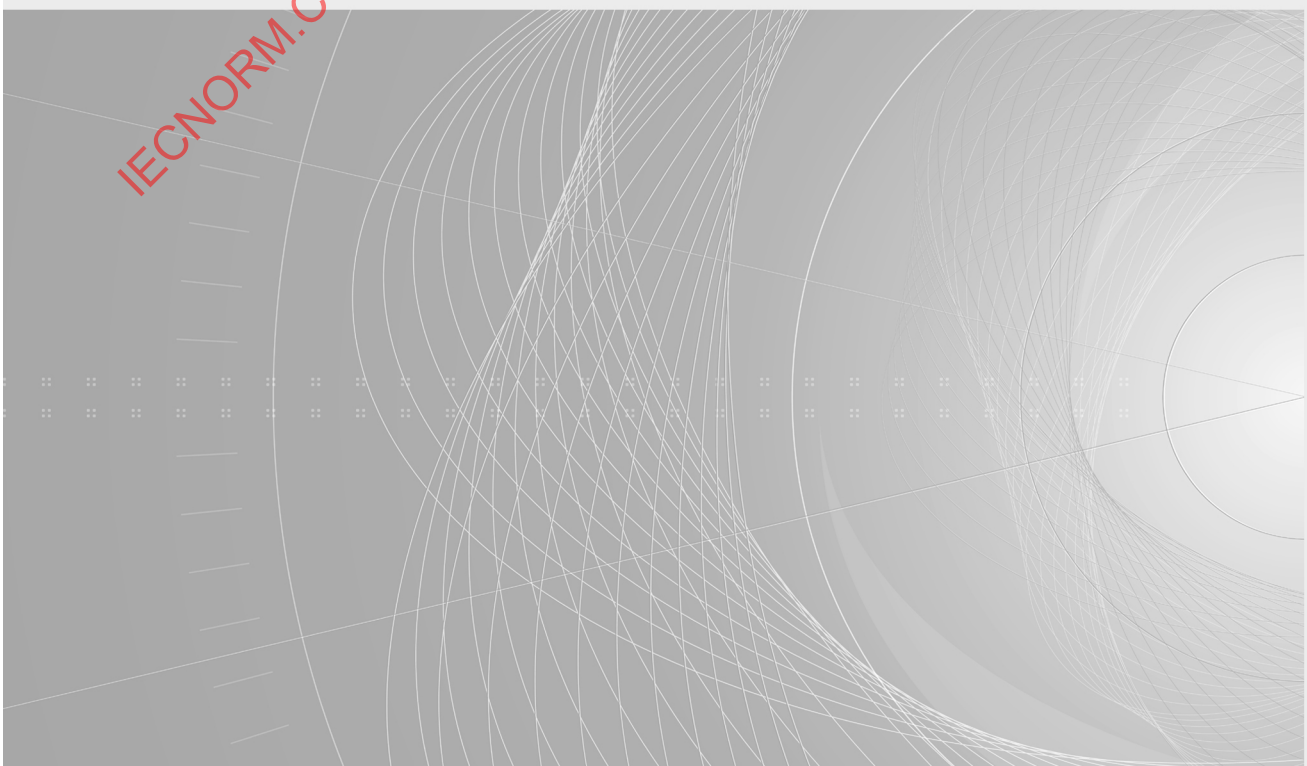
IEC/TR 61850-90-1

Edition 1.0 2010-03

TECHNICAL REPORT

colour inside

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



IEC/TR 61850-90-1:2010(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TR 61850-90-1

Edition 1.0 2010-03

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-88910-580-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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 organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61850-90-1, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/992/DTR	57/1021/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61850 series, under the general title: *Communication networks and systems for power utility automation*, can be found on the IEC website.

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

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

With existing and new applications in the field of power system operation and protection, the requirement to exchange standardized information directly between substations is increasing. 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 of the different aspects that need to be considered when 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[1)]. 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[1)].

The scope of IEC 61850 is no longer limited to substations. This is reflected in the changed title of the series. New domain specific parts have been added to the series. Working Group 10 of Technical Committee 57 is currently preparing the second edition of the basic parts of IEC 61850.

1) Under consideration.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

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

1 Scope

This part of IEC 61850 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;
- defines data as a prerequisite for interoperable applications;
- does not define implementations which guarantee interoperability between different IEDs;
- describes the usage and enhancements of the configuration language SCL.

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.

IEC 60044 (all parts), *Instrument transformers*

IEC 60834-1:1999, *Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems*

IEC 60834-2:1993, *Performance and testing of teleprotection equipment of power systems – Part 2: Analogue comparison systems*

IEC 60870-4, *Telecontrol equipment and systems – Part 4: performance requirements*

IEC/TS 61850-2, *Communication networks and systems in substations – Part 2: Glossary*

IEC 61850 (all parts), *Communication networks and systems for power utility automation*

IEC 61850-3, *Communication networks and systems in substations – Part 3: General requirements*

IEC 61850-5:2003, *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*

IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-2:2010, *Communication networks and systems for power utility automation – Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-8-1,___ *Communication networks and systems for power utility automation – Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*[2)]

IEC 61850-9-2,___ *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*[2)]

IEC 62053-22, *Electricity metering equipment (a.c.) – Particular requirements – Part 22: Static meters for active energy (classes 0,2 S and 0,5 S)*

IEC/TS 62351-6, *Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850*

IEC 62439, *High availability automation networks*

ANSI/IEEE 1588, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems / revision of ANSI/IEEE 1588-2002 / Approved 2008-09-10*

IEEE 802.1Q, *Local and metropolitan area networks – Virtual bridged local area networks*

3 Terms and definitions

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

4 Abbreviated terms

BER	Bit error ratio
Bkr	Circuit breaker
C/S	Client / Server
CE	Central equipment
DCB	Directional comparison blocking
DF	Directional relay to detect forward faults
EHV	Extreme high voltage
HV	High voltage
IF, I/F	Interface
I/F -R	Interface to receive data
I/F -S	Interface to send data
L2TP	Layer 2 tunnelling protocol
MV	Medium voltage
PDH	Plesiochronous digital hierarchy
PMU	Phasor measurement units
QA	Circuit breaker
QB	Line disconnector
QC	Earthing switch
QinQ	802.1Q in 802.1Q (VLAN stacking)
RAS	Remedial action schemes

2) To be published

RO	Overreaching distance zone
RT	Remote terminal
Rx	Receiver
SDH	Synchronous digital hierarchy
SIPS	System integrity protection scheme
SONET	Synchronous optical NETwork transport system
SS	Substation
TPI	Teleprotection interface
Tx	Transmitter
VoIP	Voice over IP (Internet protocol)
VPN	Virtual private network
WAN	Wide area network

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

5.1 General

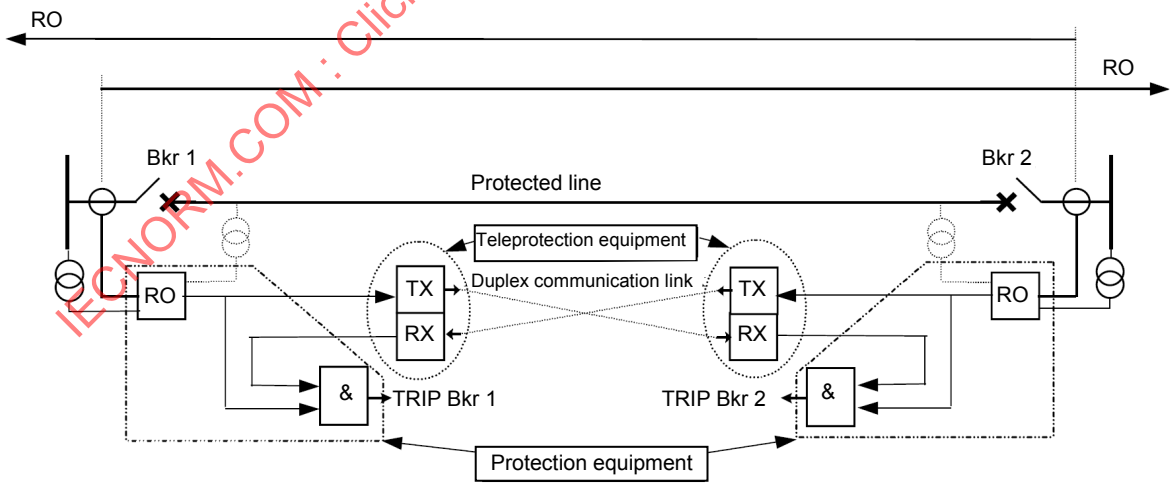
For the purpose of communication between substations, the following functions are considered.

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.

5.2 Distance line protection with permissive overreach tele-protection scheme

Summary:

When a distance relay detects a forward fault in the overreach zone, it sends a permissive signal to the remote end, see Figure 1. If that 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

IEC 503/10

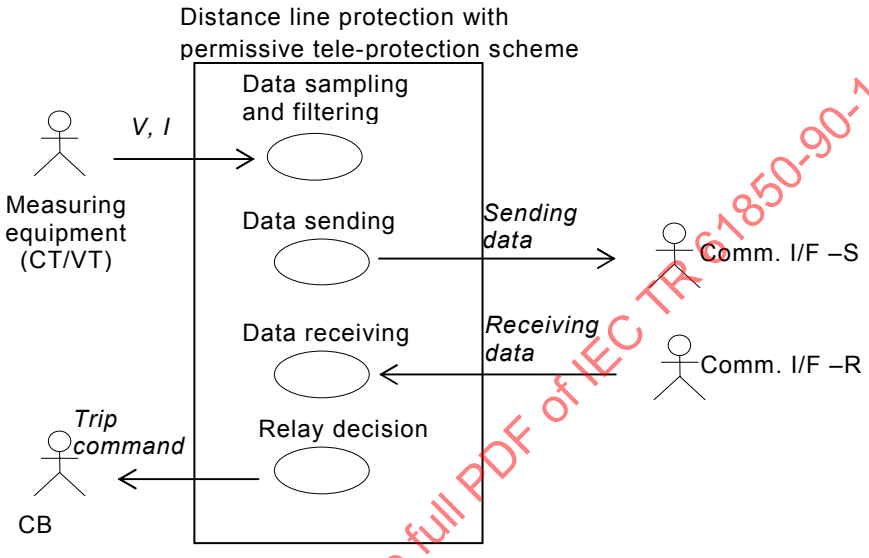
Figure 1 – Distance line protection with permissive overreach tele-protection scheme [1][3)]

3) Figures in square brackets refer to the Bibliography.

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.
- For fast tripping, the propagation, delay shall be small (e.g.: less than 5 ms).
- A high reliability is needed (e.g. BER less than 10^{-6}, alternative route, duplicated).

Use case diagram:



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)

Use case(s):

Name	Services or information provided
Data sampling and filtering	Samples current and voltage data from measuring equipment and filters 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

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 receives the data from the remote end
Step 2	Comm. I/F –R gives the received data to distance protection
Step 3	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

Exceptions / Alternate flow:

N.A.

Pre-conditions:

N.A.

Post-conditions:

N.A.

References:

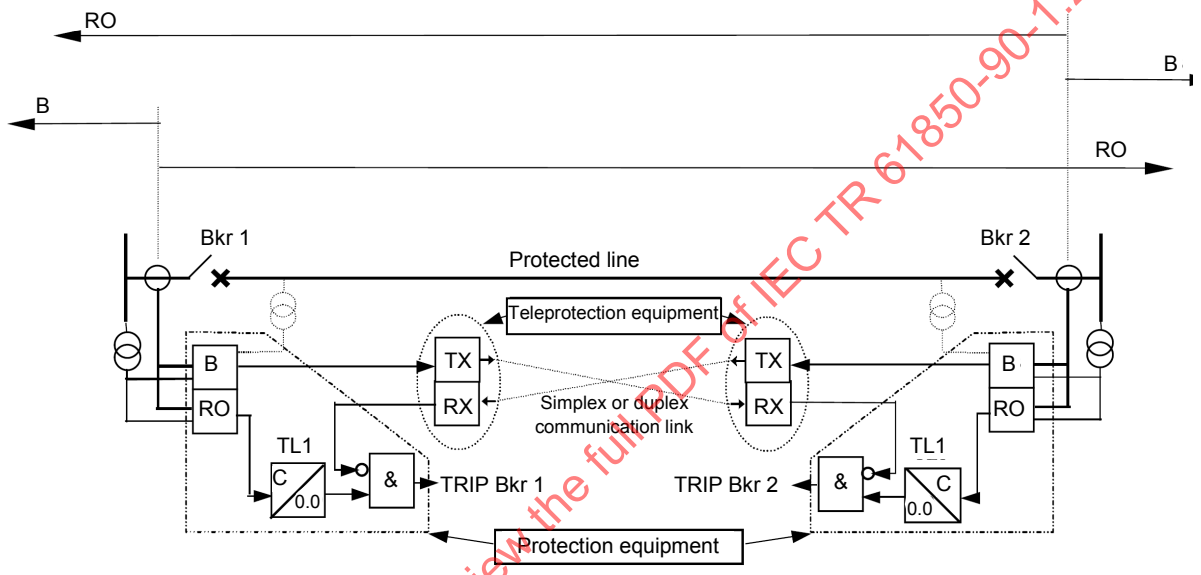
[1] Protection Using Telecommunication

5.3 Distance line protection with blocking tele-protection scheme

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, see Figure 2.

A variant involves the directional comparison blocking (DCB) using a non-directional element to send a blocking signal for any fault (other wording: “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.



