For IEC use only

57/924/DC

2008-03-14

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Technical Committee 57: Power systems management and associated information exchange

Draft IEC TR 61850-90-1: Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations

1. Background

As documented in 57/790/RVN, the national committees had approved the new work item, to standardise the use of IEC 61850 for the communication between substations. The related project was originally registered as IEC 62445-1.

The work was allocated to WG10. Instead of being a standard by itself, the result of the work will have an impact on different parts of IEC 61850. Therefore, the working group decided to first issue a technical report that describes the different aspects and solutions to the problem and later, once the report is approved, to integrate the result into the relevant parts of IEC 61850.

In addition, TC57 decided that all work done by working groups of TC57 related to IEC 61850 shall receive a publication number within the IEC 61850 series. As a consequence, the number IEC 61850-90-1 was allocated to the technical report that is the result of that work that has originally been registered as IEC 62445-1 and is described above.

2. Action

This is a first draft of the future technical report IEC 61850-90-1. It is circulated in order to get a feedback from a wider range of experts than the ones in the working groups.

The TC57 P-members are invited to submit comments on this draft

by 2008-05-16 at the latest

to the IEC electronic voting system.

On the basis of the comments received WG 10 will revise the draft and circulate a DTR which will be published, in case of approval, as IEC TR 61850-90-1.

Annex: Draft of IEC TR 61850-90-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

USE OF IEC 61850 FOR THE COMMUNICATION BETWEEN SUBSTATIONS

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organisation for standardisation comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardisation in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organisations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organisation for Standardisation (ISO) in accordance with conditions determined by agreement between the two organisations.

2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.

3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61850 consists of the following parts, under the general title *Communication networks and systems for power utility automation*.

Part 1: Introduction and overview
Part 2: Glossary
Part 3: General requirements
Part 4: System and project management
Part 5: Communication requirements for functions and device models
Part 6: Configuration description language for communication in electrical substations related to IEDs
Part 7-1: Basic communication structure – Principles and models
Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)
Part 7-3: Basic communication structure – Common data classes
Part 7-4: Basic communication structure – Compatible logical node classes and data classes
Part 7-410: Hydroelectric power plants - Communication for monitoring and control
Part 7-420: Communications systems for distributed energy resources (DER) - Logical nodes
Part 7-500: Using logical nodes to model functions of a substation automation system
Part 7-510: Using logical nodes to model functions of a hydro power plant
Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
Part 9-1: Specific communication service mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link
Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3
Part 10: Conformance testing

Part 80-1: Guideline to exchange information from a CDC based data model using IEC 60870-5-101/104

Part 90-1: Using IEC 61850 for the communication between substations

Part 90-2: Using IEC 61850 for the communication between substations and control centres

The scope of IEC 61850 is not limited anymore to substations. This is reflected in the changed title of the series. New domain specific parts have been added to the series. TC57, WG10 is currently preparing the second edition of the basic parts from IEC 61850.

INTRODUCTION

When IEC 61850 was prepared, it was intended for the use of information exchange between devices of a substation automation system. In the mean time, the concepts are as well used in other application domains of the power utility system. Therefore, IEC 61850 is on the way, to become the foundation for a globally standardized utility communication network.

With existing and new applications in the field of the power system operation and protection, the requirement to exchange standardized information directly between substations increases. IEC 61850 shall be the basis for this information exchange.

IEC 61850 provides the basic features to be used for that information exchange, however, some extensions to IEC 61850 may be required. This technical report provides a comprehensive overview on the different aspects that need to be considered while using IEC 61850 for information exchange between substations. Areas that require extension of specific parts of the existing IEC 61850 standard will later be incorporated in future editions of the affected part of IEC 61850.

A similar report discussing the use of IEC 61850 for communication between substations and control centres is under preparation as IEC 61850-90-2. Further, a similar report discussing the use of IEC 61850 for wide-area RAS (Remedial Action Schemes) is being contemplated; this will likely be IEC 61850-90-3.

This is a first draft of the future technical report that is not considered to be complete. It is a first draft circulated among the national committees to get comments from a wider audience. There are still some issues within that draft that need further improvement.

In particular, in Annexe A, some additional concepts to address security and dependability issues related to Ethernet are presented where we would like to get the feedback from the national committees.

USE OF IEC 61850 FOR THE COMMUNICATION BETWEEN SUBSTATIONS

1 Scope

This technical report provides a comprehensive overview on the different aspects that need to be considered while using IEC 61850 for information exchange between substations. In particular, this technical report:

- defines use cases that require an information exchange between substations
- describes the communication requirements
- gives guidelines for the communication services and communication architecture to be used
- describes the related logical nodes
- describes the usage of the configuration language

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

tbd

3 Terms and definitions

For the purposes of this International Standard, the terms and definitions given in IEC 61850-2 and IEC 61850-7-2 apply.

4 Abbreviated terms

NOTE Abbreviations used for the identification of the common data classes and as names of the attributes are specified in the specific Clauses of this document and are not repeated here.

5 Use cases

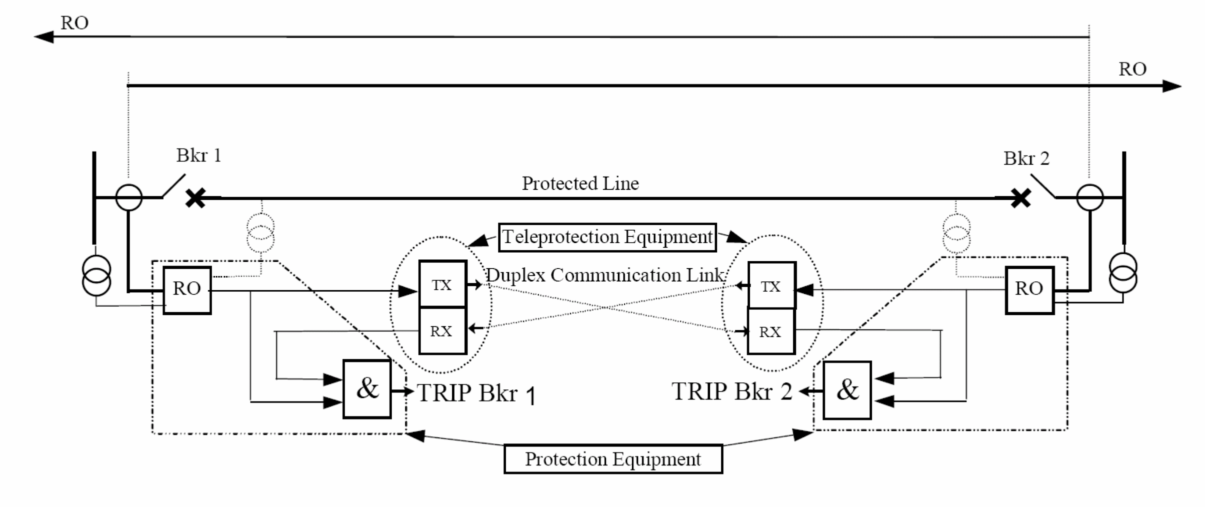
For the purpose of communication between substations, the following functions are considered.

Conventional CTs and VTs are assumed for input to relays in the following use cases. However, they could be replaced by newer technology, such as digital input based on process bus, without any significant change in the descriptions.

5.1 Distance line protection with permissive tele-protection scheme

5.1.1 Summary

When a distance relay detects a forward fault, it sends a permissive signal to the remote end. If the relay also receives a permissive signal (from the remote end), the relay sends a trip signal to the local CB.



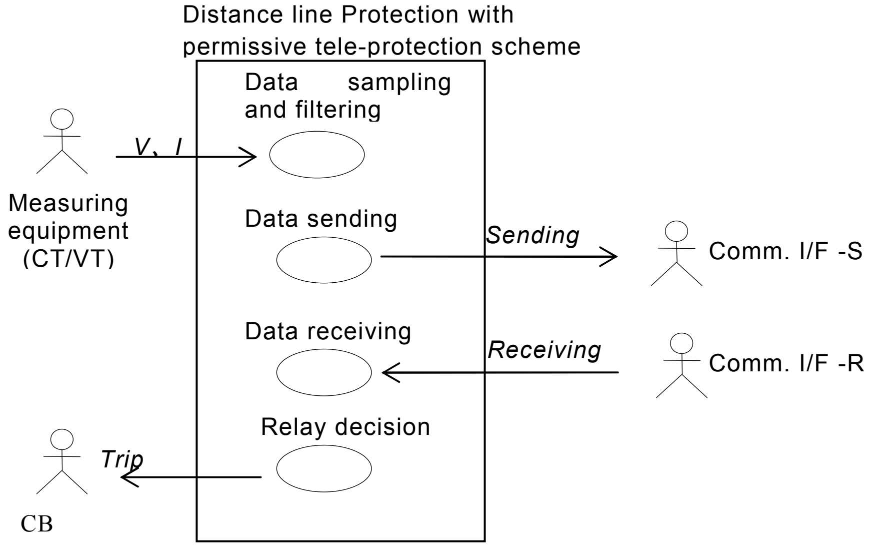
RO - overreaching trip function, must be set to reach beyond remote end teminal

Figure 1: Distance line protection with permissive overreach tele-protection scheme [1]

5.1.2 Constraints / Assumptions / Design Considerations

- The permissive signal needs a minimum of 1 bit. If it is a phase segregated signal it needs 3 bits. If it is a phase segregated, and phase-to-phase and phase-to-earth are independent, the signal needs 6 bits. Directional earth fault detection may need another 1 bit.
- Data is sent only when a forward fault is detected
- For communication channel failure alternative actions must be considered
- A small propagation delay is needed for fast tripping (e.g.: 5ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.1.3 Use case diagram


Distance line Protection with permissive tele-protection scheme
Data sampling and filtering
V, I
Measuring equipment (CT/VT)
Data sending
Sending
Comm. I/F -S
Data receiving
Receiving
Comm. I/F -R
Relay decision
Trip
CB

5.1.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from protected line
Comm. I/F –S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from other system (Circuit Breaker)

5.1.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from Measuring equipment and filter them
Data sending	Calculates a distance to the fault using filtered data. When a distance protection detects a forward fault the distance protection sends the permissive signal to Comm. I/F –S (the remote end).
Data receiving	Receives the permissive signal from Comm. I/F –R (the remote end).
Relay decision	When the distance protection detects the forward faults and receives permissive signal from remote end, the distance protection issues a trip command to the CB

5.1.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current and Voltage are given to Distance protection by Measuring equipment
Step 2	Distance Protection samples an analogue value and converts it to digital data
Step 3	Distance Protection removes any unwanted frequency components from the sampled data using a digital filter

Data sending

Use Case Step	Description
Step 1	Distance Protection stores the filtered instantaneous data
Step 2	Distance Protection calculates a distance to the fault using filtered data.
Step 3	When a distance protection detects a forward fault to a pre-determined distance, a distance protection sends the permissive signal to Comm. I/F –S (in order to send the data to a remote end relay)
Step 4	Comm. I/F –S send the information to remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to Distance Protection
Step 2	Distance Protection receives the data

Relay Decision

Use Case Step	Description
Step 1	When the distance protection detects the forward faults in a predetermined zone, and receives a permissive signal from the remote end, the distance protection issues a trip command to the CB

5.2 Distance line protection with blocking tele-protection scheme

5.2.1 Summary

When a distance relay detects reverse faults, it sends a blocking signal to the remote end. If the relay detects a forward fault and does not receive the blocking signal the relay sends a trip signal to the local CB.

The variant Directional Comparison Blocking (DCB) may use a non-directional element to send a blocking signal for any fault (in other words: “starts the carrier”). The operation of the forward element removes the blocking signal (“stops the carrier”) and sends a trip signal to the local CB.

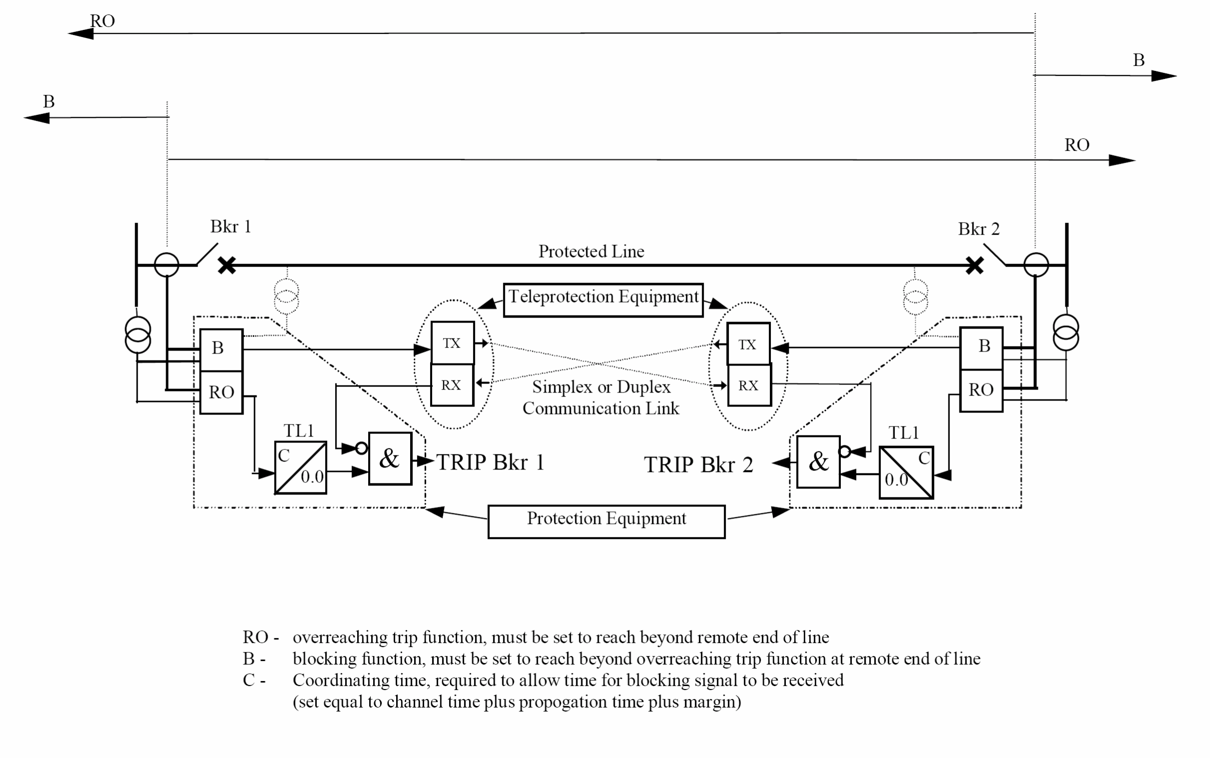
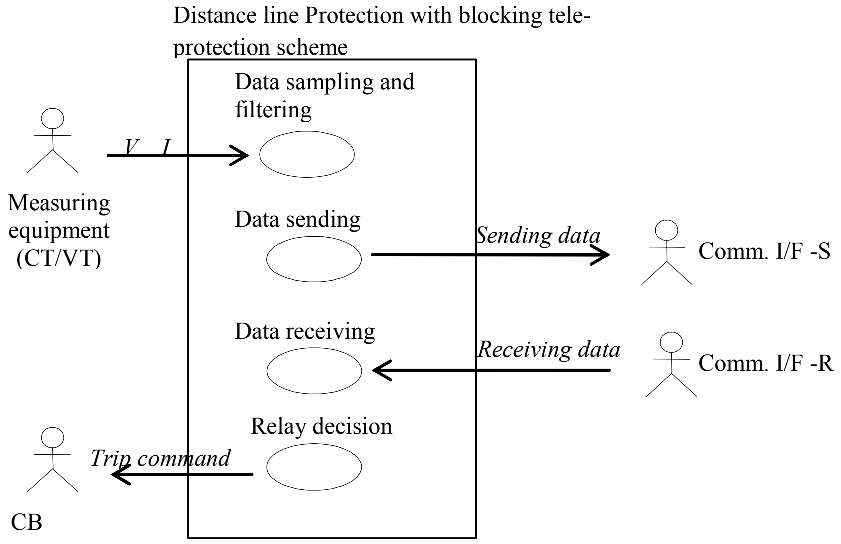

RO
B
B
RO
Bkr 1
Bkr 2
Protected Line
Teleprotection Equipment
B
RO
TX
RX
TX
RX
B
RO
Simplex or Duplex
Communication Link
TL1
C
0.0
&
TRIP Bkr 1
TRIP Bkr 2
&
TL1
C
0.0
Protection Equipment
RO - overreaching trip function, must be set to reach beyond remote end of line
B - blocking function, must be set to reach beyond overreaching trip function at remote end of line
C - Coordinating time, required to allow time for blocking signal to be received
(set equal to channel time plus propogation time plus margin)

Figure 2: Distance line protection with blocking tele-protection scheme [1]

5.2.2 Constraints / Assumptions / Design Considerations:

- The blocking signal is a minimum of 1 bit. If it is phase segregated signal it needs 3 bits. If it is phase segregated, and phase-to-phase and phase-to-earth are independent, the signal needs 6 bits. Directional earth fault detection may need another 1 bit.
- Data is sent when a reverse fault is detected or as a variant, when any fault is detected. In that variant the blocking signal is removed when the fault direction is detected as forward.
- For communication channel failure the blocking signal is typically removed
- A small propagation delay is needed for fast tripping (e.g.: 5ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.2.3 Use case diagram


Distance line Protection with blocking tele-protection scheme
Data sampling and filtering
V I
Measuring equipment (CT/VT)
Data sending
Sending data
Comm. I/F -S
Data receiving
Receiving data
Comm. I/F -R
Relay decision
Trip command
CB

5.2.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from the protected line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from the other system (Circuit Breaker)

5.2.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from the Measuring equipment and filters them
Data sending	Calculates a distance to the fault using filtered data. When a distance protection detects a reverse fault the distance protection sends the blocking signal to Comm. I/F –S (the remote end).
Data receiving	Receives the blocking signal from Comm. I/F –R (the remote end).
Relay decision	When the distance protection detects the forward faults, and does ***not*** receive a blocking signal from the remote end, the distance protection issues a trip command to the CB

5.2.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current and Voltage are given to Distance protection by the Measuring equipment
Step 2	Distance Protection samples an Analogue value, and converts it to digital data
Step 3	Distance Protection removes the unwanted frequency component from the sampled data using a digital filter

Data sending

Use Case Step	Description
Step 1	Distance Protection stores the filtered instantaneous data
Step 2	Distance Protection calculates a distance to the fault using filtered data.
Step 3	When a distance protection detects a reverse fault in a pre-determined distance, it sends a blocking signal to Comm. I/F –S (in order to send the data to a remote end relay)
Step 4	Comm. I/F –S sends the information to remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to Distance Protection
Step 2	Distance Protection receives the data

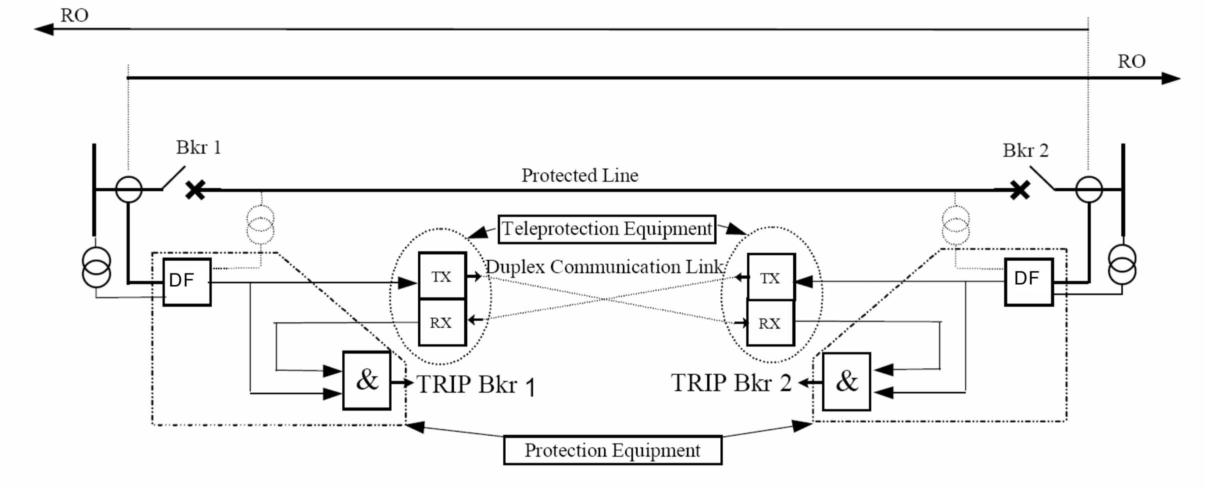
Relay Decision

Use Case Step	Description
Step 1	When the distance protection detects a forward fault in a predetermined zone, and does ***not*** receive a blocking signal from the remote end, the distance protection issues a trip command to the CB

5.3 Directional comparison protection

5.3.1 Summary

When a directional relay (typically a directional overcurrent relay) detects a forward fault, the relay sends a permissive signal to the remote end. If the relay also receives a permissive signal from the remote end, the relay sends a trip signal to the local CB.



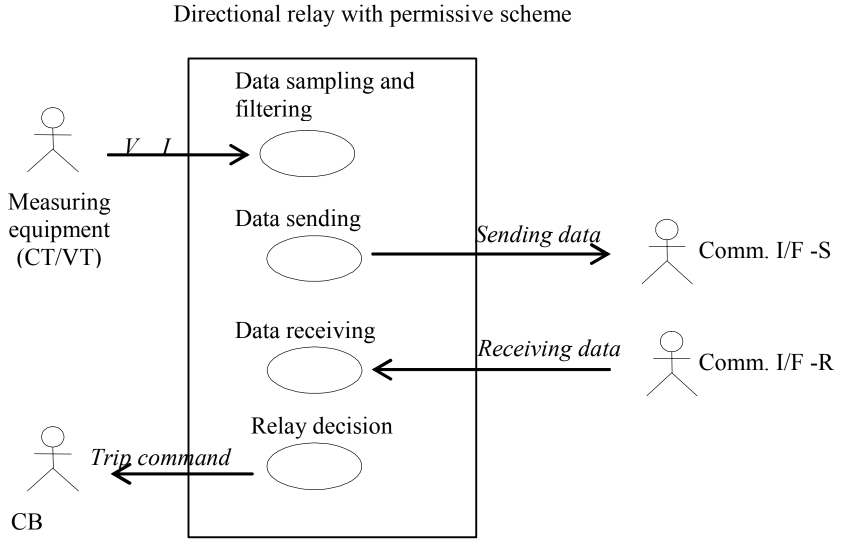
DF: Directional relay to detect forward faults

Figure 3: Directional comparison with permissive scheme

5.3.2 Constraints / Assumptions / Design Considerations

- The permissive signal is a minimum of 1 bit. If it is phase segregated the signal needs 3 bits. If it is phase segregated and phase-to-phase and phase-to-earth are independent, the signal needs 6 bits. Directional earth fault detection may need another 1 bit.
- Data is sent only when a forward fault is detected
- For communication channel failure alternative actions must be considered
- A small propagation delay is needed for fast tripping (e.g.: 5ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.3.3 Use case diagram



5.3.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from a protected line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from another system (Circuit Breaker)

5.3.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from the Measuring equipment, and filters them
Data sending	Calculates the direction of the fault. When a directional relay detects a forward fault the relay sends a permissive signal to Comm. I/F –S (the remote end).
Data receiving	Receives the permissive signal from Comm. I/F –R (the remote end).
Relay decision	When the directional relay detects a forward fault and receives a permissive signal from remote end, the directional relay issues a trip command to the CB.

5.3.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current and Voltage are given to directional relay by the Measuring equipment
Step 2	Directional relay samples an Analogue value and converts it to digital data
Step 3	Directional relay removes the unwanted frequency components from the sampled data using a digital filter

Data sending

Use Case Step	Description
Step 1	Directional relay stores the filtered instantaneous data
Step 2	Directional relay calculates a direction of the fault using filtered data.
Step 3	When a directional relay detects a forward fault, the relay sends the permissive signal to Comm. I/F –S (in order to send the data to the remote end relay)
Step 4	Comm. I/F –S sends the information to remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to the Directional relay
Step 2	Directional relay receives the data

Relay Decision

Use Case Step	Description
Step 1	When the directional relay detects a forward fault and receives a permissive signal from the remote end, the relay issues a trip command to the CB

5.4 Transfer/Direct Tripping

5.4.1 Summary

Local equipment sends a trip command to the remote equipment. This function is sometimes called inter-tripping as well.

