs are supported.
- Automate systems with flexible communication options that provide easy integration with SCADA.
- Configure easily with preprogrammed register or object maps and front-panel DIP switches.
- Alternatively, configure with acSELerator QuickSet® SEL-5030 Software.
- SEL Quality, Standards, and Global Support
- Designed and tested for harsh physical and electrical environments.
- Designed and tested to operate with dc grounded batteries and capacitive loads, and to trip breakers and interrupt inductive loads.
- Superior specification compliance, high reliability, low price, and worldwide, ten-year warranty.

13.12.1.2 Automation Features

13.12.1.2.1 Flexible Control Logic and Integration Features

The DPAC does not require special communications software. Use any system that emulates a standard terminal system for engineering access to the device.

13.12.1.2.2 Simplifies Communications

The SEL-2440 is equipped with three independently operated serial ports. Establish communication by connecting computers, modems, protocol converters, printers, an SEL Communications Processor, SCADA serial port, and an RTU for local or remote communication. Apply an SEL communications processor as the hub of a star network, with point-to-point fiber or copper connection between the hub and the SEL-2440.

13.12.1.2.3 Supports Standard Protocols

As with most SEL devices, the DPAC comes standard with the communications protocols listed below.

- IEC 61850 DNP3
- DNP3
- Modbus
- SEL ASCII, Compressed ASCII
- SEL Fast Messaging
- SEL Mirrored Bits

13.12.1.2.4 Simplifies SCADA

SEL devices provide proprietary but open, binary “fast” protocols. These protocols are self-describing and are interleaved with ASCII protocols on the same port. Simplify configuration, minimize communications wiring, and improve performance between the DPAC and other devices (e.g., communications processors) with these protocols.

13.12.1.2.5 Performs Logic and Math

Eliminate PLCs with Boolean logic, rising/falling edge triggers, and math (+, -, *, /).

13.12.1.2.6 Replaces Traditional Latching Relays

Replace as many as 32 traditional latching relays for such functions as “remote control enable” with latches. Program latch set and latch reset conditions with SELogic® control equations. Set or reset the nonvolatile latches using optoisolated inputs, Remote Bits, latches, or any programmable logic condition. The latches retain their state when the device loses power.

13.12.1.2.7 Eliminates External Timers

Eliminate external timers for custom protection or control schemes with 32 general purpose SELOGIC control equation timers. Each timer has independent time-delay pickup and dropout settings. Program each timer input with any desired element. Assign the timer output to trip logic, transfer trip communications, or other control scheme logic.

13.12.1.2.8 Eliminates External Counters

Eliminate external counters for custom control schemes with 32 counters, updated every 2 ms processing interval. Each counter element consists of five inputs (preset value; load preset value, count up, count down, and reset to zero) and three outputs (counter value; count as many as preset reached, count down to zero reached).

13.12.1.2.9 Eliminates RTU-to-Device Wiring

Eliminate RTU-to-Device wiring with 32 Remote Bits. Set, clear, or pulse Remote Bits using serial or Ethernet port commands. Program the Remote Bits into your control scheme with SELOGIC control equations. Use Remote Bits for SCADA-type control operations such as trip, close, and settings group selection.

13.12.1.2.10 Provides Annunciation

Indicators (LEDs) provide annunciation of I/O status for each input and output. In addition, device status and port activity indicators simplify commissioning and troubleshooting.

13.12.2 SEL-421 Protection and Automation System

13.12.2.1 Major Features and Benefits

The SEL-421 Protection, Automation, and Control System combines high-speed distance and directional protection with complete control for a two-breaker bay.

- **Protection.** Protect any transmission line using a combination of five zones of phase- and ground-distance and directional overcurrent elements. Select Mho or Quadrilateral characteristics for any phase or ground distance element. Use the optional high-speed elements and series compensation logic to optimize protection for critical lines or series-compensated lines. Use the ACSELERATOR QuickSet® SEL-5030 Software (a graphical user interface) to speed and simplify setting the relay. Patented Coupling Capacitor Voltage Transformer (CCVT) transient overreach logic enhances the security of Zone 1 distance elements. Best Choice Ground Directional Element™ logic optimizes directional element performance and eliminates the need for many directional settings.
- **Automation.** Take advantage of enhanced automation features that include 32 programmable elements for local control, remote control, protection latching, and automation latching. Local metering on the large format front-panel Liquid Crystal Display (LCD) eliminates the need for separate panel meters. Use serial and Ethernet links to efficiently transmit key information, including metering data, protection element and control I/O status, IEEE C37.118 Synchrophasors, IEC 61850 GOOSE messages, Sequential Events Recorder (SER) reports, breaker monitor, relay summary event reports, and time synchronization. Use expanded SELOGIC® control equations with math and comparison functions in control applications. High-isolation control input circuits feature settable assertion levels for easy combinations of elements from other systems. Incorporate up to 1000 lines of automation logic (depending on the model) to speed and improve control actions.
- **Synchrophasors.** Make informed load dispatch decisions based on actual real-time phasor measurements from SEL-421 relays across your power system. Record streaming synchrophasor data from SEL-421 relays system-wide disturbance recording. Control the power system using local and remote synchrophasor data.

- **Digital Relay-to-Relay Communications.** Use MIRRORED BITS® communications to monitor internal element conditions between relays within a station, or between stations, using SEL Fiber-Optic Transceivers. Send digital, analog, and virtual terminal data over the same MIRRORED BITS channel. Receive synchrophasor data from as many as two other devices transmitting IEEE C37.118-2005 format synchrophasors at rates up to 60 messages per second. The SEL-421 time correlates the data for use in SELOGIC control equations.
- **Primary Potential Redundancy.** Multiple voltage inputs to the SEL-421 provide primary input redundancy. Upon loss-of-potential (LOP) detection, the relay can use inputs from an electrically equivalent source connected to the relay. Protection remains in service without compromising security.
- **Ethernet Access.** Access all relay functions with the optional Ethernet card. Interconnect with automation systems using IEC 61850 or DNP3 protocol directly. Optionally connect to DNP3 networks through a communications processor. Use file transfer protocol (FTP) for high-speed data collection. Connect to substation or corporate LANs to transmit synchrophasors in the IEEE C37.118-2005 format using TCP or UDP internet protocols.
- **Dual CT Input.** Combine currents within the relay from two sets of CTs for protection functions, but keep them separately available for monitoring and station integration applications.
- **Monitoring.** Schedule breaker maintenance when accumulated breaker duty (independently monitored for each pole of two circuit breakers) indicates possible excess contact wear. Electrical and mechanical operating times are recorded for both the last operation and the average of operations since function reset. Alarm contacts provide notification of substation battery voltage problems (two independent battery monitors) even if voltage is low only during trip or close operations.
- **Reclosing Control.** Incorporate programmable single-pole or three-pole trip and reclose of one or two breakers into an integrated substation control system. Synchronism and voltage checks from multiple sources provide complete bay control.
- **Breaker Failure.** Use high-speed (5/8 cycle) open-pole detection logic to reduce coordination times for critical breaker failure applications. Apply the SEL-421 to supply single and/or three-pole breaker failure for one or two breakers. Necessary logic for single-pole and three-pole breaker failure retrip and initiation of transfer tripping is included. Logic to use different delay settings for multiphase and single phase is included.
- **Out-of-Step Blocking and Tripping.** Select out-of-step blocking of distance elements or tripping on unstable power swings. Out-of-step detection does not require settings or system studies.
- **Switch-Onto-Fault and Stub Bus Protection.** Use disconnect status inputs and voltage elements to enable high-speed protection.
- **Fault Locator.** Efficiently dispatch line crews to quickly isolate line problems and restore service faster.
- **Oscillography.** Record voltages, currents, and internal logic points at up to 8 kHz sampling rate. Phasor and harmonic analysis features allow investigation of relay and system performance.
- **Rules-Based Settings Editor.** In addition to communicating and setting the relay using an ASCII terminal, use the PC-based ACSELERATOR QuickSet to configure the

SEL-421 and analyze fault records with relay element response. View real-time phasors and harmonic levels.

- **Sequential Events Recorder (SER).** Record the last 1000 entries, including setting changes, power-ups, and selectable logic elements.
- **Thermal Overload Modeling.** Use the SEL-421 with the SEL-2600 Series RTD Module for dynamic overload protection using SELOGIC control equations.
- **Comprehensive Metering.** Improve feeder loading by using built-in, high-accuracy metering functions. Use watt and VAR measurements to optimize feeder operation. Minimize equipment needs with full metering capabilities, including: rms, maximum/minimum, demand/peak, energy, and instantaneous values.
- **Auxiliary Trip/Close Pushbuttons.** These optional pushbuttons are electrically isolated from the rest of the relay. They function independently from the relay and do not need relay power.

13.12.2.2 Protection Features

The SEL-421 contains all the necessary protective elements and control logic to protect overhead transmission lines and underground cables. The relay simultaneously measures five zones of phase and ground mho distance plus five zones of phase and ground quadrilateral distance. These distance elements, together with optional high-speed directional and faulted phase selection and high-speed distance elements, are applied in communications-assisted and step-distance protection schemes. You can further tailor the relay to your particular application using expanded SELOGIC control equations. As transmission systems are pushed to operational limits by both competitive and regulatory pressures, line protection must be able to adapt to changing conditions. The SEL-421 is easy to set and use for typical lines, while the high-speed and logic settings make it applicable for critical and hard-to-protect lines.

13.12.2.3 Functional Overview: System

The SEL-421 is a complete stand-alone protection, automation, and control device. It can also act as an integral part of a full station protection, control, and monitoring system. Each relay can be tied to a communications processor that integrates the individual unit protections for overall protection integration.

Backup protection such as the SEL-321 Relay or SEL-311 Relay can also be connected to an SEL communications processor. The SEL-421 has four serial ports that can be used for connection to a communications processor, ASCII terminal, fiber-optic transceiver, or PC.

13.12.2.4 Network Connection and Integration

Connect the SEL-421 to Local Area Networks (LANs) using the optional Ethernet card. The Ethernet card also allows connection of an SEL communications processor to a single or dual LAN. The integrated Ethernet card supports both copper and/or fiber connections with fail-over protection.

13.12.2.5 Ethernet Card

The optional Ethernet card mounts directly in the SEL-421. Use popular Telnet applications for easy terminal communications with SEL relays and other devices. Transfer data at high speeds (10 Mbps or 100 Mbps) for fast HMI updates and file uploads. The Ethernet card communicates using File Transfer Protocol (FTP) applications for easy and fast file transfers.