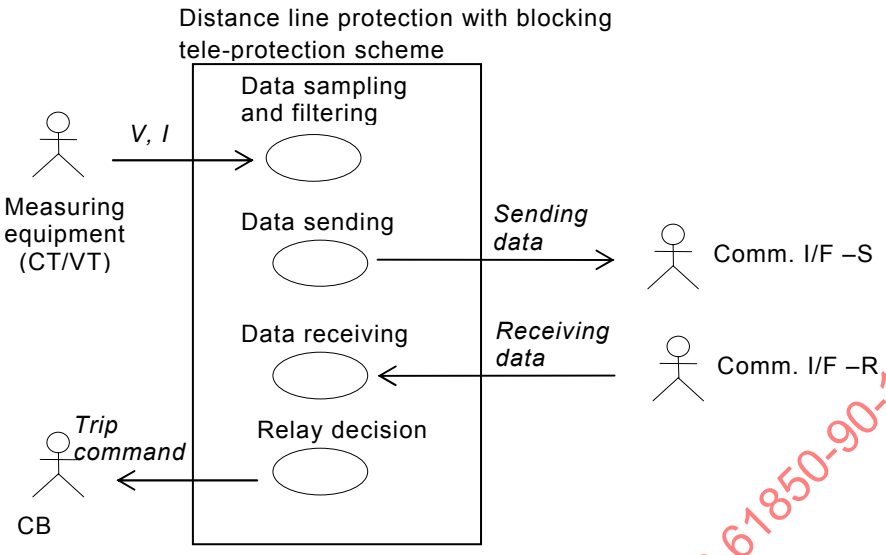
RO Overreaching trip function, must be set to reach beyond remote end of line
B Blocking function, must be set to reach beyond overreaching trip function at remote end of line
C Coordinating time, required to allow time for blocking signal to be received (set equal to channel time plus propogation time plus margin)

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

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.
- For fast tripping, the propagation delay shall be small (e.g.: less than 5 ms).
- A high reliability is needed (e.g. BER less than 10^{-6}, alternative route, duplicated).

Use case diagram:



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)

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

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

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

Exceptions / Alternate flow:

N.A.

Pre-conditions:

N.A.

Post-conditions:

N.A.

References:

[1] Protection Using Telecommunication

5.4 Directional comparison protection

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. See Figure 3.

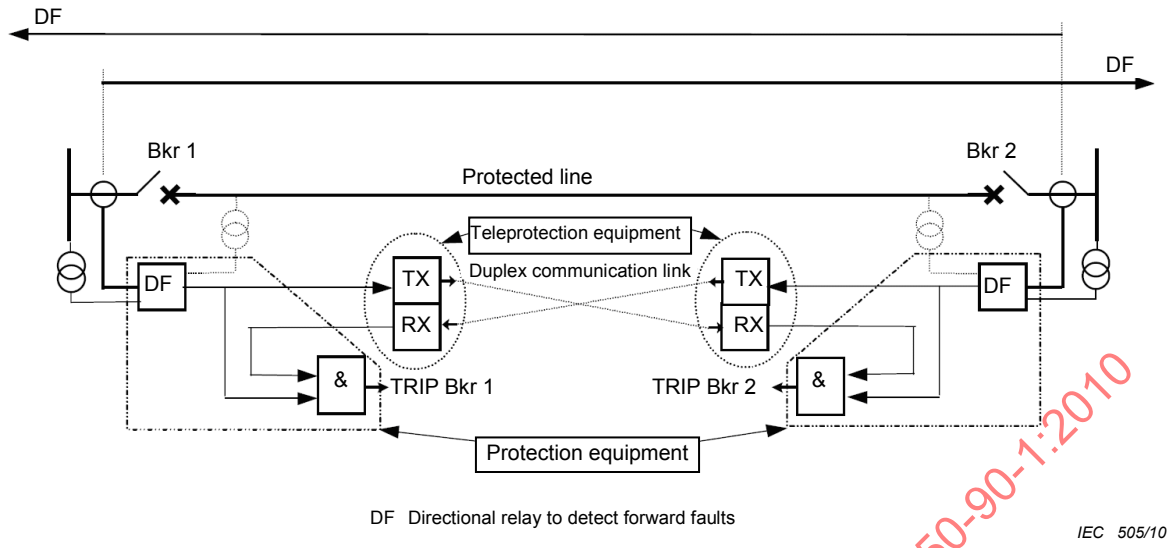
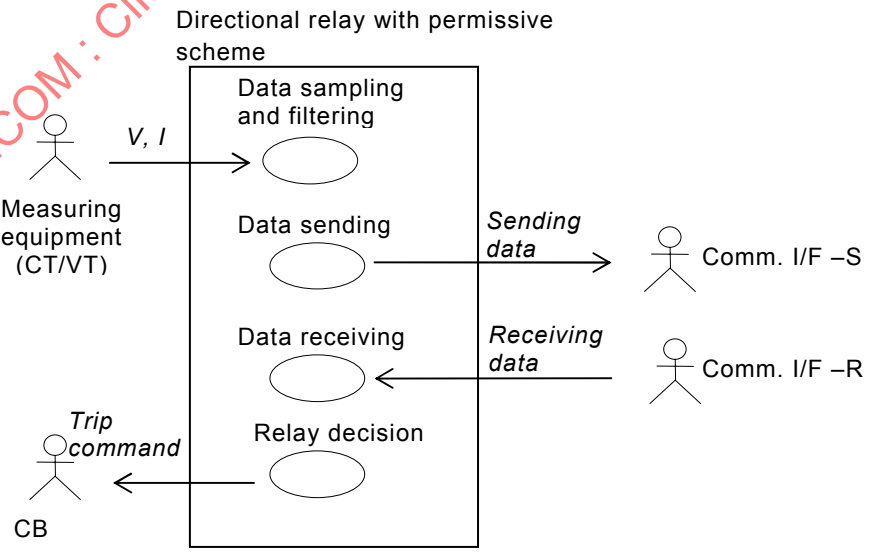


Figure 3 – Directional comparison with permissive scheme [1]

Constraints / Assumptions / Design considerations:

- The permissive 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 only when a forward fault is detected.
- For communication channel failure, alternative actions must be considered.
- For fast tripping, the propagation delay shall be small (e.g.: less than 5 ms).
- A high reliability is needed (e.g. BER less than 10^{-6}, alternative route, duplicated).

Use case diagram:



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)

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

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 receives the data from the remote end
Step 2	Comm. I/F –R gives the received data to the directional relay
Step 3	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

Exceptions / Alternate flow:

N.A.

Pre-conditions:

N.A.

Post-conditions:

N.A.

References:

[1] Protection Using Telecommunication

5.5 Transfer/Direct tripping

Summary:

Local equipment sends a trip command to the remote equipment. This function is sometimes called inter-tripping as well. See Figure 4.

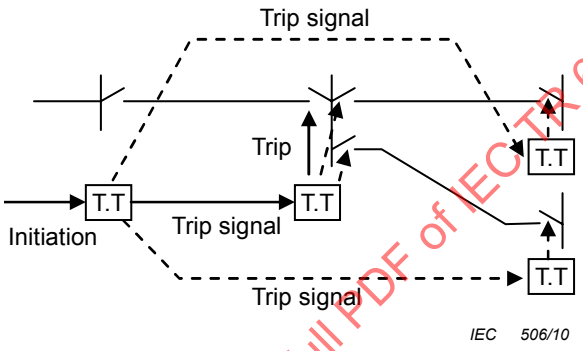
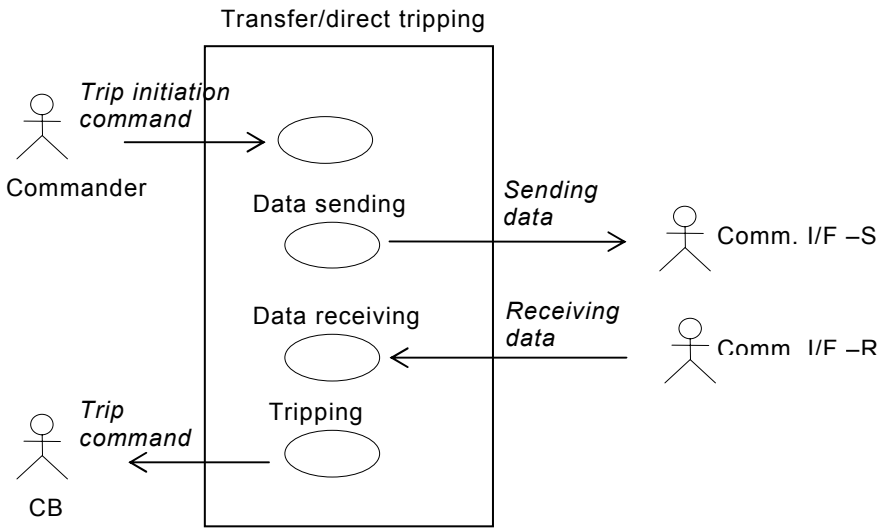


Figure 4 – Transfer/Direct tripping

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.
- For fast tripping, the propagation delay shall be small (e.g.: less than 5 ms).
- A high reliability is needed (e.g. BER less than 10^{-6}, alternative route, duplicated).

Use case diagram:



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)

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	Issues the trip command to the CB

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 issues a trip command to the CB

Exceptions / Alternate flow:

N.A.

Pre-conditions:

N.A.

Post-conditions:

N.A.

References:

N.A.

5.6 Interlocking

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. The method of under-voltage measurement may still be considered as back-up functionality in case of losing the communication link. See Figure 5.

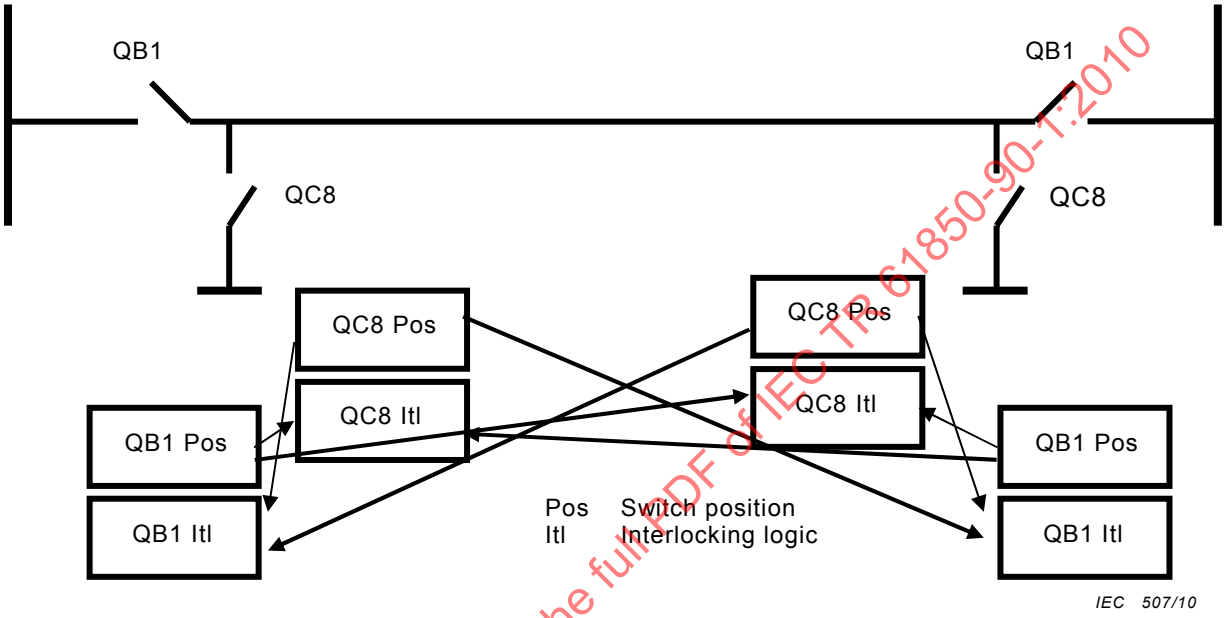
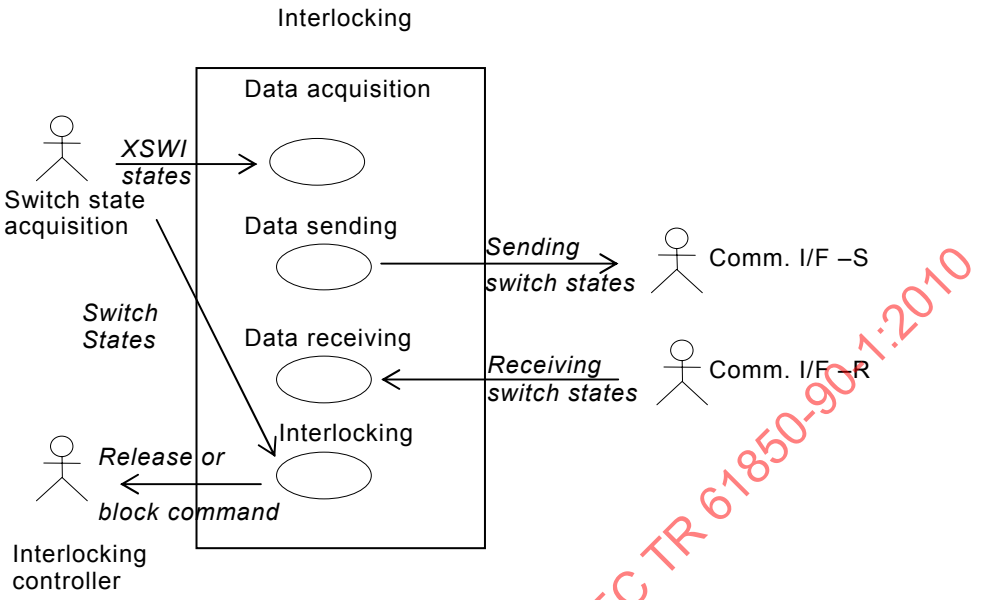


Figure 5 – Interlocking – Interoperation

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.

Use case diagram:



Actor(s):

Name	Role description
Switch state acquisition	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

Use case(s):

Name	Services or information provided
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

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

Exceptions / Alternate flow:
N.A.

Pre-conditions:
None.

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

References:
None

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

Summary:
Multi-phase auto-reclosing (1-phase, 2-phase, 3-phase) 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. See Figure 6.