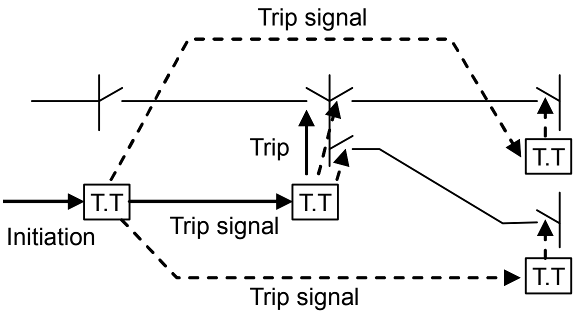
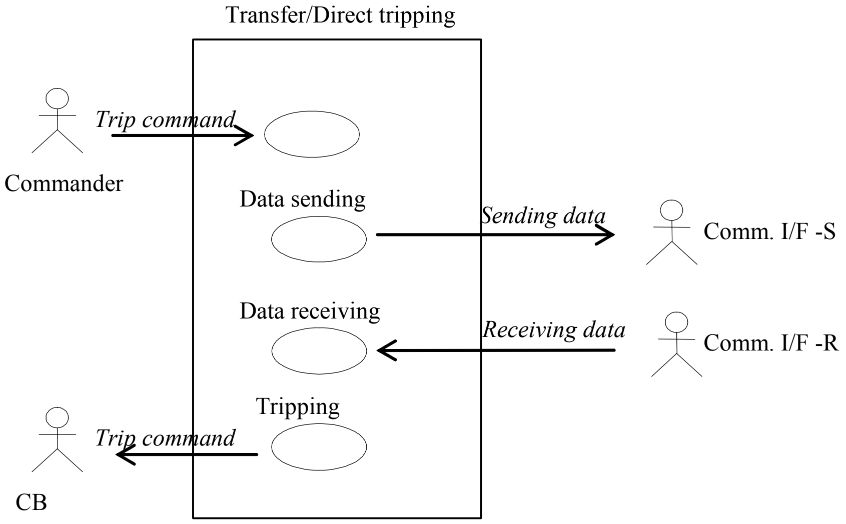


Figure 4: Transfer/Direct Tripping

5.4.2 Constraints / Assumptions / Design Considerations

- The trip signal is a minimum of 1 bit. If it is phase segregated signal it is 3 bits. If the quantity of remote equipments is more than one, more bits may be needed for the signal
- Data is sent only if a trip command is issued
- For communication channel failure alternative actions must be considered
- A small propagation delay is needed for fast tripping (e.g.: 5ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.4.3 Use case diagram



5.4.4 Actor(s)

Name	Role description
Commander	Requests local equipment to send a trip command to the remote equipment
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the line from the other system (Circuit Breaker)

5.4.5 Use Case(s)

Name	Services or information provided
Trip command issuing	Issues a trip command to the local equipment
Data sending	Sends the trip command to Comm. I/F –S (the remote end).
Data receiving	Receives the trip command from Comm. I/F –R.
Tripping	Sends the trip command to the CB

5.4.6 Basic Flow

Trip command issuing

Use Case Step	Description
Step 1	Issues the trip command to local equipment
Step 2	Local equipment receives the trip command

Data sending

Use Case Step	Description
Step 1	Local equipment sends the trip command to Comm. I/F –S (in order to send the data to the remote equipment)
Step 2	Comm. I/F –S sends the information to the remote end

Data receiving

Use Case Step	Description

Step 1	Comm. I/F –R gives the received command to the remote equipment
Step 2	Remote equipment receives the data

Tripping

Use Case Step	Description
Step 1	Remote equipment sends a trip command to the CB

5.5 Interlocking

5.5.1 Summary

The interlocking of the line earth switch depends on whether there is voltage on the line or not. To be able to detect this, the states of the earthing switch, and the line disconnector switch of the other line side, should be transferred and used; making a local voltage measurement, which is also unreliable, superfluous.

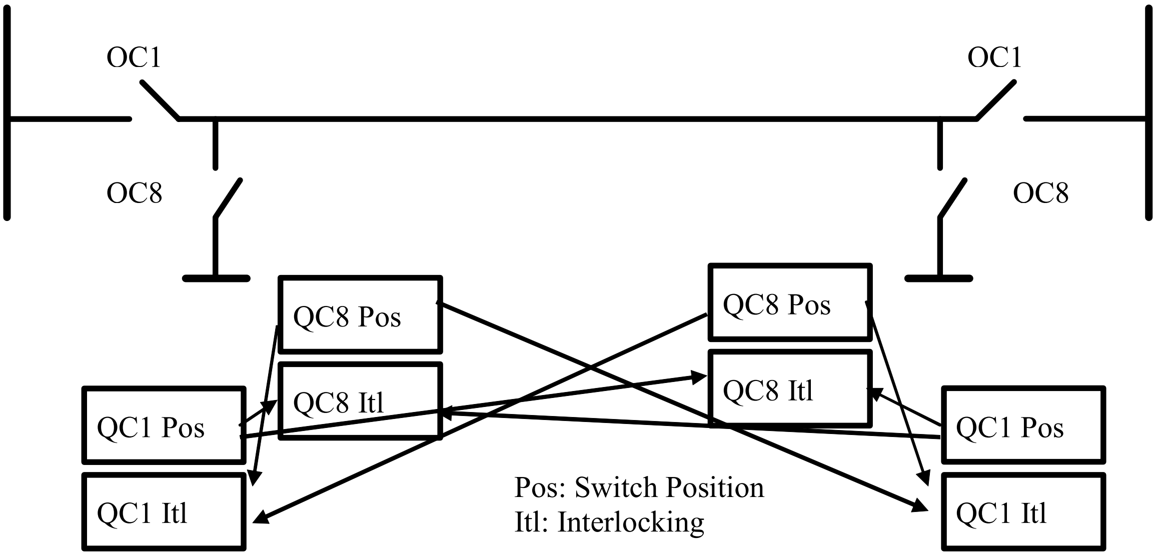
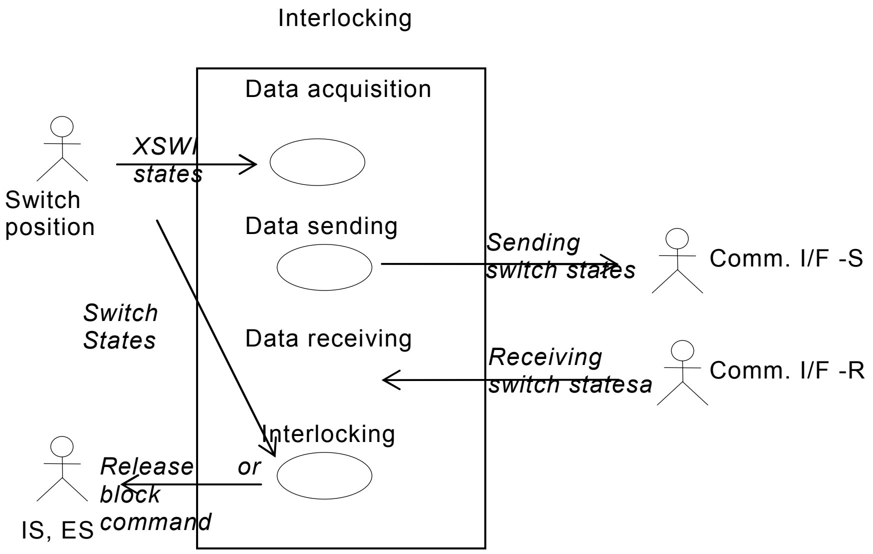


Figure 5: Interlocking – Interoperation

5.5.2 Constraints / Assumptions / Design Considerations

- Timing requirements: <= 100 ms
- Frequency of use: each switch state change is sent.
- Sizing characteristics: two switch states (maximum: all switch states of the other side, i.e. around 10 switch states).
- Communication channel failure can be considered as intermediate or failed switch state

5.5.3 Use Case Diagram



The Use Case Diagram applying to Process Control System is shown as a figure.

5.5.4 Actor(s)

Name	Role description
Switch state acquisition equipment	Switch states from line, at least earth switch and line disconnector
Comm. I/F -S	Receives data from the local acquisition, and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local interlocking controller
Interlocking controller	Uses remote switch states for local interlocking logic

5.5.5 Use Case(s)

Name	Role description
Switch state acquisition	Acquires switch states from the line, at least the earth switch and the line disconnector
Data sending	Receives data from the local acquisition, and sends the data to the remote end
Data receiving	Receives data from the remote end, and gives the data to the local interlocking controller
Interlocking calculation	Uses remote switch states for local interlocking logic

5.5.6 Basic Flow

Use Case Step	Description
Step 1	Acquires switch states from the line, at least earth the switch and the line disconnector
Step 2	Receives data from the local acquisition and sends the data to the remote end
Step 3	Receives data from the remote end and gives the data to the local interlocking controller
Step 4	Uses the remote switch states for local interlocking logic

5.5.7 Pre-conditions

None.

5.5.8 Post-conditions

Correct interlocking - no line disconnector closes on earthed line, no earthing switch closes on active (disconnector closed) line.

5.6 Multi-phase auto-reclosing application for parallel line systems

5.6.1 Summary

Multi-phase auto-reclosing (1-phase, 2-phase, 3phase) is a scheme that is applied to the double line circuit. In multi-phase auto-reclosing applications the scheme decides its actions based on CB status of the remote end (not usually used for other auto-reclosing methods).

This use case focuses on how to use or how to transmit CB status information for multi-phase auto-reclosing. Normal auto-reclosing processes (e.g. checking dead time etc.) are omitted in the explanation.

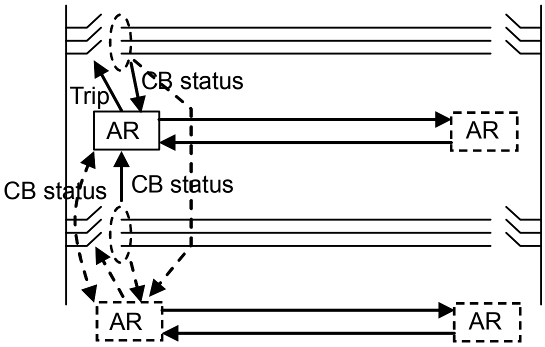
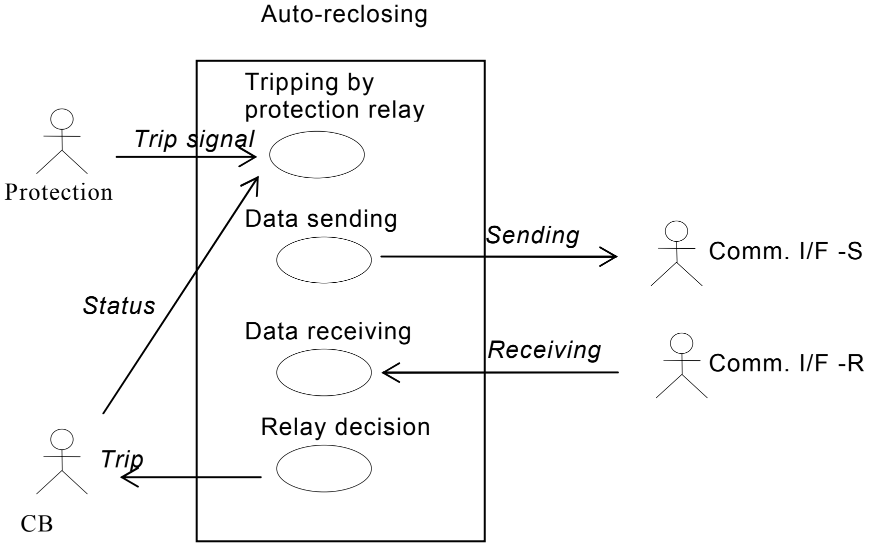


Figure 6: Auto-reclosing

5.6.2 Constraints / Assumptions / Design Considerations

- The CB status needs 3 bits or 6 bits
- Small propagation delay is preferred for quick operation (e.g.: 10ms)
- A high reliability is needed
- For communication channel failure alternative actions must be considered

5.6.3 Use case diagram



5.6.4 Actor(s)

Name	Role description
Protection relay	Gives the tripping information to the auto-reclosing scheme
Comm. I/F –S	Receives data from the local relay and sends the data to the remote end
Comm. I/F –R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from another system (Circuit Breaker)

5.6.5 Use Case(s)

Name	Services or information provided
Tripping by protection relay	Protection relay trips faulted phase, and gives that information to the auto-reclosing scheme Local CBs in protected line and in the parallel line give their status to the auto-reclosing scheme
Data sending	Sends the local CB status to Comm. I/F-S
Data receiving	Receives the remote CB status from Comm. I/F –R
Relay decision	If the auto-reclosing scheme decides to trip other phases, it sends a trip signal to the local CB

5.6.6 Basic Flow

Data sending

Use Case Step	Description
Step 1	Auto-reclosing scheme sends the local CB status to Comm. I/F –S (in order to send the data to the remote end relay) Auto-reclosing scheme also passes the information to the auto-reclosing scheme of the parallel line to share the information.
Step 2	Comm. I/F –S sends the information to the remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R give the received data to auto-reclosing scheme
Step 2	Auto-reclosing scheme receives the data from comm. I/F-R and from the Auto-reclosing scheme of the parallel line.

Tripping by protection relay

Use Case Step	Description
Step 1	If a fault occurs in the protected line, a protection relay trips the faulted phase and gives the trigger to start the auto-reclosing scheme to the auto-reclosing scheme of the protected line and of the other line located in the local substation.
Step 2	Auto-reclosing scheme receives the data

Relay Decision

Use Case Step	Description
Step 1	By using the CB status of both ends of both lines, the auto-reclosing scheme checks which phases are alive. The auto-reclosing scheme decides whether other phases must be tripped, or if the relay just continues to count up dead time by comparing the auto-reclosing conditions with the information of alive phases (*1).
Step 2	If the auto-reclosing scheme decides to trip other phases, it sends a trip signal to the local CB

(*1) More details are explained in the reference [1].

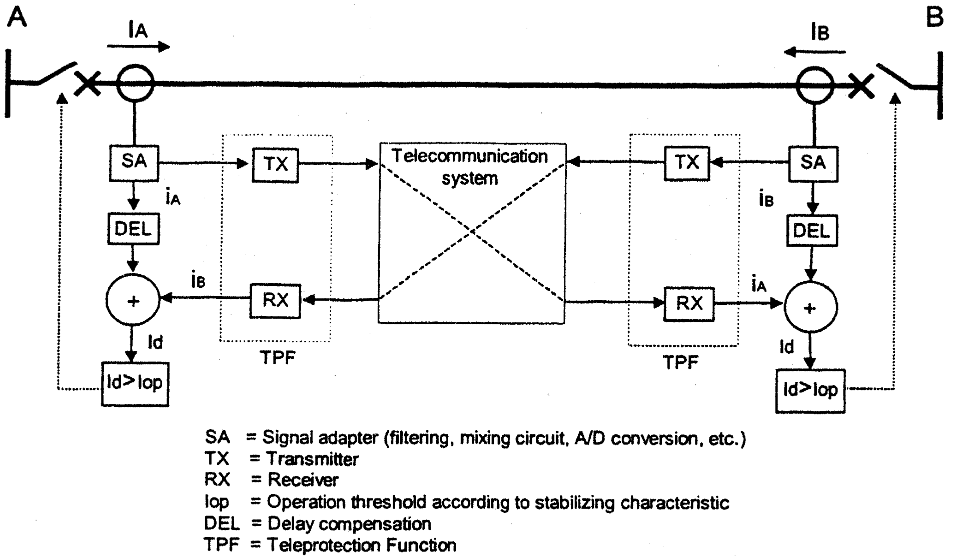
5.6.7 References

[1] K.Kasuga, Y.Sonobe “Multi-phase Autoreclose Function Installed in Line Differential Relay”, 61st Annual Georgia Tech Protective Relaying Conference, May 2-4, 2007, Atlanta, Georgia

5.7 Current differential line protection

5.7.1 Summary

Current differential relays measure the current of the protected line at both ends. A local relay sends the current data (I_A) to the remote end and receives the current data from the remote end (I_B). Current differential relays detect faults in the protected line (internal faults) by comparing the current from the remote relay with the current of the local terminal. When current differential relays detect an internal fault, they send a trip signal to the local circuit breaker.



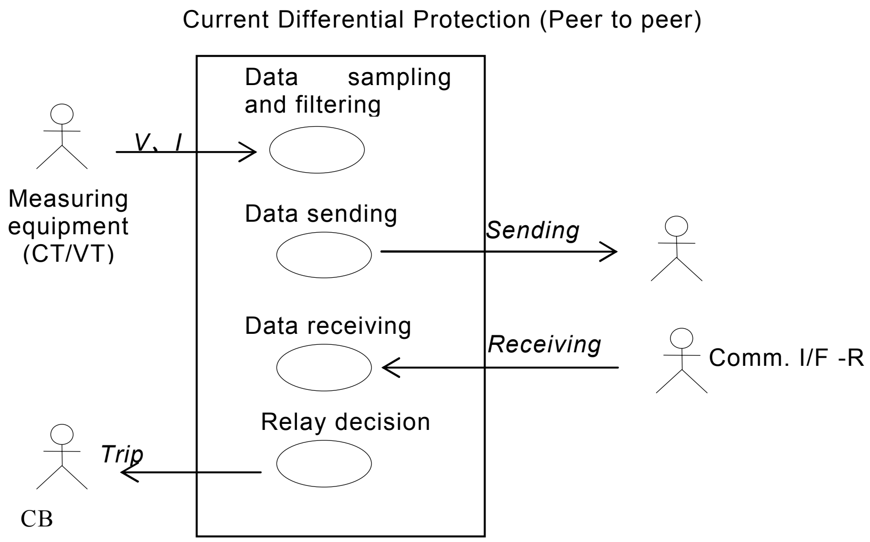
SA = Signal adapter (filtering, mixing circuit, A/D conversion, etc.)
TX = Transmitter
RX = Receiver
Iop = Operation threshold according to stabilizing characteristic
DEL = Delay compensation
TPF = Teleprotection Function

Figure 7: Current differential line protection [1]

5.7.2 Constraints / Assumptions / Design Considerations

- Representation of measured currents and any additional information
- Data must be synchronised between substations (e.g. less than 0.1 ms)
- Continuous data exchange (e.g. 12 data per power cycle)
- Enough data bandwidth to transmit three phase current data, additional information and, if applied, residual current data (e.g. 64 kbps)
- Communication channel failure typically blocks the current line differential protection
- A small propagation delay is needed for fast tripping (e.g. 5 ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.7.3 Use case diagram


Current Differential Protection (Peer to peer)
Data sampling and filtering
V、I
Measuring equipment (CT/VT)
Data sending
Sending
Data receiving
Receiving
Comm. I/F -R
Relay decision
Trip
CB

5.7.4 Actor(s)

Name	Role description
Measuring equipment	Measures current (and voltage) from protected line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from other system (Circuit Breaker)

5.7.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples the current (and voltage) data from the Measuring equipment and filters them
Data sending	Stores the filtered instantaneous data. Sends the sampled data to Comm. I/F –S (the remote end).
Data receiving	Receives the sampled current data from Comm. I/F –R (the remote end).
Relay decision	Calculates the differential current etc. If a fault in the protected line is detected, a trip command is issued to the CB

5.7.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current (and Voltage, when charging current compensation is needed) are given to the Current differential protection by the Measuring equipment
Step 2	Current Differential Protection samples an Analogue value and converts it to digital data
Step 3	Current Differential Protection removes the unwanted frequency components from the sampled data using a digital filter

Data sending

Use Case Step	Description
Step 1	Current Differential Protection stores the filtered instantaneous data
Step 2	Current Differential Protection puts the filtered instantaneous data to the sending data format with other information bits
Step 3	Current Differential Protection gives the sending data to Comm. I/F –S (in order to send the data to remote end relay)
Step 4	Comm. I/F –S sends the information to remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to the Current Differential Protection
Step 2	Current Differential Protection stores the received instantaneous data

Relay Decision

Use Case Step	Description
Step 1	Current Differential Protection calculates the differential current and the restraining current, using local data and remote end data which were sampled at the same time
Step 2	Current Differential Protection judges whether a fault exists in the protected line or not by comparing the calculated value with a threshold.
Step 3	When Current Differential Protection judges that a fault exists in the protected line, Current Differential Protection sends a trip command to the local CB

5.7.7 Pre-conditions

Synchronisation of the data between current differential relays must be established.

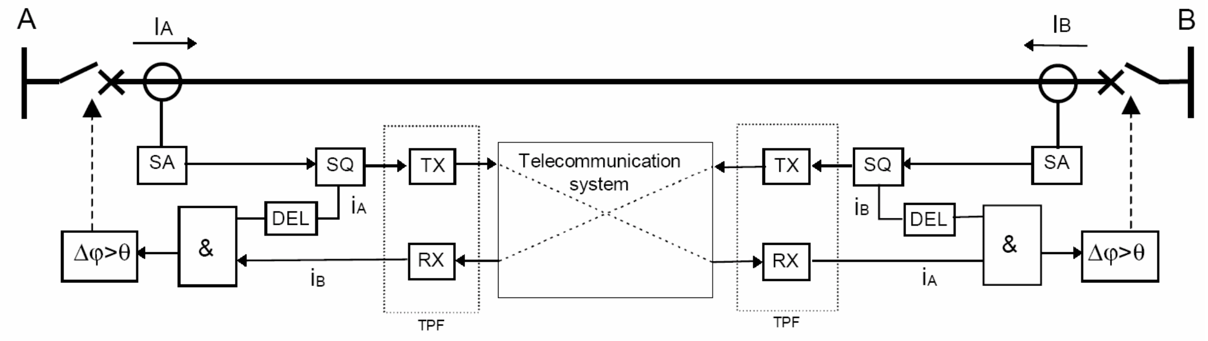
5.7.8 References

[1] Protection Using Telecommunication, CIGRE JWG 34/35.11

5.8 Phase Comparison Protection

5.8.1 Summary

When a phase comparison relay detects a positive current, the relay sends an “on” signal to the remote end. The relay compares the local data signal with that from the remote end. If the time that both signals are “on” is very short, the phases of the currents detected by both ends are opposite and the relay restrained. If the time is sufficiently long the relay recognises there is an internal fault and sends a trip signal to the local CB.



SA = Signal adapter (mixing circuit, filtering, etc.)
SQ = Squarer
TX = Transmitter
RX = Receiver
DEL = Delay compensation
Δφ = Coincidence angle
θ = Stabilizing angle
& = Logical AND
TPF = Teleprotection Function

Figure 8: Phase comparison protection

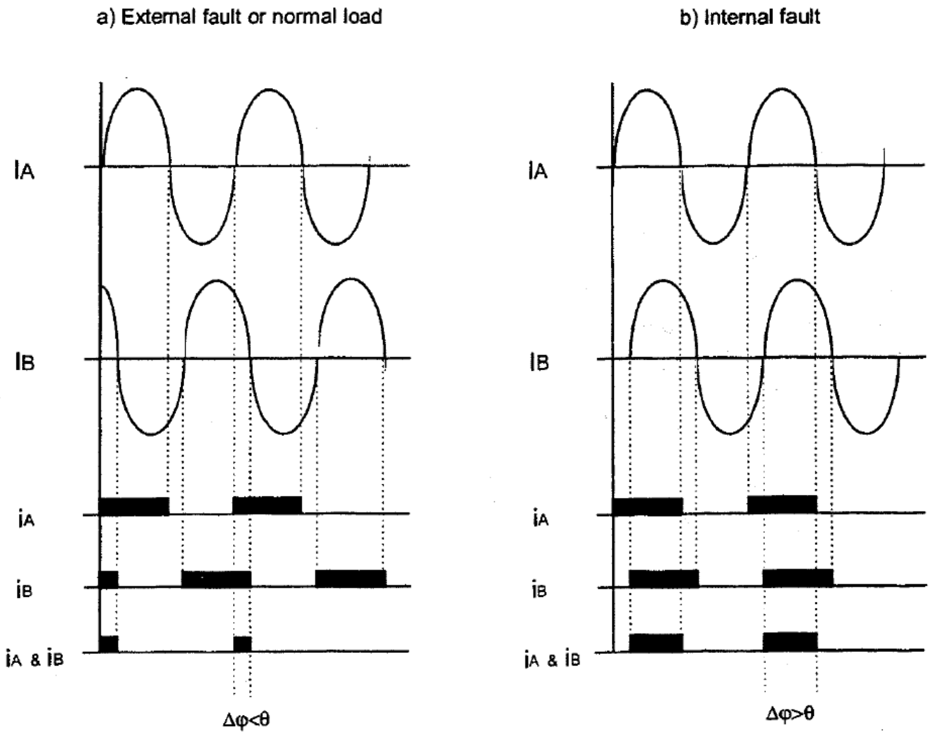
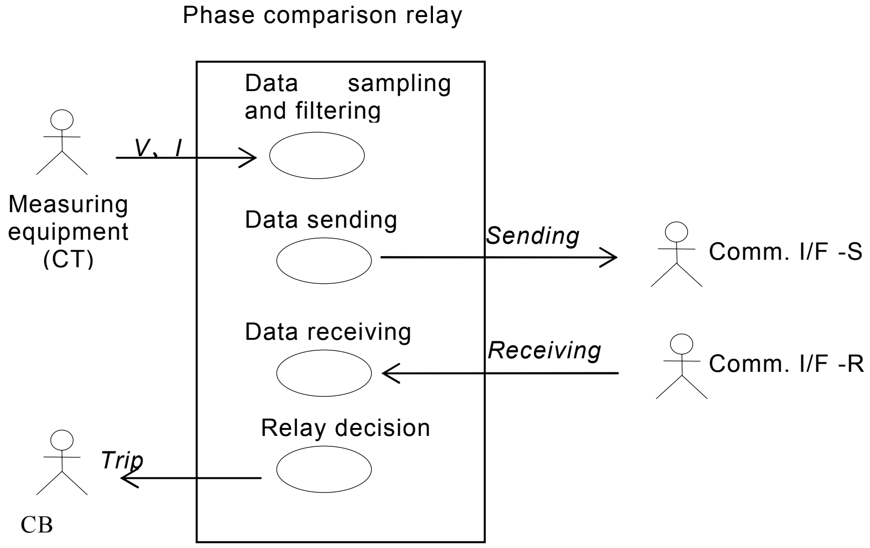


Figure 9: Principle to detect internal fault by phase comparison

5.8.2 Constraints / Assumptions / Design Considerations

- The “on” signal is a minimum of 1 bit. If it is a phase segregated signal it needs 3 bits. If the residual current phase comparison is an independent signal, it may need another 1 bit.
- The “on” signal is sent when the detected current is positive
- Communication channel failure typically results in an “on” signal being delivered to the local phase comparison function
- A small propagation delay is needed for fast tripping (e.g. 5 ms)
- A high reliability is needed (e.g. BER less than 10-6, Alternative route, Duplicated)

5.8.3 Use case diagram



5.8.4 Actor(s):

Name	Role description
Measuring equipment	Measures current from the protected line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from another system (Circuit Breaker)

5.8.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current from the Measuring equipment, and filters them
Data sending	Checks whether the current is positive or negative. When the current is positive the phase comparison relay sends the “on” signal to Comm. I/F –S (the remote end).
Data receiving	Receives the signal from Comm. I/F –R (the remote end).
Relay decision	The phase comparison relay compares the local signal with the signal from the remote end. If the time that both signals are on is not long enough, the relay issues a trip command to the CB

5.8.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current is given to the phase comparison relay by the Measuring equipment
Step 2	The relay samples the Analogue value and converts it to digital data
Step 3	The relay removes the unwanted frequency components from the sampled data using a digital filter

Data sending

Use Case Step	Description
Step 1	Phase comparison relay stores the filtered instantaneous data
Step 2	The relay checks whether the current is positive or negative..
Step 3	When the relay detects that the current is positive it sends the “on” signal to Comm. I/F –S (in order to send the data to the remote end relay) and to the local time delay compensation circuit.
Step 4	Comm. I/F –S sends the information to the remote end
Step 5	A local time delay compensation circuit compensates the propagation delay according to a predetermined setting, to adjust the local data to the data from the remote end. It passes the data to the decision circuit.