Provide Operations with situational awareness of the power system using IEEE C37.118-2005 Standard for Synchrophasors for Power Systems. Communicate with SCADA and other substation IEDs using DNP3 or IEC 61850 Logical Nodes and GOOSE messaging.

Choose Ethernet connection media options for primary and stand-by connections:

- 10/100BASE-T twisted pair Network
- 100BASE FX Fiber-Optic Network

13.12.2.6 Telnet and FTP

Order the SEL-421 with Ethernet communications and use the built-in Telnet and FTP (File Transfer Protocol) that come standard with Ethernet to enhance real communication sessions. Use Telnet to access relay settings, and metering and event reports remotely using the ASCII interface. Transfer settings files to and from the relay via the high-speed Ethernet port using FTP.

13.12.2.7 IEEE C37.118 Synchrophasors

The latest IEEE synchrophasor protocol provides a standard method for communicating synchronized phasor measurement data over Ethernet or serial media. The integrated Ethernet card in the SEL-421 provides two independent connections using either TCP/IP, UDP/IP, or a combination thereof. Each connection supports unicast data for serving data to a single client. The connections also receive data for control applications. Each data stream can support up to 60 frames per second.

13.12.2.8 DNP3 LAN/WAN

The DNP3 LAN/WAN option provides the SEL-421 with DNP3 Level 2 slave functionality over Ethernet. Custom DNP3 data maps can be configured for use with specific DNP3 masters.

13.12.2.9 IEC 61850 Ethernet Communications

IEC 61850 Ethernet-based communications provide interoperability between intelligent devices within the substation. Logical nodes using IEC 61850 allow standardized interconnection of intelligent devices from different manufacturers for monitoring and control of the substation. Reduce wiring between various manufacturers' devices and simplify operating logic with IEC

61850. Eliminate system RTUs by streaming monitoring and control information from the intelligent devices directly to remote SCADA client devices.

The SEL-421 can be ordered with embedded IEC 61850 protocol operating on 100 Mbps Ethernet. Use the IEC 61850 Ethernet protocol for relay monitoring and control functions, including the following.

- As many as 24 incoming GOOSE messages. The incoming GOOSE messages can be used to control up to 128 control bits in the relay with < 3 ms latency from device to device. These messages provide binary control inputs to the relay for high-speed control functions and monitoring.
- As many as 8 outgoing GOOSE messages. Outgoing GOOSE messages can be configured for Boolean or analog data. Boolean data is provided with < 3 ms latency from device to device. Use outgoing GOOSE messages for high-speed control and monitoring of external breakers, switches, and other devices.
- IEC 61850 Data Server. The SEL-421 equipped with embedded IEC 61850 Ethernet protocol, provides data according to predefined logical node objects. As many as six simultaneous client associations are supported by each relay. Relevant Relay Word bits are available within the logical node data, so status of relay elements, inputs, outputs, or SELOGIC equations can be monitored using the IEC 61850 data server provided in the relay.
- IEC 61850 Sampled Values. SEL-421-SV supports IEC 61850-9-2 compliant Sampled Value transmission and reception of multiple 61850-9-2LE compliant streams (4 Voltages + 4 currents with neutral measurements unused / set to zero). The IEC 61850-9-2 9-2 messages received by the relay must comply with the *UCA Users group "Implementation Guideline for Digital interface to Instrument Transformers Using IEC 61850-9-2", Rev. 3.0*, Multicast value sample control block #1 (MSVCB01) with 80 samples/cycle, 50 or 60Hz nominal frequency (4000 or 4800 samples/second). When operated with IRIG-B synchronization signal, SEL-421-SV merging unit requires that the IRIG-B signal contain the C37.118 time quality extension bits, and that the time indicated by those bits shows "high accuracy IRIG".

Use the acSELerator QuickSet Architect SEL-5032 software to manage the logical node data for all IEC 68150 devices on the network. This Microsoft Windows-based software provides easy-to-use displays for identifying and binding IEC 61850 network data between logical nodes using IEC 61850-compliant CID (Configured IED Description) files. CID files are used by the acSELerator QuickSet Architect to describe the data that will be provided by the IEC 61850 logical node within each relay.

13.12.2.10 Automation

13.12.2.10.1 Flexible Control Logic and Integration Features

Use the SEL-421 control logic to do the following:

- Replace traditional panel control switches
- Eliminate RTU-to-relay wiring
- Replace traditional latching relays
- Replace traditional indicating panel lights

Eliminate traditional panel control switches with 32 local control points. Set, clear, or pulse local control points with the front-panel pushbuttons and display. Program the local control points to implement your control scheme via SELOGIC control equations. Use the local control points for such functions as trip testing, enabling/disabling reclosing, and tripping/closing circuit breakers.

Eliminate RTU-to-relay wiring with 32 remote control points. Set, clear, or pulse remote control points via serial port commands. Incorporate the remote control points into your control scheme via SELOGIC control equations. Use remote control points for SCADA-type control operations (e.g., trip, close, settings group selection).

Replace traditional latching relays for such functions as “remote control enable” with 32 latching control points. Program latch set and latch reset conditions with SELOGIC control equations. Set or reset the latch control points via control inputs, remote control points, local control points, or any programmable logic condition. The latch control points retain states when the relay loses power.

Replace traditional indicating panel lights and switches with up to 24 latching target LEDs and up to 12 programmable pushbuttons with LEDs. Define custom messages (i.e., BREAKER OPEN, BREAKER CLOSED, RECLOSER ENABLED) to report power system or relay conditions on the large format LCD. Control which messages are displayed via SELOGIC control equations by driving the LCD display via any logic point in the relay.

13.12.2.11 Open Communications Protocols

The SEL-421 does not require special communications software. ASCII terminals, printing terminals, or a computer supplied with terminal emulation and a serial communications port are all that is required.

13.12.2.12 Bay Control

The SEL-421 provides dynamic bay one-line diagrams on the front-panel screen with disconnect and breaker control capabilities for 25 predefined user-selectable bay types. Additional user-selectable bay types are available via the ACSELERATOR Quickset interface that can be downloaded at www.selinc.com. The bay control is equipped to control as many as 10 disconnects and two breakers, depending on the one-line diagram selected. Certain one-line diagrams provide status for up to three breakers and five disconnect switches. Operate disconnects and breakers with ASCII commands, SELOGIC control equations, Fast Operate Messages, and from the one-line diagram. The one-line diagram includes user-configurable apparatus labels and as many as six user-definable Analog Quantities.

13.12.2.12.1 One-Line Bay Diagrams

The SEL-421 bay control offers a variety of preconfigured one-line diagrams for common bus configurations. Once a one-line diagram is selected, the user has the ability to customize the names for all of the breakers, disconnect switches, and buses. Most one-line diagrams contain analog display points. These display points can be set to any of the available analog quantities with labels, units, and scaling. These values are updated real-time along with the breakers and switch position to give instant status and complete control of a bay. The diagrams below demonstrate some of the preconfigured bay arrangements available in the SEL-421.

The operator can see all valuable information on a bay before making a critical control decision. Programmable interlocks help prevent operators from incorrectly opening or closing switches or breakers. The SEL-421 will not only prevent the operator from making an incorrect control decision, but can notify and/or alarm when an incorrect operation is initiated.

13.12.3 SEL ICONTM DEPENDABLE Communications for Critical Infrastructure

The versatile SEL ICON™ (Integrated Communications Optical Network) provides both intrastation and interstation communications from one easy to manage platform. The ICON supports time-division multiplexing (TDM) and Ethernet over synchronous optical networking (SONET) for internode line transport on a single platform. The ICON includes an integrated Ethernet switch and supports a wide range of applications all the way down to voice and data at the DS0 application level.

13.12.3.1 ICON System Description

The ICON combines both SONET and Ethernet technologies on a single platform. Traditional methods would require as many as four separate pieces of hardware to provide the same functionality as the ICON.

The ICON provides all the functionality of a traditional communications system, including the following components:

- Fiber-optic interstation links using SONET, with support for Gigabit Ethernet in a future release. A standalone SONET multiplexer has traditionally provided SONET transport functionality.
- Ethernet switch to provide local Ethernet connectivity. Typically this capability would require a separate Ethernet network requiring dedicated hardware. ICON supports both TDM and Ethernet traffic over SONET and provides an Ethernet switch with Ethernet drop ports.
- Drop ports for voice and data circuits. To do this using traditional approaches would require a separate channel bank or T1 terminal.
- Integrated Digital Access Cross-connect Switch (DACS). This provides the cross-connection between the voice and data circuit traffic on DS0 channels and the SONET multiplexer. In legacy systems, this functionality was typically performed using separate hardware.

The ICON combines both TDM and packet technology while offering interfaces to the lowest bandwidth applications, including serial data and voice communication. This consolidation of functionality provides economy of scale, central management of the network, and a versatile system that will provide a communications platform for many years.

13.12.3.2 Ethernet Features

- Port statistics counters for frame type (unicast, multicast, broadcast) exiting and entering the Ethernet port
- MAC table key functions and features:
    - “Learn and Lock”—user-configurable capability to learn timeout or number of MAC addresses
    - “No Learn”—user-entered MAC addresses
    - Content-addressable RAM (avoids “fail-to-learn” problems when using HASH technology)
    - “Aging field”
    - “Learn and Age”
- Port-based VLANs (transparent traffic transport)
- 802.1Q VLANs
- Nested VLANs (802.1Q VLANs in port-based VLANs)
- Power over Ethernet for four ports
- Supports eight priority queues per port
- VLAN filtering per port—list of allowed or blocked VLANs
- Port rate limiting—broadcast storm limiting

13.12.3.3 Ethernet standards supported:

- 802.1D Ethernet Bridge
- 802.1p Priority queues (or “Class of Service”)
- 802.1Q VLAN tagging
- 802.3 10BASE-T (RJ45)
- 802.3ac Frame format extensions for VLAN tagging
- 802.3af Power over Ethernet
- 802.3u 100BASE-TX (RJ45)
- 802.3u 100BASE-FX/ZX/BX
- 802.3z 1000BASE-LX/ZX/BX

13.12.3.4 Features Supported on Fiber Ethernet Ports

- FEFI (Far End Failure Indication)
- Monitor of fiber-optic transceiver parameters
    - Optic receive level
    - Temperature
    - Transmit port

13.12.3.5 Features Supported on Copper Ethernet Ports

- Autonegotiation (bit rate and duplex mode)
- Auto-MDIX (crossover cables not required)
- Port enabling and disabling
- Port mirroring—separate entrance and exit monitoring

13.12.3.6 SONET Features

- Small Form Factor Pluggable (SFP) OC-48 optical transceivers
- Optional line port encryption
- Unidirectional Path Switch Ring with < 5 ms switching time
- Path direction selection and “switch on yellow” to eliminate asymmetrical delays
- STS-12c, STS-3c, STS-1 (synchronous transport signal), and VT (virtual tributary) granular internal cross-connect for seamless inter-ring traffic between networks
- Error monitoring for individual STS-1 and VTs at predetermined and user-defined intervals
- Optical transmit and receive level monitor
- Laser current output monitor
- Ethernet mapping using generic framing procedure (GFP-F)
- Built-in test capabilities
  - Force AIS XMT and RCV
  - Line loopback
  - Section trace
  - PRBS/test bytes
  - STS-1 payload monitor
  - VT payload monitor
  - Channel latency
- Supports point-to-point, linear, ring, and multiple ring topologies. Internal cross-connect provides seamless operation between rings. Support single or dual ring interconnect ties.