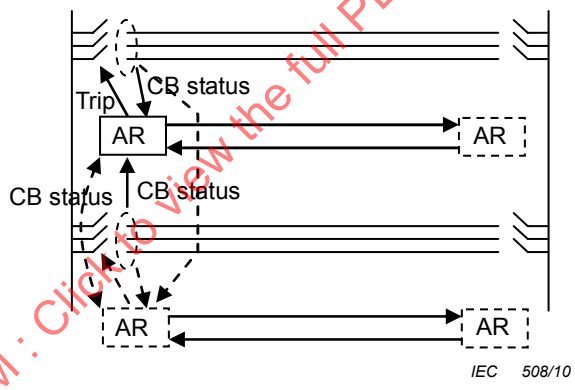
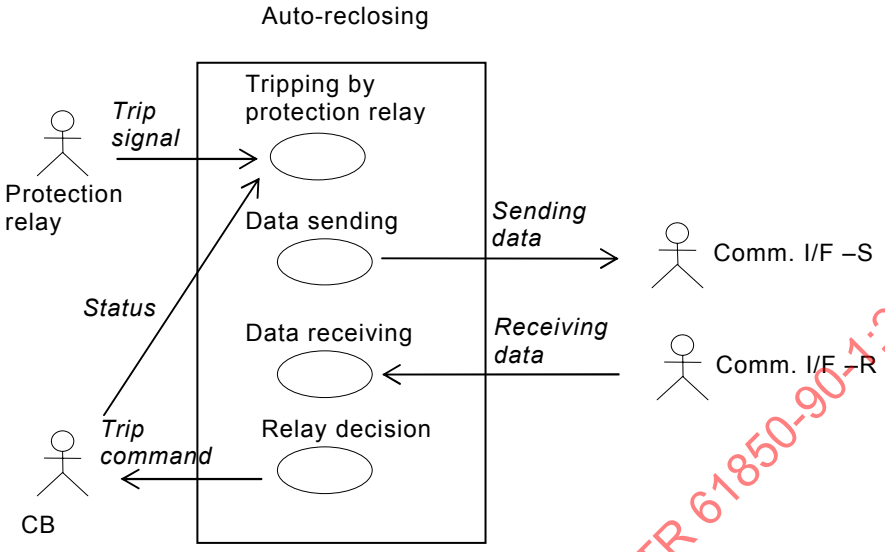


Figure 6 – Auto-reclosing

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

Use case diagram:



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)

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

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].

Exceptions / Alternate flow:
N.A.

Pre-conditions:
N.A.

Post-conditions:
N.A.

References:
[2] 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.

5.8 Current differential line protection

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. See Figure 7.

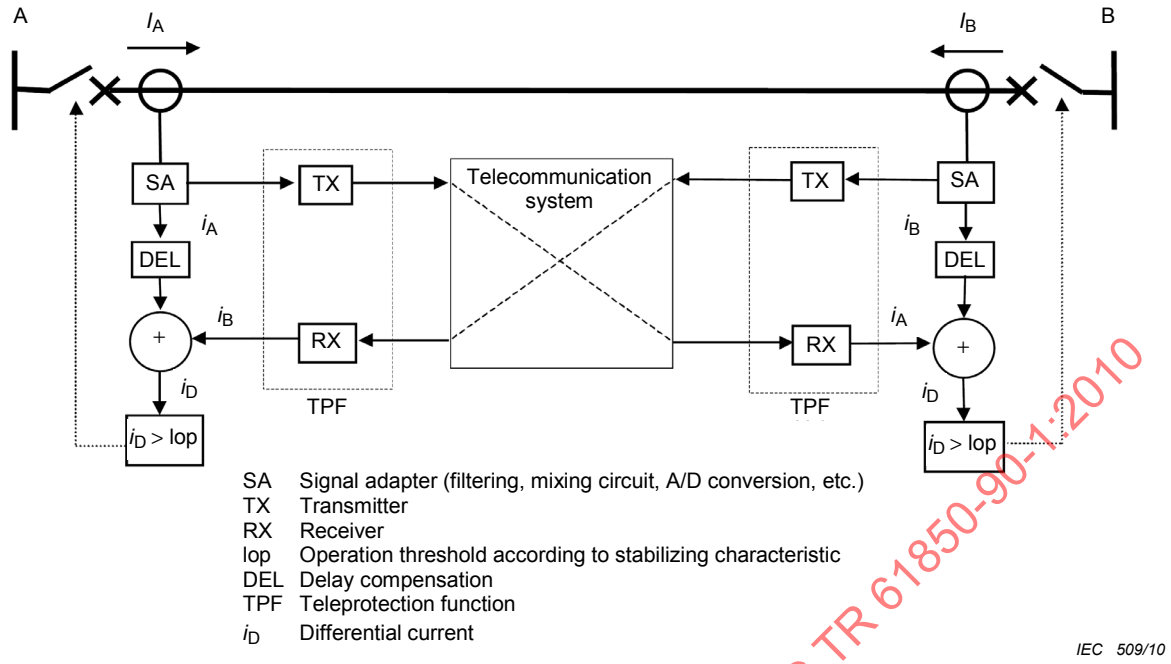
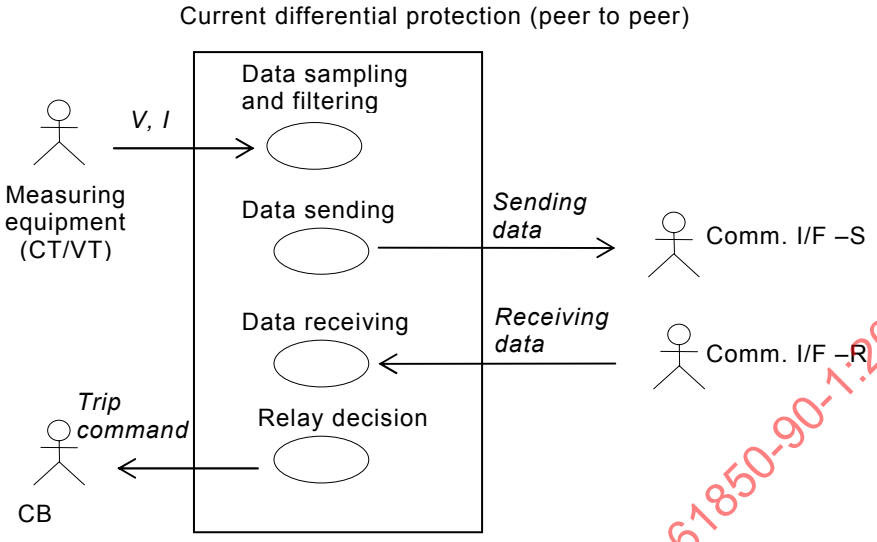


Figure 7 – Current differential line protection [1]

Constraints / Assumptions / Design considerations:

- Representation of measured currents and any additional information.
- Data must be synchronised between substations (required accuracy of synchronisation depends on design. Typically it is considerably less than 0,1 ms, if high fault current sensitivity is required even less than 0,01 ms).
- Periodic data exchange, the frequency of data exchange depends on design philosophy. One example is 12 times per power cycle (i.e. 600 times per second for 50 Hz systems), another design operates with 4 data exchange telegrams per power cycle.
- Data can be instantaneous values (sampled values), phasors or other quantities that represent the measured values.
- 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.
- For fast tripping, the propagation delay shall be small (Typically 5 ms for EHV, 10 ms to 40 ms for HV, MV), The propagation delay is negligible when direct fibre communication is applied.
- A high reliability is needed (e.g. BER less than 10^{-6}, Alternative route, Duplicated).
- Several types of telecommunication media may be used (i.e. 'Telecommunication system' in the figure above) such as direct fibre, SDH, PDH etc.
- Synchronisation can be established either by using an external signal such as GPS signal or, in applications with nearly equal delays in send an receive direction, by evaluating and considering the propagation delay during the signal exchange between the relays.

Use case diagram:



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)

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

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 receives the data from the remote end
Step 2	Comm. I/F –R gives the received data to the current differential protection
Step 3	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 issues a trip command to the local CB

Exceptions / Alternate flow:

N.A.

Pre-conditions:

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

Post-conditions:

N.A.

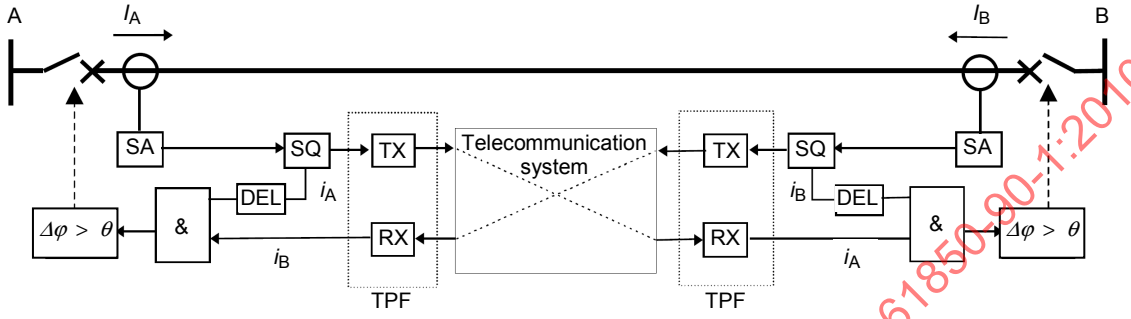
References:

[1] Protection Using Telecommunication

5.9 Phase comparison protection

Summary:

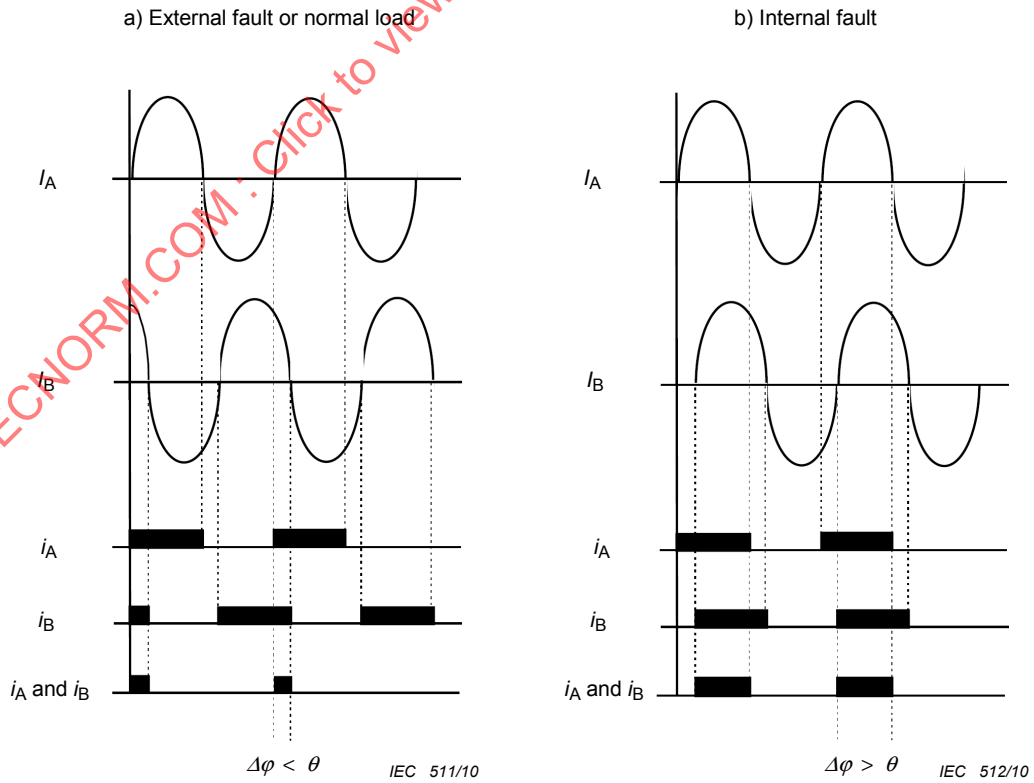
When a phase comparison relay detects a positive current, above a set threshold, the relay sends an “on” signal to the remote end. The relay compares the local data signal with that from the remote end. If the time that both signals are “on” is very short, the phases of the currents detected by both 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. See Figure 8 and Figure 9.



SA Signal adapter (mixing circuit, filtering, etc.)
SQ Squarer
TX Transmitter
RX Receiver
DEL Delay compensation
$\Delta\varphi$ Coincidence angle
θ Stabilizing angle
& Logical AND
TPF Teleprotection function

IEC 510/10

Figure 8 – Phase comparison protection [1]



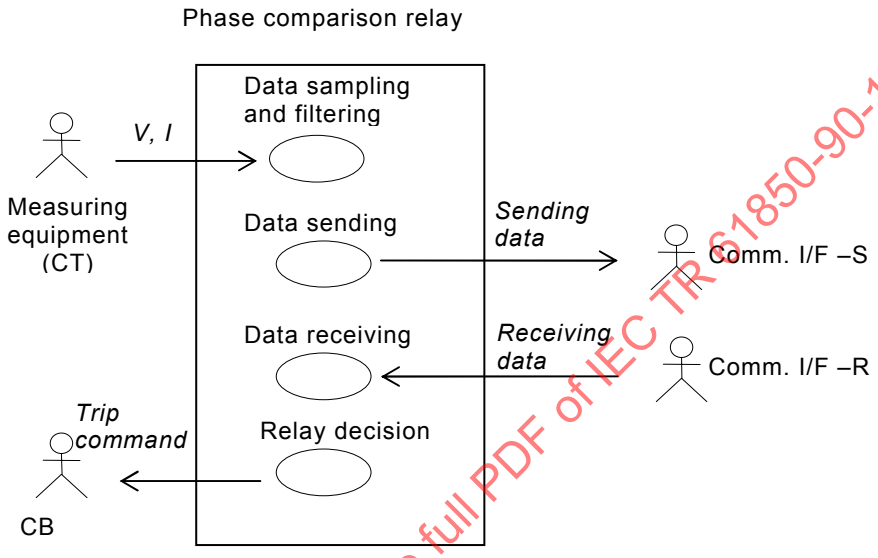
Half-wave phase comparison

Figure 9 – Principle to detect internal fault by phase comparison [1]

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.
- For fast tripping, the propagation delay shall be small (e.g. 5 ms).
- A high reliability is needed (e.g. BER less than 10^{-6}, alternative route, duplicated).

Use case diagram:



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)

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

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 receives the data from the remote end
Step 2	Comm. I/F –R gives the received data to the phase comparison relay
Step 3	The phase comparison 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 long enough, the relay issues a trip command to the CB

Exceptions / Alternate flow:

N.A.

Pre-conditions:

N.A.

Post-conditions:

N. A.

References:

[1] Protection Using Telecommunication

5.10 Other applications

5.10.1 General

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:

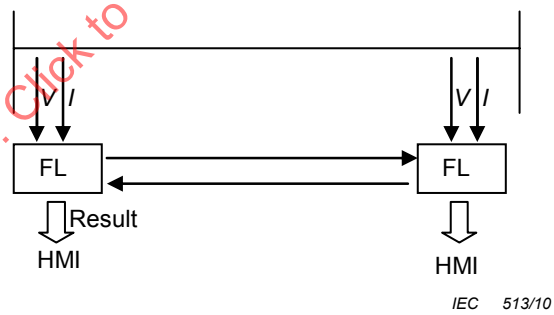
- representation of measured currents and/or voltages and any additional information;
- data must be synchronised between substations (e.g. less than 0,1 ms);
- enough data bandwidth to transmit three phase current and/or voltage data and additional information (e.g. 64 kbps);
- for communication channel 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 subclauses.