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to the phase comparison relay
Step 2	The relay receives the data

Relay Decision

Use Case Step	Description
Step 1	The phase comparison relay compares the local signal with the signal from the remote end. If the time that both signals are on is not long enough, the relay issues a trip command to the CB

5.9 Other applications

There are other applications of which the requirement for communication is almost the same as the requirement for current differential protection. Examples of the applications are as follows.

- Fault locator system (typically 2 or 3 terminals)
- System Integrity Protection Schemes (SIPS)
- Real time predictive type generator shedding
- Out-of-step detection
- Remedial Action Schemes (RAS)
- Synchrophasors from Phasor Measurement Units (PMUs)

The typical requirements for these applications are:

- Representation of measured currents and/or voltages and any additional information
- Data must be synchronised between substations (e.g. less than 0.1 ms)
- Continuous data exchange
- Enough data bandwidth to transmit three phase current and/or voltage data and additional information (e.g. 64 kbps)
- For communication channel failure alternative actions must be considered
- Propagation delay depending on the application, mostly critical e.g. 5 ms
- High reliability is needed (e.g. BER less than 10^{-6}, Alternative route, Duplicated)

Details of each application are explained in the following subsections.

5.9.1 Fault locator system (2 and/or 3 terminals)

5.9.1.1 Summary

By using all terminal information, precise estimation of the fault location is possible. The voltages and currents of all ends are necessary.

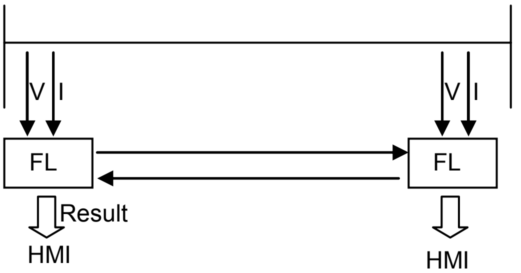
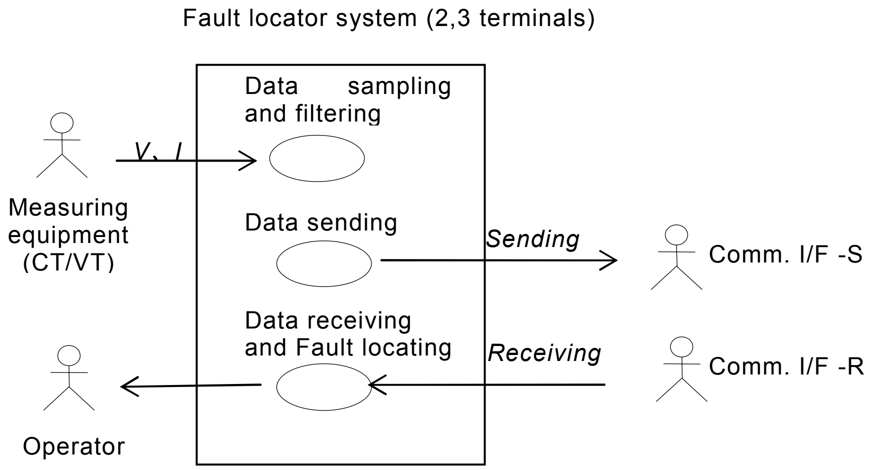


Figure 10: Fault locator system (2 and/or 3 terminals)

5.9.1.2 Constraints / Assumptions / Design Considerations

- Representation of measured currents and voltages and any additional information
- The propagation delay is not critical for fault locator calculation
- Communication channel failure may result in the fault locator calculation with data only from the local line end
- Other constraints see section 5.9

5.9.1.3 Use case diagram


Fault locator system (2,3 terminals)
Data sampling and filtering
V、I
Measuring equipment (CT/VT)
Data sending
Sending
Comm. I/F -S
Data receiving and Fault locating
Receiving
Comm. I/F -R
Operator

5.9.1.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from the line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay

5.9.1.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from the Measuring equipment, and filters them
Data sending	Sends the sampled data to Comm. I/F –S (to the Central computer).
Data receiving and fault location calculation	Receives the sampled data from Comm. I/F –R (from the Network computing terminal).

5.9.1.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Currents and Voltages are given to the local terminal by the Measuring equipment
Step 2	A network computing terminal samples the Analogue values and converts them to digital data

Data sending

Use Case Step	Description
Step 1	When a fault occurs, the local terminal freezes the sampled data. Typically the frozen data is measured from a few cycles before the fault until about 10 cycles after the fault
Step 2	The local terminal sends the frozen data to Comm. I/F –S (in order to send the data to the remote end)
Step 3	Comm. I/F –S sends the information to the remote end

Data receiving and fault locating

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to the local terminal
Step 2	The local terminal receives the data
Step 3	The local terminal estimates the location the fault. It shows and stores the result.

5.9.1.7 Pre-conditions

Synchronisation of the data between the relays must be established.

5.9.2 System Integrity Protection Schemes (SIPS)

5.9.2.1 Summary

The described system integrity protection scheme comprises Remote Terminals and a Central Equipment. Remote Terminals are located at power stations and measure voltage. These Remote Terminals periodically send measured data to the Central Equipment. The central unit calculates the differences of the voltage angles between the western generators and the other generator groups (northern group, eastern group and south-eastern group), and also estimates the future angle differences. If the central unit predicts that the generators will lose synchronisation, the central unit sends a trip signal to the circuit breaker of the tie line.

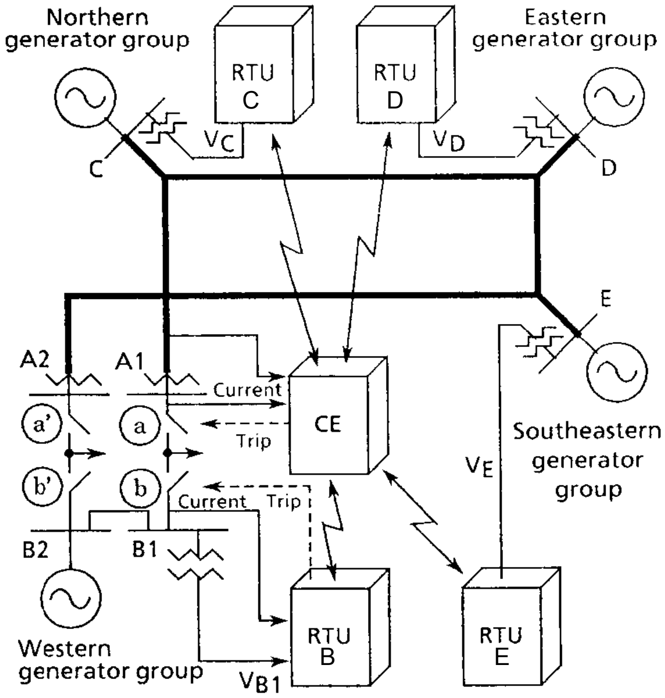
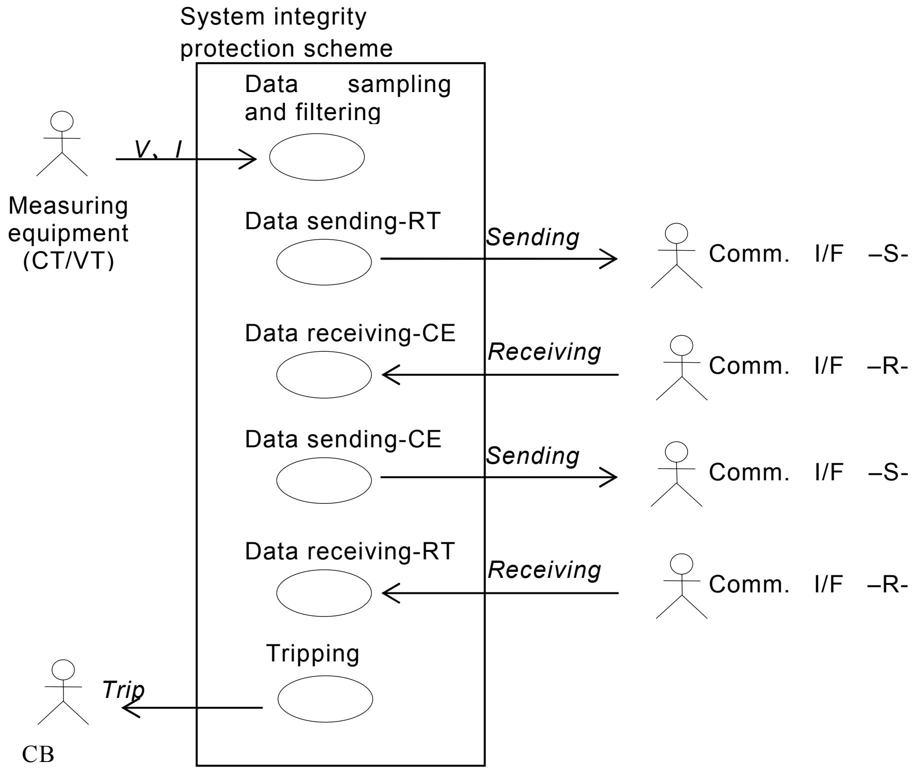


Figure 11: Example of a System Integrity Protection Scheme [7]

5.9.2.2 Constraints / Assumptions / Design Considerations

- Representation of measured currents and voltages and any additional information
- A small propagation delay is needed for fast tripping (e.g.: 5 ms)
- Communication channel failure may block the SIPS
- Other constraints see section 5.9

5.9.2.3 Use case diagram



5.9.2.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from the protected line
Comm. I/F –S-RT	Receives sampled data from the Remote Terminal and sends the data to the Central Equipment
Comm. I/F –R-RT	Receives trip command from Comm. I/F –S-CE (the Central Equipment) and passes the command to the Remote Terminal
Comm. I/F –R-CE	Receives sampled data from Comm. I/F –S-RT (the Remote Terminal) and passes the data to the Central Equipment
Comm. I/F –S-CE	Receives a trip command from the Central Equipment and sends the command to the Remote Terminal
CB	Disconnects the tie line, which is connected to the western generators, with other generator groups (Circuit Breaker)

5.9.2.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from the Measuring equipment and filters them
Data sending-RT	Sends the sampled data and information bits to Comm. I/F –S (to the Central Equipment).
Data receiving-CE	Receives the sampled data and information bits from Comm. I/F –R (from the Remote Terminal).
Data sending-CE	Sends the trip information from Comm. I/F –R (to the Remote Terminal).
Data receiving-RT	Receives the trip information from Comm. I/F –R (from the Central Equipment).
Tripping	According to the trip information from the Central Equipment, the Central Equipment and/or Remote Terminal issues a trip command to the CB

5.9.2.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Voltage is given to Remote Terminals by Measuring equipment Current is given to Central Equipment by Measuring equipment
Step 2	Remote terminal and Central Terminal samples an Analogue value and converts it to digital data
Step 3	Remote terminal and Central Equipment removes the unwanted frequency components from the sampled data, using a digital filter

Data sending -RT

Use Case Step	Description
Step 1	Remote terminal put the sampled voltage data to sending data format with other information bits
Step 2	Remote terminal sends the data to Comm. I/F –S-RT (in order to send the data to Central Equipment)
Step 3	Comm. I/F –S-RT sends the information to the Central Equipment

Data receiving -CE

Use Case Step	Description
Step 1	Comm. I/F –R-CE gives the received data to the Central Equipment
Step 2	Central Equipment receives the data

Data sending -CE

Use Case Step	Description
Step 1	Central Equipment executes a calculation for the angle difference prediction between the western generator group and the other generator groups
Step 2	If the Central Equipment predicts that the generators will go to out-of-step, the Central Equipment sends a trip command to the Comm. I/F –S-CE and/or the local CB
Step 3	Comm. I/F –S-CE sends the information to the Remote Terminal

Data receiving-RT

Use Case Step	Description
Step 1	Comm. I/F –R-RT gives a trip command to the Remote Terminal
Step 2	Remote Terminal receives the data

Tripping

Use Case Step	Description
Step 1	If the Remote terminal B receives the trip command, it issues a trip command to the CB

5.9.2.7 Pre-conditions

Synchronisation of the data between the relays must be established.

5.9.2.8 References:

[1] Y.Ohura, M.Suzuki, K.Yanagihashi, M.Yamaura, K.Omata, T.Nakamura, S.Mitamura, H.Watanabe, “A Predictive Out-of-Step Protection System Based On Observation Of The Phase Difference Between Substations”, IEEE Trans. PWRD, Vol.5, No.4, November 1990

5.9.3 Real time predictive type generator shedding

5.9.3.1 Summary

This wide area protection system comprises Remote Terminals and Central Equipment. Remote Terminal A and B measure the voltage and current at Power Station A and B. These Remote Terminals periodically send the active power, which is calculated from the voltage and current, to the Central Equipment. Remote Terminal C sends voltage data to the central unit. When a fault occurs, if the central unit predicts that the generators will loose synchronisation, the central unit sends a trip signal to the generators.

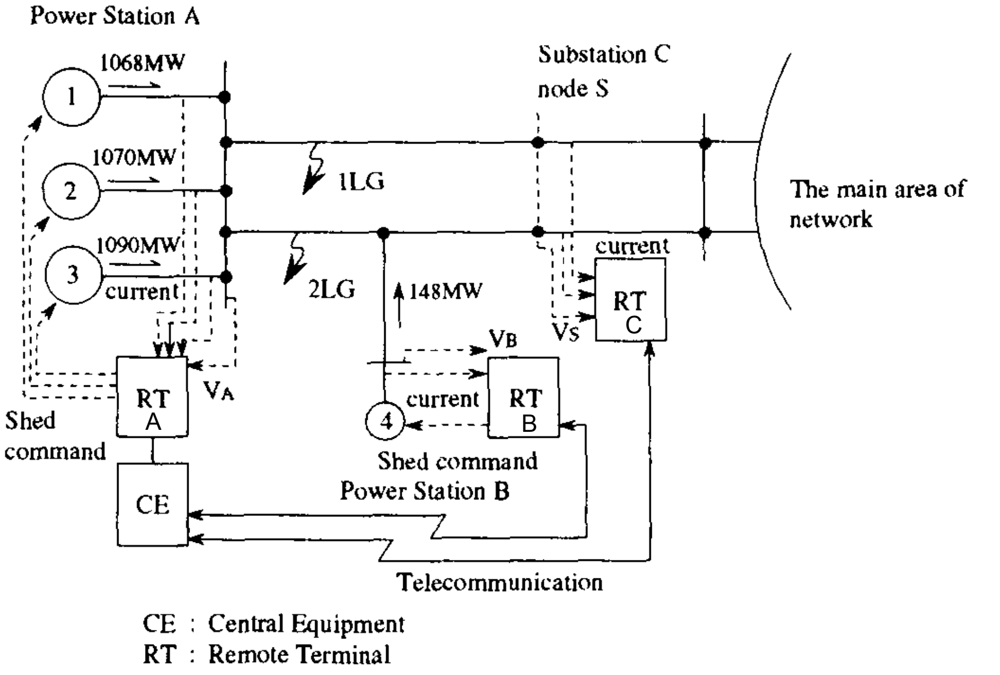
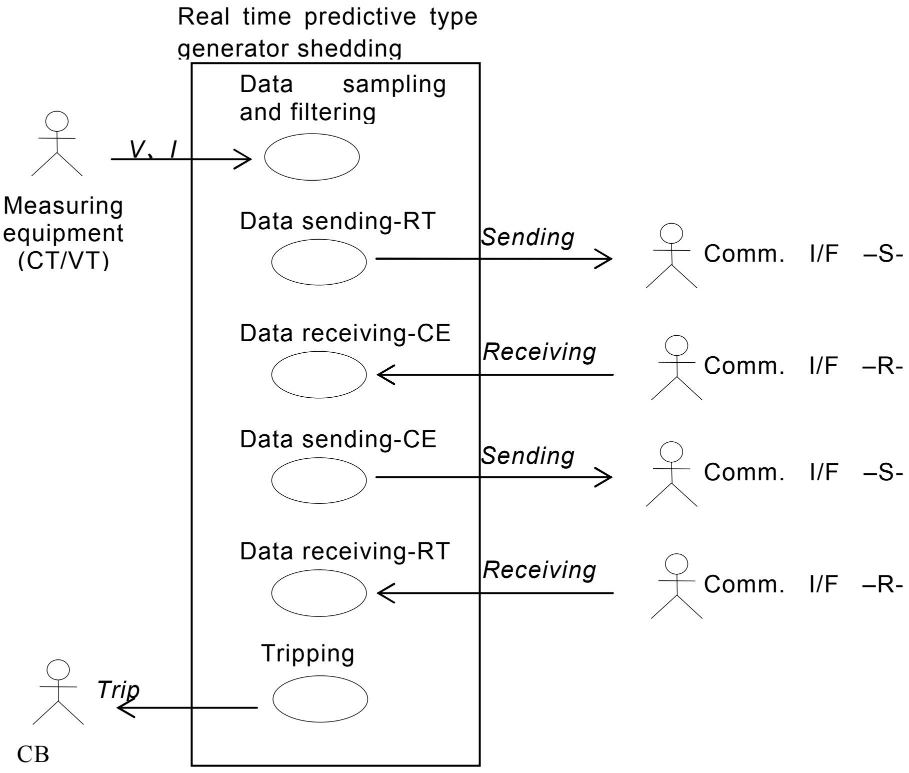


Figure 12: Real time predictive type generator shedding system [1]

5.9.3.2 Constraints / Assumptions / Design Considerations

- Representation of measured currents and voltages and any additional information
- A small propagation delay is needed for fast tripping (e.g.: 5 ms)
- For communication channel failure alternative actions must be considered
- Other constraints see section 5.9

5.9.3.3 Use case diagram



5.9.3.4 Actor(s)

Name	Role description
Measuring equipment	Measures current and voltage from a protected line
Comm. I/F –S-RT	Receives sampled data from the Remote Terminal and send the data to the Central Equipment
Comm. I/F –R-RT	Receive a trip command from the Comm. I/F –S-CE (the Central Equipment) and passes the command to the Remote Terminal
Comm. I/F –R-CE	Receives sampled data from the Comm. I/F –S-RT (the Remote Terminal) and passes the data to the Central Equipment
Comm. I/F –S-CE	Receives the trip command from the Central Equipment, and sends the command to the Remote Terminal
CB	Disconnects the line which is connected to a generator from the power station (Circuit Breaker)

5.9.3.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from the Measuring equipment, and filters them
Data sending-RT	Sends the sampled data and information bits to Comm. I/F –S (to the Central Equipment).
Data receiving-CE	Receives the sampled data and information bits from Comm. I/F –R (from the Remote Terminal).
Data sending-CE	Sends the trip information to Comm. I/F –R (to the Remote Terminal).
Data receiving-RT	Receives the trip information from Comm. I/F –R (from the Central Equipment).
Tripping	According to the trip information from Central Equipment, the Remote Terminal issues a trip command to the CB

5.9.3.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Current and Voltage are given to the Remote Terminals by the Measuring equipment
Step 2	Remote terminal samples an Analogue value, and converts it to digital data
Step 3	Remote terminal removes the unwanted frequency components from the sampled data, using a digital filter

Data sending -RT

Use Case Step	Description
Step 1	Remote terminals A and B calculate the Power, from the filtered current and voltage data
Step 2	Remote terminal puts the electrical data (Power for Terminal A and B, Current and Voltage for Terminal C) to sending data format, with other information bits
Step 3	Remote terminal sends the data to Comm. I/F –S-RT (in order to send the data to Central Equipment)
Step 4	Comm. I/F –S-RT sends the information to the Central Equipment

Data receiving -CE

Use Case Step	Description
Step 1	Comm. I/F –R-CE give the received data to Central Equipment
Step 2	Central Equipment receives the data

Data sending -CE

Use Case Step	Description
Step 1	Central Equipment executes a calculation for the generator angle prediction
Step 2	If Central Equipment predicts the generator will go to the out-of-step, it calculate the minimum number of generators which is necessary to be shed in order to stabilise the power system
Step 3	Central Equipment sends the trip information (the number of the generator to be shed) to Comm. I/F –S-CE
Step 4	Comm. I/F –S-CE sends the information to Remote Terminal

Data receiving-RT

Use Case Step	Description
Step 1	Comm. I/F –R-RT gives the trip information to the Remote Terminal
Step 2	Remote Terminal receives the data

Tripping

Use Case Step	Description
Step 1	According to the tripping information from the Central Equipment, the Remote Terminal issues a trip command to the CB

5.9.3.7 Pre-conditions

Synchronisation of the data between the relays must be established.

5.9.3.8 References

[1] K.Matsuzawa, K.Yanagihashi, J.Tsukita, M.Sato, T.Nakamura, A.Takeuchi, "Stabilizing Control System Preventing Loss Of Synchronism From Extension And Its Actual Operating Experience", IEEE Trans. PWRS, Vol.10, No.3, August 1995

5.9.4 Out-of-step detection

5.9.4.1 Summary

By comparing the angle of voltage between the two ends, it can be detected whether the centre of the out-of-step is between the two ends or not as shown in Figure 13. When the two voltages are in the opposite direction, an out-of-step occurs and the centre of out-of-step is in between the two ends.