13.12.3.7 SONET standards supported:

- Telcordia GR.253-CORE
- ITU-T G.7041

13.13 Siemens AG

IEC 61850 – simply usable

Siemens, the IEC 61850 pioneer, unfolds the entire potential of this world standard for you in an easy way

Efficient Energy Automation with the IEC 61850 Standard

The IEC 61850 standard has been defined in cooperation with manufacturers and users to create a uniform, future-proof basis for the protection, communication and control of substations. In this brochure, we present some application examples and implemented stations with the new IEC 61850 communication standard. IEC 61850 already has an excellent track record as the established communication standard on the worldwide market for the automation of substations.

Its chief advantages are:

Simple substation structure: No more interface problems. With IEC 61850, protocol diversity and integration problems are a thing of the past.

Everything is simpler: From engineering to implementation, from operation to service. Save time and costs on configuration, commissioning and maintenance.

Reduction of costs: IEC 61850 replaces wiring between feeders, control switches, and signaling devices.

More reliability: You only use one communication channel for all data – in real time, synchronized via Ethernet.

Why use IEC 61850 technology from Siemens?

Siemens is the global market leader in this area. For you, that means: You benefit from the experience of projects for more than 1000 substations and 140000 protection devices implemented in accordance with the IEC 61850 communication standard by the end of 2010. Siemens offers you IEC 61850 technology that is certified as Class A by the independent testing laboratory KEMA. Future-proof investment due to convincing migration concepts: SIPROTEC 4 protection devices manufactured since 1998 can be upgraded to make them IEC 61850-compatible without any problem. The solutions from the SICAM 1703 and SICAM PAS product lines offer you flexible configurations for seamlessly integrating the latest IEC 61850 concepts into existing substations.

Siemens is the global market leader in this area. For you, that means: You benefit from the experience of projects for more than 1000 substations and 140000 protection devices implemented in accordance with the IEC 61850 communication standard by the end of 2010. Siemens offers you IEC 61850 technology that is certified as Class A by the independent testing laboratory KEMA. Future-proof investment due to convincing migration concepts: SIPROTEC 4 protection devices manufactured since 1998 can be upgraded to make them IEC 61850-compatible without any problem. The solutions from the SICAM 1703 and SICAM PAS product lines offer you flexible configurations for seamlessly integrating the latest IEC 61850 concepts into existing substations.

While reading the brochure "Application examples" under downloads, discover the diverse efficiency potential of energy automation with the IEC 61850 worldwide communication standard.

Choose a Powerful Partnership
Energy Automation from Siemens

www.siemens.com/energy/siprotec
www.siemens.com/energy/sicam
www.siemens.com/energy/iec61850

13.13.1 SIPROTEC

13.13.1.1 SIPROTEC 4 protection devices – a sustainable success story

A homogenous system platform, the unique DIGSI 4 engineering program, and extensive experience of more than a million successfully operating devices in the field worldwide – thanks to these unique advantages, SIPROTEC 4 enjoys top recognition among users worldwide. SIPROTEC 4 is the industry standard for digital protection technology today in all fields of application.

SIPROTEC 4 protection and bay controller devices combine over one hundred years of Siemens experience in the field and have been proving their value for many years through their efficiency, reliability, and future-safety – all this, in the long-term: SIPROTEC 4 devices stand for low life cycle costs, making sustainable and profitable management possible. The implementation of the international IEC 61850 standards has played a significant role in this accomplishment, in that it forms a consistent and future-proof basis for all protection, communications, and control functions in substations.

The SIPROTEC 4 philosophy – one solution, multiple functions SIPROTEC 4 leads the way in integrating protection, control, measurement, and automation functions in one device. In many fields of application, all secondary technical functions can be carried out using just one device. This lowers investment costs, reduces installation work in every respect, and increases system availability.

The same philosophy is central to the DIGSI 4 engineering tool that manages all functions, from the setting and initial start-up of devices to the easy analysis and documentation of system faults.

Efficient and future-proof thanks to seamless communication

IEC 61850 is the worldwide accepted standard for Ethernet-based communication in substations. It was created jointly and subsequently developed by users and manufacturers for protection technology, communication and control in substations, on a future-proof and manufacturer-independent basis. With SIPROTEC 4 Siemens is the first company worldwide to manufacture a complete device range with full IEC 61850 implementation and to develop it continuously. This standard has established itself quickly and successfully. With more than 150,000 devices with an IEC 61850 interface, SIPROTEC 4 stands for incomparable proven experience in the field.

It goes without saying that future editions will continue to support IEC 61850. Continuous further development of this kind guarantees investment and futuresafety. Together with the long-term proven RSTP protocol, both PRP and HSR will feature two additional redundancy protocols in the future. In addition to IEC 61850, further standard protocols such as DNP 3 or IEC 60870-5-103, for instance, will be supported.

13.13.1.2 The advantages of IEC 61850 at a glance:

- Comprehensive engineering support right through to implementation, from operation to service. This brings costsavings to configuration, initial startup, and maintenance
- Noticeably lower costs for wiring between feeder devices, control switches, and signaling devices
- Higher safety thanks to synchronized communication in real time and through the use of a common, Ethernet-based communications channel for all data, including the retrieval of fault records
- High investment safety thanks to the separation of the communications and data models
- Simple, clear system structure without interface, protocol, and integration problems. All IEC 61850-compatible field devices are interoperable, as the FGH clearly demonstrated during testing
- Manufacturer neutrality and worldwide acceptance
- Intuitive user interface, simple to operate

DIGSI 4 forms the interface between the user’s PC and the SIPROTEC devices and brings together all important functions. Designed and created especially for industrial and energy-supply applications, DIGSI 4 makes the parameterization and analysis of the SIPROTEC devices really easy. The downward-compatible PC software features a highly modern intuitive user interface that makes all functions easy to perform, from the parameterization and initial start-up of the devices to the simple analysis and documentation of system faults. A high-performance analysis tool enables quick troubleshooting and provides important data for possible servicing. For many users, DIGSI 4 has become an established name in the business.

13.13.1.3 DIGSI 4 at a glance:

- Representation of every given system structure
- Import and export of parameter sets
- Flexible and intuitive utilization of a comprehensive range of logic editor (CFC) options – no prior programming knowledge necessary

- Precise fault analysis and visualization using SIGRA
- Innovative configuration of inputs and outputs in a visually clear matrix (no box dialogs)
- Intelligent plausibility checks eliminate error entries
- Test and diagnostic functions
- Direct operation of the device via a serial interface and remote control via modem
- Integrated IEC 61850 workstation configurator

13.13.1.4 The SIPROTEC 4 portfolio at a glance:

- SIPROTEC time overcurrent protection 7SJ6 – everything in a single device
- SIPROTEC 7SA6 and 7SA5 – much more than distance protection
- SIPROTEC 7SD5 and 7SD610 – ensures flexible line differential protection
- SIPROTEC 7UT6 – all-round safe transformers
- SIPROTEC 7SS52 – perfect protection for busbars
- SIPROTEC 7UM6 – reliable machine protection
- SIPROTEC 4 devices in power plants – highest availability guaranteed

13.13.2 SIPROTEC Compact

Simple yet comprehensive, safe and reliable

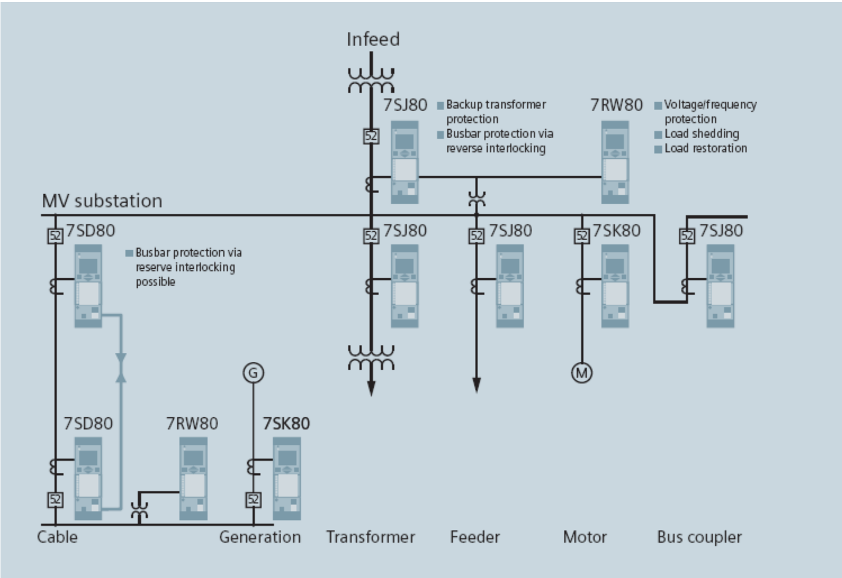
Perfectly suited for protection in distribution systems and industry, with minimal space requirement SIPROTEC Compact devices provide a comprehensive range of functions in a surprisingly compact and space-saving housing.

Whether as main or as backup protection, a single SIPROTEC Compact device provides protection functionality for every conceivable fault. And it can do even more – it supports the control, automation, and monitoring functions in the substation.