5.10.2 Fault locator system (2, 3 terminals)

Summary:

By using all terminal information, precise estimation of the fault location is possible. The voltages and currents of all ends are necessary. See Figure 10.



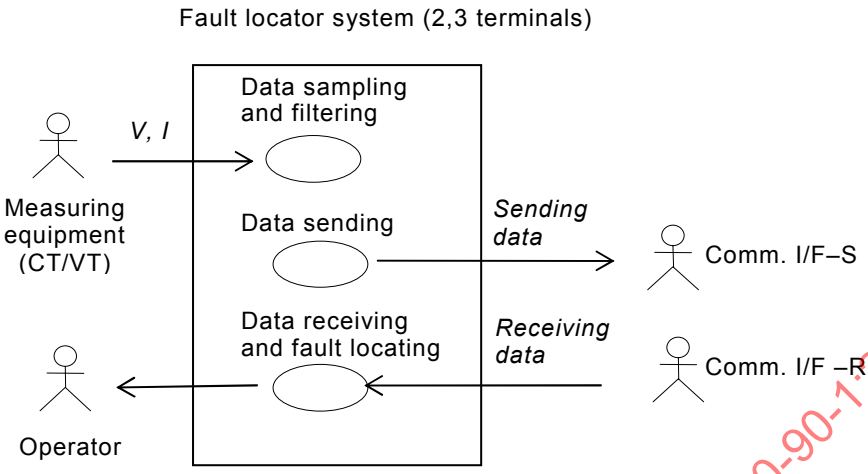
FL Fault locator
HMI Human machine interface

Figure 10 – Fault locator system (2, 3 terminals)

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 5.10.1.

Use case diagram:



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

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)

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 receives the data from the remote end
Step 2	Comm. I/F –R gives the received data to the local terminal
Step 3	The local terminal estimates the location the fault. It shows and stores the result

Exceptions / Alternate flow:
N.A.

Pre-conditions:
Synchronisation of the data between the relays must be established.

Post-conditions:
N.A.

References:
N.A.

5.10.3 System integrity protection schemes (SIPS)

Summary:
The described system integrity protection scheme comprises remote terminal units (RTU) and central equipment (CE). Remote terminal units are located at power stations and measure voltage. These remote terminal units periodically send measured data to the central equipment. The central equipment 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 equipment predicts that the generators will lose synchronisation, the central equipment sends a trip signal to the circuit breaker of the tie line. See Figure 11.

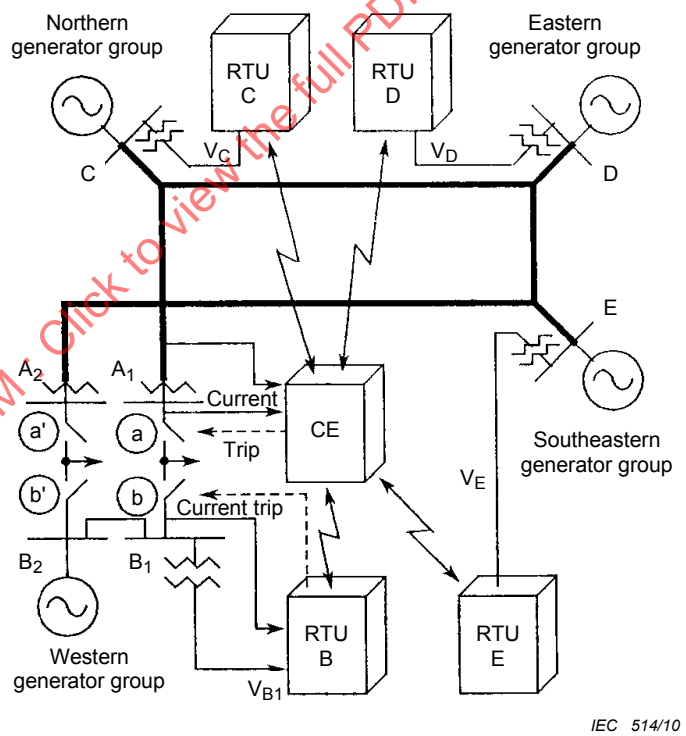
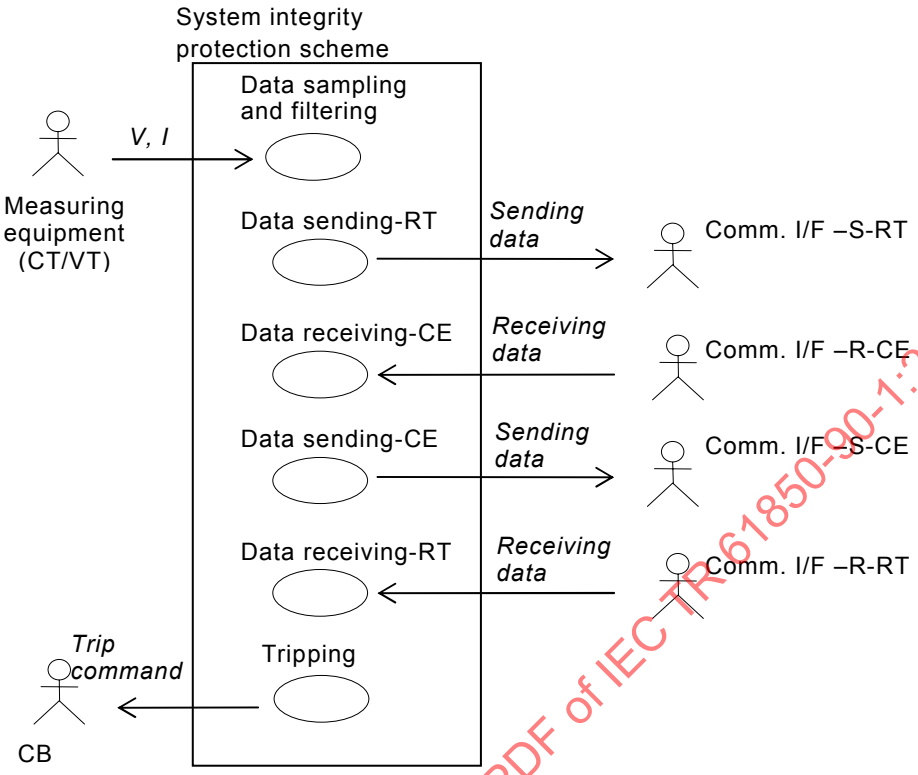


Figure 11 – Example of a system integrity protection scheme

Constraints / Assumptions / Design considerations:
- Representation of measured currents and voltages and any additional information.
- For fast tripping, the propagation delay shall be small (e.g.: less than 5 ms).
- Communication channel failure may block the SIPS.
- Other constraints, see 5.10.1.

Use case diagram:



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)

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

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 receives the data from the remote end
Step 2	Comm. I/F –R-CE gives the received data to the central equipment
Step 3	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

Exceptions / Alternate flow:

N.A.

Pre-conditions:

Synchronisation of the data between the relays must be established.

Post-conditions:

N.A.

References:

[3] 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.

5.10.4 Real time predictive generator shedding

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 equipment. When a fault occurs, if the central equipment predicts that the generators will loose synchronisation, the central equipment sends a trip signal to the generators. See Figure 12.

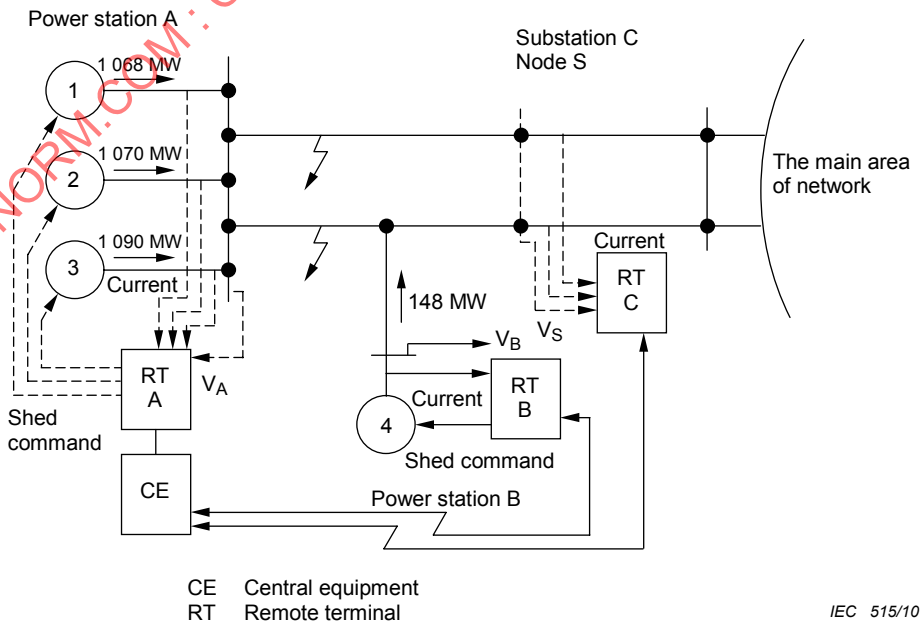
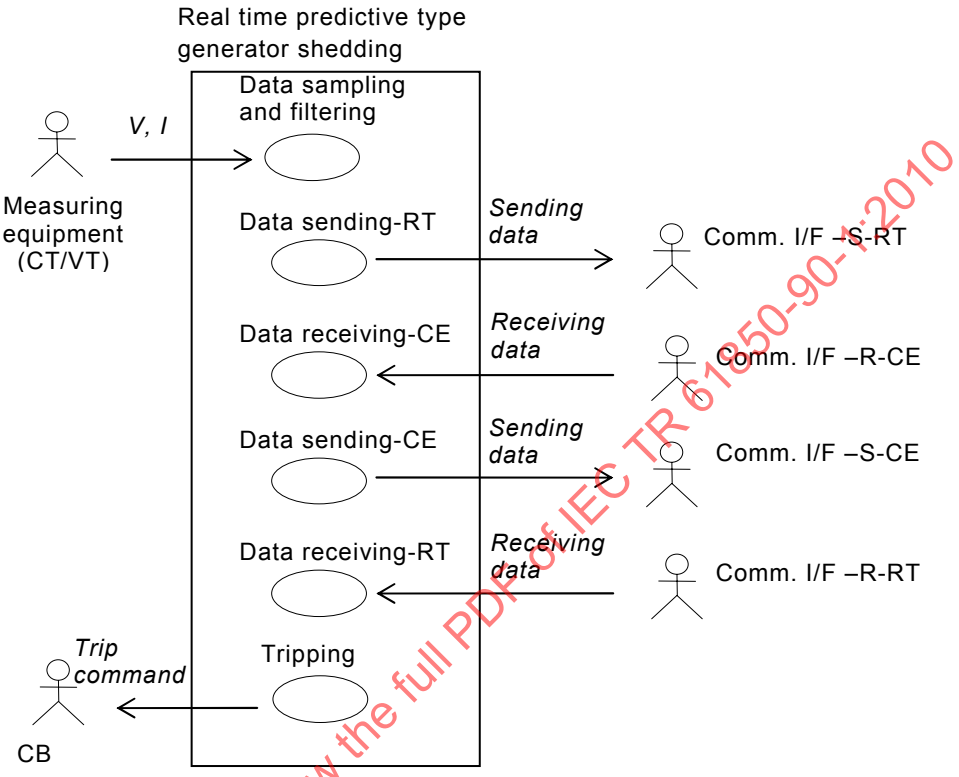


Figure 12 – Real time predictive type generator shedding system

Constraints / Assumptions / Design considerations:

- Representation of measured currents and voltages and any additional information.
- For fast tripping, the propagation delay shall be small (e.g.: less than 5 ms).
- For communication channel failure, alternative actions must be considered.
- Other constraints, see 5.10.1.

Use case diagram:



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)

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

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 receives the data from the remote end
Step 2	Comm. I/F –R-CE give the received data to central equipment
Step 3	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 calculates 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

Exceptions / Alternate flow:
N.A.

Pre-conditions:
Synchronisation of the data between the relays must be established.

Post-conditions:
N.A.

References:
[4] 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.

5.10.5 Out-of-step detection

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.

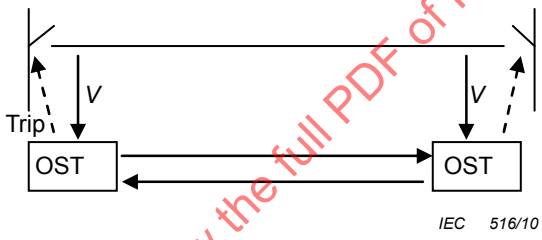
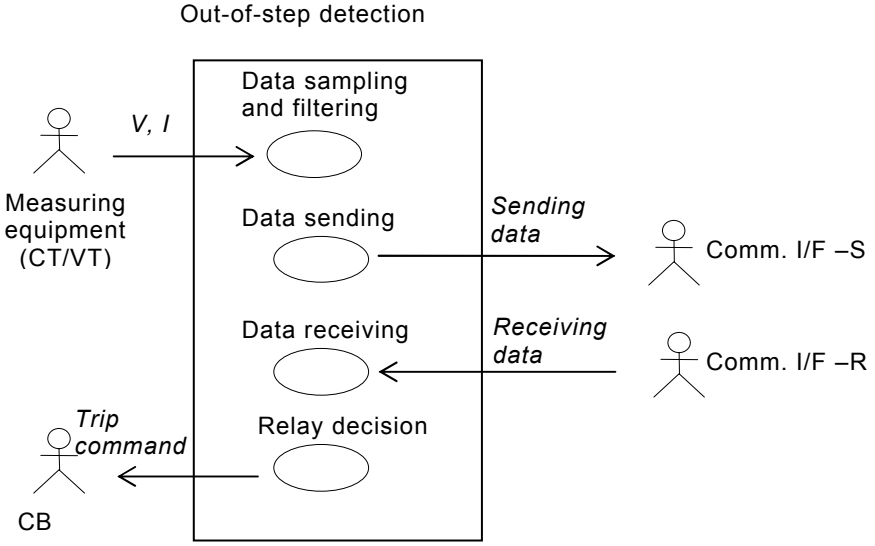


Figure 13 – Out-of-step detection

Constraints / Assumptions / Design considerations:
- Representation of measured voltages and any additional information.
- For out-of-step detection a medium propagation delay is required (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 5.10.1.

Use case diagram:



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)

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

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

Exceptions / Alternate flow:

N.A.

Pre-conditions:

Synchronisation of the data between the relays must be established.