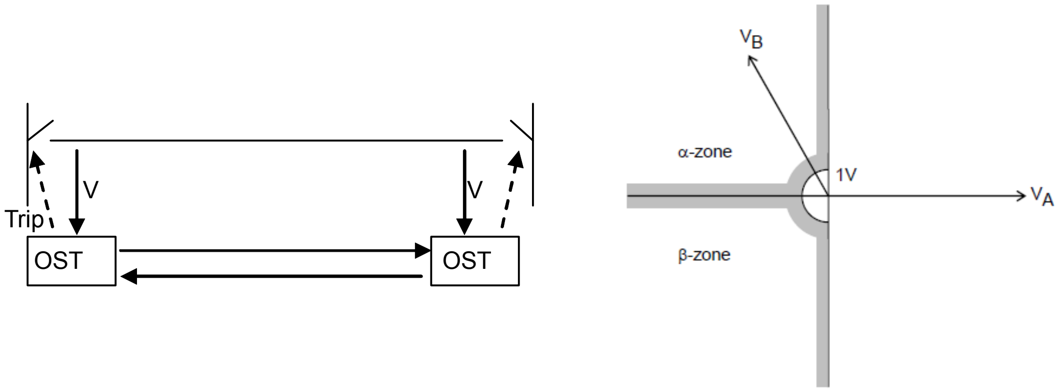
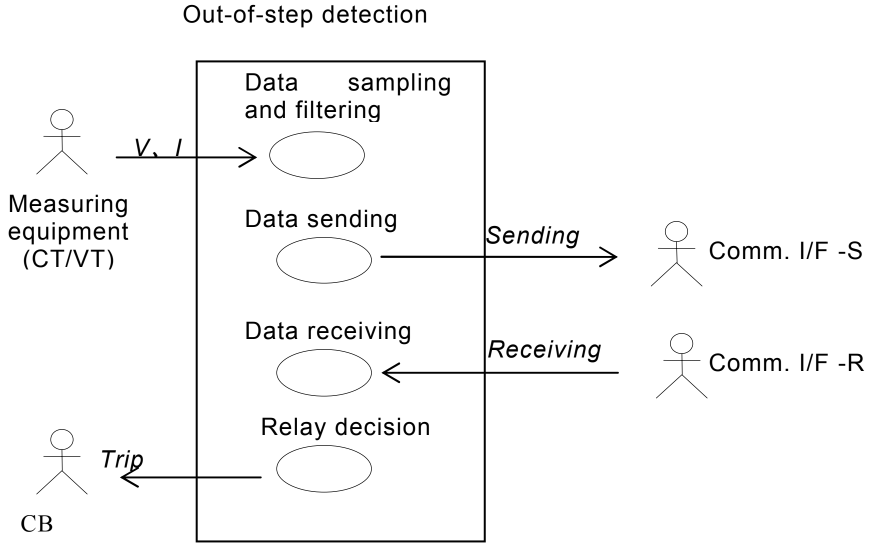


Figure 13: Out-of-step detection

5.9.4.2 Constraints / Assumptions / Design Considerations

- Representation of measured voltages and any additional information
- A medium propagation delay is needed for out-of-step detection (e.g.: 10 ms to 50 ms)
- Communication channel failure may block this kind of out-of-step detection, alternative actions must be considered
- Other constraints see section 5.9

5.9.4.3 Use case diagram



5.9.4.4 Actor(s)

Name	Role description
Measuring equipment	Measures voltage from protected line
Comm. I/F -S	Receives data from the local relay and sends the data to the remote end
Comm. I/F -R	Receives data from the remote end and gives the data to the local relay
CB	Disconnects the protected line from another system (Circuit Breaker)

5.9.4.5 Use Case(s)

Name	Services or information provided
Data sampling and filtering	Samples voltages from the Measuring equipment, and filters them
Data sending	Out-of-step detection sends the sampled voltage data to Comm. I/F –S (the remote end).
Data receiving	Receives the permissive signal from Comm. I/F –R (the remote end).
Tripping	If required, out-of-step detection sends a trip signal to the local CB

5.9.4.6 Basic Flow

Data sampling and filtering

Use Case Step	Description
Step 1	Voltage is given to Out-of-step detection by Measuring equipment
Step 2	Out-of-step detection samples an Analogue value and converts it to digital data
Step 3	Out-of-step detection removes the unwanted frequency components from the sampled data, using a digital filter

Data sending

Use Case Step	Description
Step 1	Out-of-step detection sends the sampled voltage data to Comm. I/F –S (in order to send the data to remote end relay)
Step 2	Comm. I/F –S sends the information to the remote end

Data receiving

Use Case Step	Description
Step 1	Comm. I/F –R gives the received data to Out-of-step detection
Step 2	Out-of-step detection receives the data

Relay Decision

Use Case Step	Description
Step 1	Compares the local voltage with the remote voltage and checks the angle difference between the two voltages
Step 2	When the out-of-step is detected, and if required, Out-of-step detection issues a trip command to the local CB

5.9.4.7 Pre-conditions

Synchronisation of the data between the relays must be established.

5.9.5 Synchrophasors measured via Phasor Measurement Units

5.9.5.1 Summary

Synchrophasors are measured via Phasor Measurement Units (PMUs). These units provide synchronised measured data for a certain purpose or multiple purposes. Hence the application can vary widely. System Integrity Protection Schemes (SIPS) as described in section 5.9.2, are one typical application of synchrophasors. Therefore the detail of an application is not explained here again.

5.9.6 Remedial Action Schemes (RAS)

5.9.6.1 Summary

Remedial Action Schemes (RAS) are designed to monitor and protect electrical systems. They perform automatic switching operations in response to adverse network conditions to ensure the integrity of the electrical system and to avoid a collapse of the network.

Typical automatic remedial actions include:

- Generator tripping for reduction of energy input to the system
- Tripping of load, insertion of braking resistors, series capacitors, opening of interconnecting lines and system islanding

The RAS action is generally performed by a central controller. The controller needs data collected by field units. The field units are capable of measuring currents and voltages and/or transducer quantities (W, VAr) and deliver these to the central unit for evaluation and comparison with data from other locations in the power system. The field unit also acts as a remote controller, such as performing breaker operations via programmable logic and inputs/outputs when a command is received from the central unit.

6 Communication requirements for substation-to-substation communication

(TF 20.11.07: The performance class description must be updated)

NOTE: This chapter 6 contains parts of IEC 61850-5, extended with requirements for Ethernet networks and some additions. It is prepared in such a way that it may fit in IEC 61850-5. Since part 5 doesn't know anything about the solution (use of Ethernet), these parts of chapter 6 have to be moved later to another part, maybe to part 7 of the standard.

6.1 General issues

6.1.1 Introduction (5.1 from IEC 61850-5)

The functions of a substation automation system (SAS) refer to tasks, which have to be performed in the substation. These are functions to control, monitor and protect the equipment of the substation and its feeders. In addition, there exist functions, which are needed to maintain the SAS, i.e. for system configuration, communication management or software management.

The functions of the substation automation system (SAS) are extended via links to the remote control centre (mainly Telecontrol) and to the neighboring substation (mainly line protection).

6.1.2 Logical allocation of functions and interfaces (5.2 from IEC 61850-5)

The functions of a substation automation system may be allocated **logically** on three different levels (station, bay/unit, or process). These levels are shown by the logical interpretation of Figure 14 together with the logical interfaces 1 to 10.

Interface related station level functions are functions representing the interface of the SAS to the local station operator HMI (human machine interface), to a remote control centre TCI (telecontrol interface) or to the remote engineering for monitoring and maintenance TMI (telemonitoring interface). These functions communicate via the logical interfaces 1 and 6 with the bay level and via the logical interface 7 and the remote control interface to the outside world.

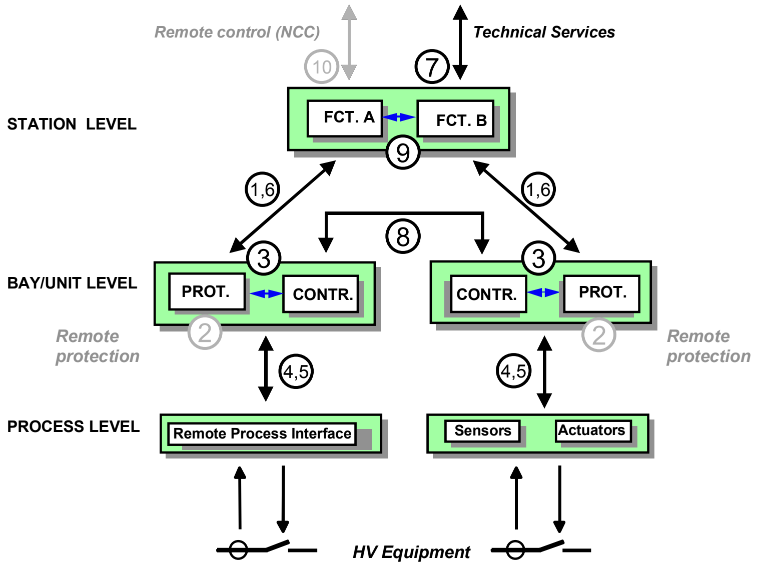


Figure 14 - Levels and logical interfaces in substation automation systems

The meaning of the interfaces

IF1: protection-data exchange between bay and station level

IF2: protection-data exchange between bay level and remote protection (also inside the scope of the Ed2 of the standard)

IF3: data exchange within bay level

IF4: CT and VT instantaneous data exchange (especially samples) between process and bay level

IF5: control-data exchange between process and bay level

IF6: control-data exchange between bay and station level

IF7: data exchange between substation (level) and a remote engineer's workplace

IF8: direct data exchange between the bays especially for fast functions like interlocking

IF9: data exchange within station level

IF10: control-data exchange between substation (devices) and a remote control centre (also inside the scope of the Ed2 of the standard)

6.1.3 The role of interfaces (from 5.4 of IEC 61850-5)

Open issue: Rewrite to include point-multipoint communications.

The interface 7 is dedicated for external communication with a remote monitoring centre. It could be realized by a direct interface to the station/interbay bus also. The interface 2 dedicated to communication with a remote protection device and the interface 10 dedicated to remote control are also inside the scope of the Ed2 of standard. It should be noted that interfaces to parts outside the substation may be interfaces to a communication network not native IEC 61850 but these networks have to allow to tunnel IEC 61850 data and services without degradation. The performance of distributed functions running in interconnected IEC 61850 based parts has to stay within the required limits.

According to the function allocation, the message types of clause 6.3 based on communication performance requirements may be assigned to the different interfaces. The free allocation of functions means that such an assignment may not be common for all substation automation systems.

6.1.4 Response behaviour requirements (6.4 from IEC 61850-5)

Since interoperability is claimed for a proper running of functions, the reaction of the application in the receiving node has to be considered.

a) The reaction of the receiving node has to fit into the overall requirement of the distributed function to be performed.

b) The basic behaviour of the functions in any degraded case, i.e. in case of erroneous messages, lost data by communication interrupts, resource limitations, out of range data, etc. has to be specified. This is important if the overall task cannot be closed successfully, e.g. if the remote node does not respond or react in a proper way.

c) The external communication system has to fit into the overall requirements of the distributed function to be performed.

These requirements are function related local issues and, therefore, outside the scope of this communication standard. But the requirement left for this standard is the provision of proper quality attributes to be transferred with the data under consideration.

6.2 List of logical nodes (11 from IEC 61850-5)

Most of the functions comprise a minimum of three logical nodes, i.e. the LN with the core

Open issue: replace LNs in Sections 6.2.1-6.2.3 with references. LNs are modeled in Sec. 8.

6.2.1 Logical Nodes for protection functions

6.2.1.1 Protection based on Substation-Substation communication (examples)

Logical Node	61850	IEEE	Description or Comments
Distance protection	**PDIS**	21	Distance relay is a relay that functions when the circuit admittance , impedance, or reactance increases or decreases beyond a predetermined value *The change of the impedance seen by PDIS is caused by a fault. The impedance characteristic is a closed line set in the complex impedance plane. - The reach of the distance protection is normally split into different zones (e.g. 1…4 forward and 1 backward) represented by dedicated characteristics.*
Differential *protection*	**PDIF**	87	Differential protective relay is a protective relay that functions on a percentage or phase angle or other quantitative difference of two currents or some other electrical quantities
Phase comparison *protection*	**PPDF**	87P	See above (PDIF/87)
Differential line *protection (1)*	**PLDF**	87L	See above (PDIF/87)

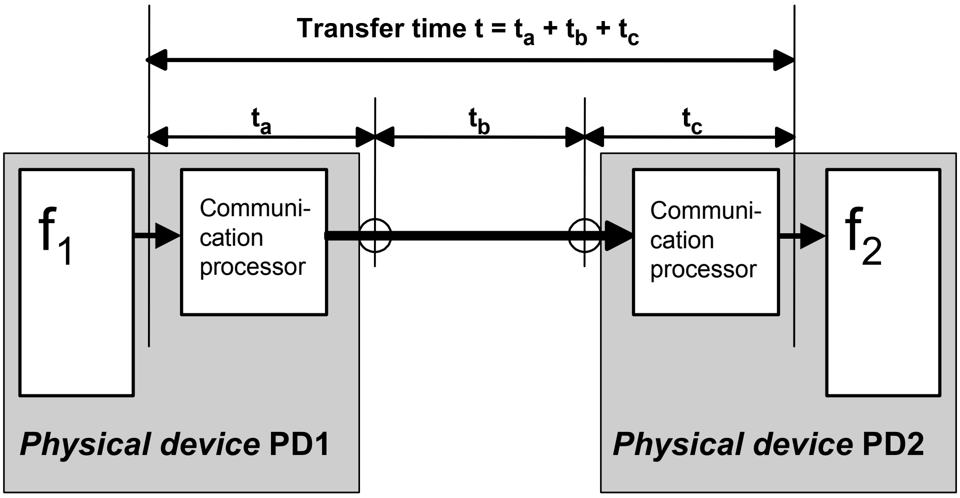
6.2.2 Logical Nodes for Control

6.2.2.1 Control Nodes based on Substation-Substation communication (examples)

Logical Node	61850	Description or Comments
Interlocking function at station and/or bay level	**CILO**	Interlocking may be totally centralized or totally decentralized. Since the interlocking rules are basically the same on bay and station level and based on all related position indications the different interlocking LNs may be seen as instances of the same LN class Interlocking (IL). 1) Interlocking of switchgear at bay level All interlocking rules referring to a bay are included in this LN. Releases or blockings of requested commands are issued. In case of status changes affecting interlocking blocking commands are issued. 2) Interlocking of switchgear at station level All interlocking rules referring to the station are included in this LN. Releases or blockings of requested commands are issued. Information with the LN bay interlocking is exchanged

6.2.3 Instrument transformers

Logical Node	61850	Description or Comments
Current transformer	**TCTR**	There is one instance per phase. These three/four instances may be allocated to different physical devices mounted in the instrument transformer per phase.



Voltage transformer	**TVTR**	There is one instance per phase. These three/four instances may be allocated to different physical devices mounted in the instrument transformer per phase.

… to represent the mentioned instrument transformers with all its data and related settings (if applicable), and communication relevant behavior in the SA system.

6.3 Message performance requirements (13 in IEC 61850-5)

6.3.1 Transfer time definition (13.4 in IEC 61850-5)

When the complete transfer time is specified below, this means the complete transmission of a message including necessary handling at both ends. The time counts from the moment the sender puts the data content on top of its transmission stack up to the moment the receiver extracts the data from its transmission stack.

The time requirement is applicable for the complete transmission chain as indicated in Figure 15. In physical device PD1, a function f_1 sends data to another function f_2, located in physical device PD2. The overall transfer time will however consist of the individual times of the communication processors and the network transfer time, including wait times and time used by routers and other devices being part of the complete network. Any testing and verification of the complete transfer time must be performed during the Site Acceptance Testing, since the physical devices and network equipment might be supplied from different manufacturers.

Figure 15 - Definition of "overall transfer time"

The time t_b is neglectable for electrical or optical cables but reasonable time may be added by active communication components like gateways and, for links outside the substation, the time consumed in the interconnecting network tunnelled by IEC 61850 messages.

All requirements are valid under normal conditions without disturbed communication links. Disturbances may need a logical reconnection of the communication link, repetition of messages or other means delaying the transfer time. This behavior is a matter of implementation and detailed in part 7-2 of this standard (services).

6.3.2 The introduction and use of message types (13.5 in IEC 61850-5)

As mentioned above, the communication requirements in terms of PICOMs between LNs result that the various communication links within a Substation Automation System are required to transport messages of varying complexity with regard to their content, length, allowed worst case transfer time and security. The message types being carried will vary from moment to moment depending on the activity both in the substation and on the system.

The main difference between PICOMs and messages types are that PICOMs refer to information transfer strictly based on a single dedicated functionality, and include source and sink. The message types are based on a grouping of the performance related PICOM attributes and, therefore, define the performance requirements to be supported. Since the performance requirements are defined per message, they are independent from the size of the substation. Scenarios with multiple messages for substations are given in Clause 6.4.

6.3.3 The introduction and use of performance classes (13.5 in IEC 61850-5)

To allow for different requirements of the substations, the some message types are also subdivided in Performance Classes. There are two independent groups of performance classes, one for control and protection, another one for metering and power quality applications. Since the performance classes are defined according to the functionality needed, they are independent from the size of the substation.

Within a specific substation, all communication links does not necessarily need to support the same performance class. Station level communications and process level communications may be selected independent of each other and within the process level, different performance classes can be used for communications in different bays, depending on the number and rating of equipment located in each bay.

6.3.3.1 Control and protection

Performance class P1 applies typically to a distribution bay or to bays, where low requirements otherwise can be accepted.

Performance class P2 applies typically to a transmission bay or if not otherwise specified by the customer.

Performance class P3 applies typically to a transmission bay with top performance synchronizing feature and breaker differential.

External links may have a lower performance if acceptable by the functions.

Open issue: Trips, performance class association needs some additional clarification.

6.3.3.2 Metering and power quality

Performance class M1 refers to revenue metering with accuracy class 0.5 (IEC 60687) and 0.2 (IEC 60044) and up to the 5th harmonic.

Performance class M2 refers to revenue metering with accuracy class 0.2 (IEC 60687) and 0.1 (IEC 60044) and up to the 13th harmonic.

Performance class M3 refers to quality metering up to the 40th harmonic.

6.3.4 Messages types and performances classes (13.7 in IEC 61850-5)

6.3.4.1 Type 1 - Fast messages (13.7.1 in IEC 61850-5)

This type of message typically contains a simple binary code containing data, command or simple message, for example "Trip", "Close", “Reclose order”, "Start", "Stop", "Block", "Unblock", “Trigger”, “Release”, “State change”, maybe “State” for some functions also. The receiving IED will normally act immediately in some way by the related function on receipt of this type of message since, otherwise, no fast messages are needed.

6.3.4.1.1 Type 1A “Trip”

The trip is the most important fast message in the substation. Therefore, this message has more demanding requirements compared to all other fast messages. Same performance may be requested for interlocking, intertrips (direct trips) and logic discrimination between protection functions.

a) For Performance Class P1, the total transfer time shall be in the order of half a cycle. Therefore, 10 ms are defined.

b) For Performance Class P2/3, the total transfer time shall be below the order of a quarter of a cycle. Therefore, 3 ms are defined.

c) Trips and similar signals of type 1A to the neighbouring substation (e.g. for line protection) request for all performance classes case a)

Open issue: make reference to IEC60834-1/-2

6.3.4.1.2 Type 1B “Others”

All other fast messages are important for the interaction of the automation system with the process but have less demanding requirements compared to the trip.

a) For Performance Class P1, the total transfer time shall be less or equal 100 ms.

b) For Performance Class P2/3, the total transfer time shall be the order of one cycle. Therefore, 20 ms are defined)

c) Fast messages of type 1B to the neighbouring substation (e.g. some automation) request for all performance classes case a)

NOTE: These messages are typical for interfaces IF3, IF5, and IF8

6.3.4.2 Type 2 - Medium speed messages (13.7.2 in IEC 61850-5)

These are messages, as defined in clause 6.3.4.1, where the time at which the message originated is important but where the transfer time is less critical. It is expected that IEDs will have their own clocks. The message shall include a time-tag set by the sender, and the receiver will normally react after an internal time delay, which then will be calculated from the time given in the time-tag. Also normal “state” information belongs to this type of message

This type may alternatively include a single measurand, such as a rms value calculated from type 4 signals.

The total transfer time shall be less than 100 ms.

NOTE: These messages are typical for interfaces IF3, IF8, and IF9

6.3.4.3 Type 3 - Low speed messages (13.7.3 in IEC 61850-5)

This type includes complex messages that may require being time-tagged. This type should be used for slow speed auto-control functions, transmission of event records, reading or changing set-point values and general presentation of system data. Whether a time-tag is required (normally) or not (exception) will be stated by the actual application. Also time tagged alarms and events for normal alarm/event handling and non-electrical measurands like temperature belong to this type, but some automatics and values (e.g. pressure) may request message type 2.

The total transfer time shall be less than 500 ms.

Commands and related SCADA information e.g. to the remote Network Control Centre belong also to these low speed messages of type 3.

NOTE: These messages are typical for nearly all interfaces, at least for its use for parameter setting: IF1, IF3, IF4, IF5, IF6, IF5, IF7, IF8, and IF9

6.3.4.4 Type 4 - Raw data messages (13.7.4 in IEC 61850-5)

This message type includes the output data from digitizing transducers and digital instrument transformers independent from the transducer technology (magnetic, optic, etc.). The analogue information needed on the other side of the line e.g. for differential line protection are also of type 4.

The data will consist of continuous streams of synchronized data from each IED, interleaved with data from other IED.

NOTE: These messages are typical for interfaces IF4, and in some applications, for IF8

Table 1 - Raw data for protection and control

Data type	Class	Transfer time [ms] defined by trip time	Resolution [Bits] *Amplitude*	Rate [Samples/s] *Frequency*
Voltage	P1	10.0	13	480
Current			13	
Voltage	P2	3.0	16	960
Current			16	
Voltage	P3	3.0	16	1920
Current			18	

For convenience, the resolution is given in bits

Table 2 - Raw data for metering

Data type	Class	Accuracy classes and harmonics	Resolution [Bits] *Amplitude*	Rate [Samples/s] *Frequency*
Voltage	M1	Class 0.5 (IEC 60687) Class 0.2 (IEC 60044) Up to 5th harmonics	12	1500
Current			14	
Voltage	M2	Class 0.2(IEC 60687) Class 0.1(IEC 60044) Up to 13h harmonics	14	4000
Current			16	
Voltage	M3	Class 0.1 (not defined by IEC) Up to 40h harmonics	16	12000
Current			18	

For convenience, the resolution is given in bits

6.3.4.5 Type 5 - File transfer functions (13.7.5 in IEC 61850-5)

This type of message is used to transfer large files of data for recording, information purposes, settings, etc. Data must be split in blocks of limited length, to allow for other communication network activities. Typically, the bit lengths of the file type PICOMs are equal or greater than 512 bits.

Transfer times are not critical; no specific limits. Typically, the time requirements are equal or greater than 1000 ms.

For remote access, the request for file transfer shall have an access control; i.e. the access needs some authorization (see Type 7 message). Therefore, this request messages shall be of type 7.

NOTE: In case of configuration setting, these messages are typical for nearly all interfaces: IF1, IF3, IF4, …In case of disturbance recording, these messages are typical for interfaces IF1, IF6, IF7 and – if the records are stored near the process, IF4.

6.3.4.6 Type 6 - Time synchronization messages (13.7.6 in IEC 61850-5)

This type of message is used to synchronize the internal clocks of the IED in the SAS. Depending of the purpose (time tagging of events or sampling accuracy of raw data) different levels of time synchronizing accuracy are required.

These are functional requirements. It's up to the implementation if e.g. the time synchronizing of the clocks in IEDs has to be one order of magnitude better than requested by the functional requirements. Part 8 and Part 9 shall define how the time synchronization mechanism is implemented.

No direct requirements for the synchronization messages are defined except for the resulting time accuracy in the whole system.

Time synchronization is also important for communication between the substations, either for a common event time or for the synchronization of samples to be compared from both sides of the line.

Open issue: IEEE 1588 reference needs to be noted in the solutions rather than here.

6.3.4.6.1 Standard IED synchronizing for control and protection events

Time Perf. Class	Accuracy [ms]	Purpose
T1	± 1	Time tagging of events
T2	± 0.1	Time tagging of zero crossings and of data for the distributed synchrocheck. Time tags to support point on wave switching.

NOTE: These messages are typical for nearly all interfaces because of the system wide synchronization: IF1, IF3, IF4, IF5, IF6, IF5, IF8, and IF9. The time performance class needed depends strongly on the supported functionality. Synchronizing of digital instrument transformers and Type 4 messages see below.

6.3.4.6.2 Standard IED synchronizing for instrument transformers

The requested time accuracy results from the referenced performance classes (column 3) introduced above. To give some indications on the related power system values columns 4,5 and 6 have been added.

Time Perf. Class	Accuracy [µs]	Reference		*Phase angle [‘] 50Hz*	*Phase angle [‘] 60Hz*	*Fault location [m]*
T3	± 25	P1		*27*	*32*	*7500*
T4	± 4	P2	M1	*4*	*5*	*1200*
T5	± 1	P3	M2/3	*1*	*1*	*300*

NOTE: The performance classes T3, T4, and T5 are typical for interfaces IF4, and in some applications, for IF8.

6.3.4.7 Type 7 - Command messages with access control (13.7.7 in IEC 61850-5)

This type of message is used to transfer control orders, issued from local or remote HMI functions, where a higher degree of security is required. All messages using interface 7 (external Technical Services) shall include access control. This type of message is based on Type 3, with additional password and/or verification procedures.

These command messages propagating over some control levels from the operator down to the switchgear or to some other controllable object may be converted to messages requesting type 1 properties at least on process level.

NOTE: These messages are typical for the operators access via a local or remote HMI: IF1, IF6 and IF7.