Simple to operate and highly flexible The proven concept behind the SIPROTEC Compact range of devices allows efficient and safe operation. The devices can be parameterized completely with the DIGSI 4 parameterization tool. The six-line display and eight LEDs indicate all operating states. The new freely programmable function keys can be integrated in the application by the user. With the programmable logic (CFC) and flexible protection functions the device can be adapted to meet the individual requirements in terms of protection for a broad range of applications. Exchangeable communications interfaces will meet future standards, thereby providing security of investment.

The comprehensive experience of the market leader in a single device The SIPROTEC Compact range stands for the cumulative experience of millions of successfully operating Siemens systems. They are based on the SIPROTEC 4 range, which has been used in countless systems and applications worldwide to date.

Cutting-edge hardware: Pluggable terminal blocks make the installation and retrofitting of all voltage and current connections a breeze. No special tools are required, and settings and adaptations are done via software parameters.



A strong communicator - much more than a protection device

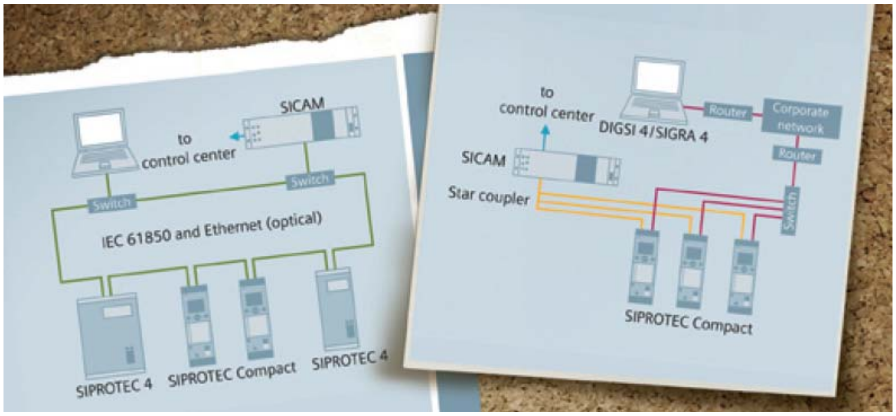
In addition to protection functions, SIPROTEC Compact devices also support control, monitoring, and automation processes. The comprehensive range of features along with communications interfaces ensure that the devices can be fully integrated in the centralized control, supporting control, and service communication. In addition, it provides for connections to be made with other devices, for example via an optical loop according to IEC 61850 with other SIPROTEC 4 devices.

13.13.2.1 Communications interfaces:

- IEC 61850
- IEC 60870-5-103
- PROFIBUS DP
- DNP 3.0
- MODBUS RTU
- Ethernet interface for DIGSI 4 or for optical protection interfaces for differential protection
- Front-mounted USB interface
- Features of Ethernet interface for IEC 61850:
- IEC 61850 with integrated redundancy (electrical or optical)
- Peer-to-peer communication between devices via Ethernet (IEC 61850 GOOSE)
- Millisecond-precise synchronization via Ethernet with SNTP
- Optional optical IEC 61850 loop configuration of SIPROTEC 4 and SIPROTEC Compact devices
- Ethernet services that can be deactivated

Intuitive user interface with really easy operation

DIGSI 4 is the application software on the user’s PC for the interface with SIPROTEC Compact devices providing all the related functionality. DIGSI 4 is specifically developed for industrial and utility applications, making the parameterization and evaluation of SIPROTEC Compact and SIPROTEC 4 devices really easy.



13.13.2.2 SIPROTEC Compact at a glance: the SIPROTEC Compact device range

- Compact design
- Simple installation without special tools
- Six-line display
- Eight freely assignable LEDs
- Nine freely parameterizable function keys
- Pluggable current and voltage terminal blocks
- Front-mounted USB interface
- Battery can be exchanged from the front panel
- Two interfaces for remote access
- Programmable logic (CFC) and flexible protection functions
- Binary input voltage threshold adjustable with DIGSI
- Current transformer rated secondary current
- (1 A/5 A) adjustable with DIGSI

13.13.2.3 The SIPROTEC Compact portfolio at a glance:

- Time-overcurrent protection 7SJ80
- Time-overcurrent protection 7SJ81 for connecting to low-power current transformers
- Motor protection 7SK80
- Voltage and frequency protection 7RW80
- Line differential protection 7SD80

13.13.3 SICAM PAS

SICAM PAS – Power Automation Up-To-Date

A state-of-the-art system SICAM PAS (Power Automation System) fully complies with IEC 61850. Networking and IT capabilities, interoperable system structure and integration into existing systems are characteristics of SICAM PAS that make it a sound investment for the future. SICAM PAS makes configuration and commissioning easy, saves you time, and helps increase the efficiency of operations management. SICAM PAS will help you increase reliability and availability of your systems and contribute to a stable power supply, making it more economical. Today. Tomorrow. Always.

SICAM PAS – Tailor-Made Flexibility, Today and Tomorrow

Economic efficiency and constant availability of the supply of electric power is a challenge that energy providers and industries are facing worldwide. A broad range of concepts are in use each tailored to its specific application. With high scalability and modern architecture, SICAM PAS adapts to these

concepts and offers room for future expansion. More than 1,000 substations equipped with SICAM PAS based on IEC 61850 are working successfully (January 2009). You also can profit from our wealth of experience.

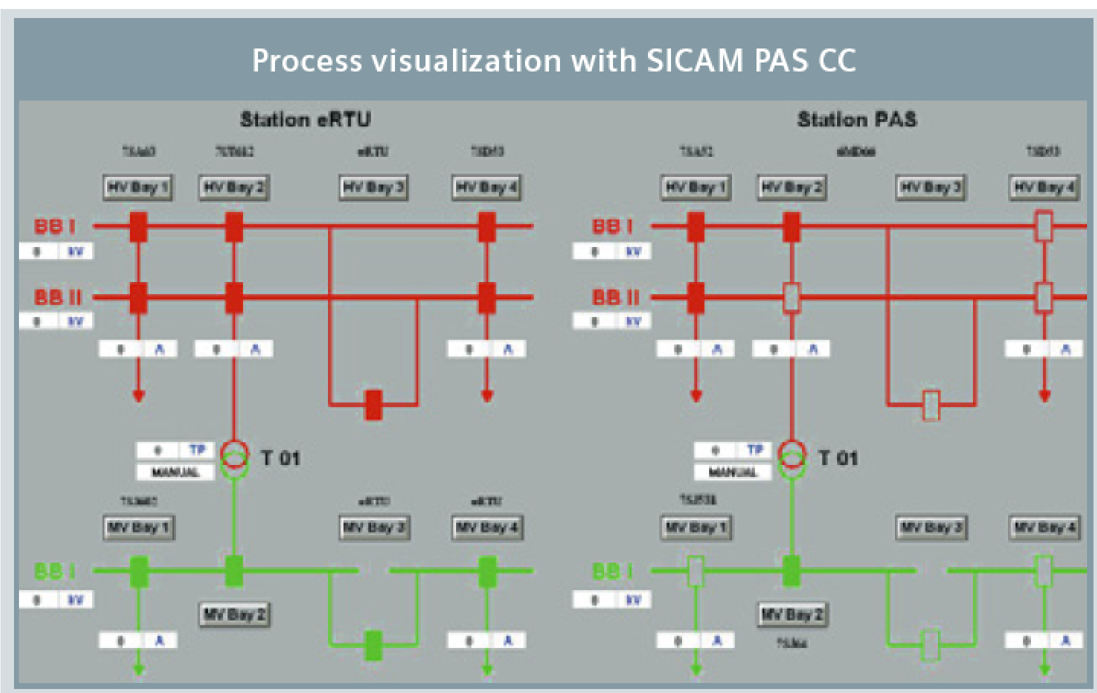
IEC 61850 – the standard of success Users and manufacturers joined forces in creating the new IEC 61850 standard adopted in early 2004. Experience gathered with the IEC 60870-5 series and with UCA.2 (developed in the USA) was pooled with optimized user benefit in mind. With Siemens participating directly in the standardization committees, SICAM PAS was developed with specific reference to the new standard. With more than 7,000 SICAM systems in use worldwide, today the incorporation of IEC 61850 now offers users the latest technology in power automation.

By using IEC 61850, the station unit of SICAM PAS now leads the way to a future oriented interoperable system structure. Thus, SICAM PAS can integrate any manufacturer's bay control units using IEC 61850. The concept and settings of SICAM PAS support a direct exchange of data at the bay level, thus avoiding communication bottlenecks. Due to extremely fast Ethernet connections and a station unit optimized for data transfer and processing, SICAM PAS is a truly pioneering power automation system.

New standards from the IT and office sectors are applied. Networking capabilities and open data interfaces such as OPC (Object Linking and Embedding for Process Control) allow easy transfer of information to the office and industrial environments. Evaluations or plain display of power data, as are frequently needed by production coordinators in the industry, are an easy matter.

SICAM PAS – the Clever Choice

Regardless of how the requirements might appear, with its fi ne function grading and flexibility SICAM PAS can be adapted to suit them all. Be it relatively simple solutions for the user in a small or medium-sized industrial world or the demands typically encountered on the high and extra-high voltage levels, SICAM PAS masters these challenges with an ideal price/performance ratio. SICAM PAS also proves cost- effective in operation. Functions can be activated at any time within the scope of the standard. There is no need for bothersome add-ons at a later stage. Project-specific options can be added to boost the flexibility of your application at any time. Your investment remains secure thanks to strong standards, a wide variety in communication and sophisticated functionality.



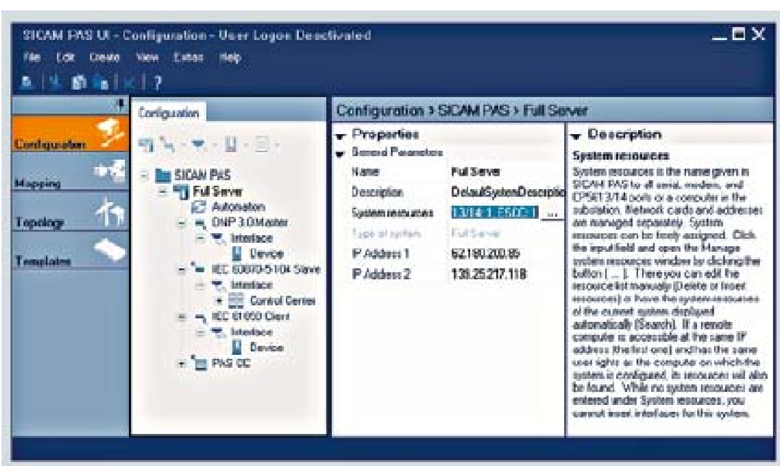
The intelligent settings engine SICAM PAS UI is structured in conformity with DIGSI and adopts configuration data directly from the bay level. XML data transfer is available for IEC 61850 and the SIPROTEC 4 relays. Standard con figurations for protective devices of other manufacturers are available in a library which can be integrated into SICAM PAS as typicals, thus avoiding double inputs or input errors. SICAM PAS provides the configuration data needed for integration in an overall solution in XML format. This minimizes the effort needed to connect a local HMI especially for SICAM PAS CC or for interfacing with a network control center.