Post-conditions:

N.A.

References:

N.A.

5.10.6 Synchrophasors

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 5.10.3 are one typical application of synchrophasors. Therefore, the detail of an application is not explained here again.

5.10.7 Remedial action schemes (RAS)

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 equipment 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 equipment.

6 Communication requirements for substation-to-substation communication

NOTE This Clause 6 collects the requirements according to IEC 61850-5 but focussed on substation-substation communication.

6.1 General issues

6.1.1 Introduction

The substation-substation communication refers to functions in substation automation systems (SAS) which are either distributed between two substations (e.g. A and B) or to functions in one substation which needs information from the other one. Examples are line protection, bay interlocking with position information from the line isolators and earthing switch from the other side of the line, and any kind of automatics including more than one substation. Supporting functions are e.g. the time synchronisation between IEDs on both sides of the substation-substation link.

6.1.2 Logical allocation of functions and interfaces (5.2 in 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 11.

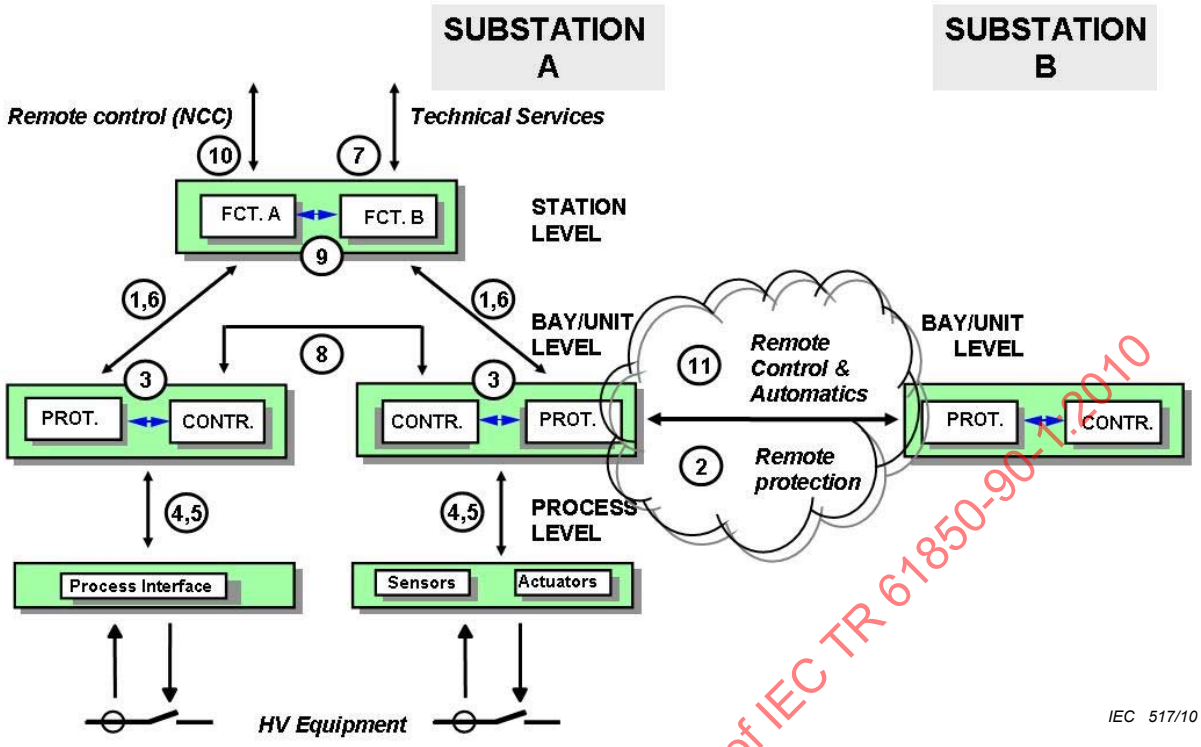


Figure 14 – Logical interfaces between substation A and substation B

Interfaces 1, 3 to 6, and 8 to 9 are connecting functions of the substation automation system inside the substation. Interface 10 represents as TCI (telecontrol interface) the communication of the SA system to the remote control centre, interface 7 represents as TMI (telemonitoring interface) the communication to remote engineering, monitoring and maintenance places. Interface 2 represents as TPI (teleprotection interface) the protection related function between substations, interface 11 represents the same for control related functions. There is some relation between the interfaces as shown in Table 1 below.

Table 1 – Grouping of protection and control interfaces

	Process interfaces	Bay-station interfaces	Substation-substation interfaces
Protection	IF 4	IF 1	IF 2
Control	IF 5	IF 6	IF 11

Interfaces:

IF1: protection-data exchange between bay and station level;

IF2: protection-data exchange between substations. This interface refers both to analog data e.g. for line differential protection and binary data e.g. for line distance protection;

IF3: data exchange within bay level;

IF4: CT and VT instantaneous data transport (especially samples) from the process to the bay level. This comprises in the reverse direction also the protection trip;

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 the substation and remote control center(s);

IF11: control-data exchange between substations. This interface refers to binary data e.g. for interlocking functions or inter-substation automatics.

6.1.3 The role of interfaces

Interface 2 is dedicated to communication with a remote protection device in the adjacent substation and the interface 11 is dedicated in the same way to communication with the remote control device. It should be noted that interfaces 2 and 11 may be interfaces to a communication network not according to IEC 61850. These networks are accepted if they allow tunnelling IEC 61850 messages and provide the requested performance between the functions running in IEC 61850 based SA systems on both sides.

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

6.1.4 Response behaviour requirements

Since interoperability is claimed for 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 finalized 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 quality attributes to be transferred with the data under consideration.

6.2 Functions based on substation-substation communication

The following functions need substation-substation communication. More detailed modelling including the communication interfaces is given in Clause 9.

6.2.1 Protection functions

Tables 2 gives the protection functions using substation-substation communication.

Table 2 – Protection functions using substation-substation communication

Function	IEC 61850	IEEE	Description or comments
Distance protection	PDIS, PSCH	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.

Function	IEC 61850	IEEE	Description or comments
Differential protection	PDIF, RMXU	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	PDIF, RMXU	87P	See above (PDIF/87)
Differential line protection	PDIF, RMXU	87L	See above (PDIF/87)

6.2.2 Control functions

Tables 3 gives the control functions using substation-substation communication.

Table 3 – Control functions using substation-substation communication

Function	IEC 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). a) 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. b) 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.

6.3 Message performance requirements

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

If not mentioned explicitly, the transfer time is specified from the user or application point of view. This means that the transfer time is the time from the sending application to the receiving one, i.e. the complete transmission of a message including the necessary coding and decoding including the media access at both ends (see Figure 15). In the physical device PD1, an application function 1 sends data to another application function 2 located in physical device PD2. 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 receiver stack. The overall transfer time t will however consist of the individual times for coding (t_a) and decoding (t_c) with or without dedicated communication processors and the pure network transfer time t_b.

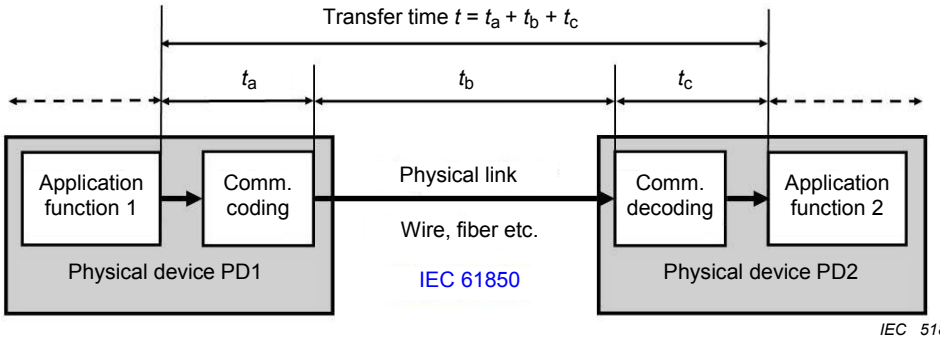


Figure 15 – Transfer time for binary and other signals over a serial connection

For binary signals, conventional output and input relays replace the coding and decoding (see Figure 16). These output and input relays have response times of around 10 ms.

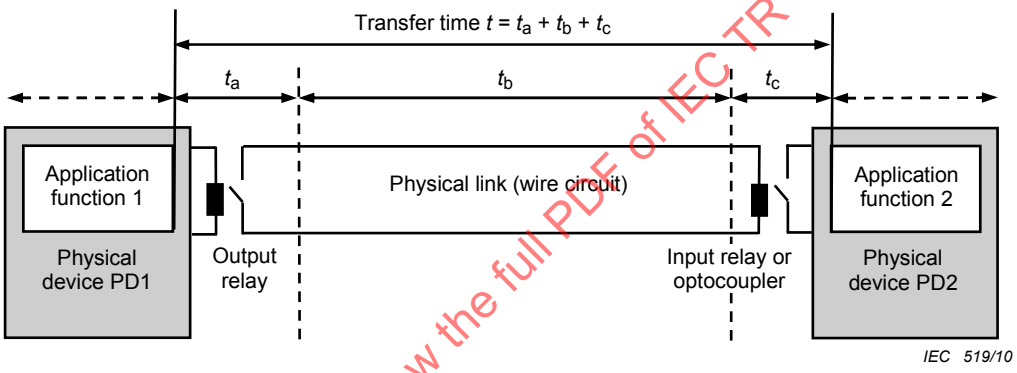


Figure 16 – Transfer time for binary signal with conventional output and input relays

If there is only one direct link, the time t_b is for distances in substations and in power systems negligible referring to the speed of light.

If there are active components in the communication path, such as routers, switches or other such components, the processing times of these elements contribute reasonable to the network transfer time t_b. If collisions or losses have to be compensated e.g. by repetitions, also theses times contribute. Any testing and verification of the transfer time must be performed during the site acceptance testing, since the physical devices and network equipment might be supplied from different manufacturers.

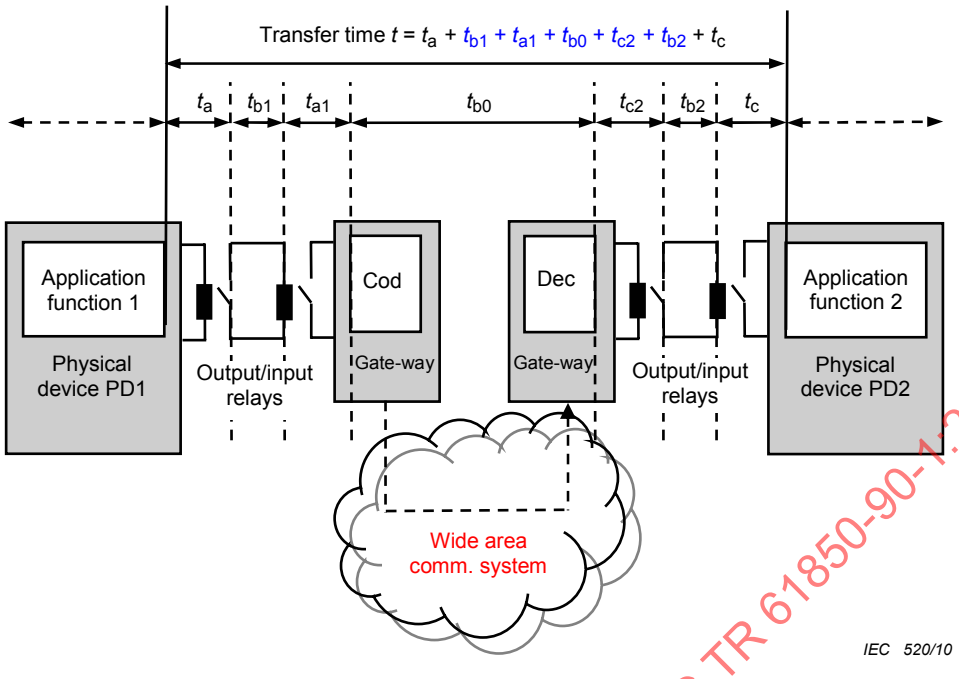


Figure 17 – Definition of transfer time *t* for binary signals in case of line protection

This is valid also for links beyond the substation boundary where the time delay in the interconnecting network is also part of t_b. In Figure 17 and Figure 18, some dedicated times contributing to t_b are shown. Relay times (Figure 17) are replaced by coding and decoding times (Figure 18). In case of full serial communication (Figure 18), coding and decoding for the wide area communication system (gateway in Figure 17) are replaced by recoding for the local area communication.

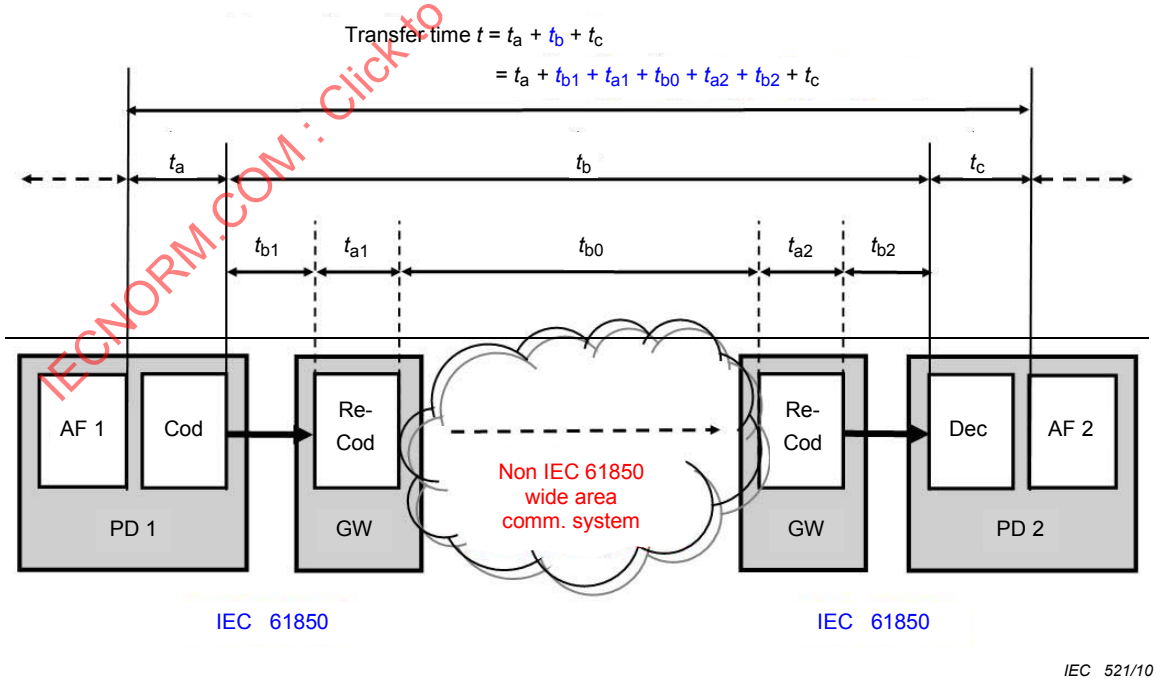


Figure 18 – Definition of transfer time *t* over serial link in case of line protection

The teleprotection operating time T_A in Figure 2 of IEC 60834-2 is defined in nearly the same way as the transfer time *t* in this document.