6.4 Requirements for data integrity (14 in IEC 61850-5)

Integrity means that for given conditions of the communication link (e.g. signal to noise ratio) the resulting errors are below a certain acceptable limit. In part IEC 61850-3, the three integrity classes according to IEC 60870-4 are referenced. Integrity was also introduced as PICOM attribute in clause 10.1.2 of IEC61850-5, 1st edition 2003.. All safety related messages like commands and trips with direct impact on the process shall have the highest integrity class, i.e class 3. All other messages may be transmitted with a lower data integrity but not lower then class 2.

Normally, the noise level is given and cannot be influenced. Nevertheless, to reach integrity three groups of known measures exist to limit its impact.

a) Proper design of devices and the communication system, e.g. protecting enclosures and the use of fibre optic links

b) Apply an appropriate coding to achieve the desired residual error rate

c) Use of at least two step sequences like select-before-operate (SBO) for commands

The use of these measures is outside the scope of part 5 but the required data integrity shall be considered in modelling the services (IEC 61850-7-2, e.g. SBO) and defining the mapping (IEC 61850-8-x, 61850-9-x, e.g. coding).

6.5 Requirements for teleprotection

6.5.1 Reliability (Security & Dependability)

For the various protection schemes, the Cigre brochure TB192 "Protection using Telecommunications" (2001) addresses the requirements from protection on the teleprotection interfaces and the communication channels.

The term "teleprotection" refers to the equipment needed to interface the protection equipment to the telecommunication equipment; for IEC 61850 systems this would comprise the equipment generating and processing the Ethernet packets for the protection functions (e.g. GOOSE).

Non-protection IEC 61850 functions are far less critical, e.g. delivery times of an order of 1 s for SCADA functions and of an order of 100 ms for automatics may be tolerable.

This section will therefore focus on delivering *protection traffic* with the required Security and Dependability.

6.5.1.1 Security Requirements of Protection Schemes, from Cigre & IEC

The "Security" requirements from protection on telecommunications, per Tables 6-1-1 and 6-1-2 in the Cigre TB192 vary from "medium" to "high", with a reference to IEC 60834-1.

The IEC 60834-1 Figure 21 shows that the probability of an "unwanted command" (from an error burst) should be less than 10^{-4} (for blocking schemes) through 10^{-8} (for intertripping schemes).

Therefore the telecommunication network shall have an unwanted-message probability of lower than 10^{-8} (for intertripping protection schemes).

(An "unwanted message" is a message that would result in a very-undesirable event, such as a false trip.)

6.5.1.2 Dependability Requirements of Protection Schemes, from Cigre and IEC

The "Dependability" requirements from protection on telecommunications, per Tables 6-1-1 and 6-1-2 in the Cigre TB192 vary from "medium" to "high", with a reference to IEC 60834-1.

The IEC 60834-1 Figure 21 shows that the probability of a "missed command" (from a 10^{-6} continuous BER) should be less than 10^{-2} (for permissive-underreach schemes) through 10^{-4} (for intertripping schemes).

The IEC 60834-1 Figure 21 also shows that the "maximum actual transmission time" (called transfer time in IEC61850) should be < 10ms for all the protection schemes.

Therefore the telecommunication network shall have a >10ms message-latency probability of lower than 10^{-4} (for intertripping protection schemes).

7 Security & Dependability issues when using Ethernet Networks

Note: Some additional concepts that are out for discussion are added in Annex A

The downside of using Ethernet for teleprotection networks is that they have a “best effort” nature.

This clause highlights the specific problems of Ethernet networks, and provides solutions so substation networks can be engineered to guarantee the security and dependability required by the teleprotection applications.

7.1 Avoiding GOOSE packets flooding the WAN

By using different VLANs for intra-substation and inter-substation GOOSE packets, the broadcast range of the former will be limited to the one substation.

(This would require IEDs to repeat some GOOSE packets, to provide packets for both VIDs.)

For applications requiring the use of GOOSE packets to provide a multipoint-to-point delivery of IED data to a central processor, the use of separate VIDs for the “up” and “down” traffic avoids the broadcasting of all the IED packets to all the other IEDs.

7.2 Requirements on IEC 61850 interfaces

For the reasons cited above, in order that typical Ethernet telecommunications networks can provide the required Security and Dependability for protection functions, the IEC 61850 packets should normally be IEEE 802.1Q “tagged” frames.

7.3 Security of Traffic

Please refer to the results of TC57 / WG15

7.4 Dependability of Traffic

As noted above, IEC 60834-1 specifies that the probability of a “command” not being received within 10 ms should be <10^{-4}.

For an Ethernet network, the reasons for a packet not being received within 10 ms comprise:

7.4.1 Congestion

Whenever two or more Ethernet packets compete for a network path, such as to egress the port of a switch, one of them must wait in a “queue”.

If for some duration the arriving packets exceed a port’s capacity, the queue depth increases, and eventually packets may be discarded.

For networks transporting different classes of traffic with different degrees of priority, the use of switches with several priority-dependent queues at each egress port will improve the latencies of the higher-priority traffic (assuming the packets have IEEE 802.1Q/p “tags” with the correct priority values).

Note that though these tags support 8 priority levels, most switches provide only 4 or 2 priority level queues.

7.4.2 Fibre Failure

The time for the network to establish an alternate link after the failure of a network's link (most links are fibre) may be too slow.

Note that none of the standard path-failure recovery algorithms for Ethernet networks come even close to the 10 ms required; SONET is < 60ms, SDH < 50ms, Ethernet Spanning Tree is about 1 minute, and Ethernet Rapid Spanning Tree takes tens of milliseconds to a few seconds.

As a result, communication vendors for the power utility market provide proprietary solutions with much faster recovery times. (These require ring topology networks.)

An alternate solution is to provide duplicate and physically-separate communication paths between the protection IEDs.

7.5 Requirements on the Telecommunications network

This clause uses the telecom terms "drop" for the equipment ports connecting to the traffic sources (e.g. for VF, data, video etc.), and "line" for the equipment ports connecting the networks' nodes (typically fibre connections).

The requirements for the Ethernet Telecommunications network are as follows:

a) If some of the Ethernet Telecommunications network equipment is outside the utility's "Security Perimeter" (e.g. when Ethernet circuits are leased from a service provider), the Ethernet links through such equipment should be secured. For further details please refer to the results of TC57 / WG15.

b) Unless dual-port IEC 61850 IEDs are used (with physically separate paths), the Ethernet network shall recover (restore traffic) from a fibre failure within 10ms.

c) All the network switches must be configured in an appropriate way.

d) The probability of a GOOSE packet taking more than 10ms to traverse the network shall be constrained to < 10^{-4}; by limiting the number of switches on the longest path, and by limiting the traffic loading (see the next sub-sections for some examples).

7.5.1 Example of packet delays

At each egress switch port, a high-priority packet may have to wait for a maximum-length lower-priority packet to egress; a 1518 byte packet takes 122us at 100 Mbit/sec, 12us at 1 Gbit/sec.

A potential 2ms extra delay could therefore be incurred for a network path comprising 16 hops if at 100 Mbit/sec, 160 hops if at 1 Gbit/sec.

At each egress switch port, a high-priority packet may also have to wait for many other high-priority packets to egress; a 600 byte packet (typical for GOOSE) requires 48us at 100 Mbit/sec, 4.8us at 1 Gbit/sec.

A potential 2ms extra delay could therefore be incurred for an event-triggered burst of 40 GOOSE packets if at 100 Mbit/sec, 400 packets if at 1 Gbit/sec.

7.6 Useful features of some Ethernet Telecommunications networks

A utility may desire its wide-area network to be used for transporting 3rd-party Ethernet traffic, (e.g. to interconnect the LANs of different sites), raising a potential conflict with the VIDs chosen for the utility's 61850's IEDs.

For such applications, the “encapsulation” of such traffic in a second 802.1Q VLAN tag (sometimes known as “nested VLANS”, or “QinQ”) is a good solution; this also preserves the original traffic’s priority tags (without such nesting, the utility would need to be able to modify the original tags to ensure that such traffic is kept out of the network’s GOOSE queues).

Some Ethernet Telecommunication networks use SONET rather than Ethernet for their transport formats (for the fibre signals); this technology allows the provisioning of a plurality of Ethernet WANs, each with its own dedicated bandwidth and immunity to the traffic on the others WANs.

Some Ethernet Telecommunication switches provide an extra set of queues on their line ports (e.g. 16 c.f. 8) so that for traffic at a particular priority level, the “through” traffic (line to line) has priority over the “add” traffic (drop to line). This mitigates the delay accumulations over multi-hop paths.

Some Ethernet Telecommunication networks monitor the latency of critical traffic paths, recording the peak values over time, so that the user can confirm that the expected performance is being realized.

7.7 Assigning VIDs

It is acknowledged that the use of the 802.1Q VIDs (VLAN IDs) to control traffic and provide security, plus the use of the 802.1Q priority field to meet dependability requirements requires the use of switches that support these features; however it has also been demonstrated that such features are required if such networks are used.

The technology for assigning these VIDs and priorities is beyond the scope of this document.

- GVRP and GMRP are IEEE standards (in 802.1p) that allow IEDs to request VLAN assignments.
- The devices could be configured manually.
- The devices could be configured by whatever configures the 61850 substation IEDs.

An important consideration is that there is a strong argument for the entire communication network’s settings and performance to be continually monitored; some utilities are already requiring this feature.

8 Communication aspects

8.1 Services

This clause provides an overview of the information that needs to be transmitted and the service from IEC 61850-7-2 that shall be used.

Status information: Status information shall be transmitted using the GOOSE service from IEC 61850-7-2.

Phasors: If phasors are acquired cyclically, the service for the transmission of sampled values shall be applied. Both the unicast as well as the multicast services can be used. If phasors are time stamped and not necessarily cyclic, the GOOSE service shall be used.

NOTE – With the sampled value transmission as defined in IEC 61850-7-2, the minimal sampling rate is 1 sample per net period. That means that, if phasors are transmitted using the sampled value service, at least one phasor per period needs to be calculated and transmitted.

EDITOR NOTE – in the case it is required to support less than one phasor per period, an extension of the sampled value model may be required. Options are: (a) to add an attribute to differentiate between samples per period and samples per second; (b) to use negative values to indicate fractions of samples per period, e.g. -2 would mean one sample per 2 periods.

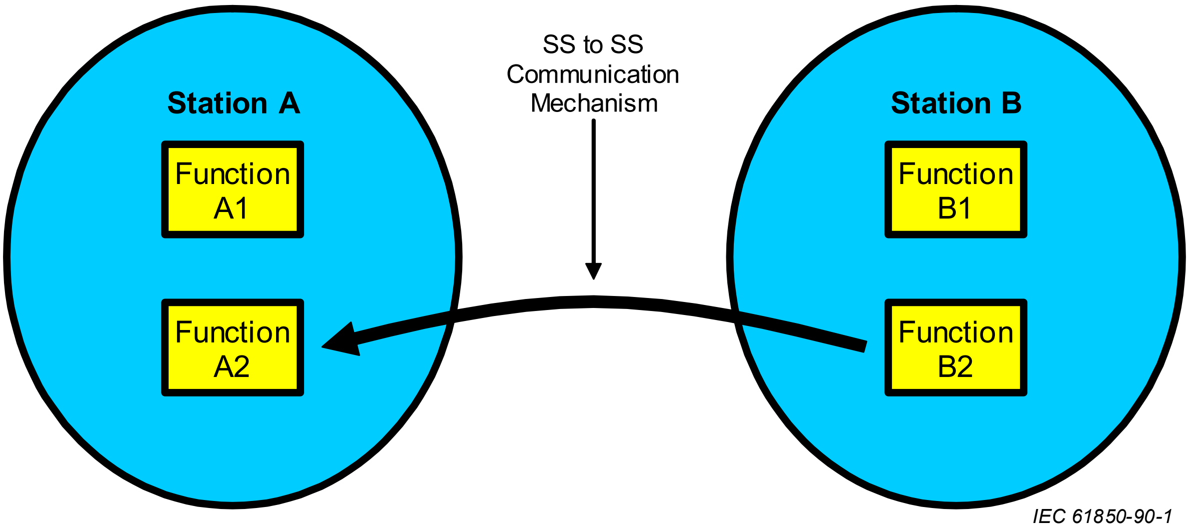
Sampled values: Where sampled values need to be transmitted, the services for unicast or multicast transmission of sampled values shall be used.

8.2 Communication architecture

8.2.1 Preliminary Notes and Definitions

To explain the basic communication mechanisms involved in SS-to-SS communications, a minimal model shall be used. It is reduced to the case, that function A2 in station A obtains data from function B2 in station B. Of course, the situation is much more complex in reality, there will be most likely also a dataflow in the opposite direction, or there will be also other functions exchanging data with each other. The example used below could be easily extended by applying the principles shown.

The situation is looked at from the viewpoint of function A2; thus station A is called "local", station B is called "remote".



IEC 61850-90-1

Figure 16 Basic SS to SS Communication Structure

The scope of this report is the communication between substations, effectively exchanging data between the station networks. Consequently, the "blue areas" containing "Station A" and "Station B" mean in fact the local communication networks (station networks). In the same sense, any of the "Functions" could be associated to a logical node when applying IEC 61850. Thus, the terms "Station" or "Station Network" and "Function" or "Logical Node" are often used synonymously in the following.

Two communication mechanisms are considered in this report:

(1) Tunnelling

(2) The Gateway approach using specific teleprotection communication equipment.

8.2.2 Tunnelling

"Tunnelling" means a method to connect multiple substation networks that allows "direct access" to functions in remote stations.

The tunnel is configured for a specific kind of traffic, e.g. based on a VLAN ID. The kinds of traffic are the only information needed for configuring the tunnel. For IEC 61850, the relevant kinds of traffic would be TCP/IP (for C/S communication) and multicast messages on Ethernet layer 2 (for GOOSE, eventually even SV).

The tunnel accepts any message of a kind it is configured for and passes it through unchanged. The tunnel does not care about the actual information content of the messages. Consequently, the tunnel does not need to be reconfigured if the "communication" becomes reconfigured, e.g. when the information exchanged between functions changes or if additional functions exchange information.

The station network becomes extended to include the remote station.

For the C/S communication, devices (servers) in the remote station become addressable; technically speaking a route is provided for the IP addresses in the remote station.

For GOOSE/SV, the broadcast domain extends into the remote station.

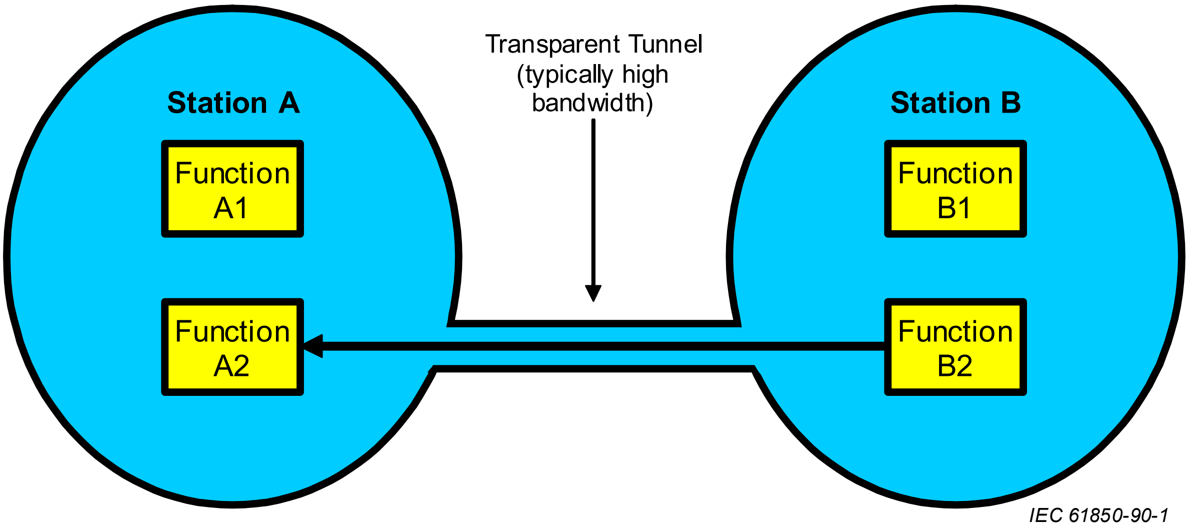


Figure 17 SS to SS Communication via Tunnel

Typically, a tunnel will be only applied if sufficient bandwidth is available. What "sufficient" means, depends on the application.

The exchange of non-time-critical status information for SCADA purposes may work well over a slower link.

Exchanging GOOSE messages for remote interlocking may require higher bandwidth just to achieve low enough latency. Even if the data volume of the GOOSE traffic is low, higher bandwidth of a communication mechanism typically correlates with lower latency.

In practice, such tunnels will be established by means of network switches or routers. In a very strict sense, such communication devices could be also seen as a kind of "teleprotection equipment". For the reasons explained above (transparency of communication, independence of communication configuration), this "teleprotection equipment view" will not be applied with tunnelling.

8.2.3 Gateway

Gateways connect multiple substation networks by establishing "oblique access" to functions in remote stations.

A gateway configuration depends on a specific communication configuration. It is fully aware of the actual information content of the messages. Consequently, the gateway must be reconfigured if the "communication" becomes reconfigured, e.g. when the information exchanged between functions changes or if additional functions exchange information.

For the gateway approach, explicit teleprotection equipment is involved. The teleprotection equipment on the sending side filters and re-codes information for the special communication mechanism used to transfer the information. On the receiving side, the teleprotection equipment re-creates the information from the remote end to provide it in a form that is usable for the functions in the substation.

Gateways can deliver a wide range of functionality. For the further considerations, two kinds of gateways shall be distinguished:

8.2.3.1 GGIO Gateway

A number of arbitrary I/O points are exchanged between the stations. In IEC 61850, this would be implemented by using GGIOs. A separate cross-reference list is necessary to interpret the actual meaning of the anonymous data points of the GGIOs. This approach provides no semantics and delivers very little value within the scope of IEC 61850 conformant engineering.

Therefore, the GGIO Gateway will not be further covered by this document.

8.2.3.2 Proxy Gateway

The teleprotection equipment on the receiving side acts as a proxy for the function on the sending side. This means it re-creates the interface and the behavior of the real function, at least for the scope that is involved in the communication between the functions.

For C/S communication, the data model of the remote function is re-created by the proxy to serve the transmitted information. For GOOSE (and eventually SV), the messages are published by the proxy with the same format as on the remote side.

Thus, the Proxy Gateway is re-iterating the functionality of the tunnelling approach.

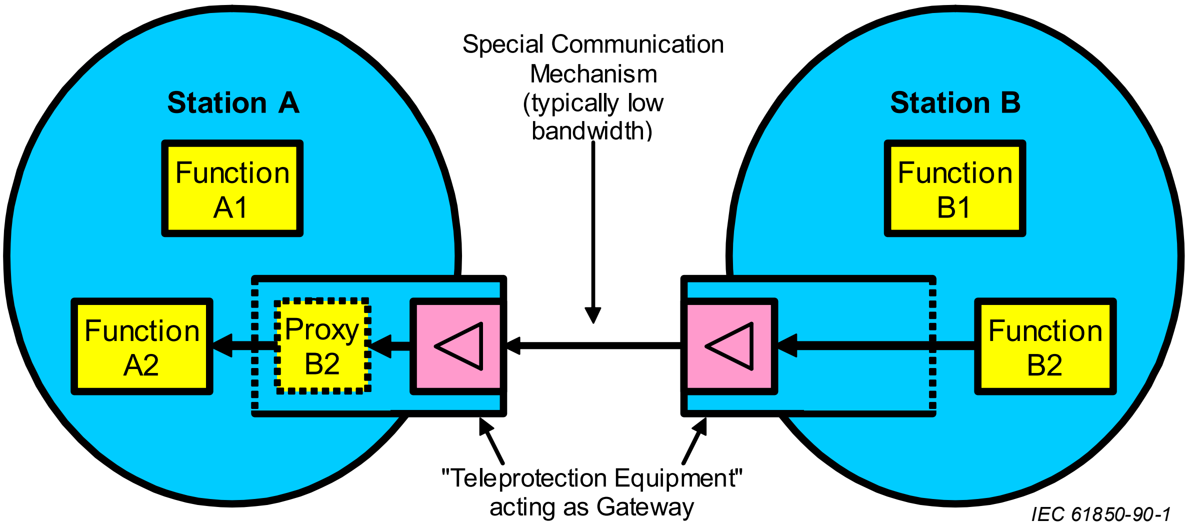

Special Communication Mechanism (typically low bandwidth)
Station A
Function A1
Function A2
Proxy B2
Station B
Function B1
Function B2
"Teleprotection Equipment" acting as Gateway
IEC 61850-90-1

Figure 18 SS to SS Communication via Proxy Gateway

From A2's perspective, Proxy B2 is providing the subset of information required for A2.The teleprotection equipment can provide other features to make efficient use of the communication mechanism. E.g. for GOOSE, only state changes might be actually transferred, while the retransmissions with constant state information may be filtered out at the sending side and the retransmission are locally re-created in the proxy. Missing retransmissions at the sending side must then be signalled via status information between the teleprotection equipment to the proxy.

Open issue: A2 in Fig. 18 is not the same function as A2 in Fig 17.

9 Modelling

Open issue: Comment which uses cases of Sec. 5 can be modelled without additional LNs.

9.1 General Architecture

The Gateway Approach:

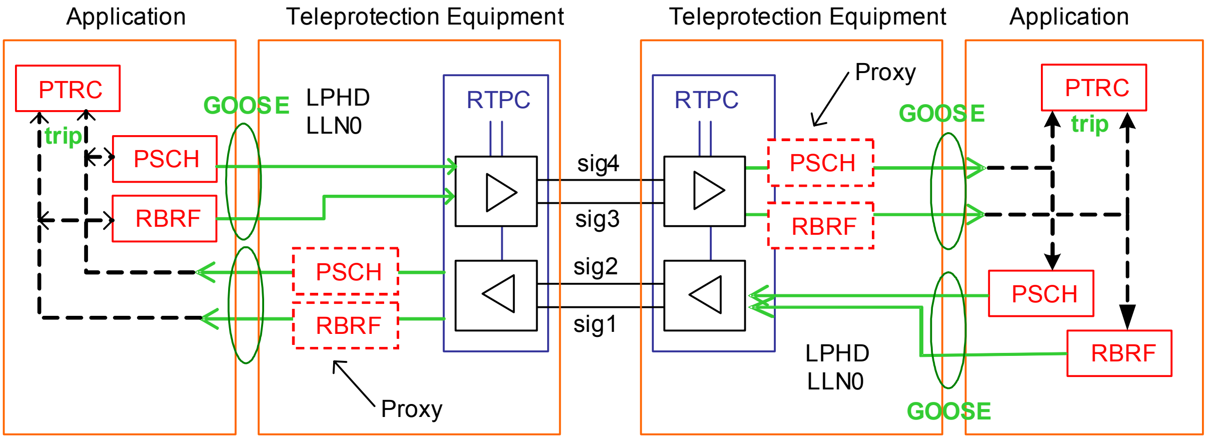


Figure 19 Allocation of the LN RTPC representing the communication channel and the LNs providing the data to be exchanged between substations

9.2 Communication interface RTPC

The LN RTPC comprises all information for communication channel setting and supervision. RTPC is not intended to generate direct process data. Thus, it does not contain the input and output data to be transmitted and it has no 'operate' data object.

Note: EEHealth is used to indicate the state of the communication channel, whereas PhyHealth is used to indicate the state of the (physical) communication device. If RTPC receives a GOOSE message with quality attribute "invalid" or "questionable" or no GOOSE message at all within Tmax, it will set PhyHealth to "Warning". Other actions are a local issue.

RTPC class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
Data				
Common Logical Node Information				
		LN shall inherit all Mandatory Data from Common Logical Node Class		M
Measured Values				
BerCh	MV	Bit Error Rate of the communication channel. Used in case of a digital communication channel		O
FerCh	MV	Frame Error Rate of the communication channel. Used in case of a digital communication channel. May be vendor specific		O
LoopTestTm	MV	Time measured at last loop test		O
CarrierLevel	MV	Power of received signal in case of an analogue communication channel		O
SNR	MV	Signal to noise ratio in dB, used in case of analogue communication.		O
Status Information				
EEHealth	INS	Communication channel health		M
GrdRxCmdRx	SPS	Alarm situation: Guard received together with the command, may indicate interference on the channel. Used in case of an analogue communication channel.		O

LosOfSignal	SPS	Alarm situation: No signal received, indicates a channel problem		O
TxCmdCnt1	INS	For diagnostics: Transmitted commands counters (for each command)		O
RxCmdCnt1	INS	For diagnostics: Received commands counters (for each command)		O
LosOfSyn	SPS	Alarm situation: Loss of synchronism. Indicates that there is no synchronization between the transmitter and the receiver, i.e., no communication is possible. Used in case of a digital communication channel.		O
Settings				
NumTxCmd	ING	Number of used binary transmit commands		O
NumRxCmd	ING	Number of used binary receive commands		O
TpcTxMod1	ING	Teleprotection application mode in Transmit direction for each command (Unused, Blocking, Permissive, Direct, Unblocking, Status)		O
TpcRxMod1	ING	Teleprotection application mode in Receive direction for each command (Unused, Blocking, Permissive, Direct, Unblocking, Status)		O
SecTmms	ING	Pickup security timer on loss of carrier guard signal: if a command is received within SecTmms after the guard has disappeared this command is considered valid, used in case of an analogue communication channel.		O
BoostRatiodB	ING	Level of increased power during the transmission of a command in dB. Used in case of an analogue communication channel		O
TxPwrPEPdBm	ING	Transmit power (peak envelope power) in dBm. Used in case of an analogue communication channel		O
TxCtrHz	ING	Transmit center frequency. Used in case of an analogue communication channel		O
RxCtrHz	ING	Receive center frequency. Used in case of an analogue communication channel		O
TxBwHz	ING	Transmit bandwidth. Used in case of an analogue communication channel		O
RxBwHz	ING	Receive bandwidth. Used in case of an analogue communication channel		O

Table 1 Logical node RTPC

9.3 Communication-aided protection schemes and direct tripping

9.3.1 Proposed model

This model is applicable for the following use cases (acc. to chapter 5):

Distance line protection with permissive tele-protection scheme
Distance line protection with blocking tele-protection scheme
Directional comparison protection
Transfer/Direct Tripping

State comparison protection schemes and direct trip signals shall be modelled by use of the logical node PSCH. The protection scheme requires the transmission of at least one binary signal from the protection device from one line end to the remote line end.