During the design of the SICAM PAS system, a high value was set on the usability of the parameter setting and diagnosis tools. By means of these unique tools integrated directly in the system, parameter setting and commissioning can be carried out easily and swiftly. What's more, no matter when changes, additions, or other work on the system are imminent, it already contains the right tools. There is no need for version checks of the parameter tools or for special test instruments.

Systems spread over wide areas call for a particular need to keep track of things. From the SICAM PAS CC (Control Center) you can monitor and control all parts of a system from a central point. The clear display of the operating situation allows you to react fast; you consequently reduce your operating costs and can quickly restore power in the event of malfunctions. As an integrated overall system, SICAM PAS supports you all the way from the bay level to the control center interface with fast data handling, with the flexibility of a programmable-logic controller and with the reliability philosophy of a classic telecontrol unit.

Driven by the new optimization potentials of IEC 61850, SICAM PAS has been created as a symbiosis of both systems. In addition to present advantages it offers the user even higher reliability and even more security of investment. Availability and flexibility will help you create state-of-the-art control and protection concepts in power automation.

SICAM PAS – Setting and Serving New Standards



- IEC 61850

Interoperability and integration capabilities facilitate supplier independent system integration and reduce planning efforts at the same time.

- Future proof

Standardized protocols ensure interoperability without the need for expensive gateways. Networking capability and remote access also make for cost optimized operating concepts.

- Security is important

SICAM PAS development is according to upcoming security standard.

- Straightforward system structure with optimum expandability

Thanks to high scalability, functionality can be adjusted to application-specific requirements. As such requirements grow, the system simply grows along with them – without the need for any reinstallation.

- Enter your data only once

Regardless of the number and variety of functions, one central database makes sure that every piece of information only needs to be entered once into the system. This ensures data consistency and minimizes effort.

- Simplified engineering

Easy handling in Windows™ environment means minimizing time to learn the system, thus ensuring highest productivity and reliability. Graphical configuration and automation con tribute to straightforward parameter definition, thus reducing engineering times.

- High-speed processing by means of distributed intelligence

A decentralized system structure with compact bay control devices reduces the complexity of wiring. At the same time, decentralized processing of switching interlocks boosts data throughput, shortens response time and thus improves system safety.

- Networking capability offers new possibilities

Existing TCP/IP networks can be used economically to achieve high data transfer rates. Information can also be transferred to an office environment for evaluation.

- Information available anywhere, anytime

Both locally and remotely, optimized diagnostic tools provide in-depth information on the process and system. Thanks to the clearly visualization, you are getting the optimum picture and can come to the right decisions quickly and reliably.

- Innovation combined with decades of experience

20 years of experience in power automation and 70 years of experience in telecontrol combined with the future oriented IEC 61850 standard – that‘s SICAM PAS, a successful symbiosis of the SICAM family, a family with long tradition. Our know-how will provide a secure return on your investment – profit from it!

13.14 SISCO

13.14.1 Unified Analytic Platform

Overview

Given the challenges of building new transmission lines, it is critical that utilities maximize the utilization of their existing assets without jeopardizing reliability. Implementing reliable and fast mitigation schemes can enable significant reduction in reserve margins while maintaining or even increasing reliability in some cases.

Traditional distributed remedial action schemes (RAS) that rely on complex device programming that interacts in real-time across multiple substations can be difficult to develop, test, and maintain. This increases the cost and slows more widespread usage of wide area RAS.

Centralized RAS can lower the cost by providing a higher-level development environment with better simulation, testing, and management capabilities. This enables more rapid and widespread implementation of RAS that can save utilities millions of dollars compared to other methods of RAS or adding capacity in existing transmission corridors.

Benefits

- Lower the reserve margin for critical lines through more effective mitigation strategies.
- Lower deployment costs by eliminating complex logic from distributed remote substations via centralized RAS processing using modern programming languages.
- Lower testing costs using simulation tools that support complex event emulation coupled with powerful analysis and debugging capabilities.
- Enables continuous improvement of RAS algorithms using fault playback for testing and validating changes by comparing new algorithm performance to past events.
- Easily integrated with existing system operations via standardized ICCP-TASE.2 interfaces.
- Leverages IEC 61850 GOOSE messaging and modern networking for maximum performance enabling wide area protection of critical assets.

Features

Integration with the OSIsoft PI System enables system events and states to be historized with application responses for analysis of system faults and application performance.

High-level analytic application development environment based on the Microsoft .Net platform provides a more productive environment for development, testing, debugging and maintaining applications versus distributed remote device programs.

High-performance interfaces to the network and PI System enable analytics to run in real time for time-critical applications like C-RAS.

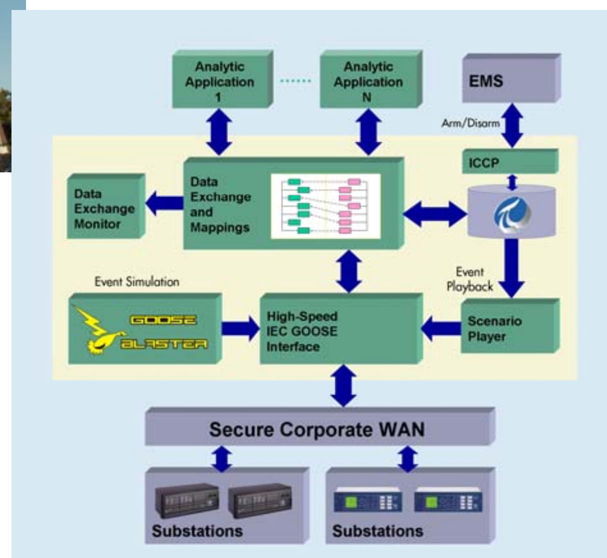
Scenario playback system allows past system event information to be played back into analytic applications for RAS testing and improvement based on actual event data.

SISCO GOOSE Blaster enables development of complex fault simulations for testing.

Flexible device configuration based on standardized Substation Configuration Language (SCL) to support multiple types and brands of substations devices.

Applications

- Wide Area C-RAS for better control and mitigation of contingencies in existing transmission corridors.
- High-speed analysis for detecting abnormalities in data streams.
- Real-time analysis and calculations using phasor and other data streams.



Unified Analytic Platform for PI

SISCO's Unified Analytic Platform provides a high-performance environment for the development, debug, and enhancement of analytic applications to support centralized remedial action and other wide area control algorithms. SISCO's Unified Analytic Platform provides a unique structured environment that integrates development, testing, simulation, results analysis, reporting, and algorithm improvement processes into a unified platform for analytic applications based on the OSIsoft PI System. The Unified Analytic Platform provides an environment for high-performance analytic applications that are:

- Redundant
- Repeatable
- Testable
- Maintainable

13.14.2 AXS4-61850

Description

AX-S4 61850 ("Access for 61850") provides access to real-time data via IEC 61850 for any Windows compatible application supporting OPC Data Access (DA) and DDE interfaces. AX-S4 61850 gives you a high-level interface to real-time data that lowers your integration cost by providing you everything needed to interface IEC 61850 with standard off-the-shelf OPC based applications on the Windows platform in a single easy-to-use package. All the essentials needed to interface Windows applications to IEC 61850 devices is bundled in a single easy-to use solution including an IEC 61850 client, an IEC 61850 server, and an IEC GOOSE publisher/subscriber.

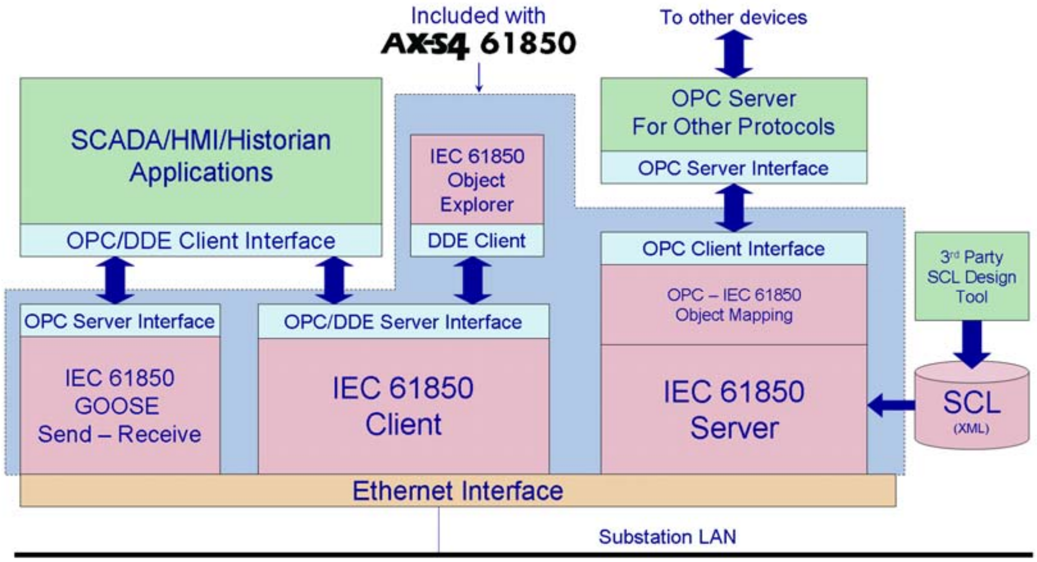
AX-S4 61850 is optimized to allow standard OPC products to interface with IEC 61850 devices by automatically handling most of the unique features of IEC 61850. This enables off-the-shelf products to be used effectively with IEC 61850 devices without complex scripting, logic, and special handling by the OPC applications.