All requirements reflect the needs of the application function and, therefore, are valid in any case 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 the services defined in IEC 61850-7-2 and of the implementation within the IEDs. Any possible delay has to be defined and considered for the transfer time. If the resulting transfer times are acceptable is a project specific question.

6.4 The introduction and use of message performance classes

6.4.1 General

To allow for different requirements of the functions in and between substations, the requirements for the message types may be divided into performance classes. There are two basic groups of performance classes, one for control and protection applications (main criterion is the transfer times) and another one for metering and power quality applications (main criterion is the accuracy requirement). Since the performance classes are defined according to the requirements of the functions to be performed, they are independent from the size of the substation and basically form the voltage level. Raw analogue data both for voltage and current are transmitted over serial links as samples, mostly in the form of synchronized streams of samples. In order not to delay any dependant actions, such as necessary protection trips for these messages, not only the accuracy and sample rate are important but also the transfer time.

Not all communication links in and between substations need to support the same message performance classes. But because of the free allocation of functions, there is not a given allocation of message performance classes. Nearly all links may have to support all such classes. Therefore, all supported classes or at least the most demanding class shall be part of the IED specification.

It is a matter of implementation if all messages are sent according to the highest performance class requested at one link. To respond also in this case to different requirements, the support of priorities is requested.

The typical use of the performance classes is indicated below but it may be overwritten by dedicated function requirements or customer specifications.

6.4.2 Control and protection

The requirements for the transfer time i.e. the communication performance are basically the same in one bay, between bays and also between substations. Therefore, the same classification scheme shall be used for all links compliant with IEC 61850.

Some classes may be not applicable for all application areas. The use of an intermediate WAN not compliant with IEC 61850 may result in higher transfer times.

As mentioned above, the requirements for the transfer time are independent from the voltage level. The fault clearance time T_C as specified e.g. in Figure 2 of IEC 60834-2 is the time between fault inception and fault clearance. If at distribution level longer fault clearance times are accepted than at transmission level, then these times are related both to slower algorithms and less powerful breakers. But these times are not based on less demanding transfer times.

6.4.2.1 Types of message performance classes

6.4.2.1.1 Type 1 – High speed messages

This type of message typically contains simple binary information like a short command or a simple message like "Trip", "Close", “Reclose order”, "Start", "Stop", "Block", "Unblock",

"Trigger", "Release", "State change", maybe also "State" for some functions. This message type is mission critical for the performance of the supported function. The receiving IED shall act immediately in some way by the related function on receipt of this type of message.

6.4.2.1.1.1 Type 1A "Trip"

The "trip" is the most important fast binary message in the substation. Between substations "block" and "release" may be same as important. 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 "trips" within the substation and within one bay, transfer times not exceeding 4 ms shall be supported.

b) For "trips" within the substation between bays, transfer times not exceeding 10 ms shall be supported but also transfer times not exceeding 4 ms may be requested.

c) For "trips" to the neighboring substation (e.g. for line protection), a whole set of transfer times for the message performance classes shall be supported according to the transfer time requirements defined in line with IEC 60834-1 which shall not be exceeded depending on the functional requirements which have to be supported by the communication system applied:

   TR1 ≤ 4 ms;
   TR2 ≤ 10 ms;
   TR3 ≤ 15 ms;
   TR4 ≤ 20 ms;
   TR5 > 20 ms.

   NOTE In IEC 60834-1, only 10 ms are defined for digital networks.

6.4.2.1.1.2 Type 1B "automation"

All other fast messages are important for automation functions between IEDs and for the interaction of the IEDs with the process but have less demanding requirements compared to the type "trip".

a) For fast state based applications, the transfer time shall not exceed 20 ms in line with TR4 above.

b) For normal state based applications, the transfer time shall not exceed 100 ms in line with TR5 (> 20 ms) above but having 100 ms as upper limit.

Therefore, these types of message performance classes are valid inside the substation and also for messages between substations.

6.4.2.1.2 Type 3 – Low speed messages

Based on the response time of an operator (> 1 s), only low speed message performance classes are needed for the communication from the process and bay level to the operator. These messages shall not exceed 500 ms. This type refers to more complex messages for commands and reports like station level data base update, update of the single line display at the screen, for the update of alarm and event lists, and also for all operator commands. Such a performance message class is not applicable for functions based on substation-substation communication.

The same is valid for file transfers which may exceed 1 000 ms depending on the size.

6.4.3 Metering and power quality

6.4.3.1 Types of message performances classes

The performance class M1 refers to revenue metering with accuracy class 0,5 (IEC 62053-22) and 0,2 (IEC 60044) and up to the 5th harmonic.

The performance class M2 refers to revenue metering with accuracy class 0,2 (IEC 62053-22) and 0,1 (IEC 60044) and up to the 13th harmonic.

The performance class M3 refers to quality metering (power quality) up to the 40th harmonic.

6.4.3.2 Raw data messages

6.4.3.2.1 General requirements for raw data

This message type includes the output data from digitizing transducers and digital instrument transformers independently from the transducer technology (magnetic, optic, etc.). The samples of current and voltage values need to be transferred from the transducer to the processing unit, i.e. typically to the protection IED. The line differential protection needs this data also across the line, i.e. from one side to the other side. To avoid any delay of protection caused by a delay of samples, the transfer time has to be according to the classes for the high speed messages as stated in 6.4.2.1.1 above. The difference to the binary messages is that these data consist not only of singular messages but of a continuous stream of synchronized samples from the source (sending IED).

Regarding phasors which are used by some functions alternatively to samples, the performance requirements regarding transfer time are the same. The difference is that the amount of data or messages in the data stream is lower compared to samples since phasors use for the angle definition normally more than one sample.

If the current and voltage values are transferred as analogue values over wires to the protection, their transfer time is the same for all voltage levels. The protection shall not be delayed by the data communication. Different transfer times, if applicable, have to be classified according to the classes for the high speed messages as stated in 6.4.2.1.1 above.

Analogue data have besides the transfer time additional features as amplitude resolution and sampling rate. The required transfer time for protection and control is:

4,0 ms acc. to Type 1A "Trip".

For digital communication beyond the substation, also transfer times ≤ 10 ms may be accepted according to the message performance class TR2. For other communication systems, also the less demanding classes TR3, TR4, etc. may be specified as long as the application function is able to work with these higher transfer times.

6.4.3.2.2 Additional requirements for time synchronisation for line differential protection

For comparing samples or phasors acquired at different places in different IEDs requires a synchronisation of these samples in µs range. The related classes are given in 6.4.3.4. This might also be a problem inside one substation which today is used with a pulse per second (pps) and in future over the IEC 61850 connections with IEEE 1588.

Table 4 – Change of transfer time and synchronisation method

Class	Acceptable change of transfer time (ΔT_A)	Applicable synchronisation method
TT1	0,2 ms	External signal synchronisation or self synchronisation (self synchronisation is outside scope of IEC 61850 because this method is not standardised)
TT2	10 ms	External signal synchronisation
TT3	20 ms	External signal synchronisation

The asymmetry of the communication path concerning transfer time between the IEDs on both sides of the line works similarly like the changes in transfer time and set some additional limits for self-synchronisation as specified as class TT1 in Table 4. If the asymmetry in the transfer times exceeds the acceptable change of class TT1 (0,2 ms), external synchronisation has to be applied.

6.4.3.3 Type 5 – File transfer functions

Not applicable for functions based on substation-substation communication.

6.4.3.4 Type 6 – Time synchronisation messages

6.4.3.4.1 General

Between substations the synchronisation takes place without dedicated time synchronisation messages as explained in 6.4.3.2.2. Nevertheless, the classes for time synchronisation according to IEC 61850-5 may be used if applicable.

6.4.3.4.2 Standard IED synchronizing for control and protection events

The performance classes for the time tagging of control and protection events are applicable according to Table 5.

Table 5 – Performance classes for time tagging of events

Time performance 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.

6.4.3.4.3 Standard IED synchronizing for instrument transformers

For instrument transformers, the time performance classes according to Table 6 are applicable.

Table 6 – Time performance classes for instrument transformer synchronisation

Time performance class	Accuracy µs
T3	± 25
T4	± 4
T5	± 1

6.4.3.5 Type 7 – Command messages with access control

Not applicable for functions based on substation-substation communication.

6.5 General requirements for data integrity

Integrity means that for given conditions of the communication link (e.g. signal to noise ratio for analogue links equivalent to the BER (bit error rate) for digital links), the resulting errors are below a certain acceptable limit. In IEC 61850-3, the three integrity classes according to IEC 60870-4 are referenced. Integrity was also introduced as PICOM attribute in 10.1.2 of IEC 61850-5 (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.

According to the CIGRE report *Protection using Telecommunications* [1], the accepted BER is as shown in Table 7.

Table 7 – The bit error rate as indication for communication quality

Protection type – communicated data	Condition	Limit for accepted BER
Distance protection – binary data	Normal	10^{-5}
Distance protection – binary data	Fault	10^{-4}
Differential protection – analog data	Normal	10^{-6}
Differential protection – analog data	Fault	10^{-5}

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 to minimize the impact of noise on the communication system;

b) apply an appropriate coding of telegrams to achieve the desired residual error rate;

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

The measures are outside the scope of IEC 61850-5 but the required data integrity should be considered in modelling the services (IEC 61850-7-2, e.g. SBO) and defining the mapping (IEC 61850-8-1, IEC 61850-9-1[4)], IEC 61850-9-2, e.g. coding).

6.6 Requirements for teleprotection – Reliability (security and dependability)

6.6.1 General

For the various protection schemes, the CIGRE report *Protection using Telecommunications* [1] addresses the requirements of protection on the teleprotection interfaces and the communication channels. The term “teleprotection” refers either to the line protection as such or to the equipment needed to interface the protection equipment to the telecommunication network. This subclause will focus on delivering protection traffic with the required security and dependability.

6.6.2 Security requirements for protection schemes according to CIGRE and IEC

“Security” *S* means the security against “unwanted commands” i.e. unwanted trips of protection if these are not requested by the protection scheme in the actual situation. If the probability for unwanted commands is P_{uc}, then the security is defined as

$$S = 1 - P_{uc}$$

4) Under consideration

The “security” requirements for protection schemes with telecommunications are declared in Tables 6-1-1 and 6-1-2 of the CIGRE report *Protection using Telecommunications* [1] as “medium” to “high” with a reference to IEC 60834-1. Figure 21 of IEC 60834-1 shows that P_{uc} should be less than 10^{-4} for blocking schemes down to 10^{-8} for inter-tripping schemes.

Therefore, the complete communication path including the protection application in the tripping IED shall allow for P_{uc} of lower than 10^{-8} to be usable for inter-tripping protection schemes. The split between the different contributing parts is a matter of modelling and functions allocation.

6.6.3 Dependability requirements for protection schemes according to CIGRE and IEC

“Dependability” D means the dependability against “missing commands” i.e. for protection missing trips if these are requested from the protection scheme in the actual situation. If the probability for missing commands is P_{mc}, then the dependability is defined as

$$D = 1 - P_{mc}$$

The “dependability” requirements for protection schemes with telecommunications are declared in Tables 6-1-1 and 6-1-2 of the CIGRE report *Protection using Telecommunications* [1] as “medium” to “high” with a reference to IEC 60834-1. Figure 21 of IEC 60834-1 shows that P_{mc} should be less than 10^{-2} for permissive under-reach schemes down to 10^{-4} for inter-tripping schemes. Figure 21 shows also that the “maximum actual transmission time” should be < 10 ms for all the protection schemes (see also 6.4.2.1.1.1 and 6.4.3.2.2 above).

Therefore, the complete communication path including the protection application in the tripping IED shall allow for >10 ms message-latency probability of lower than 10^{-4} to be usable for inter-tripping protection schemes. The split between the different contributing parts is a matter of modelling and functions allocation.

7 Considerations on security and dependability issues when using Ethernet networks

7.1 General

This clause highlights the specific issues of Ethernet networks, and provides solutions so substation networks can be engineered to guarantee the security and dependability required by applications for communication between substations.

7.2 Security of traffic

The 32-bit CRC field at the end of each Ethernet packet provides an “unwanted command” probability, from an error, 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. Breaking security from external needs some external access point to the communication system. The measures to be taken depend on the externally available access points to the communication system. If e.g. a power line carrier based WAN communication is used, access to the power line should be secure enough. If, additionally, the coupling into the substation communication level is physically secured, no externally available access points exist and no additional measures are needed. If however the coupling point between the WAN lines and the substation internal communication network is externally accessible, then security measures for authentication as described in IEC/TS 62351-6 are needed. As long as any other traffic as GOOSE and SMV is disabled at the entry port, no other measures are needed.

Two technologies are considered to restrict the access to the network either completely or to trusted partners:

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 with regard to which VLANs they will accept on each port. So assigning a VID used for protection only to those ports connected to the protection IEDs guarantees that the whole substation network can not be flooded with packets from this port.

b) Authentication
Security technologies are available that can “authenticate” the source of a received packet (reference to IEC 62351-6). This does not help against flooding, but assures that only messages from trusted partners are accepted and processed.
Though the complex processing of the authentification 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 reducing the flooding problem is recommended in any case.

7.3 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, for example 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
During a fibre failure, redundant networks like rings need to reconfigure.
Typical recovery times are: SONET < 60 ms, SDH < 50 ms, Ethernet spanning tree about 1 min, and Ethernet rapid spanning tree tens of milliseconds to a few seconds.
As long as this kind of event happens with a lower probability than 10^{-4}, it can be accepted, otherwise other architectures can be used, such as PRP from IEC 62439 or other solutions with faster recovery times.