As an example the following figure shows the relation between protection application and logical modelling according to IEC 61850.

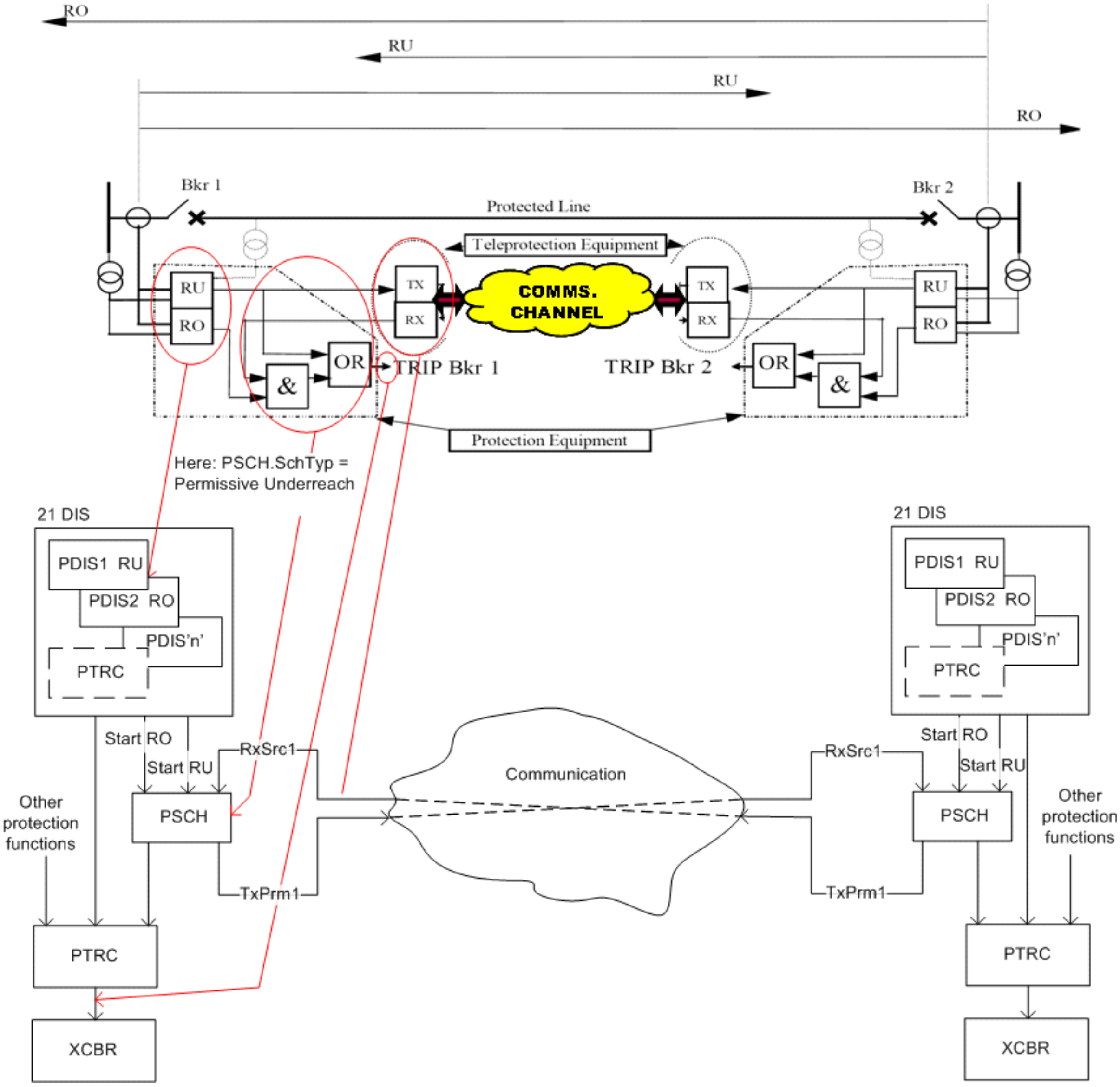


Figure 20 Protection application example for permissive underreach distance teleprotection scheme and appropriate logical node modelling

9.3.2 LN PSCH

PSCH class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
Data				
Common Logical Node Information				
		LN shall inherit all Mandatory Data from Common Logical Node Class		M
OpCntRs	INC	Resetable operation counter		O
Status Information				
TxPrm	ACT	Permissive information to be transmitted to the other side (Teleprotection permissive signal)	T	O
TxBlk	ACT	Blocking information to be transmitted to the other side (Teleprotection blocking signal)	T	O

PSCH class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
TxTr	ACT	Direct trip information to be transmitted to the other side	T	O
RxPrm1	ACT	Activation information RxPrm1 received from the other side(s), for logging purposes (Teleprotection permissive signal received)	T	O
RxBlk1	ACT	Activation information RxBlk1 received from the other side(s), for logging purposes (Teleprotection blocking signal received)	T	O
RxTr1	ACT	Activation information RxTr1 received from the other side(s), for logging purposes (direct trip signal received)		O
Op	ACT	Operate	T	M
Echo	SPS	TxPrm is being sent as echo signal (in case of weak infeed)	T	O
WeiOp	SPS	Indicates operate from weak end infeed function (typically with undervoltage control)	T	O
Blk	SPS	Teleprotection in blocked state		O
Configuration				
RxSrc1	ORG	Source for activation information RxPrm or RxBlk, must refer to data of type ACT		O
RxSrcTr1	ORG	Source for activation information RxTr, must refer to data of type ACT		O
Settings				
OpDlTmms	ING	Operate Delay Time		O
CrdTmms	ING	Co-ordination timer for blocking scheme		O
DurTmms	ING	Minimum duration of TxPerm in case of operate of PSCH		O
UnBlkMod	ING	Unblock function mode for scheme type		O
UnBlkTmms	ING	Unblocking time (check application??)		O
WeiMod	ING	Mode of weak end infeed function		O
WeiTmms	ING	Co-ordination time for weak end infeed function		O

Table 2 Logical node PSCH

Depending on the trip mode requirements the data exchange can be implemented with one general send/receive signal (e.g. PSCH.TxPrm.general) or with three phase selective send/receive signals (e.g. PSCH.TxPrm.phsA, PSCH.TxPrm.phsB, PSCH.TxPrm.phsC).

9.4 Differential protection schemes

9.4.1 Proposed model

This proposal is applied to the communication between substations. Practically it will be applied to the communication between protection relays and telecom equipment as shown Interface (A) in Fig.9.2..1 and Fig.9.2..2. Fig.9.2..1 is based on existing system. Fig.9.2..2 show the system when process bus is available.

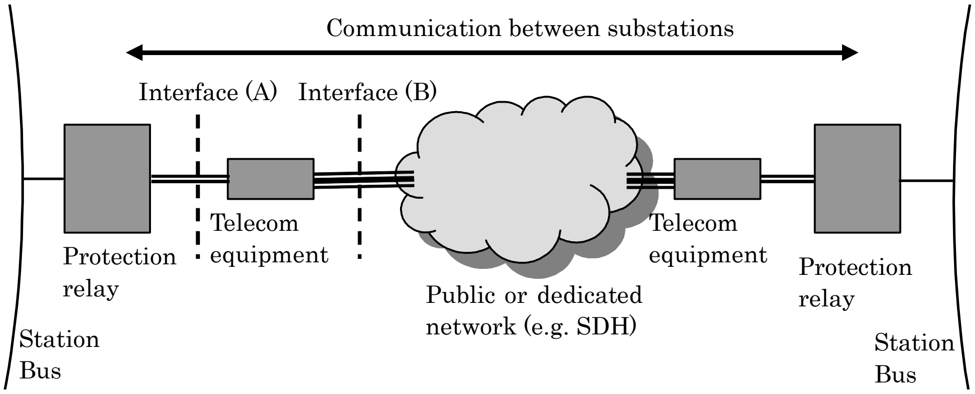


Fig.9.2.1 Communication system based on current system

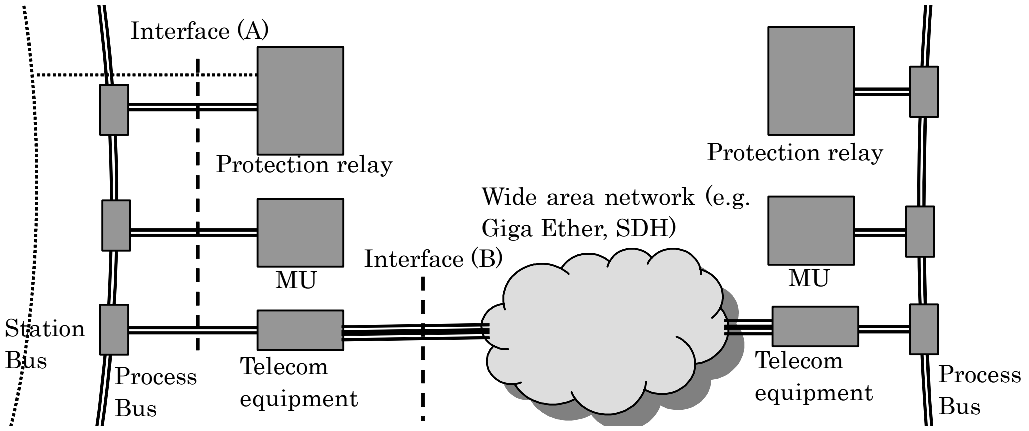


Fig.9.2.2 Communication system based on future system

Basically interface (B) is out of this scope. However if Ethernet is applied to the communication network, interface (B) will be equivalent to the interface (A).

This model can be drawn as Fig.9.2.3 for 2-terminal model and as Fig.9.2.4 for 3-terminal model.

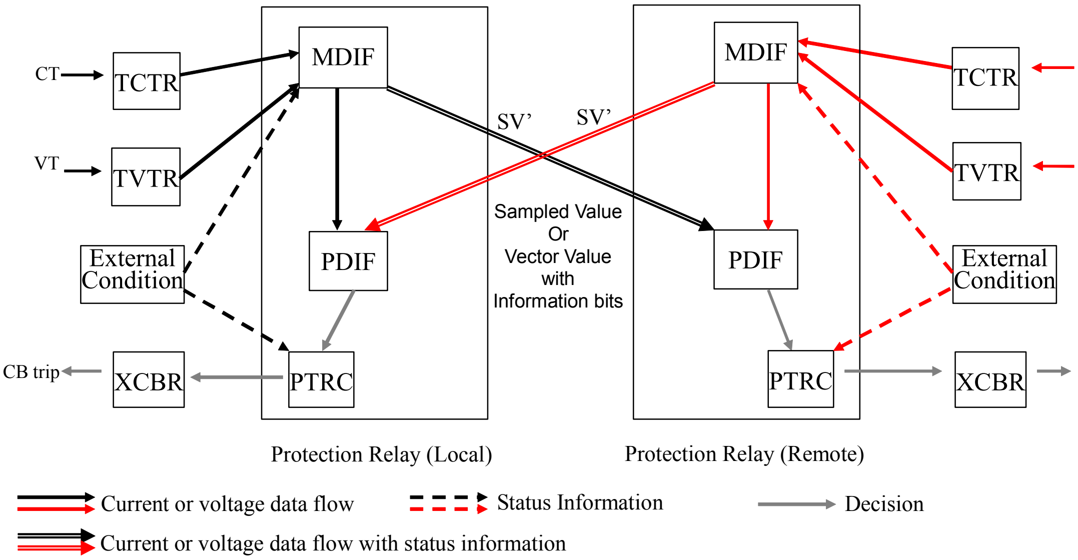

CT
VT
TCTR
TVTR
External Condition
XCBR
CB trip
MDIF
PDIF
PTRC
SV’
SV’
Sampled Value Or Vector Value with Information bits
MDIF
PDIF
PTRC
TCTR
TVTR
External Condition
XCBR
Protection Relay (Local)
Protection Relay (Remote)
Current or voltage data flow
Status Information
Decision
Current or voltage data flow with status information

Fig.9.2.3 Proposed 2-terminal current differential feeder protection relay model

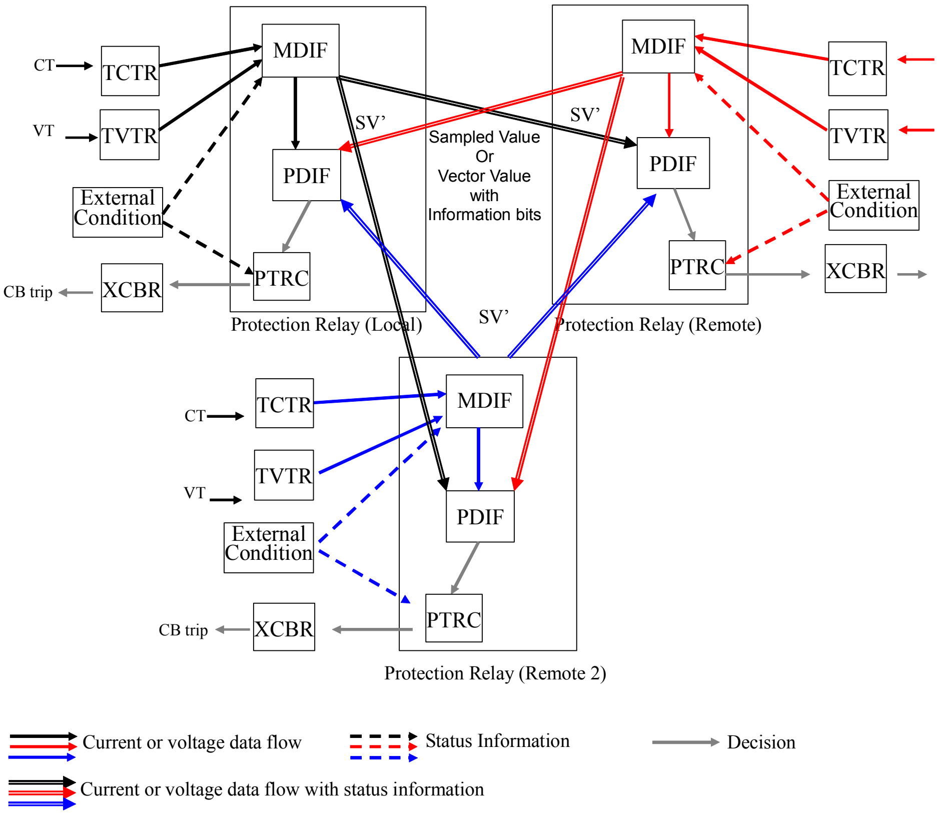


Fig.9.2.4 Proposed 3-terminal current differential feeder protection relay model

9.4.2 LN MDIF

As explained in previous section, logical node MDIF needs to be modified as follows.

LN: Differential measurements Name: MDIF

This LN shall be used to provide calculated process values representing the local calculation result which is sent to the remote end and is used for local differential protection (PDIF). The

LN MDIF is also used with function 87 according to IEEE device function number designation (IEEE 32 R.2 1996)

MDIF class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName	....	Shall be inherited from Logical-Node Class (see IEC61850-7-2)		
Data				
Common Logical Node Information				
		LN shall inherited all Mandatory Data from Common Logical Node Class		M
Measured values				
OpARem	WYE	Operate Current (Phasor) of the ~~remote~~ local current measurement		C
Amp	SAV	Operate Current (Sampled value) of the local current measurement		C
Status [1..n]	INT16U	Local status according to predetermined format		O

Condition C : Either OpARem or Amp shall be used

If possible, number of status should be configurable.

9.4.3 Extension of SV format

As explained in previous section, SV needs to be modified to be able to send phasor data and status data as follows.

Sampled value (SV) format definition

Sampled value format		
Parameter name	**Parameter type**	**Value/value range/explanation**
MsvID or **UsvID**	VISIBLE STRING65	Value from the **MSVCB** or **USVCB**
OptFlds	a	Optional fields to be included in the SV message
DatSet	ObjectReference	Value from the **MSVCB** or **USVCB**
Sample [1..n]		
Value	(*)	(*) type depends on the common data classes defined in IEC 61850-7-3. The parameter shall be derived from MSV/USV control
SmpCnt	INT16U	Sample counter
RefrTm	EntryTime	OPTIONAL; time of refresh activity
ConfRev	INT32U	Configuration revision number from the instance of **MSVCB** or **USVCB**
SmpSynch	BOOLEAN	OPTIONAL; samples are synchronized by clock signals
SmpRate	INT16U	OPTIONAL; sample rate from the instance of **MSVCB** or **USVCB**
a The type and value of this parameter shall be derived from the attribute **OptFlds** of the respective **USVCB** or **MSVCB**		

Application for the three or more end terminals, MSVCB shall be used. USVCB shall be used for two-terminal application. MSVCV and USVCB are shown in the appendix for the reference.

Existing SV format is also shown in appendix.

9.4.4 Requirement for communication

9.4.4.1 Requirement for current communication network

General requirements for data and communication are following.

- Propagation delay affects the operating time. Therefore a small propagation delay is needed for differential protection. An especially small propagation delay is required for EHV, HV feeder protection(e.g. Less than 6ms for EHV, HV feeders, less than 20ms for LV feeders)
- Any change of the propagation delay must be very small in order that the relays establish sampling synchronisation by themselves (e.g. less than 0.2ms for synchronisation). When a reliable external signal (e.g. GPS signal) is available and external signal synchronisation is applied to the relay, the requirement for changes of the propagation delay is not very strict (e.g. less than 20ms)
- High quality (e.g. BER less than 10^{-6})

Requirement for propagation delay

	Propagation Delay (T_A)	Typical application
Class 1	6ms	HV, EHV
Class 2	20ms (1cycle at 50Hz)	LV
Class 3	40ms (2 cycles at 50Hz)	LV

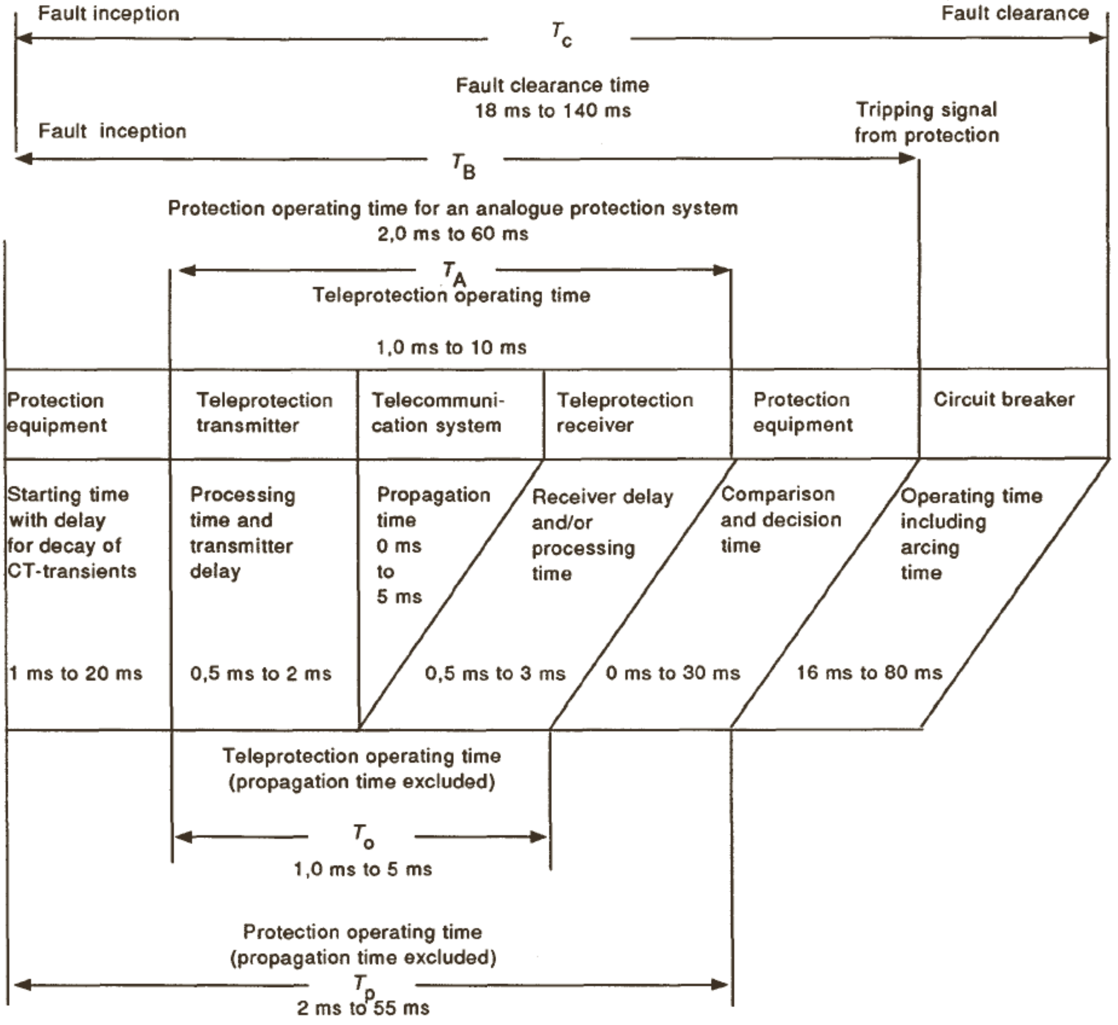
Requirement for change of propagation delay

	Change of propagation delay(ΔT_A)	Typical application
Class 1	0.2 ms	Self synchronisation
Class 2	10ms	External signal synchronisation
Class 3	20ms	External signal synchronisation

Requirement for quality

	BER	Typical application
Class 1	10^{-6}	Differential protection

Propagation delay is explained in IEC60834 as shown in the Fig.9.2..6.


Fault inception
T_c
Fault clearance
Fault clearance time
18 ms to 140 ms
Fault inception
Tripping signal from protection
T_B
Protection operating time for an analogue protection system
2,0 ms to 60 ms
T_A
Teleprotection operating time
1,0 ms to 10 ms
Protection equipment
Teleprotection transmitter
Telecommunication system
Teleprotection receiver
Protection equipment
Circuit breaker
Starting time with delay for decay of CT-transients
Processing time and transmitter delay
Propagation time 0 ms to 5 ms
Receiver delay and/or processing time
Comparison and decision time
Operating time including arcing time
1 ms to 20 ms
0,5 ms to 2 ms
0,5 ms to 3 ms
0 ms to 30 ms
16 ms to 80 ms
Teleprotection operating time (propagation time excluded)
T_o
1,0 ms to 5 ms
Protection operating time (propagation time excluded)
T_p
2 ms to 55 ms

Acceptable protection operating time may be increased under noisy conditions, i.e. T_{pac}. The relationship between T_{pac}, dependability and signal-to-noise ratio is illustrated in figure 4.

Figure 2 – Typical operating times for analogue comparison protection systems

Fig.9.2.6 Explanation of propagation delay in IEC60834

9.4.4.2 Symmetry of communication network for current differential

If the difference of the propagation times between going and coming is fixed, self synchronisation can be applied even if the communication is asymmetrical. Therefore the symmetry of the communication is not mandatory for self synchronisation. Nevertheless it is more secured for self synchronisation if symmetry of the communication is ensured especially when there is a possibility of the switching of the communication. Therefore it is useful to know whether the communication is symmetrical or asymmetrical.

Information for network symmetry

	Symmetry	Typical application
Class 1	Symmetrical	Self synchronisation
Class 2	Asymmetrical	External signal synchronisation

10 Configuration aspects

The practical approach to system configuration depends on the kind of communication system architecture as well as the split of responsibility between the engineering in the concerned substations. The following two scenarios relate to the direct communication connection (Figure 17 SS to SS Communication via Tunnel) with one method, and a dedicated tele-protection equipment hiding the communication between the two substations (Figure 18 SS to SS Communication via Proxy Gateway) as a second method.