IEC 61850 Support

- SUPPORT FOR IEC 61850:2003 PARTS 6-1, 7-2, 7-3, 7-4, 8-1, 7-410, 7-420, AND IEC 61400-25-2 INCLUDING GOOSE/GSSE MULTICAST SERVICES.
- IEC 61850 CLIENT FUNCTIONS :
  - 0 OBJECT DISCOVERY AND CONFIGURATION USING ACSI SERVICES OVER TCP/IP
  - 0 SCL IMPORT TO CONFIGURE OBJECTS AND DEVICES
  - 0 READ/WRITE OF ANY IEC 61850 OBJECT
  - 0 BUFFERED AND UNBUFFERED REPORTING
  - 0 CONTROLS (DIRECT, SBO, NORMAL/ENHANCED SECURITY)
  - 0 LOGS
  - 0 FILE TRANSFER CLIENT AND SERVER

Key Features

- AUTOMATIC REPORT SUBSCRIPTION AND DATASET HANDLING SUPPORTS RE-ENABLING OF REPORTS AFTER POWER DOWN OR DEVICE DISCONNECTS AND ENABLES DATA FLOW WITHOUT OPC CLIENT INTERACTION.
- AUTOMATED MAPPING OF IEC 61850 QUALITY AND TIMESTAMP DATA TO OPC QUALITY AND TIMESTAMPS.
- SIMPLIFIED CONTROL FUNCTIONS SUPPORT SINGLE OBJECT WRITE OPERATIONS.
- INTERACTIVE OBJECT EXPLORER FOR DEVICE AND OBJECT VISUALIZATION, DEBUG, TESTING, CONFIGURATION, AND CONTROL.
- A COMPLETE SOLUTION IN A SINGLE EASY TO USE PACKAGE THAT INCLUDES:
  - 0 IEC 61850 CLIENT – OPC/DDE SERVER
  - 0 IEC GOOSE PUB/SUB – OPC SERVER
  - 0 IEC 61850 SERVER – OPC CLIENT
  - 0 IEC 61850 OBJECT EXPLORER



A Single Solution For Maximum Flexibility

AX-S4 61850 delivers the functions needed for most applications in a single package. By including the client, server, GOOSE pub/sub, and an interactive object explorer in a single AX-S4 61850 installation you can provide more complete solutions without having to purchase multiple IEC 61850 products.

IEC 61850 Support (cont'd)

- IEC 61850 SERVER ENABLES SUPPORT FOR PROXIES, DATA CONCENTRATORS, GATEWAYS AND TO EXPOSE OPC DATA FROM APPLICATIONS AS IEC 61850 DATA
  - 0 SERVER CONFIGURATION VIA SCL (IEC 61850-6-1) SUPPORTING MAPPING OF IEC 61850 OBJECTS TO EXTERNAL OPC SERVER FOR DYNAMIC DATA AND FIXED VALUE INITIALIZATION FOR STATIC DATA.
  - 0 USER CONFIGURABLE READ/WRITE ACCESS AND GROUP UPDATE RATE TO ANY OBJECT
  - 0 BUFFERED AND UNBUFFERED REPORTING WITH DEAD BAND PROCESSING
  - 0 CONTROLS (DIRECT AND SBO VIA NORMAL SECURITY)
  - 0 OBJECT DISCOVERY BY CLIENTS USING ACSI SERVICES
- IEC 61850 GOOSE/GSSE PUBLISHER/SUBSCRIBER
  - 0 CONFIGURATION VIA SCL (IEC 61850-6-1)
  - 0 USER CONFIGURABLE RETRANSMISSION CURVE
  - 0 MAPPABLE TO IEC 61850 SERVER FOR FULLY FUNCTIONAL GOOSE CONTROL BLOCKS.

Key Features (cont'd)

- FLEXIBLE ASSOCIATION MANAGEMENT FOR THE IEC 61850 CLIENT:
  - 0 UP TO 8 IP ADDRESSES CAN BE SET FOR EACH REMOTE DEVICE. AX-S4 61850 WILL ATTEMPT TO CONNECT TO ALL ADDRESSES WHEN ESTABLISHING AN ASSOCIATION.
  - 0 AUTOMATIC RETRY AND TIMEOUTS WITH A “KEEP-ALIVE” FEATURE FOR REPORT ONLY ASSOCIATIONS.

0 ASSOCIATION CONTROL AND RECONFIGURATION ITEMS EXPOSED TO OPC CLIENTS TO OVERRIDE AUTOMATIC ASSOCIATION MANAGEMENT FUNCTIONS.

- AX-S4 61850 FUNCTIONS AND OPC APPLICATIONS CAN ALL BE RUN CONCURRENTLY ON A SINGLE COMPUTER AS A SERVICE OR APPLICATION PROCESS.
- EACH LICENSE GOOD FOR A SINGLE COMPUTER WITH NO DEVICE OR TAG LIMIT ON LICENSING.
- COMPATIBLE WITH HUNDREDS OF OPC APPLICATIONS SUPPORTING OPC DATA ACCESS V3.0 AND V2.05A.

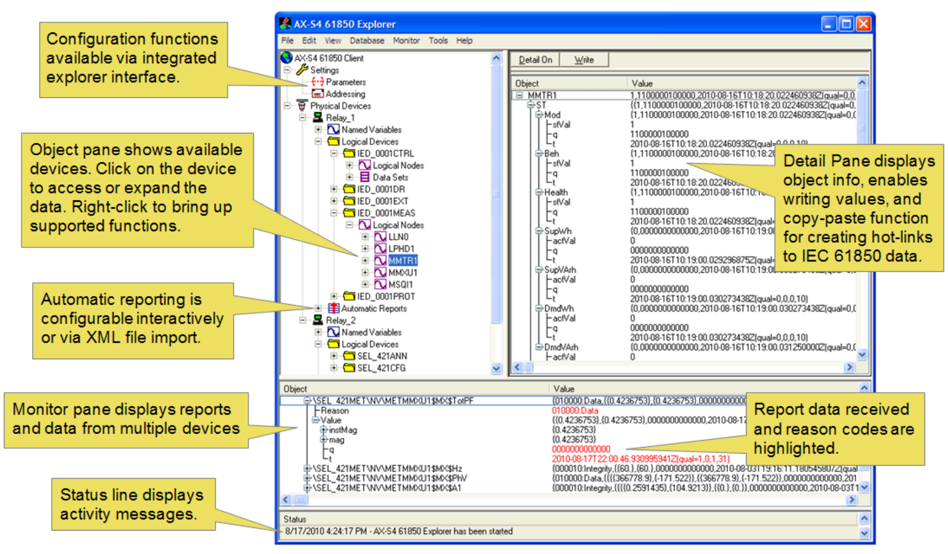
AUTOMATED CLIENT REPORT HANDLING

- AX-S4 61850 CAN MANAGE ALL THE REPORTING AND DATA SET FUNCTIONS. OPC CLIENTS NEED ONLY ACCESS THE DATA FROM A REPORT USING A NORMAL ADVISE FUNCTION TO RECEIVE ALL REPORTED DATA.

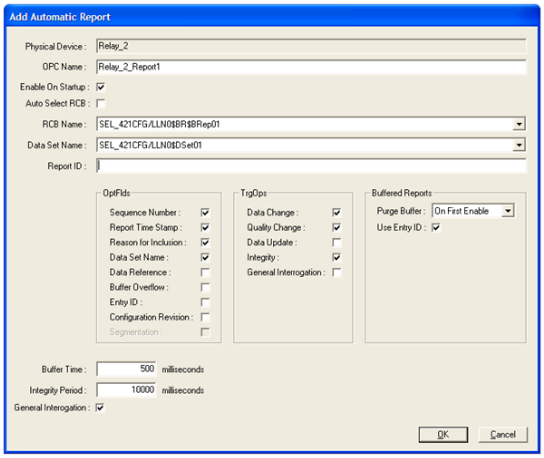
DEVICE CONFIGURATION

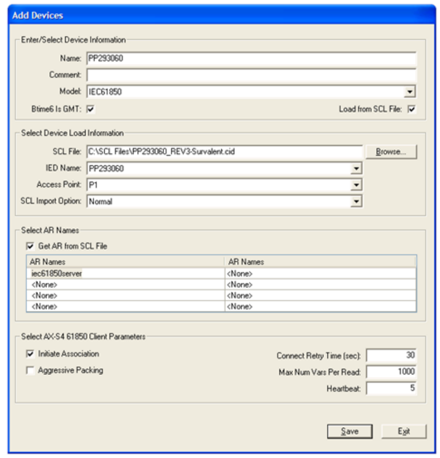
- SCL IMPORT AND ASSOCIATION MGMT. FUNCTIONS ARE CONFIGURED USING EASY TO UNDERSTAND DIALOGS. MULTIPLE IP ADDRESSES PER DEVICE ENABLE CONFIGURATION OF REDUNDANT ROUTING PATHS.

AX-S4 61850 Explorer – Interactive Interface to IEC 61850



AX-S4 61850 – Configuration





13.15 Toshiba

13.15.1 Product Description – GRZ100

GRZ100 is a fully numeric distance protection for application to transmission lines on solidly earthed network.

The GRZ100 provides the following protection schemes.