7.4 Avoiding GOOSE packets flooding the WAN

GOOSE messages and sampled value messages are typically sent as multicast. These multicast messages are distributed by switches within the whole Ethernet segment, if their flow is not restricted. The most common means to configure flow restrictions is to configure VLANs (VIDs) between all IEDs which need a certain message or belong to a certain application working with this kind of messages. Another possibility is to use MAC level filtering, but this may be more difficult to set up in a WAN environment.

In the case that there is a direct Ethernet connection between substations, or the substation – substation messages are tunnelled between the substations, using different VIDs for substation internal traffic and substation – substation traffic is a common means to avoid this, even if this might mean that some data objects are sent in two different messages from the same IED.

7.5 Summary on recommendations for using Ethernet for communication between substations

7.5.1 General

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 should recover (restore traffic) from a fibre failure within 10 ms.

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.

d) 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.

e) 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).

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

7.5.2 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 1 518 byte packet takes 122 µs at 100 Mbit/s, 12 µs at 1 Gbit/s.

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

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 48 µs at 100 Mbit/s, 4,8 µs at 1 Gbit/s.

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

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 IEC 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 so that for traffic at a particular priority level (e.g. 16 priority levels with 8 queues), 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.

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 is typically transmitted using the GOOSE service from IEC 61850-7-2. If status information must be synchronised with the samples, they can be transmitted in the same message as the samples.

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.

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: most likely there will also be a dataflow in the opposite direction, or there will also be other functions exchanging data with each other. The example used below (see Figure 19) 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".

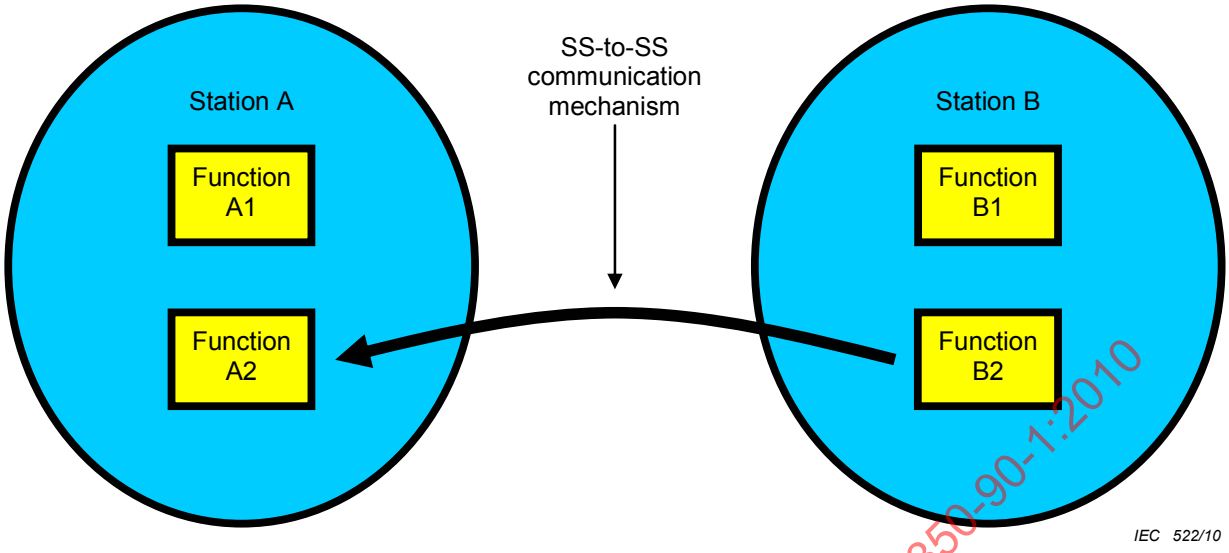


Figure 19 – Basic SS-to-SS communication structure

The scope of this technical 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:

a) tunnelling;

b) 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, see Figure 20.

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 (GOOSE and 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.

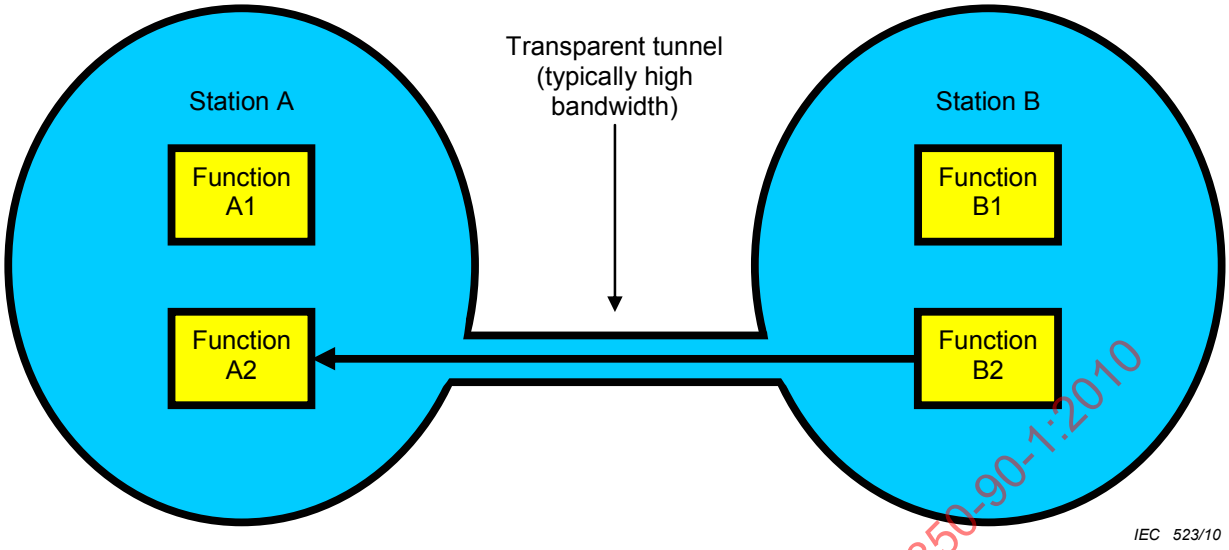


Figure 20 – SS-to-SS communication via tunnel

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".

8.2.3 Gateway

8.2.3.1 General

Gateways connect multiple substation networks by establishing "indirect access" to functions in remote stations. Gateways can be used if the communication link between substations does not fully support Ethernet communications, e.g. with power line carrier, copper, radio or PDH.

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 (see 8.2.3.2 and 8.2.3.3).

8.2.3.2 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 and because IEC 61850-7-4 anyhow forbids the use of GGIOs for data with known semantics, the GGIO gateway will not be further covered by this document.

8.2.3.3 Proxy gateway

The teleprotection equipment on the receiving side acts as a proxy for the function on the sending side, see Figure 21. 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.

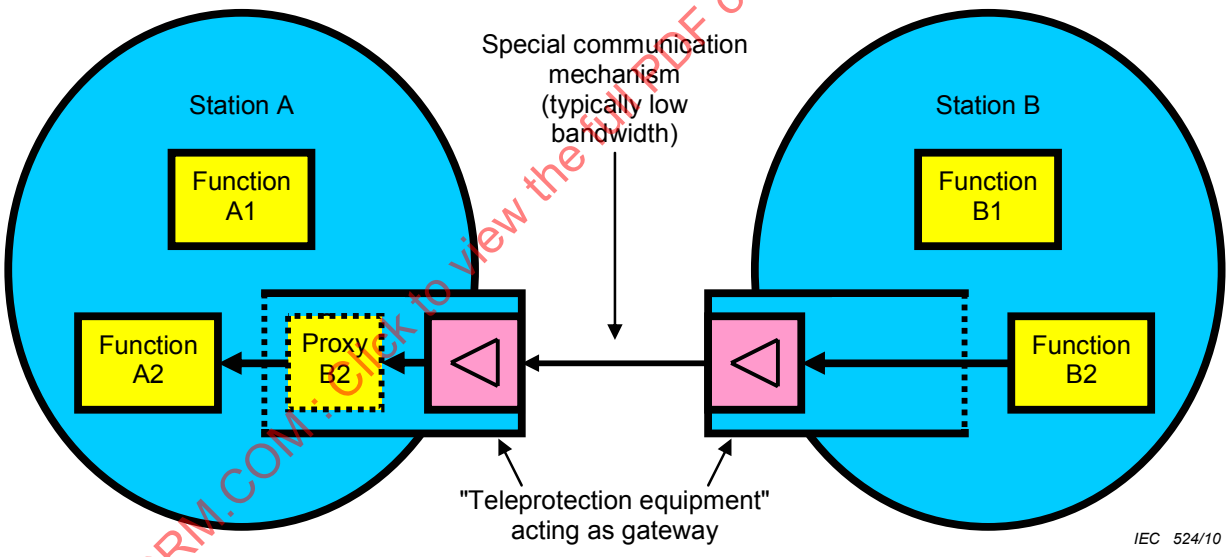


Figure 21 – SS-to-SS communication via proxy gateway

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. For example, 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 retransmissions 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.

9 Modelling

9.1 General architecture

In Figure 22, the general diagram for the gateway approach is illustrated. The basic philosophy for gateway approach and tunneling approach is to separate the supervision from

the function itself. This is illustrated in Figure 22 by the logical node ITPC for the channel supervision. Any communication failure is brought to the attention of the function by means of the data quality attribute.

The main difference between gateway approach and tunneling approach is for the second one that the proxy logical nodes do not exist (dashed proxys in Figure 22 do not exist with tunneling approach).

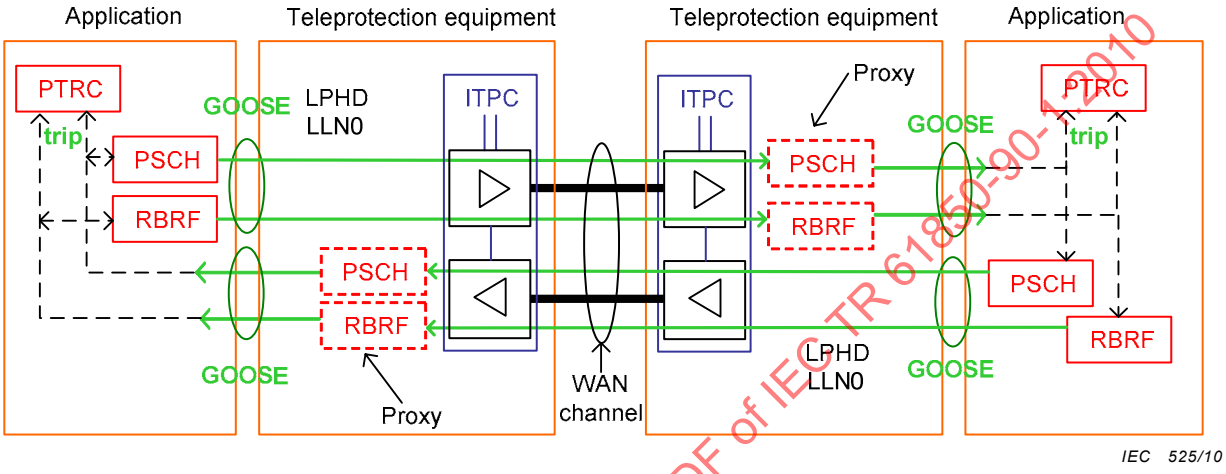


Figure 22 – Allocation of the LN ITPC representing the communication channel and the LNs providing the data to be exchanged between substations

In Clause 9, some use cases from Clause 5 are modelled as example according to IEC 61850. Other use cases, not mentioned in Clause 9, may be modelled accordingly. Other applications, not listed as use case in Clause 5, can also be modelled as long as they use the same approach.

9.2 Communication interface ITPC

The LN ITPC comprises all information for communication channel setting and supervision. ITPC 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. Table 8 shows the appropriate ITPC logical node class.

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 ITPC receives a GOOSE message with data object 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 (refer to Figure 22).

Table 8 – Logical node ITPC

ITPC class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22.		
Data objects				
EEHealth	ENS	External equipment health		O
EEName	DPL	External equipment nameplate		O
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
CarLev	MV	Power of received signal in case of an analogue communication channel		O
SigNsRat	MV	Signal to noise ratio (in dB), used in case of analogue communication		O
LoopTestTm	MV	Time measured at last loop test		O
Status information				
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
LosSig	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
LosSyn	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	ENG	Teleprotection application mode in transmit direction for each command (Unused, Blocking, Permissive, Direct, Unblocking, Status)		O
TpcRxMod1	ENG	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
BstRat	ASG	Level of increased power during the transmission of a command in dB. Used in case of an analogue communication channel		O
TxPwr	ASG	Transmit power (peak envelope power) in dBm. Used in case of an analogue communication channel		O
TxCtrHz	ASG	Transmit center frequency. Used in case of an analogue communication channel		O
RxCtrHz	ASG	Receive center frequency. Used in case of an analogue communication channel		O
TxBndWid	ASG	Transmit bandwidth. Used in case of an analogue communication channel		O
RxBndWid	ASG	Receive bandwidth. Used in case of an analogue communication channel		O

9.3 Communication-aided protection schemes and direct tripping

9.3.1 Proposed model

This model is applicable for the following use cases (according to Clause 5):

Distance line protection with permissive overreach 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, Figure 23 shows the relation between protection application and logical modelling according to IEC 61850.