10.1 Direct communication link

For high bandwidth wide area connections the IEC61850 Ethernet frame can be directly mapped to a wide area Ethernet connection. This corresponds then to a switch in the Ethernet architecture, with possibly lower performance (throughput, delay) than a real switch. To reduce the load on this 'switch', the data sent between substations should belong to an own VLAN.

Switches are currently not modelled in SCL. However, the data flow from some IEC 61850 IED in one substation to some appropriate IED in the other substation has to be described. In a meshed power network with all lines needing SS – SS communication, this can end up in the situation that the whole power network with all substations and substation IEDs must appear within one SCL file. As normally for a certain engineering purpose the concerned IEDs only have to know a part of the other system(s), it seems to be appropriate to use 'System interface Exchange Descriptions' (SED), which contain only a part of the overall system to be engineered for a certain purpose. This SED file is then transferred from one substation project to the other project, to include the needed DATA into the data flow. The engineered data flow then is transferred back to the originating system / project by means of an enhanced SED file, so that both systems then have the same consistent state regarding the data to be exchanged between them across the connecting Ethernet link.

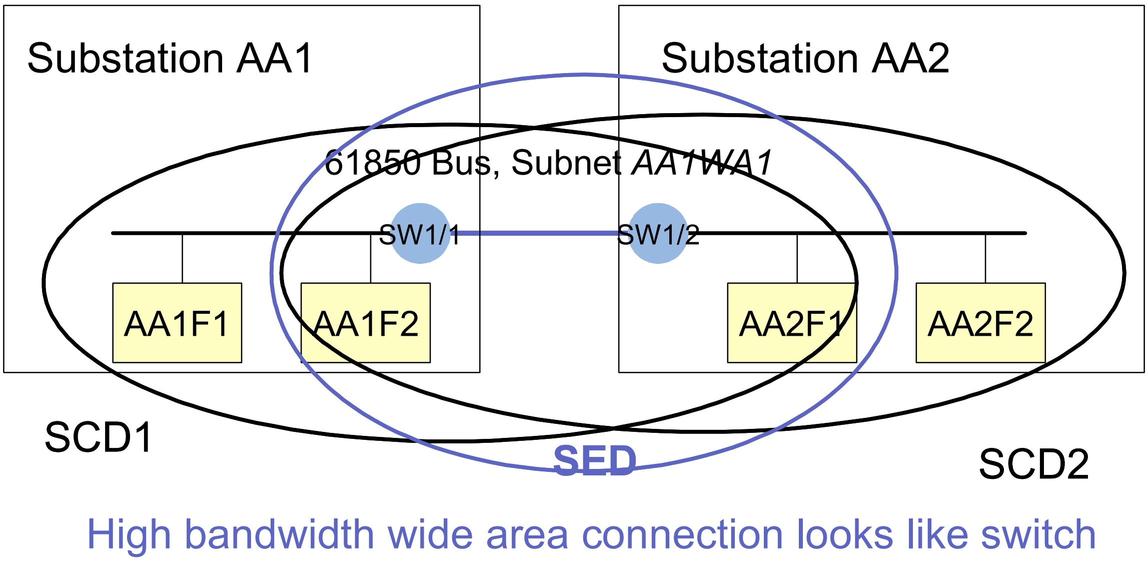

Substation AA1
Substation AA2
61850 Bus, Subnet *AA1WA1*
SW1/1
SW1/2
AA1F1
AA1F2
AA2F1
AA2F2
SCD1
SED
SCD2
High bandwidth wide area connection looks like switch

Figure 21: SCD files and SED region for SS – SS communication

From the view of the concerned tools this means that several system configuration tools exist, each responsible to configure a certain part of the overall system, i.e. each 'owner' of a certain amount of IEDs. We call a set of IEDs, which is engineered and also configured by a system tool and its connection to the corresponding IED tools, a **project**. These projects (project system configuration tools) exchange engineering data, which describe the overlapping parts. These overlapping parts are for some projects a boundary part, which they are not allowed to change, or only to change in a limited way before re-export to the 'owner' of this part. Only the IED owner project is allowed to give an SCD file to the IED tool for IED configuration. See Figure 22 for this engineering process.

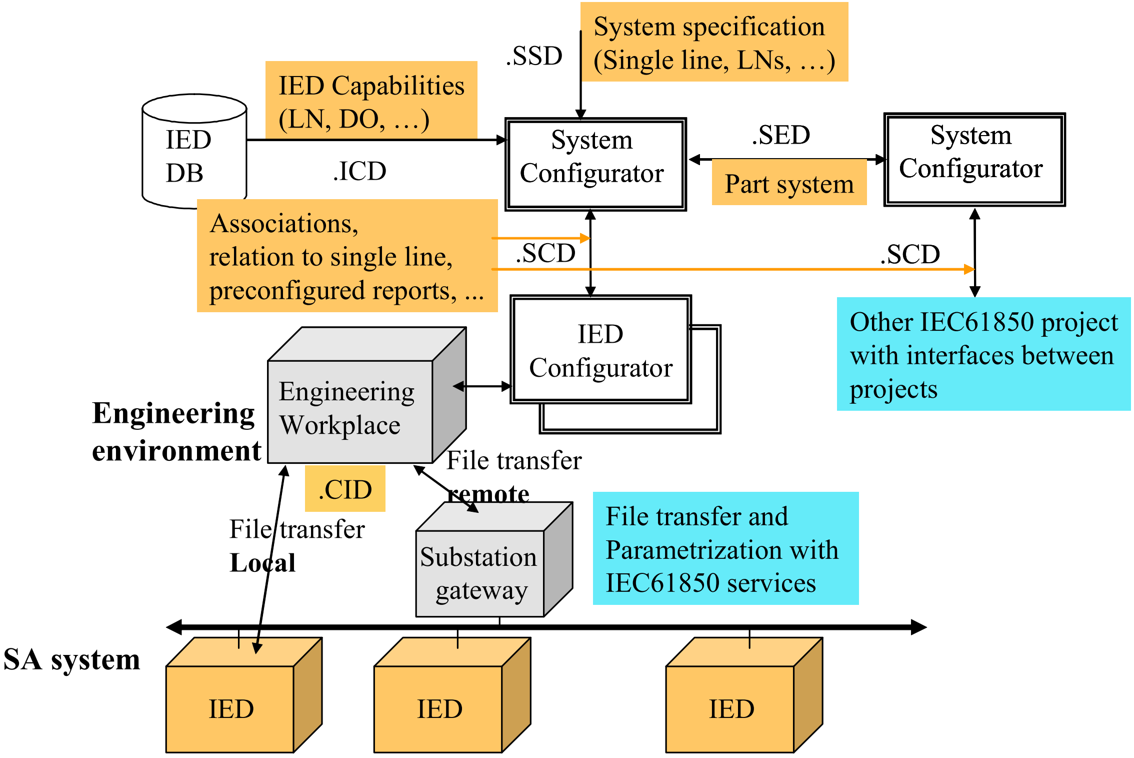


Figure 22 - Enhanced engineering process

In Figure 21 the IEDs AA1F1 and AA1F2 are owned by the system tool handling the AA1 project (substation), while AA2F1 and AA2F2 are owned by the system tool handling the AA2 project. AA1F2 is a 'boundary' IED for the AA2 project, while AA2F1 is a boundary IED for the AA1 project.

Important for SED files is how they are handled at export and import of the system configuration tools. For this purpose, at export a system tool can decide which kind of engineering rights another system tool might have. The engineering rights as defined in IEC61850-6 are shown in the following table.

It should be remembered, that the only tool which is allowed to change the IED data model, is the IED tool. So, changes of data model are only allowed by the IED tool, and the handling after system integration is described in IEC61850-6.

IED Engineering right	Meaning / purpose	Export handling	Import handling	Remarks
fix	Fix boundary IED, no change allowed by other tools; ownership stays at exporting project (system tool)	Only those parts of the data model (access points, LDevice, LNs) and data flow definitions (data sets, control blocks) are exported, which are already referenced by the dataflow IEDs in this SED. All version information shall be in the exported parts.	If the importing project is the owner, then the IED is ignored and only the internal state set to full again. Is imported, if it does not exist. If it exists as fix / dataflow IED with lower version info, the old IED has to be replaced. If it exists as dataflow IED with same version, state should be set to fix.	Changes allowed only at owner. Might be referenced as client in owned IEDs.
dataflow	Boundary IED, additions in data flow definitions are allowed in the limits	Only those parts of the data model (access points, LDevice, LNs) and data flow definitions	If the importing project is the owner, the part must be checked for added data sets, control blocks, data flow	Changes at owner are blocked after export; at importing projects:no change of

	of the IED engineering capability (especially new client references); ownership stays at exporting project	(data sets, control blocks) are exported, which are needed / allowed for further engineering. Note that if new clients can be added for report control blocks, then all existing clients must also be contained at least as fix IEDs, else the RCB instance allocation would be disturbed. Similar it is with input section references.	definitions (also in existing control blocks) and new Input sections, and these modified / imported; then state is set to full again. This might mean that previously all other IEDs of the SED have to be imported, which are referenced. If the owner is some other project, it is imported. If it exists already, the versions of existing parts should be checked, and only newer parts imported, replacing existing parts.	data model allowed, no removal of already engineered parts, no change in existing data sets & control blocks (confRev unchanged). Only additions of DS and CBs are allowed. Engineering capabilities can be restricted at export by setting the capability options appropriately.
full	Full engineering of data flow is allowed. This right can not be formally transferred	Not allowed to export in a SED file.	Should not appear within a SED file – stop import	

Table 3 - IED engineering control types

When an IED is exported to a SED file, then the IED ownership is marked by means of the (new) *owner* attribute of the IED, which is set to the SCD header identification respective project identification, and an IED exported as *dataflow* is blocked for changes within the owning system tool, e.g. by setting it to fix.

If a *dataflow* IED with same owner id as the project id is re-imported, then the change block is taken away again. The owner attribute at IEDs with fix and dataflow engineering right marks to which project they belong, to block changes at the owner after dataflow export.

The different IED states within a project and the triggers from one to the other are shown in Figure 23. Observe that there are two automata. One is valid in case that a system configuration tool starts with full control, the other is for an IED imported with dataflow control.

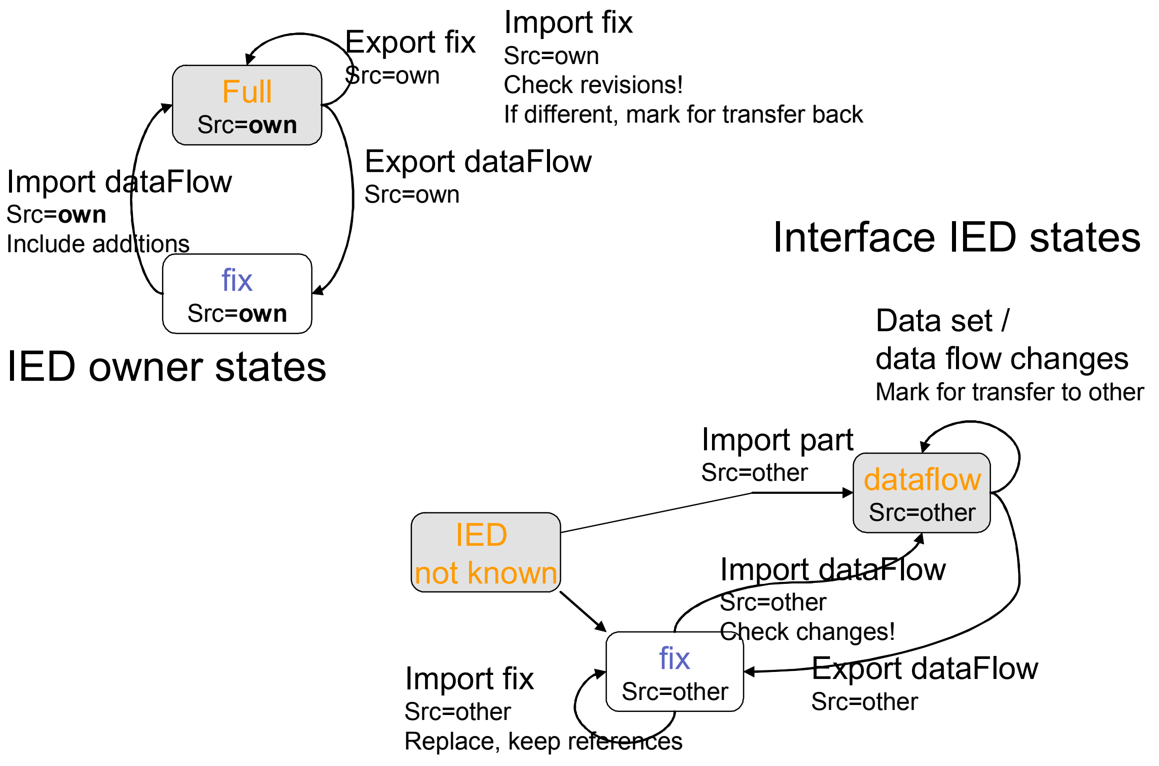


Figure 23 - IED states when exchanging SED files

Above definitions only concern IED sections. IEDs can also be referenced by the Communication section, and by the Substation section. Therefore these must also be considered:

- **Communication section**: all parts belonging to exported IEDs respective IED parts must be contained. For part IEDs and fixed IEDs only those parts of access points and control block parameters shall appear, which are still contained in the exported IED part. Both is not allowed to be changed. If address coordination is an issue, all access points with addresses can be exported (and the IED as fix, just containing the access point).
- **Substation section**: All elements down to bay, which contain references to LNs on some of the exported IEDs, have also to be exported, inclusive the references to IEDs to be exported. For any concerned bay its topology as well as primary equipment has to be exported completely, only references to logical nodes not contained in the exported part are allowed to be removed. No links are allowed to be modified or added for exported IEDs, just for newly introduced own IEDs. Also new bays and new IEDs might be added, but it is not allowed to delete bays or primary equipment.

It might happen, that several SED files from the same system part are exported at different points in time. Each of them shall have an identification and a revision index with time of modification. This allows identifying the latest version of a certain SED file, which then also indicates a specific purpose respective an export to a specific project. It is the responsibility of the importing project engineer, to identify different SED files and their versions. In any case, any owned IED marked as fix should only be exported as fix, if needed at all.

It is the responsibility of the project engineer as well as the exporting system tool, that a SED file containing IEDs with dataflow right for a certain engineering purpose is only used for this purpose, and not in parallel for another purpose in another (third) system tool / project. This also includes that an exporting system tool is only allowed to export dataflow IEDs once for a certain purpose, and not a second time in parallel as dataflow IED for another purpose, before the possibly modified IED has been again re-imported. Fixed IEDs can be exported as fix in parallel as often as needed, because they do not have to be re-imported. The owner attribute value at fix and dataflow IEDs supports the system tool to remember, that it is the 'owner' of the IED, so that it can reset the state to 'full' after a re-import of the IED.

10.1.1 SCL enhancements

For the purpose defined above, the following SCL enhancements are introduced (see IEC61850-6):

a) Optional attribute **engRight** at the IED element with values fix, dataflow; the default value, if missing, is full, which is not allowed within a SED file.
b) Optional attribute **owner** of type string at the IED element with default value identical to the Header id. This id contains the SCL ID / project ID of the system configurator project, which has exported this IED to a SED file. The SED identification must be different from the owner values.

An example of a SED file for SS-SS communication is contained in the next clause.

10.1.2 SCL example

The example is based on the system configuration of Figure 21. The engineering process in this case works as follows:

a) Project AA2 exports a SED file for IED AA2F1, with AA2F1 as data flow IED, and all needed source IEDs as fix IEDs.
b) Project AA1 imports the SED file, and engineers the data flow between AA1F2 and AA2F1.
c) Project AA1 now can configure AA1F2 with its IED tool; then it exports a SED file with same identification as the imported SED, containing AA1F2 as fixed IED and AA2F1 as

original data flow IED (plus all needed source IEDs as fix) with the added data flow definitions.

d) Project AA2 imports the SED file, and finalizes any engineering on AA2F1 based on its now complete system description; now AA2F1 can be configured by its IED tool.

Note that it is the responsibility of the project engineer, to communicate any project changes (e.g. in project AA1) which influence the boundary IEDs owned by other projects (e.g. AA2F1 in project AA2), to the appropriate project. If this is forgotten, a sudden failure in communication especially with GOOSE and SAV services between the concerned IEDs might happen due to mismatch of message confRev values.

An alternative engineering approach could have been to export AA2F1 in step1 as fix, but with already preconfigured data set and control block to be sent to AA2F1. In this case within step 2 only the data flow from AA1F2 to AA2F1 could be engineered, and within step 4 the still missing data flow from AA1F2 to AA2F1 has to be added. This simplifies the tasks of the tools, because they have only to handle import and export of fix IEDs, however might complicate the engineering, because the complete communication engineering between AA1F2 and AA2F1 has been split into several parts (steps 1, 2, 4) instead of one step (step 2). Especially, it can not be indicated in step 1, that AA1F2 is the GOOSE client of AA2F1.