- Time-stepped distance protection with four forward zones, three reverse zones, and one
- non-directional zone
- Zone 1 extension protection
- Command protection (Distance protection using telecommunication)
- Overcurrent backup protection
- Thermal overload protection
- Switch-on-to-fault and stub protection
- Circuit breaker failure protection
- Broken conductor detection
- Out-of-step protection
- Overvoltage and undervoltage protection
- For high-resistance earth faults, the GRZ100 provides the following directional earth fault protections.
- Directional earth fault protection
- Directional earth fault protection utilizing telecommunications facilities
- The GRZ100 actuates high-speed single-shot autoreclose or multi-shot autoreclose.
- The GRZ100 provides the following metering and recording functions.
- Metering
- Fault record
- Event record
- Fault location
- Disturbance record

The GRZ100 provides the following menu-driven human interfaces for relay setting or viewing of stored data

- Relay front panel; LCD, LED display and operation keys
- Local PC
- Remote PC
- Password protection is provided to change settings.
- Eight active setting groups are provided. This allows the user to set one group for normal operating conditions while other groups may be set to cover alternative operating conditions.
- GRZ100 can provide the following serial interface ports:
- RS232C for a local PC and Relay Setting and Monitoring System (RSM100)
- RS485 for a remote PC, and Relay Setting and Monitoring System (RSM100) or Substation control and Automation System (SAS) with IEC60870-5-103 protocol
- Fibre Optic (FO, option) for a remote PC, and Relay Setting and Monitoring System (RSM100) or Substation control and Automation System (SAS) with IEC60870-5-103 protocol
- 100BASE-TX, or -FX (option) for Substation control and Automation System (SAS) with IEC61850 protocol
- Another interface IRIG-B port is provided for an external clock connection.
- The RS232C port is located on the front panel of the relay. Other ports (RS485, FO, 100BASE-TX, 100BASE-FX and IRIG-B) are located on the rear of the relay.
- Further, the GRZ100 provides the following functions.
- Configurable binary inputs and outputs
- Programmable logic for I/O configuration, alarms, indications, recording, etc.
    - Automatic supervision

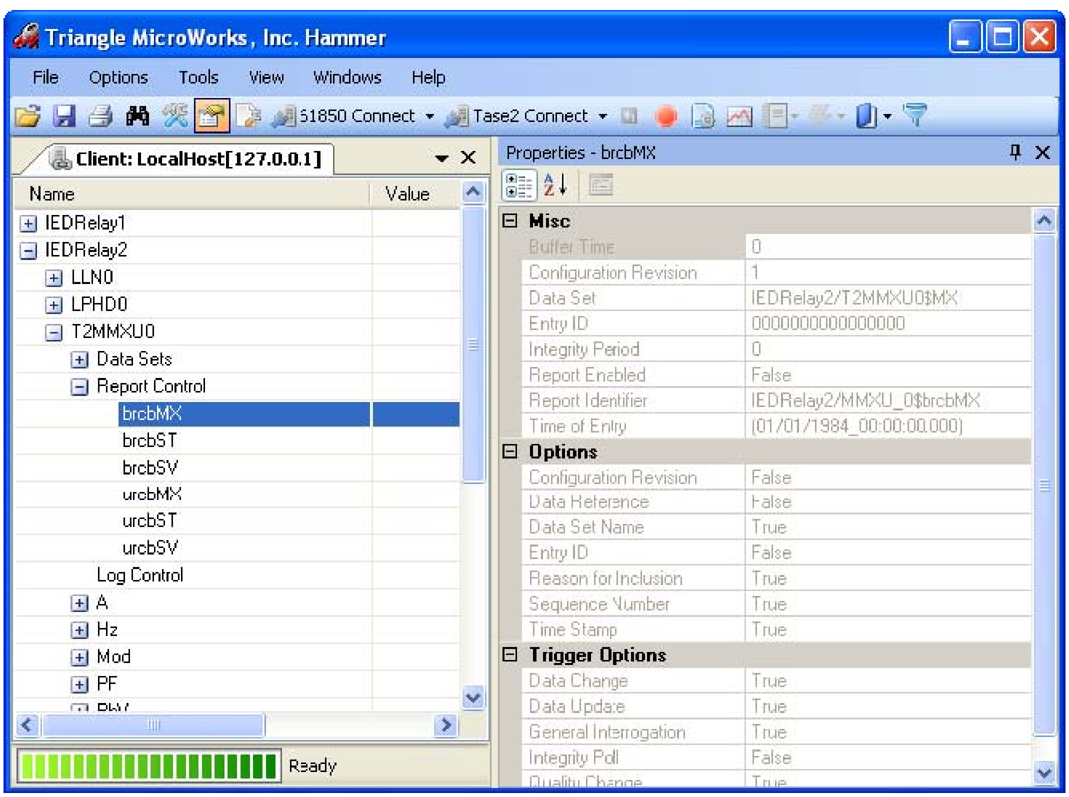
13.16 Triangle Microworks

13.16.1 Hammer

The Hammer is a part of the Triangle MicroWorks 61850 Test Suite. It provides an IEC 61850 Test Client in order to validate IEC 61850 Server implementations. The functionality provided in each is based client is based on the features supported in the protocol:

HIGHLIGHTS

- IEC 61850 Client
- Browse any IEC 61850 Server
- Exercise Reporting, Logging, GOOSE, Controls, and File Services
- Create and delete dynamic data sets
- Save discovered model to an SCL file
- Select Flexible views and save/load Workspaces
- IEC 60870-6 (TASE.2/ICCP) Client
- Browse any IEC 60870-6 Server
- Exercise Reports and Controls
- Create and delete dynamic data sets
- Save discovered model to an XML file



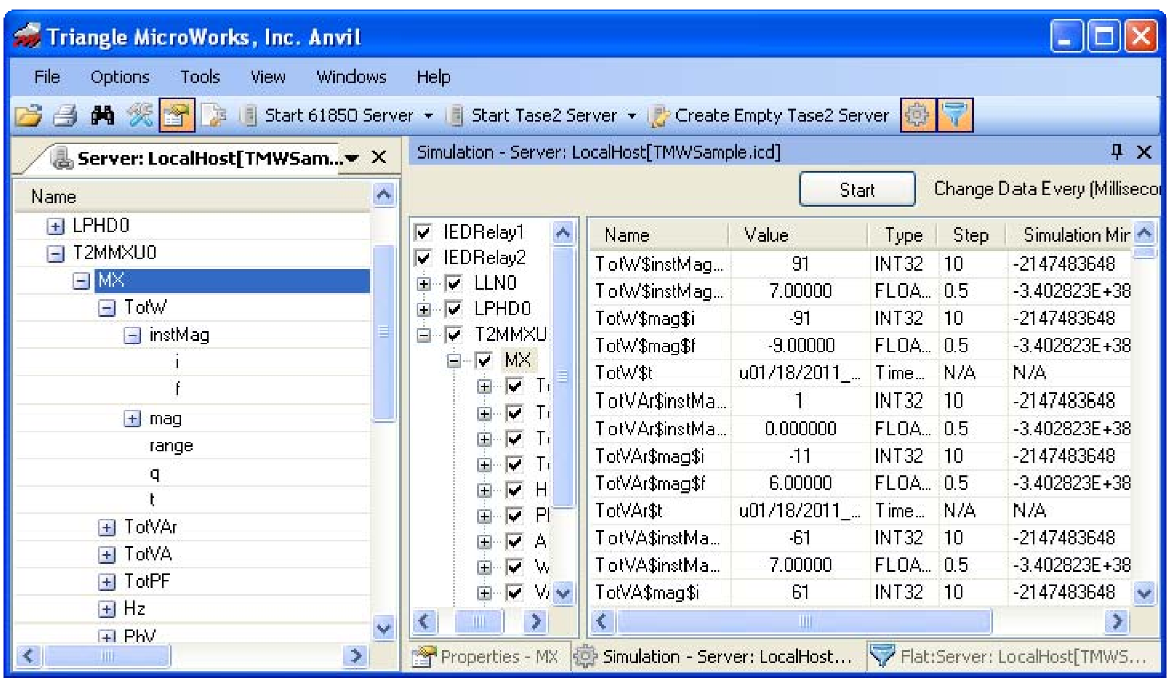
13.16.2 Anvil

The Anvil is a part of Triangle MicroWorks 61850 Test Suite. It provides an IEC 61850 Test Server in order to exercise IEC 61850 Client implementations. It currently supports two protocols. The functionality provided in each is based on the features supported in the protocol.

HIGHLIGHTS

- IEC 61850 Server
  - Create a compliant IEC 61850 Server by loading an arbitrary Object Model via an SCL file
  - Generates simulation data automatically, manually, or table driven
  - Supports GOOSE, Reports, Logs, Controls, and File Services
  - Supports Dynamic Data Sets
  - Select flexible views and save/load Workspaces

- IEC 60870-6 (TASE.2/ICCP) Server
  - Generates simulation data automatically, manually, or table driven
  - Supports Reports
  - Save/Edit/Reload of object models



13.17 ZIV

13.17.1 7IDV-D

13.17.1.1 TRANSFORMER DIFFERENTIAL MULTIFUNCTION PROTECTION & CONTROL IED

PROTECTION FEATURES

Three phase differential protection with percentage and harmonic restraint (87) There are three differential elements, which use operating and restraint magnitudes calculated with data from the currents of the machine’s windings. They have percentage as well as 2nd and 5th harmonic restraint. These restraints block the differential unit when there are external faults, in-rush currents due to energizing the transformer (2nd harmonic) and situations of over excitation (5th harmonic).

- External Fault Detector
- instantaneous three-phase differential without restraint (87/50)
- restricted earth fault (2 units per ground channel) (87N/87REF).
- instantaneous phase overcurrent for each of the windings (2 units/winding)(50)
- instantaneous negative sequence overcurrent for each of the windings (50Q)
- instantaneous ground overcurrent calculated (3I0) for each of the windings (2 units/ winding) (50N)
- instantaneous ground overcurrent with independent input (ground) (50G),
- time phase overcurrent (inverse / fixed) for each of the windings (2 units / winding) (51N),
- time ground overcurrent (inverse / fixed) with independent input (ground) (2 units / channel) (51G),
- thermal unit (49)
- breaker failure (1 unit / winding) (50BF)
- overexcitation protection unit, also known as 59 V/Hz or 59/81 (1 unit) (24),
- undervoltage element with phase-ground / phase-phase metering (selectable) (2 units) (27),
- overvoltage element with phase-ground / phase-phase metering (selectable) (2units) (59)
- overfrequency (4 units) (81M)
- underfrequency (4 units) (81m)

- rate of change (4 units) (81D)

13.17.1.2 Unit for protecting against aging of the insulation.

GENERAL FEATURES

Measurements: Phase-currents. Differential currents, restraint currents. Positive, negative and zero sequence of of currents of each winding. Power calculated from the magnitude of current and voltage: active, reactive and apparent power. Frequency. Thermal image.