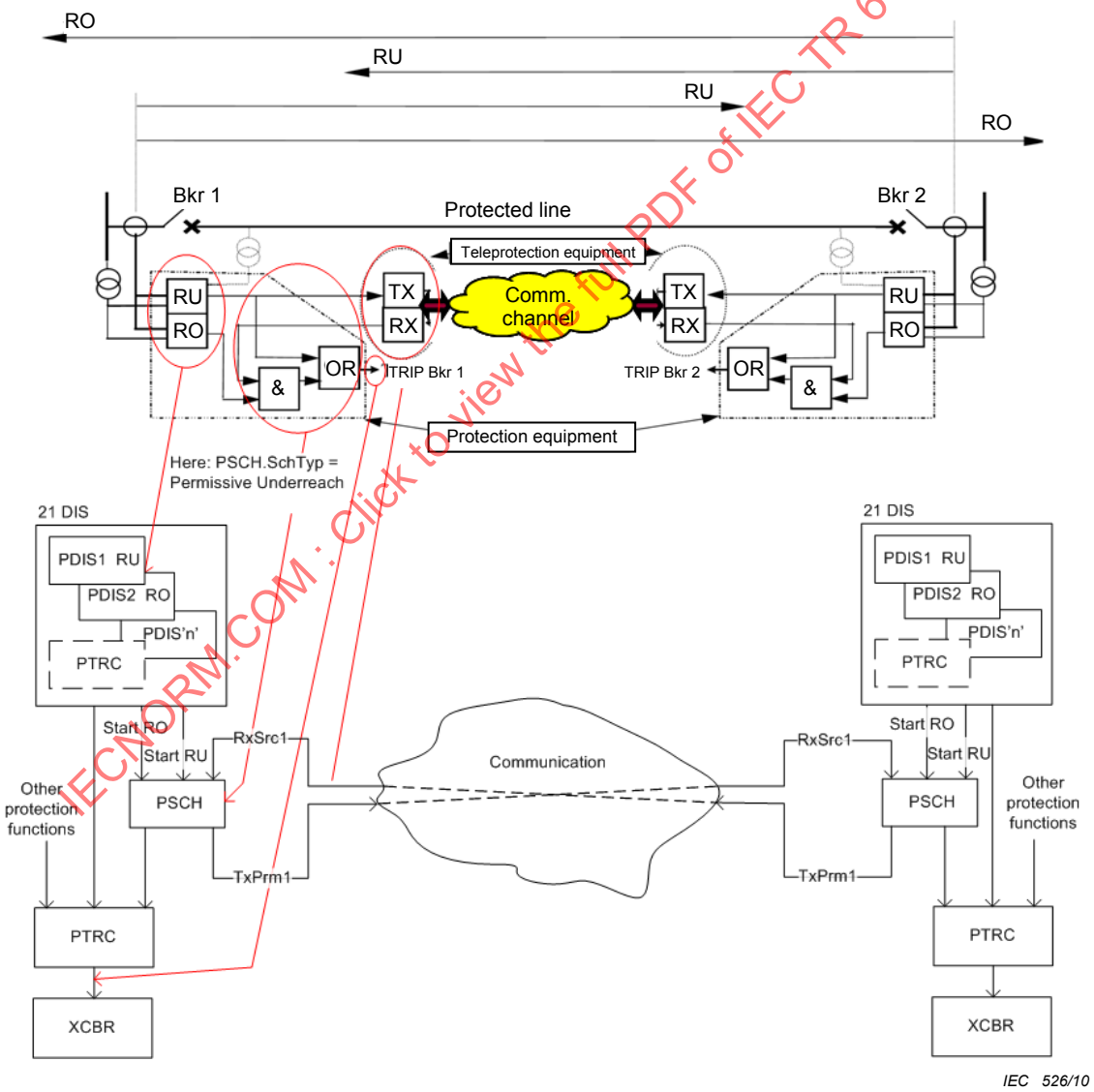


Figure 23 – Protection application example for permissive underreach distance teleprotection scheme and appropriate logical node modelling

9.3.2 LN PSCH

The logical node PSCH according to Table 9 shall be used to model the logical scheme for line protection function co-ordination.

Table 9 – Logical node PSCH

PSCH class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22.		
Data objects				
Status Information				
OpCntRs	INC	Resetable operation counter		O
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
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
EchoWei	SPS	TxPrm is being sent as echo signal or in case of weak end infeed	T	O
EchoWeiOp	SPS	Additional indication that Op is the operate from the weak end infeed or echo 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		O
WeiMod	ING	Mode of weak end infeed function		O
WeiTmms	ING	Co-ordination time for weak end infeed function		O

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 Figure 24 and Figure 25. Figure 24 is based on existing system. Figure 25 shows another system architecture approach.

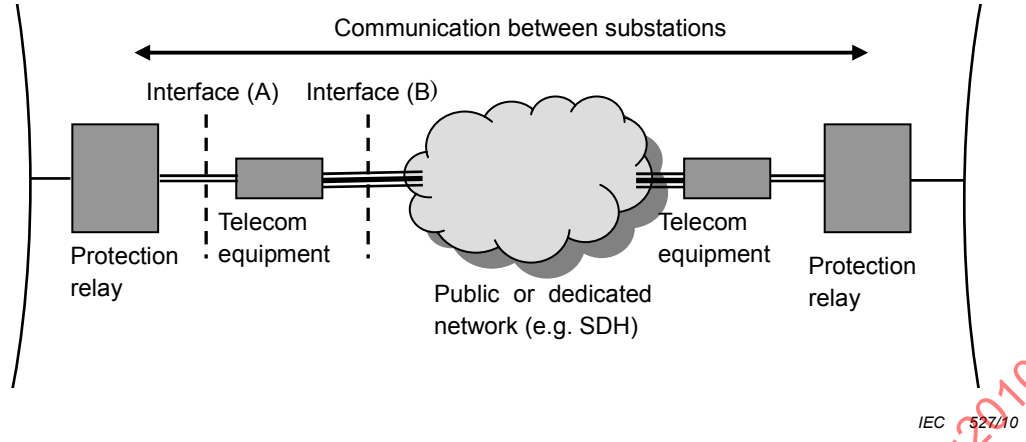


Figure 24 – Communication system based on current system

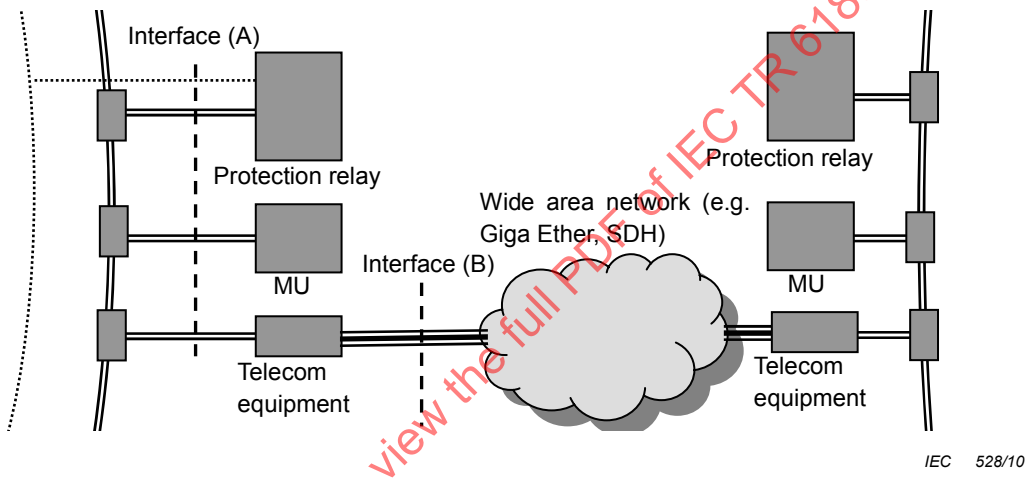


Figure 25 – Communication system based on future system

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 Figure 26 for a 2-terminal model and as Figure 27 for a 3-terminal model.

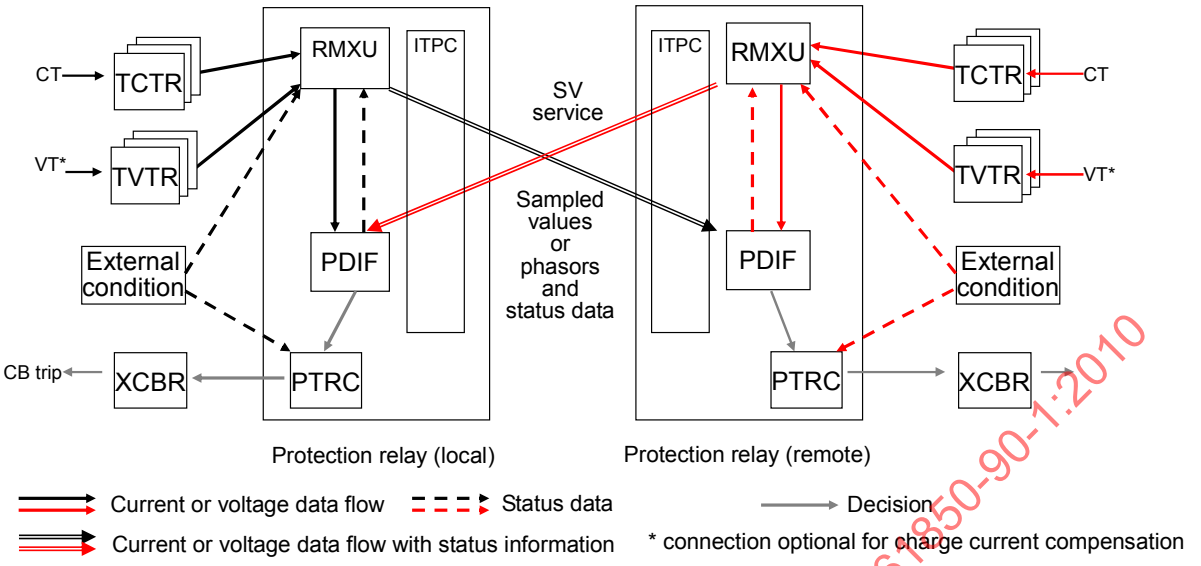


Figure 26 – Proposed 2-terminal current differential feeder protection relay model

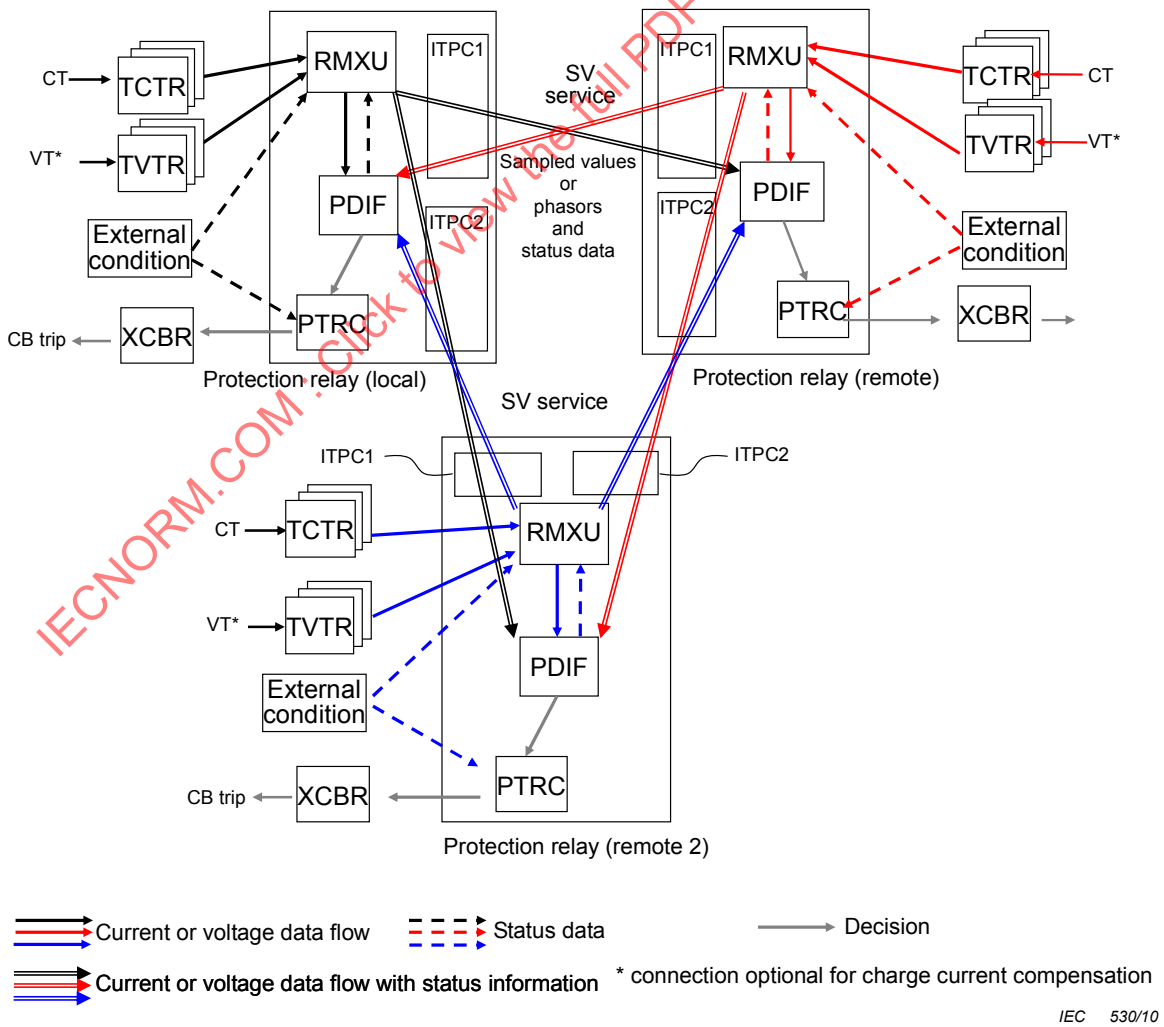


Figure 27 – Proposed 3-terminal current differential feeder protection relay model

9.4.2 LN RMXU

This technical report proposes the change of the logical node name from MDIF in IEC 61850-7-4 ed.1 (2003) to RMXU in IEC 61850-7-4 ed. 2. Compared to MDIF, the logical node RMXU needs to be modified as follows.

LN: Differential measurements Name: RMXU

This LN shall be used to provide locally calculated process values (phasors calculated out of samples or the samples itself) representing the local current values which are sent to the remote end and which are used for the local differential protection function (PDIF). Therefore, the LN RMXU together with LN PDIF models the core functionality of the differential protection function number 87 according to the IEEE designation (C37.2). In addition, the LNs RMXU on both sides of the line also represent the function of synchronizing the samples. Therefore, also the samples sent from the local TCTR to the local PDIF are routed through the function represented by RMXU. The local RMXU is therefore the source of synchronized samples or phasors from the local current sensor which sends its information to the local PDIF and to all required remote PDIF nodes. See Table 10.

Table 10 – Logical node RMXU

RMXU class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22.		
Data objects				
Measured Values				
ALoc	WYE	Current (phasor) of the local current measurement		C
AmpLocPhsA	SAV	Current (sampled value) of the local current measurement (Phase L1)		C
AmpLocPhsB	SAV	Current (sampled value) of the local current measurement (Phase L2)		C
AmpLocPhsC	SAV	Current (sampled value) of the local current measurement (Phase L3)		C
AmpLocRes	SAV	Current (sampled value) of the local current measurement (residual current)		O
Condition C: Either ALoc or AmpLocPhsA…AmpLocPhsC shall be used.				

9.4.3 SV format

As explained in previous subclause, SV will be able to transmit any attribute of any CDC. Thus, it can send phasor data as well as sampled values and status data as follows. See Table 11.