The following shows the SED file example to be imported in engineering step 4. It also contains the modelling of the line connection between the two substations as ConductingEquipment of type LIN (overhead line), to make the primary system modelling complete and show, that the two bays in the substations are connected by a common line. Further, the protection IED AA1FP2, which in principle is the same IED type as AA2FP1, is exported as fix, and therefore only the relevant (interface) parts for AA1FP2 are contained in it. It might contain more, but this is not necessary.

```
<?xml version="1.0"?>
<SCL xmlns:sxy="http://www.iec.ch/61850/2003/SCLcoordinates" xmlns="http://www.iec.ch/61850/2003/SCL">
 <Header id="SS-SS AA1 - AA2" toolID="SSI-Tool" nameStructure="IEDName" />
 <Substation name="AA1" desc="Substation">
  <VoltageLevel name="D1" desc="Voltage Level">
   <Bay name="Q1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
    <LNode iedName="AA1FP1" ldInst="LD1" lnClass="PTOC" lnInst="1" />
    <LNode iedName="AA1FP1" ldInst="LD1" lnClass="PTRC" lnInst="1" />
    <LNode iedName="AA1FP1" ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" />
    <LNode iedName="AA1FP1" ldInst="LD1" prefix="F21" lnClass="PDIS" lnInst="1" />
    <ConductingEquipment name="BI1" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="15"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
     <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QC2" desc="Isolator" type="DIS" sxy:x="10" sxy:y="21" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
     <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BU2" desc="Voltage Transformer 3Phase" type="VTR" sxy:x="12" sxy:y="14"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QB2" desc="Isolator" type="DIS" sxy:x="12" sxy:y="4" sxy:dir="vertical">
     <Terminal name="AA1D1QBBN4" connectivityNode="AA1/D1/QBB/N4" substationName="AA1"
voltageLevelName="D1" bayName="QBB" cNodeName="N4" />
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
    </ConductingEquipment>
    <ConductingEquipment name="QC1" desc="Isolator" type="DIS" sxy:x="10" sxy:y="8" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
     <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BI3" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="19"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
     <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
    </ConductingEquipment>
    <ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="8" sxy:y="11" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
    </ConductingEquipment>
    <ConductingEquipment name="BI2" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="17"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
     <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
    </ConductingEquipment>
    <ConductingEquipment name="QB1" desc="Isolator" type="DIS" sxy:x="6" sxy:y="4" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
     <Terminal name="AA1D1QBBN1" connectivityNode="AA1/D1/QBB/N1" substationName="AA1"
voltageLevelName="D1" bayName="QBB" cNodeName="N1" />
    </ConductingEquipment>
    <ConductingEquipment name="QB4" desc="Isolator" type="DIS" sxy:x="8" sxy:y="23" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
     <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
    </ConductingEquipment>
    <ConductingEquipment name="QC3" desc="Isolator" type="DIS" sxy:x="10" sxy:y="35" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
     <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConnectivityNode name="N1" pathName="AA1/D1/Q1/N1" sxy:x="8" sxy:y="31" />
    <ConnectivityNode name="N2" pathName="AA1/D1/Q1/N2" sxy:x="8" sxy:y="16" />
    <ConnectivityNode name="N3" pathName="AA1/D1/Q1/N3" sxy:x="9" sxy:y="13" />
    <ConnectivityNode name="N6" pathName="AA1/D1/Q1/N6" sxy:x="8" sxy:y="21" />
    <ConnectivityNode name="N5" pathName="AA1/D1/Q1/N5" sxy:x="9" sxy:y="6" />
    <ConnectivityNode name="N4" pathName="AA1/D1/Q1/N4" sxy:x="8" sxy:y="18" />
   </Bay>
   <Bay name="QBB" desc="Bay" sxy:x="63" sxy:y="36" sxy:dir="vertical">
    <ConnectivityNode name="N3" pathName="AA1/D1/QBB/N3" sxy:x="48" sxy:y="12" />
    <ConnectivityNode name="N2" pathName="AA1/D1/QBB/N2" sxy:x="47" sxy:y="17" />
    <ConnectivityNode name="N4" pathName="AA1/D1/QBB/N4" sxy:x="25" sxy:y="18" />
    <ConnectivityNode name="N1" pathName="AA1/D1/QBB/N1" sxy:x="22" sxy:y="20" />
   </Bay>
  </VoltageLevel>
 </Substation>
 <Substation name="AA2" desc="Substation">
  <VoltageLevel name="D1" desc="Voltage Level">
   <Bay name="Q1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
    <LNode iedName="AA2FP1" ldInst="LD1" lnClass="PTOC" lnInst="1" />
    <LNode iedName="AA2FP1" ldInst="LD1" lnClass="PTRC" lnInst="1" />
    <LNode iedName="AA2FP1" ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" />
    <LNode iedName="AA2FP1" ldInst="LD1" prefix="F21" lnClass="PDIS" lnInst="1" />
    <ConductingEquipment name="BI1" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="15"
sxy:dir="vertical">
     <Terminal name="AA2D1Q1N2" connectivityNode="AA2/D1/Q1/N2" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
     <Terminal name="AA2D1Q1N3" connectivityNode="AA2/D1/Q1/N3" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QC2" desc="Isolator" type="DIS" sxy:x="10" sxy:y="21" sxy:dir="vertical">
     <Terminal name="AA2D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
     <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BU2" desc="Voltage Transformer 3Phase" type="VTR" sxy:x="12" sxy:y="14"
sxy:dir="vertical">
```

```
     <Terminal name="AA2D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QB2" desc="Isolator" type="DIS" sxy:x="12" sxy:y="4" sxy:dir="vertical">
     <Terminal name="AA2D1QBBN4" connectivityNode="AA2/D1/QBB/N4" substationName="AA2"
voltageLevelName="D1" bayName="QBB" cNodeName="N4" />
     <Terminal name="AA2D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
    </ConductingEquipment>
    <ConductingEquipment name="QC1" desc="Isolator" type="DIS" sxy:x="10" sxy:y="8" sxy:dir="vertical">
     <Terminal name="AA2D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
     <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BI3" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="19"
sxy:dir="vertical">
     <Terminal name="AA2D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
     <Terminal name="AA2D1Q1N4" connectivityNode="AA2/D1/Q1/N4" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
    </ConductingEquipment>
    <ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="8" sxy:y="11" sxy:dir="vertical">
     <Terminal name="AA2D1Q1N3" connectivityNode="AA2/D1/Q1/N3" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
     <Terminal name="AA2D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
    </ConductingEquipment>
    <ConductingEquipment name="BI2" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="17"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N2" connectivityNode="AA2/D1/Q1/N2" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
     <Terminal name="AA1D1Q1N4" connectivityNode="AA2/D1/Q1/N4" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
    </ConductingEquipment>
    <ConductingEquipment name="QB1" desc="Isolator" type="DIS" sxy:x="6" sxy:y="4" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
     <Terminal name="AA1D1QBBN1" connectivityNode="AA2/D1/QBB/N1" substationName="AA2"
voltageLevelName="D1" bayName="QBB" cNodeName="N1" />
    </ConductingEquipment>
    <ConductingEquipment name="QB4" desc="Isolator" type="DIS" sxy:x="8" sxy:y="23" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N1" connectivityNode="AA2/D1/Q1/N1" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
     <Terminal name="AA1D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
    </ConductingEquipment>
    <ConductingEquipment name="QC3" desc="Isolator" type="DIS" sxy:x="10" sxy:y="35" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N1" connectivityNode="AA2/D1/Q1/N1" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
     <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConnectivityNode name="N1" pathName="AA2/D1/Q1/N1" sxy:x="8" sxy:y="31" />
    <ConnectivityNode name="N2" pathName="AA2/D1/Q1/N2" sxy:x="8" sxy:y="16" />
    <ConnectivityNode name="N3" pathName="AA2/D1/Q1/N3" sxy:x="9" sxy:y="13" />
    <ConnectivityNode name="N6" pathName="AA2/D1/Q1/N6" sxy:x="8" sxy:y="21" />
    <ConnectivityNode name="N5" pathName="AA2/D1/Q1/N5" sxy:x="9" sxy:y="6" />
    <ConnectivityNode name="N4" pathName="AA2/D1/Q1/N4" sxy:x="8" sxy:y="18" />
   </Bay>
   <Bay name="QBB" desc="Bay" sxy:x="63" sxy:y="36" sxy:dir="vertical">
    <ConnectivityNode name="N3" pathName="AA2/D1/QBB/N3" sxy:x="48" sxy:y="12" />
    <ConnectivityNode name="N2" pathName="AA2/D1/QBB/N2" sxy:x="47" sxy:y="17" />
    <ConnectivityNode name="N4" pathName="AA2/D1/QBB/N4" sxy:x="25" sxy:y="18" />
    <ConnectivityNode name="N1" pathName="AA2/D1/QBB/N1" sxy:x="22" sxy:y="20" />
   </Bay>
  </VoltageLevel>
 </Substation>
 <Substation name="AA12" desc="Line between AA1 and AA2">
  <VoltageLevel name="D1" desc="Line Voltage Level">
   <Bay name="W1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
    <ConductingEquipment name="WA1" desc="Overhead line" type="LIN" sxy:x="2" sxy:y="12" >
     <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
     <Terminal name="AA2D1Q1N1" connectivityNode="AA2/D1/Q1/N1" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
```

```
    </ConductingEquipment>
   </Bay>
  </VoltageLevel>
 </Substation>
 <Communication>
  <SubNetwork name="AA1WA1" desc="IEC61850 through both stations" type="8-MMS">
   <ConnectedAP iedName="AA2FP1" apName="S1">
    <Address>
     <P type="SA">0</P>
     <P type="IP">172.17.1.4</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-TSEL">0001</P>
     <P type="OSI-PSEL">00000001</P>
     <P type="OSI-SSEL">0001</P>
    </Address>
    <GSE ldInst="LD1" cbName="SSAA2dist">
     <Address>
      <P type="MAC-Address">01-0C-CD-01-02</P>
      <P type="APPID">2001</P>
     </Address>
     <MinTime unit="s">2</MinTime>
     <MaxTime unit="s">1000</MaxTime>
    </GSE>
   </ConnectedAP>
   <ConnectedAP iedName="AA1FP1" apName="S1">
    <Address>
     <P type="SA">0</P>
     <P type="IP">172.16.1.3</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-TSEL">0001</P>
     <P type="OSI-PSEL">00000001</P>
     <P type="OSI-SSEL">0001</P>
    </Address>
    <GSE ldInst="LD1" cbName="SSAA2dist">
     <Address>
      <P type="MAC-Address">01-0C-CD-01-01</P>
      <P type="APPID">2001</P>
     </Address>
     <MinTime unit="s">2</MinTime>
     <MaxTime unit="s">1000</MaxTime>
    </GSE>
   </ConnectedAP>
   <ConnectedAP iedName="AA2OPC1" apName="S1">
    <Address>
     <P type="SA">0</P>
     <P type="IP">172.17.0.100</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-TSEL">0001</P>
     <P type="OSI-PSEL">00000001</P>
     <P type="OSI-SSEL">0001</P>
    </Address>
   </ConnectedAP>
  </SubNetwork>
 </Communication>
 <IED name="AA2OPC1" type="OPCServer" manufacturer="XYZ" configVersion="1.0" engRight="fix"
owner="AA2" >
  <AccessPoint name="S1">
   <LN inst="1" lnClass="IHMI" lnType="IHMI_OPCServer_IEC61850" />
  </AccessPoint>
 </IED>
 <IED name="AA1FP1" type="REL316-4" manufacturer="ABC" configVersion="1.0" engRight="fix" owner="AA1" >
  <Services>
   <DynAssociation />
   <SettingGroups>
    <SGEdit />
   </SettingGroups>
   <GetDirectory />
   <GetDataObjectDefinition />
   <DataObjectDirectory />
   <GetDataSetValue />
   <ConfDataSet max="50" maxAttributes="240" />
   <ReadWrite />
   <ConfReportControl max="100" />
   <GetCBValues />
   <ReportSettings datSet="Conf" rptID="Dyn" optFields="Dyn" bufTime="Dyn" trgOps="Dyn" intgPd="Dyn" />
   <GSESettings datSet="Conf" appID="Conf" />
   <GOOSE max="20" />
  </Services>
  <AccessPoint name="S1">
   <Server>
    <Authentication none="true" />
    <LDevice inst="LD1">
     <LN0 inst="" lnClass="LLN0" lnType="LLN0_REL316-4_IEC61850">
      <DataSet name="PSCHtoAA2">
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="general" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsA" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsB" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsC" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="q" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="ProRx" daName="stVal" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="ProRx" daName="q" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="WeiOp" daName="general" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="WeiOp" daName="q" fc="ST" />
      </DataSet>
      <GSEControl name="SSAA2dist" desc="to AA2" datSet="PSCHtoAA2" confRev="1" appID="">
       <IEDName>AA2FP1</IEDName>
      </GSEControl>
     </LN0>
     <LN inst="1" lnClass="PSCH" lnType="F21_Distance Scheme_REL316-4_IEC61850" prefix="F21" />
     <LN inst="1" lnClass="LPHD" lnType="Physical Device_REL316-4_IEC61850" />
    </LDevice>
   </Server>
  </AccessPoint>
 </IED>
 <IED name="AA2FP1" type="REL316-4" manufacturer="ABC" configVersion="1.0" engRight="dataflow"
owner="AA2" >
  <Services>
   <DynAssociation />
   <SettingGroups>
    <SGEdit />
   </SettingGroups>
   <GetDirectory />
   <GetDataObjectDefinition />
   <DataObjectDirectory />
   <GetDataSetValue />
   <ConfDataSet max="50" maxAttributes="240" />
   <ReadWrite />
   <ConfReportControl max="100" />
   <GetCBValues />
   <ReportSettings datSet="Conf" rptID="Dyn" optFields="Dyn" bufTime="Dyn" trgOps="Dyn" intgPd="Dyn" />
   <GSESettings datSet="Conf" appID="Conf" />
   <GOOSE max="20" />
  </Services>
  <AccessPoint name="S1">
   <Server>
    <Authentication none="true" />
    <LDevice inst="LD1">
     <LN0 inst="" lnClass="LLN0" lnType="LLN0_REL316-4_IEC61850">
      <DataSet name="PSCHtoAA1">
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="general" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsA" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsB" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="phsC" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="Op" daName="q" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="ProRx" daName="stVal" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="ProRx" daName="q" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="WeiOp" daName="general" fc="ST" />
       <FCDA ldInst="LD1" prefix="F21" lnClass="PSCH" lnInst="1" doName="WeiOp" daName="q" fc="ST" />
      </DataSet>
      <DataSet name="StatUrgentA" desc="Status Data used to update process pictures and to generate alarms.">
       <FCDA ldInst="LD1" prefix="" lnClass="LPHD" lnInst="1" doName="Alm1" fc="ST" />
       <FCDA ldInst="LD1" prefix="" lnClass="PTRC" lnInst="1" doName="Op" fc="ST" />
       <FCDA ldInst="LD1" prefix="" lnClass="TVTR" lnInst="1" doName="FuFail" fc="ST" />
      </DataSet>
      <ReportControl name="rcb_A" rptID="" datSet="StatUrgentA" confRev="1" bufTime="100" buffered="true">
       <TrgOps dchg="true" qchg="true" />
       <OptFields />
       <RptEnabled max="5">
        <ClientLN iedName="AA2OPC1" ldInst="none" lnInst="1" lnClass="IHMI" />
       </RptEnabled>
      </ReportControl>
      <GSEControl name="SSAA2dist" desc="to AA1" datSet="PSCHtoAA1" confRev="1" appID="">
       <IEDName>AA1FP1</IEDName>
      </GSEControl>
     </LN0>
     <LN inst="1" lnClass="LPHD" lnType="Physical Device_REL316-4_IEC61850" />
     <LN inst="1" lnClass="PSCH" lnType="F21_Distance Scheme_REL316-4_IEC61850" prefix="F21" />
     <LN inst="1" lnClass="PTOC" lnType="NPS DT_REL316-4_IEC61850" />
     <LN inst="1" lnClass="PTRC" lnType="System Protection_REL316-4_IEC61850" />
     <LN inst="1" lnClass="TCTR" lnType="CT_REL316-4_IEC61850" />
     <LN inst="1" lnClass="TVTR" lnType="VT_REL316-4_IEC61850" />
     <LN inst="1" lnClass="PDIS" lnType="F21_Distance Z1_REL316-4_IEC61850" prefix="F21" />
    </LDevice>
   </Server>
  </AccessPoint>
 </IED>
 <DataTypeTemplates>
………………
 </DataTypeTemplates>
</SCL>
```

10.2 Tele-protection equipment between substations

This case (corresponding to Figure 18 SS to SS Communication via Proxy Gateway), where dedicated teleprotection equipment connects the substations offering a certain fixed amount of signals to be transferred between them, can from the engineering approach be used for high bandwidth as well as low bandwidth communications. From the engineering point of view, here the teleprotection equipment is introduced as a separate IEC 61850 IED in each system (project), needing its own IED tool.

The teleprotection equipment communicates with the IEC 61850 IEDs in the substation by means of IEC 61850, typically GOOSE or SAV type of service, i.e. it is an IEC 61850 IED within each of the substations. To retain the semantics of the communicated signals, here the proxy gateway approach is used, which works like this (see also Figure 21):

- Each end of the teleprotection is a client (ITCI logical node), which receives the DATA to be sent and used in the other substation(s).
- These DATA to be sent to the other substation are mapped onto a proxy gateway data model within the other substation; e.g. substation AA1 contains a proxy GW for substation AA2 and vice versa, if data flow is bidirectional.
- The data model of the proxy contains as image all those logical devices and logical nodes from IEDs at the other side, which contain data to be used in the receiving substation (e.g. all LDs from the IEDs, which would have been exported with dataflow right in the previous method). This could be defined by analysing the data to which the proxy subscriber has been configured as client in the source substation, or as a separate proxy engineering step, which then at the end generates this client data flow. Together with the logical devices also the part of the substation section to which the LNs to be used are bound, should be put into the proxy IID file.
- The proxy has an own LPHD logical node, which shows its state and by means of the (new) RTPC logical node also the state of the wide area communication link.
- The proxy defines a message (typically GOOSE or SAV, but also reports are possible) by gathering the data communicated for use in the receiving substation into a data set, allocated to a (GOOSE, SV or report) control block.
- Based on this message definition the client/subscriber at the sending substation, which could be a part of the corresponding proxy or a separate (client) IED, connects its client/subscriber input signals to the corresponding channels and message bits on the wide area connection. It is recommended to use the proxy data model's sAddr attributes or the ITCI client's intAddr attribute (or both) to identify the telecommunication signal used for transfer.

The proxy logical devices and their kept references to the substation section define the source meaning of the data for the destination SA system, and define which signals to receive, to transfer via the wide area connection, and to map to the possibly predefined (GOOSE or SAV) telegram at the source substation. This works even for simple proxies, which can only send a fix GOOSE data set, by assuring in the teleprotection IED tool, that only data from the LD with a matching data type is mapped to the appropriate preconfigured GOOSE signal.

Naturally, for high speed connections the proxy method has the disadvantage that it defines a further (proxy) IED, which might introduce delays. On the other hand it might be implemented replacing the switch coupling to the WAN connection in the high speed scenario, so that in reality the performance loss will be small or even zero.

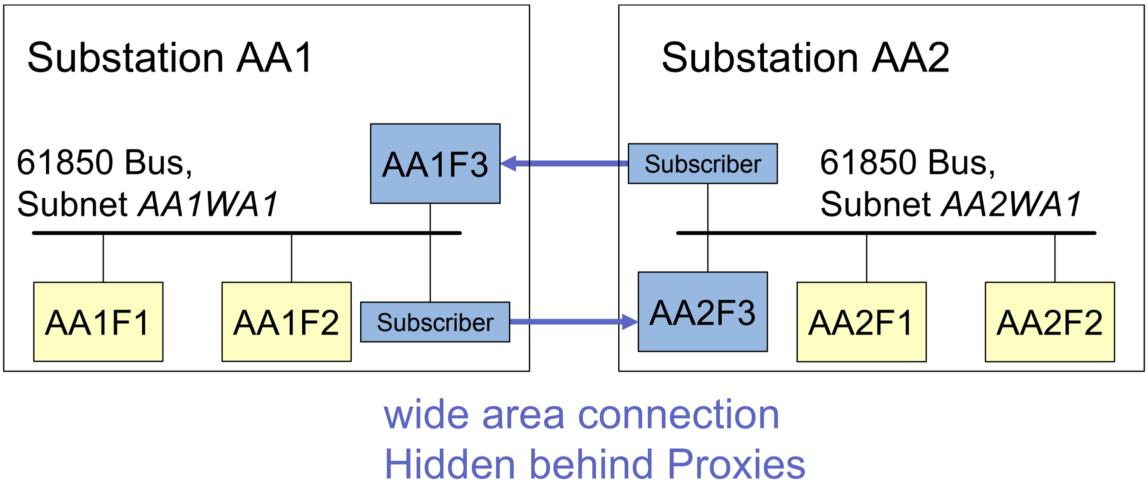


Figure 24 - Proxy gateway method (AA1F3, AA2F3 are Proxy gateways)

Above figure assumes, that data has to be sent from substation AA1 to AA2, represented there in the proxy IED AA2F3, as well as the other way round, there represented locally in AA1 at the proxy IED AA1F3.

The subscriber IED can either be considered the (ITCI) client part of the Proxy IED, or can be considered to be an own IED, which then must have an own IED name to configure sending DATA to it.

As the proxy SCL files look from SCL point of view like any other proxy gateway files, there is no example given. After the IID SCL file for the proxy has been generated from the SCD file of the other substation, this can be included into the project like any other IED's ICD or IID file, and configuring the subscriber is done with the Proxy's IED tool. All in all this is a three step system engineering process for each substation, flowed by the proxy IED engineering step:

a) Engineer the system without proxy gateway.

b) Generate the proxy GW IID file for substation AA1 from the SCD file from substation AA" and vice versa.

c) Include the generated IID files into the systems, and finalize the data flow engineering.

d) Use the proxy GW IED tool to configure the teleprotection IED(s).

Annex A

Additional considerations on security an dependability issues when using Ethernet Networks

A.1 Introduction remark

This annex includes some additional concepts on how to address security and dependability issues when using Ethernet networks. We expect experts to comment on these concepts in order to decide whether they shall be included in the final technical report.

A.2 Security of Traffic

The 32-bit CRC field at the end of each Ethernet packet provides an “unwanted command” probability, from an error burst, of < 10^{-9} (meeting the IEC 60834-1 < 10^{-8}).
Of more concern are attempts at sabotage through the injection of rogue Ethernet packets into the network; two mitigating technologies for consideration comprise:

(a) VLANs
The IEEE 802.1Q standard adds a 4-byte “tag” to the headers of Ethernet packets in order to provide a 12-bit VLAN-ID (“VID”) and a 3-bit priority level for each packet.
Ethernet switches supporting VLANs can be configured for which VLANs it will accept on each port, so by assigning a VID used for protection only to those ports connected to the protection IEDs guarantees that rogue protection packets cannot be injected (the removal of an IED’s connection, to get access to a port can be detected if of concern).

(b) Authentication
Cyber Security technologies are available that can “authenticate” the source of a received packet.
Typically the sender processes each packet through a key-dependent “hash” algorithm (e.g. SHA-1), and appends the result; by repeating the process with a matching key the recipient can have some degree of confidence that the packet was from the correct source.
Though the complex processing is a challenge for time-critical messages, the main implementation issue is the “key management” required to maintain the expected security. As an example, a frequent security requirement is to be able to replace all the keys within a few hours of a security breach; a hierarchical approach to key management reduces truck rolls, but adds complexity.

Since VLANs provide other benefits (see later), their use for solving the rogue-packet security concern looks very attractive, arguably a simpler and more robust solution for most applications; the one application for authentication being for inter-substation telecommunications utilizing an “untrusted” 3rd-party network.

A.3 Dependability of Traffic

As noted above, IEC 60834-1 specifies that the probability of a “command” not being received within 10 ms should be <10^{-4}.
For an Ethernet network, the reasons for a packet not being received within 10 ms comprise:

(a) Congestion
Whenever two or more Ethernet packets compete for a network path, such as to egress the port of a switch, one of them must wait in a “queue”.
If for some duration the arriving packets exceed a port’s capacity, the queue depth increases, and eventually packets may be discarded.
For networks transporting different classes of traffic with different degrees of priority, the use of switches with several priority-dependent queues at each egress port will improve the latencies of the higher-priority traffic (assuming the packets have IEEE 802.1Q/p “tags” with the correct priority values).

Note that though these tags support 8 priority levels, most switches provide only 4 or 2 priority level queues.

(b) Fibre Failure
The time for the network to establish an alternate link after the failure of a network's link (most links are fibre) may be too slow.
Note that none of the standard path-failure recovery algorithms for Ethernet networks come even close to the 10 ms required; SONET is < 60ms, SDH < 50ms, Ethernet Spanning Tree is about 1 minute, and Ethernet Rapid Spanning Tree takes tens of milliseconds to a few seconds.
As a result, communication vendors for the power utility market provide proprietary solutions with much faster recovery times. (These require ring topology networks.)
An alternate solution is to provide duplicate and physically-separate communication paths between the protection IEDs.

A.4 Other Security Issues with telecommunications to the Protection IEDs

The IEC 61850 Protection IEDs generally support other services using the same Ethernet port; these include remote configuration, remote firmware updates, status monitoring, file transfers (waveforms), WEB browser servers, and remote vendor access.
If the packets for all these services share a common VLAN, the security of the IEDs depends on "firewalls" and "authentication" services, both of which have significant problems.
If the packets for all these services are on separate VLANs, the security of the IEDs depends on the correct configuration of the network's switch ports' VLAN memberships, which should be part of the SCL so it can be verified and monitored.
For example, a vendor can be given access to a particular instance of one of his products by (temporarily) enabling that specific device to respond to requests on packets with the "remote vendor access" VLAN. This limits a possible rogue vendor to changing only the one device.

A.5 Avoiding GOOSE packets flooding the WAN

By using different VLANs for intra-substation and inter-substation GOOSE packets, the broadcast range of the former will be limited to the one substation.
(This would require IEDs to repeat some GOOSE packets, to provide packets for both VIDs.)
For applications requiring the use of GOOSE packets to provide a multipoint-to-point delivery of IED data to a central processor, the use of separate VIDs for the "up" and "down" traffic avoids the broadcasting of all the IED packets to all the other IEDs.

A.6 Requirements on IEC 61850 interfaces

For the reasons cited above, in order that typical Ethernet telecommunications networks can provide the required Security and Dependability for protection functions, the IEC 61850 packets should normally be IEEE 802.1Q "tagged" frames.
For the VIDs used, a consistency amongst utilities would be attractive.
The table below shows the recommended VID assignments; all IEDs shall be configurable to support these ranges (though compatibility with non-61850 devices on the network may require the use of other VIDs in some situations).
The VIDs shall use the shown "dotted-nibble" format to facilitate the grouping of IEDs' VIDs to share common network routing.
The value for "x" shall be 0 to 14 (so that 15 may be used for group routing ("filtering")).
(All the numbers in this clause are in decimal.)
The following formula converts a VID of "a.b.c" to the usual representation "n":

$$n = (256*a) + (16*b) + (c)$$

Examples:

4.5.12 would be used for a VID of 1116
12.1.x would route VIDs from 3088 through 3102 (12.1.0 through 12.1.14)
6.1.x would route VIDs from 1552 through 1566 (6.1.0 through 6.1.14)
6.x.x would route VIDs from 1536 through 1774 (6.0.0 through 6.14.14)

The VID could also be converted to hex if desired.
Example: 4.5.12 would become 0x45C in hex.

Ref.	**Service**	**VLAN-ID (VID)** **(12-bits)**	**Priority** **(0-7)**
1	Intra-substation GOOSE	4.x.x & 5.x.x	7 (highest)
2	Inter-substation GOOSE	6.x.x & 7.x.x	7 (highest)
3	Intra-substation SV (Sampled Values)	8.x.x & 9.x.x	6
4	Inter-substation SV (Sampled Values)	10.x.x & 11.x.x	6
5	MMS over TCP (C/S) (Client/Server)	12.1.x	4
6	Configuration	12.2.x	5
7	NMS (Network Management System)	12.3.x	5
8	File transfer (e.g. event waveforms)	12.4.x	3
9	WEB server	12.5.x	3
10	Vendor access (treat as “untrusted”)	12.6.x	3
11	IEEE 1588 (PTP Time Distribution)	12.7.x	6
12	Non-61850 traffic	<4.0.0 (<1024) >=12.0.0 (>3071)	< 6

A.7 Requirements on the Telecommunications network

This clause uses the telecom terms “drop” for the equipment ports connecting to the traffic sources (e.g. for VF, data, video etc.), and “line” for the equipment ports connecting the networks’ nodes (typically fibre connections).
The requirements for the Ethernet Telecommunications network are as follows:

(a) If some of the Ethernet Telecommunications network equipment is outside the utility’s “Security Perimeter” (e.g. when Ethernet circuits are leased from a service provider), the Ethernet links through such equipment should be secured through a technology such as “L2TP” (Layer 2 Tunnelling Protocol) to create a “VPN” (Virtual Private Network), and the security should be maintained through the implementation of the associated key-management requirements. Note that this technology provides authentication of each message’s source (encryption is not required for protection applications, and may significantly increase the messages latencies).

(b) Unless dual-port IEC 61850 IEDs are used (with physically separate paths), the Ethernet network shall recover (restore traffic) from a fibre failure within 10ms.

(c) All the network switches’ “drop” ports connected to IEC 61850 IEDs should be configured for memberships only in the VLANs supported by the connected IEDs.
Such connections should be monitored to detect momentary link loss events; this allows the detection of malicious attempts to use such ports to access other IEDs on the critical VLANs.

(d) All the network switches’ “drop” ports connected to other services (e.g. Video, Corporate, VoIP, 3rd-party WANs) shall be configured to block ingressing traffic with VIDs for the critical VLANS, and to prevent ingressing traffic using the network’s priority queues handling the GOOSE protection traffic (e.g. by controlling the priority fields of the ingressing packets’ IEEE 802.1Q tags).

(e) The probability of a GOOSE packet taking more than 10ms to traverse the network shall be constrained to < 10^{-4}; by limiting the number of switches on the longest path, and by limiting the traffic loading (see the next sub-sections for some examples).

A.8 Example of packet delays

At each egress switch port, a high-priority packet may have to wait for a maximum-length lower-priority packet to egress; a 1518 byte packet takes 122us at 100 Mbit/sec, 12us at 1 Gbit/sec.

A potential 2ms extra delay could therefore be incurred for a network path comprising 16 hops if at 100 Mbit/sec, 160 hops if at 1 Gbit/sec.

At each egress switch port, a high-priority packet may also have to wait for many other high-priority packets to egress; a 600 byte packet (typical for GOOSE) requires 48us at 100 Mbit/sec, 4.8us at 1 Gbit/sec.

A potential 2ms extra delay could therefore be incurred for an event-triggered burst of 40 GOOSE packets if at 100 Mbit/sec, 400 packets if at 1 Gbit/sec.

A.9 Useful features of some Ethernet Telecommunications networks

A utility may desire its wide-area network to be used for transporting 3rd-party Ethernet traffic, (e.g. to interconnect the LANs of different sites), raising a potential conflict with the VIDs chosen for the utility's 61850's IEDs.

For such applications, the "encapsulation" of such traffic in a second 802.1Q VLAN tag (sometimes known as "nested VLANS", or "QinQ") is a good solution; this also preserves the original traffic's priority tags (without such nesting, the utility would need to be able to modify the original tags to ensure that such traffic is kept out of the network's GOOSE queues).

Some Ethernet Telecommunication networks use SONET rather than Ethernet for their transport formats (for the fibre signals); this technology allows the provisioning of a plurality of Ethernet WANs, each with its own dedicated bandwidth and immunity to the traffic on the others WANs.

Some Ethernet Telecommunication switches provide an extra set of queues on their line ports (e.g. 16 c.f. 8) so that for traffic at a particular priority level, the "through" traffic (line to line) has priority over the "add" traffic (drop to line). This mitigates the delay accumulations over multi-hop paths.

Some Ethernet Telecommunication networks monitor the latency of critical traffic paths, recording the peak values over time, so that the user can confirm that the expected performance is being realized.

A.10 Assigning VIDs

It is acknowledged that the use of the 802.1Q VIDs (VLAN IDs) to control traffic and provide security, plus the use of the 802.1Q priority field to meet dependability requirements requires the use of switches that support these features; however it has also been demonstrated that such features are required if such networks are used.

The technology for assigning these VIDs and priorities is beyond the scope of this document.

GVRP and GMRP are IEEE standards (in 802.1p) that allow IEDs to request VLAN assignments.

The devices could be configured manually.

The devices could be configured by whatever configures the 61850 substation IEDs.

An important consideration is that there is a strong argument for the entire communication network's settings and performance to be continually monitored; some utilities are already requiring this feature.