- Measurement accuracy:
- Measured currents (phases) +/- 0.1 % or +/- 2 mA (the greater)
- Measured currents (ground) +/- 0.1 % or +/- 1 mA (the greater)
- Measured voltages +/- 0.1 % or +/- 50 mV (the greater)
- Active and reactive powers (In=5A and Iphases>1A)
- +/- 0.3% (0º or +/-90º or 180º)
- +/- 1% (+/-45º or +/-135º)
- +/- 5 / 0.5% (+/-75º / +/-115º)
- Fault reporting. Capacity of storing up to 15 fault reports with relevant data.
- Oscillographic recording. The oscillography record allows up to 64 oscilographs to be saved in a cyclical memory
- Time Synchronization. Via GPS (IRIG-B protocol) or by communications through the remote communications port.
- Communication ports. The relay can have up to five remote communication ports.
- Local: RS232+USB front panel ports

Remote:

- Up to 3 non IEC 61850 (DNP 3.0, Modbus, Procome) ports, each of which can be chosen (in any combination) between:
- RS232/485
- Ethernet
- Fiber Optics.
- Three choices for IEC61850 ports
    - 2xRJ45 100TX ports
    - 1xRJ45 port and one Fiber Optic MTRJ port.
    - 2xFiber Optic (ST Connector) ports
- Power supply: 48-250 Vd.c./Va.c. (+/- 20%)
- Current circuit burden < 0.2 VA
- Voltage circuit burden < 0.55 VA
- Power supply burden: quiescent 7 W, maximum < 20 W
- Breaker trip and close outputs and auxiliary outputs:
    - I DC maximum limit (with resistive load) 60A (1s)
    - I DC continuous service (with resistive load) 16 A
    - Breaking capacity (with resistive load) 110 W (80 Vdc-250Vdc)
    - Break (L/R 0 0.04 s) 120 W at 125 Vdc
- 400-record-capacity sequence of events log stored in non-volatile memory.

13.17.1.3 Substation Central Control Unit CPT.

The CPT is designed to solve all communication and data processing needs with a substation's protection, control and metering equipment, providing new functions that make most of the information available to these units. The CPT is responsible for communications with level 1 equipment and for real-time database maintenance, incorporation of automatic devices and logic at substation level being possible.

CPT relays are also provided with a web server to access the Integrated Web Console (built into the CPT itself) that can at the same time be accessed via web client from any substation computer, serving the purpose of interface between user and system. On the other hand, CPT relays can be used to establish communications with the remote control office or SCADA.

The entire system can be configured through *Zivergraph©* software. This program enables the system to be configured to adapt to the substation's characteristics: equipment connected, signals associated with each unit, representation of the information on displays, logic functions at the substation level, desired functionality, etc.

COMMUNICATIONS

Communication between CPT relays and substation protection and control equipment is made via standard IEC-61850 communications protocol through a network interface Ethernet 100-BaseT. However, communications between CPT relays and level 1 equipment can be established via serial connections (fibre optic – plastic or glass- or RS-232) using conventional protocols such as PROCOME, DNP3.0, MODBUS, IEC103, SPABUS.

SYNCHRONIZATION

The CPT is responsible for keeping the entire system synchronized with a single clock source.

DATABASES

The CPT collects data from the substation's IED, control and metering units and maintains a database with this data, updated in real time (the update cycle will depend on the number of units connected, on the communication parameters and on the protocol used).

COMMANDS

The CPT allows commands to be executed on the installation's configurable elements.

LOGIC

The CPT has an internal task responsible for executing a fully programmable logic program by means of certain functions: logic gates (AND, OR, NOT, etc.), flip-flop (RS, JK), commands, etc.

EVENT MANAGEMENT

The CPT captures level 1 device data following the guidelines of the communications protocol used, but in all cases the first step is to request the status of all available signals, measurements and counters. Standard IEC-61850 provides services for level 1 devices to spontaneously send to the CPT all signal, measurement and counter changes.

ALARM MANAGEMENT

The same as with the events, not all signal changes are alarms. The CPT is responsible for managing the alarms occurring at the substation filtering at CPT integrated web console level, which level 1 device changes received are alarms and which not.

CONTROL FUNCTIONS

The CPT can execute certain control functions at the substation level, in which signals from different equipment take part.

CONTROL FUNCTIONS

In some relevant systems a redundant system must be installed. CPT redundancy can be of two types: Hot-Stand-By (HSB) and Complete.

HISTORY RECORDS

Another optional functionality of the CPT is to log changes in signals, measurements and meters. These are daily history records of data to be stored into the CPT flash disk.

SELF-CHECKING

The central unit periodically checks the integrity of the hardware and the software stored on its permanent memory devices.

HMI INTERFACE

There is an operator interface that allows to obtain information regarding the equipment's functionality, as well as information that will enable the supervision of the central unit's performance and operability at all times.

WEB CONSOLE

- The Embedded Web HMI features the following main functions:
  - Databases.
  - Commands.
  - Event management.
  - Alarm management.

13.17.1.4 3SWT ETHERNET SWITCH

The 3SWT, is an Ethernet Switch model designed to operate in environments with large electromagnetic fields or other adverse conditions.

The 3SWT fulfil all the required functions to set up a reliable network within an electrical substation. 3SWT switches have the right double port configuration to set up any of the topologies a network architect could imagine.

MAIN FEATURES

- **IEC61850 certified:** IEC61850-3 hardware environmental requirements. IEC61850 functional requirements.
- **Modularity in number and type of ports.** Different combinations in number and type of copper, multimode fiber and singlemode fiber in 10/100 Mbps and 1000 Mbps ports.
- **DHCP Relay and Option 82 Redundancy in power supply.** Possibility to increase the switch availability by having a second power source in case the first one fails.
- **Power over Ethernet enabler.** uSysCom switches can directly power up any PoE enabled device following the 802.3af standard. This way an IP phone or a wireless access point, can be powered with the same cable that is used for data transmission.
- **Failure contact alarm.** Hardware contact that is activated when a link problem occurs.
- **Logs and alarms.**3SWT creates logs where statistics about linkstatus alarms are stored with the achúrate timestamp, so all events can be traced.
- **Advanced security features.** 3SWT has advanced security features implemented to avoid unauthorized access to the system. It has different user levels with different passwords, the possibility to work with different VLANs, following the 802.1Q standard, port security based on MAC addresses, possibility to disable unused ports,authentication protocols.
- **High Speed implementation of RSTP and MSTP.** In high availability networks it is important to have a fast path recovery when any failure occurs. 3SWT not only follows the STP and RSTP protocols, but also exceeds the usual recovery time of these protocols due to its high speed implementation of RSTP, which grants fault recovery times lower than 4 ms. per link, always fulfilling the RST protocol.
- **SNMP management.** Easy integration of monitoring tools and alarms notifications in an SNMP based central management system, such as HP Openview.
- **NTP client.** 3SWT internal clock can be synchronized from a network SNTP/NTP server, so all time stamped events can be referenced from a reliable time reference.

- **Port bandwidth limiting.** 3SWT allows the limitation on bandwidth accepted for unicast, broadcast, multicast, or all type of traffic per port. This way resources for non critical services can be limited. Broadcast Storm Control and IGMP snooping. Limiting broadcast traffic grants that no malfunctioning device saturates the network with undesired and uncontrolled broadcast traffic.
- **Port mirroring.** User can configure one port to replicate traffic flows of different ports, so the system administrator can monitor the incoming, outgoing, or all kind of traffic that is going through the ports under study.
- **Statistics.** User can access the traffic statistics per port live.
- **Quality of service.** User can define different priorities for different ports, so critical traffic is dealt with first.

APPLICATION FIELDS

- **Reliable architecture.** Network topologies within the electrical substation may vary depending on the number of services, number of substation cabinets, and number of different networks the electrical company would like to define. 3SWT switches have the right double port configuration to set up any of the topologies a network architect could imagine. The typical architectures within substations are stars, double stars, rings, double rings, and concatenated rings.
- **Grouping services.** It is convenient for electrical companies to have the different services within the substation separated and not accessible one from the other. In order to achieve this separation of traffic, different VLANs per service can be used. This way, different company departments will have access to their VLANs, and hence, only to the devices and equipment, under their own responsibility.
- **Critical Services.** The services running in an electrical substation may be different in importance. It is not the same to have IP telephony as it is to send orders to open a breaker. Using the quality of service feature for the different services allows electrical companies network architects to identify the critical services within the substation, warranting that all that traffic is treated with the adequate priority.
- **GOOSE management.** Above all the critical traffic in an IEC-61850 substation, you have the GOOSEs traffic, which can be tripping orders from protection relays. 3SWT is designed to treat that special traffic as its highest priority, so, even when the network is congested, a GOOSE will reach its destination in less than the time defined (4-10 ms depending on the performance class) in the IEC-61850 standard.

13.17.1.5 TPU-1 Universal teleprotection terminal

The modular design of TPU-1 terminals allows the use of different types of modules according to the teleprotection needs of each application. This modularity allows TPU-1 terminals to manage one or two digital and/or analog channels. In cases where the TPU-1 terminal manages two channels, it can be configured to operate as two independent teleprotection terminals (in a single shelf) or one teleprotection with main and back-up channels.

- TPU-1 terminals operating in analog channels can transmit and receive up to four teleprotection commands. TPU-1 terminals configured to operate in digital channels (with electrical or optical interface) enable two-way transmission of up to eight teleprotection commands.
- TPU-1 terminals are IEC 61850 compatibles, so communication between a TPU-1 and a protection device inside a substation can be carried out according to this standard (GOOSE messages). However, if a protection device is not compatible with IEC 61850 standard, TPU-1 terminals can also communicate with it using analog protection interfaces (relays).
- The TPU-1 terminals, furthermore, incluye an SNMP agent able to send notifications (unsolicited information spontaneously transmitted) about alarms and events of the terminal to the devices specified by the user, and this makes it possible to monitor the TPU-1 terminal from an SNMP management application, such as, HP Openview.
- All variables of the TPU-1 terminal that can be monitored are to be found in the MIB of the terminal, which can be integrated into the management platform.
- TPU-1 terminals comply with ANSI C37.90.1 and ANSI C37.90.2 standards.
- Management system Choose between integrated Web management with the possibility of a LAN connection or local management system based on a Web interface:
- Integrated Web management system DIMAT TPU-1 terminals are equipped with a Web server module integrating all HTML pages necessary for programming and monitoring, as well as Ethernet interfaces.

APPLICATIONS

TPU-1 terminals can be used in any type of application, providing the appropriate modules. Apart from the back-up channel and being able to protect two lines with a single TPU-1 terminal, other examples of useful and innovating applications are:

- **Mixed protection interfaces.** Provides simultaneous operation with analog protection interfaces and IEC 61850 protection interfaces, in order to simplify the migration to IEC 61850 in substations.
- **Transits.** Possibility of transiting teleprotection commands in T (Teed-line),

- **Telesignalling and remote measurements.** Possibility of transmitting and receiving analog measurements and digital signals, using the TPU-1 as an intertripping and remote measurements terminal in cogeneration applications.